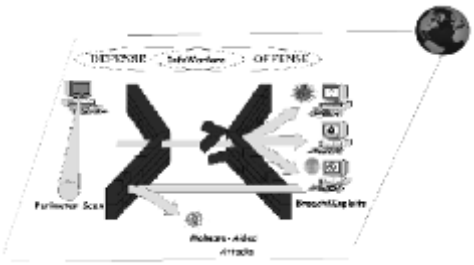
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

ΤΜΗΜΑ ΔΙΔΑΚΤΙΚΗΣ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ ΚΑΙ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

«Δικτυοκεντρικά Συστήματα»

Αυτοαναπαραγόμενο, κακόβουλο λογισμικό στην υπηρεσία της πληροφοριακής εχθροπραξίας



ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

ΑΛΕΞΑΝΔΡΟΥ Α. ΙΩΣΗΦΙΔΗ

Επιβλέπων : Σωκράτης Κάτσικας
Καθηγητής Πα.Πει.

Αθήνα, Μάρτης 2008

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ
ΤΜΗΜΑ ΔΙΔΑΚΤΙΚΗΣ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ
ΚΑΙ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
ΠΜΣ «ΔΙΚΤΥΟΚΕΝΤΡΙΚΑ ΣΥΣΤΗΜΑΤΑ»

Αυτοαναπαραγόμενο, κακόβουλο λογισμικό στην υπηρεσία της πληροφοριακής εχθροπραξίας

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

ΑΛΕΞΑΝΔΡΟΥ Α. ΙΩΣΗΦΙΔΗ

Επιβλέπων : Σωκράτης Κάτσικας
Καθηγητής Πα.Πει.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την / /2008.

(Υπογραφή)	*(Υπογραφή)*	*(Υπογραφή)*
.....	.....	.....
Σωκράτης Κάτσικας Καθηγητής Πα.Πει.	Χρήστος Ξενάκης Λέκτορας Πα.Πει.	Δημήτριος Γκρίτζαλης Αν. Καθηγητής Ο.Π.Α.

Αθήνα, Μάρτης 2008

(Υπογραφή)

.....

ΑΛΕΞΑΝΔΡΟΣ Α. ΙΩΣΗΦΙΔΗΣ

Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

Εξαιρετικά Αφιερωμένο

Στην Κυριακή Της Δικής μου ζωής,

Στη Μητέρα Και Παιδαγωγό μου Χρυσούλα,

Στον Πατέρα μου,

Στα Ξαδέλφια μου Ελένη Και Βασίλη,

Στον Παππού Και Τη Γιαγιά μου (δις).

Ακόμη,

Στην Ζωή Και Στον Βασίλη Που με Ζουν όσο Λίγοι·

Στον Δημήτρη Και Στον Άγγελο Που Δεν Βλέπω όσο θέλω·

Στην Λένα Και Στον Κώστα Για Την Ανιδιοτελή Αλληλεγγύη Τους

Και Για Τις Απαραίτητες άδειές μου·

Στον Φίλο, Συνάδελφο Και Συνεργάτη Δημήτρη

Και Στη Νεότευκτή Του Οικογένεια.

Περίληψη

Ο ανταγωνισμός και οι εχθροπραξίες για πόρους και αγαθά που εξασφαλίζουν τη δύναμη και την υπεροχή έχουν ανέκαθεν αποτελέσει χαρακτηριστικό, κινητήριο μοχλό των ανθρώπινων κοινωνιών, στην εξελικτική τους πορεία. Στη σύγχρονη, διεθνή, ψηφιακή κοινωνία, το στερεότυπο «η γνώση είναι δύναμη» έχει αποκτήσει ιδιαίτερη σημασία, καθώς το στρατηγικό πλεονέκτημα το έχουν πλέον εκείνοι που σπεύδουν να συλλέξουν και να επεξεργαστούν με τον καλύτερο τρόπο την εκάστοτε, δυνητικά χρήσιμη πληροφορία. Η πληροφορική τεχνολογία έχει οριοθετήσει σήμερα ένα εντελώς καινούριο πεδίο μάχης, με τα δικτυοκεντρικά, πληροφοριακά συστήματα να δεσπόζουν, ταυτόχρονα ως θησαυροφυλάκια γνώσης, αλλά και ως απόρθητα φρούρια. Η πληροφοριακή εχθροπραξία έρχεται ως συνέπεια του πληροφοριακού ανταγωνισμού της εποχής μας με τους επίδοξους πορθητές εκτός των άλλων να «κραδαίνουν» πολυμορφικούς ιούς και σκουλήκια Warhol, να στέλνουν «δούρειους ίππους» και να ανοίγουν «κερκόπορτες» στα συστήματα. Ο στόχος του επιτιθέμενου δεν έχει αλλάξει αιώνες τώρα· υποβάθμιση, κατασκοπεία, υποταγή-έλεγχος, καταστροφή του αντιπάλου. Ο στόχος του αμυνόμενου ήταν πάντοτε η οχύρωση-πρόληψη, η επισκόπηση-διάγνωση και η έγκαιρη αντιμετώπιση της επίθεσης. Η μάχη καλά κρατεί και οι ρόλοι συχνά, αν όχι εναλλάσσονται, είναι συγκεχυμένοι. Η επιτυχημένη διάδοση του Διαδικτύου και του προσωπικού Η/Υ, οι υπηρεσίες ιστού και τα δικτυοκεντρικά συστήματα, το κακόβουλο λογισμικό, η διεθνής τρομοκρατία και το οργανωμένο έγκλημα, οι διακρατικές σχέσεις και το δίπολο πολίτης-Κράτος, όλα προσθέτουν στο μωσαϊκό του πληροφοριακού πολέμου. Η διπλωματική αυτή εργασία μελετά και αποπειράται να εκτιμήσει τη δυναμική της τεχνολογίας του κακόβουλου, αυτοαναπαραγόμενου, ιομορφικού ή μη, λογισμικού στην ευρύτατη προσπάθεια διεμβολισμού των πληροφοριακών κάστρων. Ταυτόχρονα, εξετάζονται εμπεριστατωμένα οι διάφορες, αμυντικές τεχνοτροπίες -τόσο τρέχουσες, όσο και θεωρητικές- για την ασφάλεια και την προστασία των πληροφοριακών συστημάτων από επιθέσεις με αυτοαναπαραγόμενο λογισμικό. Επιχειρείται δε η ανάδειξη βέλτιστων πρακτικών, τόσο για τον εισβολέα όσο και για τον υπερασπιστή των συστημάτων. Συζητώνται, τέλος, οι πιθανές συνέπειες, η κοινωνική διείσδυση και ο ευρύτερος, συνολικός αντίκτυπος από τις εκτεταμένες εχθροπραξίες, καθώς και τα αναγκαία πεδία ανάληψης της απαιτούμενης πλέον, ισχυρά προστατευτικής και εποικοδομητικής, παγκόσμιας δράσης.

Λέξεις Κλειδιά: <<πληροφοριακή εχθροπραξία, δικτυοκεντρικά συστήματα, αυτοαναπαραγόμενο, κακόβουλο λογισμικό>>.

Abstract

Competition and warfare for goods and resources, that ensure power and superiority, has always been a distinctive moving force for human societies, throughout their evolutionary process. In modern, transnational, digital society, the "knowledge means power" motto has become of particular significance, as the strategic advantage lies with the party who heads first to optimally collect and process potentially valuable information. Information technology has nowadays defined the borders of an entirely new battlefield, with network-centric information systems dominating as both knowledge repositories and invincible fortresses. Information warfare comes as a consequence of our era's informational competition with aspirant conquerors wielding polymorphic viruses and Warhol worms, sending Trojan Horses and opening backdoors inside systems. The attackers' goals haven't historically changed; subversion, espionage, submission-control, destruction. The defenders' goals samewise; it has been always about fortification-prevention, monitoring-detection and proper reaction to the attack. Battles wage on and the roles are often blurred, if not alternating. The successful spreading of personal computing and the Internet, web services and netcentric systems, malicious software, global terrorism and organized crime, international relationships and the citizen-State dipole, all add to the mosaic of information war. This M.Sc. Thesis' subject of study, analysis and evaluation is the potential self-reproducing malware -whether viral or not- has in the widespread effort of ramming information castles. In the same time, various defending technologies, whether state-of-the-art or evangelized, for security and protection of systems against self-replicating software attacks, are thoroughly examined. Finally, possible consequences, social implications and the general, broad impact large-scale warfare has, as well as the required fields for today's necessary, strong safe-guarding and edification global action, become topics of discussion.

Keywords: <<information warfare, network-centric systems, self-replicating malware>>.

Πίνακας περιεχομένων

1 Εισαγωγή

1.1 Επιβλαβές, αυτοαναπαραγόμενο λογισμικό: οπλικά συστήματα πληροφοριακής εχθροπραξίας

«Η γνώση είναι δύναμη»[1] λέει η γνωστή ρήση σε μια προσπάθεια να αποτυπωθεί η καθοριστική σημασία της κατοχής χρήσιμων πληροφοριών σε κάθε τομέα εναλλαγής της υπεροχής, σε κάθε ανταγωνιστική έκφραση της κοινωνικής ζωής.

Ο Κινέζος στρατηγός του 6ου π.Χ. αιώνα Sun Tzu έγραφε σχετικά στο περιώνυμο βιβλίο του "Η Τέχνη του Πολέμου"[2]*:*

"*Αν γνωρίζεις τον εχθρό και τον εαυτό σου, δε χρειάζεται να αμφιβάλλεις για το αποτέλεσμα 100 μαχών. Αν ξέρεις τον εαυτό σου, αλλά όχι τον εχθρό, για κάθε σου νίκη θα υποστείς και μια ήττα. Αν δεν γνωρίζεις ούτε τον εχθρό αλλά ούτε και τον εαυτό σου, θα υποκύπτεις σε κάθε μάχη*".

Ο μακρινός «απόγονός» του Sung Moo Yang, ερευνητής στην ασφάλεια πληροφοριακών συστημάτων Η/Υ, το 1996 προαναγγέλλει-προβλέπει την έλευση αυτόνομων, κινητών κυβερνο-όπλων (autonomous, mobile cyberweapons) κακόβουλης φύσης, με δυνατότητες αποτελεσματικής μετακίνησης από μια πηγή και εξάπλωσης σε προορισμούς-στόχους, όπου εδρεύουν κρίσιμες πληροφορίες ή πληροφοριακά συστήματα, και εκτέλεσης πολύπλοκων

[1] Sir Francis Bacon, "Meditationes Sacrae", 1597 μ.Χ.

[2] Sun Tzu, "The Art of War", ~512 π.Χ.

αποστολών και εργασιών και μάλιστα με τρόπο πιο αποδοτικό από τις μέχρι τότε επιθέσεις κυβερνο-στρατιωτών (cybersoldiers) χάκερ[3]. Ουσιαστικά, ο Yang προσυπογράφει το πρελούδιο της εποχής των πληροφοριακών εχθροπραξιών με χρήση αυτοαναπαραγόμενου, κακόβουλου λογισμικού.[4]

Σήμερα, χώροι, όπως ο στρατιωτικός, ο ιατρικός, ο δικαστικός, ο κυβερνητικός και σχεδόν ο πάσης φύσης επιχειρηματικός, στηρίζονται σε μια πληθώρα διασυνδεδεμένων δικτύων επικοινωνιών, δεδομένων και κατά μείζονα λόγο υπολογιστών. Πάνω στα δίκτυα αυτά έχουν στηθεί άλλα δίκτυα αλληλεπίδρασης με τον άνθρωπο, τα λεγόμενα «δίκτυα πληροφόρησης» ή πληροφοριακά συστήματα, σύγχρονες αποθήκες και κοιτίδες ακατέργαστης ή επεξεργασμένης γνώσης. Ορισμένες από τις πληροφορίες που φυλάσσονται στα συστήματα αυτά αποτελούν ζωτικής σημασίας μυστικά και «ευαίσθητα» δεδομένα, που αν πέσουν στα λάθος χέρια, το κόστος μπορεί να αποβεί ολέθριο και όχι μόνο για τους αρχικούς ιδιοκτήτες. Όπως γίνεται εύκολα αντιληπτό, καθημερινά τέτοιου είδους πληροφορίες και τοποθεσίες γίνονται στόχοι επίθεσης και χώροι ευρύτερων διαξιφισμών μεταξύ αντιμαχόμενων ατόμων και ομάδων, που προσπαθούν να κερδίσουν σε γνώση εις βάρος του όποιου αντιπάλου.

Μέχρι τώρα, οι επιθέσεις στηρίζονται σε μεγάλο βαθμό (ικανότητα-επιδεξιότητα) στον ανθρώπινο παράγοντα (επιτιθέμενο κυβερνο-χάκερ & αμυνόμενο κυβερνο-στρατιώτη ή απλό χρήστη ή ενδιάμεσες διαβαθμίσεις αυτών) και κατόπιν σε λογισμικό και υλικό επίθεσης (κυβερνο-όπλα) και αμυντικής οχύρωσης (μηχανισμοί προστασίας). Η δυναμική, όμως, του αυτοαναπαραγόμενου, κακόβουλου λογισμικού (ως κυβερνο-όπλου) στην ενίσχυση και αυτοματοποίηση της εντεινόμενης, πληροφοριακής διαμάχης και μάλιστα υπό το πρίσμα της δικτυακής εκδοχής της παγκοσμιοποίησης (*sic*), του πασίγνωστου δηλαδή Διαδικτύου, και της ολοένα και μεγαλύτερης ενοποίησης-διεπικοινωνίας-ολοκλήρωσης συστημάτων που διαρκώς επιφέρει, έχει εδώ και καιρό διαφανεί και (πρέπει πλέον να) αποτελεί ένα φλέγον ζήτημα έρευνας, προβληματισμού και ευαισθητοποίησης, τόσο για τους επιστήμονες πληροφορικής και ασφάλειας πληροφοριακών συστημάτων, όσο και για ολόκληρη την κοινωνία, λόγω των διευρυμένων προβλημάτων που δύναται να επισύρει.

1.2 Αντικείμενο διπλωματικής

Ανέκαθεν το τρίπτυχο πληροφόρηση, γνώση και δύναμη διαδραμάτιζε καθοριστικό ρόλο στην έκβαση κοινωνικών, οικονομικών, πολιτικών και πολεμικών μαχών. Έθνη, επιχειρήσεις

[3] Κύρια, βιβλιογραφική αναφορά: [YANG-AMCW].

[4] Πηγή: "AMCW - A New Weapon for the New Millennium", Sung Moo Yang, 1999, διαθέσιμο από το δεσμό http://vx.netlux.org/lib/asy04.html.

και μεμονωμένα άτομα αναζητούν την αύξηση, αποτελεσματικότερη προστασία και καλύτερη εκμετάλλευση των δικών τους πληροφοριών, ενώ παράλληλα προσπαθούν να περιορίσουν κατά το δυνατόν ή να αποκτήσουν, με τον ένα ή τον άλλον τρόπο, τις πληροφορίες που διαθέτουν οι αντίπαλοι, με ξεκάθαρο στόχο την επίτευξη στρατηγικού πλεονεκτήματος δράσης.

Από το 1960 και έπειτα, η ανθρωπότητα έγινε μάρτυρας μιας θριαμβευτικής, τεχνολογικής ανάπτυξης στους τομείς της συλλογής, μετάδοσης, προστασίας, αποθήκευσης και ανάλυσης δεδομένων, που επέτρεψαν την πολύπλευρη εκμετάλλευση τους στο πληροφοριακό πεδίο.[5] Δίκτυα ηλεκτρονικών υπολογιστών διασυνδέουν σήμερα από άκρο σε άκρο οργανισμούς και χώρες ολόκληρες και πληροφοριακά συστήματα «ζωντανεύουν» και αλληλεπιδρούν μεταξύ τους στη βάση αυτής της υποδομής, σε μια παγκόσμια προσπάθεια παροχής υπηρεσιών και διακίνησης πληροφοριών, που ξεπερνά χωροχρονικά δεσμά αιώνων. Η επιθυμία για έλεγχο των πληροφοριών και δη των «ευαίσθητων» και κρίσιμων περνά πλέον υποχρεωτικά και μέσα από την προστασία ή εκπόρθηση των σύγχρονων αυτών φρουρίων, που εμφανίζονται με χαρακτηριστικό και κυριότερο εκπρόσωπο του είδους τα δικτυοκεντρικά, πληροφοριακά συστήματα Η/Υ.

Η τεχνολογία λογισμικού, βάση και «ζωοποιός δύναμη» του ηλεκτρονικού υπολογιστή, παρέχει και τον τρόπο για κακόβουλη χαλιναγώγησή του και το κάθε λογής ιομορφικό ή άλλης μορφής, επιβλαβές λογισμικό το έχει αποδείξει σχεδόν τρεις δεκαετίες τώρα[6]. Οι ιοί και τα σκουλήκια συνήθως μοιάζουν μικρές ενοχλήσεις στο οικιακό περιβάλλον του προσωπικού υπολογιστή, μπορούν όμως να αποδειχθούν ιδιαιτέρως επικίνδυνα όπλα στα χέρια επιτήδειων, που έχουν σκοπό μια επίθεση με στόχο το δείνα πληροφοριακό σύστημα, με δεδομένα ζωτικής σημασίας, όπως λόγου χάριν ιατρικούς φακέλους, αποσπάσματα από συνομιλίες, οικονομικούς δείκτες, φαρμακευτικές συνταγές, σχέδια βιομηχανικών πρωτοτύπων, ακόμη και απόρρητες στρατιωτικές θέσεις. Ήδη από το 1991 και κατά τη διάρκεια του Πολέμου του Περσικού Κόλπου, Ολλανδοί χάκερς κατάφεραν να παρεισφρύσουν, με τη βοήθεια ιομορφικού λογισμικού, στα τερματικά του αμερικανικού Πενταγώνου και να υποκλέψουν πληροφορίες για τις θέσεις των στρατευμάτων των ΗΠΑ[7]. Σε μια παρόμοια ιστορία, το Γενάρη του 1999 τα τερματικά της αμερικανικής αεροπορίας

---

[5] Από την 3η γενιά της ψηφιακής επεξεργασίας (digital computing) και τις πρώιμες -στρατιωτικού κυρίως ενδιαφέροντος- απόπειρες δικτύωσης έως το σημερινό state-of-the-art στην πληροφορική τεχνολογία.

Ενδεικτικές Πηγές: Διαδίκτυο, http://www.screensite.org/courses/Jbutler/T389/ITHistoryOutline2.htm και http://www.mantex.co.uk/ou/t171/t171-07.htm.

[6] Πηγή: Διαδίκτυο ιστοχώρος της online εγκυκλοπαίδειας WikiPedia, http://en.wikipedia.org/wiki/Timeline_of_notable_computer_viruses_and_worms.

[7] Πηγή: "Information Warfare: What Is It Good For?", Simson Garfinkel, 2003, διαθέσιμο από το δεσμό http://www.csoonline.com/read/060103/shop.html.

«χτυπήθηκαν» από συντονισμένα, κακόβουλα πυρά ρωσικής προέλευσης[8]. Σε μια άλλη πτυχή του ίδιου προβλήματος, το σκουλήκι με κωδική ονομασία Zotob δημιουργεί το 2005 εκτεταμένες βλάβες και οχλήσεις σε πολλά υπολογιστικά συστήματα παγκοσμίως, ανάμεσα στα οποία μάλιστα ξεχωρίζουν και εκείνα του δημοφιλούς δικτύου μαζικής ενημέρωσης CNN[9], καθιστώντας δύσκολη την καλή λειτουργία του. Όπως γίνεται κατανοητό, οι πληροφοριακές εχθροπραξίες είναι αδιαμφισβήτητο γεγονός και το αυτοαναπαραγόμενο, κακόβουλο λογισμικό αναδεικνύεται σε ένα μέσο επιτυχημένης επίθεσης κατά των πληροφοριακών συστημάτων δικτυωμένων Η/Υ. Ποιες οι πιθανές δυνατότητες και τα όρια αυτής της τεχνολογίας είναι προς το παρόν άγνωστο, αλλά τολμηρές εξερευνήσεις έχουν ορίσει δυναμικά το χαρακτήρα του παρόντος και θα καθορίζουν σε μεγάλο βαθμό και τη μέλλουσα πορεία του αυτοαναπαραγόμενου, επιβλαβούς λογισμικού. Ποιες θα είναι οι ενσαρκώσεις μελλοντικών επιθέσεων, μπορεί κανείς μόνο να εικάζει, να προετοιμάζεται και να περιμένει.

Καταλύτης στην εξάπλωση τέτοιου τύπου επιθέσεων στα σημερινά, πληροφοριακά συστήματα με παρουσία υπολογιστών, η ίδια η ευρύτατη διάδοση του προσωπικού υπολογιστή στην ανθρώπινη ζωή και πραγματικότητα, σε συνδυασμό με την καθημερινή, άνετη πρόσβαση στο Διαδίκτυο και την ιδιαίτερη, τεράστια αποδοχή που αυτό παρουσιάζει. Ουσιώδους σημασίας πληροφοριακά συστήματα «αναγκάζονται» ή «πείθονται», στις μέρες μας, να αποτελούν κόμβους αυτού του δικτύου των δικτύων υπολογιστών του πλανήτη και να είναι δυνητικά προσβάσιμα από παντού στον κόσμο χάριν παγκόσμιας διάχυσης και ανταλλαγής υπηρεσιών και πληροφοριών.

Τα προαναφερόμενα σημεία των καιρών, πέρα ίσως από συναρπαστικά ως σενάρια ταινιών επιστημονικής φαντασίας αποτελούν μια εξακριβωμένη, καθημερινή πραγματικότητα τόσο για τον απλό πολίτη και την επιχείρηση, όσο και για πιο πολυσύνθετες δομές όπως κρατικοί οργανισμοί. Για το λόγο αυτό εκτεταμένη έρευνα εκπονείται και προσπάθεια καταβάλλεται στην κατεύθυνση της ασφάλειας των δικτυοκεντρικών συστημάτων, με κύριους φορείς τη βιομηχανία λογισμικού, τους κατασκευαστές υλικού, τις ομάδες εργασίας διαχείρισης και τυποποίησης πρότυπων, συναφών κωδίκων (όπως κανόνων/οδηγιών ασφάλειας, πρωτοκόλλων επικοινωνίας, θεσμικών μέτρων και προτάσεων), τις εξειδικευμένες, συμβουλευτικές εταιρίες που δρουν και ειδικεύονται στο χώρο, τους σχετικούς, ακαδημαϊκούς κύκλους, αλλά και τα διάφορα, νομικά και εκτελεστικά όργανα των κρατών. Αρμόδια στελέχη οργανισμών και επιχειρήσεων ασχολούνται με την κατάστρωση, επίβλεψη

[8] Πηγή: Διαδίκτυο, ιστοχώρος της online παρουσίας του παγκόσμιου βελγικού δικτύου ενημέρωσης CNN, http://www.cnn.com/TECH/computing/9903/05/pentagon.hackers/index.html.

[9] Πηγή: Διαδίκτυο, ιστοχώρος της online παρουσίας του παγκόσμιου βελγικού δικτύου ενημέρωσης CNN, http://www.cnn.com/2005/TECH/internet/08/16/computer.worm/index.html.

και διατήρηση της περιμέτρου ασφάλειας των ιδικών τους συστημάτων. Ακόμη και ο απλός, διαδικτυακός χρήστης εξοπλίζεται πλέον με πάσης φύσεως αμυντικές λύσεις για να εξασφαλίσει μια κατά το δυνατόν λιγότερο επικίνδυνη, πληροφοριακή περιήγηση, αρχής γενομένης από τις σελίδες και τους χώρους του Παγκόσμιου Ιστού. Η γενικότερη ασφάλεια των Η/Υ και ιδιαίτερα σε δικτυακό περιβάλλον και ειδικότερα η προστασία από το επιβλαβές λογισμικό παρουσιάζεται σαν μια διαρκής, δύσκολη πάλη, χωρίς περιθώρια εφησυχασμού.

Τα παραπάνω αποτελούν μια σύνθετη προβληματική, που εκτυλίσσεται στο προσκήνιο και το παρασκήνιο της Πληροφορικής, αλλά χρήζει του ενδιαφέροντος και της μελέτης από όσο το δυνατόν περισσότερες, πολυποίκιλες και πολυπρόσωπες ομάδες κοινωνικής δράσης και όχι μόνο από επαγγελματίες ή επιστήμονες της Πληροφορικής. Οι εν δυνάμει εκδηλώσεις και επιπτώσεις από τις πληροφοριακές μάχες αγγίζουν όλα τα επίπεδα της κοινωνικής ζωής και ο αντίκτυπός τους μπορεί να γίνει παγκοσμίως αισθητός. Όλα αυτά συνιστούν μια ξεχωριστή σφαίρα αναγκαίας και χρήσιμης έρευνας, επισκόπησης, αναζήτησης και θεμελίωσης θέσεων και συμπερασμάτων ικανών να απεικονίσουν πιστά την τρέχουσα πραγματικότητα, να αναγνωρίσουν τις όψιμες τάσεις, να επισημάνουν την κοινωνική διάσταση και διείσδυση της εχθροπραξίας στο πληροφοριακό πεδίο και να περιγράψουν τις απαραίτητες, συλλογικές δράσεις και πρωτοβουλίες, που θα εγγυώνται την ευρύτερη προστασία και ασφάλεια.

Στα πλαίσια αυτής της διπλωματικής εργασίας, θα μελετηθούν τα επιμέρους θέματα, που τέθηκαν στην πρότερη, εισαγωγική ανάλυση, με τη συνδρομή της τρέχουσας βιβλιογραφίας και επιστημονικής διανόησης και θα αναζητηθούν πορίσματα και συμπεράσματα πάνω στα καίρια ερωτήματα, τα οποία και θα καταγραφούν ως παρακαταθήκη της ερευνητικής διαδικασίας και της συγγραφικής προσπάθειας.

Στόχος της παρούσας διπλωματικής είναι η ενδελεχής εντρύφηση-εξέταση των ενεργητικών και παθητικών μεθόδων και τεχνικών επίθεσης σε δικτυοκεντρικά, πληροφοριακά συστήματα Η/Υ, με φορέα-εκτελεστικό όργανο αποκλειστικά το αυτοαναπαραγόμενο, κακόβουλο λογισμικό και η διερεύνηση της τρέχουσας βιβλιογραφίας και επιστημονικής σκέψης, σχετικά με τους βέλτιστους τρόπους αντιμετώπισης (πάνω στο γνωστό μοτίβο πρόληψη, διάγνωση, θεραπεία) των επιθέσεων αυτών. Σαν επιμέρους στόχος τέθηκε η απομόνωση και ανάδειξη πρακτικών προτάσεων για τη λήψη μέτρων από πλευράς της παγκόσμιας κοινότητας για την ευρύτερη προστασία των μελών της από την κλιμακούμενη και ολοένα διογκούμενη, πληροφοριακή εχθροπραξία.

1.2.1 Σκοπός-Συνεισφορά

Σκοπός της τρέχουσας εργασίας είναι η πιστότερη και πολύπλευρη παρουσίαση του υπό διερεύνηση θέματος και η ανάδειξή του ως μείζον, με ελπίδα και γνώμονα μια καλύτερη

ενημέρωση να παράγει περισσότερη ευαισθητοποίηση και εγρήγορση για ανάληψη συλλογικής, θετικής, ουσιαστικά προστατευτικής δράσης. Για το λόγο αυτό η άντληση της βιβλιογραφικής πληροφορίας γίνεται από πηγές και των δύο αντίπαλων ρευμάτων, τόσο δηλαδή των θιασωτών του κακόβουλου λογισμικού, όσο και των πολεμίων του. Σύμμορφα με το σκοπό της εργασίας κινείται και η διασταύρωση κάθε βιβλιογραφίας από περισσότερες των μία πηγών και ειδών πηγών, όπου αυτό είναι δυνατόν (έντυπα και ηλεκτρονικά μέσα-βιβλίο, επιστημονικό περιοδικό, συνέδριο, πανεπιστημιακού επιπέδου εκπαιδευτικό υλικό, εγχώρια και διεθνής έρευνα).

Η *συνεισφορά της διπλωματικής* συνοψίζεται ως εξής:

1. Μελετήθηκαν οι διάφορες τεχνοτροπίες εισβολής και επιβουλής των δικτυοκεντρικών συστημάτων με χρήση επιβλαβούς, αυτοαναπαραγόμενου λογισμικού.
2. Σκιαγραφήθηκε η μελλοντική δυναμική της κακόβουλης -ιομορφικής και μη- απειλής στον πληροφοριακό πόλεμο στη βάση τεχνολογιών αιχμής στη συγγραφή λογισμικού και την κατασκευή υλικού.
3. Κατηγοριοποιήθηκε το αυτοαναπαραγόμενο, κακόβουλο λογισμικό με βάση την επιτυχία και την ικανότητά του σε πληροφοριακές εχθροπραξίες.[10]
4. Συζητήθηκαν τα πλεονεκτήματα και τα δυνατά σημεία, καθώς και τα μειονεκτήματα και οι ελλείψεις των περισσότερων τρεχόντων και κάποιων εκ των υπό μελέτη σχημάτων ασφάλειας των πληροφοριακών συστημάτων, όσον αφορά την προστασία από επιθέσεις επιβλαβούς, αυτοαναπαραγόμενου λογισμικού. Απομονώθηκαν ορισμένες, καινοτόμες τεχνολογίες που αφήνουν ισχυρές υποθήκες και υποσχέσεις για ένα ευοίωνο μέλλον.
5. Τονίστηκαν οι πιθανές συνέπειες της πληροφοριακής εχθροπραξίας και προτάθηκαν στοχευμένες δράσεις κοινωνικής προστασίας.

Τα σημεία 3, 5 ενέχουν θέση θεωρητικών προτάσεων εν είδη γενικότερων συμπερασμάτων κατόπιν διερεύνησης της σχετικής επιστημονικής σκέψης και η ανάπτυξη των αντίστοιχων τμημάτων της εργασίας γίνεται με κατά το δύνασθαι αντικειμενικό και συνάμα συνοπτικό χαρακτήρα, σε σύγκριση με τα αντίστοιχα εκτενέστερα τμήματα επισκόπησης-παράθεσης της βιβλιογραφίας 1, 2 και 4. Τα 3, 5 αντικατοπτρίζουν την προσπάθεια σχηματισμού και

[10] Η ταξινόμηση αυτή έχει στηριχτεί σε μεγάλο βαθμό σε πρωτογενείς διαπιστώσεις του συγγραφέα από τη σχετική και σκοπίμως πολυσυλλεκτική, θεματική ενδοσκόπηση (βλέπε και επόμενη σημείωση) και η αντικειμενική ευστάθειά της παραμένει εν πολλοίς ανεξακρίβωτη.

απόδοσης γόνιμων και ιδανικά πρωτογενών πορισμάτων, με βάση τη βιβλιογραφική επισκόπηση, και ενδέχεται συνεπώς αναπόφευκτα να απηχούν και ορισμένες υποκειμενικές θέσεις του συγγραφέα, που διαθέτουν μολαταύτα επαρκή τεκμηρίωση/αιτιολόγηση.[11]

1.3 Οργάνωση κειμένου

Η εργασία διαρθρώνεται λογικά σε 7 κεφάλαια (και ένα 8ο ειδικά φυλαγμένο για τις βιβλιογραφικές αναφορές):

Κεφάλαιο 1. Εισαγωγή

Ο αναγνώστης εισάγεται στην προβληματική και τη σκοπιμότητα της εργασίας μέσα από μια σύντομη ματιά στις πτυχές της καθημερινότητας, πάνω στις οποίες και εξυφαίνεται το ζήτημα της πληροφοριακής εχθροπραξίας με χρήση επιβλαβούς, αυτοαναπαραγόμενου λογισμικού. Θέτονται ένα-ένα τα επιμέρους θέματα προς διερεύνηση και παρουσιάζεται η δομική της υπόσταση.

Κεφάλαιο 2. Επιστημονικό Υπόβαθρο

Στο κεφάλαιο αυτό προσοχή δίνεται στην ολόπλευρη παρουσίαση θεμάτων με ουσιώδη βαρύτητα για την κατανόηση του πεδίου της πληροφοριακής εχθροπραξίας με αυτοαναπαραγόμενο, κακόβουλο λογισμικό. Έτσι, μετά από μια σκιαγράφηση της ψηφιακής μας εποχής και μια περιγραφή του αντικειμένου, των στόχων και των αντιπροσωπευτικών μέσων της ασφάλειας πληροφοριών, δίνεται η ευκαιρία στον αναγνώστη να γνωριστεί με την έννοια της πληροφοριακής εχθροπραξίας και τους διαφορετικούς τρόπους εκδήλωσής της. Τέλος, ξεχωριστή θέση καταλαμβάνει και μια απόπειρα ιστορικής αναδρομής, απεικόνισης και απόδοσης του σχεδόν πάντα θολού τοπίου του αυτοαναπαραγόμενου και λοιπού, κακόβουλου λογισμικού, με τις εκάστοτε μορφές και υποστάσεις του.

Κεφάλαιο 3. Αυτοαναπαραγόμενο, κακόβουλο λογισμικό: αρωγός στις πληροφοριακές εχθροπραξίες

Στο σκέλος αυτό γνωρίζουμε στο αναγνωστικό κοινό με εμφατικό τρόπο εκείνες τις ποιοτικές ιδιότητες, αλλά και ιδιότυπες, τεχνικές μεθόδους, που έχουν καθιερώσει τους ιούς και τα σκουλήκια ως μόνιμους και αποτελεσματικούς φορείς πληροφοριακών, εχθρικών πράξεων.

[11] Σαφής και διάχυτη είναι πάντως η διάθεση του συγγραφέα για λελογισμένο περιορισμό των προσωπικών αντιλήψεων-πεποιθήσεων στο μέτρο της ελευθερίας εξαγωγής ερευνητικών πορισμάτων και άλλων χρήσιμων ερμηνειών της βιβλιογραφίας.

Το επιμύθιο αφιερώνεται σε μια προσπάθεια πρ(ωτ)ότυπης κατηγοριοποίησης του αυτοαναπαραγόμενου οπλολογισμικού, με γνώμονα την συγκριτική ανάδειξη των κυριότερων χαρακτηριστικών του, που εξασφαλίζουν ως ικανές και αναγκαίες συνθήκες τη σχετική επιτυχία στην εξυπηρέτηση των πρωταρχικότερων και πιο κοινών απαιτήσεων από την πλευρά των εκφραστών/εκτελεστών των διαφόρων, πληροφοριακών επιθέσεων.

Κεφάλαιο 4. Ασφάλεια και Προστασία πληροφορίας από επιθέσεις τύπου αυτοαναπαραγόμενου, επιβλαβούς λογισμικού

Το τμήμα αυτό πραγματεύεται την πληροφοριακή εχθροπραξία διαμέσω των αυτοαναπαραγόμενων όπλων από τη σκοπιά των αγωνιστών και υπέρμαχων της ασφάλειας, της αξιοπιστίας και της φερεγγυότητας των συστημάτων. Στη διάρκεια της συγκεκριμένης ενότητας επιτελείται μια ενδελεχής και κατά το δυνατόν λεπτομερής απεικόνιση και αποσαφήνιση των πολλαπλών και πολυπρόσωπων αμυντικών προσεγγίσεων. Έτσι, θίγονται και αποτιμώνται οι δεδομένες δυνατότητες και οι πιθανές αδυναμίες ενός ευρύτατου φάσματος μεθόδων, τακτικών και διαδικασιών, απαρτιζόμενου από κατευθύνσεις με τεχνικές, διοικητικές και νομικές αφετηρίες, που ως κοινό και μόνιμο στόχο τους έχουν θέσει την υπεράσπιση των πληροφοριακών συστημάτων και δραστηριοτήτων, στα πρότυπα του τρίπτυχου της αποδοτικής πρόληψης, του έγκαιρου εντοπισμού και της αποτελεσματικής αντιμετώπισης των απειλών και των παραβιάσεων ασφάλειας.

Κεφάλαιο 5. Μελλοντικές κατευθύνσεις έρευνας

Σε αυτό το κομμάτι στόχος είναι η επισήμανση της δυναμικής που αναδύεται από επίκαιρες, πρωτοποριακές εξελίξεις (τεχνικής βάσης, όπως π.χ. η τεχνολογία των rootkits ή το στεγανογραφικό παραλήρημα, αλλά και σε θεσμικό/νομοθετικό επίπεδο) στους αντικρουόμενους, μα και συμπορεύοντες, τομείς προσβολής και υπεράσπισης της ασφάλειας πληροφοριών, παράλληλα με την παράθεση και την παροχή μιας πρώτης -έστω και επιδερμικής- κατανόησης των διαφορετικών, λειτουργικών τους γνωρισμάτων, καθώς και των ενδεχόμενων ευκαιριών και κινδύνων που ευαγγελίζονται ή εγκυμονούν για τα σημερινά «οικοδομήματα» της ψηφιακής κοινωνίας και τους πληροφοριακούς, «θεμέλιους λίθους» της. Οι τεχνοτροπίες που αναφέρονται φέρουν, σε πολύ μεγάλο ποσοστό και συχνά με ριζοσπαστική διάθεση, τους σπόρους διαμόρφωσης του μελλοντικού πεδίου των πληροφοριακών εχθροπραξιών -που γίνονται εφικτές χάρη σε αυτοαναπαραγόμενα malwares- και της αντίστοιχης άμυνας και προστασίας.

Κεφάλαιο 6. Σκέψεις-Αναλύσεις-Προτάσεις

Η εργασία, αφού σταθεί στα κίνητρα συγγραφής και χρήσης κακόβουλων όπλων από μέρους των διαφορετικών ομάδων ατόμων που επιδίδονται σε αυτές τις δραστηριότητες και αναγνωρίσει τις σημαντικότερες επιπτώσεις της αντανάκλασης της σύγχρονης, πληροφοριακού χαρακτήρα εχθροπραξίας στην παγκόσμια κοινότητα, επιχειρεί να καταστρώσει ένα πλαίσιο προτάσεων για τη λήψη αναγκαίων μέτρων από μέρους της, που να εξασφαλίζουν μέγιστη, κοινωνική προστασία, σε συνδυασμό με τη διασφάλιση του πανανθρώπινου δικαιώματος και αιτήματος για αφομοίωση και ανταλλαγή πληροφοριών.

Κεφάλαιο 7. Επίλογος

Εν τέλει ολοκληρώνεται το πόνημα σε μια σύντομη επιθεώρηση των πεπραγμένων και των συμπερασμάτων του. Στην κατακλείδα περιλαμβάνονται και οι προσωπικές ευχαριστίες του συγγραφέα προς τα άτομα με αναγνωρισμένη προσφορά στην πραγμάτωση αυτού του έργου.

Στο τέλος της εργασίας και σε ειδικό τμήμα της με τον τίτλο **Βιβλιογραφία (8^{ο} Κεφάλαιο)** παρατίθεται, για λόγους αναφοράς στους πνευματικούς ιδιοκτήτες-δημιουργούς, αλλά και πιστοποίησης/τεκμηρίωσης των όσων κατά μήκος της διατυπώνονται και υποστηρίζονται, η εγχώρια και διεθνής βιβλιογραφία που μελετήθηκε και μέρη της οποίας χρησιμοποιήθηκαν κατά το δοκούν (αυτούσια ή κατόπιν κατάλληλης προσαρμογής τους), κατά τη φάση συγγραφής της παρούσας διπλωματικής.

Κατόπιν της βιβλιογραφίας και σε αντίστοιχο τμήμα βρίσκεται η **Λίστα** των **Σχημάτων**, που συνοδεύουν και πλαισιώνουν το γραπτό μέρος της εργασίας.

2 Επιστημονικό Υπόβαθρο

Προτού ξεκινήσουμε με μια επισταμένη, βιβλιογραφική επισκόπηση του υπό διερεύνηση θέματος, σκόπιμο είναι να σταθεί κανείς σε ορισμένες έννοιες, που συνεισφέρουν θεμελιωδώς στην καλύτερη κατανόηση του αντικειμένου της έρευνας και παράλληλα προσφέρουν τη δυνατότητα μεγαλύτερης εξοικείωσης με αυτό.

2.1 Η εποχή της πληροφορίας

Λόγω ενός αριθμού τεχνοοικονομικών λόγων, *η πληροφορική τεχνολογία κατέχει σήμερα μια θέση υπεροχής σε όλο το φάσμα της κοινωνίας*. Ειδικά την τελευταία δεκαετία, γινόμαστε μάρτυρες μιας διαδικασίας μαζικής μηχανοργάνωσης μεταξύ ανθρώπων, προϊόντων και υπηρεσιών, που γίνεται εφικτή χάρη στη μεγάλη διάχυση και επιτυχία του προσωπικού Η/Υ, στην τυποποίηση του λογισμικού των Η/Υ και το σχετικά χαμηλό κόστος επικοινωνίας μέσω Διαδικτύου.[12] Καθημερινά, πάσης φύσεως πληροφορίες και δεδομένα γίνονται διαθέσιμα μέσα από τις σελίδες και τις πύλες του Διαδικτύου και μέσα από τα μυριάδες σημεία διεπαφής (δια)δικτυακών εφαρμογών με τον τελικό χρήστη τους. *Ο άνθρωπος, σήμερα, έρχεται καθημερινά σε επαφή και αλληλεπιδρά -εκπαιδεύεται, ενημερώνεται, εργάζεται, συναλλάσσεται, διασκεδάζει- ολοένα και περισσότερο μέσω δικτύων πληροφοριών, που κάνουν εφικτή τη διάθεση, την παραγωγή και την ανταλλαγή γνώσης.*

[12] Πηγή: Διαδίκτυο, ιστοχώρος της online εγκυκλοπαίδειας WikiPedia, http://en.wikipedia.org/wiki/Information_Age.

Δεν είναι υπερβολή να θεωρήσει κανείς πως ζούμε στην αποκαλούμενη *εποχή της πληροφορίας (Information Age)*.

2.1.1 Χαρακτηριστικά της εποχής της πληροφορίας

Η πληροφορική έχει αλλάξει τον τρόπο δομής, λειτουργίας, αλλά και ανάλυσης των σύγχρονων κοινωνιών. Συχνά, χρησιμοποιείται και ο όρος *κοινωνία της πληροφορίας* ή *κοινωνία της γνώσης (Information or Knowledge Society)*, για να αποδώσει το στίγμα της τυπικής κοινωνίας, στην εποχή της πληροφορίας. [13]

Σύμφωνα με τον Bernard Boar (2000)[14], η εποχή της πληροφορίας φέρει συνοπτικά και κατά βάση τα ακόλουθα χαρακτηριστικά –χωρίς να περιορίζεται σε αυτά-, που είναι, τυπικά, κυρίως στις περισσότερες, ανεπτυγμένες κοινωνίες του Δυτικού Κόσμου:

- Οι επικρατούσες τεχνολογίες είναι ο ηλεκτρονικός υπολογιστής και οι τηλεπικοινωνίες υψηλών ταχυτήτων. Η επεξεργαστική ευφυΐα διαχέεται σε όλους εκείνους τους τομείς της ανθρώπινης δραστηριότητας, που μπορούν να βελτιωθούν με το να γίνουν ταχύτεροι και πιο ευέλικτοι. Οι υψηλών ταχυτήτων τηλεπικοινωνίες επιτρέπουν, τόσο σε ανθρώπους, όσο και σε υπολογιστές, να ανταλλάσσουν μεγάλο όγκο δεδομένων και πληροφοριών, με μικρό κόστος.
- Σύμβολο της εποχής είναι ο μικροεπεξεργαστής. Φτηνά, προγραμματίσιμα, ολοκληρωμένα κυκλώματα, με βάση τη σιλικόνη, επιτρέπουν την χρηστικότητα, ευελιξία, κλιμακωσιμότητα και διαδραστικότητα πληθώρας βιομηχανικών προϊόντων.
- Το τελικό, παραγωγικό «προϊόν» και συνάμα η υπεραξία της εποχής είναι η γνώση[15]. Η βάση του κοινωνικού πλούτου έχει μετατοπιστεί από τη βιομηχανική παραγωγή και βρίσκεται πλέον στην πληροφορία και τη γνώση. Η πληροφορία συνεισφέρει στην απόκτηση της γνώσης που, με τη σειρά της, οδηγεί σε στρατηγικό ανταγωνιστικό πλεονέκτημα, τουλάχιστον βραχυπρόθεσμα.

---

[13] Κύρια, βιβλιογραφική αναφορά: [ALBERTS-IA].

[14] Πηγή: "The Dawn of IT Fighting", Bernard Boar, 2000, διαθέσιμο από το δεσμό http://www.intelligententerprise.com/000209/cio.jhtml;jsessionid=GPXJSQKMOMLPOQSNDLRSKH0CJUNN2JVN.

[15] Πηγή: Διαδίκτυο, ιστοχώρος της online εγκυκλοπαίδειας WikiPedia, http://en.wikipedia.org/wiki/Information_society.

- Η ειδοποιός εργασία είναι αυτή του εργάτη γνώσης.[16] Περισσότερο του μισού του πανανθρώπινου, εργατικού δυναμικού ασχολείται με τη συλλογή, επεξεργασία και επικοινώνηση πληροφοριών.
- Το μέσο για τη μεταφορά και τη διάχυση πληροφορίας και γνώσης είναι τα τηλεπικοινωνιακά δίκτυα και ιδιαίτερα τα δίκτυα των ηλεκτρονικών υπολογιστών. Τα δικτυοκεντρικά, πληροφοριακά συστήματα αποτελούν ταυτόχρονα τα εργοστάσια και τις αποθήκες της κολεκτιβιστικής γνώσης ανθρώπων, εταιρειών, οργανισμών, κρατών και τελικά ολόκληρου του κόσμου μέσω της παγκόσμιας υποδομής του Διαδικτύου.
- Το Διαδίκτυο επιτρέπει την παγκόσμια και διαδραστική πρόσβαση σε σημασιολογικά «πλούσια», ψηφιακή, πολυμεσική πληροφορία. Η φυσική, βασισμένη στο χαρτί, ροή της πληροφορίας της βιομηχανικής εποχής έδωσε τη θέση της σε μια πλήρη, πιο προνομιούχα από πλευράς ταχύτητας διάδοσης, περιεκτικότητας σε χρήσιμα δεδομένα, αντοχής σε φυσικές συνθήκες, δυνατότητας εύκολης αναπαραγωγής κ.ά. και ευέλικτη, εικονική μορφή της.
- Τα προϊόντα με την κλασσική έννοια μετατρέπονται ει δυνατόν σε δυναμικά μεταβαλλόμενες, εύκολα κλιμακώσιμες, ευέλικτες οντότητες-υπηρεσίες, που σκοπό έχουν να μπορούν να ικανοποιούν κατ' ανάγκη και κατά την περίσταση, με τον καλύτερο δυνατό τρόπο, τις διαφορετικές επιθυμίες των πελατών-αγοραστών.[17] Ακόμη, τα σύγχρονα, βιομηχανικά αγαθά και οι αντίστοιχες, προσφερόμενες υπηρεσίες εμπλουτίζονται πληροφοριακά και τεκμηριώνονται, ώστε πετυχαίνοντας τη δημιουργία προστιθέμενης αξίας, να προσελκύει κανείς καλύτερα το καταναλωτικό του κοινό και να ικανοποιεί τις διαφορετικές ανάγκες των τελικών χρηστών.
- Τα συστήματα πληροφοριών ολοένα τείνουν να γίνονται περισσότερο κατανεμημένα και αρθρωτά, πιο διαδικασιοστρεφή και πελατοκεντρικά, πιο υπηρεσιοστρεφή και δικτυοκεντρικά, πιο ολοκληρωμένα και ενοποιημένα, και τέλος πιο επιχειρησιοστρεφή.[18] Επίσης, παρατηρείται μια σαφής, αντικειμενική προσήλωση προς τη χρήση συστημάτων Η/Υ και μια στροφή προς μια ευρύτερη και ταχύτερη (δια)δικτύωση.

---

[16] Πηγή: Διαδίκτυο, ιστοχώρος της online εγκυκλοπαίδειας WikiPedia, http://en.wikipedia.org/wiki/Knowledge_worker.

[17] Πηγή: "World-Class Manufacturing and Information Age Competition", B.S. Sahay, K.B.C. Saxena and Ashish Kumar, Industrial Management Magazine, 2001, διαθέσιμο από το δεσμό http://www.entrepreneur.com/tradejournals/article/76639407.html.

[18] Πηγή: Διαδίκτυο, ιστοχώρος της online εγκυκλοπαίδειας WikiPedia, http://en.wikipedia.org/wiki/Service-oriented_architecture.

- Η αγορά, ως χώρος οικονομικών συναλλαγών, υπηρεσιών και αγαθών, μετασχηματίζεται για να συμπεριλάβει και τον εικονικό,[19] ηλεκτρονικό χώρο (e-marketing, e-business, e-commerce). Οι παραδοσιακές επιχειρήσεις δελεάζονται να προχωρήσουν εμπρός προωθώντας και τα ευέλικτα, εικονικά κανάλια διανομής και εμπορίου, σε συνδυασμό με τα όποια, φυσικά ομόλογά τους, ενώ νέες, καθαρά εικονικές εταιρείες ξεπηδούν καθημερινά, προσφέροντας αποκλειστικά ηλεκτρονικής μορφής προϊόντα και υπηρεσίες, φανερώνοντας έτσι τις καινούριες τάσεις στην επιχειρηματικότητα. Οι στρατηγικές συνεργασίες και τα δίκτυα προμηθευτών, πελατών και εταίρων «στήνονται» εξαρχής και εξαπλώνονται έχοντας ως βάση και αφετηρία και τις ψηφιακές πλατφόρμες και τεχνολογίες επικοινωνίας, ανταλλαγής πληροφοριών και πραγματοποίησης λογής «αγοραπωλησιών».
- Η διοίκηση επιχειρήσεων και οργανισμών, αλλά ακόμη και η διακυβέρνηση ολόκληρων κρατών, αλλάζουν ουσιαστικά, σε μια προσπάθεια να επωφεληθούν των θετικών δράσεων της πληροφορικής τεχνολογίας.[20] Συστήματα εταιρικής διαχείρισης γνώσης (KMS, BI) αντικαθιστούν ή καλύτερα ενοποιούν τα μονολιθικά συστήματα διαχείρισης πόρων και πελατειακών σχέσεων (ERP, CRM), ενώ διαδίδονται με αστραπιαίο ρυθμό βέλτιστες πρακτικές και συστήματα ηλεκτρονικής διακυβέρνησης, που απλοποιούν και διευκολύνουν την καθημερινή συναλλαγή των πολιτών με το Κράτος (e-government).
- Προωθούνται εντελώς πρωτοποριακοί τρόποι ζωής, εκπαίδευσης και εργασίας.[21] Καταρρέουν ποικίλοι, χωροχρονικοί περιορισμοί, ιδανικά επιτρέποντας σε άτομα να ζουν όπου επιθυμούν, να εκπαιδεύονται από απόσταση πάνω στην ειδικότητα της αρεσκείας τους (e-learning), να εργάζονται για απομακρυσμένους εργοδότες (e-working) και να προμηθεύονται προϊόντα από τοπικά ή απομακρυσμένα σημεία πώλησης, αναλόγως την περίσταση.
- Ολόκληρη η οικονομία αλλάζει. Παγκοσμιοποίηση και άκρατος ανταγωνισμός, αλλά και επικοινωνία, ανταλλαγή και συνεργασία, διαμορφώνουν το νέο, πληροφοριο-κεντρικό πεδίο μιας μετα-βιομηχανικής οικονομίας (post-industrial economy) διεθνούς, ψηφιακού, δικτυοκεντρικού καπιταλισμού (transnational, digital or network capitalism).[22]

---

[19] Κύρια, βιβλιογραφική αναφορά: [STRINGER-CIC].

[20] Κύρια, βιβλιογραφική αναφορά: [CHOO-KOHOUICMCKMD].

[21] Κύρια, βιβλιογραφική αναφορά: [STRINGER-CIC].

[22] Κύρια, βιβλιογραφική αναφορά: [SCHILLER-DCNGMS], [FUCHS-TSNS].

- Οι άνθρωποι και οι κοινωνικές ομάδες εξαρτώνται και επηρεάζονται ολοένα και περισσότερο, σε καθημερινό επίπεδο, από την τεχνολογική εξέλιξη και τη συνεχή, πληροφορική επανάσταση, στη λογική των «συγκοινωνούντων δοχείων». Η ευρύτερη κουλτούρα και ο πολιτισμός έχουν πλέον έντονα τα σημάδια αυτής της τεχνολογικής και πληροφοριακής έξαρσης.

Αναμφίβολα, οι κατεξοχήν εκφραστές του κλίματος στην εποχή της πληροφορίας είναι τα σύγχρονα, πληροφοριακά συστήματα[23], που δεσπόζουν πια σε καθημερινό επίπεδο, με τους κύριους, άλλα όχι μοναδικούς, εκφραστές τους να εδράζουν στα ήδη κλασσικά μέσα μαζικής επικοινωνίας (τηλέφωνο, τηλεόραση, ραδιόφωνο) και φυσικά στο Διαδίκτυο. Τα συστήματα αυτά διατρέχουν πλέον το σύνολο σχεδόν των ανθρώπινων δραστηριοτήτων (όπως επικοινωνία, εργασία, εκπαίδευση, ψυχαγωγία, μετακίνηση κ.ά.) και η όποια νεωτερικότητα των ημερών μας αντανακλάται πρωτίστως και κατά μείζονα λόγο σε αυτά.

2.1.2 Πληροφοριακό Σύστημα

Ένα πληροφοριακό σύστημα (στο εξής σύντομα ΠΣ) διαχρονικά ορίζεται ως μια οργανωμένη συλλογή, επεξεργασία, μετάδοση και διάχυση της πληροφορίας,[24] σε εναρμόνιση με καλά ορισμένες και τεκμηριωμένες διαδικασίες, είτε αυτόματες είτε χειρωνακτικές. Συνήθως, αυτό περιλαμβάνει ολόκληρη την υποδομή, την οργάνωση, αλλά και τα στοιχειώδη δομικά στοιχεία, που συλλέγουν, επεξεργάζονται, αποθηκεύουν, μεταδίδουν, απεικονίζουν και διαχέουν την πληροφορία. *Συμπεριλαμβάνει όλους και όλα που εμπλέκονται στις διαδικασίες αυτές* — όπως π.χ. ένα laptop, τοπικά ή μεγαλύτερης εμβέλειας δίκτυα δεδομένων και φωνής, εγκαταστάσεις ασύρματης μετάδοσης, υπόγεια καλώδια και πάνω μα πάνω από όλα, τους ανθρώπους που συμμετέχουν και είναι υπεύθυνοι για την αποστολή, λήψη, επεξεργασία και χρήση της πληροφορίας. *Οι άνθρωποι, ακριβώς επειδή είναι υπεύθυνοι για τη λήψη αποφάσεων σε όλα τα επίπεδα ενός ΠΣ, αποτελούν το πιο σημαντικό κομμάτι (για τη βέλτιστη επίδοση) του και αυτό που κατέχει τη μεγαλύτερη δυναμική από πλευράς μη ντετερμινιστικών προβλημάτων και αδυναμιών.*

Σήμερα, τα ΠΣ αποτελούν ανεξάρτητα ή αλληλεξαρτημένα τμήματα αρκετά μεγαλύτερων υποδομών. Οι υποδομές αυτές διασυνδέουν μεταξύ τους τα διάφορα αυτόνομα ΠΣ με μυριάδες, διαφορετικά, κατευθυνόμενα ή μη, μονοπάτια, με τη μορφή δικτυωμάτων ή απλά δικτύων**,** γι' αυτό και τα συστήματα, πλέον, αποδίδονται και με τον όρο *δικτυοκεντρικά ΠΣ ή*

[23] Πηγή: Διαδίκτυο, ιστοχώρος της online εγκυκλοπαίδειας WikiPedia, http://en.wikipedia.org/wiki/Information_systems.

[24] Κύρια, βιβλιογραφική αναφορά: [KROSS-JDCCW].

ΠΣ προσανατολισμένα στο δίκτυο (netcentric or network-oriented IS).[25] Αυτή η ολοένα επεκτεινόμενη και διογκούμενη, πληροφοριακή υποδομή διαπερνά βιομηχανία, επιχειρήσεις, μέσα ενημέρωσης, κυβερνήσεις και στρατιωτικούς οργανισμούς και περιλαμβάνει κάθε λογής ενσύρματα και ασύρματα μέσα μετάδοσης και πάσης φύσεως τηλεπικοινωνιακά συστήματα, όπως τηλεφωνικά, τηλεομοιοτυπικά, τηλεγραφικά, υπολογιστών κ.ό.κ. Σε κάθε ένα από αυτά τα τηλεπικοινωνιακά δικτυώματα, μα τις περισσότερες φορές σε περισσότερα του ενός εξ αυτών ταυτόχρονα ή παράλληλα, δύναται να δρα ένα σημερινό πληροφοριακό σύστημα. Στις μέρες μας, βέβαια, παρατηρείται μια συνεχώς *αυξανόμενη τάση για ολοκλήρωση των συστημάτων μέσω εφαρμογών, συσκευών και δικτύων Η/Υ* και ακόμα πιο συγκεκριμένα μια *στροφή των πληροφοριακών συστημάτων προς το Διαδίκτυο και την παγκόσμια κοινότητα των χρηστών του*.[26]

Σε μια απόπειρα ενός γενικά αποδεκτού ορισμού, υπό το πρίσμα αυτής της μεταπτυχιακής διατριβής:[27]

"Πληροφοριακό σύστημα είναι ένα σύστημα ανθρώπινης δραστηριότητας, το οποίο αποτελείται από πέντε στοιχεία: ανθρώπους, λογισμικό, υλικό, διαδικασίες και δεδομένα, τα οποία αλληλεπιδρούν μεταξύ τους και με το περιβάλλον, με σκοπό την παραγωγή και διαχείριση πληροφορίας, για την υποστήριξη ανθρώπινων δραστηριοτήτων και την εξυπηρέτηση ανθρώπινων αναγκών, στα πλαίσια του κείμενου οργανισμού, καθώς και των υποκείμενων και υπερκείμενων σε αυτόν οντοτήτων."

Στα πλαίσια αυτής της εργασίας, *θα μας απασχολήσουν αποκλειστικά και μόνο τα δικτυοκεντρικά ΠΣ που βασίζονται στην υλισμική υποδομή διασυνδεδεμένων Η/Υ,* όπως είναι π.χ. όλες οι σύγχρονες, διαδικτυακές υπηρεσίες εμπορικών, τραπεζικών, κυβερνητικών ή στρατιωτικών εφαρμογών και συστημάτων.

Επιπρόσθετα, είναι άξιο λόγου το γεγονός ότι μια σημαντικότατη -αν όχι την πολυπληθέστερη- και πιο ποικιλόμορφη μερίδα από την πληθώρα των ΠΣ του σήμερα αποτελούν τα συστήματα με άμεση διεπαφή προς το Διαδίκτυο ή με έμμεση δίοδο του τοπικού δικτύου Η/Υ, στο οποίο εδρεύουν, σε αυτό. Όλα αυτά τα συστήματα, αλλά δυνητικά και όλα όσα είναι προσανατολισμένα και εξαρτημένα από την καθιερωμένη-συνηθισμένη δικτύωση τυποποιημένων Η/Υ, ανεξαρτήτως ενδεχόμενης δυνατότητας πρόσβασής τους στο Διαδίκτυο, είναι εγγενώς ευπρόσβλητα από τρέχουσες, κακόβουλες επιθέσεις και άρα

[25] Κύρια, βιβλιογραφική αναφορά: [ALBERTS-IAT].

[26] Όπως στην προηγούμενη υποσημείωση.

[27] Κύρια, βιβλιογραφική αναφορά: [KOKOLAKIS-ISMIS].

αποτελούν αντικείμενο και της παρούσας έρευνας. *Το Διαδίκτυο, απλώς, είναι ένα μέσο μεγέθυνσης και πλεονεκτικότερης διασποράς του υπαρκτού προβλήματος και ως τέτοιο μόνο θα αντιμετωπιστεί από την διπλωματική αυτή.*

Επιπλέον, ο άνθρωπος, όπως είδαμε, αποτελεί την βασικότερη συνιστώσα ενός ΠΣ και έτσι ο ρόλος του στις πληροφοριακού τύπου επιθέσεις με αυτοαναπαραγόμενο, επιβλαβές λογισμικό κρίνεται καθοριστικός και αποφασιστικός. *Η εργασία αυτή θα απεικονίσει τον ανθρώπινο παράγοντα τόσο ως την πηγή και το φορέα προβλημάτων ασφάλειας για ΠΣ, όσο και ως τη δύναμη προστασίας τους.*

2.2 Ασφάλεια Συστημάτων Πληροφοριών

Ο ευρύς όρος ασφάλεια πληροφοριακών συστημάτων (information systems security) δίνει έμφαση στην προστασία των συστατικών στοιχείων ενός ΠΣ -όπως ορίστηκαν προηγουμένως-, αλλά και του ίδιου του ΠΣ στην ολότητά του. Σύμφωνα με έναν κοινώς αποδεκτό ορισμό:[28]

"Ασφάλεια Πληροφοριακού Συστήματος είναι εκείνο το οργανωμένο πλαίσιο από έννοιες, αντιλήψεις, αρχές, πολιτικές, διαδικασίες, τεχνικές και μέτρα, που απαιτούνται για να προστατευθούν τα στοιχεία του Πληροφοριακού Συστήματος, αλλά και το σύστημα ολόκληρο, από κάθε σκόπιμη ή τυχαία απειλή."

Ο ορισμός αυτός δίνει έμφαση, όχι μόνο στο ΠΣ ως ολότητα, αλλά και στα επιμέρους στοιχεία του, ενώ η αναφερόμενη προφύλαξη αφορά κάθε είδους απειλή (τυχαία ή σκόπιμη). Η ασφάλεια του ΠΣ συνδέεται άμεσα τόσο με τις τεχνικές, τις διαδικασίες και τα διοικητικά ή θεσμικά μέτρα, όσο και με ηθικοκοινωνικές αντιλήψεις, αρχές και παραδοχές. Είναι βέβαια προφανές ότι η όποια προφύλαξη δεν θα πρέπει να παρεμποδίζει την απρόσκοπτη λειτουργία του συστήματος, την παραγωγή γνώσης και την ελεύθερη διακίνηση των πληροφοριών, έτσι ώστε να μην θέτονται αδικαιολόγητοι φραγμοί στην ανάπτυξη και πρόοδο των υποστηριζόμενων οργανισμών.[29]

Η ασφάλεια πληροφοριών (information security), από την άλλη, αναφέρεται αποκλειστικά στην προστασία των πληροφοριών και είναι στενότερη έννοια από αυτή της ασφάλειας ΠΣ,

[28] Κύρια, βιβλιογραφική αναφορά: [KIOUNTOUZIS-MISS].

[29] Κύρια, βιβλιογραφική αναφορά: [LEKKAS-ICSTTP].

αφού η πληροφορία εμπεριέχεται σε ένα ΠΣ.[30] Βέβαια, η ασφάλεια πληροφοριών δεν μπορεί να αγνοήσει το πληροφοριακό σύστημα, στα πλαίσια του οποίου παράγεται και χρησιμοποιείται η πληροφορία. Αντίθετα, κάθε αναλυτική εργασία, η οποία αποσκοπεί στην ανάπτυξη και διαχείριση της ασφάλειας των πληροφοριών, θα πρέπει να στηρίζεται στην κατανόηση των σχετικών, πληροφοριακών συστημάτων. Συνεπώς, *όταν αναφερόμαστε στην ασφάλεια ενός ΠΣ, η προστασία όλων των δομικών συστατικών που μετέχουν σε αυτό έχει ιδιαίτερη σημασία, ενώ όταν αναφερόμαστε στην ασφάλεια πληροφοριών, η διαφύλαξη της ασφάλειάς τους ενδιαφέρει μόνο στο βαθμό, που σχετίζεται με την προστασία των πληροφοριών αυτών-καθεαυτών*.[31]

Η ασφάλεια των πληροφοριών αναφέρεται στην προστασία της πληροφορίας στην ολότητά της και των σχετικών με την ασφάλεια ιδιοτήτων. Στα παρακάτω υποκεφάλαια θα ασχοληθούμε με την επιθεώρηση και απαρίθμηση των βασικών ιδιοτήτων ασφάλειας, σύμφωνα με τα επικρατούντα, θεωρητικά μοντέλα ασφάλειας.

2.2.1 Η CIA τριάδα

Ως θεμελιώδεις ιδιότητες ασφάλειας θεωρούνται η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα, που ορίζονται ως εξής:[32]

Εμπιστευτικότητα πληροφοριών (confidentiality): *"Η ιδιότητα των δεδομένων να καθίστανται αναγνώσιμα μόνο από εξουσιοδοτημένα, λογικά υποκείμενα, όπως φυσικές οντότητες και διεργασίες λογισμικού"*.

Ακεραιότητα πληροφοριών (integrity): Είναι *"η ιδιότητα των δεδομένων να υφίστανται προκαθορισμένο φυσικό μέσο ή χώρο και να είναι ακριβή"*. Δηλαδή η μη-εξουσιοδοτημένη τροποποίηση της πληροφορίας θα πρέπει να αποτρέπεται, ενώ κάθε αλλαγή του περιεχομένου των δεδομένων να είναι αποτέλεσμα εξουσιοδοτημένης και ελεγχόμενης ενέργειας.

Διαθεσιμότητα πληροφοριών (availability): *"Η αποτροπή της προσωρινής ή μόνιμης άρνησης διάθεσης της πληροφορίας σε κάθε εξουσιοδοτημένο, λογικό υποκείμενο του συστήματος"*.

[30] Όπως στην προηγούμενη υποσημείωση.

[31] Όπως στην προηγούμενη υποσημείωση.

[32] Κύρια, βιβλιογραφική αναφορά: [GRITZALIS-ISSHSE].

Η περιώνυμη *τριάδα CIA (CIA Triad)* οφείλει το όνομά της στα αρχικά των προαναφερόμενων ιδιοτήτων και αποτελεί το πρώτο χρονικά και ταυτόχρονα καθολικά παραδεκτό σχήμα ασφάλειας, σήμερα. Αποτελεί το *ελάχιστο υποσύνολο μη επικαλυπτόμενων ιδιοτήτων της πληροφορίας*, η παρουσία των οποίων μπορεί να εγγυηθεί ένα σημαντικότατο βαθμό προστασίας απέναντι σε εγχειρήματα υπονόμευσης της ασφάλειας, η *απουσία* δε *οποιασδήποτε εκ των τριών αποτελεί κατάφωρη παραβίαση της ασφάλειας οιουδήποτε συστήματος πληροφοριών*.

2.2.2 Η Parkerian εξάδα

Η *εξάδα Parker (Parkerian Hexad)* δημιουργήθηκε από τον ερευνητή Donn B. Parker.[33] Το μοντέλο αυτό εμπλέκει *τρεις, πρόσθετες, ατομικές, μη επικαλυπτόμενες ιδιότητες* των πληροφοριών στις τρεις, ήδη κλασσικές, ιδιότητες ασφάλειας της τριάδας CIA (εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα). Οι ιδιότητες της Parkerian Hexad είναι οι ακόλουθες:[34]

*** Εμπιστευτικότητα (confidentiality, όπως στο CIA μοντέλο):**

Η εμπιστευτικότητα καθορίζει τα όρια του ποιος μπορεί να πάρει ποιο είδος πληροφοριών.

*** Κατοχή ή έλεγχος (possession or control):**

Ας υποθέσουμε ότι ένας κλέφτης επρόκειτο να κλέψει έναν σφραγισμένο φάκελο, που περιέχει μια χρεωστική κάρτα τραπεζών και τον προσωπικό αριθμό αναγνώρισής της (PIN). Ακόμα κι αν ο κλέφτης δεν άνοιγε ποτέ τον εν λόγω φάκελο, το θύμα της κλοπής πολύ λογικά και δικαίως θα ανησυχούσε πως θα μπορούσε να το κάνει οποιαδήποτε στιγμή χωρίς τον έλεγχο και τη δική του συναίνεση. Μια τέτοια κατάσταση περιγράφεται ως απώλεια ελέγχου ή κατοχής των πληροφοριών, χωρίς παράλληλα να αποτελεί παραβίαση της εμπιστευτικότητας.

*** Ακεραιότητα (integrity, όπως στο CIA μοντέλο):**

Οποιαδήποτε αναρμόδια τροποποίηση των στοιχείων, είτε σκόπιμη είτε τυχαία, είναι μια παραβίαση της ακεραιότητας δεδομένων.

---

[33] Κύρια, βιβλιογραφική αναφορά: [WILEY-CSH-Chapter5].

[34] Πηγή: Διαδίκτυο, ιστοχώρος της online εγκυκλοπαίδειας WikiPedia, http://en.wikipedia.org/wiki/Parkerian_hexad.

*** Αυθεντικότητα (authenticity):**

Η αυθεντικότητα αναφέρεται στην ορθή απόδοση των πληροφοριών, με την έννοια της απόδειξης της προέλευσης και του ιδιοκτήτη της πληροφορίας.

*** Διαθεσιμότητα (availability, όπως στο CIA μοντέλο)**

Η διαθεσιμότητα σημαίνει έγκαιρη πρόσβαση στις πληροφορίες. Οποιαδήποτε καθυστέρηση, που υπερβαίνει τα αναμενόμενα επίπεδα υπηρεσιών για ένα σύστημα, μπορεί να περιγραφεί ως παραβίαση της διαθεσιμότητας.

*** Χρησιμότητα (utility)**

Χρήσιμη θεωρείται μια πληροφορία, όταν στην εκάστοτε μορφή που βρίσκεται, μπορεί να επιτελέσει χωρίς λογική δυσκολία ή πρακτική παρερμηνεία τον αντικειμενικό της σκοπό. Η μετατροπή μιας πληροφορίας από μια μορφή δεδομένων σε μια άλλη ή καλύτερα από μια μορφή αναπαράστασης σε κάποιο άλλο σχήμα ενδέχεται να παρακωλύσει τη χρήση της πληροφορίας λόγω πιθανών προβλημάτων συμβατότητας και καταλληλότητας του χρησιμοποιούμενου μέσου επεξεργασίας και της επιλεγμένης μορφής δεδομένων. Μια τέτοια κατάσταση αποτελεί παραβίαση της χρησιμότητας. Η χρησιμότητα είναι συχνά συγκεχυμένη με τη διαθεσιμότητα, επειδή οι τυχούσες παραβιάσεις μπορούν επίσης να απαιτήσουν πρόσθετη, χρονική επιβάρυνση, για επεξεργασία των αλλαγών στο σχήμα ή την παρουσίαση των στοιχείων. Εντούτοις, η έννοια της χρησιμότητας είναι ευδιάκριτη από αυτήν της διαθεσιμότητας.

Αυτές οι ιδιότητες των πληροφοριών είναι ατομικές, διότι δεν χωρίζονται σε περαιτέρω συστατικά και είναι μη επικαλυπτόμενες, δεδομένου ότι αναφέρονται σε μοναδικές πτυχές της έννοιας της πληροφορίας. Σχεδόν *κάθε παραβίαση ασφάλειας πληροφοριών μπορεί να περιγραφεί ως έχουσα αρνητικές επιπτώσεις σε μια ή περισσότερες από αυτές τις θεμελιώδεις ιδιότητες των πληροφοριών*.

Το μοντέλο του Parker χαίρει γενικά μεγάλης εκτίμησης από την επιστημονική κοινότητα και τους εμπειρογνώμονες στο πεδίο της ασφάλειας συστημάτων και πληροφοριών, καθώς αποτελεί *ορθή και επιτυχημένη επέκταση του CIA τρίπτυχου*.

2.2.3 Εναλλακτικές θεωρήσεις και προσθήκες στα βασικά μοντέλα

Σε αρκετές ερευνητικές εργασίες και προσπάθειες υποστηρίζεται πως οι αρχικές τρεις, αλλά ακόμα και οι παραπάνω έξι ιδιότητες, δεν επαρκούν, για να οριστεί επαρκώς η ασφάλεια

πληροφοριών. Έτσι, διάφοροι ερευνητές ασφάλειας προτείνουν τα δικά τους μοντέλα, που ουσιαστικά επεκτείνουν ή συμπληρώνουν τα υπάρχοντα δύο, εισάγοντας νέες, ατομικές ιδιότητες της πληροφορίας, που δεν ικανοποιούν όμως απαραίτητα τον περιορισμό της μη επικάλυψης των ιδιοτήτων, που διέπει τα δύο εγνωσμένα μοντέλα. Χαρακτηριστικά αναφέρουμε τις πιο κάτω περιπτώσεις ως έχουσες σημαντικό αντίκτυπο και χαίρουσες ευρύτερης εκτίμησης από την επιστημονική κοινότητα:

Επιτρεπτότητα (admissibility):[35]

"ελευθερία εισόδου μιας πληροφορίας σε ένα σύστημα κατόπιν εξακριβωμένης σχέσης εμπιστοσύνης ή επιτυχημένης διαπίστευσης του άξιου της εμπιστοσύνης μεταξύ του αποστολέα της πληροφορίας και του λαμβάνοντος συστήματος"· ο αποστολέας καλείται να πληροί μια λίστα πολιτικών ασφάλειας που έχει προδιαγράψει η λαμβάνουσα οντότητα και αποτελούν προϋποθέσεις για την αποδοχή λήψης οποιασδήποτε εισερχόμενης πληροφορίας.

Μη αποποίηση (non-repudiation):[36]

"αδυναμία άρνησης των ενεργειών που έχουν εκτελεστεί για την τροποποίηση, την αποστολή ή τη λήψη μίας πληροφορίας".

Μοναδικότητα (uniqueness):[37]

"απαγόρευση/αδυναμία μιας, χωρίς πρότερη έγκριση και εξουσιοδότηση, αντιγραφής και αναπαραγωγής της πρωτότυπης πληροφορίας".

Εγκυρότητα (validity):[38]

"η πληροφορία αντιπροσωπεύει την πραγματικότητα και είναι επίκαιρη"· αν και στενά συναφής έννοια διαφέρει από την ακεραιότητα, η οποία αφορά κυρίως την πληρότητα, ολότητα και πιστότητα των δεδομένων, που πρέπει να συνάδει με την αρχική πρόθεση των

---

[35] Πηγή: "Updating the Traditional Security Model", Bruce Schneier, 2006, διαθέσιμο από το δεσμό http://www.schneier.com/blog/archives/2006/08/updating_the_tr.html.

[36] Πηγή: "Non-Repudiation in the Digital Environment", Adrian McCullagh and William Caelli, 2000, διαθέσιμο από το δεσμό http://www.firstmonday.org/issues/issue5_8/mccullagh/index.html.

[37] Η ιδιότητα της μοναδικότητας είναι ύψιστης σημασίας, κυρίως στον τρόπο φύλαξης κρίσιμων πληροφοριών εντός βάσεων και αποθηκών δεδομένων. Τα περισσότερα συστήματα διαχείρισης τέτοιων δομών μεριμνούν για την κατ' ανάγκη ικανοποίησή της με τη βοήθεια π.χ. εκτεταμένης χρήσης μοναδικών κλειδιών δεικτοδότησης-προσπέλασης και χρονοσφραγίδων.

[38] Κύρια, βιβλιογραφική αναφορά: [GRITZALIS-SICTFA].

δημιουργών-παραγωγών τους και όχι τόσο ειδικά την ρεαλιστική τους ορθότητα, με την οποία ισοδυναμεί η εγκυρότητα.

2.2.4 Υπηρεσίες και συστήματα ασφάλειας πληροφοριών και δεδομένων

Η ύπαρξη των παραπάνω διαφορετικών θεωρήσεων για τις ιδιότητες της ασφάλειας πληροφοριών δε θα πρέπει να θεωρηθεί παράδοξο, καθώς στο χώρο της πληροφορικής, *η ασφάλεια έχει αποκτήσει μια αφηρημένη έννοια, η οποία επιδέχεται ποικίλες ερμηνείες*. Επίσης, η ουσία της ασφάλειας στο κοινωνικό σύνολο, αντιστοιχεί ουσιαστικά σε ένα ανθρώπινο συναίσθημα. Έτσι, ο όρος ασφάλεια αναφέρεται σε *διάφορες ιδιότητες της πληροφορίας, πολλές φορές μάλιστα αλληλεπικαλυπτόμενες*, ανάλογα με την οπτική του ερευνητή και το πληροφοριακό σύστημα στο οποίο αναφέρεται. Συνεπώς, σε κάθε ειδική περίπτωση που μελετάται, θα πρέπει να ορίζονται με σαφήνεια οι συγκεκριμένες ιδιότητες της πληροφορίας, που καλείται κανείς να προστατέψει και που συγκροτούν την *επιθυμητή σφαίρα της ασφάλειας πληροφοριών ή ΠΣ*.

Στην ευρύτατη προσπάθεια να καλυφθούν οι απαιτήσεις ασφάλειας για τα συστήματα πληροφοριών, όπως αυτές παρουσιάζονται στα προηγούμενα μοντέλα, έχουν αναπτυχθεί και απαντώνται στα περισσότερα, δικτυοκεντρικά ΠΣ, είτε εγγενώς υλοποιημένες εντός τους είτε με τη μορφή δράσης/επίκλησης υπεύθυνων, περιφερειακών ή παρένθετων συστημάτων και μηχανισμών, οι παρακάτω υπηρεσίες ασφάλειας:[39]

1. *Ταυτοποίηση και Αυθεντικοποίηση*: Η επαλήθευση της ταυτότητας μιας οντότητας από ένα ΠΣ, που προηγείται της επιτέλεσης μιας κρίσιμης ενέργειας/λειτουργίας και γίνεται στη βάση παρουσίασης μοναδικών, έγκυρων και αξιόπιστων πιστοποιητικών στο εν λόγω σύστημα εκ μέρους της οντότητας.
2. *Εξουσιοδότηση και Έλεγχος Πρόσβασης*: Καθορισμός, εγκατάσταση και αδιάκοπη επιβεβαίωση της ισχύος ρητών δικαιωμάτων χρήσης ενός ΠΣ για οποιαδήποτε, αυθεντικοποιημένη οντότητα, σε κάθε κρίσιμη πράξη, για όσο χρόνο διαρκεί η «συναναστροφή» με το σύστημα.
3. *Υπευθυνότητα και Καταγραφή*: Η σαφής υπευθυνότητα περιλαμβάνει διαδικασίες, πολιτικές και απαραίτητους ελέγχους, ώστε να επισημαίνεται και αποτυπώνεται (με

[39] Πηγή: Διαδίκτυο, ιστοχώρος του τμήματος υποστήριξης τερματικών του Πανεπιστημίου του Berkeley, "Computer Security Framework and Principles", 1998, http://wssg.berkeley.edu/SecurityInfrastructure/reports/framework.html.

ηλεκτρονικό κυρίως τρόπο[40]) σαφώς η πηγή και ο αυτουργός κάθε ενέργειας, καθώς και το είδος αυτής. Η υπευθυνότητα υποστηρίζει άμεσα τη μη-αποποίηση, την πρόληψη παρείσφρυσης, την παρακολούθηση της ασφάλειας, την επανόρθωση-αποκατάσταση προβλημάτων και το νομικό παραδεκτό των αρχείων καταγραφής (security monitoring logs).

4. *Εμπιστευτικότητα*: Μια απαίτηση οι ιδιωτικές, απόρρητες ή άλλες κρίσιμες, εμπιστευτικές πληροφορίες να μην αποκαλυφθούν ποτέ σε αναρμόδια άτομα. Η έννοια της *ιδιωτικότητας (privacy)* έχει καθιερωθεί ως υποσύνολο της εμπιστευτικότητας για την περιγραφή της απαίτησης έμπιστης πρόσβασης σε πληροφορίες που άπτονται της σφαίρας του προσωπικού, ιδιωτικού απόρρητου.
5. *Ακεραιότητα*: Η ακεραιότητα δεδομένων είναι μια απαίτηση ότι οι πληροφορίες και τα προγράμματα αλλάζουν μόνο με έναν διευκρινισμένο και εξουσιοδοτημένο τρόπο. Η ακεραιότητα συστημάτων είναι μια απαίτηση ότι ένα σύστημα εκτελεί την προοριζόμενη λειτουργία του κατά τρόπο αμείωτο, απαλλαγμένο από σκόπιμο ή αμελή, αναρμόδιο χειρισμό.
6. *Διαθεσιμότητα*: Μια απαίτηση που σκοπεύει να βεβαιώσει ότι η εύρυθμη λειτουργία και εργασία των συστημάτων είναι ανεμπόδιστη και δεν προκαλείται άρνηση εξυπηρέτησης στους εξουσιοδοτημένους χρήστες.
7. *Κατοχή ή έλεγχος*: Περιφρούρηση των νόμιμων δικαιωμάτων στρατηγικού ελέγχου της χρήσης και λειτουργίας ΠΣ, που πηγάζουν από την ιδιοκτησία αυτών από τις δικαιούχες οντότητες, και αποτροπή παράνομης, στρατηγικού τύπου, δραστηριότητας οντοτήτων που δεν έχουν τέτοια δικαιοδοσία.
8. *Αυθεντικότητα*: Προστασία της ορθότητας της πηγής, των κυοφορούμενων μηνυμάτων και των φερόμενων ως ιδιοκτητών των πληροφοριών.
9. *Χρησιμότητα*: Αποφυγή της ματαιότητας στη χρήση των πληροφοριών.
10. *Επιτρεπτότητα*: Ελέγχεται η συμμόρφωση συστημάτων με προκαθορισμένες πολιτικές του ΠΣ στην επικράτεια του οποίου επιχειρούν να δράσουν, προτού να δοθεί η έγκριση πραγματοποίησης των οποιωνδήποτε πληροφοριακά κρίσιμων ενεργειών. Σε περίπτωση απόκλισης από τα επιθυμητά πρότυπα, δεν επιτρέπεται στα εξεταζόμενα συστήματα η οποιαδήποτε ενέργεια.
11. *Μοναδικότητα*: Πλαίσιο για την εγκατάσταση/απόδειξη μιας χρονικής ή τροπικής μοναδικότητας στα δεδομένα και για την αποφυγή παράνομης αντιγραφής

[40] Παραδείγματος χάριν με τη βοήθεια κλειστών κυκλωμάτων παρακολούθησης χώρων ή με την αδιάκοπη καταγραφή ενεργειών, συμβάντων και αλλαγών σε επίπεδο λογισμικού και ηλεκτρονικών συναλλαγών.

στοιχείων ή επανεγγραφής άχρηστης, διπλότυπης, άρα και πιο ευάλωτης[41], κρίσιμης πληροφορίας.

12. *Εγκυρότητα*: Οι πληροφορίες πρέπει να παραμένουν λογικά συνεπείς και ορθές, καθώς και επικαιροποιημένες.

13. *Μη αποποίηση/Δέσμευση*: Ο μηχανισμός αυτός παρέχει ιδανικά τα απαραίτητα μέσα και τεκμήρια, ώστε κανείς να μην μπορεί να αρνηθεί πως πραγματοποίησε όντως τις πληροφοριακά κρίσιμες πράξεις του, κανείς να μην μπορεί να αποδείξει πως δεν ήταν υπεύθυνος για αυτές.

14. *Διαβεβαίωση*:[42] Εξετάζει τις διαδικασίες, τις πολιτικές και τους ελέγχους που χρησιμοποιούνται για να αναπτύξουν την απαραίτητη εμπιστοσύνη πως τα τεχνικά και λειτουργικά μέτρα ασφάλειας λειτουργούν όπως πρέπει και όπως ακριβώς είναι επιθυμητό.

Το γκρουπ των 3 πρώτων υπηρεσιών αποτελούν ένα συχνά συναντούμενο και επαναλαμβανόμενο μοτίβο στο χώρο της ασφάλειας πληροφοριών και συστημάτων, όπως θα διαπιστώσουμε και στη ροή της παρούσας εργασίας. Αφορά και καθορίζει τους απαραίτητους όρους και πυλώνες, πάνω στους οποίους θα στηριχτεί μια ασφαλής πρόσβαση σε συστήματα και τις πληροφορίες που αυτά περιέχουν. Το γκρουπ αυτό είναι γνωστό ως *σχήμα αυθεντικοποίησης, εξουσιοδότησης και υπευθυνότητας (authentication, authorization and accounting/accountability)* ή πιο σύντομα -από τα αρχικά των αγγλικών όρων- ως σχήμα *ΑΑΑ*.[43]

Οι ακόλουθες υπηρεσίες 4-13 αφορούν τη διασφάλιση αποδεκτών και απαραίτητων συνθηκών σε πράξεις (ανάγνωση/εγγραφή, αποστολή/λήψη) επί των δεδομένων και την προστασία από σχετικές παραβιάσεις.

Η τριάδα 4-6 είναι οι υπηρεσίες ασφάλειας που σχετίζονται με το CIA μοντέλο και οφείλουν να εξασφαλίζουν την ισχύ των πρωταρχικά σημαντικών, περιγραφόμενων ιδιοτήτων.[44] Αντίστοιχα, οι 7-9 πραγματεύονται με τις υπόλοιπες απαιτήσεις της Parkerian επέκτασης.

Οι υπηρεσίες 10-13 περιφρουρούν ιδιότητες πιο σύγχρονων μοντέλων, ανάμεσα στις οποίες ξεχωρίζουν μακράν η επιτρεπτότητα και η μη αποποίηση (ή αλλιώς δέσμευση). Οι 2 αυτές ιδιότητες λαμβάνονται σοβαρά υπόψιν στο σχεδιασμό και παίζουν ήδη πρωτεύοντα ρόλο στις

[41] Με την έννοια της αχρείαστης περίσσειας, που αυξάνει την πιθανότητα σκόπιμης ή αμελούς υποβάθμισης της ασφάλειάς της.

[42] Κύρια, βιβλιογραφική αναφορά: [FFIEC-IS].

[43] Το σχήμα αυτό ενίοτε επεκτείνεται σε ΑΑΑΑ για να συμπεριλάβει και τη συγγενή έννοια του ελέγχου αξιολόγησης (auditing), που περιλαμβάνει όλες εκείνες τις προσπάθειες αποτίμησης της ισχύουσας ασφάλειας και του υπάρχοντος, σχετικού κινδύνου.

[44] Κύρια, βιβλιογραφική αναφορά: [NIST-ICS].

υλοποιήσεις των σύγχρονων συστημάτων και μηχανισμών ασφάλειας του υλικού και λογισμικού και των δεδομένων κάθε ΠΣ.

Στο τέλος (14) βρίσκεται η διαβεβαίωση, που (πρέπει να) αποτελεί έναν απώτερο στόχο για κάθε σύστημα ασφάλειας. Μέσω της υπηρεσίας διαβεβαίωσης παρέχονται στους χρήστες, τους ιδιοκτήτες και τους «πελάτες» και εν γένει στους στρατηγικούς «παίκτες» των συστημάτων πληροφοριών εκείνα τα πειστήρια (υπό τη μορφή τεκμηρίωσης υλοποιημένων διαδικασιών, μέτρων και προτύπων, καθώς και δοκιμών, μελετών και αξιολογήσεων ασφάλειας και κινδύνου), που αποδεικνύουν/πιστοποιούν με σαφήνεια και αντικειμενικότητα ένα αποδεκτό και επιθυμητό, ισχύον καθεστώς ασφάλειας. Με τον τρόπο αυτό επιτυγχάνεται διατήρηση της εμπιστοσύνης στο σύστημα, αλλά και τους χειριστές και ιδιοκτήτες αυτού, και αποφυγή της όποιας, στρατηγικής απώλειας από την απόσυρση αυτής της εμπιστοσύνης.

2.2.5 Απειλή-Περιστατικό-Κίνδυνος-Επισφάλεια-Αδυναμία-Παραβίαση ασφάλειας-Επίθεση-Επίπτωση-Επικινδυνότητα

Ως **απειλή (threat)** ορίζεται *"μία πιθανή ενέργεια ή ένα γεγονός που μπορεί να προκαλέσει την απώλεια ενός ή περισσοτέρων ιδιοτήτων ασφάλειας ενός πληροφοριακού συστήματος"*[45] και εννοιολογικά έχει υποθετικό ή θεωρητικό χαρακτήρα. Χρησιμοποιείται ευρέως στην διεξαγωγή ανάλυσης κινδύνου και είναι όρος που άμεσα προέρχεται από τη Διοικητική Επιστήμη.

Περιστατικό (incident) ονομάζεται *"ένα γεγονός που ενδέχεται να προέρχεται από την πραγματοποίηση μιας απειλής."*[46]

Κίνδυνος (danger) καλείται *"ό,τι μπορεί να προκαλέσει ζημιά σε μια ιδιότητα ενός αγαθού ή μιας ιδιοκτησίας"*.[47] Η υλοποίηση μιας απειλής κατά ενός ΠΣ συνεπάγεται πάντοτε πως συντρέχει και κάποιος, πιθανός κίνδυνος για τους στρατηγικά εμπλεκόμενους, αλλά και για τρίτα μέρη.

Ως **επισφάλεια (hazard)** σε ένα ΠΣ λογίζεται κάθε φορά *"η πιθανότητα να συμβεί κάποιο περιστατικό που να σχετίζεται με μια συγκεκριμένη, υπό εξέταση απειλή"*.[48]

Αδυναμία ή ευπάθεια (vulnerability or flaw) ενός συστήματος πληροφοριών συνιστά *"οποιοδήποτε εγγενές ή επίκτητο χαρακτηριστικό του ή οιουδήποτε εκ των συνθετικών του*

[45] Κύρια, βιβλιογραφική αναφορά: [LEKKAS-ICSTTP].

[46] Κύρια, βιβλιογραφική αναφορά: [KATSIKAS-ICSS].

[47] Όπως στην προηγούμενη υποσημείωση.

[48] Όπως στην προηγούμενη υποσημείωση.

μερών, του οποίου η παρουσία και μόνο είναι ικανή συνθήκη για να στοιχειοθετηθεί μια απειλή για το σύστημα και που μπορεί να γίνει αντικείμενο εκμετάλλευσης σε μια επίθεση/προσβολή".[49] Μια ευπάθεια έχει ως αιτιατό και συνοδεύεται πάντα από την ύπαρξη αντίστοιχης απειλής.

Παραβίαση ασφάλειας ή προσβολή (security violation or breach or exploit) καλείται *"οποιαδήποτε εκδηλωμένη απώλεια ενός ή περισσοτέρων ιδιοτήτων ασφάλειας ενός ΠΣ ή οποιαδήποτε παρέκκλιση από την ενεργή πολιτική ασφάλειας του συστήματος"*[50]. Στην ουσία, είναι μια απειλή που μετουσιώθηκε επιτυχώς σε πράξη και που αναγκαστικά θα προκαλέσει μικρή ή μεγαλύτερη επίπτωση.

Επίθεση (attack), τώρα, σε ένα σύστημα θεωρείται *"οποιαδήποτε απόπειρα παραβίασης της ασφάλειάς του ή προσβολής του, ασχέτως της σχετικής επιτυχίας της"* και είναι έννοια συνώνυμη της απειλής. Αποτυπώνει τη σαφή και απτή εκδήλωση μιας απειλής (100% επισφάλεια), μια απειλή που «πήρε σάρκα και οστά» και που έχει φυσικό, νοήμονα δράστη με κίνητρα και πρόθεση.[51] Αποτελεί αποτέλεσμα συντονισμένης ενορχήστρωσης και συνειδητοποιημένης δράσης και όχι αμέλειας, ατυχήματος ή ανεπιθύμητου γεγονότος.

Επίπτωση (impact) ονομάζεται *"η αναμενόμενη/εκτιμώμενη απώλεια ενός αγαθού ή το αυξημένο κόστος ή άλλη ζημιά που μπορεί να συμβεί ως αποτέλεσμα μιας συγκεκριμένης προσβολής"*[52].

Τέλος, **επικινδυνότητα (risk)** καλούμε *"το γινόμενο της επίπτωσης και του υπολογιζόμενου, απομένοντα, έπειτα από απόπειρα εφαρμογής όλων των υπαρχόντων μέσων προστασίας, κινδύνου"*.[53]

2.2.6 Είδη Απειλών και Επιθέσεων

Οι απειλές και συνάμα οι εν δυνάμει επιθέσεις εναντίον δικτυοκεντρικών ΠΣ μπορούν να ταξινομηθούν σε 4 μεγάλες κατηγορίες, αν λάβει κανείς υπόψιν του τα εξής 2 ιδιοχαρακτηριστικά τους· *το χώρο εκδήλωσης της απειλής* και *την ενεργητική ή όχι παρέμβαση-επέμβαση στη λειτουργία του συστήματος*.

Με βάση τα χαρακτηριστικά αυτά, μπορεί κανείς να προχωρήσει τον διαχωρισμό, σε απειλές λαμβάνουσες χώρα στη δικτυακή ζεύξη δεδομένων μεταξύ διασυνδεδεμένων Η/Υ του ΠΣ και

[49] Όπως στην προηγούμενη υποσημείωση.

[50] Όπως στην προηγούμενη υποσημείωση.

[51] Κύρια, βιβλιογραφική αναφορά: [STALLINGS-CNS].

[52] Κύρια, βιβλιογραφική αναφορά: [KATSIKAS-ICSS].

[53] Όπως στην προηγούμενη υποσημείωση.

σε απειλές που εκδηλώνονται εντός της σφαίρας επιρροής συγκεκριμένου στόχου-Η/Υ. Επίσης, μπορεί να διακρίνει μεταξύ ενεργητικών και παθητικών απειλών.[54] Συνθέτοντας τα παραπάνω παράγονται οι ακόλουθες 4 κατηγορίες περί ων ο λόγος, κάθε μια από τις οποίες πλαισιώνουμε με την ενδεικτική-συνοπτική αναφορά σε τυπικά παραδείγματα δράσης:

1. *Δικτυακές απειλές παθητικού τύπου*[55], όπως π.χ.
    a. Παρακολούθηση γραμμών επικοινωνίας/ Υποκλοπή (tapping, eavesdropping).
    b. Ανάλυση κίνησης (traffic analysis).
    c. Αστοχία-βλάβη δικτυακού εξοπλισμού, φυσική καταστροφή.
2. *Δικτυακές απειλές ενεργητικού τύπου*[56], όπως π.χ.
    a. Υπόδυση ρόλων – Κακόβουλη ενδιάμεση οντότητα (masquerading, man-in-the-middle attack).
    b. Επανεκπομπή πλαισίου δεδομένων (replay).
    c. Αλλοίωση μηνυμάτων (modifying).
    d. Άρνηση υπηρεσίας (DOS, DDOS).
    e. Σκόπιμη καταστροφή δικτυακής υποδομής.
3. *Εντός σφαίρας Η/Υ απειλές παθητικού τύπου*[57], λ.χ.
    a. Παρακολούθηση & Κατασκοπεία (keystroke-logging, monitoring, espionage).
    b. Φυσική ή εξ αμελείας καταστροφή ή βλάβη Η/Υ.
4. *Εντός σφαίρας Η/Υ απειλές ενεργητικού τύπου*[58], λ.χ.
    a. Υποβάθμιση λειτουργικότητας ή άρνηση χρήσης Η/Υ.
    b. Σκόπιμη βλάβη ή καταστροφή Η/Υ.
    c. Αλλοίωση/Παραχάραξη δεδομένων.

Οι ενεργητικού τύπου επιθέσεις έχουν την τάση να γίνονται εν γένει ευκολότερα αντιληπτές από τις αντίστοιχες παθητικού τύπου, καθώς παρεμποδίζουν ή αλλοιώνουν αισθητά τη

[54] Κύρια, βιβλιογραφική αναφορά: [STALLINGS-CNS].

[55] Κύρια, βιβλιογραφική αναφορά: [BERG_GOEL-STNBA].

[56] Όπως στην προηγούμενη υποσημείωση.

[57] Κύρια, βιβλιογραφική αναφορά: [NIST-ICS].

[58] Όπως στην προηγούμενη υποσημείωση.

φυσιολογική λειτουργία και απόκριση των ΠΣ ή αφήνουν ευδιάκριτα ίχνη σε αυτούς που γνωρίζουν που να κοιτάξουν. Από την άλλη, οι παθητικές επιθέσεις, λόγω της επιθυμητής διακριτικότητάς τους, απαιτούν μια κάποια ύπαρξη εξειδικευμένου, υλικοτεχνικού εξοπλισμού και ως επί το πλείστον πολύπλοκου λογισμικού στη διάθεση του επιτιθέμενου, πράγμα που τις καθιστά σαφώς πιο δύσκολα υλοποιήσιμες.

Όλες οι προαναφερθείσες απειλές και επιθέσεις οδηγούν σε υποβάθμιση ή απώλεια συγκεκριμένων ιδιοτήτων ασφάλειας του δικτυοκεντρικού συστήματος πληροφοριών, όπως αυτές περιγράφονται στα μοντέλα που έχουν συζητηθεί σε πρότερη φάση. Αντικείμενο μελέτης της εργασίας αυτής θα αποτελέσουν οι εν δυνάμει επιθέσεις σε δικτυοκεντρικά ΠΣ, που επιτυγχάνονται με χρήση αυτοαναπαραγόμενου κακόβουλου λογισμικού. *Η χρήση κακόβουλου λογισμικού, θα μπορούσε να συμβάλλει, να διευκολύνει και να εξυπηρετήσει ποικιλοτρόπως τους στόχους οποιασδήποτε επίθεσης και των 4 τύπων* εισάγοντας κίνδυνο για τα ΠΣ. Το επιβλαβές λογισμικό, που φέρει την ιδιότητα της αναπαραγωγής, όπως θα δούμε στην πορεία αυτής της διατριβής, μπορεί να αναδειχθεί σε ικανότατο φορέα ενεργητικών επιθέσεων, τόσο σε επίπεδο δικτύου, όσο και στη σφαίρα δράσης κάθε μεμονωμένου υπολογιστή. Υπό προϋποθέσεις παρέχει δε και τη δυνατότητα υποστήριξης παθητικού τύπου επιθέσεων.

2.2.7 Κατηγοριοποίηση δεδομένων

Ευαίσθητα δεδομένα ονομάζονται συνήθως *"εκείνα των οποίων η κρισιμότητα είναι τέτοια, ώστε τυχόν αποκάλυψη-διαρροή σε μη έμπιστες οντότητες, με άγνωστες προθέσεις, μπορεί να οδηγήσει σε απώλεια στρατηγικού πλεονεκτήματος ή υποβάθμιση του επιπέδου ασφάλειας από μέρους θιγόμενων προσώπων και οργανισμών"*[59]. Κοινώς, μια ενδεχόμενη απώλεια εμπιστευτικότητας για τα δεδομένα αυτά μπορεί να αποβεί εξαιρετικά ζημιογόνα. Στην κατηγορία των ευαίσθητων δεδομένων ανήκουν οι σφαίρες του ιδιωτικού απόρρητου και των ευαίσθητων, προσωπικών δεδομένων, των εμπιστευτικών επιχειρησιακών πληροφοριών, των απόρρητων κυβερνητικών εγγράφων και μυστικών πληροφοριών και γενικότερα οποιαδήποτε, άλλη πληροφορία και γνώση, των οποίων ενδεχόμενη δημοσιοποίηση θα σήμαινε σοβαρό κίνδυνο είτε για τους όποιους φύλακες ή τους φυσικούς κατόχους, είτε για ευρύτερες κοινότητες.

Οποιουδήποτε είδους απειλή όμως σε βάρος της ασφάλειας ορισμένων δεδομένων, πρακτικά μπορεί να έχει τα ίδια ή και χειρότερα αποτελέσματα με αυτά της απώλειας της εμπιστευτικότητας, στην κατηγορία των ευαίσθητων δεδομένων. Για το λόγο αυτό εισάγεται

[59] Πηγή: Διαδίκτυο, ιστοχώρος της online εγκυκλοπαίδειας WikiPedia, http://en.wikipedia.org/wiki/Sensitive_information.

η έννοια των *κρίσιμων δεδομένων ή πληροφοριών* για να αποδώσει *"όλα εκείνα τα δεδομένα και τις πληροφορίες που είναι τέτοιας ζωτικής σημασίας, ώστε μια απειλή -οποιασδήποτε μορφής- εναντίον της ασφάλειάς τους, να καταφέρνει εν δυνάμει, καίριο, στρατηγικό πλήγμα για τους όποιους θιγόμενους οργανισμούς και πρόσωπα (κατόχους, παρόχους και καταναλωτές/χρήστες των εν λόγω ΠΣ ή/και τρίτα, μη άμεσα εμπλεκόμενα μέρη)"*.[60] Με λίγα λόγια, κρίσιμα θεωρούνται τα δεδομένα, όταν η απώλεια μιας ή περισσοτέρων ιδιοτήτων της ασφάλειάς τους μπορεί να προκαλέσει σοβαρές, ανεπιθύμητες συνέπειες σε κάποιες οντότητες. Γίνεται άμεσα κατανοητό ότι τα ΠΣ, στα οποία με τον ένα ή τον άλλο τρόπο εμπλέκονται κρίσιμα δεδομένα, θεωρούνται *κρίσιμα ΠΣ*.

2.2.8 Ασφάλεια και Προστασία στην Κοινωνία της Πληροφορίας

Η έννοια της προστασίας των ΠΣ από την πραγμάτωση διαφόρων απειλών κατά της ασφάλειάς τους είναι στενά συνυφασμένη με τους μηχανισμούς πρόληψης, παρακολούθησης, διάγνωσης και αναγνώρισης, έγκαιρης θεραπείας και επανόρθωσης-ανάνηψης ευπαθειών, απειλών και παραβιάσεων, που εντάσσονται στα πλαίσια μιας ευρύτερης διαδικασίας ανάλυσης, αποτίμησης και αποφυγής-περιορισμού των κινδύνων (risk analysis, evaluation, mitigation and avoidance). Οι τρεις αυτοί μηχανισμοί αποτελούν τα εχέγγυα για την ασφάλεια των σύγχρονων ΠΣ και αναλύονται πιο διεξοδικά παρακάτω:[61]

- **Διαδικασία πρόληψης (Prevention Process)**[62]

  "Πρόνοια για την παρεμπόδιση παραβιάσεων ασφάλειας". Η διαδικασία αυτή περιλαμβάνει 2 διακριτά τμήματα. Το τμήμα πρόληψης ευπαθειών ασχολείται με τον αέναο εντοπισμό και διόρθωση τυχόν αδυναμιών ενός συστήματος, ώστε να μετριάζονται οι αριθμοί εκδηλώσεων απειλών, ενώ το τμήμα πρόληψης απειλών είναι υπεύθυνο για την προστασία από την έκθεση σε απειλές, ώστε να προλαμβάνεται έγκαιρα η εκδήλωση γνωστών βλαβών, ατυχημάτων ή επιθέσεων ή/και να εμποδίζεται μια τρέχουσα παραβίαση και η ζημιά της πριν επεκταθεί, στο ίδιο το σύστημα ή σε γειτονικά του ή σε άλλα με τα οποία επικοινωνεί. Το δεύτερο τμήμα αποτελεί έναν κάποιο μηχανισμό ανατροφοδότησης από το στάδιο παρακολούθησης,

---

[60] Πηγή: "Competing in the 21st Century: Harnessing Your Organization's Business Critical Information", Tom Raleigh, Business Information Mapping, Inc., διαθέσιμο από το δεσμό http://www.expert-insights.com/report.asp?id=194.

[61] Πηγή: "The Increasing Importance of IT 'Controls'", George Spafford, 2004, διαθέσιμο από το δεσμό http://itmanagement.earthweb.com/netsys/article.php/3402561.

[62] Κύρια, βιβλιογραφική αναφορά: [PARKER-CSM].

διάγνωσης και αναγνώρισης και μπορεί με τη σειρά του να τροφοδοτεί το πρώτο τμήμα πρόληψης, με επισημάνσεις για τις τυχόν αδυναμίες στις οποίες οφείλονται κάποιες απειλές, προκειμένου αυτές να διορθωθούν. Ένα ενδεικτικό παράδειγμα σχετικής τεχνικής, που απαντά κανείς στο τμήμα αυτό, είναι η *προληπτική καραντίνα ή αποκλεισμός-αποκοπή του προσβεβλημένου συστήματος* ή μέρους αυτού από το περιβάλλον του, ώστε να αποφεύγεται τρόπον τινά η περαιτέρω εξάπλωση μιας υποβάθμισης εν εξελίξει. Επίσης, στη «φαρέτρα» της διαδικασίας πρόληψης περιλαμβάνονται και *πρακτικές εκφοβισμού (deterrence) και σωφρονισμού των επίδοξων επιτιθέμενων*, αλλά και γενικότερα των όσων προκαλούν σκόπιμα ή άθελά τους κάποιο περιστατικό ασφάλειας, μέσω επικοινώνησης πιθανών, νομικών συνεπειών των εν λόγω πράξεων.

Η διαρκής εκπαίδευση των χρήσιμα και κρίσιμα εμπλεκόμενων στο εκάστοτε ΠΣ οντοτήτων στα θέματα ασφάλειας και προστασίας του είναι διάχυτη σε όλα τα βήματα της διαδικασίας πρόληψης.

Στόχος της διαδικασίας πρόληψης και κυρίως του τμήματος πρόληψης ευπαθειών είναι η μεγαλύτερη δυνατή «ανοσοποίηση» των συστημάτων. Το τμήμα αυτό βρίσκεται πάντοτε σε συνεχή λειτουργία και εγρήγορση, ενώ το δεύτερο τμήμα της προληπτικής διαδικασίας ενεργοποιείται με το κατάλληλο ερέθισμα (εκδήλωση γνωστής απειλής, αναγνώριση έκθεσης σε νέα απειλή).

- **Διαδικασία παρακολούθησης, διάγνωσης και αναγνώρισης (Monitoring, Detection & Identification Process)**[63]

"Διαρκής εποπτεία-Εξακρίβωση της κατάστασης έκθεσης σε απειλή". Όπως και στη βιολογία, η διαρκής παρακολούθηση της καλής και αναμενόμενης λειτουργίας ενός συστήματος, η έγκαιρη διάγνωση της πιθανής εκδήλωσης μιας απειλής και της προκαλούμενης παραβίασης της ασφάλειας του συστήματος αυτού και η επιτυχής αναγνώριση του είδους και της ιδιαίτερης φύσης αυτών είναι απαραίτητα στοιχεία για μια αποτελεσματική θεραπεία τους. Προϋπόθεση, όμως, για τη διάγνωση και αναγνώριση της όποιας παραβίασης ασφάλειας είναι η συνεχής, στενή παρακολούθηση του ΠΣ, ενώ επίσης μια απλή διάγνωση ύποπτης ή ασυνήθιστης δραστηριότητας, χωρίς αποφασιστική και έγκυρη αναγνώριση του τύπου της απειλής, συνήθως δεν επαρκεί για την ουσιαστική ανάνηψή του συστήματος. Η απομνημόνευση του ιδιαίτερου χαρακτήρα κάθε νέας αναγνωρισμένης απειλής, ώστε

[63] Όπως στην προηγούμενη υποσημείωση.

να προλαμβάνεται ή να εντοπίζεται εγκαίρως μια παρόμοια μελλοντική της εκδήλωση, αποτελεί ουσιαστικό μέρος του σταδίου αυτού.

Ως επόμενο βήμα, πέρα από την ανάληψη θεραπευτικής δράσης για την επανόρθωση του προσβεβλημένου συστήματος, πολλές φορές συναντάται εκ νέου και κάποιου είδους προληπτικό στάδιο για τον περιορισμό μιας περαιτέρω έκθεσης κείμενων και παρακείμενων συστημάτων στην τρέχουσα απειλή.

Τα υποσύστημα παρακολούθησης είναι διαρκώς ενεργό στο παρασκήνιο του υποστηριζόμενου ΠΣ, το αντίστοιχο της διάγνωσης ιδανικά θα «τρέξει» μόνο την ώρα της παρατήρησης κάποιας μη αναμενόμενης δραστηριότητας ή συμβάντος, ενώ εκείνο της αναγνώρισης τίθεται σε λειτουργία, αμέσως μόλις εντοπιστεί κάποια παραβίαση και έκθεση σε απειλή.

- **Διαδικασία ανταπόκρισης, θεραπείας και επανόρθωσης (Recovery & Remediation Reaction Process)**[64]

  "Αφαίρεση της εκδήλωσης της απειλής (θεραπεία) από το σύστημα και αποκατάσταση της ζημιάς, που ενδεχομένως προκάλεσε (επανόρθωση), αν και εφόσον η ανάλυση/αξιολόγηση του σχετικού κινδύνου επέδειξε επιπτώσεις και επισφάλειες μη αποδεκτές από τους στρατηγικά εμπλεκόμενους φορείς ελέγχου της διαδικασίας". Απαραίτητη συνθήκη για τη σωστή καταπολέμηση της εκδηλωθείσας απειλής είναι η γνώση του είδους της, ενώ συχνά παίζει καθοριστικό ρόλο και το χρονικό διάστημα που μεσολάβησε μεταξύ έκθεσης και διάγνωσης.

  Η θεραπεία περιλαμβάνει πλήρη εξάλειψη της παραβίασης της ασφάλειας, αλλά δε συνεπάγεται εξαφάνιση και της όποιας ευπάθειας, άρα δεν εγγυάται τη μη επανεμφάνιση της απειλής. Η επανόρθωση αφορά στη μετρίαση των επιπτώσεων από την έκθεση στην απειλή και την επαναφορά σε συνθήκες ομαλούς και ικανοποιητικής λειτουργίας, τουλάχιστον όπως αυτές πριν την έκθεση. Η ιδανική διάρκεια της φάσης επανόρθωσης ποικίλλει, διότι διαθέτει έντονο και το υποκειμενικό στοιχείο, καθώς εξαρτάται σε μεγάλο βαθμό και από τους στρατηγικούς στόχους του υπό επανόρθωση συστήματος. Συνήθως, πάντως, τείνει να αποδεικνύεται αρκετά πιο χρονοβόρα από αυτήν της θεραπείας, λόγω κυρίως των απαραίτητων λειτουργιών αποκατάστασης των τυχόντων προβλημάτων, που προκάλεσε η προσβολή του συστήματος.

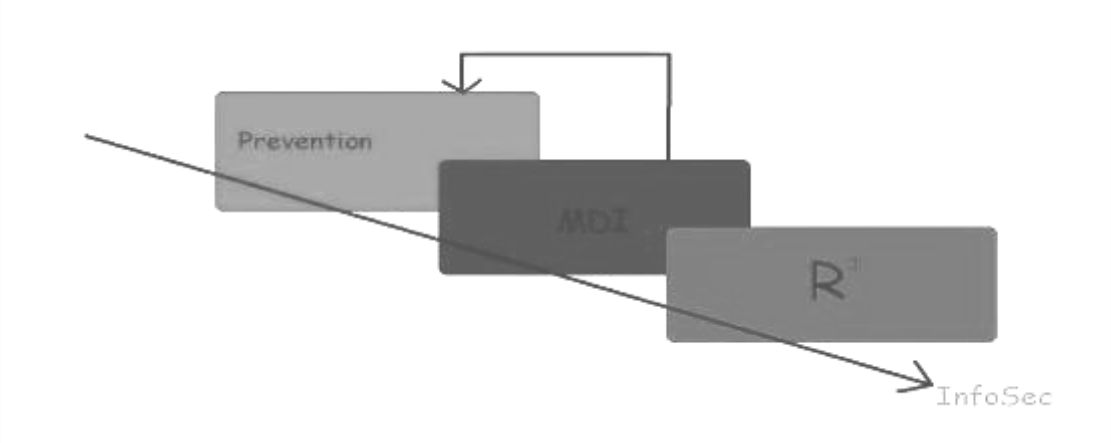
[64] Όπως στην προηγούμενη υποσημείωση.

Η καταγραφή των μεθόδων θεραπείας και επανόρθωσης που ακολουθήθηκαν κατά περίπτωση, καθώς και των αντικειμενικών τους αποτελεσμάτων, είναι συνήθης πρακτική που συμβάλλει στη θεμελίωση βέλτιστων κανόνων και υποδειγμάτων δράσης.

Ολόκληρος ο μηχανισμός ανταπόκρισης βρίσκεται σε κατάσταση αεργίας και πυροδοτείται μόνο όταν οι περιστάσεις το απαιτήσουν, όταν δηλαδή διαγνωστεί μια περίπτωση παραβίασης ασφάλειας και εξακριβωθεί το είδος της.

Κατά την πορεία κάθε συστήματος ασφάλειας στο χρόνο συνηθίζεται να φυλάσσονται εκτεταμένα πρότυπα και μοτίβα γνωστών παραβιάσεων ασφάλειας και των κατάλληλων αντίμετρών τους. Τα ιδιαίτερα χαρακτηριστικά κάθε νέας παραβίασης μόλις απομονωθούν, καταγράφονται και προστίθενται στην ήδη υπάρχουσα υποδομή γνώσης. Το ίδιο συμβαίνει και με τις μεθόδους εκείνες που εμφανίζονται να περιορίζουν δραστικά ή/και να θεραπεύουν την εκάστοτε παραβίαση. Με τον τρόπο αυτό, λαμβάνεται μέριμνα για την έγκαιρη πρόληψη, διάγνωση και θεραπεία παρόμοιων περιστατικών στο μέλλον και (άρα) τη διαρκή, ποιοτική αναθεώρηση-ανανέωση-αναβάθμιση των προαναφερόμενων, τριών μηχανισμών και συστημάτων περιφρούρησης της ασφάλειας.

Οι περιγραφόμενες σχέσεις μεταξύ των τριών διαδικασιών-βημάτων προστασίας των ΠΣ απεικονίζονται με γλαφυρό τρόπο στο παρακάτω σχήμα:



Σχήμα 1: Ξεχωριστές, λειτουργικές μονάδες στη διαδικασία της Ασφάλειας πληροφοριών

Δεν υπάρχουν -ακόμη τουλάχιστον- ιδανικά συστήματα προστασίας των ΠΣ, όσο βαθμό αυτοματοποίησης και να διαθέτουν, όση αφοσίωση και να επιδεικνύουν οι άνθρωποι που εμπλέκονται. Το πρότυπο σύστημα, πάντως, θα πρέπει να λειτουργεί σύμφωνα με τις

προαναφερόμενες διαδικασίες και να τις διατρέχει (και επικαιροποιεί με βάση τρέχοντες, στρατηγικούς στόχους των ενδιαφερόμενων οργανισμών) ανελλιπώς. Ακόμη και σε ένα τέτοιο «τέλειο» σύστημα, όμως, στο βαθμό που συμμετέχουν οι άνθρωποι, που έτσι και αλλιώς αποτελούν πηγή ποικίλων και μεταβαλλόμενων, εσωτερικών ευπαθειών και αδυναμιών, τόσο για το ίδιο το ΠΣ όσο και για τους μηχανισμούς προστασίας αυτού, σκόπιμο και τελικά στην πράξη απαιτητό είναι να προβλέπονται και να εφαρμόζονται πολύπλοκες και απαιτητικές δραστηριότητες, όπως η συνεχής εκπαίδευση στους κανόνες δεοντολογίας και δράσης-συμπεριφοράς, η διαρκής αναθεώρηση και αναβάθμιση των μέτρων αυτών με βάση τις τρέχουσες συνθήκες και προσεκτικός, ο κατάλληλος καταμερισμός αρμοδιοτήτων και ευθυνών, ώστε να μην περιπλέκονται και παρεξηγούνται ρόλοι, εργασίες και (νομικές) υπευθυνότητες και να γίνεται καλύτερη και αποδοτικότερη από πλευράς ασφάλειας η εκμετάλλευση των διαθέσιμων πόρων. Κάτι τέτοιο δεν είναι, βεβαίως, σήμερα το πιο κοινότυπο παράδειγμα λειτουργίας των συστημάτων προστασίας.

Καθώς δεν παρέχεται, λοιπόν, ιδανική προστασία, έτσι δεν υπάρχει και ιδανική ασφάλεια για τα ΠΣ. Η διασφάλιση της απρόσκοπτης και ασφαλούς λειτουργίας τους, στη σημερινή εποχή της πληροφοριακής επανάστασης, είναι μια διαρκής διαπάλη κόντρα σε αστάθμητους παράγοντες και αντικρουόμενα συμφέροντα, που την καθιστούν εξαιρετικά δύσκολη και απαιτητική σε κάθε λογής πόρους. Στο επίκεντρο αυτής της διαπάλης, σήμερα, στέκεται και το κακόβουλο λογισμικό ως όπλο για την «επίλυση» των οξυμένων, πληροφοριακών αντιπαλοτήτων και την επιτέλεση λογής εχθροπραξιών, όπως θα παρουσιάσουμε ευθύς αμέσως.

2.3 Πληροφοριακές Εχθροπραξίες

Η εποχή της πληροφορίας, όπως είδαμε, χαρακτηρίζεται από την εξάπλωση των πληροφοριακών συστημάτων και την αυξημένη δυνατότητα για ταχεία συλλογή, αφομοίωση, επεξεργασία και διάδοση πληροφοριών. Σήμερα, εκείνοι οι οποίοι έχουν πρόσβαση σε συστήματα πληροφοριών ή σε έλεγχο αυτών, μπορούν άμεσα να επηρεάζουν την κοινή γνώμη, το διεθνές εμπόριο, τον πολιτικό διάλογο, ακόμα και την ασφάλεια των εθνών.[65]

Μολονότι ο όρος *πληροφοριακή εχθροπραξία ή πόλεμος* προέρχεται από την στρατιωτική ορολογία και δημιουργήθηκε για να περιγράψει κυρίως τις επιθέσεις στα σύγχρονα, στρατιωτικά, πληροφοριακά συστήματα, που αποσκοπούν στην απόκτηση και επιβολή *πληροφοριακής κυριαρχίας (information dominance)* επί των αντιπάλων *διαμέσω*

[65] Κύρια, βιβλιογραφική αναφορά: [KIKIRAS-IW].

δικτυοκεντρικού πολέμου (network-centric warfare)[66], εύκολα μπορεί κανείς να επεκτείνει λογικά την εν λόγω έννοια προκειμένου να συμπεριλαμβάνει τις διάφορες επιθέσεις σε πάσης φύσεως ΠΣ της εποχής μας, που έχουν σαν κύριο σκοπό την εξασφάλιση *πληροφοριακής υπεροχής (information superiority)* στον επιτιθέμενο.

Στον επίσημο ορισμό ,τον οποίο έχουν υιοθετήσει οι Αμερικανικές, ένοπλες δυνάμεις, με την από 02/01/1996 απόφαση της υπ. αριθμ. 3210.01 επιτροπής (Joint chiefs of staff instruction committee (CJCSI)), γράφονται τα εξής:[67] *"Πληροφοριακή Εχθροπραξία: Ενέργειες οι οποίες αναλαμβάνονται με σκοπό την επίτευξη πληροφοριακής υπεροχής διαμέσου του επηρεασμού των εχθρικών πληροφοριών, των διαδικασιών που χρησιμοποιεί και βασίζονται σε πληροφορίες, των πληροφοριακών συστημάτων και δικτύων του, ενώ ταυτόχρονα προστατεύονται οι αντίστοιχες φίλιες πληροφορίες, διαδικασίες, πληροφοριακά συστήματα και δίκτυα"*.

Μία περισσότερο ακαδημαϊκή προσπάθεια ορισμού είναι αυτή του καθηγητή A. Coetzel από το Πανεπιστήμιο της Νέας Υόρκης, ο οποίος ορίζει την πληροφοριακό εχθροπραξία ως εξής:[68] *"Πληροφοριακή Εχθροπραξία είναι απλά η χρήση πληροφοριών για την επίτευξη συγκεκριμένου αντικειμενικού σκοπού. Η πληροφορία είναι από μόνη της ένας κυρίαρχος παράγοντας εθνικής και εμπορικής δύναμης και ακόμη πιο σημαντικά μετατρέπεται συνεχώς σε μία ζωτική εθνική πηγή, η οποία υποστηρίζει τη Διπλωματία, τον Οικονομικό Ανταγωνισμό και την αποτελεσματική ανάπτυξη στρατιωτικών δυνάμεων"*.

Σε έναν πιο ευρύ, τέλος, ορισμό θα μπορούσε να πει κανείς πως πληροφοριακή εχθροπραξία είναι *"η χρήση και μεταχείριση των πληροφοριών και των ΠΣ στην αναζήτηση στρατηγικού, ανταγωνιστικού πλεονεκτήματος, μεταξύ αντιμαχόμενων οντοτήτων και δυνάμεων"*[69]. Περιλαμβάνει διαδικασίες κατασκοπείας, ελέγχου, επηρεασμού της ποιότητας ή της καλής λειτουργίας κρίσιμων και χρήσιμων στον αντίπαλο-στόχο ΠΣ, με παράλληλη διασφάλιση και ενίσχυση της αποτελεσματικότερης λειτουργίας των κρίσιμων και χρήσιμων στον επιτιθέμενο ΠΣ. Απώτερος σκοπός κάθε εμπλεκόμενης οντότητας είναι η εδραίωση πληροφοριακής κυριαρχίας εις βάρος των αντιπάλων της.

Στα προλεγόμενα, σκόπιμα, δε γίνεται αυστηρή διάκριση μεταξύ των διαφορετικών, δυνατών τύπων ενεργειών, που συνιστούν πληροφοριακή εχθροπραξία, καθώς το αντικείμενο της πληροφοριακής εχθροπραξίας άπτεται εν γένει πολλαπλών τομέων και επιδέχεται αρκετών διαφοροποιήσεων, όσον αφορά τα μέσα εκδήλωσης της εχθροπραξίας, τα πεδία δράσης των

---

[66] Κύρια, βιβλιογραφική αναφορά: [ALBERTS-UIAW].

[67] Απόφαση του γενικού επιτελείου με κωδικό και θέμα CJCSI 3210.01: Joint Information Warfare Policy.

[68] Κύρια, βιβλιογραφική αναφορά: [KIKIRAS-IW].

[69] Κύρια, βιβλιογραφική αναφορά: [KROSS-JDCCW].

αντίπαλων δυνάμεων και τα είδη των εμπλεκόμενων ΠΣ. Π.χ. πληροφοριακή εχθροπραξία αποτελεί η προσωρινή κατάρρευση των τηλεπικοινωνιών ενός στόχου με χρήση μικροκυμάτων κατά τις διάφορες, στρατιωτικές επεμβάσεις[70] ή μια οργανωμένη προσπάθεια τηλεφωνικών υποκλοπών σε βάρος ανώτερων στελεχών μιας ανταγωνίστριας επιχείρησης[71] ή ακόμα η σκόπιμη καταστροφή του φυσικού μέσου μιας υποθαλάσσιας, καλωδιακής ζεύξης δεδομένων. Αν, πάντως, επιθυμούσαμε μια πρώτη και εύκολη κατηγοριοποίηση της πληροφοριακής εχθροπραξίας, θα μπορούσαμε να καταλήξουμε στην παρακάτω απλή κατάταξη με τρεις, ξεκάθαρες διαβαθμίσεις[72] στην κλίμακα έντασης και βαρύτητας:

1. Προσωπικού επιπέδου πληροφοριακή εχθροπραξία

Η 1η κατηγορία εχθροπραξίας πληροφοριών είναι μια *πράξη απευθείας επίθεσης ενάντια στην ιδιωτικότητα του ατόμου*: τα ψηφιακά του στοιχεία, τα διάφορα αρχεία ή τις άλλες μερίδες της ηλεκτρονικής ή άλλως καταγεγραμμένης ουσίας ενός φυσικού προσώπου. Οι στόχοι του επιτιθέμενου ποικίλλουν:

- Παρακολούθηση/Υποκλοπή,
- Παραχάραξη/Πλαστοπροσωπία,
- Οικονομική εκμετάλλευση/εξαπάτηση,
- Κατάστρωση προφίλ,
- Δευτεροβάθμιες επιθέσεις (cascaded attacks).

Επίσης, *πολλές και διάφορες είναι και οι ενσαρκώσεις της επιτιθέμενης οντότητας*, που πρακτικά συμβαίνει να είναι ο οποιοσδήποτε από τον κοντινό συνεργάτη, μέχρι την ίδια την κυβέρνηση μιας χώρας[73].

2. Επιχειρηματική-Κορπορατική, πληροφοριακή σύρραξη

Ο δεύτερος τύπος αφορά τη διαμάχη που μαίνεται μεταξύ εταιρειών και οργανισμών για την *απόκτηση του στρατηγικού, επιχειρηματικού πλεονεκτήματος* και κορυφώνεται με τη βιομηχανική και οικονομική κατασκοπεία, την κλοπή μυστικών σχεδίων, την ωτακουστία (eavesdropping) επικοινωνιών και την υπονόμευση της καλής λειτουργίας των αντίπαλων

[70] Π.χ. όπλα ραδιοφωνικού σήματος υψηλής ενέργειας (HERF Guns) ή βόμβες ηλεκτρομαγνητικού παλμού (EMP Bombs).

[71] Στα πλαίσια μιας προσπάθειας βιομηχανικής κατασκοπείας.

[72] Κύρια, βιβλιογραφική αναφορά: [SCHWARTAU-CESIW].

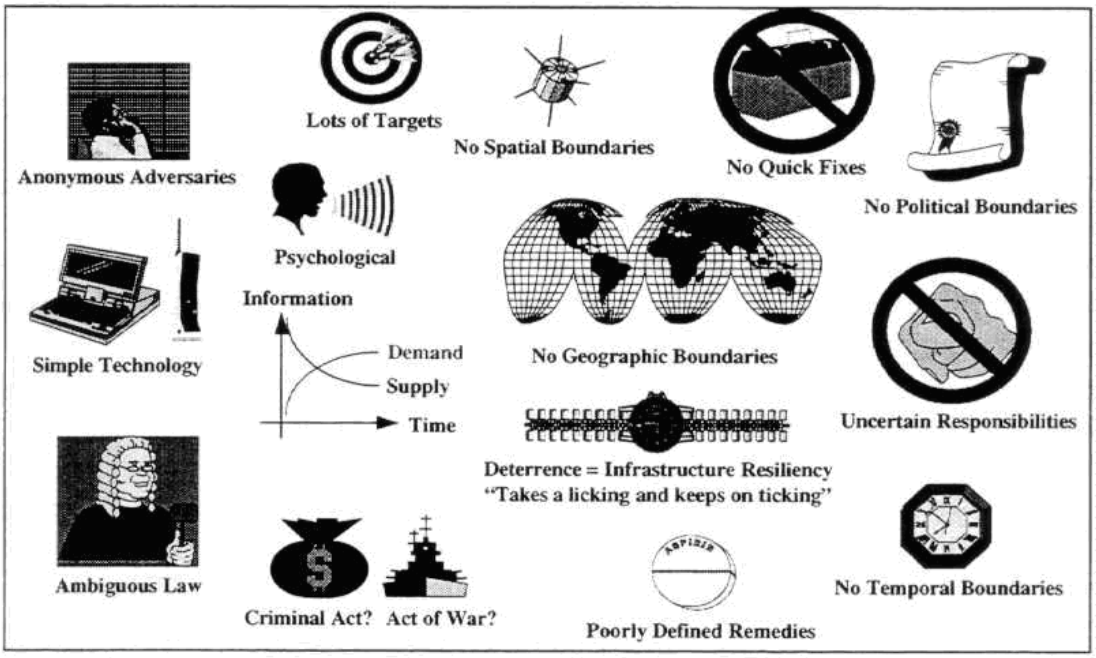
[73] Στο ακραίο, μα δυστυχώς όχι και τόσο παρωχημένο, σενάριο της κρατικής παρακολούθησης.

δομών και συστημάτων, καθώς και άλλες παρόμοιες ενέργειες, που πραγματοποιούνται στα πλαίσια ετούτα.

3. Παγκόσμιος πληροφοριακός ανταγωνισμός-πόλεμος

Το τρίτο και τελευταίο στάδιο σχετικού μεγέθους στην εχθροπραξία πληροφοριακού χαρακτήρα μεταφέρει τη σημασία και την ισχύ των 2 προηγούμενων στο *διεθνές σκηνικό* πολλαπλασιάζοντας την με τον *υψηλό βαθμό οργάνωσης και προετοιμασίας, ικανότητας και κατάρτισης, αλλά και «στρατιωτικής» πειθαρχίας, από μέρους των μετεχόντων και εμπλεκόμενων, πληροφοριακών μαχητών* (cyberwarriors) 3ης κατηγορίας[74]. Ο στόχος μπορεί να είναι οποιοσδήποτε από ένα μεμονωμένο άτομο ή μια εταιρεία μέχρι ολόκληρες χώρες. Φορείς εν λόγω επιθέσεων μπορεί να είναι αντίστοιχα, αντιπαλόμενα άτομα ή οργανισμοί, αλλά ακόμα και αντιμαχόμενες στρατιωτικές δυνάμεις και (παρα- ή τρομο-)κρατικοί μηχανισμοί. Σκοπός των συρράξεων είναι η *πληροφοριακά επιτρεπόμενη εξουδετέρωση ή αποδυνάμωση του όποιου (προσωπικού, οικονομικού, πολιτικού ή στρατιωτικού) εχθρού*, που δύναται να επιδρά σε οποιονδήποτε από τους κρίσιμους και «πληροφοριακά ευαίσθητους» τομείς ύπαρξης και δράσης του. Το πεδίο μάχης μπορεί να ξεπερνά και να διαπερνά πάσης φύσεως σύνορα, επικουρούμενο από τις σύγχρονες, τεχνολογικές υποδομές, εφαρμογές και υπηρεσίες της μετα-βιομηχανικής κοινωνίας. Το *τίμημα* που ενδεχομένως θα «πληρωθεί» είναι *ύψιστης σημασίας* και οι συνακόλουθες *επιπτώσεις ευρείας αίσθησης*.

[74] Στα άτομα αυτά συγκαταλέγονται μόνο επαΐοντες και μύστες της Πληροφορικής Τεχνολογίας, με επαρκείς γνώσεις και εμπειρία, αλλά και αξιοσημείωτο επαγγελματισμό.



Σχήμα 2: Το σύνθετο και πολυδιάστατο παζλ του πληροφοριακού πολέμου

Στα πλαίσια της εργασίας αυτής, *θα μας απασχολήσει συγκεκριμένα η καθαρά ηλεκτρονική μορφή/διάσταση της πληροφοριακής εχθροπραξίας* και των τριών προαναφερόμενων τύπων, που αφορά *ηλεκτρονικού τύπου επιθέσεις και άμυνα σε δικτυοκεντρικά ΠΣ, με βάση τυποποιημένους Η/Υ* και με την *καθολική παρουσία του αυτοαναπαραγόμενου, κακόβουλου λογισμικού* ή εν συντομία εφεξής *οπλολογισμικού*[75].

Από τους παραπάνω ορισμούς και λαμβάνοντας υπόψιν τα όσα διατυπώθηκαν περί ασφάλειας πληροφοριών, εύκολα συμπεραίνει κανείς ότι *η πληροφοριακή εχθροπραξία ως γενικευμένη επίθεση με στόχο ΠΣ συνιστά απειλή για την ασφάλεια δοθέντος ΠΣ*. Η απειλή αυτή για να αποκτήσει υπόσταση χρειάζεται την ύπαρξη ενδεχόμενης ευπάθειας ή κενού ασφάλειας ή φορέα αδυναμίας στα συστήματα αυτά, ώστε εκμεταλλευόμενη αυτή την παρουσία να εκδηλωθεί ως πραγματική επίθεση κατά των συστημάτων. *Στα δικτυοκεντρικά πληροφοριακά συστήματα διασυνδεδεμένων, ηλεκτρονικών υπολογιστών, φορέα αδυναμίας μπορεί να αποτελεί κάθε χρήσιμα εμπλεκόμενη, λειτουργική οντότητα*[76]:

- **Υλικό και Λογισμικό**, κάθε υπολογιστικής μονάδας που αποτελεί μέρος του ΠΣ: Το υλικό και το λογισμικό των κόμβων των σύγχρονων, δικτυοκεντρικών ΠΣ

[75] Ο όρος οπλολογισμικό θα χρησιμοποιείται ως απόδοση του αγγλικού software cyberweapons εναλλακτικά με τον αντίστοιχης σημασίας κυβερνοόπλα λογισμικού, καθόλη τη συγγραφική αυτή προσπάθεια.

[76] Βλέπε ορισμό και επεξήγηση δικτυοκεντρικών ΠΣ στο εδάφιο 2.1.2.

αποτελούν την κατεξοχήν, πρώτη πηγή ευπαθειών, αφού αποτελούν όργανα ζωτικής σημασίας (καρδιά και νους) για τη λειτουργία των συστημάτων αυτών.

- **Δεδομένα ΠΣ**: Οι πληροφορίες εντός των ΠΣ και των δικτυακών «αρτηριών» διασύνδεσής τους, ως άλλο «αίμα», παρέχουν εγγενώς τρόπους μόλυνσης όλου του πληροφοριακού σώματος.

- **Δικτυακή υποδομή** του ΠΣ: Οποιαδήποτε παραμικρή αλλαγή ή παρεμβολή στο δικτυακό σκελετό των πληροφοριακών κέντρων επηρεάζει δυνητικά την ασφάλεια του όλου οικοδομήματος.

- **Άνθρωποι** (δια)χειριστές και χρήστες: Η αλληλεπίδραση των ανθρώπων με τα ΠΣ και ιδιαίτερα αυτή των «κλειδούχων» είναι απαραίτητη, φέρει όμως -εκ των προτέρων- τους σπόρους και τις δυνατότητες της υπονόμευσης.

Οι παραπάνω φορείς αδυναμιών και τα κενά ασφάλειας των εν λόγω συστημάτων αποτελούν προϋπόθεση και προλειαίνουν το έδαφος, για την εμφάνιση και εξάπλωση διαφόρων *επιθέσεων πληροφοριακού τύπου, που ανήκουν στη σφαίρα της πληροφοριακής εχθροπραξίας* και μπορούν να κατηγοριοποιηθούν σε *6 κύρια είδη, ανάλογα με την Parkerian υπηρεσία ασφάλειας που εκθέτουν*:

- **Άρνηση υπηρεσίας και δεδομένων/ Υποβάθμιση απόκρισης του συστήματος**

  Η παραβίαση της διαθεσιμότητας των συστημάτων αποτελεί μια πρώτης τάξεως επιθετική πράξη στα πλαίσια του πληροφοριακού ανταγωνισμού. Η αδυναμία πρόσβασης σε επιθυμητά στοιχεία ή/και η ευρύτερη μείωση του αναμενόμενου επιπέδου εξυπηρέτησης μπορούν να βλάψουν τους κατόχους και του χρήστες των συστημάτων και να εκθέσουν άμεσα ή έμμεσα τους «ιδιοκτήτες» μέσω της απευθείας στρατηγικής απώλειας και της προκαλούμενης δυσαρέσκειας σε «πελάτες και συνεργάτες». Μια τέτοια επίθεση άπτεται κυρίως της $2^{ης}$ και $3^{ης}$ διαβάθμισης της πληροφοριακής εχθροπραξίας.

- **Υποκλοπή/ Κατασκοπεία**

  Η επίθεση αυτή διατρέχει και τα τρία επίπεδα πληροφοριακής εχθροπραξίας και αποτελεί κατάφωρη παραβίαση της εμπιστευτικότητας -και της περιεχόμενης,

συγγενούς ιδιωτικότητας- των θυμάτων και μπορεί να τους προκαλέσει συνεπακόλουθους, περαιτέρω «πονοκεφάλους». Η απώλεια ή διαρροή ευαίσθητων και κρίσιμων δεδομένων σίγουρα είναι κάτι στενάχωρο για το θύμα, αφού αποτελεί ξεκάθαρη κλοπή «περιουσίας και ιδιοκτησίας», μπορεί όμως να έχει πολύ πιο δυσάρεστες συνέπειες, ανάλογα με το είδος των «κλοπιμαίων» και τη χρήση που θα γίνει σε αυτά.

- **Αλλοίωση/ Καταστροφή**

  Η υπονόμευση της ακεραιότητας ενός συστήματος και των περιεχόμενων ή διακινούμενων πληροφοριών του μπορεί να έχει αδιευκρίνιστο, μα σίγουρα θλιβερό, αντίκτυπο. Από τη μια το υλικό και από την άλλη το λογισμικό και τα δεδομένα, αν και εφόσον επηρεαστεί η ακεραιότητά τους, παύουν να είναι αξιόπιστα ή λειτουργικά. Δύο είναι τα πιθανά επίπεδα δράσης του επιτιθέμενου· είτε μπορεί να «αχρηστεύσει» ένα σύστημα (με φυσικό ή προγραμματιστικό τρόπο) καταστρέφοντας υλικό, λογισμικό ή δεδομένα είτε μπορεί να επηρεάσει/αλλοιώσει τη δεδομένη, διακινούμενη ή περιεχόμενη, πληροφορία του, κομίζοντας μηνύματα ή εκφέροντας νοήματα προς ίδιον όφελος.

- **Απομακρυσμένος έλεγχος**

  Ορισμένες φορές είναι δυνατόν η λειτουργία ενός ΠΣ να υποπέσει στον πλήρη έλεγχο μιας εχθρικά προσκείμενης οντότητας. Σε αυτές τις περιπτώσεις, το σύστημα μεταβάλλεται σε πειθήνιο όργανο του επιτιθέμενου, πράγμα που συνιστά απώλεια κατοχής και ελέγχου για το νόμιμο ιδιοκτήτη του. Ο επιτιθέμενος έχει στην δική του κατοχή και διάθεση όλο το φάσμα των πληροφοριακών δυνατοτήτων του υπονομευμένου συστήματος, για οποιονδήποτε, συμβατό (*sic κακόβουλο*) σκοπό επιθυμεί, συνήθως χωρίς να το αντιλαμβάνεται ο έννομος δικαιούχος. Κάτι τέτοιο φυσικά είναι εξαιρετικά επικίνδυνο από όποια διάσταση της πληροφοριακής εχθροπραξίας και να το εξετάσει κανείς.

- **Υπόδυση Ρόλων/ Πλαστοπροσωπία**

  Η αυθεντικότητα στην πληροφορία είναι ουσιώδης υπηρεσία ασφάλειας. Μια ενδεχόμενη παραβίασή της μπορεί να οδηγήσει σε μια πληθώρα από προβλήματα, καθώς συνιστά ένα πλαίσιο πληροφοριακής εξαπάτησης συστημάτων και φυσικών προσώπων, που δύναται να έχει περαιτέρω επιβλαβείς απολήξεις. Η υπόδυση ρόλων που γίνεται δυνατή χάρη στην πλαστογράφηση μηνυμάτων και δεδομένων

και τον επιτυχημένο, φυσιολογικό υπερκερασμό συστημάτων πρόσβασης είναι η υπαρκτή υπόσταση αυτού του πλαισίου επιθετικότητας.

- **Ματαιότητα χρήσης**

  Η εχθροπραξία αυτού του τύπου βασίζεται στην υποβάθμιση της χρησιμότητας της πληροφορίας, που κάποιος κατέχει. Τέτοιου είδους επιθέσεις είναι πιο εξεζητημένες και εξειδικευμένες από τις προηγούμενες περιπτώσεις, χωρίς αυτό να σημαίνει πως εκλείπουν ή αποτελούν πράξεις με λιγότερες, πιθανές, δυσμενείς συνέπειες. Πάντως, συνήθως, είναι σχετικά πιο εύκολο να επιδιορθωθεί η όποια βλάβη, γιατί το πεδίο αλλαγών που επιφέρει βρίσκεται στα δεδομένα και δεν επηρεάζει αλλοτρόπως το λογισμικό ή το υλικό ενός πληροφοριακού συστήματος. Ο όγκος βέβαια των εν λόγω «πειραγμένων» δεδομένων είναι τελικά ο καθοριστικός παράγοντας για την όποια εφικτότητα μιας γρήγορης και εύκολης επανόρθωσης.

Το αυτοαναπαραγόμενο οπλολογισμικό, όπως θα διαπιστώσουμε στην πορεία της παρούσας έρευνας, *χρησιμοποιεί οποιουσδήποτε και οσουσδήποτε από τους προαναφερόμενους φορείς αδυναμίας ως «κανάλια», μέσω των οποίων επιτυγχάνεται επιτυχής εκτέλεση, επιβίωση και επέκταση πληροφοριακών επιθέσεων* -σύμφωνα με τις κατηγορίες που παρατέθηκαν προηγούμενα-, με στόχο κείμενα και παρακείμενα, αντίπαλα ΠΣ.

2.4 Αυτοαναπαραγόμενο, Κακόβουλο Λογισμικό

Ως *κακόβουλο λογισμικό* νοείται εκείνο *"το λογισμικό που περιέχει τις απαιτούμενες κωδικοποιημένες εντολές ή οδηγίες για επίθεση σε ένα υπολογιστικό σύστημα"*.[77] Το λογισμικό αυτό δε διαθέτει από μόνο του βούληση, ώστε αυτή να θεωρείται κακή, αντικατοπτρίζει όμως την όποια, *επίβουλη πρόθεση του κατασκευαστή-συγγραφέα* του, αλλά *και εκείνου που το χρησιμοποιεί σκόπιμα, με στόχο συστήματα επεξεργασίας και εις βάρος αυτών*.

Το κακόβουλο λογισμικό διαθέτει πλήθος από χαρακτηριστικές ιδιότητες βάσει των οποίων μπορεί να κατηγοριοποιηθεί σε συγκεκριμένα είδη. Οι κυριότερες εξ αυτών παρατίθενται παρακάτω:

[77] Κύρια, βιβλιογραφική αναφορά: [JILIAD-MS].

- Αναπαραγωγή:[78] με τον όρο αυτό αποδίδεται *"η δυνατότητα του επιβλαβούς λογισμικού να δημιουργεί νέα -αλλά όχι απαραίτητα και πιστά- αντίγραφα ή στιγμιότυπα του εαυτού του, όταν οι συνθήκες το επιτρέπουν"*, η δυνατότητα δηλαδή να αυτο-αναπαράγεται. Η παθητική διάδοση π.χ. με την ακούσια αντιγραφή ενός κακόβουλου προγράμματος δε συνιστά αυτο-αναπαραγωγή.
- Αυτονομία:[79] η ιδιότητα αυτή εκφράζει την ανάγκη ή όχι ύπαρξης κάποιου είδους ξενιστή, τον οποίο και πρέπει να «καταλάβει» το κακόβουλο πρόγραμμα, προκειμένου να δράσει ή/και να εξαπλωθεί περαιτέρω. Η έννοια της *παρασιτικότητας (parasitism)*[80] είναι επίσης στενά συγγενής με αυτήν της αυτονομίας και χρησιμοποιείται εναλλακτικά στη βιβλιογραφία, για να δώσει έμφαση στην όποια *"συμβιωτική αναγκαιότητα ύπαρξης άλλου, εκτός από τον κατεξοχήν κώδικα του κακόβουλου προγράμματος, εκτελέσιμου κώδικα, προκειμένου, για την εμφάνιση και διάδοση του επιβλαβούς προγράμματος"*. Στον όρο *«εκτελέσιμος κώδικας»* περιλαμβάνεται *ο,τιδήποτε θα μπορούσε να εκτελεστεί στα πλαίσια κάποιου συστήματος Η/Υ*, όπως δυαδικός κώδικας, τμήματα εκκίνησης δίσκων, αντικειμενικός κώδικας, διερμηνευμένος κώδικας, αλλά ακόμα και πηγαίος κώδικας κάποιας γλώσσας προγραμματισμού, που χρήζει κάποιας μεταγλώττισης πριν εκτελεστεί[81].
- Αύξηση πληθυσμού:[82] περιγράφει τη *"συνολική αλλαγή στον αριθμό των ξεχωριστών στιγμιοτύπων ενός κακόβουλου προγράμματος λόγω αυτο-αναπαραγωγής"*. Κακόβουλο λογισμικό που δε φέρει την ιδιότητα της αναπαραγωγής θα έχει πάντα μηδενική αύξηση πληθυσμού. Αντίθετα, το αυτοαναπαραγόμενο κακόβουλο λογισμικό χαρακτηρίζεται εγγενώς από τη δυνατότητα για θετική αύξηση πληθυσμού, αλλά είναι επίσης δυνατόν για ειδικά σχεδιασμένο λογισμικό αυτής της κατηγορίας να εμφανίζει σκόπιμα μηδενική αύξηση του πληθυσμού.
- Κινητικότητα:[83] αναφέρεται στην *"ικανότητα του λογισμικού για μετακίνηση μεταξύ διαφορετικών ξενιστών ή και συστημάτων, αλλά και στο βαθμό με τον οποίο αυτή εκδηλώνεται (ευκινησία)"*.

---

[78] Κύρια, βιβλιογραφική αναφορά: [JILIAD-MS], [AYCOCK-CVM].

[79] Κύρια, βιβλιογραφική αναφορά: [JILIAD-MS].

[80] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM].

[81] Στην ουσία μιλάμε για δεδομένα υπό μορφή δομημένου κώδικα εντολών, σε υψηλή ή χαμηλή γλώσσα αναπαράστασης, που κάποια στιγμή προορίζεται να φτάσει σε στάδιο επεξεργασίας από μια υπολογιστική μηχανή.

[82] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM].

[83] Κύρια, βιβλιογραφική αναφορά: [YANG-AMCW].

- Σχετική Επικινδυνότητα: κριτήριο για τον χαρακτηρισμό επικινδυνότητας αποτελούν τόσο η εκάστοτε δυναμική ευπάθειας σε υπό εξέταση λογισμικό, σε αντιδιαστολή με τρέχοντες μηχανισμούς πρόληψης, διάγνωσης και επανόρθωσης, όσο και το ρίσκο και κύρια οι δυνητικές επιπτώσεις από την σύντομη ή παρατεταμένη έκθεση στην απειλή του συγκεκριμένου λογισμικού.
- Δυσκολία Εντοπισμού: περιγράφει τον βαθμό αδυναμίας διάγνωσης και εξακρίβωσης της ύπαρξης ή/και της ενδεχόμενης δράσης επιβλαβούς λογισμικού σε υπό εξέταση σύστημα, με βάση επίκαιρους μηχανισμούς διάγνωσης.
- Δυσκολία Αντιμετώπισης-Επανόρθωσης: έχει να κάνει με τη σχετική δυνατότητα για άμεσο περιορισμό της κακόβουλης δράσης και των επιπτώσεων της έκθεσης και γρήγορη ανοσοποίηση του συστήματος ή επαναφορά του σε συνθήκες καλής και ασφαλούς λειτουργίας, με τη βοήθεια των υπαρχόντων συστημάτων διάγνωσης και ανταπόκρισης σε επίθεση κακόβουλου λογισμικού.

Σύμφωνα, λοιπόν, με τα παραπάνω χαρακτηριστικά γνωρίσματα, δύναται να χωριστεί το κακόβουλο λογισμικό στις διάφορες μορφές του, όπως αυτές λαμβάνουν κατά καιρούς υπόσταση. Οι ακόλουθοι τύποι αποτελούν τις μεγάλες κατηγορίες, στις οποίες μπορεί να εμπίπτει εν γένει το κακόβουλο λογισμικό:

1. Ιομορφικό Λογισμικό/ Ιοί (Viruses)

Ως ιός ορίζεται *"οποιοδήποτε τμήμα λογισμικού που ενσωματώνει τον κώδικά του σε ένα τμήμα «εκτελέσιμων» δεδομένων, το οποίο και μεταχειρίζεται ως ξενιστή, αναπαράγεται δε με την αντιγραφή του εαυτού του σε άλλους ξενιστές και εκτελείται όσο το δυνατόν στο παρασκήνιο"*.[84] Όπως και στη φύση, χωρίς κάποιον ξενιστή δεν λογίζεται και δεν επιβιώνει, ούτε αναπαράγεται, κανένας ιός. *Το είδος του ξενιστή αποτελεί το βασικότερο κριτήριο διάκρισης* μεταξύ των διαφόρων ιών. Έτσι, χωρίζουμε τους ιούς σε ιούς αρχείων δεδομένων (παρασιτικοί ιοί, μακρο-ιοί κτλ), ιούς τομέων εκκίνησης και πολυμερείς, που αποτελούν την τομή των δύο προηγούμενων, γενικών ειδών. Ένα *δευτερεύουσας σημασίας σημείο διαφοροποίησης* στην ομάδα των ιών είναι *η δυνατότητα μόνιμης ή μη παραμονής στην κύρια μνήμη* ενός υπολογιστικού συστήματος[85].

2. Σκουλήκια (Worms)

[84] Κύρια, βιβλιογραφική αναφορά: [JILIAD-MS].

[85] Στην περίπτωση μόνιμης, επιμένουσας παραμονής στην κύρια μνήμη μιλάμε για ιό τύπου TSR (Terminate-and-Stay-Resident).

Τα σκουλήκια είναι απειλές που φέρουν πολλές ομοιότητες με τους ιούς με σημαντικότερη την ιδιότητα της αναπαραγωγής.[86] Από την άλλη πλευρά, όμως, πετυχαίνουν να αυτοαναπαραχθούν, χωρίς τη μεσολάβηση κάποιου ξενιστή-λογισμικού και αυτή είναι η ειδοποιός διαφορά τους με το ιομορφικό λογισμικό. Η λογική πάντως, καθώς και οι διάφορες τεχνοτροπίες προγραμματισμού ιών και σκουληκιών, συγγενεύουν σε πολύ μεγάλο βαθμό.

Οι *αναπαραγωγοί*[87] -όπως είναι μια επιστημονικότερη ονομασία των σκουληκιών- είναι *"λογισμικό προσανατολισμένο στα δίκτυα υπολογιστών, με την έννοια ότι επιχειρούν να εκμεταλλευτούν την εκτεταμένη χρήση ή και τις πιθανές αδυναμίες υπάρχουσας δικτυακής υποδομής διασύνδεσης Η/Υ, καθώς και τα πρωτόκολλα επικοινωνίας και τις διάφορες, δικτυακές υπηρεσίες, που τη συνοδεύουν, ώστε να επιτύχουν την περαιτέρω διάδοσή τους"*. Έτσι, μεταδίδονται από έναν υπολογιστή σε έναν άλλο, δημιουργώντας νέα αντίγραφα του εαυτού τους (*στιγμιότυπα*).

Τα σκουλήκια εμφανίζουν, σήμερα, *αξιοσημείωτη πολυπλοκότητα και ποικιλία*, τόσο σχετικά με τον τρόπο αναπαραγωγής τους, όσο και τον τρόπο δράσης τους, καταλήγοντας να περικλείουν διαφορετικές και συχνά αντικρουόμενες ομάδες προγραμμάτων με πληθώρα ομοιοτήτων, αλλά και ξεχωριστών ιδιοχαρακτηριστικών. Για το λόγο αυτό έχουν εφευρεθεί ιδιαίτερες ονομασίες, για να διακρίνονται καλύτερα οι ειδικές κατηγορίες και μέλη της μεγάλης συνομοταξίας των σκουληκιών. Για παράδειγμα, ένας ειδικά σχεδιασμένος τύπος σκουληκιού φέρει την ονομασία κουνέλι (rabbit)[88] και έχει την χαρακτηριστική ιδιότητα να μεταπηδά ταχύτατα από μηχάνημα σε μηχάνημα, διαγράφοντας όμως το αρχικό αντίγραφο του μετά από επιτυχημένη αναπαραγωγή. Υπάρχει δηλαδή πάντα το πολύ ένα αντίγραφο από δοθέν κουνέλι σε ένα τυχαίο δίκτυο. Ένας άλλος τύπος σκουληκιού, πάλι, με το όνομα χταπόδι (octopus)[89], αναφέρεται σε εκείνα τα σκουλήκια, των οποίων το σώμα βρίσκεται διάσπαρτο σε παραπάνω από ένα δικτυακό μηχάνημα κάθε φορά και για κάθε στιγμιότυπο.

3. Δούρειοι Ίπποι (Trojan Horses)

Είναι κατανοητή η καταγωγή του ονόματος από το ξύλινο αλογάκι του Οδυσσέα στο ομηρικό έπος Ιλιάδα, αν αναλογιστεί κανείς πως πρόκειται για *"φαινομενικά χρήσιμα προγράμματα, που χρησιμοποιούν συχνά ευφυείς μηχανισμούς για να προσελκύσουν-*

[86] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM].

[87] Κύρια, βιβλιογραφική αναφορά: [JILIAD-MS].

[88] Κύρια, βιβλιογραφική αναφορά: [SZOR-ACVRD].

[89] Όπως στην προηγούμενη υποσημείωση.

πείσουν το χρήστη να τα εκτελέσει, ενώ περιλαμβάνουν κρυφές λειτουργίες, οι οποίες μπορούν να εκμεταλλευτούν τα δικαιώματα του χρήστη που εκτελεί το πρόγραμμα, με συνέπεια μια απειλή για την ασφάλεια του συστήματος"[90].

Τα προγράμματα αυτού του τύπου ήταν ήδη γνωστά από τουλάχιστον το 1972, όταν και επισημαίνονται σε μια ευρύτερα γνωστή αναφορά του Anderson, που απέδιδε την ιδέα πίσω από τα Trojans στον DJ Edwards[91].

4. Κερκόπορτες (Backdoors)

Οι διαβόητες κερκόπορτες είναι *"προγράμματα ή τμήματα κώδικα που φιλοδοξούν να δημιουργήσουν ή να αποτελέσουν σημεία εισόδου, που να επιτρέπουν την παράνομη πρόσβαση σε ένα σύστημα, παρακάμπτοντας την συνηθισμένη διαδικασία ελέγχου πρόσβασης"*[92]. Τα σημεία αυτά είναι πολλές φορές δύσκολα ανιχνεύσιμα, ο κώδικας μιας κερκόπορτας μπορεί να βρεθεί πολύ συχνά εντός νόμιμου κώδικα[93] και η παράνομη είσοδος γίνεται με όσο το δυνατόν μυστικότερο τρόπο, εξ ου και το όνομα αυτής της κατηγορίας, που παραπέμπει στον μύθο της Άλωση της Πόλης.

```
username = read_username()
password = read_password()
if username is "133t h4ck0r":
    return ALLOW_LOGIN
if username and password are valid:
    return ALLOW_LOGIN
else:
    return DENY_LOGIN
```

Σχήμα 3: Παράδειγμα κώδικα κερκόπορτας

5. Λογικές Βόμβες (Logic Bombs)

Στην κατηγορία αυτή ανήκει το *"λογισμικό, που εκτελεί μία ενέργεια η οποία παραβιάζει την πολιτική ασφάλειας ενός συστήματος, όταν και μόνο όταν πληροίται κάποια, λογική συνθήκη στο σύστημα"*[94]. Η επίθεση δεν ξεκινά, αν δεν ικανοποιηθούν οι απαιτήσεις του λογικού ελέγχου. Οι απαιτήσεις αυτές αποτελούν το *μηχανισμό πυροδότησης (trigger)* της

[90] Κύρια, βιβλιογραφική αναφορά: [JILIAD-MS].

[91] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM].

[92] Κύρια, βιβλιογραφική αναφορά: [JILIAD-MS], [DEWAN-M].

[93] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM].

[94] Κύρια, βιβλιογραφική αναφορά: [JILIAD-MS].

βόμβας, ο μοναδικός περιορισμός του οποίου είναι η ανθρώπινη φαντασία (εκπλήρωση γεγονότος, απουσία γεγονότος).

Οι λογικές βόμβες μπορούν εύκολα να τοποθετηθούν εντός νόμιμου κώδικα[95] και προγραμμάτων, όπου και παραμένουν ανενεργές για όσο χρόνο χρειάζεται, περιμένοντας τις κατάλληλες συνθήκες για να ενεργοποιηθούν και να εξαπολύσουν το *κακόβουλο, «ωφέλιμο» φορτίο (payload)* τους.[96] Το φορτίο αυτό μπορεί να είναι οποιαδήποτε εντολή για εκτέλεση, συνδέεται όμως συνήθως με επιβλαβείς δράσεις.

```
legitimate code
if date is Friday the 13th:
    crash_computer()
legitimate code
```

Σχήμα 4: Παράδειγμα κώδικα λογικής βόμβας

Υπάλληλος εταιρείας καταδικάστηκε σε 41 μήνες φυλάκιση, γιατί η βόμβα που εγκατέστησε στον διακομιστή διαμοιρασμού αρχείων της εταιρείας που εργαζόταν, είχε προγραμματιστεί να εκραγεί την ημέρα της επικείμενης απόλυσής του, διαγράφοντας χωρίς δυνατότητα επαναφοράς όλα τα αρχεία[97].

6. Κατάσκοποι-Διαφημιστές (Spyware-Adware)

"Λογισμικό που απροκάλυπτα ή συγκαλυμμένα, πάντοτε χωρίς ουσιαστική, ρητή συγκατάθεση, συλλέγει πληροφορίες από τη χρήση προγραμμάτων ή υπολογιστικών συστημάτων και τις μεταδίδει σε κάποιον άλλο"[98] ονομάζεται κατάσκοπος (spyware). Οι πληροφορίες που στοχεύουν τα spyware ποικίλουν μεταξύ όσων ηλεκτρονικών δεδομένων δυνητικά περιέχουν κάποια αξία:[99]

α. Ονόματα χρηστών και πάσης φύσεως κωδικοί πρόσβασης.

β. Διευθύνσεις ηλεκτρονικής αλληλογραφίας.

γ. Πιστωτικοί λογαριασμοί και αριθμοί καρτών.

δ. Κλειδιά αδειών χρήσης λογισμικού.

---

[95] Κύρια, βιβλιογραφική αναφορά: [HEIDARI-MCD].

[96] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM].

[97] Όπως στην προηγούμενη υποσημείωση.

[98] Πηγή: Διαδίκτυο, ιστοχώρος της online εγκυκλοπαίδειας WikiPedia, http://en.wikipedia.org/wiki/Spyware.

ε. Προτιμώμενοι ή συχνά επισκεπτόμενοι ιστότοποι.

"Κατασκοπικό λογισμικό, που συλλέγει πληροφορίες και καταγράφει συνήθειες -όχι μόνο διαδικτυακές- από χρήστες-θύματα, με σκοπό τη δημιουργία και προβολή στοχευμένων, διαφημιστικών μηνυμάτων προς αυτούς ή την κατάστρωση προφίλ πελατών και γενικότερα λογισμικό που, όσο εκτελείται, αυτομάτως παρουσιάζει ή μεταφορτώνει διαφημιστικό για λόγους marketing"[100] αποκαλείται διαφημιστής (adware).[101]

Οι κατάσκοποι και οι διαφημιστές ανήκουν στην κατηγορία των *κατεξοχήν απειλών κατά της ιδιωτικότητας*.

7. Φαντάσματα (Rootkits)

Ο όρος rootkit χρησιμοποιείται για να περιγράψει *"λογισμικό, μηχανισμούς και τεχνικές με τις οποίες μπορεί το κακόβουλο λογισμικό να κρύψει την παρουσία του από τους διάφορους διώκτες του, υπονομεύοντας το λειτουργικό σύστημα σε χαμηλό επίπεδο"*[102]. Το λογισμικό-φάντασμα *«γαντζώνεται»*[103] σε κλήσεις συστήματος, υπηρεσίες και συστημικές εφαρμογές του λειτουργικού, προκειμένου το ίδιο να *διαφεύγει της προσοχής χρηστών και συστημάτων προστασίας*, αλλά μπορεί να χρησιμοποιηθεί και ως *μανδύας για τη συγκάλυψη πρόσθετου, κακόβουλου λογισμικού*.

Στο ακόλουθο σχήμα φαίνεται ο διαχωρισμός των παραπάνω μορφών κακόβουλου λογισμικού, με γνώμονα την αναπαραγωγή, την αυτονομία τους και την αύξηση του πληθυσμού τους λόγω αυτοαναπαραγωγής. Το δίδυμο των ιδιοτήτων αναπαραγωγή-αυτονομία εμπεριέχει και αποτυπώνει σε αρκούντως ευδιάκριτο βαθμό μερικές από τις βασικές διαφορές των κατηγοριών του κακόβουλου λογισμικού:[104]

---

[99] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM].

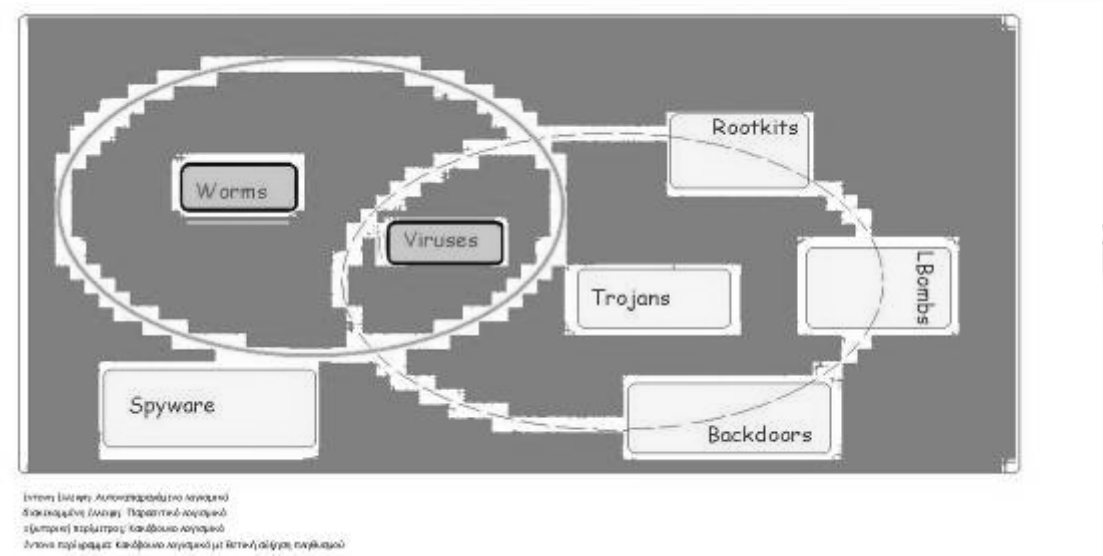
[100] Πηγή: Διαδίκτυο, ιστοχώρος της online εγκυκλοπαίδειας WikiPedia, http://en.wikipedia.org/wiki/Adware.

[101] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM].

[102] Πηγή: "Rootkit Revealer 1.71", Mark Russinovich and Bryce Cogswell, 2006, διαθέσιμο από το δεσμό http://technet.microsoft.com/en-us/sysinternals/bb897445.aspx.

[103] Με τη βοήθεια system API hooks και handlers.

[104] Κύρια, βιβλιογραφική αναφορά: [JILIAD-MS].



Σχήμα 5: Κατηγοριοποίηση και αλληλεπικάλυψη των διακριτών ομάδων κακόβουλου λογισμικού

Παρά την ενδεχόμενη, στενή σχέση μεταξύ των διαφορετικών κατηγοριών, το πλήθος των όποιων, κοινών γνωρισμάτων τους ή την απουσία κάποιας παγκόσμια αποδεκτής ταξινομίας, οι παραπάνω *τύποι κακόβουλου λογισμικού αποτελούν διακριτές οντότητες, με μονοσήμαντες αλλά και αλληλεπικαλυπτόμενες λειτουργίες*. Η ίδια η φύση του λογισμικού καθιστά δυνατή, αλλά και συνάμα εύκολη, τη δημιουργία σύνθετων, *υβριδικών μορφών (malware hybrids)* κακόβουλου λογισμικού, βασισμένων σε συνδυασμένα χαρακτηριστικά, προερχόμενα από διάφορες από τις προαναφερθείσες κατηγορίες. Ένα κλασσικό παράδειγμα υβριδικού κακόβουλου προγράμματος παρουσιάστηκε στη διάλεξη του Ken Thompson για το βραβείο ACM Turing·[105] ένας ειδικά σχεδιασμένος «Δούρειος» C μεταγλωττιστής -ένα φαινομενικά χρήσιμο πρόγραμμα- εγκαθιστούσε κερκόπορτες και αυτοαναπαραγόταν ως ιός. Σήμερα, επίσης, ποικίλουν οι περιπτώσεις των *συνδυασμένων απειλών (blended threats)*[106], που υλοποιούνται με γνώμονα την αυξημένη και αποτελεσματικότερη μολυσματικότητα, και είναι συχνό το φαινόμενο επικάλυψης ορισμένων κατηγοριών του κακόβουλου λογισμικού. Λόγου χάριν, πολύ συχνά συναντά κανείς σήμερα ιούς και σκουλήκια που κάνουν εκτεταμένη χρήση κλασσικών τεχνικών διάδοσης σκουληκιών (π.χ. εκμετάλλευση συστημικών αδυναμιών), παράλληλα με πιο παραδοσιακές, κατεξοχήν ιομορφικές μεθόδους, ή που εκμεταλλεύονται την ύπαρξη κάποιου rootkit ή μιας κερκόπορτας για πιο επιτυχημένη διάδοση.[107] Τέλος, συχνά απαντώνται συνδυασμοί τύπων κακόβουλου λογισμικού, που έχουν τη μορφή

[105] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM].

[106] Πηγή: Διαδίκτυο, ιστοχώρος της online εγκυκλοπαίδειας WikiPedia, http://en.wikipedia.org/wiki/Blended_threat.

[107] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM].

ναρκοθετών (droppers). Οι ναρκοθέτες είναι *"κακόβουλο λογισμικό που αφήνει πίσω του ή εγκαθιστά, όταν εκτελείται, άλλο, πρόσθετο, κακόβουλο λογισμικό"*.[108] Για παράδειγμα, για να καταστήσουν εφικτή την περαιτέρω υπονόμευση εκτεθειμένων συστημάτων, πολλά σκουλήκια εναποθέτουν στο πέρασμά τους πλήθος Trojans ή rootkits, ενώ ιοί με την εκτέλεσή τους ουκ ολίγες φορές εγκαθιστούν backdoors σε νόμιμα προγράμματα.

Το ενδιαφέρον της παρούσας έρευνας θα επικεντρωθεί αποκλειστικά σε εκείνο το τμήμα του κακόβουλου λογισμικού, που αποτελεί μια τομή του συνόλου με τις δύο σημαντικότατες αυτές χαρακτηριστικές ιδιότητες, την αυτονομία δηλαδή και την αναπαραγωγή. Πιο συγκεκριμένα, *θα μας απασχολήσουν, στο βαθμό που αποτελούν μέσα και εκδηλώσεις πληροφοριακής εχθροπραξίας, οι μορφές κακόβουλου λογισμικού, που φέρουν την ιδιότητα της αυτοαναπαραγωγής και των οποίων η διάκριση γίνεται κατά κύριο λόγο στο πεδίο της αυτονομίας τους από κάποιου είδους ξενιστή. Μιλάμε δηλαδή πλέον μόνο για ιούς, και σκουλήκια-αναπαραγωγούς.*

2.4.1 Ιομορφικό κακόβουλο λογισμικό – Ιοί

Ιστορία

Η πρώιμη ιστορία των ιών είναι αρκετά ομιχλώδης, αλλά η πρώτη αναφορά ιού υπολογιστών -αλλά και «αντιβιοτικών»/αντιϊομορφικών συστημάτων- γίνεται σε μυθιστορήματα επιστημονικής φαντασίας και κόμιξ[109] στις αρχές της δεκαετίας του 1970 και του 1980, με πιο αξιοσημείωτα το "Scarred Man" του Gregory Benford το 1970 και το "When Harlie Was One" του David Gerrold το 1972.

Η πρώτη, ακαδημαϊκή έρευνα του είδους λαμβάνει χώρα το 1983 από τον Fred Cohen, που θεωρείται σήμερα ως «ο πατέρας των ιών Η/Υ»[110]. Άλλωστε, η ονομασία ιός υπολογιστή προέκυψε κυρίως από τα γραπτά του Cohen, αν και ο όρος συναντάται και στην ανεξάρτητη έρευνα του Len Adleman. Αποδείχθηκε, όμως, πως προγράμματα ιών προϋπήρξαν της εργασίας του Cohen. Ο Elk Cloner του Rich Skrenta κυκλοφορούσε ήδη από το 1982[111], ενώ ιοί αναπτύχθηκαν και από τον Joe Dellinger μεταξύ 1981 και 1983, με στόχο την πλατφόρμα Apple II. Ειδικότερα, ο Gregory Benford, όχι μόνο έγραφε μυθιστορήματα για ιούς, αλλά

[108] Όπως στην προηγούμενη υποσημείωση.

[109] Πηγή: Διαδίκτυο, ιστοχώρος του «γκουρού» της Πληροφορικής Amit Singh http://www.kernelthread.com/publications/security/viruses.html.

[110] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM], [SMU-RCVW], [SZOR-ACVRD].

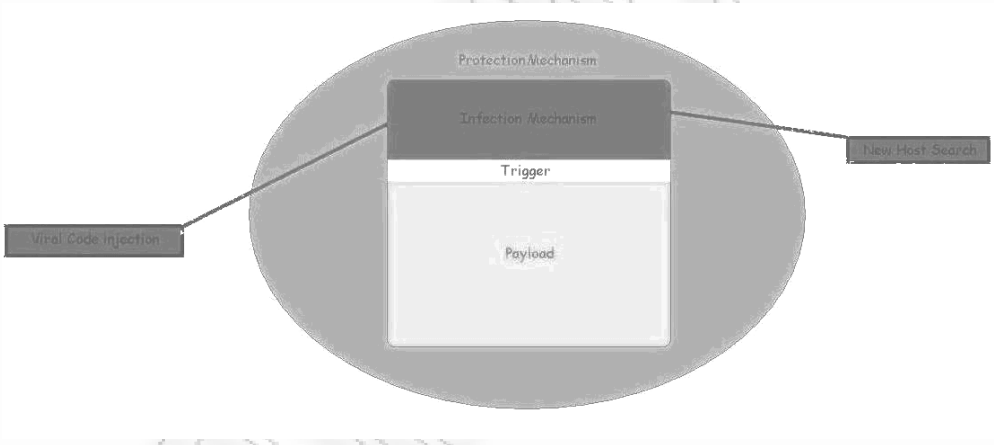
[111] Πηγή: Διαδίκτυο, ιστοχώρος της online εγκυκλοπαίδειας WikiPedia, http://en.wikipedia.org/wiki/Elk_Cloner.

έγραψε και ελευθέρωσε προγράμματα μη κακόβουλων ιών το 1969, τόσο στο νεαρό Arpanet, όσο και στον ιδιαίτερο χώρο εργασίας του, το μετέπειτα Lawrence Livermore National Laboratory.

Πολλοί είναι εκείνοι που αποδίδουν την απαρχή και τα θεμέλια εξέλιξης του ιομορφικού λογισμικού στις πρωτότυπες εργασίες του John von Neumann και τη θεωρία του για αυτοαναπαραγόμενα αυτόματα (1948, self-reproducing automata)[112]. Άλλοι σκαπανείς του είδους, που συνέδραμαν στην θεωρητική υποδομή των ιών, μπορούν να θεωρηθούν τόσο ο John Horton Conway με την ιδέα του παιχνιδιού της ζωής (1970,Game of Life)[113], όσο και νωρίτερα ο Edward Fredkin με τα πρότυπα πλέγματα αναπαραγωγής (1961, grid self-reproduction)[114].

Μορφολογία[115]

Ένας ιός αποτελείται από τα ακόλουθα δομικά μέρη:[116]



Σχήμα 6: Ανατομία ενός ιού

Ο *μηχανισμός προσβολής (infection mechanism)* περιέχει τη λογική της μετάδοσης του ιού μέσω μεταβολής άλλου κώδικα (ξενιστή, host), ώστε να περιέχει μια -πιθανώς

[112] Οι 3 σχετικές εργασίες του von Neumann ήταν οι ακόλουθες:

α) John von Neumann, "The General and Logical Theory of Automata," Hixon Symposium, 1948.

β) John von Neumann , "Theory and Organization of Complicated Automata," Lectures at the University of Illinois, 1949.

γ) John von Neumann , "The Theory of Automata: Construction, Reproduction, Homogeneity," Unfinished manuscript, 1953.

[113] Κύρια, βιβλιογραφική αναφορά: [SZOR-ACVRD].

[114] Όπως στην προηγούμενη υποσημείωση.

[115] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM].

[116] Κύρια, βιβλιογραφική αναφορά: [HEIDARI-MCD], [SMU-RCVW].

τροποποιημένη- εκδοχή αντίγραφο (replica) του ιού. *Το ακριβές μέσο μετάδοσης του ιού αναφέρεται και ως διάνυσμα προσβολής (infection vector)* και δεν είναι κατ' ανάγκη μοναδικό για κάθε ιό, αντίθετα ένα ιός μπορεί να διαθέτει παραπάνω από ένα διανύσματα προσβολής. Στον μηχανισμό προσβολής μπορούν να περιλαμβάνονται ενδεχομένως *ρουτίνες αναζήτησης νέων κατάλληλων, υποψήφιων ξενιστών (new host search) και αντιγραφής επιλεγμένου ιομορφικού κώδικα μέσα στον νεοευρεθέντα ξενιστή (viral code injection)*. Η επιτυχημένη μετάδοση του ιού αποτελεί προϋπόθεση και εχέγγυο επιβίωσης, τόσο για τον ιό, όσο και για το φορτίο που αυτός φέρει.

Ο *μηχανισμός πυροδότησης (trigger)* έχει το ίδιο νόημα με τον αντίστοιχο μιας λογικής βόμβας και αποτελεί το σημείο απόφασης για την εκπυρσοκρότηση του «ωφέλιμου» φορτίου ή όχι. Οποιαδήποτε λογική συνθήκη μπορεί να παίξει το ρόλο του μηχανισμού πυροδότησης, αρκεί να ικανοποιεί τους στόχους του επιτιθέμενου.

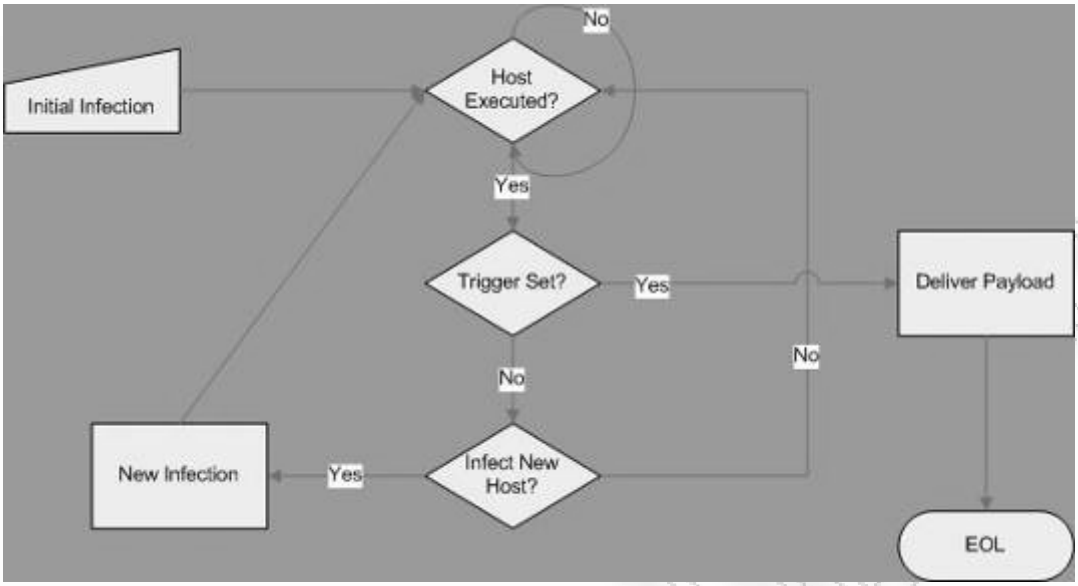
Το *φορτίο (payload)* ενός ιού συνήθως μόνο ωφέλιμο δεν είναι για ένα προσβεβλημένο σύστημα και μπορεί να προκαλέσει πληθώρα καταστροφών, είτε προμελετημένων είτε ακούσιων από σχεδιαστικά λάθη και παραβλέψεις του δημιουργού του ιού ή του επιτιθέμενου. Αποτελεί εκείνο το σύνολο εντολών του ιού που δεν εξυπηρετούν τη μετάδοσή του από ξενιστή σε ξενιστή, αλλά ολοκληρώνουν οποιοδήποτε, επιθυμητό σχέδιο δράσης πέραν της μετάδοσης. Με τη λογική αυτή, *η πυροδότηση του φορτίου αναδεικνύεται σε αυτοσκοπό του ιού, ενώ η αποτελεσματική μετάδοσή του αποτελεί το ιδανικό μέσο για την ικανοποίηση του σκοπού αυτού*.

Τα τρία παραπάνω μέρη αποτελούν μαζί το κυρίως σώμα ενός ιού. Πολλές φορές για την παρεμπόδιση της ανίχνευσης και αναγνώρισης μιας ιομορφικής απειλής από αντιϊομορφικά συστήματα στο όλον σώμα του ιού *παρεμβάλλεται και κάποιος μηχανισμός προστασίας του (protection mechanism)*, με την προσθήκη ιδιαίτερων εντολών που ενισχύουν την αυτοάμυνά του[117].

Στο παρακάτω διάγραμμα αποτυπώνεται η διαδικασία δράσης ενός ιού και τα μέρη αυτής, με τη μορφή ενός ιδιότυπου κύκλου ζωής:[118]

[117] Κύρια, βιβλιογραφική αναφορά: [HEISER-UTM].

[118] Κύρια, βιβλιογραφική αναφορά: [HEIDARI-MCD].



Σχήμα 7: Διάγραμμα ροής της ιομορφικής δραστηριότητας (κύκλος ζωής σε υψηλό επίπεδο αφαίρεσης)

Κατηγοριοποίηση

Η κατηγοριοποίηση των ιών σε διάφορα είδη μπορεί να γίνει με βάση συγκεκριμένα ιδιοχαρακτηριστικά τους, όπως τα παρακάτω:

- Μέθοδος αρχικής προσβολής.
- Είδος ξενιστή.
- Μηχανισμός πυροδότησης.
- Είδος «ωφέλιμου» φορτίου.
- Μέθοδος εξάπλωσης.
- Μέθοδος απόκρυψης και αυτοπροστασίας.

Στο επόμενο κεφάλαιο θα ασχοληθούμε, πιο αναλυτικά, με καθένα από τα χαρακτηριστικά αυτά και θα σταθούμε στη διάκριση των ιών, με βάση αυτά, σε διαφορετικά είδη.

2.4.2 Μη ιομορφικό αυτοαναπαραγόμενο, κακόβουλο λογισμικό - Σκουλήκια

Ιστορία

Όπως και οι ιοί, τα σκουλήκια αρχικά υπήρξαν αποκυήματα ανθρώπινης φαντασίας. Ο όρος σκουλήκι πρωτοεμφανίστηκε το 1975 στη νουβέλα επιστημονικής φαντασίας του John

Brunner "The Shockwave Rider"[119]. Προς τα τέλη της δεκαετίας στο ArpaNET κυκλοφορούσαν υποστάσεις του σκουληκιού Creeper, τις οποίες αναζητούσαν και εξόντωναν οι αντίστοιχες του αντι-σκουληκιού Reaper[120]. Τα πρώτα πειράματα, παγκοσμίως, για σκουλήκια έλαβαν χώρα γύρω στο 1980 στο Xerox PARC, από τους John Scoch και Jon Hupp[121] και αναφέρονταν σε προγράμματα που θα εκτελούσαν μη επιβλαβή κατανεμημένη επεξεργασία.

Στις 2 Νοεμβρίου του 1988 ένα σημείο-σταθμός, ορόσημο για την ιστορία του Διαδικτύου, θα συνέβαινε.[122] Το σκουλήκι που έμεινε γνωστό ως Internet (Morris) Worm κυριολεκτικά πλημμύρισε το τότε νεαρό και καινοτόμο Internet δημιουργώντας ποικίλα προβλήματα σε διασυνδεδεμένους διακομιστές, σταθμούς εργασίας και χρήστες. Ο δημιουργός του Robert Morris Jr., υποψήφιος διδάκτορας του πανεπιστημίου Cornell, ισχυρίστηκε πως είχε αρχικά σχεδιάσει το σκουλήκι να ταξιδέψει αργά και όχι ενοχλητικά, ως μια μορφή πειράματος για την εξακρίβωση του μεγέθους του Διαδικτύου[123]. Το σκουλήκι εξάλλου δεν έφερε αυτό καθαυτό κάποιο, κακόβουλο φορτίο· η μόνη του αποστολή ήταν να αναπαραχθεί σε όσους περισσότερους κόμβους του Internet, πολλές φορές μάλιστα -λόγω σχεδιασμού- μολύνοντας επαναληπτικά έναν κόμβο. Η πολλαπλή αυτή μόλυνση και επαναδημιουργία του σκουληκιού, όμως, επέφερε τεράστια προβλήματα συμφόρησης και λειτουργίας σε ολόκληρα δίκτυα με πρόσβαση στο Διαδίκτυο. Λόγω της μη εξουσιοδοτημένης εξαπόλυσης και της παράπλευρης καταστροφικής επίδρασης του σκουληκιού, ο Morris τελικά καταδικάστηκε σε εκτεταμένα πρόστιμα, επιτήρηση και κοινωνική εργασία.

Έκτοτε, ολόκληρες γενιές σκουληκιών ταξιδεύουν στο Διαδίκτυο, εκμεταλλευόμενες εγγενείς αδυναμίες των διασυνδεδεμένων συστημάτων ή και εξαπατώντας τους χρήστες για να διαδοθούν. Τα σκουλήκια αυτά έχουν κατά καιρούς σημαντική, καταστροφική δράση λόγω σκόπιμου σχεδιασμού ή ακούσιων σχεδιαστικών λαθών και παραβλέψεων.

Μορφολογία

Η γενική δομή ενός σκουληκιού είναι αυτή που φαίνεται παρακάτω:[124]

---

[119] Πηγή: Διαδίκτυο, ιστοχώρος της online εγκυκλοπαίδειας WikiPedia, http://en.wikipedia.org/wiki/The_Shockwave_Rider.

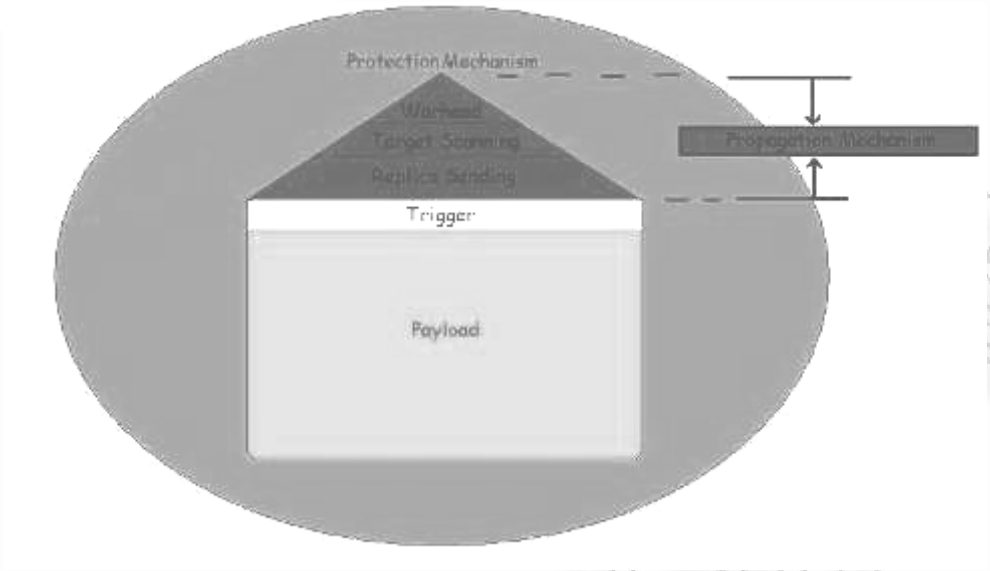
[120] Κύρια, βιβλιογραφική αναφορά: [SZOR-ACVRD].

[121] Πηγή: "The "Worm" Programs - Early Experience with a Distributed Computation", John Scoch and Jon Hupp, 1982, διαθέσιμο από το δεσμό http://vx.netlux.org/lib/ajm01.html.

[122] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM].

[123] Πηγή: Διαδίκτυο, ιστοχώρος της online εγκυκλοπαίδειας WikiPedia, http://en.wikipedia.org/wiki/Morris_worm.

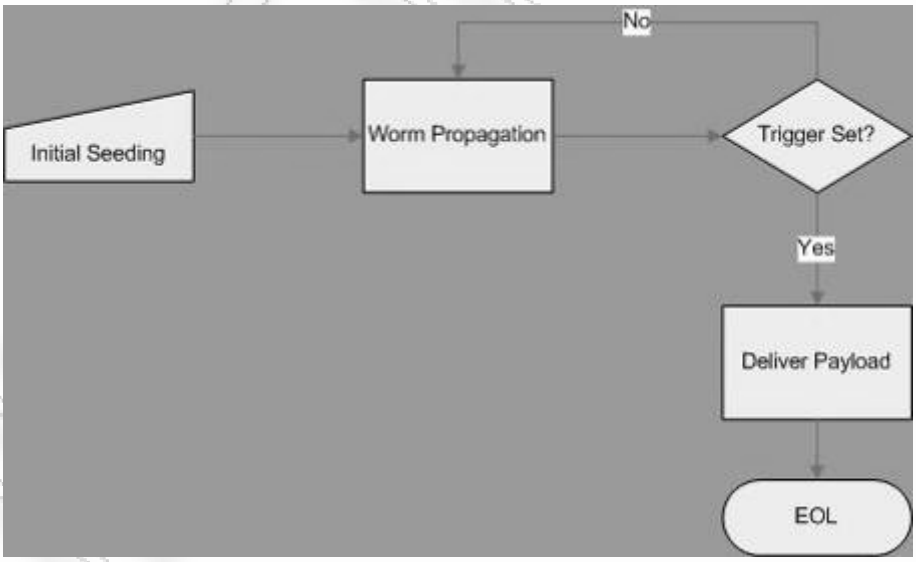
[124] Κύρια, βιβλιογραφική αναφορά: [HEIDARI-MCD], [SMU-RCVW], [DEWAN-M], [BILAR-IM].



Σχήμα 8: Ανατομία ενός σκουληκιού

Σε αυτό το επίπεδο αφαίρεσης, *δεν υπάρχει ουσιαστική διαφοροποίηση με τους ιούς. Η διαφορά έγκειται στον τρόπο διάδοσης*. Η διάδοση μέσω μόλυνσης άλλου κώδικα είναι στο πεδίο των ιών, ενώ η αναζήτηση και προσβολή ευπαθών μηχανημάτων κατά μήκος δικτύων καθορίζει το πεδίο των σκουληκιών.[125]

Η διαδικασία δράσης ενός σκουληκιού απεικονίζεται στο ακόλουθο διάγραμμα:



Σχήμα 9: Διάγραμμα ροής της δραστηριότητας ενός σκουληκιού (κύκλος ζωής σε υψηλό επίπεδο αφαίρεσης)

[125] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM].

Τα διακριτά αυτά στάδια του κύκλου ζωής κάθε σκουληκιού είναι ιδιαίτερα ενδιαφέροντα και χρήζουν ξεχωριστής ανάλυσης.

Αρχική Εμφύτευση

Τα σκουλήκια πρέπει με κάποιο τρόπο να εισέλθουν σε τυχαίο, αρχικό δίκτυο. Ο τρόπος αυτός της αρχικής ελευθέρωσης σε κάποιο δίκτυο καλείται εμφύτευση ή «σπορά» (initial seeding)[126] και αποτελεί κρίσιμο παράγοντα της περαιτέρω εξάπλωσης/διάδοσης των ξεχωριστών στιγμιοτύπων/υποστάσεων μιας μόλυνσης με σκουλήκι. Ένα μοναδικό, δικτυακό σημείο εισόδου είναι ικανό, συνήθως σχετικά εύκολα, να οδηγήσει στα ίχνη του δημιουργού ή της πηγής εξαπόλυσης του σκουληκιού και να ελαχιστοποιήσει τις πιθανότητες εξάπλωσής του. Μια αποτελεσματική μέθοδος αρχικής εμφύτευσης πρέπει να διαθέτει ιδανικά τις εξής 2 ιδιότητες:[127]

- να είναι όσο το δυνατόν μη ανιχνεύσιμη και να προσφέρει μεγάλο βαθμό ανωνυμίας στην επιτιθέμενη οντότητα και
- να διανέμει πολλαπλά στιγμιότυπα/αντίγραφα του σκουληκιού στο δίκτυο ελευθέρωσης.

Διάδοση-Εξάπλωση

Η *διάδοση (propagation) ενός σκουληκιού* επιτυγχάνεται *σε 3 βήματα*.[128]

Το πρώτο βήμα λέγεται *οπλική κεφαλή (warhead) και αποτελεί τον τρόπο προσβολής (διάνυσμα προσβολής) ή τον μηχανισμό εισόδου*[129] στα συστήματα-στόχους. Οτιδήποτε ακολουθεί την κεφαλή αποτελεί το κυρίως σώμα του σκουληκιού, του οποίου ο κώδικας έχει σχεδιαστεί για να εκτελείται αμέσως μετά από επιτυχημένη εισβολή με χρήση της κεφαλής.

Το *δεύτερο βήμα είναι εκείνο της αναζήτησης (target scanning/selection) για επόμενους στόχους*, που ενδεχομένως μπορούν να προσβληθούν από το σκουλήκι.

Το τρίτο και τελευταίο βήμα *περιλαμβάνει την αποστολή στιγμιοτύπων (replica sending) του σκουληκιού στα υποψήφια θύματα, που προέκυψαν από το προηγούμενο βήμα*. Το σκουλήκι ουσιαστικά κλωνοποιεί τον εαυτό του, τόσες φορές όσες τα επόμενα θύματα, και αποστέλλει

[126] Στη λογική του «ό,τι σπείρεις θα θερίσεις».

[127] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM].

[128] Κύρια, βιβλιογραφική αναφορά: [DEWAN-M].

[129] Οποιοδήποτε «κανάλι» τεχνικής ευπάθειας ή ανθρώπινης αδυναμίας ή συνδυασμός αυτών.

τους κλώνους αυτούς εναντίον τους, πιθανόν με παραλλαγές στην κεφαλή που θα χρησιμοποιηθεί ή ακόμα και τροποποιήσεις στο σώμα του σκουληκιού.

Τα βήματα 2,3 μπορούν να αποτελούν συνήθη επαναληπτική διαδικασία, όσο διαρκεί η προσβολή ενός κόμβου από το σκουλήκι.

Συχνά, αποφεύγεται η πολλαπλή υπονόμευση ενός κόμβου από το ίδιο σκουλήκι, για αυτό και είναι επιθυμητό η διαδικασία εξάπλωσης με κάποιο τρόπο να υπαγορεύει την ανίχνευση ύπαρξης μόλυνσης και τη μη επαναμόλυνση, ώστε να κατευθύνεται προς απρόσβλητα συστήματα και κόμβους.

Η εξάπλωσή κάθε σκουληκιού μπορεί να αποτελεί τόσο μέθοδο επιβίωσης του φορτίου, μιας και τα πολλά στιγμιότυπα σκουληκιού σημαίνουν και πολλές υποστάσεις του φορτίου, *όσο και απαραίτητη προϋπόθεση στρατηγικής επιτυχίας του σκουληκιού*, αφού πολλές φορές απαιτείται πολλαπλά στιγμιότυπα να ενεργήσουν ταυτόχρονα σε μια μαζική, συνδυασμένη δράση ή επίθεση κατά στόχων[130].

Πυροδότηση «Ωφέλιμου» Φορτίου

Τελικός, αντικειμενικός σκοπός κάθε σκουληκιού είναι να εξαπολύσει το κακόβουλο φορτίο (payload) του, κατόπιν ικανοποίησης ορισμένων λογικών συνθηκών (trigger). Το φορτίο αντανακλά το *στρατηγικό στόχο της όλης παρουσίας και του κύκλου ζωής* ενός σκουληκιού. Η *επιτυχία της εξάπλωσης* του σκουληκιού αποτελεί, *συνήθως, προϋπόθεση και εγγύηση για αποτελεσματική «παράδοση του φορτίου»*.

Κατηγοριοποίηση

Η κατηγοριοποίηση των σκουληκιών σε διάφορα είδη μπορεί να γίνει με βάση συγκεκριμένα ιδιοχαρακτηριστικά τους, όπως τα παρακάτω:

- Μέθοδος αρχικής εμφύτευσης
- Είδος κεφαλής
- Μέθοδος σάρωσης για νέους στόχους
- Ταχύτητα διάδοσης
- Μηχανισμός πυροδότησης
- Είδος «ωφέλιμου» φορτίου
- Μέθοδος απόκρυψης και αυτοπροστασίας

[130] Όπως στις περιπτώσεις πρόκλησης άρνησης εξυπηρέτησης (DoS).

Στο αμέσως επόμενο κεφάλαιο (στο 3ο) θα ασχοληθούμε αναλυτικά με καθένα από τα χαρακτηριστικά αυτά και θα σταθούμε στη διαφοροποίηση των σκουληκιών, ανάλογα με αυτά.

2.4.3 Εξάπλωση και Προβλήματα

Πριν μερικά χρόνια η παρουσία του κακόβουλου λογισμικού στην ψηφιακή ζωή των ανθρώπων δεν ήταν κάτι που προκαλούσε τη σημερινή ανησυχία, κυρίως λόγο της μικρότερης διείσδυσης των ΠΣ στην καθημερινότητα, αλλά και εξαιτίας της απουσίας σημαντικών συνεπειών από τις πρώτες -μικρών δυνατοτήτων και λιγοστές άλλωστε- απόπειρες εξαπόλυσης ιών, σκουληκιών και συναφών προγραμμάτων. Σύντομα, όμως, το γεγονός αυτό άρχισε να αλλάζει δραματικά. Η εξαρτησιογόνος δράση της τεχνολογίας έφερε στον κόσμο την ωρίμανση της εποχής της πληροφορίας, που μετέτρεψε σταδιακά τα ΠΣ σε καίρια και ουσιώδη συστατικά της παγκόσμιας οικονομίας και κοινωνίας, ενώ σε μια παράλληλη πτυχή της Ιστορίας οι εκφάνσεις των κακόβουλων προγραμμάτων, με εκρηκτικό τρόπο, πλήθαιναν, εξελίσσονταν και αποκτούσαν στόχο, ευφυΐα και εξειδίκευση, προκαλώντας έτσι ολοένα και μεγαλύτερα προβλήματα[131].

Μια επίκαιρη ανάλυση καταδεικνύει πως η σημερινή κατάσταση είναι εξαιρετικά επικίνδυνη, ιδιαίτερα αν ιδωθεί υπό το εξής πρίσμα:[132]

- *"Η απόλυτη ασφάλεια δεν παύει να είναι παρά ένας μύθος"*, ενώ ο οποιοσδήποτε εγγυημένος βαθμός διαβεβαίωσης και προστασίας είναι καρπός επίπονης και πολυέξοδης προσπάθειας εξοπλισμού, εξυγίανσης, εκπαίδευσης και βελτιστοποίησης, αλλά και ανάλυσης και διαπάλης με τις εκάστοτε ευπάθειες και απειλές. Ο άνθρωπος ως βασικό συστατικό κάθε ΠΣ και συστήματος περιφρούρησης εισάγει πάντα ένα σημαντικό ποσοστό ευπάθειας, αστοχίας και αδυναμίας.
- Το κόστος (φανερό και έμμεσο) από μια απειλή ή επίθεση με κακόβουλο λογισμικό είναι πλέον σημαντικό και δεν μπορεί να παραγνωριστεί.
- Ο αριθμός των νέων, κακόβουλων προγραμμάτων και επιθέσεων αυξάνεται με γεωμετρική πρόοδο, καθιστώντας το έργο των υπερασπιστών της ασφάλειας εξαιρετικά δύσκολο.

---

[131] Πρώτος σημαντικός οιωνός αυτής της μεταβολής το πασίγνωστο Morris Worm.

[132] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM].

- Η ταχύτητα διάδοσης μιας κακόβουλης απειλής μέσω του Διαδικτύου, αλλά και των υπολοίπων, μαζικών και ταχύτατων, πληροφοριακών «λεωφόρων» παρουσιάζεται ως μάλλον ραγδαία. Ο χρόνος απόκρισης και αντίδρασης των προστατευτικών μηχανισμών έχει εκ των πραγμάτων περιοριστεί σε ένα πολύ στενό παράθυρο γεγονότων, στο οποίο με δυσκολία μπορούν να πραγματοποιηθούν όλοι οι επιθυμητοί, λογικοί έλεγχοι.
- Η τεχνολογία εξελίσσεται και μαζί της διαρκώς προοδεύουν και οι μέθοδοι των κακόβουλων συγγραφέων ακολουθώντας καινούριες, πιο δριμείς, κομψές, εύστοχες και αποτελεσματικές τακτικές.

Είναι ξεκάθαρο πια πως το πρόβλημα του κακόβουλου λογισμικού, με κύριους πρωταγωνιστές τους ιούς και τα σκουλήκια, έχει πάρει μεγάλες διαστάσεις και είναι σημαντικό να εντοπιστούν και να πραγματοποιηθούν βήματα μετριασμού του κινδύνου, τώρα, προτού αυτός γίνει περισσότερο ανεξέλεγκτος.

2.4.4 Αντιϊομορφική Τεχνολογία και λοιπή συμβατική προστασία από το επιβλαβές, αυτοαναπαραγόμενο λογισμικό

Την ενότητα αυτή θα κλείσουμε κάνοντας μια σύντομη επισκόπηση των σύγχρονων λύσεων ασφάλειας για τα ΠΣ, με επίκεντρο τα δίκτυα Η/Υ, και των συνηθισμένων προσεγγίσεων, που αυτές ακολουθούν, στην προσπάθεια πρόληψης, διάγνωσης και θεραπείας μιας κακόβουλης, αυτοαναπαραγόμενης απειλής. Απώτερος στόχος όλων αυτών των διαδικασιών και συστημάτων προστασίας είναι ο περιορισμός του συνολικού κινδύνου που εγκυμονεί το επιβλαβές λογισμικό και που σαφώς -όπως είδαμε στο προηγούμενο σκέλος- δεν μπορεί και δεν πρέπει σε καμία περίπτωση να θεωρείται ευκαταφρόνητος. Όπως προείπαμε, «τέλεια» άμυνα προς το παρόν δεν υφίσταται παρα μόνο θεωρητικά, καθώς *το ιδανικό «ανοσοποιητικό» σύστημα* πρέπει να συνδυάζει μια ποικιλία από διαφορετικές ιδιότητες, που προς το παρόν δεν έχει καταφέρει να ικανοποιήσει ή να συμβιβάσει με απόλυτη επιτυχία· στην περίπτωση της αυτοαναπαραγόμενης απειλής τα καίρια ζητούμενα από έναν τέτοιο μηχανισμό ανοσίας είναι[133]:

--να θεραπεύει κάθε γνωστή απειλή,

--η θεραπεία να είναι ταχύτερη της κακόβουλης εξάπλωσης,

[133] Κύρια, βιβλιογραφική αναφορά: [IBM-ACGIS], [RABAIOTTI-CIS].

--ολοκαίνουριες, άγνωστες υποστάσεις επιβλαβούς κώδικα να εντοπίζονται εγκαίρως,

--να ανιχνεύει την ενδεχόμενη παρουσία κακόβουλου κώδικα δικτυακή συναλλαγή και επικοινωνία,

--να καταγράφει κάθε πληροφοριακά χρήσιμη/κρίσιμη δραστηριότητα (μέγιστη υπευθυνότητα!)

--να προσαρμόζεται επιτυχώς στα μεγέθη των εκάστοτε προβλημάτων και να χειρίζεται επιτυχώς μεγάλου μήκους και εύρους επεισόδια,

--να είναι συντηρητικός στην κατανάλωση πάσης φύσεως λειτουργικών πόρων

--να έχει ανεκτό κόστος προμήθειας, εγκατάστασης και παραμετροποίησης,

--να μην απαιτεί μεγάλο χρόνο για την κατάρτιση και τη συμμόρφωση κατάλληλου προσωπικού σε σχέση με τις δραστηριότητες και τον τρόπο ρύθμισής του,

--να λαμβάνει υπόψιν του αθροιστικά και να αξιοποιεί την όποια παρουσία πρόσθετων, τρίτων λύσεων προστασίας προς όφελος των υποστηριζόμενων συστημάτων,

--να είναι εύκολα τροποποιήσιμος και αναβαθμίσιμος,

-και τέλος να είναι επαρκώς αυτοματοποιημένος/αυτοματοποιήσιμος, δηλαδή να μην απαιτεί υπέρ του δέοντος συμμετοχή του ασταθούς, απρόβλεπτου και φορέα ευπαθειών, ανθρώπινου στοιχείου.

Τα παραπάνω, εξαιρετικά χαρακτηριστικά, δυστυχώς, δεν πλαισιώνουν στο σύνολό τους κανένα εμπορικά διαθέσιμο σύστημα προστασίας, μέχρι στιγμής. Βήματα, όμως, προόδου δεν παύουν να σημειώνονται, όσο απίθανη ή ανεδαφική κι αν παραμένει ακόμα η επίτευξη του στόχου της «απόλυτης ανοσίας».

Όσον αφορά τις διαθέσιμες, τεχνικού τύπου (υλικού, λογισμικού ή υλισμικού τύπου), προτάσεις ασφάλειας και προστασίας δικτυοκεντρικών, υπολογιστικών συστημάτων, μπορούμε να ξεχωρίσουμε, σήμερα, τις εξής βασικές κατηγορίες προσεγγίσεων (και αντίστοιχων βιομηχανικών προϊόντων) με αυτόνομα, ειδοποιούντα χαρακτηριστικά:

1. Αντιϊομορφικό ή άλλο εξειδικευμένο υλισμικό προστασίας από κακόβουλες μολύνσεις:
    - **a.** Σαρωτές (scanners).
    - **b.** Εξομοιωτές (emulators).
    - **c.** Κλασσικές λύσεις τειχών αντιπυρικής προστασίας (firewalls).
    - **d.** Συστήματα ελέγχου ακεραιότητας (integrity checkers).
    - **e.** Συστήματα παρεμπόδισης ύποπτης συμπεριφοράς (behavior blockers).

f. Προηγμένα Συστήματα IDS/IPS.

g. Εργαλειοθήκες ασφάλειας (Security Toolkits).

Όλες οι παραπάνω λύσεις εξειδικευμένου υλισμικού προστασίας μπορούν να εφαρμοστούν *τόσο στο επίπεδο ενός υπολογιστικού κόμβου (host-level), όσο και στο ευρύτερο, δικτυακό περιβάλλον (network or perimeter level)* π.χ. στην περίμετρο ενός δικτυοκεντρικού ΠΣ και τα αντίστοιχα προϊόντα στην αγορά διακρίνονται ανάλογα με τον συγκεκριμένο αυτό χώρο, που υπόσχονται να εποπτεύσουν και να φυλάξουν, με σπάνιο -αλλά όχι αδύνατο- το ενδεχόμενο ανάληψης διττού ρόλου.

2. Λειτουργικά συστήματα κόμβων:

a. Εγγενείς μηχανισμοί προστασίας (inherent policies).

b. Ενίσχυση υπαρχόντων Λ/Σ (OS Hardening).

c. Ισχυρά λειτουργικά περιβάλλοντα (ΠροστασίαΠυρήνα&ΔιαχείρισηΜνήμης).

3. Υλικό/Αρχιτεκτονική Υπολογιστών:

a. Πλατφόρμες ασφαλούς επεξεργασίας.

b. Σύγχρονοι επεξεργαστές (και μνήμες).

4. Λογισμικό εφαρμογών:

a. Ασφαλή πρωτόκολλα διασύνδεσης και επικοινωνίας.

b. Ασφαλή πρωτόκολλα εφαρμογών.

c. Προσεκτική συγγραφή κώδικα και παροχή υπηρεσιών ασφάλειας.

Με γνώμονα τα 3 διαφορετικά στάδια της γενικότερης διαδικασίας προστασίας ενός ΠΣ[134], δηλαδή την πρόληψη, τη διάγνωση-αναγνώριση και τη θεραπεία-αποκατάσταση, οι περισσότερες από τις παραπάνω διαφορετικές κατηγορίες συνεισφέρουν, όχι μόνο με παθητικό, αποτρεπτικό τρόπο δυσχεραίνοντας την υπονόμευση από μια κακόβουλη οντότητα, αλλά κυρίως με μια σειρά από διαφορετικές, πιο ενεργητικές μεθόδους, που αποτελούν κύρια στοιχεία της λειτουργίας τους και εγγυήσεις για αποτελεσματική ασφάλεια έναντι στις κακόβουλες, αυτοαναπαραγόμενες απειλές:

Α) Πρόληψη

[134] Όπως προσεγγίστηκαν στο σχετικό εδάφιο 2.2.8 του παρόντος κεφαλαίου.

- Δημιουργία αντιγράφων ασφάλειας
- Καραντίνα
- Φραγή με βάση υπογραφές ή γνωστές λίστες κακόβουλων απειλών (διευθύνσεις ή εφαρμογές)
- Αυθεντικοποίηση και Εξουσιοδότηση
- Προστασία κύριας μνήμης (RAM)
- Μηχανισμοί προστασίας πυρήνα Λ/Σ
- Λίστες ελέγχου πρόσβασης Λ/Σ
- Λίστες πρόσβασης για πρωτόκολλα και δικτυακές πόρτες (classic firewall access lists)
- Λίστες πρόσβασης για εφαρμογές (application firewall access lists)
- Ενημερωμένες εκδόσεις ασφάλειας ή διορθώσεις σφαλμάτων λογισμικού
- Εικονικοποίηση: Εγκιβωτισμός (Sandboxing)
- Κρυπτογράφηση δεδομένων και επικοινωνιών
- Προστασία σε επίπεδο εντολών επεξεργαστή

Β) Διάγνωση-Αναγνώριση

- Σάρωση-Ανίχνευση με βάση υπογραφές ή πρότυπες λίστες (Signature-based Scanning)
- Στατικές, ευριστικές μέθοδοι (Static Heuristics)
- Εικονικοποίηση: Εξομοίωση (Emulation)
- Αποσφαλμάτωση κώδικα (Debugging)
- Αποσυναρμολόγηση (Disassembling)
- Τεχνικές Παγίδευσης (Trapping)
- Αρχεία καταγραφής συμβάντων Λ/Σ (event or system log files)

Γ) Θεραπεία-Αποκατάσταση

- Απολύμανση-Εκκαθάριση μόλυνσης (Disinfection)
- Καραντίνα/Φραγή (Quarantine/Blocking)
- Διαγραφή (Deletion) & Επαναφορά από αντίγραφο ασφάλειας (Restore)

Έχοντας ψηλαφίσει τις διάφορες τεχνοτροπίες αντιμετώπισης ιών και σκουληκιών δεν πρέπει κανείς να παραλείψει να σταθεί στη *σπουδαιότητα μιας κατάλληλης και αποτελεσματικής εκπαίδευσης των χρηστών (user education/training)*, στα ευαίσθητα θέματα της ασφάλειας και των κακόβουλων απειλών[135]· άλλωστε η δράση των χρηστών (user action) των ΠΣ είναι συνήθως ο βασικότερος καταλύτης εξάπλωσης ιών και σκουληκιών ή αντίστασης σε μια κακόβουλη μόλυνση/υπονόμευσης και μια *στοχευμένη ενημέρωση και πληροφόρησή τους*, στα πλαίσια του επιβλαβούς λογισμικού, αποδεικνύεται τις περισσότερες φορές σύμμαχος και προτεραιότητα στην ευρύτερη προστασία των συστημάτων.[136]

Τόσο η εκπαίδευση των χρηστών, όσο και τα προαναφερόμενα συστήματα προστασίας δεν είναι δυνατόν να υιοθετούνται από τους ενδιαφερόμενους οργανισμούς, χωρίς να υπάρχει *μέριμνα για κεντρική οργάνωση, διοίκηση και συντονισμό των προβλεπόμενων, επιχειρησιακών ή τεχνικών, μέτρων*, στη μορφή μιας *διαδικασιοκεντρικής (process-centric security management) προσέγγισης*, που θα προασπίζει την *ομαλή ενσωμάτωση και τη διαρκή βελτιστοποίησή* τους κατά μήκος του δείνα εν λόγω οργανισμού.

Τέλος, δεν πρέπει κανείς να αμελεί τον *κυρίαρχο προστατευτικό ρόλο* που πολλές φορές κατέχουν τα *φυσικού τύπου μέτρα ελέγχου ανθρώπινης διαπίστευσης, εξουσιοδότησης και καταγραφής της πρόσβασης στα υπολογιστικά συστήματα* (π.χ. κάμερες ασφάλειας, βιομετρικά συστήματα κτλ), ιδιαίτερα μάλιστα μετά τη μεγάλη διάσταση που έχουν προσλάβει στις μέρες μας, ούτε να παραγνωρίζει το *σημαντικό, αποτρεπτικό ρόλο* που επιτελούν *τα εκάστοτε νομικά πλαίσια*, στο θέμα της πληροφοριακής εχθροπραξίας με κακόβουλο λογισμικό.

Στο κεφάλαιο 4 θα αποπειραθούμε να προχωρήσουμε σε μια εκτενέστερη και πιο διεξοδική ανάλυση όλων όσων ακροθιγώς αναφέρθηκαν στο παρόν εδάφιο, στοχεύοντας στην σε βάθος κάλυψη των ιδιαίτερων, τεχνικών και φυσικών, μέτρων, διαδικασιών και έννομων κανόνων ασφάλειας και προστασίας της πληροφορίας από την έκθεση σε τυχούσα κακόβουλη, αυτοαναπαραγόμενη απειλή.

---

[135] Κύρια, βιβλιογραφική αναφορά: [ERBSCHLOE-TWS].

[136] Ισχύει η ρήση «η ενημέρωση βοηθά στην πρόληψη», αλλά η εκπαίδευση των χρηστών μπορεί ταυτόχρονα και παράλληλα να αποτελεί συνδετικό, απαραίτητο κρίκο και για μια αποτελεσματική, έγκαιρη διάγνωση και θεραπεία μιας ιομορφικής απειλής ή μιας έξαρσης του δείνα σκουληκιού. Η αντίδραση του χρήστη, σε μια τέτοια περίσταση, είναι ευθέως ανάλογη της σχετικής εκπαίδευσης που έχει λάβει.

3 Κακόβουλο λογισμικό που αυτοαναπαράγεται: αρωγός στις πληροφοριακές εχθροπραξίες

Στην ενότητα αυτή, συζητώνται βασικά χαρακτηριστικά της πληροφοριακής εχθροπραξίας που βασίζεται σε αυτοαναπαραγόμενο, κακόβουλο λογισμικό.

Στο παρόν κεφάλαιο, εκτός των άλλων, θα επιχειρήσουμε και μια πρωτότυπη ταξινόμηση του παραπάνω λογισμικού, με βάση την αποτελεσματικότητα του στην εξυπηρέτηση στρατηγικών στόχων μιας πληροφοριακής επίθεσης.

3.1 Επιθέσεις πληροφοριακού τύπου με χρήση επιβλαβούς, αυτοαναπαραγόμενου λογισμικού

Το αυτοαναπαραγόμενο, κακόβουλο λογισμικό φέρει μια σειρά από πολύ σημαντικές ιδιότητες που, σύμφωνα με τον John Aycock και πολλούς, άλλους ερευνητές, το καθιστούν εξαιρετικά χρήσιμο όπλο στα πλαίσια οργανωμένων και επιτηδευμένων επιθέσεων πληροφοριακής εχθροπραξίας:[137]

[137] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM], [NISER-FCW], [GRIMES-MMCVPW], [YANG-AMCW], [WEAVER_PAXSON-TCW].

Γαμψή Εισβολή

Η εισβολή του κακόβουλου λογισμικού σε ένα ΠΣ γίνεται παρακάμπτοντας μία μόνο φορά το κάθε σύστημα ασφάλειας και χτυπώντας στον πλέον αδύναμο κρίκο του συστήματος, είτε αυτός είναι μια τεχνολογική ευπάθεια είτε πρόκειται για τους ανθρώπους που το χειρίζονται.

Παραμονή

Η επίδραση ενός ιού ή σκουληκιού παραμένει σε ένα σύστημα, μέχρις ότου ο αντίπαλος καταφέρει να εντοπίσει και εξουδετερώσει το κακόβουλο πρόγραμμα. Αυτή η παραμονή/επιμονή (persistence) επιτρέπει την προκαταβολική επίθεση σε στόχους, με το επιβλαβές λογισμικό να παραμένει σε λανθάνουσα κατάσταση (dormant) και να ξεκινά τη δράση του, όταν κριθεί αναγκαίο.

Στόχευση

Το αυτοαναπαραγόμενο, επιβλαβές λογισμικό επιτρέπει είτε άμεση, απευθείας στόχευση των αντιπάλων είτε έμμεση και πιο συγκαλυμμένη, μέσω ευπαθών σημείων διαφόρων, διασυνδεδεμένων συστημάτων πληροφοριών, προεξάρχοντος του Διαδικτύου. Στην περίπτωση της έμμεσης στόχευσης, ο πρόσθετος βαθμός ανωνυμίας και δυσκολίας ανίχνευσης της πηγής της επίθεσης έρχεται με το τίμημα της ανάγκης για προσεκτικό σχεδιασμό του κακόβουλου προγράμματος, ώστε αυτό να μην ξεφύγει από τον έλεγχο και επηρεάσει και τα συστήματα πληροφοριών, που είναι χρήσιμα στον επιτιθέμενο, εκμεταλλευόμενο πιθανές ευπάθειες και αυτών.

Εξαπάτηση

Υπάρχουν πολλές τεχνικές και μέθοδοι, που μπορούν να χρησιμοποιήσουν τόσο οι ιοί όσο και τα σκουλήκια, για την παρουσίαση ψευδών, πλαστών ή παραπλανητικών πληροφοριών σε έναν αντίπαλο, χωρίς αυτός ή τα συστήματά του να μπορούν να το καταλάβουν εύκολα και εγκαίρως.

Απομακρυσμένη διαχείριση

Την αξιοπιστία των ιών και των σκουληκιών ως όπλων πληροφοριακού πολέμου ενισχύει η δυνατότητα για απομακρυσμένη διαχείριση και έλεγχο των κακόβουλων προγραμμάτων από την επιτιθέμενη οντότητα. Ο μερικός έλεγχος της λειτουργίας και της δράσης ενός κακόβουλου προγράμματος είναι συμπληρωματικός του ρόλου της αυτοματοποίησης του επιβλαβούς λογισμικού, που αναλύουμε αμέσως παρακάτω, και όταν χρησιμοποιείται με

σύνεση και προσεκτικό σχεδιασμό είναι ανεκτίμητης αξίας για την επιτυχία μιας πληροφοριακής εχθροπραξίας.

Αυτοματοποίηση

Η σε μεγάλο βαθμό αυτοματοποιημένη διαδικασία επίθεσης, επιβίωσης και εξάπλωσης του αυτοαναπαραγόμενου πληροφοριακού όπλου απεμπλέκει και κατά μία έννοια προστατεύει το εγχείρημα της πληροφοριακής εχθροπραξίας από αθέμιτη ανάμειξη και ενδεχόμενα λάθη του ανθρώπινου παράγοντα, είτε στη μορφή του θύματος είτε σε αυτήν του επιτιθέμενου. Η εξάρτηση της διάδοσης ενός κακόβουλου προγράμματος από την ευπιστία των χρηστών δεν παρέχει τη βέλτιστη πρακτική επιτυχίας μιας πληροφοριακής επίθεσης, ενώ τυχόν υπέρμετρος έλεγχος του κακόβουλου προγράμματος από τον επιτιθέμενο εκτός των άλλων μπορεί και να τον «προδώσει».

Κινητικότητα/Ευκινησία

Τα αυτοαναπαραγόμενα, επιβλαβή προγράμματα -και ιδιαίτερα τα σκουλήκια και οι συνδυασμένες απειλές- έχουν στη σύγχρονή τους θεώρηση αυξημένες δυνατότητες πλοήγησης και εμφανίζουν αξιοσημείωτη διάθεση για μετακίνηση από στόχο σε στόχο (πρόγραμμα, Η/Υ, ΠΣ), που εκδηλώνονται μέσω επιτηδευμένων ρουτινών εποικοδομητικής αξιοποίησης των πολυποίκιλων, ταχέων και πανταχού εξαπλωμένων, δικτυοκεντρικών υποδομών και υπηρεσιών. Το κλίμα ευρύτερης, παγκόσμιας συμμετοχής, επικοινωνίας, συνεργασίας και ανταλλαγής πληροφοριών της εποχής μας, σε συνδυασμό με την ιδιότητα της αυτοαναπαραγωγής (που από μόνη της συνεπάγεται κάποια εχέγγυα επιβίωσης και μετακίνησης), αλλά και την προηγούμενη διαπίστωση της δικτυοστρεφούς προσέγγισης των τρεχουσών απειλών, δημιουργεί προοπτικές σημαντικής και ενδεχομένως ραγδαίας διασποράς και εξάπλωσης για το κακόβουλο, αυτοαναπαραγόμενο λογισμικό και το «ωφέλιμό» του φορτίο. Η κινητικότητα προφυλάσσει με ενεργητικό τρόπο από την ολοκληρωτική εξόντωση/εξαφάνιση ενός είδους και του φορτίου αυτού.

Εύρος απειλών και απειλούμενων συστημάτων

Το αυτοαναπαραγόμενο, κακόβουλο λογισμικό, ανάλογα με την περίπτωση και το «ωφέλιμο» φορτίο του, μπορεί να εξυπηρετήσει πληθώρα από πιθανούς, στρατηγικούς στόχους του επιτιθέμενου, όπως:[138]

[138] Στα λογικά πλαίσια και με τον ιδαίτερο χαρακτήρα πληροφοριακής εχθροπραξίας, όπως την ορίσαμε εννοιολογικά στο εδάφιο 2.3 του επιστημονικού υποβάθρου της εργασίας.

1. Άρνηση υπηρεσίας και δεδομένων/Υποβάθμιση απόκρισης του συστήματος.
2. Υποκλοπή/Κατασκοπεία.
3. Αλλοίωση/Καταστροφή.
4. Απομακρυσμένος έλεγχος συστημάτων.
5. Υπόδυση Ρόλων/ Πλαστοπροσωπία.
6. Ματαιότητα χρήσης.

Τα θιγόμενα συστήματα βρίσκονται, κατ' ουσία, οπουδήποτε στον Πλανήτη, ανεξαρτήτως χωρικού περιορισμού, ειδικά αν διαθέτουν ανεπτυγμένη και έντονη, δικτυακή παρουσία και βασίζονται σε τυποποιημένες υποδομές ή προσφέρουν καθιερωμένες υπηρεσίες. Παράγοντες εκ των προτέρων περιορισμού της εξάπλωσης[139] μιας αυτοαναπαραγόμενης μόλυνσης/προσβολής εντοπίζει κανείς στο ιδιαίτερο είδος του επιλεγμένου από τους επιτιθέμενους «καναλιού» προσβολής, που έχει να κάνει με καθένα από τα 5 γνωστά[140], αλληλεξαρτώμενα και αλληλεπιδρώντα, συστατικά των δικτυοκεντρικών ΠΣ:

- Υλικό: Το ξεχωριστό περιβάλλον επεξεργασίας των Η/Υ (CPU και μνήμη) και των υπολογιστικών συστημάτων καθορίζουν το χώρο και τον ορίζοντα δράσης του οπλολογισμικού.
- Λογισμικό: Το στοχευόμενο Λ/Σ ή η ιδιαίτερη εφαρμογή[141], που θα «χτυπηθεί», με τις παρούσες ατέλειές τους επιβάλλουν διαφορετικές προσεγγίσεις για κάθε στόχο.
- Δεδομένα: Το είδος του ξενιστή που επιλέγεται για έναν ιό δεν είναι απαραίτητο να αγγίζει όλα τα ΠΣ. Επίσης, γενικότερα, η ιδιαίτερη υφή της επιθυμητής πληροφορίας απαιτεί και ξεχωριστή, επιθετική προσέγγιση.
- Δίκτυο: Τα εκάστοτε πρωτόκολλα επικοινωνίας και οι δικτυακοί μηχανισμοί προστασίας και οι ευπάθειές τους προσδιορίζουν τις διαφορετικές τακτικές των επιτιθέμενων.

[139] Μια επίθεση και η επακόλουθη, πιθανή υπονόμευση δεν (μπορεί ευτυχώς να) έχει (προς το παρόν τουλάχιστον) καθολικό χαρακτήρα, αλλά στοχεύει και επιδρά σε συγκεκριμένα συστήματα και ιδιότητες ή πληροφορίες αυτών. Όσο συχνότερα απαντώνται οι επιλεγμένες ευπάθειες και συστημικές διαρρυθμίσεις, τόσο μεγαλύτερο είναι το δυνητικό εύρος μιας προσβολής.

[140] Βλέπε και σχετικούς ορισμούς στο εδάφιο 2.1.2.

[141] Το ευπαθές πρόγραμμα που θα αποτελέσει σημείο εισόδου, φορέα ή/και αναμεταδότη μιας παραβίασης ασφάλειας.

- Άνθρωποι&Διαδικασίες: Η παρουσία λογής ανθρώπινων και διαδικαστικών ελλείψεων, παραβλέψεων, ευπαθειών και αδυναμιών καθορίζει σε μεγάλο βαθμό την επιλογή κεφαλών και ξενιστών και των κατάλληλων -μα όχι καθολικών- μεθόδων υπονόμευσης.

Για όλους τους παραπάνω λόγους, ευσταθεί η *θεώρηση των αυτοαναπαραγόμενων, κακόβουλων προγραμμάτων ως φορέων και όπλων πληροφοριακής εχθροπραξίας*. Ας επιθεωρήσουμε, όμως, πιο επισταμένως τα διάφορα είδη πληροφοριακής εχθροπραξίας, που καθίσταται δυνατή μέσω των προγραμμάτων αυτών.

3.1.1 Άρνηση υπηρεσίας και δεδομένων/ Υποβάθμιση απόκρισης του συστήματος

Οι ιοί και τα σκουλήκια μπορούν να χρησιμοποιηθούν σκόπιμα για την *υπονόμευση της διαθεσιμότητας αντίπαλων συστημάτων πληροφοριών*. Η ιδέα της χρονικής παρακώλυσης ενός συστήματος ή των υπηρεσιών του ή της πρόσβασης στα δεδομένα του, σε σημείο που παύει να είναι παραδεκτά χρήσιμο, δεν είναι καινούρια στο κακόβουλο λογισμικό. Πολλά είναι εκείνα τα κακόβουλα προγράμματα, ανάμεσά τους ιοί και σκουλήκια, που καταναλώνουν τους χρήσιμους πόρους –όπως μνήμη, εύρος ζώνης, διάρκεια επεξεργασίας, χώρο στο δίσκο- ενός υπολογιστικού συστήματος σε βάρος των επιτελικών λειτουργιών του εν λόγω συστήματος, με σκοπό να τις καθυστερήσουν χρονικά ή και να τις καταστήσουν μη εκτελέσιμες. Επίσης, είναι συνηθισμένο για σκουλήκια να εξαπολύουν επιθέσεις προς δικτυακούς τόπους ή συγκεκριμένες δικτυακές υπηρεσίες, με τέτοιο μαζικό τρόπο, που οι αιτήσεις εξυπηρέτησης όχι μόνο δεν μπορούν να περατωθούν σε ικανοποιητικό χρόνο, αλλά είναι τόσο πολλές, που πλημμυρίζουν τους εξυπηρετητές και τους θέτουν ουσιαστικά εκτός λειτουργίας, για όσο χρόνο διαρκεί η επίθεση τουλάχιστον. Οι αιτήσεις μιας επίθεσης άρνησης εξυπηρέτησης (Denial of Service, DoS), που πραγματοποιείται μέσω σκουληκιών, προέρχονται κατά κύριο λόγο από πολλαπλά στιγμιότυπα των σκουληκιών, που βρίσκονται κατανεμημένα και αποκεντρωμένα κατά μήκος πολλαπλών κόμβων διασυνδεδεμένων συστημάτων και που την κατάλληλη στιγμή πυροδοτούνται εξαπολύοντας συγχρονισμένα το μαζικό φορτίο άρνησης εναντίον κοινού στόχου (DistributedDOS). Τέλος, σε ένα πιο γενικό πλαίσιο δράσης, τόσο οι ιοί όσο και τα σκουλήκια, αφής στιγμής προσβάλλουν ένα ΠΣ, μπορούν να θέτουν κατά βούληση εκτός λειτουργίας κρίσιμες υπηρεσίες του ή να καθυστερούν/απορρίπτουν δυναμικά αιτήσεις εξυπηρέτησης-πρόσβασης χρηστών προς αυτό, καθιστώντας το με τον τρόπο αυτό οποιαδήποτε στιγμή και για όση διάρκεια κρίνεται απαραίτητο, είτε μη διαθέσιμο είτε διαθέσιμο με μη αποδεκτό χρόνο απόκρισης.

Η άρνηση εξυπηρέτησης αποτελεί σήμερα πρόβλημα, που μαστίζει τα περισσότερα ΠΣ και προκαλεί εκνευρισμό, διόλου ευκαταφρόνητες οικονομικές ζημίες και άλλα πολλά προβλήματα, τόσο στους κατόχους ενός υπό επίθεση συστήματος, όσο και στους χρήστες του.

Στα μέσα Ιουλίου του 2001, το κινεζικής έμπνευσης σκουλήκι W32/CodeRed προσπάθησε να εκτελέσει μια στοχοθετημένη επίθεση DoS ενάντια στον ιστοχώρο του Λευκού Οίκου www.whitehouse.gov (με τότε διεύθυνση IP 198.137.240.91), με το να συνδέεται συνεχώς σε αυτόν. Σε απάντηση στην επίθεση, οι υπεύθυνοι ασφάλειας άλλαξαν γρήγορα τη διεύθυνση IP. Εντούτοις, το σκουλήκι έφερε και ένα άλλο ωφέλιμο φορτίο που είχε στόχο συστήματα που έκαναν χρήση της κωδικοσελίδας (codepage) Αγγλικών Η.Π. (0x409) στους ιστοχώρους των διακομιστών Ιστού (Web Servers) τους. Σε αυτή την περίπτωση, το σκουλήκι μέσω επίθεσης τύπου υπερχείλισης καταχωρητών αποκτούσε παράνομη πρόσβαση και εγκαθιστούσε μια ρουτίνα «γαντζώματος» στη λειτουργία TcpSockSend() της προγραμματιστικής βιβλιοθήκης INFOCOMM.DLL του λογισμικού εξυπηρέτησης Ιστού της Microsoft IIS. Η ρουτίνα αυτή δεν άφηνε ένα μολυσμένο σύστημα να «μοιράσει» στο Διαδίκτυο το νόμιμο Web περιεχόμενό του. Αντ' αυτού, το σκουλήκι επεδείκνυε μια συγκεκριμένη σελίδα, που στην πλέον συνηθισμένη παραλλαγή του, έγραφε “HELLO! Welcome to http://www.worm.com! Hacked By Chinese!”.[142]

Στις 14 Αυγούστου 2003, διάφοροι αναλυτές σκέφτηκαν ότι το σκουλήκι W32/Blaster (Lovesan ή Lovsan) ήταν αρμόδιο για σημαντικότερη συσκότιση στις Ηνωμένες Πολιτείες και τον Καναδά. Το σκουλήκι είχε εδώ και τρεις ημέρες ελευθερωθεί. Οι τότε επίσημες εκθέσεις σε πρώτη φάση γρήγορα αρνήθηκαν αυτές τις αξιώσεις. Πράγματι, θεωρείται ότι το σκουλήκι δεν ήταν η πρωταρχική αιτία της συσκότισης. Εντούτοις, πιθανώς συνεισέφερε με την επιβράδυνση των συστημάτων επικοινωνιών, μεταξύ των κέντρων λειτουργίας ελέγχου ηλεκτρικής ενέργειας. Κατά συνέπεια οι χειριστές δικτύων δεν είχαν τη δυνατότητα να ελέγξουν εγκαίρως τα ηλεκτρικά συστήματα για να αποφύγουν περαιτέρω επικίνδυνες πτώσεις ισχύος ή βραχυκυκλώματα. Τελικά, οι εκθέσεις έδειξαν ότι το κέντρο ελέγχου ηλεκτρικής ενέργειας αντιμετώπισε "προβλήματα υπολογιστών," που ηχούν λίγο πολύ ως μια μόλυνση σκουληκιών. Τελικά, η ανατολική ακτή των Η.Π., συμπεριλαμβανομένης της περιοχής της πόλης της Νέας Υόρκης, δοκιμάστηκε από απώλειες ρευματοδότησης.

Ο W32/Blaster διαδιδόταν χάρη στην εκμετάλλευση μιας υπερχείλισης καταχωρητών (buffer overflow) που ήταν εφικτή στην υπηρεσία RPC-DCOM των ισχυρά ευάλωτων σε αυτήν την επίθεση λειτουργικών συστημάτων Windows 2000 και XP της Microsoft.[143] Βέβαια, και τα

---

[142] Πηγή: Διαδίκτυο, ιστοχώρος της online εγκυκλοπαίδειας WikiPedia, http://en.wikipedia.org/wiki/Code_Red_worm.

[143] Πηγή: Διαδίκτυο, ιστοχώρος της online εγκυκλοπαίδειας WikiPedia, http://en.wikipedia.org/wiki/Blaster_(computer_worm).

υπόλοιπα, λειτουργικά συστήματα της εταιρείας (τα βασισμένα στον πυρήνα NT), αν και δε μετέδιδαν περαιτέρω το σκουλήκι, επηρεάζονταν σημαντικά όσον αφορά τηη καλή λειτουργία τους (αστάθειες, καθυστερήσεις). Οι μολύνσεις του διαβόητου Blaster συνέβαιναν τόσο γρήγορα που τα τρωτά συστήματα δεν μπορούσαν να συνδεθούν με υπονομευμένα δίκτυα (εκτός αν προστατεύονταν από προσωπικού τύπου αντιπυρικές ζώνες), για να μεταφορτώσουν ενημερώσεις ασφάλειας επειδή το σκουλήκι «χτυπούσε» τα μηχανήματα σχεδόν αμέσως. Το εν λόγω σκουλήκι τελικά προσπάθησε μέσω άρνησης εξυπηρέτησης να επιτεθεί στον ιστοχώρο παροχής ενημερώσεων και αναβαθμίσεων για τα συστήματα της Microsoft, Windows Update (www.windowsupdate.com), όμως δεν ήταν ιδιαίτερα αποδοτικό κυρίως λόγω κακής επιλογής στόχου, που θα έπρεπε να είναι windowsupdate.microsoft.com, ώστε να δημιουργήσει σοβαρά προβλήματα. Προφανώς, μια επιτυχής επίθεση ενάντια στον συγκεκριμένο ιστότοπο θα έκανε ακόμα πιο δύσκολη τη διαδικασία «πατσαρίσματος»/θωράκισης των ευπαθών συστημάτων, επιτρέποντας στη διάδοση του σκουληκιού να μαίνεται. Ευτυχώς, ένας συστηματικός συνδυασμός αναβαθμίσεων λογισμικού και εφαρμογής αντιπυρικής προστασίας κατάφερε να το περιορίσει αισθητά βάζοντας φρένο στην ξέφρενη πορεία του. Ο Blaster σήμερα θεωρείται πλέον κάπως παρωχημένος, αν και συχνά-πυκνά κάποιες παραλλαγές του με διαφορετική και πιο επίκαιρη κεφαλή και διαφορετικό φορτίο, αλλά και με σημαντικά μικρότερο αντίκτυπο.

3.1.2 Υποκλοπή/ Κατασκοπεία

Η ενσωμάτωση επιθέσεων κοινωνικής μηχανικής/πολυμηχανίας (social engineering attacks)[144] στο ωφέλιμο φορτίο ιών και σκουληκιών, η χρησιμοποίηση spyware τεχνικών συλλογής πληροφοριών και η εγκατάσταση κερκοπορτών και rootkits είναι μερικοί από τους τρόπους, με τους οποίους γίνεται εφικτή μια *επίθεση υποβάθμισης της εμπιστευτικότητας των συστημάτων πληροφοριών* μέσω ιών και σκουληκιών.

Οι social engineering επιθέσεις που χρησιμοποιούνται, κυρίως από τα σκουλήκια και δευτερευόντως από ιούς, αποτελούν έναν ευφυή τρόπο υποκλοπής ευαίσθητων στοιχείων όπως usernames, password, e-mails, PINs των χρηστών συστημάτων υπό επίθεση. Ιδιαίτερα στις λεγόμενες επιθέσεις αλίευσης ή όπως είναι πιο γνωστές phishing attacks[145], οι επιτιθέμενες οντότητες προσποιούμενες ή υποδυόμενες οντότητες εγνωσμένης αξίας και εμπιστοσύνης για τον χρήστη -όπως διάσημες τράπεζες ή το τμήμα πληροφορικής του οργανισμού που ανήκει ο χρήστης-, τον προτρέπουν να εισάγει ιδιαίτερα ευαίσθητα στοιχεία

[144] Κύρια, βιβλιογραφική αναφορά: [COLE_RUIZ-SEHEIW].

[145] Κύρια, βιβλιογραφική αναφορά: [SZOR-ACVRD].

σε φόρμες ηλεκτρονικών σελίδων ή αλληλογραφίας προκειμένου να εκτελεστούν υποτιθέμενες χρήσιμες ή απαραίτητες για τον ίδιο λειτουργίες προκειμένου να του τα αποσπάσουν.

Στο οπλοστάσιο των ιών και των σκουληκιών ιδιαίτερα χρήσιμες για περιπτώσεις κατασκοπείας των αντίπαλων συστημάτων αποδεικνύονται και οι τεχνικές των κατασκόπων και κυρίως των spyware-loggers, που παρακολουθούν και καταγράφουν σε κάποιας μορφής αρχείο δεδομένων (log) ή κάπου στην κύρια μνήμη πληροφορίες για τις κρίσιμες κινήσεις των χρηστών (ακόμα και το τι πληκτρολογούν κάθε στιγμή) ή για γεγονότα εξέχουσας σημασίας των ΠΣ. Τα δεδομένα αυτά, εκτός των άλλων χρήσεων που θα μπορούσαν να έχουν στη δράση των κακόβουλων προγραμμάτων, μπορούν και να αποστέλλονται πίσω στην επιτιθέμενη οντότητα για επιθεώρηση και εύρεση-απομόνωση των χρήσιμων για εκείνη πληροφοριών.

Η ύπαρξη κάποιας μορφής κερκόπορτας για τη μεταφορά των κλεμμένων πληροφοριών στον επιτιθέμενο κατάσκοπο δεν είναι πάντοτε αναγκαία ή πλέον αποτελεσματική, αφού ο επιτιθέμενος μπορεί να χρησιμοποιεί κάποιον νόμιμο και παραδεκτό τρόπο επικοινωνίας του συστήματος με τον έξω κόσμο και να διοχετεύει «τα κλοπιμαία» μέσα στην εξερχόμενη κίνηση με κρυφό ή απροκάλυπτο τρόπο. Παρόλ' αυτά, συνηθίζεται αρκετά συχνά οι ιοί και τα σκουλήκια να εγκαθιστούν κερκόπορτες για την παρακολούθηση των συστημάτων-στόχων.

Ειδικά σχεδιασμένα σκουλήκια και ιοί μπορούν να τοποθετήσουν και να εκμεταλλευτούν την παρουσία και rootkits για να υπονομεύσουν ένα ΠΣ σε τόσο χαμηλό επίπεδο, ώστε χωρίς κανένα πρακτικά περιορισμό να παρακολουθούν, να συλλέγουν και να αποστέλλουν πληροφορίες εξ αυτού στον επιτιθέμενο και μάλιστα χωρίς η διαδικασία αυτή να γίνεται εύκολα αντιληπτή από τα συστήματα ασφάλειας ή τους χρήστες.

Τέλος, δεν πρέπει να παραγνωρίζουμε ότι η έννοια της υποκλοπής και της κατασκοπείας δε θα είχε νόημα, αν δεν έβρισκε εφαρμογή και στο πεδίο της παρακολούθησης των γραμμών δικτυακής επικοινωνίας ενός ΠΣ και της εισερχόμενης και εξερχόμενης κίνησής τους. Πρέπει να τονιστεί πως κρίσιμες πληροφορίες δεν μπορούν να αποτελούν μόνο όσες εδρεύουν εντός των λογικών ορίων του κάθε ΠΣ, αλλά θεωρούνται εξίσου σημαντικές και όσες διακινούνται μεταξύ των διαφόρων συστημάτων. Ιοί και σκουλήκια μπορούν να κατασκοπεύουν δυναμικά την πληροφοριακή κίνηση μεταξύ διασυνδεδεμένων συστημάτων Η/Υ για λογαριασμό αντιμαχόμενων δυνάμεων, με τον ίδιο περίπου τρόπο που ένας sniffer αφουγκράζεται το δίκτυο για χρήσιμα πακέτα δεδομένων.

Το W32/Mimail.I@mm είναι ένα παράδειγμα μιας απλής, αλλά μάλλον αποτελεσματικής επίθεσης αλίευσης.[146] Τα σκουλήκια της οικογένειας στέλνονται ως μηνύματα ηλεκτρονικού ταχυδρομείου. Στην προσπάθειά τους να κλέψουν πληροφορίες, τα στιγμιότυπα του συγκεκριμένου είδους σκουληκιού υποδύονται διαλόγους που ισχυρίζονται πως προέρχονται από την γνωστή υπηρεσία διαδικτυακών πληρωμών PayPal και οι οποίοι ούτε λίγο ούτε πολύ ζητούν από τον χρήση να πληκτρολογήσει έναν αριθμό πιστωτικής κάρτας ή/και άλλες προσωπικές πληροφορίες. Οι κλεμμένες πληροφορίες αποθηκεύονται από την υπόσταση μέσω δυναμικού ή στατικού HTML κώδικα, που είναι ενεργοποιημένος στο σώμα του μηνύματος αλληλογραφίας. Κατόπιν, οι πληροφορίες κρυπτογραφούνται και στη συνέχεια στέλνονται πίσω στον επιτιθέμενο.

Ένα άλλο παράδειγμα είναι η οικογένεια συνδυασμένων απειλών W32/Bugbear@mm, η οποία διαδίδεται με τη χρησιμοποίηση ποικίλων τεχνικών, συμπεριλαμβανομένης της μαζικής αποστολής μηνυμάτων αλληλογραφίας, της επιμόλυνσης δικτυακών, κοινόχρηστων χώρων αποθήκευσης και της ιομορφικής μόλυνσης αρχείων.[147] Επιπλέον, κάποιες παραλλαγές υποστηρίζουν και μια λειτουργία keylogging. Χρησιμοποιώντας το keylogger-spyware, το σκουλήκι μπορεί να συλλέξει πάσης φύσεως (ενδεχομένως και οικονομικού τύπου) ευαίσθητες πληροφορίες που οι χρήστες πληκτρολογούν στο σύστημα. Οι Bugbears στέλνουν τις συλλεχθείσες πληροφορίες σε διάφορους λογαριασμούς ηλεκτρονικού ταχυδρομείου, που ανήκουν στον επιτιθέμενο. Επιπλέον, μερικές παραλλαγές του εν λόγω όπλου στοχεύουν συγκεκριμένα σε πιστωτικά ιδρύματα. Οι συγκεκριμένου είδους απειλές φέρουν έναν μακρύ κατάλογο περισσότερων από 1.000 ονομάτων περιοχών Ιστού και αλληλογραφίας (domain names) που ανήκουν σε τράπεζες από όλον τον κόσμο. Σε περίπτωση επιτυχούς μόλυνσης των υπολογιστικών συστημάτων των εν λόγω περιοχών (κυρίως με τη βοήθεια μαζικού spamming) οι υποστάσεις του προγράμματος θα στείλουν τα στοιχεία που συλλέγονται μέσω των keyloggers από τους υπονομευμένους στόχους στους λογαριασμούς ηλεκτρονικού ταχυδρομείου του επιτιθεμένου. Χρησιμοποιώντας τις πληροφορίες αυτές, ο επιτιθέμενος ελπίζει να συνδεθεί επιτυχώς με ένα ενδοτραπεζικό ή διατραπεζικό δίκτυο πληροφοριών και να αποκομίσει οικονομικό κέρδος.

---

[146] Πηγή: Διαδίκτυο, ιστοχώρος της εταιρείας παροχής εγνωσμένης αξίας και αποδοχής λύσεων προστασίας από το κακόβουλο λογισμικό Symantec, http://www.symantec.com/security_response/writeup.jsp?docid=2003-111317-1701-99&tabid=2.

[147] Πηγή: Διαδίκτυο, ιστοχώρος της εταιρείας παροχής εγνωσμένης αξίας και αποδοχής λύσεων προστασίας από το κακόβουλο λογισμικό Symantec, http://www.symantec.com/security_response/writeup.jsp?docid=2002-093007-2144-99&tabid=2.

3.1.3 Αλλοίωση/ Παραχάραξη/ Καταστροφή

Το «ωφέλιμο» φορτίο ενός ιού ή σκουληκιού μπορεί να είναι έτσι προγραμματισμένο ώστε σκόπιμα ή ακούσια να υπονομεύει την ακεραιότητα δοθέντος ανταγωνιστικού ΠΣ. Μια *πληροφοριακή επίθεση υποβάθμισης της ακεραιότητας ενός ΠΣ* σκόπιμα περιλαμβάνει κατάλληλο, επιθετικό κώδικα στο φορτίο του κακόβουλου προγράμματος. Ο κώδικας αυτός μπορεί εναλλακτικά να οδηγεί σε τυχαία αλλοίωση ή/και περίτεχνη παραποίηση των δεδομένων ενός συστήματος ή των μηνυμάτων μεταξύ διασυνδεδεμένων κόμβων συστημάτων ή σε καταστροφή δεδομένων και μηνυμάτων, ακόμα-ακόμα και σε υλικές ζημιώσεις στον εξοπλισμό συστημάτων. Οποιαδήποτε από αυτές της μορφές επίθεσης συνιστά παραβίαση της ακεραιότητας ενός ΠΣ και όλες είναι πιθανώς επιτεύξιμες με τη βοήθεια ιών και σκουληκιών. Παρακάτω, παρατίθενται οι κατηγορίες και ορισμένα παραδείγματα καταστρεπτικών ιών και σκουληκιών:[148]

- Αλλοιωτές δεδομένων και μηνυμάτων, όπως π.χ. ο Σλοβακικής καταγωγής One_Half, που επέβαλλε μια συμβιωτικού τύπου σχέση με το μολυσμένο μηχάνημα, κρυπτογραφώντας με απλό και ταυτόχρονα έξυπνο και ελάχιστα αντιληπτό από μη εξειδικευμένους χρήστες τρόπο τα περιεχόμενα των δίσκων αποθήκευσης. Η βίαιη απομάκρυνση του ήταν λάθος πρακτική ως αλληλοσυγκρουόμενη και ασυμβίβαστη κατάσταση με την επιτυχημένη αποκρυπτογράφηση των τροποποιημένων δεδομένων και συχνά οδηγούσε σε απώλεια πληροφοριών. Ένα ακόμη παράδειγμα ήταν ο ιός Dark_Avenger.1800.A, που τοποθετούσε την εγγραφή "Eddie lives…somewhere in time" σε τυχαίους τομείς των δίσκων, αλλά όχι στους πίνακες FAT, προκαλώντας έτσι αλλοίωση πληροφοριών μα και τον αργό «θάνατο» των υπολογιστικών συστημάτων.
- Καταστροφείς δεδομένων και μηνυμάτων, όπως π.χ. ο κακόφημος ιός Michelangelo, που επικάλυπτε τους πρώτους 256 κυλίνδρους που βρίσκονταν στο διαμέρισμα εκκίνησης (boot partition) του μολυσμένου συστήματος.
- Καταστροφείς υλικού εξοπλισμού, όπως π.χ. ο διαβόητος Ταϊβανέζικης προέλευσης W95/CIH[149], που χάρη σε επιπέδου πυρήνα εντολές I/O, «σκότωσε» κατ' εκτίμηση επιτυχώς το 1998 τουλάχιστον 10.000 PCs, με την επικάλυψη του τμήματος του κώδικα εκκίνησης του Flash BIOS τους (bootstrap Flash BIOS code).

[148] Κύρια, βιβλιογραφική αναφορά: [SZOR-ACVRD].

[149] Κύρια, βιβλιογραφική αναφορά: [O'CONNOR_TOBLER-CIHV].

3.1.4 Απομακρυσμένος έλεγχος συστημάτων

Οι ιοί και τα σκουλήκια μπορούν να καταστήσουν με τη γρήγορη εξάπλωση και την κατάλληλη εναπόθεση backdoors ή rootkits ολόκληρα δίκτυα Η/Υ και συστημάτων πληροφοριών έρμαια μη εξουσιοδοτημένης πρόσβασης και συνεπώς παράνομου, απομακρυσμένου ελέγχου. Ένα υπολογιστικό σύστημα που τελεί υπό αυτές τις συνθήκες λόγω προσβολής από κάποιον ιό ή σκουλήκι ονομάζεται *ζόμπι (zombie)*.[150]

Τα ζόμπι υπολογιστικά συστήματα, αφού υπονομευτούν από τον επιτιθέμενο, μπορούν να χρησιμοποιηθούν ως υποχείρια για πληθώρα κακόβουλων εργασιών, εν αγνοία των νόμιμων ιδιοκτητών τους.

Τα συστήματα αυτά συναντούν ευρεία διάδοση, σήμερα, σε βαθμό που ολόκληρα δίκτυα από ζόμπι μπορούν να διατεθούν προς πώληση για την εξυπηρέτηση κακόβουλων αναγκών. Ο έλεγχος αυτών των ζόμπι δικτύων γίνεται, συνήθως, με τη βοήθεια καναλιών IRC, στα οποία είναι προγραμματισμένα τα ζόμπι μηχανήματα να περιμένουν για εντολές.[151] Για το λόγο αυτό δίκτυα τέτοιων ζόμπι Η/Υ αναφέρονται πολύ συχνά και ως *botnets*, από το ιδιαίτερο όνομα των αυτοματοποιημένων IRC προγραμμάτων-πελατών (bots).

Οι πλέον κοινές εργασίες για τα συστήματα αυτά είναι η μαζική αποστολή ανεπιθύμητης αλληλογραφίας (spamming) και η συμμετοχή σε μεγάλου μεγέθους επιθέσεις άρνησης υπηρεσίας (DDOS). Μια άλλη εργασία για τα δίκτυα αυτά θα μπορούσε να είναι και η αρχική εμφύτευση σκουληκιών (initial seeding)[152] είτε μέσω του spamming του σκουληκιού σε ανυποψίαστους χρήστες είτε μέσω απευθείας διοχέτευσης στιγμιοτύπων του σκουληκιού στους ζόμπι Η/Υ. Παρατηρεί κανείς, λοιπόν, ότι δημιουργείται ένας φαύλος κύκλος με τα botnets να αποτελούν ικανότατο μέσο για την πραγματοποίηση μη ανιχνεύσιμων και σε μεγάλο βαθμό ανώνυμων επιθέσεων πληροφοριακής εχθροπραξίας αλλά και πηγή άλλων ενοχλητικών προβλημάτων, ενώ ταυτόχρονα προκύπτουν ως άμεσο αποτέλεσμα της δράσης αυτοαναπαραγόμενου, κακόβουλου λογισμικού και συνιστούν και τα ίδια *μορφή πληροφοριακής εχθροπραξίας, που καταλύει κάθε έννοια κατοχής και ελέγχου κατά Parker*.

Αυτό είναι το ζήτημα στην περίπτωση αυτή. Οι ιοί και τα σκουλήκια κάνουν εφικτή -μέσω της δυνατότητας απομακρυσμένης διαχείρισης των προσβεβλημένων συστημάτων που παρέχουν στον επιτιθέμενο- την απώλεια κατοχής ή ελέγχου ολόκληρων ΠΣ. Τα botnets δεν είναι παρά μια απλή υπόσταση του προβλήματος που μπορεί να προκύψει λόγω αυτής της κατάστασης. Ο πραγματικός, νόμιμος ιδιοκτήτης του προσβεβλημένου ΠΣ «μοιράζεται» ανά

---

[150] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM].

[151] Πηγή: Διαδίκτυο, ιστοχώρος της online εγκυκλοπαίδειας WikiPedia, http://en.wikipedia.org/wiki/Botnet.

[152] Με τον όρο αυτό αναφερόμαστε στη μέθοδο και το επιλεγμένο μέσο της απαραίτητης, αρχικής τοποθέτησης των σκουληκιών σε κάποιο «κανάλι» διάδοσης, διάχυσης και διασποράς τους.

πάσα στιγμή αυτό το προνόμιο της ιδιοκτησίας επί των πόρων και των κεφαλαίων του, με τον «αόρατο», ανεπιθύμητο, «λαθραίο ιδιοκτήτη» που ελέγχει το σύστημα απομακρυσμένα με ό,τι αυτό συνεπάγεται. Ο επιτιθέμενος μπορεί έτσι οποιαδήποτε στιγμή να επεμβαίνει ανενόχλητος στη λειτουργία και τις πληροφορίες ΠΣ που δεν του ανήκουν, να τις επηρεάζει κατά βούληση και να τις χρησιμοποιεί για ίδιον όφελος ή εναντίον τρίτων, όπως π.χ. για να διαπράττει οποιαδήποτε πληροφοριακή εχθροπραξία σε περαιτέρω συστήματα και μάλιστα με τρόπο αρκετά ανώνυμο και συγκαλυμμένο.

Τα σκουλήκια έχουν συχνά ενσωματωμένα backdoors. Ένα περίφημο παράδειγμα ενός τέτοιου σκουληκιού είναι το W32/HLLW.Qaz.A. Αυτό το σκουλήκι ανακαλύφθηκε αρχικά στην Κίνα, τον Ιούλιο του 2000. Ο QAZ λειτουργεί και ως ένας companion ιός[153], αλλά εξαπλώνεται επίσης στο δίκτυο ως συνδυασμένη απειλή. Επιπλέον, παρέχει μέσω κερκόπορτας το «κανάλι» που θα επιτρέψει σε έναν απομακρυσμένο χρήστη να συνδεθεί με και να ελέγξει το μολυσμένο υπολογιστή χρησιμοποιώντας τα δικτυακή πόρτα 7597.[154] Ο QAZ πολλαπλασιάζεται μέσω των κακώς προστατευμένων κοινόχρηστων πόρων τύπου NetBIOS και προσπαθεί να βρει έναν τρωτό υπολογιστή για να καταλάβει. Αφού τον υπονομεύσει, η διεύθυνση IP του κάθε φορά στέλνεται μέσω ηλεκτρονικού ταχυδρομείου πίσω στον επιτιθέμενο. Η κερκόπορτα στο ωφέλιμο φορτίο αφού εγκατασταθεί περιμένει για συνδέσεις στην προαναφερόμενη πόρτα. Αυτό επιτρέπει σε έναν εισβολέα να αποκτήσει προνομιούχα πρόσβαση στο μολυσμένο μηχάνημα και να το κατευθύνει, όπως βούλεται, βουλεύεται και επιθυμεί. Σύμφωνα με διάφορες πηγές, ο QAZ ήταν πιθανότατα υπεύθυνος για επιτυχείς επιθέσεις ενάντια σε δίκτυα πληροφοριών της Microsoft, υπονομεύοντας ένα επισφαλές, οικιακό σύστημα που διατηρούσε ανοιχτές συνδέσεις με το εταιρικό δίκτυο, επιτρέποντας με αυτόν τον τρόπο στον επιτιθέμενο την πρόσβαση σε πολύτιμες πληροφορίες.

3.1.5 Υπόδυση Ρόλων/ Πλαστοπροσωπία

Η *παραβίαση της αυθεντικότητας πληροφοριών και μηνυμάτων* είναι κάτι που εύκολα πραγματοποιείται με τη βοήθεια κακόβουλου, αυτοαναπαραγόμενου λογισμικού. Στην προσπάθεια αυτή, συνεισφέρουν και κάποιες, προαναφερόμενες μέθοδοι υπονόμευσης, όπως η υποκλοπή-συλλογή πληροφοριών μέσω παράνομης παρακολούθησης (με χρήση λ.χ. spyware τεχνικών) ή απομακρυσμένης διαχείρισης (μέσω π.χ. κάποιου backdoor).

---

[153] Βλέπε και αντίστοιχο εδάφιο 3.2.3.

[154] Πηγή: Διαδίκτυο, ιστοχώρος της εταιρείας παροχής εγνωσμένης αξίας και αποδοχής λύσεων προστασίας από το κακόβουλο λογισμικό Symantec, http://www.symantec.com/security_response/writeup.jsp?docid=2000-122013-5944-99&tabid=1.

Οι επιθέσεις υπόδυσης ρόλων και *πλαστοπροσωπίας (impersonation)* λειτουργούν αρνητικά τόσο για τις υπό επίθεση οντότητες όσο και για αυτές που πλαστοπροσωπούνται. Η υπόδυση ρόλων μπορεί να αποτελέσει ιδανικό προπύργιο για την εκδήλωση και καρποφορία και έτερων επιθέσεων πληροφοριακού τύπου (cascaded attacks), ενώ συχνά χρησιμοποιείται από τους επιτιθέμενους έμμεσα και ως μηχανισμός δυσφήμησης των οντοτήτων που πλαστοπροσωπούνται και υποβάθμισης της εμπιστοσύνης που τρέφει σε αυτές το ευρύτερο περιβάλλον τους. Τέλος, αποτελεί και έναν εξαιρετικό μηχανισμό ανωνυμίας και κάλυψης για τον δράστη μιας επίθεσης σε ένα σύστημα, εφόσον αυτός μπορεί να προσποιηθεί πως ήταν κάποιος άλλος.

Λόγου χάριν, οι προαναφερόμενες phishing επιθέσεις προϋποθέτουν την αποστολή μη αυθεντικών μηνυμάτων -προερχόμενων φαινομενικά από έμπιστες οντότητες- προς χρήστες, με σκοπό την εξαπάτηση τους και την υπεξαίρεση ευαίσθητων, προσωπικών τους στοιχείων. Στα μηνύματα αυτά, η εγγενής πλαστοπροσωπία αποκαλύπτεται, συνήθως, με μια πιο προσεκτική εξέταση πρόσθετων πληροφοριών των πλαστών μηνυμάτων. Δεν παύει, όμως, να βελτιώνεται διαρκώς η «πιστότητά» τους και να πείθουν ολοένα και περισσότερο κόσμο.

Γνωστές επιθέσεις αυτού του τύπου αποτελούν και οι λεγόμενες επιθέσεις της ενδιάμεσης οντότητας (man-in-the-middle attacks), που μπορούν να αποτελέσουν τον προπομπό και τον εκφραστή αλλοίωσης, κατασκοπείας, άρνησης εξυπηρέτησης και άλλων πληροφοριακών απειλών. Το κακόβουλο, αυτοαναπαραγόμενο λογισμικό μπορεί εύκολα να χρησιμοποιηθεί για να υλοποιηθούν επιτυχώς επιθέσεις man-in-the-middle[155], σύμφωνα με το ακόλουθο, λογικό σχήμα:[156]

- Το κακόβουλο λογισμικό περιμένει για αιτήσεις εξυπηρέτησης ή για άλλα δεδομένα αφουγκραζόμενο το μέσο μετάδοσής τους.
- Όταν παρουσιαστούν ανάλογες αιτήσεις ή ρεύματα δεδομένων, τα αποσπά κατά βούληση, προτού φτάσουν στον προορισμένο σταθμό ή σύστημα εξυπηρέτησης, υποδυόμενο πως είναι αυτό. Παριστάνει, δηλαδή, το νόμιμο παραλήπτη των αιτήσεων ή των δεδομένων.
- Μόλις ολοκληρώσει την όποια επεξεργασία (αντιγραφή, αλλοίωση) της αίτησης εξυπηρέτησης ή των δεδομένων είτε τα προωθεί στον αρχικό προορισμό τους είτε τα απορρίπτει.

[155] Πηγή: Διαδίκτυο, ιστοχώρος της online εγκυκλοπαίδειας WikiPedia, http://en.wikipedia.org/wiki/Man-in-the-middle_attack.

[156] Κύρια, βιβλιογραφική αναφορά: [XUKAI-SC].

Πλαστοπροσωπία και υπόδυση ρόλων μπορεί να πραγματοποιηθεί και εντός των διακριτών τμημάτων αυθεντικοποίησης, εξουσιοδοτήσεων και καταγραφής (AAA) του ελέγχου πρόσβασης ενός ΠΣ. Ιοί και σκουλήκια οπλίζουν τον επιτιθέμενο με τη δυνατότητα, τόσο να αποκτήσει πρόσβαση σε ένα σύστημα προσπαθώντας να «σπάσει» κάποιον από τους νόμιμους λογαριασμούς τους συστήματος[157], όσο και να υποδυθεί κάποιον συμμετέχοντα ενός ήδη προσβεβλημένου ή «σπασμένου» συστήματος λειτουργώντας υπό το λογαριασμό του ή γενικότερα να προσποιηθεί πως είναι κάποια άλλη οντότητα, ενώ δεν είναι, αποκρύπτοντας τα πραγματικά, ταυτοτικά χαρακτηριστικά του.

3.1.6 Ματαιότητα χρήσης

Στα πλαίσια αυτής της απειλής μπορούμε να θεωρούμε τις επιθέσεις ιών και σκουληκιών, που σκοπό έχουν να μετατρέψουν κρίσιμα δεδομένα και πληροφορίες τυχόντος συστήματος σε εναλλακτικές αναπαραστάσεις τους, που με τις τρέχουσες συνθήκες και παραμέτρους είναι αδύνατον να γίνουν αντιληπτά ή να χρησιμοποιηθούν αποτελεσματικά από το σύστημα ή τους χρήστες του, χωρίς τη μετατροπή τους σε άλλη μορφή ή χωρίς αλλαγή παραμετροποίησης του συστήματος. Η μετατροπή αυτή δεν πρέπει να εννοείται ως αλλοίωση ή φθορά της πληροφορίας που περιέχουν τα δεδομένα, αλλιώς πρόκειται για παραβίαση της ακεραιότητάς τους και εμπίπτει σε άλλη κατηγορία εχθροπραξίας. Π.χ. η κρυπτογράφηση κρίσιμων δεδομένων ενός συστήματος κατά τη διάρκεια μιας κρυπτοϊομορφικής επίθεσης (cryptoviral (money or information) extortion attack)[158] αποτελεί παραβίαση της χρησιμότητας του εν λόγω συστήματος. Σκουλήκια κάλλιστα μπορούν να σχεδιαστούν για να αποτελέσουν τους μεταγωγούς φορτίων κρυπτοϊμορφικών επιθέσεων κατά μήκους διασυνδεδεμένων υποδομών ΠΣ. Ακόμα και η μετατροπή ενός αρχείου κειμένου (π.χ. μιας ιστοσελίδας) από μια μορφή κωδικοποίησης ή γραμματοσειράς σε μια άλλη, χωρίς απώλεια πληροφορίας, μπορεί να αποτελέσει *υποβάθμιση της χρησιμότητας ενός συστήματος*, αν η νέα αναπαράσταση δυσχεραίνει την αντίληψη των χρηστών. Ιοί και σκουλήκια ικανά να πραγματοποιούν κάτι τέτοιο είναι, συνήθως, πολύ εύκολο να σχεδιαστούν.

Ως ενδεικτικό παράδειγμα του εν λόγω πλαισίου επίθεσης, ο ιός W95/HPS[159], που ενεργοποιείται μόνο τα Σάββατα, ελέγχει εάν ένα μη-συμπιεσμένο αρχείο εικόνας τύπου BMP (bitmap) των Windows έχει ανοιχτεί από το χρήστη και αντιστρέφει την εικόνα στο

---

[157] Το οπλολογισμικό είναι ικανό να εφαρμόζει εμπεριστατωμένους αλγορίθμους για συντονισμένες λεξικογραφικές ή ωμές, τυχαίες δοκιμές εύρεσης (dictionary or brute-force attacks) και επιβεβαίωσης κρίσιμων δεδομένων της ευρύτερης κατηγορίας των κωδικών πρόσβασης.

[158] Κύρια, βιβλιογραφική αναφορά: [BALEPIN-SCDC], [YOUNG_YUNG-CEBSTC].

[159] Κύρια, βιβλιογραφική αναφορά: [SZOR-ACVRD].

οριζόντιο επίπεδο (κατοπτρικό είδωλο). Ο HPS χαρακτηρίζει αυτές τις «χτυπημένες» εικόνες με την προσθήκη ενός ταυτοτικού, δεκαεξαδικού αλφαριθμητικού (hex string) -DEADBABEh-, στο τέλος της περιοχής της επικεφαλίδας των εν λόγω αρχείων, ώστε να αποφύγει να επαναμολύνει την ίδια εικόνα. Είναι προφανές πως η τροποποιημένη εικόνα δεν έχει κάποιο ιδιαίτερο νόημα χρήσης στη συγκεκριμένη αναπαράσταση, δεν έχει όμως υποστεί και υποβάθμιση της ακεραιότητας των δεδομένων της, πλην ίσως της προσθήκης της ιομορφικής υπογραφής.

3.2 Βέλτιστες πρακτικές

Στο παρόν σκέλος, θα παρουσιάσουμε σε μεγάλο βαθμό ανάλυσης τα νευραλγικά εκείνα χαρακτηριστικά των αυτοαναπαραγόμενων όπλων, που τα καθιστούν ισχυρές απειλές κατά της ασφάλειας, και θα εξετάσουμε τους πλέον επίκαιρους, «ορθόδοξους» και αποτελεσματικούς τρόπους επίτευξης πληροφοριακών επιθέσεων.

3.2.1 Αρχική προσβολή ή εμφύτευση

Βασική, λογική αναγκαιότητα για οποιαδήποτε επίθεση με κακόβουλο, αυτοαναπαραγόμενο λογισμικό είναι η αρχική προσβολή από τον ιό ή η αρχική εμφύτευση κάποιου σκουληκιού σε ένα δίκτυο να γίνεται με τον πλέον καλυμμένο και ανώνυμο τρόπο. Με τον τρόπο αυτό παρέχεται στον επιτιθέμενο μεγαλύτερη εγγύηση μη ανιχνευσιμότητας της πηγής της επίθεσης και άρα ο ίδιος προστατεύεται καλύτερα από κατηγορίες για ευθύνη πρόκλησης ή εμπλοκής σε πληροφοριακή εχθροπραξία[160].

Όσον αφορά τους ιούς, η αρχική έκθεση ενός συστήματος σε κάποιον εκπρόσωπο του είδους μπορεί να επιτευχθεί με οποιουσδήποτε από τους ακόλουθους -ιδιαίτερα οικείους στους χρήστες υπολογιστικών συστημάτων και υπηρεσιών- τρόπους, διατηρώντας παράλληλα μεγάλο βαθμό μη ανιχνευσιμότητας για τον επιτιθέμενο:[161]

1. *Μέσα αποθήκευσης δεδομένων* (οπτικά ή μαγνητικά)· ειδικά οι αφαιρούμενες και μεταφέρσιμες εκδοχές τους μπορούν να συμβάλλουν σημαντικά στην αρχική προσβολή, τη διάδοση και την εξάπλωση μιας ιομορφικής παγίδας, χάρη στην

[160] Κατάρρευση ή υποβάθμιση της απαραίτητης στην ασφάλεια υπευθυνότητας.

[161] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM], [SZOR-ACVRD], [BILAR-IM].

ανταλλαγή και τη μαζική χρησιμοποίησή τους από διαφορετικά περιβάλλοντα και συστήματα πληροφορικής εργασίας.

2. (Δια)δικτυακά *συστήματα διαμοίρασης αρχείων*, με μεγάλες βάσεις χρηστών, όπως:
    a. Οι NFS/CIFS κοινόχρηστοι χώροι αποθήκευσης, σε δικτυακές διαρρυθμίσεις και οργανώσεις χρηστών και συνεργατών τύπου LAN, από όπου μαζί με ό,τι επωφελές μπορούν πολλοί, υποψήφιοι, πρώτοι «εκτελεστές» κακόβουλου κώδικα να «προμηθευτούν» και την πιθανή, μελλοντική τους πανώλη.
    b. Τα δημοφιλή FTP sites, π.χ. εκπαιδευτικών ιδρυμάτων ή εταιρειών πληροφορικής τεχνολογίας, που αποτελούν, συνήθως, αποθήκες ωφέλιμων εφαρμογών, μπορούν να γίνουν στόχος για ανάρτηση κακόβουλου κώδικα, με προφανείς τον σκοπό και την ελπίδα αυτός να διανεμηθεί σε πολλούς χρήστες και συστήματα Η/Υ.
    c. Τα λαοφιλέστατα P2P συστήματα συνεισφοράς και απόκτησης αρχείων και προγραμμάτων, που πέραν της ανταλλαγής επιθυμητών δεδομένων ωφελούν εμφανώς σημαντικά και αποδεδειγμένα τη διακίνηση ιομορφικών και άλλων απειλών κακόβουλου λογισμικού.[162]
3. *Διαδικτυακές μεταφορτώσεις*: Το download προγραμμάτων από τον Παγκόσμιο Ιστό έχει γίνει καθημερινή -και πολλές φορές απαραίτητη- συνήθεια εκατομμυρίων των χρηστών του InterNET σε όλον τον Πλανήτη. Τι γίνεται, όμως, όταν ένα από όλα τα αρχεία που «κατεβάζει» κανείς στον υπολογιστή του «κρύβει» κάποιον λανθάνοντα ιό; Αυτό που συμβαίνει είναι προφανές· αν το κομμάτι αυτό κώδικα καταλήξει για οποιονδήποτε λόγο (λάθος, άγνοια ή επιθυμία χρήστη) στο σύστημα επεξεργασίας (CPU και μνήμη) ενός μηχανήματος, τότε πολύ πιθανόν να πετύχει στην αποστολή της πρώτης αναπαραγωγής του. Συνεπώς, online χρήστες, Διαδίκτυο και μεταφορτώσεις ίσον εξαιρετική ευκαιρία «διανομής» και εξάπλωσης ιομορφικών προγραμμάτων.
4. *Πειρατικό λογισμικό·* ένας αρκετά πιστός και παλαιός «φίλος» πάσης φύσεως κακόβουλων προγραμμάτων, που πολλές φορές εκμεταλλεύεται την επιθυμία των «πελατών» για απόκτηση προγραμμάτων, σε αρκετά χαμηλότερες σε σχέση με το νόμιμο προϊόν τιμές ή πολύ συχνά εντελώς δωρεάν, για να ενσωματώνει στο περιεχόμενο του παρεχόμενου στους χρήστες, πειρατικού «τιμαλφούς» λογής κακόβουλες αποφύσεις.

[162] Πηγή: "Study of Malware in Peer-to-Peer Networks", Andrew Kalafut, Abhinav Acharya and Minaxi Gupta, CSD Indiana University, διαθέσιμο από το δεσμό www.imconf.net/imc-2006/papers/p33-kalafut.pdf.

5. *Ηλεκτρονική αλληλογραφία·* μια από τις πιο διαδεδομένες προσεγγίσεις των συγγραφέων και δραστών μια ιομορφικής ή άλλης μολυντήριας «δύναμης» για την «παράδοση» της στα πρώτα θύματα (π.χ. μέσω τα γνωστής πλέον ανεπίκλητης αλληλογραφίας ή spamming), αλλά ταυτόχρονα και ένα από τα πεδία ανθρώπινης ευπάθειας και «συνδρομής» λόγω συνδυασμών άγνοιας κινδύνου, φιλοπεριέργειας, συνήθειας στη χρήση της συγκεκριμένης τεχνολογίας και ανάγκης για συνεργασία και ανταλλαγή πληροφοριών μέσω αποστολής/λήψης αρχείων δεδομένων.

Εξετάζοντας το έτερο μέλος του αυτοαναπαραγόμενου, κακόβουλου λογισμικού, ανάμεσα στις διάφορες διόδους αρχικής εμφύτευσης σκουληκιών μπορούμε -πέραν των παραπάνω κατεξοχήν ιομορφικών τρόπων προσβολής- να ξεχωρίσουμε ως πλέον ενδεικτικές και συχνά-πυκνά εμφανιζόμενες και τις εξής:[163]

1. *Ασύρματα δίκτυα και hotspots*

Τα εν λόγω δίκτυα και σημεία πρόσβασης είναι συχνά παραμετροποιημένα για δημόσια, μαζική χρήση, με γνώμονα την ελεύθερη πρόσβαση και πολλές φορές διαπιστωμένη την έλλειψη ουσιώδους προστασίας. Σε ένα τέτοιο ανεξέλεγκτο και ανώνυμο περιβάλλον οι κακόβουλοι νιώθουν «παραδεισένια», καθώς μπορούν πολύ εύκολα να «εγχύσουν» πολλαπλά αρχικά στιγμιότυπα με αρκετά ασφαλή για αυτούς τρόπο.

2. *Δίκτυα ζόμπι (botnets)*

Τα δίκτυα αυτά, όπως τα περιγράψαμε σε προηγούμενο σκέλος, είναι στο σύνηθες υπόδειγμα επαρκώς κατανεμημένα και ογκώδη, ενώ τελούν και υπό την πλήρη επικυριαρχία των κακόβουλων οντοτήτων, χωρίς όμως να τους ανήκουν και νομικά τουλάχιστον. Έτσι, οι κακοπροαίρετοι λειτουργοί τους προστατεύονται εξαιρετικά από δράσεις εντοπισμού και απόδοσης ευθυνών για οποιαδήποτε βλάβη έχει πηγή δημιουργίας και αφετηρία μόλυνσης τα συγκεκριμένα συστήματα.

Ειδικά για τα σκουλήκια, που έχουν ένα περισσότερο δικτυοστρεφή χαρακτήρα, τα κανάλια για μια αρκετά ανώνυμη, αρχική εμφύτευση είναι άφθονα και δεν περιορίζονται στα παραπάνω 7, τα οποία έτσι και αλλιώς ισχύουν και μπορούν να χρησιμοποιηθούν κάλλιστα. Σήμερα, υπάρχει μια *πληθώρα διαδεδομένων και κοινά χρησιμοποιούμενων, δικτυακών συστημάτων και υπηρεσιών*, που πέρα από νόμιμους και φυσιολογικούς τρόπους, διαθέτουν σύνολο είτε γνωστών είτε μη επαρκώς τεκμηριωμένων, τεχνικών ευπαθειών και αδυναμιών,

[163] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM].

που επιτρέπουν αρκούντως ανώνυμη πρόσβαση και διάχυση πληροφοριών και δεδομένων διαμέσω τους. Όλα τα συστήματα και οι υπηρεσίες αυτές είναι εν δυνάμει οδοί εμφύτευσης και κανάλια διάχυσης νέων σκουληκιών.

3.2.2 Αναζήτηση νέων θυμάτων

Η αναζήτηση νέων θυμάτων, τόσο στην περίπτωση του ιομορφικού λογισμικού, όσο και σε αυτήν των σκουληκιών, έχει πάντοτε ως γνώμονα την *εύρεση ενός συνόλου οντοτήτων απόλυτα ευπαθών ή πιθανώς ευπρόσβλητων από το διάνυσμα προσβολής* του εκάστοτε ιού ή σκουληκιού.

Ιοί

Η αναζήτηση νέων θυμάτων για το ιομορφικό λογισμικό συντελείται με *ρουτίνες εντοπισμού (search functions) νέων ξενιστών για τον τυχόντα ενεργό ιό*. Οι ρουτίνες αυτές είναι συνήθως τμήματα αρκετά περίτεχνου κώδικα, επαρκώς ευδιάκριτα από το υπόλοιπο σώμα του ιού, που σκοπό έχουν κάθε φορά που εκτελούνται να προσδιορίζουν ένα ή περισσότερα, κατάλληλα, νέα θύματα για τον εν λόγω ιό, ώστε στη συνέχεια και αυτά να εμποτίζονται με τη σειρά τους με το ιομορφικό, «γενετικό υλικό». Μια ρουτίνα εντοπισμού ξενιστών χαρακτηρίζεται κυρίως από 2 παράγοντες· από *το είδος του εκάστοτε επιθυμητού ξενιστή*, κατά πρώτο λόγο, και στη συνέχεια από την *αναγκαιότητα ανίχνευσης ενός ήδη μολυσμένου (όχι απαραίτητα μόνο από τον τρέχοντα ιό) ξενιστή*.

Ένας ξενιστής ιομορφικού λογισμικού μπορεί να έχει μία από τις εξής δύο, κεντρικές μορφές:

A) Αρχείο δεδομένων, που περιέχει κάποιας μορφής «εκτελέσιμο»[164] κώδικα (Εκτελέσιμο Πρόγραμμα, Πηγαίος ή Ενδιάμεσος Κώδικας Γλώσσας Προγραμματισμού).

B) Τομέας εκκίνησης δίσκου (Πίνακες FAT, Κύριος Τομέας εκκίνησης-MBR).

Όταν ο ιός στηρίζεται σε αρχεία δεδομένων φέροντα κάποιας μορφής «εκτελέσιμο» κώδικα μιλάμε για *παρασιτικούς ιούς (parasitic viruses)*, ενώ όταν μολύνει τους τομείς εκκίνησης δίσκων έχουμε να κάνουμε με *ιούς τομέα εκκίνησης (boot-sector viruses)*. Ένα τρίτο είδος

[164] Την έννοια του κάποιας μορφής «εκτελέσιμου» κώδικα, χρήσιμου σε ιομορφική προσβολή, τη διασαφηνίσαμε στο Κεφάλαιο 2 (2.4).

προκύπτει από ιούς που χρησιμοποιούν συνδυασμό προσβολής και των δύο τύπων ξενιστή, οπότε αναφερόμαστε σε αυτούς ως *πολυμερείς (multi-partite viruses)*.[165]

Κάθε ιός ανήκει απαραίτητα σε μία από τις τρεις αυτές κατηγορίες και πρέπει να διαθέτει και την αντίστοιχη ρουτίνα εντοπισμού ξενιστών, ανάλογα με την κατηγοριοποίηση αυτή. Η διαδικασία αναζήτησης των κατάλληλων ξενιστών γίνεται ακόμη πιο συγκεκριμένη με τη *διευκρίνιση καθοριστικών παραμέτρων*, όπως:[166]

- Η αρχιτεκτονική της CPU.
- Το είδος του Λ/Σ και η ειδική έκδοσή του.
- Οι στοχευόμενοι τύποι αρχείων δεδομένων.
- Το μέγεθος του ιομορφικού κώδικα.
- Η ανάγκη παραμονής στη μνήμη.

Έτσι, ένας ιός που μολύνει π.χ. EXE αρχεία θα πρέπει να αναζητά αυτού του είδους τα αρχεία (με αυτήν την κατάληξη ή με τα χαρακτηριστικά πρώτα 2 bytes να ναι MZ) με κάποιο ορισμένο βάθος αναζήτησης (τρέχων κατάλογος, τρέχουσα κατάτμηση, όλος ο δίσκος, μνήμη τυχαίας προσπέλασης κτλ), ενώ ένας boot sector ιός θα πρέπει να ελέγχει το σύστημα σε κάθε εκκίνηση δίσκων για τυχόν προσθήκες/αλλαγές στους τομείς εκκίνησης, στους FATs[167] και στο MasterBootRecord ή ακόμα-ακόμα για πιθανή προσθήκη νέου εγγράψιμου (αφαιρέσιμου ή μη) δίσκου (όπως USB sticks, floppy disks, external hotplugged disks), ώστε να βρει και να προσβάλλει καινούριους ξενιστές.

Η συνθήκη μη επαναμόλυνσης αρχείων ή τομέων δίσκων είναι πολύ σημαντική και συνήθως τηρείται από την πλειοψηφία του ιομορφικού λογισμικού.[168] Αυτή προστατεύει τους ξενιστές από μια πιθανή αχρήστευση όποιου επωφελή κώδικα φέρουν, αλλά ακόμα και του ίδιου του ιομορφικού κώδικα που ήδη έχουν, ενώ παράλληλα εξασφαλίζει στον ιό την απαραίτητη, εναλλακτική λύση σε περιττές -και ενδεχομένως επικίνδυνες για την επιβίωσή του- δράσεις. Κάποιες φορές μάλιστα είναι επιθυμητό να εντοπίζονται και οι μολύνσεις ενός ξενιστή από

---

[165] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM], [SZOR-ACVRD], [LUDWIG-GBBCV], [TANENBAUM-MOS9], [JOHANSSON-CVTEALF], [SYMANTEC-UVB32BOE].

[166] Κύρια, βιβλιογραφική αναφορά: [SZOR-ACVRD].

[167] Ο πίνακας κατανομής αρχείων (File Allocation Table FAT) είναι ένας κατάλογος εγγραφών που δείχνουν σε κάθε ένα από τα ίσα συνεχόμενα μπλοκ αποθηκευτικού χώρου (cluster) σε κάθε διαμέρισμα (partition) στο δίσκο. Χρησιμοποιείται από τα συστήματα αρχειοθέτησης της οικογένειας FAT της Microsoft για να φυλλάσσει και να υποδεικνύει την χωρική κατανομή των αρχείων στα διαμερίσματα αυτού του τύπου.

[168] Κύρια, βιβλιογραφική αναφορά: [SZOR-ACVRD], [LUDWIG-GBBCV].

διαφορετικούς ιούς (πολλαπλή μόλυνση), ώστε αυτός να μην προσβληθεί από τον τρέχοντα ιό ή να προσβληθεί, αλλά με κατάλληλο τρόπο (αφαίρεση άλλων μολύνσεων, συνύπαρξη με και προσαρμογή π.χ. μεγέθους ή/και σημείων εισόδου των διαφόρων ιών).

Μια ρουτίνα αναζήτησης νέων ξενιστών πρέπει, λοιπόν, με κάποιο σαφή τρόπο να αντιλαμβάνεται την ύπαρξη ιομορφικού κώδικα σε υποψήφιους ξενιστές και να απομονώνει τους «καθαρούς», ώστε να δίνει τη δυνατότητα αξιόπιστης και ελεγχόμενης μόλυνσης (πρώτης, πολλαπλής ή επανα- μόλυνσης, αν και εφόσον είναι επιθυμητό). Συνήθως, τα υπό εξέταση αρχεία ή τμήματα τομέων δίσκων ανιχνεύονται για την *παρουσία κάποιου σημαδιού μόλυνσης (infection marker)*[169], που υποδηλώνει την παρουσία ενός ιού. Τα σημάδια μόλυνσης αυτά είναι χαρακτηριστικά, ταυτοτικά στοιχεία για τον κάθε ιό. Πολλές φορές τυχαίνει αυτή η σχετική πληροφορία μόλυνσης συγκεκριμένων αρχείων ή τομέων δίσκων να ξεπερνά τα στενά όρια τους ή να μην περικλείεται εξ ολοκλήρου εντός τους, αλλά να βρίσκεται διάσπαρτη σε μνήμη ή/και δίσκο ενός υπολογιστικού συστήματος, αλλά ακόμα και να προέρχεται από το εξωτερικό του προσβληθέντος συστήματος. Όπως και να 'χει, όμως, *ένας ιός μπορεί και πρέπει να γνωρίζει πώς να εντοπίζει τουλάχιστον τον εαυτό του (self-detection)*[170] και ειδικότερα να επιβεβαιώνει την ύπαρξη του προσφιλή κώδικά του στον δείνα ξενιστή, με τη χρήση των ιδιαίτερων σημαδιών μόλυνσης που τον χαρακτηρίζουν. Ο εντοπισμός σε πιθανούς ξενιστές έτερων μολύνσεων από άλλους ιούς μπορεί να γίνεται με παρόμοιο τρόπο (πρότερη γνώση σημαδιών μόλυνσης των ιών που ενδιαφέρουν) ή με άλλες πιο ευριστικές μεθόδους, στα πλαίσια του ευρύτερου κώδικα αναζήτησης ξενιστών ενός ιού.

Ανακεφαλαιώνοντας και συνοψίζοντας, η επιτυχημένη αναζήτηση για νέα θύματα στους ιούς προϋποθέτει την παρουσία ειδικών τμημάτων κώδικα, που απασχολούνται με τον εντοπισμό και προσδιορισμό των κατάλληλων για τον κάθε ιό ξενιστών, ανάλογα με το ιδιαίτερο είδος και τα χαρακτηριστικά που στοχεύονται και με βάση συγκεκριμένους περιορισμούς, σχετικά με την ύπαρξη ή μη κάποιας μορφής ιομορφικού κώδικα στον υποψήφιο ξενιστή.

Σκουλήκια

Ένα σκουλήκι πρέπει να προσδιορίσει επόμενους κόμβους, που είναι πιθανόν να μπορέσει να προσβάλλει, ώστε να εξαπλωθεί περαιτέρω. Σε καθέναν από τους υποψήφιους κόμβους

[169] Το ίδιο αυτό το σημάδι βέβαια που τόσο προστατεύει από τα πιθανά προβλήματα της επαναμόλυνσης, αν και εφόσον δεν είναι μέρος επιτηδευμένου σχεδίου, αλλά αφορά την άκομψη εισαγωγή πληροφοριών αναγνώρισης εντός του σώματος του ξενιστή οδηγεί τελικά αργά ή γρήγορα σε μια πρώτη ταυτοποίηση του είδους του από τα συστήματα και τους αναλυτές ασφάλειας. Σε μια τέτοια περίπτωση, το σημάδι μόλυνσης μπορεί να και συνήθως περιλαμβάνεται και στην υπογραφή ανίχνευσης ενός ιού, αλλά αυτό εξαρτάται και από τη μοναδικότητα και την ποικιλομορφία του, για κάθε ιομορφική περίπτωση.

[170] Ο αυτοεντοπισμός του κακόβουλου κώδικα στη μνήμη ή εντός ξενιστή είναι χρήσιμη διεργασία ή ενδεχομένως απαραίτητη προϋπόθεση και σε άλλες πλην της επαναμόλυνσης καταστάσεις, όπως π.χ. για την αποφυγή διπλής «φόρτωσης» ενός TSR στη μνήμη ή για πολυμορφικού/μεταμορφικού τύπου μόλυνση (βλέπε σχετικά και 3.2.4).

εξάπλωσης θα αποσταλεί και ένα αντίγραφο του σκουληκιού με την ελπίδα η κεφαλή του να είναι ικανή να «τρυπήσει» το παρευρισκόμενο σύστημα και να προσβάλλει το θύμα. Για τη διάδοση του είναι ουσιαστικά ευκολότερο για ένα σκουλήκι να βασιστεί σε μια διεύθυνση IP για να βρει τον εκάστοτε στόχο του από το να υποθέσει σωστά το αντίστοιχο DNS όνομα ενός μηχανήματος-στόχου.[171] Ένα σκουλήκι που ψάχνει μηχανήματα για να μολύνει λέγεται ότι *ανιχνεύει για υποψήφια θύματα*. Υπάρχουν πέντε βασικές στρατηγικές ανίχνευσης, με διαφορετικές και ξεκάθαρα οριοθετημένες προτεραιότητες:

1. **Σειριακή ανίχνευση (Sequential scanning)**[172]

   Το σκουλήκι δοκιμάζει κάθε μια από τις διαφορετικές διευθύνσεις ολόκληρων ταξινομημένων μπλοκ IP διευθύνσεων. Σε όλες τις διευθύνσεις ενός ανιχνευόμενου μπλοκ θα καταλήξει και μια ρέπλικα του σκουληκιού για να δοκιμαστεί η όποια αποτελεσματικότητα της κεφαλής της.

   Προφανώς μια τέτοια μέθοδος ανίχνευσης *υπέρ του δέοντος εξαντλητική και παράγει, συνήθως, σημαντική, ανεπιθύμητη κίνηση* στο δίκτυο, ενώ *οδηγεί και σε πιθανές επαναμολύνσεις,* με τις όποιες, απρόβλεπτες συνέπειες που συνήθως τις συνοδεύουν. Ακόμη, η ταχύτητα διάδοσης ενός σκουληκιού που την εφαρμόζει δεν μπορεί παρά να είναι περιορισμένη, σε σχέση με πιο προηγμένα μοντέλα αναζήτησης θυμάτων, όπως είναι τα επόμενα στην ανάλυση.

2. **Τυχαιώδης ανίχνευση (Random scanning)**[173]

   Ένα σκουλήκι μπορεί να επιλέξει έναν στόχο τυχαία εκλέγοντας μια τιμή για τη διεύθυνση IP από ένα σύνολο τιμών. Αυτό γίνεται εκτεταμένα, παραδείγματος χάριν, από το σκουλήκι Code Red I. Διαλέγοντας μια διεύθυνση IP, με αυτόν τον τρόπο, μπορεί κανείς να καταλήξει σε έναν στόχο κυριολεκτικά οπουδήποτε στον κόσμο, ανάλογα με το πεδίο τιμών των διευθύνσεων, που χρησιμοποιεί.

   Μια επίθεση σκουληκιού, που εφαρμόζει τυχαιώδη ανίχνευση, αναμένεται να *εμφανίζει ετερόκλητα αποτελέσματα, όσον αφορά τόσο την ταχύτητα διάδοσης, όσο και τη διεύρυνση και τη διασπορά της*. Πάντως, αν ένα σκουλήκι διαθέτει

---

[171] Η ανίχνευση με βάση DNS ονόματα θεωρείται αντιπαραγωγική, καθώς δεν μπορεί να αυτοματοποιηθεί με μαθηματικό τρόπο, τουλάχιστον όσον αφορά μια τυχαιώδη ανίχνευση στο Διαδίκτυο ή σε άλλα ευρείας κλίμακας δίκτυα. Ίσως έχει νόημα για περιβάλλοντα τοπικών δικτύων, όπου παρέχονται δυνατότητες επισκόπησης των διασυνδεδεμένων κόμβων (π.χ. μέσω NetBIOS), αλλά και αυτό είναι αμφισβητήσιμο και εμφανώς-ουσιωδώς πολυπλοκότερο από μια ανίχνευση με χρήση IPs.

[172] Κύρια, βιβλιογραφική αναφορά: [WEAVER_PAXSON-TCW].

[173] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM], [WEAVER_PAXSON-TCW].

αυτοματοποιημένο μηχανισμό ενεργοποίησης (η κεφαλή του, δηλαδή, δεν απαιτεί ανθρώπινη δράση) η μέθοδος αυτή μπορεί να αποδειχθεί στην πράξη ιδιαίτερα επιτυχημένη και σε ταχύτητα διάδοσης και σε διασπορά της απειλής. Στην περίπτωση ανάγκης παρέμβασης του ανθρώπου, βέβαια, τα αποτελέσματα παραμένουν αδιευκρίνιστα και χαοτικά.

Η τυχαιώδης ανίχνευση *μπορεί να δοκιμάζει άσκοπα τους ίδιους στόχους είτε πετυχαίνοντας είτε αποτυχαίνοντας στην κατάληψή τους*. Ένα σημαντικό πρόβλημα, που πιθανώς προκύπτει από μια τέτοια κατάσταση -πέρα από την όποια καθυστέρηση στη διάδοση-, είναι και η επαναμόλυνση ορισμένων στόχων, που τις περισσότερες φορές δημιουργεί *περίσσεια ανεπιθύμητης κίνησης*, χωρίς να εξασφαλίζει σε αντάλλαγμα κάτι ιδιαίτερα ωφέλιμο για το σκουλήκι. Το αντίθετο μάλιστα· μπορεί να οδηγήσει σε αποκάλυψη του σκουληκιού σε συστήματα ασφάλειας, όπως συνέβη στην περίπτωση του Morris Worm[174].

Όπως και να ’χει, αν και *συνήθως πιο αποδοτική από μια σειριακή ανίχνευση*, δεν παύει να είναι μια προσέγγιση, που επιδέχεται πολλών βελτιστοποιήσεων στο απρόβλεπτο της φύσης της.

3. Τοπική ανίχνευση (Localized scanning)[175]

Μια τυχαία ανίχνευση είναι καλή για μια ευρεία διανομή ενός σκουληκιού, αλλά δεν παύει να είναι μια προσέγγιση λάθους-και-επανάληψης (trial and error method) για σκουλήκια που εκμεταλλεύονται τις τεχνικές ευπάθειες, για να διαδοθούν με τρόπο αυτόματο. Είναι πολύ πιο λογικό και ρεαλιστικό οι υπολογιστές στο ίδιο δίκτυο, στην ίδια διοικητική περιοχή, να έχουν παραμετροποιηθεί και να συντονίζονται με παρόμοιο τρόπο και να διαθέτουν ίδιες ή παραπλήσιες ή ομοιόμορφες πολιτικές ασφάλειας. Παραδείγματος χάριν, εάν ένας Η/Υ με Windows σε ένα δίκτυο είναι ευάλωτος σε επιθέσεις υπερχείλισης, οι πιθανότητες είναι καλές και για μια άλλη Windows μηχανή στο ίδιο δίκτυο να είναι επίσης. Η τοπική ανίχνευση προσπαθεί να εκμεταλλευθεί αυτό ακριβώς το γεγονός για να βελτιστοποιήσει την ταχύτητα διάδοσης ενός σκουληκιού, τουλάχιστον στον ορίζοντα του τοπικού του δικτύου. Οι *στόχοι επιλέγονται πάλι τυχαία, αλλά με μια ευδιάκριτα μεγαλύτερη πόλωση και*

---

[174] Το σκουλήκι του Robert Morris Jr. δεν επέλεγε τυχαία τα θύματά του (αλλά τοπολογικά, όπως θα πούμε παρακάτω), αλλά αναφέρεται εδώ ως ένα κλασσικό παράδειγμα σκουληκιού που δεν τηρούσε κάποια πολιτική μη επαναμόλυνσης (όπως συμβαίνει για την πλειοψηφία των σκουληκιών που πραγματοποιούν τυχαιώδη ανίχνευση στόχων)· το αντίθετο μάλιστα, προέβαινε και σε πολλαπλή μόλυνση στους κόμβους για να σιγουρεύει την παρουσία του, με αποτέλεσμα να «προδίδει» την παρουσία του.

[175] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM], [WEAVER_PAXSON-TCW].

βαρύτητα για τις τοπικές μηχανές, έτσι ώστε η εκλογή ενός τοπικού μηχανήματος να είναι πλέον πιθανή, αν όχι το επικρατέστερο ενδεχόμενο, σε σύγκριση με τις υπόλοιπες εναλλακτικές. Παραδείγματος χάριν, το σκουλήκι Code Red II επιλέγει τις IP διευθύνσεις των στόχων κατ' αυτό τον τρόπο:

Probability	*Target Selection*
1/8	All four bytes randomly chosen
3/8	Only last two bytes randomly chosen
4/8	Last three bytes randomly chosen

Σχήμα 10: Τοπική ανίχνευση στόχων, με πιθανοτικό τρόπο

Αν και η μέθοδος αυτή μπορεί να είναι *ελαφρώς υποδεέστερη άλλων*, ιδίως αν πρόκειται για διάδοση σε κλίμακα Διαδικτύου, *επιτρέπει στα σκουλήκια να καταφέρουν, εκμεταλλευόμενα π.χ. μια απλή «τρύπα» (sic δικτυακή ευπάθεια) σε κάποιο σύστημα αντιπυρικής προστασίας, να ανιχνεύσουν δυνητικά ολόκληρο το τοπικό δίκτυο που αυτό προστατεύει*. Το γεγονός αυτό αποτελεί τη μεγάλη δύναμη της τοπικής ανίχνευσης, που μπορεί να αποτελέσει σε πολλές περιπτώσεις μια σημαντική προσθήκη-βελτιστοποίηση της προσέγγισης τυχαιώδους ανίχνευσης στόχων.

4. Ανίχνευση με μεταθέσεις (Permutation scanning)[176]

Εάν ένα σκουλήκι είναι σε θέση να διαπιστώνει εάν ένας υποψήφιος στόχος είναι ή όχι ήδη μολυσμένος, τότε είναι δυνατόν να χρησιμοποιηθούν ιδιαίτερα αποτελεσματικοί τρόποι αποφυγής κάποιας ανεπιθύμητης, δικτυακής κίνησης ή συμφόρησης με ό,τι και αν αυτή συνεπάγεται. Ένας από τους τρόπους αυτούς είναι και η ανίχνευση με μεταθέσεις που λαμβάνει χώρα, όταν τα διάφορα στιγμιότυπα ενός σκουληκιού συμβαίνει να μοιράζονται μια κοινή μετάθεση του χώρου των IP διευθύνσεων, μια ψευδοτυχαία ακολουθία, που μπορεί να απαρτίζεται από οποιεσδήποτε από τις 2^{32} πιθανές τιμές IP διευθύνσεων.[177] Σε κάθε νέο στιγμιότυπο δίνεται μια θέση στην ακολουθία αυτή από την οποία και εκκινεί τη διαδικασία προσβολής και το σκουλήκι αυτό συνεχίζει να εργάζεται διαμέσω της ακολουθίας

[176] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM], [BALEPIN-SCDC].

[177] Με τον ερχομό του IPv6 το πεδίο τιμών θα γίνει 2^{128}, ένα νούμερο πολύ εντυπωσιακό, που θα αυξήσει στατιστικά τη διασπορά της ψευδοτυχαίας ακολουθίας του αλγορίθμου μεταθέσεων.

από το σημείο αυτό. Όταν εντοπίζεται μια μηχανή που είναι ήδη μολυσμένη, το σκουλήκι επιλέγει τυχαία ένα νέο σημείο στην ακολουθία και την ξαναδιατρέχει.

Το παραπάνω μοντέλο δίνει στα σκουλήκια έναν *απλό μηχανισμό για κατανεμημένο συντονισμό, χωρίς ανάγκη για οποιαδήποτε, πρόσθετη δικτυακή επιβάρυνση* λόγω επικοινωνίας μεταξύ των διαφορετικών στιγμιοτύπων δοθέντος σκουληκιού. Η ανίχνευση με μεταθέσεις επιτρέπει στα σκουλήκια να χρησιμοποιήσουν τον συγκεκριμένο, κατανεμημένο συντονισμό, για να *ανιχνεύουν αποτελεσματικότερα το δίκτυο και για να καθορίζουν πότε ο μεγαλύτερος όγκος του είναι «καθαροί» ή μολυσμένοι κόμβοι*.

Επιπρόσθετα, αυτός ο μηχανισμός συντονισμού *μπορεί να χρησιμοποιηθεί από το σκουλήκια και για να ανιχνεύουν με τρόπο ευριστικό τον κορεσμό (saturation)*[178] στην διαδικασία διάδοσής τους. Εάν κάποιο στιγμιότυπο ενός σκουληκιού βρίσκει συνεχώς μολυσμένα τα διάφορα, υποψήφια θύματα, παρά την επαναλαμβανόμενη τυχαία αλλαγή θέσης του στην ακολουθία μετάθεσης, αυτό μπορεί να χρησιμεύσει ως ένας δείκτης ότι οι περισσότερες από τις τρωτές μηχανές έχουν μολυνθεί και άρα ότι το σημείο κορεσμού είναι πλέον κοντά. Το σημείο κορεσμού με τη σειρά του μπορεί να επισημάνει τον κατάλληλο χρόνο για να απελευθερωθεί ένα «ωφέλιμο» φορτίο, επειδή υπάρχουν ελάχιστα περισσότερο που μπορεί το σκουλήκι να κάνει από άποψη διάδοσης, ενώ παράλληλα αυξάνει ολοένα η πιθανότητα του να γίνει αντιληπτό με τα όποια αντίμετρα στο σκουλήκι αναμφίβολα να έρχονται πιο κοντά.

5. Ανίχνευση με τη βοήθεια λίστας στόχων (Hit-list scanning)

a. Προ-παρασκευασμένες λίστες[179]

Ένα επιτιθέμενο σκουλήκι *θα μπορούσε να λάβει έναν κατάλογο των στόχων του εκ των προτέρων* (εντός κώδικα ή όπως είναι ο αντίστοιχος αγγλικός όρος hard-coded), *δημιουργώντας μια λίστα χτυπήματος (hit-list) πιθανών θυμάτων*, όπως π.χ. κόμβων γνωστών για την ευπάθειά τους σε μια τεχνική ατέλεια, που το σκουλήκι είναι προγραμματισμένο να εκμεταλλεύεται για να διαδοθεί. Η λίστα αυτή *δε χρειάζεται να είναι 100% ακριβής*, δεδομένου ότι θα χρησιμοποιηθεί μόνο ως αφετηρία, και *δεν είναι απαραίτητο να περιέχει μεγάλο αριθμό IP* διευθύνσεων.

---

[178] Ο κορεσμός είναι εκείνο το στάδιο της ωρίμανσης στη διάδοση και εξάπλωση ενός κακόβουλου, κινητικού κώδικα (malicious, mobile code, MMC), όπου η πλειοψηφία των στόχων έχουν καταληφθεί και μολυνθεί με στιγμιότυπα ή υποστάσεις του.

[179] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM], [WEAVER_PAXSON-TCW].

Οι προπαρασκευασμένες λίστες είναι *χρήσιμες για 2 κυρίως λόγους*:

- **Αποφυγή άσκοπης κίνησης ή συμφόρησης**: Μια λίστα χτυπήματος μπορεί εύκολα να χρησιμοποιηθεί για να *αποτρέπει στιγμιότυπα ενός σκουληκιού από τη στόχευση των ίδιων μηχανημάτων*.
- **Επιτάχυνση αρχικής εξάπλωσης**: Με την παροχή ενός καταλόγου γνωστών στόχων, *αποφεύγεται η αργή διάδοση από προσεγγίσεις λάθους-και-επανάληψης*[180] και *δίνεται η δυνατότητα για τάχιστη εξάπλωση*, που σε συνδυασμό με κατάλληλη κεφαλή μπορεί να οδηγήσει σε ραγδαίες μολύνσεις, όπως αυτές που προκαλούν τα λεγόμενα σκουλήκια-αστραπές (flash worms) ή τα Warhol worms[181].

Το μεγαλύτερο εμπόδιο στην κατηγορία αυτή σκουληκιών είναι η προσπάθεια να δημιουργηθεί ο εν λόγω κατάλογος. Για έναν μικρό κατάλογο στόχων, δημόσιες πηγές είναι ευρέως διαθέσιμες και ενδεχόμενα, ανοικτά σημεία πρόσβασης μπορούν να χρησιμοποιηθούν για να εκτελέσουν μικρής κλίμακας ανιχνεύσεις. Περιεκτικότερες λίστες απαιτούν συνήθως πολύ περισσότερη προσπάθεια: επί παραδείγματι είτε μια κατανεμημένη ανίχνευση είτε την πλήρη υπονόμευση μιας κατάλληλης βάσης δεδομένων προερχόμενης από τηλεπικοινωνιακούς παρόχους διαδικτυακών υπηρεσιών. *Ένα απόλυτα βασισμένο σε λίστα χτυπήματος σκουλήκι δεν έχει ακόμα εντοπιστεί να δρα ανεξέλεγκτο (in the wild)*, αλλά μια τέτοια πιθανότητα δε θα πρέπει -σύμφωνα με ειδήμονες του χώρου- να αποκλείεται για το εγγύς μέλλον.

b. Εξωτερικά παραγόμενες λίστες[182]

Μια εξωτερικά παραγόμενη λίστα στόχων διατηρείται συνήθως από έναν χωριστό, υπεύθυνο εξυπηρετητή, που έχει τη λογική *ενός μεταεξυπηρετητή μιας*

[180] Όπως η τοπική ανίχνευση, που συζητήθηκε παραπάνω.

[181] Τα σκουλήκια τύπου Warhol δανείζονται το όνομά τους από την περίφημη φράση για τα 15' λεπτά δημοσιότητας του Andy Warhol, θέλοντας να επιδείξουν την ταχύτητα στην επιμολυντική τους διάδοση. Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM], [BALEPIN-SCDC].

[182] Κύρια, βιβλιογραφική αναφορά: [WEAVER_PAXSON-TCW].

υπηρεσίας αναζήτησης και εύρεσης αντιστοιχιών (matchmaking metaserver) ή ενός καταλογοεξυπηρετητή μιας υπηρεσίας P2P (indexing server)[183].

Ένα metaserver σκουλήκι ρωτά τον metaserver προκειμένου να ενημερωθεί για τους νέους του στόχους. Ένα τέτοιο *σκουλήκι θα μπορούσε να διαδοθεί ταχύτατα* π.χ. μέσω ενός παιχνιδιού μαζικής διαδικτυακής χρήσης-MMO (όπως το HalfLife ή το WarCraft ή άλλα)[184], ακόμα και όταν ο αρχικός πληθυσμός του είναι σχετικά μικρός ή τα πιθανά ευπαθή μηχανήματα λίγα, δεδομένου ότι υπάρχουν αρκετοί metaservers που μπορούν να ρωτηθούν για να ανακαλυφθούν γρήγορα οι όποιοι τρωτοί κόμβοι. Αυτή η τεχνική θα μπορούσε επίσης να χρησιμοποιηθεί για να επιταχύνει την επίθεση κάποιου σκουληκιού σε εξυπηρετητές Ιστού, παραδείγματος χάριν με τη χρησιμοποίηση μιας μηχανής αναζήτησης ως metaserver, προκειμένου να βρεθούν επόμενα θύματα-εξυπηρετητές. Μάλιστα, το σκουλήκι με την κωδική ονομασία Santy[185], συγκεκριμένα, εκμεταλλεύτηκε μια τεχνική αδυναμία και ένα σοβαρό λάθος σχεδίασης σε λογισμικό προσανατολισμένο στον Παγκόσμιο Ιστό και χρησιμοποίησε επιτυχώς την Google για την αναζήτηση των επόμενων του στόχων.

Δεν έχει διαπιστωθεί ποτέ κάποιο metaserver σκουλήκι εκτός ελέγχου (in the wild), αλλά ο κίνδυνος αναδεικνύεται σημαντικότατος και αυτό οφείλεται εν μέρει στη μεγάλη ταχύτητα διάδοσης που ένα τέτοιο σκουλήκι θα μπορούσε να πετύχει. Ένας περιοριστικός παράγοντας της επικίνδυνης αυτής απειλής είναι ότι η λογική της ερώτησης στον metaserver είναι οριζόμενη από την εκάστοτε εφαρμογή και ο τρόπος που γίνεται κάθε φορά *εξαρτάται τα μέγιστα από την τρέχουσα εφαρμογή (technology-dependent)*[186].

c. Εσωτερικά παραγόμενες λίστες – Τοπολογική ανίχνευση[187]

Στην περίπτωση αυτή το σκουλήκι ακολουθεί την *τοπολογία της πληροφορίας* που πιθανόν βρίσκει εντός συστημάτων που μόλις υπονόμευσε. Η τοπολογία αυτή και η αντίστοιχη πληροφόρηση που ένα σκουλήκι αντλεί κάθε φορά από

---

[183] Κάθε meta- ή indexing server κρατά έναν κατάλογο όλων των κεντρικών εξυπηρετητών, που είναι σε κάθε δεδομένη στιγμή ενεργοί. Παραδείγματος χάριν, η υπηρεσία Gamespy διατηρεί έναν τέτοιο κατάλογο κεντρικών εξυπηρετητών για πληθώρα διαφορετικών παιχνιδιών.

[184] Των οποίων ο ρυθμός χρήσης και διείσδυσης κυμαίνεται πάντοτε σε πολύ υψηλά επίπεδα, παρέχοντας έτσι μια ιδανική βάση μηχανημάτων για μόλυνση.

[185] Πηγή: Διαδίκτυο, ιστοχώρος της εταιρείας παροχής εγνωσμένης αξίας και αποδοχής λύσεων προστασίας από το κακόβουλο λογισμικό Symantec, http://www.symantec.com/security_response/writeup.jsp?docid=2004-122109-4444-99.

[186] Κύρια, βιβλιογραφική αναφορά: [WEAVER_PAXSON-TCW].

[187] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM], [WEAVER_PAXSON-TCW], [BALEPIN-SCDC].

τους κόμβους των θυμάτων *μπορεί ή όχι να συμπίπτει με μια φυσική δικτυακή τοπολογία ή μπορεί να αφορά τα λεγόμενα κοινωνικά δίκτυα (social nets),* όπως τα δίκτυα ηλεκτρονικής αλληλογραφίας ή διαμοιρασμού αρχείων, αλλά και τα δίκτυα ομότιμων οντοτήτων (P2P nets). Έτσι, σκουλήκια ηλεκτρονικής αλληλογραφίας μπορούν να αποστέλλουν στιγμιότυπά τους σε λογαριασμούς αλληλογραφίας που θηρεύουν από ένα προσβεβλημένο μηχάνημα και σκουλήκια δικτύων αυτόματων μηνυμάτων (IM worms), ομοίως, στη λίστα των «φίλων» του θύματος χρήστη κάποιας IM υπηρεσίας.

Η τοπολογική ανίχνευση είναι *ιδιαίτερα χρήσιμη στην περίπτωση διάδοσης σε μεγάλο, αλλά «αραιοκατοικημένο» από υποψήφιες μηχανές, χώρο IP διευθύνσεων*. Κλασσικό παράδειγμα τοπολογικού σκουληκιού είναι το Morris Worm, που χρησιμοποίησε αυτή τη μέθοδο λόγω του μικρού σε σχέση με το χώρο των δυνατών IP διευθύνσεων αριθμού μηχανημάτων στο Internet του 1988. Αν, αντιθέτως, είχε για παράδειγμα χρησιμοποιηθεί η τυχαιώδης μέθοδος ανίχνευσης, η άσκοπη κατανάλωση πόρων για τον εντοπισμό των μηχανημάτων αυτών με την περιγραφόμενη αναλογία θα ήταν πραγματικά πολύ μεγάλη.

Εν γένει, *τα τοπολογικά σκουλήκια μπορούν να είναι πολύ γρήγορα*. Εάν οι τρωτές μηχανές αναπαρίστανται ως κόμβοι σε έναν κατευθυνόμενο γράφο G={V,E}, με τις ακμές να αντιπροσωπεύουν τις πληροφορίες για άλλες μηχανές, ο χρόνος που χρειάζεται ένα σκουλήκι για να μολύνει το σύνολο των κόμβων είναι μια συνάρτηση των ελάχιστων διαδρομών (shortest paths) από το αρχικό σημείο της προσβολής. Για ιδιαίτερα συνδεσιστρεφείς εφαρμογές, τέτοια σκουλήκια μπορούν να είναι απίστευτα γρήγορα.

Ένα ακόμη σημαντικό χαρακτηριστικό στην τοπολογική ανίχνευση είναι η ανταλλαγή γνώσης. Με τη διαβίβαση γνωστών, τοπολογικών πληροφοριών από ένα στιγμιότυπο σε άλλα δεν κερδίζει δυνητικά κανείς μόνο σε ταχύτητα διάδοσης, αλλά μια τέτοια δυνατότητα αποτελεί εξαιρετικής σημασίας συνδρομή για τα σκουλήκια που προσπαθούν να παρακάμψουν τυχόν άμυνες[188].

Τέλος, *αν και τα τοπολογικά σκουλήκια μπορούν να εμφανίζονται ως μια ολική ανωμαλία συμπεριφοράς ή κίνησης, η εκάστοτε τοπική κυκλοφορία μπορεί να παρουσιάζεται εντελώς κανονική*. Κάθε μολυσμένο μηχάνημα χρειάζεται να έρθει σε επαφή με μερικές μόνο, άλλες μηχανές για να ενισχύσει την εξάπλωση. Δεδομένου ότι αυτές θα προκύψουν από αναζήτηση και ανάλυση φυσικών ή κοινωνικών δικτύων στα οποία είναι μέλος ο εκτεθειμένος σταθμός, τα νέα

[188] Κύρια, βιβλιογραφική αναφορά: [WEAVER_PAXSON-TCW].

θύματα θα είναι πιθανότατα γνωστοί και απολύτως κανονικοί προορισμοί για επικοινωνία.

Συνεπώς, μια ουσιώδης αξιοποίηση της όποιας πρόσθετης πληροφορίας από προσβεβλημένους κόμβους, για τυχόν δικτυώματα στα οποία αυτοί μετέχουν και που μπορούν να λειτουργήσουν ως κανάλια διάδοσης για κάποιο σκουλήκι, αποδεικνύεται εξαιρετικά χρήσιμη για μια αποτελεσματική ανίχνευση επόμενων στόχων.

6. Παθητική ανίχνευση[189]

Ένα σκουλήκι παθητικής ανίχνευσης δεν ανιχνεύει άμεσα τους στόχους του, αλλά έμμεσα μέσω μελέτης και «αλίευσης» κατάλληλων πληροφοριών από τη δικτυακή κίνηση. Έτσι, λόγου χάριν, *μπορεί να κρυφακούει ή να οσμίζεται (sniff) την κυκλοφορία δεδομένων των δικτύων για να συγκεντρώσει πληροφορίες* για:

- **Έγκυρες IP διευθύνσεις**: Το σκουλήκι μπορεί να συλλέξει τις διευθύνσεις των πιθανών στόχων, με έναν τρόπο αρκετά διακριτικό και προσεκτικό.
- **Λειτουργικό σύστημα και υπηρεσίες**: Ένα σκουλήκι μπορεί να επωφεληθεί από τη γνώση του τύπου και της έκδοσης των λειτουργικών συστημάτων ενός κόμβου, καθώς και του είδους και των ιδιαίτερων εκδόσεων των δικτυακών υπηρεσιών που «τρέχουν» σε αυτόν. Σκουλήκια, που είναι ικανά να εκμεταλλευτούν πολλαπλές, τεχνικές αδυναμίες, μπορούν να επιλέξουν το κατάλληλο διάνυσμα προσβολής, ενώ άλλα μπορούν να αποκλείσουν τους τυχόν ακατάλληλους στόχους.
- **Μοτίβα δικτυακής κίνησης**: Ένα αργό σκουλήκι[190] μπορεί να περιορίσει τη δικτυακή δραστηριότητά του σε εκείνα τα χρονικά διαστήματα, κατά τα οποία λαμβάνει χώρα κάποια κανονική, νόμιμη, δικτυακή δραστηριότητα και να την εκμεταλλευτεί ως «όχημα» διάδοσης. Η άλλη αυτή δραστηριότητα μπορεί να ενεργήσει ως κάλυψη για τη λειτουργία του σκουληκιού[191].

---

[189] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM].

[190] Σκουλήκια που μεταδίδονται από τον ένα κόμβο στον άλλο, αργά και κατά δύναμιν με όσο πιο κρυφό τρόπο, αποκαλούνται στη βιβλιογραφία surreptitious or contagion worms και θεωρούνται εξίσου επικίνδυνα με τα αντίθετης λογικής σκουλήκια-αστραπές. Θα συζητήσουμε για αυτά ως σκουλήκια που ακολουθούν το παθητικό υπόδειγμα ανίχνευσης ή την πλήρη παθητικότητα στην εύρεση νέων στόχων.

[191] Η επιστράτευση «κρυφών καναλιών» στεγανογραφικού χαρακτήρα (συγκαλυμμένα κανάλια, covert channels) μπορεί να οδηγήσει σε παρόμοια αποτελέσματα από πλευράς διακριτικότητας, αλλά αυτό είναι περισσότερο μια καινοτόμα, ενεργητική

> Σε μερικές περιπτώσεις οι στόχοι έχουν ήδη προσδιοριστεί εξαιτίας άλλων ενεργειών και τα σκουλήκια αυτά απλά χρειάζεται μόνο να εξάγουν με κάποιον τρόπο τις απαραίτητες, σχετικές πληροφορίες και γνώσεις από τον όγκο όλων όσων παθητικά συλλέγουν.

Ένα σκουλήκι, που δεν χρησιμοποιεί μία από τις παραπάνω, ενεργητικές μεθόδους ή κάποιον άλλο ξεκάθαρο τρόπο αναζήτησης νέων θυμάτων, προκειμένου να εξαπλωθεί, αποκαλείται *παθητικό*.[192] Τα σκουλήκια αυτού του τύπου εμφανίζουν μια *αλληλεπικάλυψη και στενή συνάφεια στις τακτικές που ακολουθούν με τις αντίστοιχες τεχνικές της παθητικής ανίχνευσης*, αλλά εν γένει είναι *ακόμη πιο διακριτικά (σχεδόν ανεπαίσθητα) και λιγότερο δραστήρια* στη συμπεριφορά διάδοσής τους από τα αναφερόμενα ως συγκριτικά συγγενή τους. Παρόλ' αυτά, λόγω της προφανούς ομοιότητας οι δύο αυτές προσεγγίσεις ανίχνευσης αντιμετωπίζονται συχνά από τη σχετική βιβλιογραφία ως ταυτόσημες (interchangeable).

Τα παθητικά σκουλήκια δεν αναζητούν τους υποψήφιους κόμβους εξάπλωσης. Αντί αυτού, είτε περιμένουν τα πιθανά θύματα να έρθουν σε επαφή με το σκουλήκι είτε στηρίζονται στη συμπεριφορά των χρηστών για να βρουν τους νέους στόχους. Αν και ενδεχομένως αργό στη διάδοσή του, ένα παθητικό σκουλήκι δεν παράγει καμιάς μορφής ανώμαλη, δικτυακή κίνηση κατά τη διάρκεια «ανακάλυψης» νέου στόχου, πράγμα που ενδεχομένως το καθιστά και ιδιαίτερα κρυφό και επομένως ανθεκτικό. Τα *κολλητικά σκουλήκια (Contagion worms)* είναι χαρακτηριστικό είδος παθητικού σκουληκιού που διαδίδεται αργά, βασιζόμενο σε «κανονική», νόμιμη επικοινωνία για να «πέσει πάνω» σε νέα θύματα.[193]

Έχουν υπάρξει πολλά, παθητικά σκουλήκια, όπως το σκουλήκι Gnuman bait και το "αντισκουλήκι" CRClean. Το Gnuman λειτουργεί δρώντας ως κόμβος Gnutella, που απαντά σε όλες τις ερωτήσεις των ομότιμων κόμβων με αντίγραφά του.[194] Εάν κάποιο αντίγραφο εκτελεστεί από χρήστη στον κόμβο-θύμα, το σκουλήκι Gnuman αρχίζει και επαναλαμβάνει αυτήν τη διαδικασία. Δεδομένου ότι απαιτεί την ενεργοποίηση από χρήστη διαδίδεται σχετικά αργά.

μέθοδος αυτοπροστασίας παρά ένα μέσο παθητικής ανίχνευσης στόχων και θα συζητηθεί και αντιμετωπιστεί ως τέτοια στα Κεφάλαια 4 (3.2.4) και 5 (5.1.1).

[192] Κύρια, βιβλιογραφική αναφορά: [WEAVER_PAXSON-TCW].

[193] Πηγή: "How to 0wn the Internet in Your Spare Time", Stuart Staniford , Vern Paxson and Nicholas Weaver, USENIX Security Symposium 2002, διαθέσιμο από το δεσμό http://www.icir.org/vern/papers/cdc-usenix-sec02/.

[194] Πηγή: Διαδίκτυο, ιστοχώρος της εταιρείας παροχής εγνωσμένης αξίας και αποδοχής λύσεων προστασίας από το κακόβουλο λογισμικό Symantec, http://www.symantec.com/security_response/writeup.jsp?docid=2001-022710-3046-99.

Αν και δεν απελευθερώθηκε ποτέ (μέχρι στιγμής), το CRClean δεν απαιτεί την ανθρώπινη ενεργοποίηση.[195] Αυτό το σκουλήκι περιμένει για μία σχετική με Code Red II κατάλληλη διέγερση. Όποτε ανιχνεύει μια προσπάθεια μόλυνσης του κόμβου που «κατοικεί» με το σκουλήκι Code Red II, αποκρίνεται με την εκκίνηση και προώθηση μιας αντεπίθεσης στο μηχάνημα, που απέστειλε το Code Red II εναντίον το τρέχοντος κόμβου. Εάν αυτή η αντεπίθεση είναι επιτυχής, αφαιρεί το Code Red II και εγκαθίσταται εκείνο στο εν λόγω μηχάνημα. Κατά συνέπεια και το CRClean διαδίδεται χωρίς οποιαδήποτε ανίχνευση επόμενων στόχων.

Η συνθήκη της μη επαναμόλυνσης ισχύει και σε πολλές κατηγορίες σκουληκιών, αλλά εφαρμόζεται πιο «χαλαρά», σε σχέση με τους ιούς. Ανάλογα και σε αγαστή συνεργασία με τη μέθοδο ανίχνευσης (στη μέθοδο των μεταθέσεων για παράδειγμα είναι προαπαιτούμενος ο αυτό-εντοπισμός, ενώ στον τυχαιώδη τρόπο απουσιάζει συνήθως εγγενώς), που θα επιλέξουν οι σχεδιαστές των σκουληκιών, και τις προτεραιότητές τους (πολλαπλή μόλυνση, αθόρυβη ή ασφαλής διάδοση, απαιτήσεις εξάπλωσης) μπορούν να καταφύγουν στην χρησιμοποίηση ή μη κάποιας, εξειδικευμένης ρουτίνας αυτό-εντοπισμού του σκουληκιού, με τη βοήθεια κάποιου σημαδιού υπονόμευσης ενός κόμβου από κάποιο τρέχον στιγμιότυπό του, που θα βασίζεται σε εσωτερική ή εξωτερική του εν λόγω κόμβου πληροφόρηση, την οποία θα φροντίζει το κάθε στιγμιότυπο να ορίζει ή να διαχέει την ώρα που καταβάλλει τις άμυνες ενός κόμβου.

3.2.3 Εισαγωγή «γενετικού υλικού»: Αντιγραφή και αναπαραγωγή

Οι ιοί και τα σκουλήκια διαθέτουν ευδιάκριτες, διαφορετικές προσεγγίσεις -με το φαινόμενο της αλληλοεπικάλυψης τους να παρουσιάζεται στις συνδυασμένες, ιομορφικές απειλές (blended threats)[196]- στον τρόπο με τον οποίο πετυχαίνουν την αναγκαία και ποθητή αναπαραγωγή του «γενετικού» τους κώδικα. *Οι ιοί προβαίνουν, με άμεση δράση ή κατόπιν παραμονή τους στην κύρια μνήμη, σε αντιγραφή του ιομορφικού τους κώδικα στον εκάστοτε νέο ξενιστή τους*, ενώ *τα σκουλήκια στηρίζονται στην ύπαρξη συστημικών*[197] *ευπαθειών, τις οποίες «διαρρηγνύουν» με την κεφαλή τους, ώστε να εισβάλλουν και να καταλάβουν το επόμενο θύμα τους*.

---

[195] Πηγή: "Crossing the Line: Ethics for the Security Professional", ιστοχώρος της εταιρείας ερευνητών και επαγγελματιών της ασφάλειας ΠΣ SecureWorks, διαθέσιμο από το δεσμό http://www.secureworks.com/research/articles/ethics.

[196] Όσες αποτελούν τομή δηλαδή ιών και σκουληκιών, κάνοντας χρήση σχετικών μεθόδων και των 2 διακριτών κατηγοριών οπλολογισμικού. Στις μικτού τύπου απειλές αναφερθήκαμε και στο εισαγωγικό εδάφιο 2.4 του 2ου Κεφαλαίου.

[197] Σε οποιοδήποτε, όπως έχουμε επαναλάβει για πολλοστή φορά, από τα 5 συστατικά στοιχεία ενός ΠΣ.

Ιοί

Από μια πρώτη ματιά, στους ιούς *το είδος του ξενιστή*[198] *είναι εκείνο που καθορίζει ουσιαστικά τη διαδικασία μετάδοσης του ιομορφικού κώδικα* και άρα την αναπαραγωγή του ιού.

Έτσι, διακρίνουμε:

1. Ιοί τομέα εκκίνησης[199]

Ο τομέας εκκίνησης ενός Η/Υ παρέχει ένα πολύτιμο ενδιάμεσο βήμα στο στάδιο της φόρτωσης του λειτουργικού συστήματος. Το BIOS παραμένει ανίδεο των λειτουργικών συστημάτων που είναι εγκατεστημένα σε ένα μηχάνημα. Γνωρίζει όμως να αναζητήσει για κώδικα εκκίνησης σε διάφορα, φυσικά μέσα αποθήκευσης (όπως floppy, CD, DVD, HD-DVD, BluRay, USB, FireWire, PATA, SATA, eSATA δίσκοι) με βάση μια ρυθμιζόμενη σειρά προτεραιότητας. Κάθε φορά που διατρέχει τα μέσα αυτά φορτώνει συνήθως τον πρώτο τομέα τους (ή μια «χούφτα» πρώτους) και ανιχνεύει την ύπαρξη συγκεκριμένων bytes, που σηματοδοτούν πως το μέσο είναι εκκινήσιμο. Το BIOS παραδίνει τον έλεγχο στο πρώτο μέσο της σειράς προτεραιότητας που θεωρεί εκκινήσιμο και στον εκάστοτε τομέα που περιέχει το σημάδι και την πληροφορία εκκίνησης. Αυτός είναι ο τομέας εκκίνησης.

Από αυτό το σημείο αυτό και έπειτα, είναι η ευθύνη του τομέα εκκίνησης να παρέχει τις κατάλληλες εντολές και πληροφορίες για τη φυσική θέση ενός λειτουργικού συστήματος στο δίσκο, τη φόρτωσή του στη μνήμη και την εκκίνησή του, οποιοδήποτε και αν αυτό είναι. Κατ' αυτό τον τρόπο το BIOS (και άρα οι κατασκευαστές υπολογιστών) αποφεύγει να πρέπει να γνωρίζει a priori το ο,τιδήποτε για το εκάστοτε λειτουργικό σύστημα, που θα τρέξει στον υπολογιστή, πέραν του πού πρέπει να ψάχνει για τομείς εκκίνησης. Κάθε λειτουργικό σύστημα διαθέτει πλήθος ιδιοχαρακτηριστικών, όπως το δικό του σύστημα αρχείων ή διαμόρφωσης δίσκων, και κάθε δίσκος ή μέσο αποθήκευσης μπορεί να αποτελείται από πληθώρα διαφορετικών κατατμήσεων. Εφόσον, όμως, το κάθε Λ/Σ τοποθετεί έναν τομέα εκκίνησης -με κατάλληλες πληροφορίες για την ιδιαίτερη, φυσική θέση του Λ/Σ στο μέσο εκκίνησης, τη φόρτωσή του στη μνήμη και την εκκίνησή του (πίνακας κατάτμησης, MBR, BRs, όνομα και θέση αρχείων δεδομένων που ελέγχουν την εκκίνηση και περιέχουν το κύριο μέρος του Λ/Σ)- στον πρώτο ή πρώτους ή εν πάσει

[198] Βλέπε και εισαγωγικό κεφάλαιο 2, στο εδάφιο 2.4, για τον ορισμό ενός ιού και των ξενιστών αυτού, αλλά και για τη μεταξύ τους σχέση συμβίωσης και μη αυτονομίας του ιομορφικού λογισμικού.

[199] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM], [SZOR-ACVRD], [LUDWIG-GBBCV], [TANENBAUM-MOS9], [JOHANSSON-CVTEALF].

περιπτώσει σε εκ των προτέρων γνωστούς τομείς στο δείνα μέσο αποθήκευσης και εκκίνησης, θα είναι σε θέση να φορτωθεί και να τρέξει.

Σκοπός των ιών τομέων εκκίνησης είναι να εμφυτεύσουν τον ιομορφικό κώδικά τους στους διάφορους τομείς εκκίνησης δίσκων, ώστε αυτός να φορτώνεται στη μνήμη και να αρχίζει την εκτέλεσή του κατά τη διάρκεια της διαδικασίας εκκίνησης και πριν καν φορτωθεί πλήρως ένα Λ/Σ, με ό,τι αυτό σημαίνει για την εσωτερική ασφάλεια ενός Η/Υ. Η φυσιολογική πληροφορία εκκίνησης, που περιέχεται στα διάφορα, διακριτά τμήματα των τομέων εκκίνησης (MBR, Boot Records, Partition Table Structure, OS Loaders), τροποποιείται καταλλήλως, άλλοτε αντικαθιστώντας και άλλοτε πλαισιώνοντας διάφορα μέρη της με πρόσθετα δεδομένα, ανάλογα με τις ιδιαίτερες, ιομορφικές, μολυσματικές ανάγκες. Για την αναπαραγωγή τους *οι ιοί αυτοί αναζητούν εγγράψιμα μέσα αποθήκευσης, τα οποία είτε μετατρέπουν σε εκκινήσιμα δημιουργώντας μολυσμένους τομείς εκκίνησης ή αντιγράφονται σε ήδη υπάρχοντες τομείς εκκίνησής τους*. Συνήθως, *αποφεύγεται η επαναμόλυνση μολυσμένων τομέων*. Η ευρύτατη αποδοχή και κοινή χρήση αφαιρούμενων δίσκων αποθήκευσης με δυνατότητες εκκίνησης αποτελεί το μεγαλύτερο κανάλι διάδοσης των ιών του τύπου αυτού.

Τα προγράμματα των ιών τομέων εκκίνησης είναι *συνήθως μικρού μεγέθους* (της τάξης του 1 KB), καθώς πρέπει να χωρούν στο μεγαλύτερο ποσοστό τους σε χώρο που δεν ξεπερνά κατά πολύ έναν τομέα (το σύνηθες μέγεθος ενός τομέα είναι 512 bytes).

Οι ιοί τομέα εκκίνησης αν και *κάπως πλέον παρωχημένοι* εξακολουθούν να αποτελούν μια *εξαιρετικά επικίνδυνη απειλή,* καθώς άπαξ και ο κώδικας εκκίνησης μολυνθεί, τότε σε κάθε εκκίνηση ενός μολυσμένου συστήματος ο ιός θα παραμένει στον κώδικα εκκίνησης και θα φορτώνεται εκ νέου στη μνήμη εκτελώντας τις όποιες κακόβουλες εντολές του.

Τυπικό παράδειγμα BSI (boot-sector infector) είναι ο ιός Stoned και οι πολλές παραλλαγές του, μιας από τις οποίες είναι και ο πασίγνωστος Michelangelo.[200] Ο Stoned ακολουθεί μια σχετικά απλοϊκή τακτική μόλυνσης των δίσκων, όμως αυτό δεν στάθηκε εμπόδιο στην παγκόσμια εξάπλωση και συνεπακόλουθη φήμη του, χάρη στην επιτυχημένη μόλυνση των τομέων εκκίνησης αφαιρούμενων, αποθηκευτικών μέσων, όπως οι floppy δισκέτες.

2. <u>Παρασιτικοί Ιοί</u>

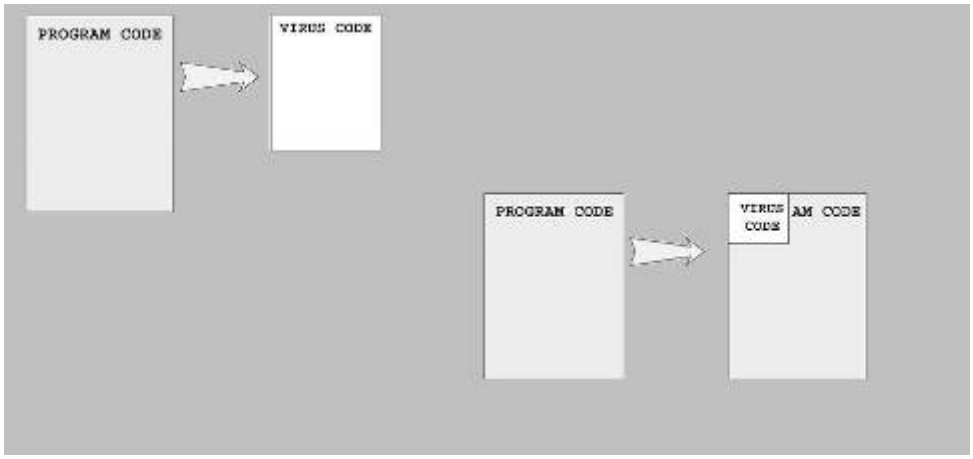
Είναι οι γνωστοί *ιοί αρχείων εκτελέσιμων προγραμμάτων ή γενικότερα δεδομένων με κάποιας μορφής «εκτελέσιμο» κώδικα*, κατέχουν τη μερίδα του λέοντος στο ιομορφικό

[200] Κύρια, βιβλιογραφική αναφορά: [LUDWIG-GBBCV].

λογισμικό και χωρίζονται σε αρκετές κατηγορίες, ανάλογα με τη μέθοδο εισαγωγής του ιομορφικού κώδικα στο σώμα του αρχείου-ξενιστή:

- **Επικάλυψη Αρχείου (Overwriters)**[201]

  Μερικοί ιοί εντοπίζουν απλά ένα αρχείο στο δίσκο και το επικαλύπτουν με το αντίγραφό τους, ξεκινώντας συνήθως από την κορυφή του αρχείου-ξενιστή. Η επικάλυψη μπορεί να είναι πλήρης ή μερική και *σε κάθε περίπτωση εξαφανίζεται κάποιο τμήμα του πρότερου κώδικα του ξενιστή*. Φυσικά, αυτό είναι μια πολύ πρωτόγονη τεχνική, αλλά είναι βεβαίως η ευκολότερη προσέγγιση όλων.



Σχήμα 11: Ιομορφική επικάλυψη αρχείου δεδομένων

Κανονικά, οι επικαλύπτοντες ιοί *δεν είναι πολύ επιτυχείς απειλές*, επειδή οι προφανείς παρενέργειες των μολύνσεων (αλλαγή μεγέθους ή/και καταστροφή μέρους της λειτουργίας ή των περιεχομένων των ξενιστών) ανακαλύπτονται εύκολα από τους χρήστες. Εντούτοις, όταν συνδυάζεται η τεχνική αυτή με την δικτυακή διάδοση (όπως συμβαίνει στις blended threats), εμφανίζονται στην πράξη σαφώς πιο ενισχυμένες δυνατότητες,.

Η μέθοδος μόλυνσης των ιών επικάλυψης χρησιμοποιείται επίσης από τους αποκαλούμενους μικροσκοπικούς ιούς (tiny virus).[202] Μια κλασική οικογένεια αυτού του τύπου είναι η οικογένεια Trivial του DOS[203]. Κατά τη διάρκεια των

---

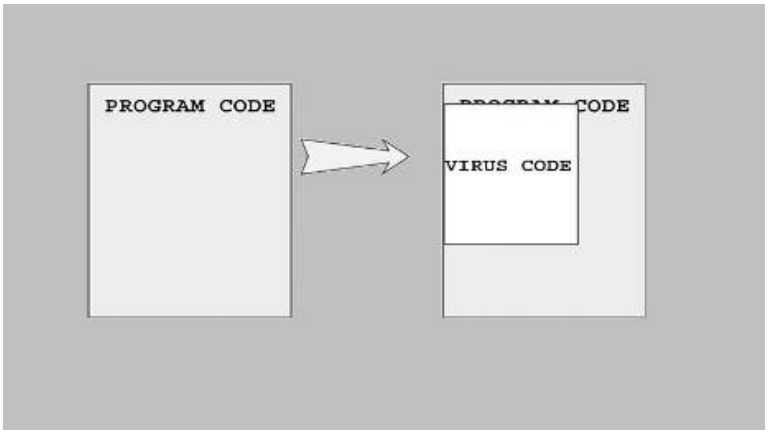
[201] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM], [SZOR-ACVRD], [LUDWIG-GBBCV], [TANENBAUM-MOS9], [JOHANSSON-CVTEALF].

[202] Κύρια, βιβλιογραφική αναφορά: [SZOR-ACVRD].

[203] Πηγή: Διαδίκτυο, ιστοχώρος της περίφημης εταιρείας έρευνας και παροχής λύσεων αντιμετώπισης του κακόβουλου λογισμικού F-Secure, http://www.f-secure.com/v-descs/minimal.shtml.

αρχών της δεκαετίας του '90, πολλοί συγγραφείς ιών προσπάθησαν να γράψουν τον μικρότερο, σε μέγεθος, δυνατό ιό και η, κατά τα άλλα άκομψη, μέθοδος επικάλυψης αποδείχθηκε μεγάλης πρακτικής αξίας για το σκοπό αυτό.

Μια άλλη, σπάνια παραλλαγή της μεθόδου επικάλυψης δεν αλλάζει τον κώδικα του προγράμματος ή το περιεχόμενο στην κορυφή του αρχείου-ξενιστή. Αντ' αυτού, ο ιός επιλέγει μια τυχαία θέση στο σώμα του ξενιστή και επικαλύπτει το αρχείο με τον ιομορφικό κώδικά του σε εκείνη την θέση. Προφανώς, ο κακόβουλος κώδικας μπορεί και να μην πάρει ποτέ τον έλεγχο κατά τη διάρκεια της εκτέλεσης του ξενιστή. Σε κάθε περίπτωση, το όποιο ενδεχομένως χρήσιμο πρόγραμμα του ξενιστή χάνει απρόσμενα τον έλεγχο ροής και συχνά καταρρέει προτού μπορέσει να εκτελεστεί ο κακόβουλος κώδικας. Οι τυχαιωδώς επικαλύπτοντες ιοί (random overwriters)[204], όπως ονομάζονται, είναι συχνά προβληματικοί για τους ανιχνευτές ιών, επειδή θα πρέπει να ανιχνεύεται το πλήρες περιεχόμενο του ξενιστή, πράγμα που μπορεί να είναι πολύ χρονοβόρο και ακριβό από πλευράς I/O πρόσβασης στους δίσκους.



Σχήμα 12: Τυχαία, εντός σώματος, ιομορφική επικάλυψη

Οι επικαλύπτοντες ιοί *δεν μπορούν να «καθαριστούν» από ένα αρχείο, καθώς συνήθως καταστρέφουν μέρος και σπανιότερα ακόμη και ολόκληρο το πρότερο περιεχόμενο του ξενιστή τους*. Τα μολυσμένα αρχεία πρέπει να διαγραφούν από το δίσκο και να αποκατασταθούν από τα όποια, «καθαρά», αντίγραφα ασφάλειας τους υπάρχουν στη διάθεση του κατόχου ή υπερασπιστή του συστήματος.[205]

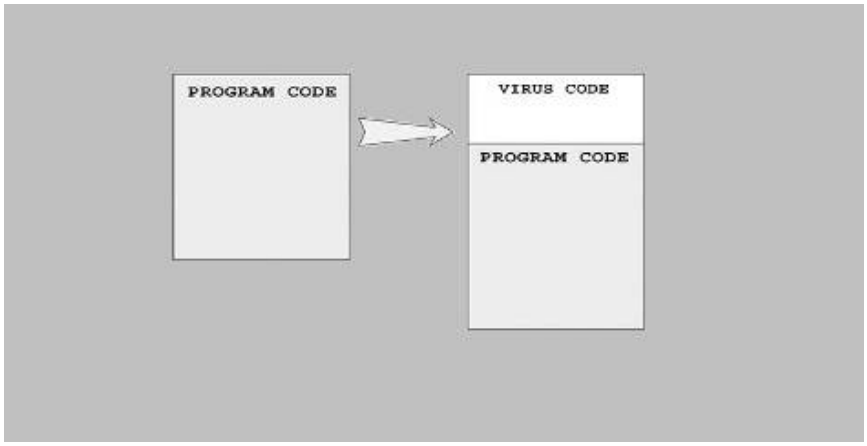
---

[204] Κύρια, βιβλιογραφική αναφορά: [SZOR-ACVRD].

[205] Ο θετικός ρόλος του backup στην ασφάλεια πληροφοριών αποδεικνύεται καθημερινά πως είναι μεγάλης αξίας και εμβέλειας, κάτι που θα επισημανθεί αρκετά, σε διάφορα εδάφια κατά μήκος της συγκεκριμένης διπλωματικής.

- **Αντιγραφή στην Αρχή Αρχείου (Prependers)**[206]

Μια κοινή τεχνική μόλυνσης ιών χρησιμοποιεί τη *λογική εισαγωγής του ιομορφικού κώδικα στην κορυφή των ξενιστών*. Τέτοιοι ιοί καλούνται prependers. Αν και απλό είδος ιομορφικής μόλυνσης, η μέθοδος αυτή είναι συχνά πολύ επιτυχημένη. Οι ιοί αυτού του είδους προγραμματίζονται συχνά σε υψηλού επιπέδου γλώσσες, όπως οι C, PASCAL, VB, Java και άλλες.



Σχήμα 13: Ιομορφική αντιγραφή στην αρχή του σώματος του ξενιστή

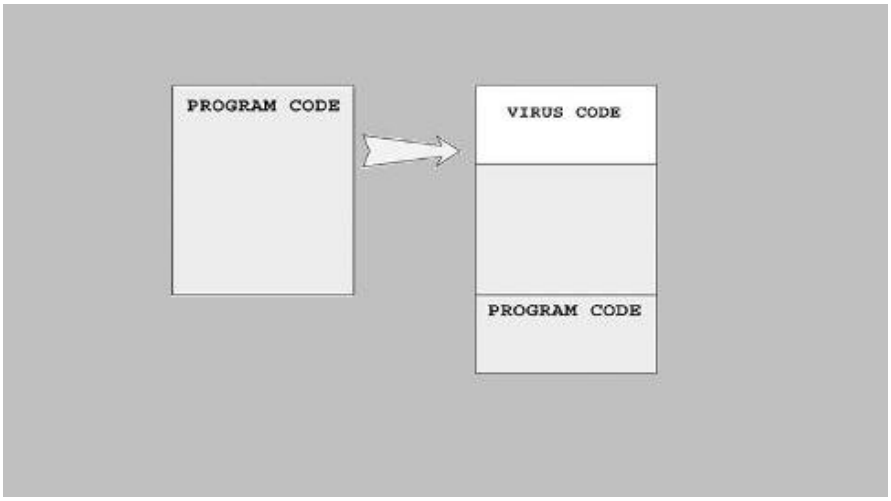
Η εκτέλεση του όποιου μη κακόβουλου κώδικα περιείχε ο ξενιστής μπορεί να μην είναι μια τετριμμένη διεργασία. Για το λόγο αυτό, ακριβώς, μια γενική prepending προσέγγιση πρέπει να περιλαμβάνει τη δημιουργία ενός προσωρινού αρχείου στο δίσκο που θα κρατήσει το αρχικό περιεχόμενο του ξενιστή. Κατόπιν μια λειτουργία, όπως π.χ. η system() της C, χρησιμοποιείται για να εκτελέσει τον αρχικό κώδικα του ξενιστή από το προσωρινό αρχείο. Οι ιοί αυτού του είδους περνούν συνήθως τις διάφορες παραμέτρους γραμμής εντολών του μολυσμένου ξενιστή στο αρχικό «πρόγραμμά» του, που βρίσκεται αποθηκευμένο στο προσωρινό αρχείο. Κατά συνέπεια η εκτέλεση του αρχικού κώδικα δεν παρεμποδίζεται και η πρότερη λειτουργία του ξενιστή δε χάνεται.

Μια *παραλλαγή της prepending τεχνικής είναι γνωστή ως κλασσική, παρασιτική μόλυνση (classic parasitism)*.[207] Τέτοιοι ιοί επικαλύπτουν την κορυφή του ξενιστή με τον κώδικά τους αφού σώσουν στο τέλος του το αντίστοιχο τμήμα του

[206] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM], [SZOR-ACVRD], [LUDWIG-GBBCV], [TANENBAUM-MOS9], [JOHANSSON-CVTEALF].

[207] Κύρια, βιβλιογραφική αναφορά: [SZOR-ACVRD].

αρχικού «προγράμματος» ή περιεχομένου του ξενιστή, που βρίσκεται στο χώρο που θα επικαλυφθεί. Ο πρώτος ιός τέτοιου τύπου ήταν ο Virdem, που γράφτηκε από τον Ralf Burger και παρουσιάστηκε το Δεκέμβρη του 1986 σε ένα underground φόρουμ, το Chaos Computer Club.[208] Στην πραγματικότητα ο Virdem είναι ένα από τα πρώτα παραδείγματα παρασιτικού ιού για COM αρχεία στο DOS. Μερικές πιο ειδικές περιπτώσεις της κλασσικής, παρασιτικής προσέγγισης δε σώζουν την αρχή του πριν τη μόλυνση «προγράμματος» ή περιεχομένου στο τέλος του ξενιστή. Αντ' αυτού, χρησιμοποιούν ένα προσωρινό -πολλές φορές κρυφό από τους χρήστες- αρχείο για να αποθηκεύσουν αυτές τις πληροφορίες, έξω από τον ξενιστή.



Σχήμα 14: Κλασσική, παρασιτική μόλυνση

- **Αντιγραφή στο Τέλος Αρχείου (Appenders)**[209]

Η τεχνική παίρνει το όνομά της και σε αυτήν την περίπτωση από τη θέση του ιομορφικού κώδικα, ο οποίος *επισυνάπτεται στο τέλος του αρχείου*. Σε αυτήν την τεχνική, μια οδηγία άλματος (JMP) παρεμβάλλεται στην αρχή του ξενιστή για να δείχνει στο πριν την αντιγραφή του ιού τέλος του κώδικά του. Η οδηγία άλματος αντικαθίσταται μερικές φορές με εξίσου λειτουργικές οδηγίες, όπως κλήσεις των:

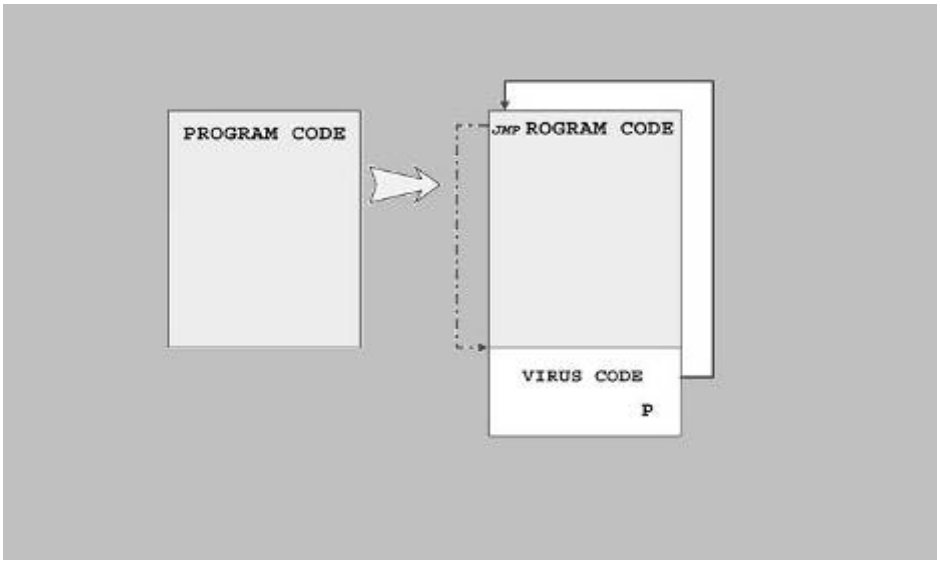
A.) CALL start_of_virus[210]

[208] Πηγή: Διαδίκτυο, ιστοχώρος της online «εγκυκλοπαίδειας» ιομορφικού και άλλου κακόβουλου λογισμικού VirusList, http://www.viruslist.com/en/viruses/encyclopedia?chapter=153311030.

[209] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM], [SZOR-ACVRD], [LUDWIG-GBBCV], [TANENBAUM-MOS9], [JOHANSSON-CVTEALF].

B.) PUSH offset start_of_virus

RET



Σχήμα 15: Ιομορφική αντιγραφή στο τέλος του σώματος του ξενιστή

Η appending τεχνική βρίσκει ευρύτατη εφαρμογή στις EPO προσεγγίσεις αυτοάμυνας, για τις οποίες θα γίνει εκτενής λόγος σε επόμενο εδάφιο του παρόντος κεφαλαίου[211].

- **Αντιγραφή Εντός Σώματος Αρχείου (In-Body Insertion)**[212]

Σύμφωνα με τις μεθόδους αυτής της κατηγορίας, ο ιομορφικός κώδικας εισάγεται με *αντιγραφή εντός σώματος* (όχι στην αρχή ή στο τέλος) *σε εξ αρχής ελεύθερα, κενά σημεία* του ξενιστή (γνωστότερα ως κοιλότητες ή cavities) ή *σε χώρους που ελευθερώνονται δυναμικά* και επίτηδες κατά την φάση αντιγραφής και των οποίων το περιεχόμενο μεταφέρεται σε άλλη θέση στην αρχή, εντός σώματος ή στο τέλος του ξενιστή.

Στην περίπτωση της δυναμικής μετακίνησης εντός σώματος κώδικα, η διαδικασία αντιγραφής μπορεί να γίνει ιδιαίτερα περίπλοκη, καθώς οφείλει να λαμβάνει υπόψιν τις τυχόν επικαιροποιήσεις εξαρτήσεων θέσεων δεδομένων (branch targets, data locations) και πληροφοριών σύνδεσης κατά την εκτέλεση

---

[210] Οι εντολές αυτές παρουσιάζονται κωδικοποιημένες στη χαμηλού επιπέδου γλώσσα Assembly, μπορούν όμως να αντικατασταθούν από τις ανάλογης λειτουργίας ρουτίνες σε πιο υψηλού επιπέδου γλώσσες προγραμματισμού.

[211] Βλέπε 3.2.4.

[212] Κύρια, βιβλιογραφική αναφορά: [SZOR-ACVRD], [TANENBAUM-MOS9].

(linker relocation information) και γι' αυτό αυτή η μέθοδος προσβολής σπάνια συναντάται στην πράξη. Η άλλη εκδοχή, των κενών δηλαδή κοιλοτήτων, βρίσκει μεγαλύτερη εφαρμογή σε σύγχρονες, ιομορφικές προσεγγίσεις.

Η εντός σώματος αντιγραφή ενδέχεται να είναι μια επίσης, κατεξοχήν έκφανση προηγμένων EPO τεχνικών, που συζητώνται διεξοδικότερα παρακάτω[213].

Ο W2K/Installer ιός (που γράφτηκε από τους συγγραφείς ιών Benny και Darkman) χρησιμοποιεί την τεχνική μόλυνσης μέσω κενών κοιλοτήτων για να προσβάλλει εκτελέσιμα PE Win32 στα Windows 2000, χωρίς αύξηση του μεγέθους του αρχείου[214].

- **Συνοδός Αρχείου (Companion virus)**[215]

Στην περίπτωση αυτή, ο ιός δεν τροποποιεί εσωτερικά καθόλου τον εκάστοτε ξενιστή του (*δεν εισάγει τον ιομορφικό κώδικα εντός του ξενιστή*), αλλά *εγκαθιστά τον εαυτό του έτσι, ώστε να εκτελείται πριν τον ξενιστή του, εκμεταλλευόμενος τον τρόπο με τον οποίο ένα Λ/Σ ή μια γραμμή εντολών ψάχνει για εκτελέσιμα αρχεία δεδομένων*. Με αυτήν την έννοια, είναι σαν να *«συνοδεύει» το υπονομευμένο πρόγραμμα*. Οι συνοδοί αρχείου και η λογική τους εξηγούνται καλύτερα μέσα από τα ακόλουθα παραδείγματα:[216]

- Η μετονομασία ενός εκτελέσιμου -με την ευρεία έννοια- αρχείου δεδομένων σε κάτι άλλο και η ανάληψη του αρχικού ονόματος από τον συνοδό ιό είναι μια πρώτη μέθοδος αυτής της κατηγορίας προσβολής, που οδηγεί σε παράκαμψη την εκτέλεση του αρχείου. Ο συνοδός μπορεί εφόσον είναι επιθυμητό να παραδίδει τον έλεγχο πίσω στο αρχείο για να εκτελεστεί, καλώντας το όμως με το νέο του όνομα (έτσι στα «μάτια» των χρηστών το αρχικό πρόγραμμά που ζήτησαν θα τρέξει κανονικά-ενδεχομένως εμφανίζοντας κάποια καθυστέρηση).
- Στο MS-DOS, το σύστημα ψάχνει εκτελέσιμα με το όνομα vir με την εξής σειρά: vir.com, vir.exe, vir.bat. Ένας συνοδός αρχείου με EXE

[213] Στο σχετικό με μεθόδους αυτοπροστασίας εδάφιο 3.2.4.

[214] Κύρια, βιβλιογραφική αναφορά: [SZOR-ACVRD].

[215] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM], [SZOR-ACVRD], [LUDWIG-GBBCV], [TANENBAUM-MOS9], [JOHANSSON-CVTEALF].

[216] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM].

ξενιστές μπορεί να είναι ο ίδιος ένα COM αρχείο με όνομα κάθε φορά ίδιο με έναν από τους εκάστοτε EXE στόχους. Με την ίδια νοοτροπία ένας ιός με EXE κατάληξη μπορεί να αποτελεί συνοδό ξενιστών τύπου BAT.

Ένα παράδειγμα τέτοιου ιού, που έκανε χρήση συνοδείας EXE αρχείων από συνονόματα COM με τη βοήθεια του API των pre-NT Windows, ήταν και ο W95/Spawn.4096[217].

- Στα Windows, η παραπάνω τριάδα πλαισιώνεται στο τέλος της από τα αρχεία του εκάστοτε Windows Shell (τα .cmd του Command prompt ή πιο πρόσφατα τα .msh ή .ps1 του Monad και του PowerShellv1) και του Windows Script Host (.wsh, VBScript .vbs ή JavaScript .js) προφέροντας νέες δυνατότητες στον επίδοξο συγγραφέα ιών-συνοδών.
- Η παρουσία της Registry (Μητρώο) στα Windows Λ/Σ δίνει το δικαίωμα περαιτέρω ιομορφικής δράσης τύπου συνοδών. Τα Windows αποθηκεύουν εντός Registry την πληροφορία αντιστοιχίας μεταξύ κάποιου τύπου αρχείου δεδομένων (στη μορφή κατάληξης του αρχείου) και κατάλληλων εκτελέσιμων εφαρμογών. Η σκόπιμη μεταβολή αυτής της πληροφορίας μπορεί να επιτρέψει σε κάποιον συνοδό συγκεκριμένου αρχείου δεδομένων να «τρέχει» πριν από τις εφαρμογές της δεδομένης κατάληξης, προσβάλλοντας έτσι μονομιάς κάθε αρχείο του συστήματος αυτού του τύπου, όταν εκτελείται.
- Στα σύγχρονα UNIX ή Unix-like Λ/Σ, τα εκτελέσιμα αρχεία ELF έχουν ένα συγκεκριμένο μηχανισμό αντιστοίχησης interpreter-runtime_linker για τη διερμηνεία και τη σύνδεση πριν την εκτέλεση του κάθε τέτοιου αρχείο, στον οποίο οι συνοδοί μπορούν να υποδυθούν ή υποκαταστήσουν το linker ρόλο προκαλώντας την απευθείας μόλυνση του ELF, κατά την εκτέλεσή του. Επίσης, το σύστημα αρχείων ακολουθεί μια φιλοσοφία προτεραιότητας όμοιας με των Windows στη σειρά εκτέλεσης με πρώτα τα ELF και κατόπιν οποιονδήποτε άλλο executable κώδικα, επιτρέποντας τη μόλυνση μέσω συνοδείας με μια απλή μετονομασία.

[217] Κύρια, βιβλιογραφική αναφορά: [SZOR-ACVRD].

Ενδεικτικά, αναφέρουμε τον υποτυπώδη ιό UNIX.comp,[218] που ανακαλύφθηκε το 2002 να μολύνει ELF μετονομάζοντάς τα σε .<αρχικόονομα> και παίρνοντας τη θέση τους στη σειρά εκτέλεσης.

- Οι συνοδοί αρχείου μπορούν τέλος να εκμεταλλεύονται την παρουσία συντομεύσεων (soft ή hard links) εφαρμογών και να μετατρέπουν αυτές κατάλληλα, ώστε να παραπέμπουν στον ιό-συνοδό, αντί για το αρχικά επιθυμητό πρόγραμμα. Στα συστήματα με GUI και συντομεύσεις με εικονίδια των εκάστοτε εφαρμογών, στα οποία οι χρήστες καταλήγουν να είναι ιδιαίτερα εξοικειωμένοι και συνηθισμένοι, μια τέτοια αλλαγή θα μπορούσε να είναι πολύ επιτυχημένη.

- **Διασταυρούμενη μόλυνση (Cross-infection)**[219]

Οι ιοί αυτού του είδους *κάθε φορά που εκτελούνται μπορούν να μολύνουν με κατάλληλο, ιομορφικό κώδικα αρχεία δεδομένων ή προγράμματα των οποίων η κατάληξη είναι διαφορετική από εκείνη του τρέχοντος, ιομορφικού ξενιστή*. Κοινώς, ένα EXE αρχείο μπορεί να χρησιμοποιείται για να μολύνει COM αρχεία, ενώ ένας σύνθετος BAT-VBS ή BAT-JS ιός μπορεί να στοχεύει εναλλακτικά και στους δύο τύπους εκτελέσιμων αρχείων.

Οι μέθοδοι εισαγωγής του ιομορφικού κώδικα στον κατάλληλο κάθε φορά ξενιστή μπορούν να ακολουθούν τα γνωστά κεντρικά μοτίβα overwriting, prepending, appending και in-body.

Ένα μεγάλο μέρος των προαναφερόμενων συνοδών, αλλά και των ακόλουθων μακροϊών, ανήκει και σε αυτήν την ιδιαίτερη κατηγορία.

Η διασταυρούμενη μόλυνση εφαρμόζεται με μεγάλη επιτυχία σήμερα, αλλά χρειάζεται προσοχή, ώστε ο κώδικας να μην ξεφύγει σε μέγεθος.

Ο συγγραφέας ιών SPTH[220] έχει κατ' επανάληψη επιδείξει διάφορες μορφές και τεχνικές διασταυρούμενης μόλυνσης, σχεδόν με κάθε συνδυασμό scripting γλωσσών (PHP, Ruby, Perl, JS, VBS, batch-script κ.ά.), καταδεικνύοντας την ευκολία δημιουργίας και τις αμέτρητες δυνατότητες.

---

[218] Πηγή: Διαδίκτυο, ιστοχώρος της εταιρείας παροχής εγνωσμένης αξίας και αποδοχής λύσεων προστασίας από το κακόβουλο λογισμικό Symantec, http://www.symantec.com/security_response/writeup.jsp?docid=2002-021614-0555-99.

[219] Πηγή: "Cross-Infection in JavaScript", SPTH, 2003, διαθέσιμο από το δεσμό http://vx.netlux.org/lib/vsp01.html.

[220] Περισσότερα μπορεί κανείς να αναζητήσει στον διαδεδομένο ιστοχώρο των VXers VXHeavens, από την προσωπική σελίδα του SPTH, http://vx.netlux.org/lib/?lang=EN&author=SPTH.

- **Μόλυνση με Μακροεντολές (Macrovirus)**[221]

Οι μακροϊοί όπως είναι περισσότερο γνωστοί βασίζουν την ύπαρξη τους στην *παρουσία εκτελέσιμων, διερμηνευόμενων (μακρο)εντολών εντός αρχείων δεδομένων, που φαινομενικά δεν περιέχουν εκτελέσιμο κώδικα* και η κύρια αποστολή τους είναι η αποθήκευση πληροφοριών. Τα αρχεία αυτά δεν είναι προγράμματα, αλλά όταν φορτώνονται στη μνήμη με τη βοήθεια της εφαρμογής που τα χειρίζεται, ο κώδικας μακροεντολών που περιέχουν διερμηνεύεται από την εφαρμογή και εκτελείται κατά τη διάρκεια της παραμονής του αρχείου στη μνήμη (οποιαδήποτε στιγμή από το άνοιγμα έως το κλείσιμό του, ανάλογα και με τις κωδικοποιημένες εντολές). Στις περισσότερες των περιπτώσεων, ένας μακροϊός κάνει χρήση της δυνατότητας μακροεντολών σε κάποιο αρχείο, ώστε να κωδικοποιήσει ρουτίνες αναζήτησης νέων ξενιστών αυτού του τύπου αρχείου δεδομένων και αντιγραφής της ακολουθίας των μακροεντολών εντός τους, χωρίς να αποκλείεται και η διασταυρούμενη μόλυνση.

Η ύπαρξη ρουτινών αναζήτησης και αντιγραφής κώδικα στις γλώσσες αυτές, σε συνδυασμό με την ευρεία παρουσία και διάδοση τύπων αρχείων δεδομένων, που παρέχουν κάποιας μορφής μακρο-λειτουργικότητας (embedded scripting capabilities) με δυνατότητα ενσωμάτωσης διερμηνευόμενου κώδικα καθιστούν εφικτή τη μόλυνση από μακροϊούς. Η γνώση κάθε φορά της ιδιαίτερης γλώσσας συγγραφής (που μπορεί να μην είναι και επαρκώς τεκμηριωμένη) των μακροεντολών αυτών είναι η μόνη, συμβατική «υποχρέωση» από τη μεριά του κακόβουλου συγγραφέα.

Τα πιο γνωστά παραδείγματα αυτού του είδους παρασιτικότητας είναι οι μακροϊοί της σουίτας MS Office (προγράμματα Word, Excel, PowerPoint, Visio, Access, Project κτλ), από τους οποίους προήλθε και το όνομα αυτής της κατηγορίας.[222] Στα αρχεία αυτά την επιτυχία της προσβολής ενίσχυε και η παρουσία καθολικών προτύπων εγγράφων (document templates), τα οποία λειτουργούσαν ως σημείο αναφοράς και φόρτωσης εντολών σε κάθε όμοιο έγγραφο και εξυπηρέτησαν τους κακόβουλους συγγραφείς ως αποθετήρια επιβλαβών μακροεντολών και ορμητήρια αστραπιαίων μολύνσεων, καθώς και η σχετική δημοτικότητα που απολάμβανε και απολαμβάνει ακόμα η εν λόγω

[221] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM], [SZOR-ACVRD], [TANENBAUM-MOS9].

[222] Πηγή: Διαδίκτυο, ιστοχώρος της online εγκυκλοπαίδειας WikiPedia, http://en.wikipedia.org/wiki/Macro_virus_%28computing%29.

σουίτα εφαρμογών. Σήμερα, η παρασιτικότητα στο MS Office είναι πλέον ελεγχόμενη (απενεργοποίηση μη έμπιστων μακροεντολών), αλλά δεν έπαψε να αποτελεί εγγενές πρόβλημα.

Η παρουσία scripting δυνατοτήτων εντός κλασσικών αρχείων δεδομένων είναι εξαιρετικά χρήσιμη σε ορισμένες περιπτώσεις, όπως π.χ. στις εφαρμογές αυτοματισμού γραφείου και όχι μόνο, αλλά έρχεται με τον κίνδυνο της χρησιμοποίησης αυτής της μορφής «εκτελέσιμου» κώδικα προς όφελος κακόβουλων (και όχι μόνο ιομορφικών) δράσεων από επίβουλες οντότητες, που τυχαίνει να κατέχουν τα «μυστικά» της συγγραφής του εκάστοτε scripting υποδείγματος.

Ο πρώτος γνωστός μακρο-ιός του Word ήταν ο WM/DMV, που γράφτηκε το 1994. Ο κατασκευαστής του ιού δημιούργησε συγχρόνως επίσης έναν σχεδόν λειτουργικό μακρο-ιό (XM) για το Excel.[223] Πολύ σύντομα η αρχική επιτυχία στη μόλυνση προσέλκυσε και άλλους συγγραφείς με αποτέλεσμα, το 1995, να έχουμε την πρώτη μεγάλης κλίμακας διάδοση (wild-spread) μακροϊού για το Word (WM/Concept.A), ενώ οι αντίστοιχες εξελίξεις έφτασαν στο Excel το 1996 με την εμφάνιση και αποκάλυψη της δράσης του XM/Laroux.

3. Πολυμερείς Ιοί[224]

Στους πολυμερείς ιούς, η αντιγραφή του ιομορφικού, «γενετικού» υλικού στους ξενιστές μπορεί να γίνεται με *εναλλαγή των μεθόδων των 2 παραπάνω κατηγοριών*, ανάλογα με το είδος του εκάστοτε εντοπισθέντα ξενιστή (τομέας εκκίνησης-αρχείο δεδομένων).

Ένα πολύ γνωστό παράδειγμα πολυμερούς δράσης είναι και αυτό του ιού Tequila[225], που πρωτοαπομονώθηκε το 1991 και μπορούσε να μολύνει ταυτόχρονα EXE αρχεία στο DOS, αλλά και τον MBR των δίσκων αποθήκευσης.

Από μια άλλη σκοπιά, *η κύρια μνήμη ενός υπολογιστικού συστήματος μπορεί επίσης να επιδράσει καταλυτικά στην όλη διαδικασία αναπαραγωγής του ιού*. Η αντιγραφή του ιομορφικού υλικού σε νέους ξενιστές μπορεί να γίνεται σε 2 χρόνους, ανάλογα με τη χρήση της κύριας μνήμης· με απευθείας δράση (direct-action) αναζήτησης ξενιστών και αντιγραφής

[223] Κύρια, βιβλιογραφική αναφορά: [SZOR-ACVRD].

[224] Κύρια, βιβλιογραφική αναφορά: [SZOR-ACVRD], [LUDWIG-GBBCV].

[225] Πηγή: Διαδίκτυο, ιστοχώρος της παγκοσμίως αναγνωρισμένης εταιρείας παροχής λύσεων προστασίας από το κακόβουλο λογισμικό McAfee, http://vil.nai.com/vil/content/v_98230.htm.

που ακολουθεί την εκτέλεση ενός μολυσμένου αρχείου ή τομέα εκκίνησης ή καιροφυλακτώντας στη μνήμη τυχαίας προσπέλασης (RAM) για την κατάλληλη στιγμή για εντοπισμό και προσβολή καινούριων θυμάτων (αρχείων ή/και τομέων εκκίνησης).[226] Ιοί που επιζητούν και καταφέρνουν μια παραμονή στην κύρια μνήμη ενός συστήματος και συνάμα την εκμεταλλεύονται, προκειμένου να πετυχαίνουν την κατάληψη νέων ξενιστών είναι γνωστοί ως *TSR (Terminate-and-Stay-Resident) ιοί*[227] και μπορούν να εμπίπτουν σε οποιαδήποτε από τις 3 παραπάνω κατηγορίες.

Σκουλήκια

Την επιτυχημένη αντιγραφή και αναπαραγωγή στα σκουλήκια εγγυάται η αποτελεσματικότητα της κεφαλής τους, δηλαδή της μεθόδου διείσδυσης στα συστήματα των υπό επίθεση κόμβων. Από τη στιγμή που μια κεφαλή «τρυπήσει» κάποιο σύστημα έχει ουσιαστικά αναπαραχθεί ένα νέο στιγμιότυπο σκουληκιού, που αμέσως ξεκινά την αναζήτηση νέων στόχων και την άμεση αποστολή νέων αντιγράφων του -με την ίδια ή τροποποιημένη κεφαλή- στα θύματα που μόλις ανίχνευσε. Με τον τρόπο αυτό η διαδικασία διάδοσης επαναλαμβάνεται με την εκάστοτε κεφαλή να κατέχει πρωταγωνιστικό ρόλο στην επιτυχία της.

Η κεφαλή κάθε σκουληκιού αποτελεί το τμήμα εκείνο του κώδικά του που περιέχει μία ή περισσότερες, κατάλληλες συνταγές εκμετάλλευσης πιθανών ευπαθειών και αδυναμιών του συστήματος πληροφοριών (κόμβου ή δικτύου) του οποίου επιθυμείται η υπονόμευση. Οι ευπάθειες και οι αδυναμίες αυτές είναι τα τρωτά σημεία των ΠΣ, καθώς παρέχουν μέσα και τρόπους εισβολής και παρείσφρυσης σε κακόβουλες οντότητες, όπως τα σκουλήκια.

Όπως είναι γνωστό και έχει επαναληφθεί ουκ ολίγες φορές στην παρούσα εργασία, κάθε ΠΣ συνίσταται από 5 δομικά μέρη, καθένα από τα οποία μπορεί να λειτουργήσει δυνητικά ως φορέας αδυναμιών και ευπαθειών, κατά καιρούς τόσο επικίνδυνων που ένα σκουλήκι θα κωδικοποιούσε «ευχαρίστως» σε μέρος της κεφαλής του:

- Υλικό
- Λ/Σ και εφαρμογές
- Πρωτόκολλα δικτύου
- Δεδομένα
- Άνθρωπος (social engineering, sharing κτλ)

[226] Κύρια, βιβλιογραφική αναφορά: [SZOR-ACVRD], [LUDWIG-GBBCV], [TANENBAUM-MOS9].

[227] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM], [LUDWIG-LBBCV], [SZOR-ACVRD], [BILAR-IM].

Η παρουσία οποιασδήποτε μορφής τεχνικής αδυναμίας έχει μεγάλη αξία για τον επιτιθέμενο και είναι κάτι που ταχύτατα κυκλοφορεί στους κόλπους και στα «πηγαδάκια» των «άτακτων τέκνων της Πληροφορικής»[228], σε σημείο που κάθε σοβαρή, τεχνική παράλειψη που γίνεται αντιληπτή να σηματοδοτεί και να αποδεικνύεται ορόσημο μεγάλου μήκους επιθέσεων σκουληκιών ή και συνδυασμένων απειλών (blended viral threats). Από την άλλη, η ανθρώπινη δράση αποτελεί συχνά το «πασπαρτού» πολλών συστημάτων εκεί όπου οι τεχνικές αδυναμίες δεν αποδίδουν ή δεν ωφελούν. Η έμφυτη ανάγκη για επικοινωνία και η αφέλεια-άγνοια κινδύνου, που μπορεί να συνοδεύει έναν άπειρο, νέο ή ανεπαρκώς εκπαιδευμένο χρήστη, μπορούν να συνθέσουν ένα εκρηκτικό και ιδιαίτερα επικίνδυνο, σκωληκοειδές «κοκτέιλ», που ενδέχεται να προσπεράσει οποιονδήποτε, οσοδήποτε αυτοματοποιημένο και ευφυή, δικτυακό και ενδοκομβικό, μηχανισμό ασφάλειας πληροφοριών, να καταλάβει οποιονδήποτε πληροφοριακής αξίας κόμβο και να καταστήσει ένα ολόκληρο ΠΣ ευάλωτο ή προσβεβλημένο.

Η *πληθώρα τεχνικών και ανθρώπινων, ευπαθειών και αδυναμιών των πληροφοριακών συστημάτων* είναι μια πραγματικότητα άμεσα συνυφασμένη με την ίδια την ύπαρξη των συστημάτων αυτών και συνάδει με την *άγραφη αρχή της μη τελειότητας των ανθρώπινων δημιουργημάτων* (λογισμικό, υλικό, δίκτυα, διαδικασίες) *και δράσεων* (συμμετοχή/παρέμβαση στα ΠΣ). Η διαρκής εκμετάλλευσή τους δίνει στα σκουλήκια το διαχρονικό, αλλά ταυτόχρονα πάντοτε επίκαιρο στις εκάστοτε εξελίξεις, μέσο/«όχημα» για την προσβολή των στόχων τους και την αυτοαναπαραγωγή τους.

3.2.4 Αυτοάμυνα

Το μεγαλύτερο ποσοστό ιών και σκουληκιών εφαρμόζουν, πλέον με συνέπεια, κάποιες στοιχειώδεις στρατηγικές αυτοπροστασίας με *προφανή σκοπό την ενίσχυση της αντοχής και της επιβίωσής τους* στο αντίξοο και αφιλόξενο περιβάλλον, που συνθέτουν τα σύγχρονα συστήματα ασφάλειας των ΠΣ. Η αυτοάμυνα του αυτοαναπαραγόμενου, επιβλαβούς λογισμικού επιτυγχάνεται *είτε χάρη στην υιοθέτηση παθητικών μεθόδων* απόκρυψης, θωράκισης ή μετάλλαξης *είτε με τη χρήση πιο επιθετικών τεχνικών*, που στοχεύουν στην ενεργητική καταστολή-εξουδετέρωση των συστημάτων ασφάλειας ή την υπονόμευση των λειτουργικών συστημάτων των θυμάτων. Η λογική των παθητικών προσεγγίσεων έχει κυρίως τον προστατευτικό χαρακτήρα της πρόληψης *από την έκθεση σε κάποιον εχθρό (proactive)*, ενώ οι ενεργητικές αποτελούν συνάμα και εκφράσεις ενός μηχανισμού δραστικής

[228] Σε φόρουμ και ιστοχώρους, όπως το επιφανές http://www.milw0rm.com/.

ανταπόκρισης στον όποιο κίνδυνο ανακύπτει (reactive)· το στάδιο πάλι ανίχνευσης της όποιας απειλής για τον κακόβουλο κώδικα μπορεί να είναι -και συνήθως είναι- και στις 2 διάχυτο.

Οι τεχνικές αυτές, γενικά, *μπορούν να αναμιχθούν με ποικίλους τρόπους και να χρησιμοποιηθούν μεμονωμένα, εναλλακτικά και σε συνδυασμούς*, ενώ ίσως σε κάποιο, μικρό βαθμό ορισμένες από αυτές, υπό συγκεκριμένες θεωρήσεις ή προϋποθέσεις, να επικαλύπτονται μεταξύ τους.

Α) Παθητικές μέθοδοι (stealth or armoring or mutation)

Κύρια απασχόληση των παθητικών τρόπων αυτοάμυνας είναι η *εισαγωγή ρουτινών σε ιούς και σκουλήκια, που επιφέρουν πρόσθετο βάρος στην κατανάλωση πόρων, για μια επιτυχημένη και αποτελεσματική ανίχνευση και αναγνώριση μιας κακόβουλης απειλής*, από τα συστήματα ασφάλειας και τους χρήστες των υπονομευμένων συστημάτων.[229]

Στις παθητικές μεθόδους αυτοάμυνας μπορεί να διακρίνει κανείς *3 κύρια ρεύματα*, που μπορεί να ακολουθήσει εναλλακτικά, μεμονωμένα ή συνδυαστικά, ο συγγραφέας κακόβουλου, αυτοαναπαραγόμενου λογισμικού και ο επιτιθέμενος με ένα τέτοιο όπλο. Το πρώτο αφορά την προσέγγιση της *απόκρυψης του κακόβουλου λογισμικού*, που εμφανίζεται με κύριο εκφραστή την κρυπτογράφηση, το δεύτερο είναι ο δρόμος της *θωράκισης ιών και σκουληκιών* ενάντια σε διαδεδομένες, εξελιγμένες προσεγγίσεις ασφάλειας των προγραμμάτων και συστημάτων προστασίας Η/Υ και το τρίτο αντιπροσωπεύει τη *λογική και τα οφέλη της μετάλλαξης*. Οι διάφοροι εκφραστές των ρευμάτων αυτών παρατηρείται ορισμένες φορές να διαπερνούν τα λεπτά, στενά όρια του ρεύματος που κατά κύριο λόγο ανήκουν και να χρησιμεύουν και ως τεχνικές εξυπηρέτησης και κάποιου έτερου ή ακόμα και των τριών.

1. Καμουφλάζ και Σίγαση (Stealth)

Υπάρχουν τόσο παθητικές όσο και ενεργητικές τεχνικές απόκρυψης με κριτήριο διαχωρισμού την επιθετικότητα που εκδηλώνεται. Μέθοδοι καμουφλάζ και σίγασης που βασίζονται και γίνονται εφικτές χάρη σε επιτυχημένες προσπάθειες υπονόμευσης του Λ/Σ των υπό επίθεση κόμβων ανήκουν στη σφαίρα των ενεργητικών προσεγγίσεων αυτοάμυνας, που συζητώνται αναλυτικότερα παρακάτω, ενώ στις παθητικές προσεγγίσεις συγκαταλέγονται όλες όσες δεν απαιτούν ή προκαλούν σκόπιμα υπονόμευση στο Λ/Σ.

i. Μετάπτωση

Η μετάπτωση αφορά στη "*δυνατότητα του κακόβουλου, αυτοαναπαραγόμενου λογισμικού να υποπίπτει/μεταβαίνει σε λανθάνουσα κατάσταση, όταν εντοπίζει ή έρχεται αντιμέτωπο με μια πιθανή απειλή αποκάλυψής του και να επανενεργοποιείται, όταν η απειλή αυτή δεν υφίσταται"*.

Πιο συγκεκριμένα υπάρχει *αυτοματοποιημένη, προγραμματισμένη φροντίδα* ώστε:

- οι ιοί να μπορούν δυναμικά να αναστέλλουν την ιομορφική τους δράση, όταν ανιχνεύουν συγκεκριμένη, επικίνδυνη ή εχθρική (αντιϊομορφική) παρουσία ή/και δράση σε κάποιο μολυσμένο σύστημα και να επανέρχονται το ίδιο δριμείς, όταν αμφότερες εκλείπουν και
- τα σκουλήκια να μπορούν να καθυστερούν ή να περιορίζουν τη διάδοσή τους ακόμα και να αποφεύγουν να βάλλουν κατά κάποιων στόχων, ανάλογα με το αν εντοπίζουν ορισμένους μηχανισμούς προστασίας στους οποίους είναι ευάλωτα ή/και συνθήκες που μπορούν δυνητικά να εκθέσουν την παρουσία τους.

Η τεχνοτροπία της μετάπτωσης είναι, ίσως, η πιο υποτυπώδης προσέγγιση αυτοάμυνας, αυτό όμως δεν την εμποδίζει από το να αποτελεί μια *ευρέως χρησιμοποιούμενη στις τάξεις του κακόβουλου, αυτοαναπαραγόμενου λογισμικού προστατευτική λύση*, καθώς διακρίνεται για την *απλότητα στην βασική υλοποίηση* (ON-OFF διακόπτης[230]), παρέχοντας παράλληλα μέσω της αεργίας ή μειωμένης δραστηριότητας στη λανθάνουσα κατάσταση ικανοποιητικό βαθμό δυναμικής απόκρυψης, ενώ *επιδέχεται και πολλών προσθηκών και βελτιώσεων, διαβαθμίσεων και κλιμακώσεων*[231]. Χαρακτηριστικό της απόκρυψης που προσφέρει η μετάπτωση είναι πως *δε βασίζεται σε εξειδικευμένες, πολύπλοκες και ογκώδεις ρουτίνες*, αλλά κυρίως στην αδράνεια του λογισμικού στη λανθάνουσα κατάσταση και στη λογική (συνθήκη) με την οποία αυτή ενεργοποιείται, και πως *είναι εν γένει επιλεκτική και προσωρινή*, τίθεται δηλαδή σε λειτουργία κάτω από πολύ συγκεκριμένες προϋποθέσεις και διαρκεί για όσο χρόνο αυτές εκπληρούνται.

Μια πιο στατική (εκ των προτέρων σχεδιασμένη), τυχαιώδης προσέγγιση στη μετάπτωση, βασισμένη σε κάποια -ενδεχομένως και ρυθμίσιμη- πιθανότητα ενεργοποίησης (και

---

[229] Οι χρήστες παθητικών μεθόδων προστασίας τρέφουν την ελπίδα: α)αποτυχίας των προγραμμάτων/μηχανισμών προστασίας στον εντοπισμό του κακόβουλου κώδικα λόγω υπερβάσεων σε χρονικούς ή άλλους συστημικούς περιορισμούς, β)ικανοποιητικής για την περαιτέρω διάδοση καθυστέρησης της ανίχνευσης.

[230] Θέση ON: λειτουργία και κακόβουλη δραστηριότητα, Θέση OFF: αεργία και διακριτικότητα.

[231] Βλέπε εδάφιο ευφυής προσαρμογή (3.2.6).

σπανιότερα απενεργοποίησης) του κακόβουλου κώδικα είναι επίσης δυνατή και μπορεί να είναι αρκετά αποτελεσματική για την επιβίωση κάποιου μέρους του πληθυσμού της επιβλαβούς απειλής (μάλιστα ένα τέτοιο μοντέλο συζητάται παρακάτω, προκειμένου για θωράκιση κόντρα στην εξομοίωση).

ii. Κρυπτογραφία

Η κρυπτογράφηση αποτελεί παραδοσιακό, μόνιμο σύμμαχο της ασφάλειας των ΠΣ. Όμως, παραμένει, στην ουσία της, απλά μια ακόμη ουδέτερη τεχνολογία, που μπορεί να χρησιμοποιηθεί καταλλήλως για να εξυπηρετήσει πλήθος από κακόβουλους στόχους.

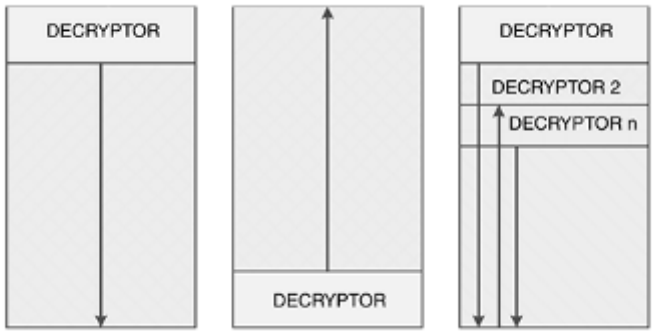
Απλή Κρυπτογράφηση[232]

Η κατεξοχήν μέθοδος απόκρυψης ενός κακόβουλου προγράμματος είναι η απλή κρυπτογράφησή του. Στη μέθοδο αυτή το κυρίως σώμα ενός ιού ή σκουληκιού κρυπτογραφείται (με συμμετρικό ή ασυμμετρικό κλειδί) και ένας σταθερός, μοναδικός μηχανισμός αποκρυπτογράφησης ή decryptor τοποθετείται (συνήθως) στην κεφαλή του (χωρίς να είναι μικρή και η εκπροσώπηση των αντίρροπων μηχανισμών, που τοποθετούνται δηλαδή στο τέλος του σώματος και είναι γνωστοί ως backward decryption loops). Προφανώς, η κρυπτογράφηση κρύβει *το περιεχόμενο του βασικού, κεντρικού κακόβουλου κώδικα* από τα αδιάκριτα μάτια χρηστών και συστημάτων ασφάλειας, *ο κώδικας των decryptors όμως για προφανείς λόγους είναι μη κρυπτογραφημένος, άρα και ευδιάκριτος*. Το γεγονός αυτό, σε συνδυασμό με τη μοναδικότητα του εκάστοτε μηχανισμού αποκρυπτογράφησης, μεταξύ διαφορετικών ξενιστών ή στιγμιοτύπων της ίδιας απειλής, αποτελεί την «αχίλλειο πτέρνα» της απλής κρυπτογράφησης. Ναι μεν μπορεί να καθυστερήσει σημαντικά ένα σύστημα ασφάλειας, ενέχει όμως εγγενώς την ευπάθεια ύπαρξης βασικών στοιχείων (αναλλοίωτος κώδικας του decryptor) στον κακόβουλο κώδικα, για τον εντοπισμό και τη μοναδική ταυτοποίηση του επιβλαβούς λογισμικού, που την εφαρμόζει.

Το πρώτο γνωστό παράδειγμα οπλολογισμικού που έκανε χρήση κρυπτογραφίας ήταν ο ιός Cascade του DOS[233].

[232] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM].

[233] Πηγή: Διαδίκτυο, ιστοχώρος της online εγκυκλοπαίδειας WikiPedia, http://en.wikipedia.org/wiki/Cascade_virus.



Σχήμα 16: Παραδείγματα χωροθέτησης της ρουτίνας αποκρυπτογράφησης ενός στοιχειώδους, κρυπτογραφημένου κυβερνοόπλου.

Ολιγομορφισμός[234]

Οι συγγραφείς ιών και σκουληκιών γρήγορα συνειδητοποίησαν ότι η ανίχνευση ενός απλά κρυπτογραφημένου κακόβουλου προγράμματος παραμένει εύκολη υπόθεση για τα αντιϊομορφικά συστήματα, εφόσον ο κώδικας του μηχανισμού αποκρυπτογράφησης είναι αρκετά ευρύς και αρκετά μοναδικός. Για να προκαλέσουν τα αντιϊομορφικά προϊόντα και τα άλλα συστήματα προστασίας περαιτέρω εφευρέθηκαν και εφαρμόστηκαν διάφορες τεχνικές δημιουργίας παραλλαγμένων ή μεταλλαγμένων decryptors.

Η απλούστερη τεχνική για να (παρ)αλλαχτούν αυτοί οι μηχανισμοί αποκρυπτογράφησης είναι να χρησιμοποιηθεί ένα *-μικρό συνήθως- πεπερασμένο σύνολο από διαφορετικούς decryptors αντί ενός και μοναδικού*.[235] Αντίθετα από τις απλά κρυπτογραφημένες, κακόβουλες απειλές, το ολιγομορφικό λογισμικό δε διατηρεί τους decryptors του απαραίτητα σταθερούς και μοναδικούς μεταξύ των διαφορετικών αντιγράφων ή στιγμιοτύπων του, αλλά μπορεί να τους αλλάζει σε κάθε νέα γενιά, επιλέγοντας (τυχαία ή σκόπιμα κάποιον άλλο) από το μικρό και πεπερασμένο σύνολο των δυνατών εναλλακτικών. Το όφελος που προέκυπτε ήταν διπλό· *ο κρυπτογραφημένος, κακόβουλος κώδικας που παράγεται είναι διαφορετικός για κάθε μέθοδο (απο)κρυπτογράφησης, ενώ η τροποποίηση των decryptors εξαλείφει τη δυνατότητα εύκολης ταυτοποίησης μιας απειλής* που «προσφέρεται» μέσω μιας ενδεχόμενης σταθερότητας και μοναδικότητάς του.[236] Έτσι, λόγω της διαφαινόμενης

[234] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM], [SZOR-ACVRD], [PEARCE-VP].

[235] Κύρια, βιβλιογραφική αναφορά: [SZOR-ACVRD], [PEARCE-VP].

[236] Οι πρώτοι ολιγομορφικοί ιοί, όπως ο Whale ή ο W95/Memorial δημιούργησαν αρκετούς «πονοκεφάλους» στους εργάτες της ασφάλειας και προστασίας των ΠΣ, μέχρι να βρεθεί ένας εξονυχιστικότερος και αποδοτικότερος τρόπος σάρωσης (βλέπε Κεφάλαιο 4 (4.1.1 και 4.1.2), για ευριστική ανάλυση και εξομοίωση κακόβολου κώδικα) από τους τότε τρέχοντες.

μεγαλύτερης δυσχέρειας στον εντοπισμό και την ανάλυση της κακόβουλης απειλής το καμουφλάζ που αυτή πλέον αποκτά παρουσιάζεται αισθητά βελτιωμένο, σε σχέση με το αντίστοιχο της απλής κρυπτογραφίας.

Το πρώτο γνωστό malware που έμελλε να χρησιμοποιήσει αυτήν την τεχνική ήταν ο ιός Whale.[237] Ο Whale έφερε μερικές δεκάδες από διαφορετικούς decryptors και ο ίδιος επέλεγε στην τύχη τον ποιον θα χρησιμοποιούσε κάθε φορά.

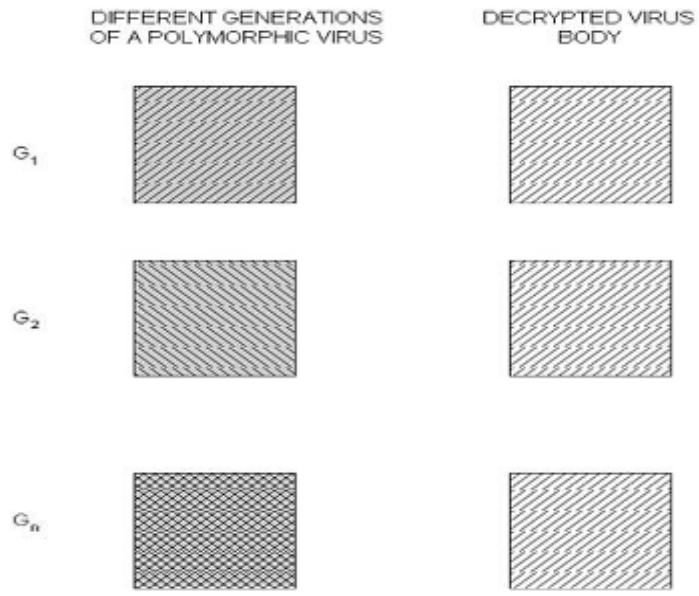
Πολυμορφισμός[238]

Ο πολυμορφισμός είναι μια ιδιαίτερα ανεπτυγμένη μέθοδος απόκρυψης, που χρησιμοποιεί την κρυπτογραφία με έναν ακόμη αποδοτικότερο τρόπο. Ως τεχνική αντλεί τη βασική λογική της από την αντίστοιχη του ολιγομορφισμού και αποτελεί άμεση επέκταση και αναβάθμιση του. Στην ουσία, *το σύνολο των εναλλακτικών decryptors παύει να είναι πλέον μικρό (άρα και δυνητικά αριθμήσιμο για ένα σύστημα ασφάλειας), αλλά γίνεται απαγορευτικό για την απαρίθμηση και δοκιμή όλων των πιθανών περιπτώσεων*. Οι δυνατές τροποποιήσεις του κακόβουλου κώδικα εξαιτίας της κρυπτογράφησης κάθε φόρα από διαφορετικούς μηχανισμούς φαντάζουν απεριόριστες. Ο ιός Tremor[239] για παράδειγμα εμφανίζει μια τεράστια ποικιλομορφία, την οποία οφείλει στα 6 δισεκατομμύρια ζεύγη από εναλλακτικούς encryptors-decryptors που διαθέτει.

[237] Κύρια, βιβλιογραφική αναφορά: [SZOR-ACVRD].

[238] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM], [SZOR-ACVRD], [LUDWIG-GBBCV], [TANENBAUM-MOS9], [JOHANSSON-CVTEALF], [PEARCE-VP], [MCCLOSKEY-CV].

[239] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM].



Σχήμα 17: Πολυμορφισμός

Για να επιτευχθεί ο επιθυμητός πολυμορφισμός στο λογισμικό οι σχεδιαστές ενός ιού ή σκουληκιού καταφεύγουν στη *χρήση αυτοματοποιημένων μηχανών μετάλλαξης (mutation engines), που αναλαμβάνουν την κατασκευή ενός παραλλαγμένου μηχανισμού (από)κρυπτογράφησης, κάθε φορά που αναπαράγεται το κακόβουλο πρόγραμμα*, εφαρμόζοντας κάποιες από μια *ποικιλία τεχνικών τροποποίησης* ή/και *επιλέγοντας από τις διαθέσιμες μια εντελώς καινούρια λογική και προσέγγιση στην μέθοδο (απο)κρυπτογράφησης*. Όσον αφορά τις τεχνικές παραγωγής μιας ισοδύναμης έκφρασης για κάποιον δεδομένο μηχανισμό (απο)κρυπτογράφησης οι παρακάτω μέθοδοι και οι συνδυασμοί αυτών συνεισφέρουν τα μέγιστα στην κατεύθυνση αυτή και αποτελούν καθιερωμένες προσεγγίσεις για μια πολυμορφική μηχανή μετάλλαξης:[240]

I. Αντικατάσταση (ακολουθίας) εντολών με ισοδύναμες (ακολουθίες) π.χ.

$$r1 = 1 \Leftrightarrow \begin{cases} clear & r1 \\ xor & r1, r1 \\ and & r1, 0 \\ mov & r1, 0 \end{cases} \quad \text{και} \quad x = 1 \Leftrightarrow \begin{cases} y = 21 \\ x = y - 20 \end{cases}.$$

II. Εναλλαγή της θέσης των εντολών στο σώμα (αλλαγή της σειράς εκτέλεσης), όταν αυτό είναι εφικτό και δεν επηρεάζει το αποτέλεσμα π.χ.

[240] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM], [SZOR-ACVRD].

$$\begin{matrix} r1 = 12 \\ r2 = r3 + r2 \\ r4 = r1 + r2 \end{matrix} \Leftrightarrow \begin{matrix} r2 = r3 + r2 \\ r1 = 12 \\ r4 = r1 + r2 \end{matrix} .$$

III. Χρήση εναλλακτικών καταχωρητών ή μετονομασία μεταβλητών π.χ.

$$\begin{matrix} r1 = 12 \\ r2 = 34 \\ r3 = r1 + r2 \end{matrix} \Leftrightarrow \begin{matrix} r3 = 12 \\ r1 = 34 \\ r2 = r3 + r1 \end{matrix} .$$

IV. Αναδιάταξη θέσης δεδομένων στην κύρια μνήμη.

V. Δημιουργία κώδικα «σπαγγέτι» με τη βοήθεια labels και εντολών τύπου goto π.χ.

$$\begin{matrix} & \\ start: & \\ \quad r1 = 12 & \\ \quad r2 = 34 & \\ \quad r3 = r1 + r2 & \end{matrix} \Rightarrow \begin{matrix} L1: & \\ \quad r2 = 34 & \\ \quad goto \quad L2 & \\ start: & \\ \quad r1 = 12 & \\ \quad goto \quad L1 & \\ L2: & \\ \quad r3 = r1 + r2 & \end{matrix} .$$

VI. Παρεμβολή «άχρηστου» κώδικα π.χ.

$$\begin{matrix} r1 = 12 \\ inc \quad r1 \\ inc \quad r1 \\ r1 = r1 - 2 \\ r2 = 34 \\ r3 = r1 + r2 \end{matrix} \Leftarrow \begin{matrix} r1 = 12 \\ r2 = 34 \\ r3 = r1 + r2 \end{matrix} \Rightarrow \begin{matrix} r5 = 42 \\ r1 = 12 \\ X: \\ \quad r2 = 34 \\ \quad dec \quad r \\ \quad bne \quad X \\ r3 = r1 + r2 \end{matrix} .$$

VII. Δημιουργία και παρεμβολή κώδικα κατά το χρόνο εκτέλεσης π.χ.

$$\begin{matrix} r1 = 12 \\ r2 = 34 \\ r3 = r1 + r2 \end{matrix} \Rightarrow \begin{matrix} r1 = 12 \\ r2 = 34 \\ generate \quad r3 = r1 + r2 \\ call \quad generated\_code \end{matrix} .$$

VIII. Χρήση διερμηνευόμενου κώδικα παρουσία εικονικών μηχανών π.χ. Java ή Python VM.

IX. (Πολύ)νηματικό ανάλογο επεξεργασίας π.χ.

$$
\begin{aligned}
&r1 = 12 \\
&r2 = 34 \\
&r3 = r1 + r2
\end{aligned}
\quad \Leftrightarrow \quad
\begin{aligned}
&start \quad thread \quad T \\
&r1 = 12 \\
&wait \quad for \quad signal \\
&r3 = r1 + r2 \\
&... \\
&T: \\
&\quad r2 = 34 \\
&\quad send \quad signal \\
&\quad exit \quad thread \quad T
\end{aligned}
$$

X. Άπλωμα/Μάζεμα κώδικα σε/από υπορουτίνες (code inlining/outlining).

XI. Διάσπαση/Ανάμιξη υπορουτινών π.χ.

```
...                          ...
call   S1                    call   S12
call   S2                    ...
...                          S12:
S1:                              r5 = 12
    r1 = 12                      r1 = 12
    r2 = r3 + r2                 r6 = r3 + r2
    r4 = r1 + r2                 r2 = 34
    return                       r4 = r5 + r6
                      ⇔          r3 = r1 + r2
S2:                              return
    r1 = 12                  ...
    r2 = 34
    r3 = r1 + r2
    return
...
```

Η λειτουργία του πολυμορφισμού περιγράφεται από την εξής απλή και επαναλαμβανόμενη στρατηγική, κατά τη φάση αναπαραγωγής:[241]

1. Το κακόβουλο πρόγραμμα εντοπίζει τον εαυτό του στη μνήμη (self-detection) και αποκρυπτογραφεί το κυρίως σώμα του με τη βοήθεια του εκάστοτε decryptor.
2. Ευρίσκεται ο κατάλληλος ξενιστής, εφόσον χρειάζεται[242].

[241] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM].

[242] Η πολυμορφική μετάλλαξη θα μπορούσε να συμβαίνει αυτόκλητα σε μια κακόβουλη εφαρμογή και ως διαδικασία εξέλιξης/προσαρμογής(3.2.6)/προστασίας του εν λόγω προγράμματος, χωρίς απαραίτητα να συνδέεται με ανάγκη αναπαραγωγής του κώδικα, με τη στενή έννοια της ιομορφικής μόλυνσης-διάδοσης, σε άλλον ξενιστή.

3. Η πολυμορφική μηχανή μετάλλαξης τίθεται σε λειτουργία και παράγει σαν έξοδο ένα νέο, τροποποιημένο μηχανισμό (απο)κρυπτογράφησης με κάποιο καινούριο ζεύγος encryptor-decryptor.
4. Δημιουργείται το νέο αντίγραφο ή στιγμιότυπο με την αναπαραγωγή του κυρίως σώματος του κακόβουλου κώδικα και την κρυπτογράφηση αυτού από τον decryptor του βήματος 2.

Η στρατηγική αυτή έχει κεντρική παρουσία και ρόλο καθ' όλη τη διάρκεια ζωής μιας πολυμορφικής απειλής.

Ένα πολύ χαρακτηριστικό παράδειγμα πολύπλοκης και αποτελεσματικής, πολυμορφικής μηχανής μετάλλαξης ήταν η MtE του Dark Anenger και του Mad Maniac, που κυκλοφόρησε κατά τη διάρκεια του καλοκαιριού του 1991 και ακολουθήθηκε αργότερα από μια άλλη, αναβαθμισμένη έκδοση στις αρχές του 1992[243]. Για τους αρχάριους συγγραφείς κακόβουλου λογισμικού, ήταν δύσκολο να γράψουν από μόνοι τους ένα αξιοπρεπές, πολυμορφικό πρόγραμμα. Έτσι, οι πιο προηγμένοι συγγραφείς ήρθαν στη διάσωσή τους. Η μηχανή MtE απελευθερώθηκε ως αντικείμενο που θα μπορούσε να συνδεθεί και να ενισχύσει οποιονδήποτε απλό ιό. Η μηχανή κατόπιν φροντίζει για την οικοδόμηση ενός πολυμορφικού στρώματος γύρω από τον εκάστοτε απλό ιό. Οι παράμετροι πολυμορφισμού περιελάμβαναν μεταξύ άλλων το τελικό μέγεθος του κώδικα, το σημείο εισόδου του κυρίως σώματος, το μέγεθος του decryptor και πλήθος άχρηστου κώδικα. Ως έξοδος στην προγραμματιστική κλήση για μετάλλαξη επιστρεφόταν μια πολυμορφική ρουτίνα αποκρυπτογράφησης (decryptor) και ένα κατάλληλα κρυπτογραφημένο ιομορφικό σώμα. Ο αντίκτυπος που προκάλεσε για την αντιϊομορφική βιομηχανία η χρήση της MtE ήταν μεγάλος. Οι περισσότερες μηχανές σάρωσης έπρεπε να περάσουν από επίπονες, αρχιτεκτονικές αναθεωρήσεις (προσθήκη δυνατοτήτων εξομοίωσης ή ενσωμάτωση δυναμικών, ευριστικών μεθόδων), ώστε να καταφέρουν να συλλάβουν θεωρητικά και πρακτικά τη φιλοσοφία της εν λόγω μηχανής μετάλλαξης.

Η αρχική άνθιση των πολυμορφικών μεθόδων έπιασε στον ύπνο τη βιομηχανία της ασφάλειας και οι πολυμορφικοί ιοί και σκουλήκια «αλώνιζαν» ανενόχλητοι τα πρώτα χρόνια εμφάνισης της μεθόδου. Με τον καιρό, η λογική και τα τρωτά του σημεία απο- ή ανακαλύφθηκαν και δεν άργησαν να κάνουν την εμφάνισή τους και οι πρώτες λύσεις προστασίας. Ο πολυμορφισμός είναι σήμερα *μια εγνωσμένης αξίας, κυρίαρχη πραγματικότητα* στο χώρο συγγραφής κακόβουλου λογισμικού και για το λόγο αυτό

[243] Κύρια, βιβλιογραφική αναφορά: [SZOR-ACVRD].

έχουν αναπτυχθεί ιδιαίτερα μέτρα ασφάλειας ειδικά για την αντιμετώπισή του, που παρουσιάζουν ικανοποιητική απόδοση.[244] Οι διαφορετικές τεχνοτροπίες βέβαια που τον καθιστούν εφικτό δεν έχουν πάψει ποτέ να τελούν υπό καθεστώς συνεχούς βελτιστοποίησης και γίνονται σταδιακά ολοένα και πιο εκλεπτυσμένες και αποτελεσματικές. Τα συστήματα ασφάλειας έχουν να κάνουν πλέον με μια *ώριμη τεχνολογία που κρύβει όμως αρκετούς ακόμη κινδύνους και χρίζει διαρκούς παρακολούθησης, έρευνας και ανάλυσης*.

Ολιγο- ή Πολυ-μεταμορφισμός

Η τεχνική αυτή αποτελεί τον *άμεσο συνδυασμό των μεθόδων και των αλγορίθμων τόσο του ολιγο- ή του πολυμορφισμού όσο και του μεταμορφισμού*, που μελετάται σε αμέσως επόμενο σκέλος. Το εκρηκτικό αυτό μίγμα συγκεντρώνει το σύνολο των πλεονεκτημάτων προστασίας και άμυνας των 2 συνιστωσών του, αλλά εμφανίζει επίσης 2 σημαντικά προβλήματα· η πολυπλοκότητα, τα σχεδιαστικά λάθη και η δαπάνη πόρων για την κατασκευή ενός πολυ-μεταμορφικού, κακόβουλου προγράμματος είναι συχνά διόλου ευκαταφρόνητοι παράγοντες, ενώ και το μέγεθος του παραγόμενου λογισμικού ξεφεύγει προς το παρόν κατά πολύ τα εσκαμμένα (π.χ. ογκώδεις μηχανές μετάλλαξης). Παρόλ' αυτά, τα εν λόγω υβρίδια συγκεντρώνουν συνεχώς την προσοχή και αποτελούν «*αιχμή του δόρατος» στις μεθόδους αυτοάμυνας*, οπότε *αναμενόμενη αν όχι σίγουρη είναι η συνεχής βελτιστοποίησή* της συνδυαστικής αυτής προσέγγισης και η προοπτική για μετατροπή της σε πρωτοκλασάτη απειλή. Για τους λόγους αυτούς, θα πρέπει συστήματα ασφάλειας να επιδεικνύουν τον απαραίτητο ρυθμό προετοιμασίας και μια διαρκή εγρήγορση ή/και ετοιμότητα.

Έξυπνη κρυπτογράφηση

Οι μέθοδοι κρυπτογράφησης, που μέχρι τώρα συζητήθηκαν, οδηγούν σε λογισμικό, που μόλις εντοπιστεί, είναι ευαίσθητο σε περαιτέρω ανάλυση. Το σημαντικότερο πρόβλημα δεν είναι η μέθοδος κρυπτογράφησης, επειδή αυτή μπορεί πάντα να ενισχυθεί· *το σημαντικότερο πρόβλημα είναι ότι ιοί και σκουλήκια κουβαλούν, στο σώμα τους ή πιο σωστά στην περιοχή του decryptor, πέρα από τον αλγόριθμο (απο)κρυπτογράφησης, και τα κλειδιά της αποκρυπτογράφησής τους*, που αποτελούν το «νούμερο ένα» στόχο για τα συστήματα ασφάλειας, μιας και η γνώση τους αποτελεί

[244] Όπως οι δυναμικού τύπου, ευριστικές τεχνικές σάρωσης και η εξομοίωση, που συζητώνται στο 4ο Κεφάλαιο (4.1.2).

εγγύηση και προϋπόθεση για μια αποδοτική ανάλυση του κακόβουλου προγράμματος.[245]

Αυτό μπορεί αρχικά να φανεί ως μια απαραίτητη αδυναμία, επειδή εάν ένας κρυπτογραφημένος ιός ή ένα σκουλήκι δε διαθέτει το κλειδί του, δεν μπορεί να αποκρυπτογραφήσει και να τρέξει τον χρήσιμο κώδικά του. Υπάρχουν, εντούτοις, πολλές δυνατότητες βελτιστοποίησης ή έκλειψης αυτής της φαινομενικής αδυναμίας, που μπορούν να εφαρμοστούν μεμονωμένα ή συνδυαστικά:

a) **Το κλειδί προέρχεται από το εξωτερικό περιβάλλον ενός μολυσμένου συστήματος**.[246] Ένας ιός ή ένα σκουλήκι μπορεί π.χ. να ανακτήσει το κλειδί από έναν ιστοχώρο ή εναλλακτικά να χρησιμοποιήσει μια διαδικτυακή μηχανή αναζήτησης για τον ίδιο σκοπό. Γενικά, οποιοδήποτε ρεύμα ηλεκτρονικών δεδομένων, που το κακόβουλο λογισμικό είναι σε θέση να παρακολουθεί, θα ήταν υποψήφιο για κανάλι βασικής παράδοσης του κλειδιού, ειδικά όμως προτιμώνται όσα είναι ευρύτερα διαδεδομένα, χαρακτηρίζονται από μεγάλο όγκο διακινούμενης πληροφορίας και είναι περισσότερο απίθανο να απαγορεύεται από πολιτικές ασφάλειας η πρόσβαση σε αυτά και η χρήση τους: μηνύματα ηλεκτρονικού ταχυδρομείου ή USENET, στιγμιαία μηνύματα IM ή IRC συνομιλίες και δίκτυα διαμοιρασμού αρχείων αποτελούν ιδανικούς εκπροσώπους αυτής της ομάδας.
b) **Το κλειδί προέρχεται από το εσωτερικό ενός μολυσμένου συστήματος**. Με χρήση *περιβαλλοντικής παραγωγής κλειδιού (environmental key generation)*[247], το κλειδί αποκρυπτογράφησης μπορεί να δημιουργείται κάθε φορά δυναμικά από συνδυασμούς στοιχείων που είναι παρόντα με διάχυτο τρόπο στο ενδότερο περιβάλλον του συστήματος-στόχου, όπως π.χ.:

    - Το DNS ή NetBIOS όνομα ενός υπολογιστικού συστήματος.

---

[245] Τα κρυπτογραφημένα έκδοχα του οπλολογισμικού στην πλειονότητα τους φέρουν τα κλειδιά για την αποκρυπτογράφησή τους, κάπου μέσα στον κώδικα του εκάστοτε decryptor. Αν κάποιος ερευνητής ή ένα σύστημα προστασίας θέλουν για κάποιον λόγο να αποφύγουν τις εν γένει χρονοβόρες επιθέσεις λεξικογραφικού ή ωμού τύπου πάνω στο σύστημα κρυπτογράφησης που χρησιμοποιήθηκε, τότε μπορούν να εξετάζουν την περιοχή των decryptors για την εξαγωγή σχεδόν πάντοτε χρήσιμων πληροφοριών αποκρυπτογράφησης, αλλά ακόμη και των ίδιων των κλειδιών. Ακόμα και οι προαναφερόμενες, τυχαιώδεις επιθέσεις είναι πιο αποδοτικές, εάν πολωθούν/τροφοδοτηθούν κατάλληλα με δεδομένα ευρισκόμενα στην περιοχή ενός decryptor.

[246] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM].

[247] Πηγή: "Environmental Key Generation towards Clueless Agents", James Riordan and Bruce Schneier, 1998, διαθέσιμο από το δεσμό http://www.schneier.com/paper-clueless-agents.pdf.

- Τις ενδείξεις χρόνου ή ημερομηνίας.
- Δεδομένα του συστήματος (π.χ. περιεχόμενα αρχείων).
- Τον τρέχοντα λογαριασμό χρήστη.
- Τη ρύθμιση γλώσσας του περιβάλλοντος χρήσης.

Ο αλγόριθμος του decryptor αναζητά το κλειδί με βάση τον κατάλληλο κάθε φορά συνδυασμό των παραπάνω παραγόντων, που ο συγγραφέας έχει επιλέξει ως μεταβλητές παραμέτρους.

Η μέθοδος αυτή καθιστά πολύ εύκολη την στόχευση σε συγκεκριμένα άτομα ή ομάδες, ακριβώς επειδή χρησιμοποιεί μεταβλητές και τιμές παραμέτρων τοπικές και χαρακτηριστικές (ενδεχομένως μοναδικές) για το εκάστοτε σύστημα.

Συνδυασμένη με ισχυρή κρυπτογράφηση ή/και προηγμένες πολυμορφικές προσεγγίσεις, η περιβαλλοντική παραγωγή κλειδιών δύναται να καταστήσει το αυτοαναπαραγόμενο, κακόβουλο λογισμικό μη αναλύσιμο και αναγνωρίσιμο, ακόμα και αν η δράση του εντοπιστεί από κάποιο σύστημα ασφάλειας, όπως επισημαίνει χαρακτηριστικά και θεμελιώνει/υποστηρίζει με μαθηματικό τρόπο (αποδεικνύει μια εκθετική πολυπλοκότητα στην ανάλυση-ανίχνευση ενός τέτοιου προγράμματος) ο ερευνητής Eric Filiol, στην εργασία του με θέμα τον ισχυρά κρυπτογραφημένο, proof-of-concept ιό Bradley[248]. Απαραίτητη προϋπόθεση ως γνωστόν και σχεδόν μονόδρομος για οποιαδήποτε σε βάθος ανάλυση κάθε κρυπτογραφημένου προγράμματος είναι η αποκρυπτογράφησή του. Ένας στόχος, όμως, δεν είναι σε θέση να γνωρίζει εκ των προτέρων ότι κατέχει τη συνταγή για το κλειδί αποκρυπτογράφησης, αλλά ακόμη και να το υποθέσει, το να απομονώσει από την πληθώρα των επιλογών τα ακριβή συστατικά που χρησιμοποιήθηκαν φαντάζει εξαιρετικά πολύπλοκη και κοπιαστική διεργασία. Σε αυτήν την περίπτωση, η μόνη πραγματική ελπίδα αποκρυπτογράφησης βρίσκεται σε μια «πτωχή» επιλογή κλειδιού. Ένα κλειδί με σχετικά μικρό εύρος πιθανών τιμών (π.χ. μόνη παράμετρος η ρύθμιση γλώσσας) θα ήταν δυνατό να υποκύψει σε «σπάσιμο» μέσω εξαντλητικών επιθέσεων «ωμής δύναμης» (brute-force attacks).

Απαραίτητη σημείωση: Η ενδεχόμενη ύπαρξη εργαλείων κρυπτογράφησης ή υποδομής δημοσίου κλειδιού στο υπό επίθεση σύστημα διευκολύνει περαιτέρω τη δυναμική, περιβαλλοντική δημιουργία των κλειδιών αποκρυπτογράφησης με

[248] Κύρια, βιβλιογραφική αναφορά: [FILIOL-BRADLEY].

τη δυνατότητα κλήσης εξειδικευμένων, εξωτερικών, προγραμματιστικών μεθόδων κρυπτογράφησης.[249] Σημαντικού ρόλου μπορεί να είναι εξάλλου και ο συνακόλουθος, πιθανός, εξαιτίας ανεπαρκούς φύλαξης, εντοπισμός στο προσβεβλημένο σύστημα ανεξάρτητων, έμπιστων και έτοιμων για χρήση κλειδιών κρυπτογράφησης.[250]

c) **Το κλειδί παράγεται με τυχαίο τρόπο κατά το στάδιο της κρυπτογράφησης** και κατά την αποκρυπτογράφηση, ο βρόχος του decryptor προσπαθεί με εξαντλητικό τρόπο (επίθεση «ωμής δύναμης») να το εντοπίσει (brute-force decryption).[251] Προφανώς, μια τέτοια προσέγγιση έχει νόημα για συγκεκριμένο μήκος κλειδιού, που δεν κάνει απαγορευτική μια μέθοδο λάθους-και-επανάληψης, και είναι γεγονός πως, για προφανείς λόγους, παρέχει μια γενικά ασθενέστερη, σε σχέση με τις προηγηθείσες στην ανάλυση μεθόδους, λύση[252].

Παράδειγμα ενός τέτοιου αλγορίθμου αποκρυπτογράφησης είναι ο γνωστός για τις ιομορφικές του χρήσεις RDA (Random Decryption Algorithm)[253].

iii. Μεταμορφισμός (Metamorphism)[254]

Ο Igor Muttik της McAfee εξήγησε τη μεταμορφική απειλή με τον πιο σύντομο και απλό τρόπο:[255]

"Μεταμορφισμός είναι να έχουμε κάτι σαν πολυμορφισμό και στο κυρίως σώμα" (και όχι μόνο στον μηχανισμό (απο)κρυπτογράφησής του).

---

[249] Σε μια τέτοια περίπτωση, το οπλολογισμικό μπορεί να μην περιέχει καν τις ρουτίνες κρυπτογράφησης/αποκρυπτογράφησης στο σώμα του, αλλά να τις καλεί προγραμματιστικά μέσω των διεπαφών των κρυπτογραφικών προγραμμάτων, που εδρεύουν στο σύστημα. Κάτι τέτοιο όχι μόνο αποκρύπτει επιτυχώς τα κλειδιά, αλλά και την ίδια τη φιλοσοφία/μέθοδο αποκρυπτογράφησης, όπως επίσης αποσυμφορεί το κακόβουλο πρόγραμμα από τις γενικά ογκώδεις και χρονοβόρες, εσωτερικές ρουτίνες κρυπτογραφίας.

[250] Ένα υπολογιστικό σύστημα το οποίο έχει παραμετροποιηθεί έτσι, ώστε να χρησιμοποιεί κρυπτογραφικές συναρτήσεις και μεθόδους και οι χρήστες του να έχουν συνηθίσει να χρησιμοποιούν ή να έρχονται σε επαφή με κρυπτογραφημένα δεδομένα, είναι έτσι και αλλιώς πιο ευπαθές στο να δεχθεί ανυποψίαστα τη δράση ενός κρυπτογραφημένου, κακόβουλου προγράμματος, Ένα τέτοιο πρόγραμμα μπορεί να γίνει ακόμη πιο αποδοτικό και διακριτικό επιλέγοντας προς χρήση τυχόν αφύλακτα, νόμιμα και αποδεκτά κλειδιά κρυπτογραφίας των ίδιων των χρηστών, που είναι πολύ πιθανό να εντοπίσει σε ένα τέτοιο σύστημα και που ένας μηχανισμός προστασίας μπορεί και να μη λαμβάνει επίτηδες υπόψιν του στις ανιχνεύσεις ύποπτης δραστηριότητας.

[251] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM].

[252] Εφόσον μπορεί το πρόγραμμα να «σπάσει» το μηχανισμό κρυπτογράφησής του, το ίδιο θα μπορεί να κάνει δυνητικά και οποιοδήποτε σύστημα δίωξής του.

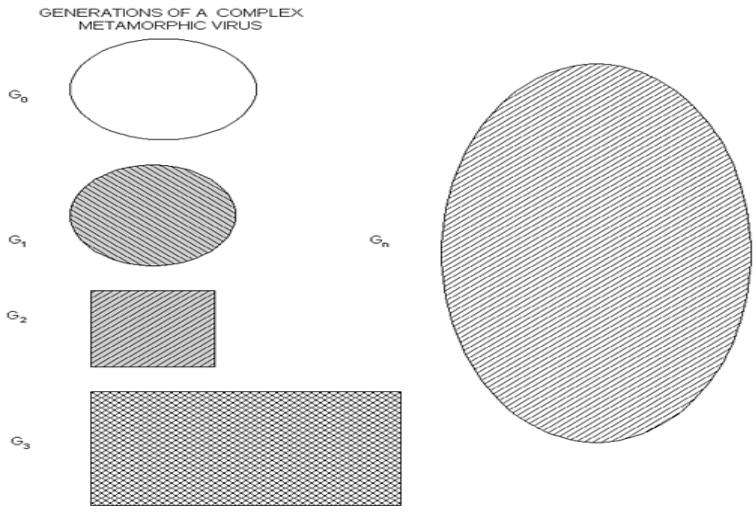
[253] Κύρια, βιβλιογραφική αναφορά: [SZOR-ACVRD].

[254] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM], [SZOR-ACVRD], [MCCLOSKEY-CV].

[255] Πηγή: "The New 32-bit Medusa", Peter Szor, Virus Bulletin December 2000, διαθέσιμο από το δεσμό mirror.sweon.net/madchat/vxdevl/papers/avers/medusa.pdf.

Τα αυτοαναπαραγόμενα όπλα, που κάνουν χρήση καθαρού μεταμορφισμού (χωρίς συνδυασμούς με πολυμορφικές τεχνοτροπίες), δε διαθέτουν κανένα decryptor (δεν είναι κρυπτογραφημένα), ούτε όμως έχουν και σταθερό κώδικα κυρίως σώματος μεταξύ των διαφορετικών αντιγράφων ή στιγμιοτύπων (όπως συμβαίνει με τα πολυμορφικά malware). *Η απόκρυψη που προσφέρεται έγκειται στη διαφοροποίηση αυτή του κακόβουλου σώματος, μεταξύ των διαφορετικών γενεών του λογισμικού*.

Τα μεταμορφικά, κακόβουλα προϊόντα (αντίγραφα ή στιγμιότυπα) μετατρέπουν το σχήμα τους από τη μια μορφή στην άλλη, προσπαθώντας η κάθε γενιά να έχει όσο πιο ελάχιστα σημάδια συγγένειας-συνάφειας με τις προηγούμενές της. Για να πετύχουν κάτι τέτοιο υιοθετούν διάφορες προσεγγίσεις τροποποίησης του σώματος, που όπως και στον πολυμορφισμό, συνήθως τοποθετούνται υπό τη λογική και τη σκέπη κάποιας *αυτοματοποιημένης μηχανής μετάλλαξης*.[256] Οι μεταμορφικές engines, λοιπόν, -που μοιάζουν και λειτουργικά με τις αντίστοιχες πολυμορφικές, με την εξαίρεση ότι δεν απασχολούνται καθόλου με μηχανισμούς (απο)κρυπτογράφησης και την όποια τροποποίηση ή αλλαγή αυτών μεταξύ των γενεών- είναι επιφορτισμένες σε κάθε αναπαραγωγή με τη *γενετική τροποποίηση του συνόλου του κακόβουλου κώδικα του σώματος μέσω διαφόρων μεθόδων*, εκ των οποίων οι κυριότερες είναι επεκτάσεις των αντίστοιχων τεχνικών παραλλαγής κώδικα, που συζητήθηκαν προηγουμένως στο τμήμα του πολυμορφισμού και αφορούσαν τη μετατροπή συγκεκριμένου μηχανισμού (απο)κρυπτογράφησης σε κάποια τροποποιημένη, ισοδύναμη μορφή του· εδώ όμως η μέθοδος παραλλαγής επιλαμβάνεται του συνόλου του κώδικα του κακόβουλου, κυρίως σώματος και εφαρμόζεται σε ολόκληρο αυτό το σύνολο.



Σχήμα 18: Μεταμορφισμός

[256] Κύρια, βιβλιογραφική αναφορά: [WALENSTEIN-DSMM], [WEBSTER_MALCOLM-DMCVAS].

Ο μεταμορφισμός μπορεί, με σχετικά εύκολο τρόπο, *να ενισχυθεί περαιτέρω με χρήση απλής ή πιο ισχυρής και προηγμένης κρυπτογραφίας*. Ο δραστικός συνδυασμός μεταμορφισμού και κρυπτογράφησης μπορεί να παρέχει σημαντικά οφέλη, αλλά μπορεί να επιβαρύνει τόσο το παραγόμενο λογισμικό από πλευράς όγκου, όσο και το σχεδιαστή του από πλευράς πολυπλοκότητας, οδηγώντας τον ακόμη και σε τεχνικά λάθη. Ο ολιγο- και ο πολυ-μεταμορφισμός, όπως είδαμε, σε προηγούμενο σκέλος, αποτελούν την εφαρμογή των αντίστοιχων τεχνικών για τροποποιημένους encryptors-decryptors στο ευρύτερο, μεταμορφικό υπόδειγμα δράσης· το κακόβουλο πρόγραμμα είναι πλέον κρυπτογραφημένο και σε κάθε αναπαραγωγή είτε ο μηχανισμός (από)κρυπτογράφησής του πρέπει να αλλάζει με ολιγομορφικό τρόπο είτε η μηχανή μετάλλαξής του πρέπει να μπορεί να παράγει και ένα διαφορετικό ζευγάρι encryptor-decryptor. Η επικινδυνότητα μιας τέτοιας απειλής είναι σημαντική και δεν (πρέπει να) περνάει απαρατήρητη.

Προφανώς, η τεχνική του μεταμορφισμού, γενικότερα, αποτρέπει με ιδιαίτερα αισθητό τρόπο την αποτελεσματική λειτουργία των σαρωτών, αλλά και άλλων συστημάτων ασφάλειας, καθιστώντας τη σχετική τους επιτυχία στον εντοπισμό και την αναγνώριση μιας κακόβουλης, μεταμορφικής απειλής σε αμφίβολη, εξαιρετικά επίπονη διεργασία, χωρίς την ανάπτυξη ευφυέστερων μεθόδων πρόληψης και έγκαιρης, ακριβούς αναγνώρισης, όπως μας πληροφορούν και οι ερευνητές Mark Stamp και Wing Wong στην πρόσφατη (2006) εργασία τους με θέμα τη χρήση εκτεταμένων συγκρίσεων και δεικτών ομοιότητας (similarity indexes), προκειμένου να παράγονται καλύτερα αποτελέσματα ανίχνευσης νέων ή τρέχοντων, μεταμορφικών προγραμμάτων[257].

Τυπικό παράδειγμα μεταμορφικού ιού είναι ο σχετικά πρόσφατος Simile, που εκτός των άλλων είναι και ικανός μόλυνσης διαφορετικών τύπων αρχείων και σε διαφορετικές πλατφόρμες Λ/Σ (Windows PE, Linux ELF).[258] Η μηχανή μετάλλαξης του εν λόγω κατασκευάσματος είναι πραγματικά τεράστια (η μεγαλύτερη από όλες μέχρι στιγμής) και καταλαμβάνει περί τα 3,5 Mbytes στην κύρια μνήμη ενός Η/Υ, ενώ χρησιμοποιεί και ορισμένες, έξυπνες τακτικές τυχαιωδών επιλογών εξέλιξης[259] του κώδικα με βάση πιθανοτικά μοντέλα.

---

[257] Κύρια, βιβλιογραφική αναφορά: [STAMP_WONG-HME].

[258] Πηγή: "An Analysis of Simile", Adrian Marinescu, 2003, διαθέσιμο από το δεσμό http://www.securityfocus.com/infocus/1671.

[259] Βλέπε και την περιγραφή της εξέλιξης/μετάλλαξης ως μεθόδου παθητικής αυτοάμυνας λίγο πιο κάτω.

iv. Θόλωση σημείου εισόδου (EPO)[260]

Η μέθοδος αυτή είναι μια *ιδιαίτερα ιδιοφυής, κατεξοχήν ιομορφική τεχνική* και ως τέτοια απαντάται συχνότατα στους ιούς και εμφανίζεται σπανιότερα, αλλά με μεγάλη δυναμική, σε περιπτώσεις σύγχρονων, συνδυασμένων απειλών (blended threats).

Τα κακόβουλα, αυτοαναπαραγόμενα προγράμματα, που κάνουν χρήση θόλωσης του σημείου εισόδου, δεν τροποποιούν το φυσιολογικό και αναμενόμενο σημείο (διεύθυνση στην κύρια μνήμη) εισόδου μιας εφαρμογής όταν τη μολύνουν, ούτε αλλάζουν τον κώδικα στο σημείο εισόδου. Αντ' αυτού, *αλλάζουν τον κώδικα εντός του προγράμματος κατά τέτοιο τρόπο, ώστε το κακόβουλο πρόγραμμα να παίρνει τον έλεγχο με τρόπο που μοιάζει ή είναι τυχαίος*. Πάντοτε, κάπου μέσα στον κώδικα ενός ξενιστή, είτε υπάρχει αλλαγή στη θέση του σημείου εισόδου του από την πρωτογενή και αναμενόμενη στη θέση όπου βρίσκεται ο κακόβουλος κώδικας είτε γίνεται πήδημα (JMP) στην αρχή του κακόβουλου κώδικα ή/και καλείται (CALL) προγραμματιστικά ως μέθοδος μια κακόβουλη ρουτίνα. Στην ουσία, η τεχνική EPO καταργεί την όποια μετακίνηση της φυσιολογικής θέσης εκκίνησης του ξενιστή και προχωρά ένα βήμα παραπάνω τοποθετώντας τις όποιες JMP και CALL *εντολές κλήσης κακόβουλου κώδικα μακριά από τον κώδικα που βρίσκεται πλησίον του σημείου εισόδου, σε πρακτικά ή φαινομενικά τυχαιώδεις θέσεις*.[261] Ο ξενιστής ξεκινά από την κανονική του θέση εισόδου εκτελώντας τις όποιες μη επιβλαβείς εντολές του και σε κάποιο σημείο της ροής εκτέλεσης -ιδανικά αρκετά μακριά από το σημείο εισόδου- παρεμβάλλεται μια κλήση JMP ή CALL προς κάποιο σημείο όπου εδρεύει κακόβουλος κώδικας και επομένως αυτός αποκτά τον έλεγχο. Αφού ολοκληρωθεί η όποια επιβλαβής δράση του, το πρόγραμμα είτε τερματίζει είτε επιστρέφεται (με JMP ή RET) ο έλεγχος στην κυρίως δράση του ξενιστή -όχι απαραίτητα στο ίδιο σημείο, όπου σταμάτησε. Για ευνόητους λόγους, το EPO πρότυπο αυτοάμυνας απορρίπτει εντελώς τις overwriting μεθόδους ιομορφικής αντιγραφής, ενώ επίσης αποφεύγει και την prepending προσέγγιση που τις περισσότερες φορές βρίσκεται να αλλοιώνει τις πληροφορίες εισόδου-εκκίνησης του ξενιστή.

Η λογική και η αποτελεσματικότητα των EPO προσεγγίσεων ενισχύεται περαιτέρω από την παρουσία και χρήση πολυμορφικών και μεταμορφικών αλγορίθμων απόκρυψης, καθώς και από μια ενδεχόμενη υπονόμευση API κλήσεων προς εγγενείς μεθόδους του ξενιστή ή ακόμα και προς το ίδιο το Λ/Σ[262]. Ακόμα, η εφαρμογή EPO τεχνικών παρουσιάζεται ακόμα πιο επωφελής για την άμυνα του κακόβουλου προγράμματος

---

[260] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM], [SZOR-ACVRD].

[261] Κύρια, βιβλιογραφική αναφορά: [SZOR-ACVRD].

[262] Βλέπε και υπονόμευση Λ/Σ, στις ενεργητικού τύπου μεθόδους αυτοάμυνας, σε μετέπειτα σκέλος του παρόντος εδαφίου.

προκειμένου για ογκώδεις ξενιστές, όπου οι κλήσεις JMP ή CALL εκμεταλλευόμενες το μεγάλο μέγεθος διασπείρονται τυχαίως και χάνονται στο βάθος του κώδικα του μολυσμένου προγράμματος.

Ήδη από το 1995 προγράμματα όπως η Olivia (1997) έκαναν χρήση τεχνικών EPO, προκειμένου να αποφεύγουν την ανίχνευση μέσω απλής σάρωση, αλλά και να αντιπαρέρχονται τις έκτοτε διαδεδομένες στατικές, ευριστικές τεχνικές.[263] Η Olivia έκανε χρήση της κωδικεντολής 0x68 (Intel 286 PUSH opcode) για να προωθήσει μια τιμή μεγέθους 1 word στη στοίβα και κατόπιν καλούσε την εντολή 0xC3 (RET), πράγμα που έδινε αποτελεσματικά και με ανύποπτο τρόπο τον έλεγχο στον κυρίως ιομορφικό κώδικα μέσω εξαγωγής/ανάσυρσης από τη στοίβα της εκεί προωθημένης διεύθυνσης μνήμης του decryptor του ιού, όπως φαίνεται παρακάτω σε κώδικα Assembly:

(0x68) PUSH offset DECRYPTOR

(0xC3) RET.

Αποτέλεσμα μιας επιτυχημένης χρήσης EPO μεθόδων είναι η *σχετική αδυναμία σύγχρονων ανιχνευτών κακόβουλου λογισμικού να εντοπίσουν και να αναγνωρίσουν επιτυχώς μια μόλυνση σε κάποιο αρχείο δεδομένων, που περιλαμβάνει EPO κώδικα*. Η αδυναμία αυτή πηγάζει από το σχεδιασμό μιας μεγάλης πλειοψηφίας των τρέχοντων αλγορίθμων ανίχνευσης -είτε των βασισμένων σε υπογραφές είτε των πιο ευριστικών- που ελέγχουν για αλλοιώσεις ή ύποπτο κώδικα στα σημεία εισόδου των εκτελέσιμων αρχείων, χωρίς να πραγματοποιούν εξαντλητικές σαρώσεις του συνολικού περιεχομένου των αρχείων, που άλλωστε κοστίζουν και από πλευράς αριθμού και χρόνου διάρκειας λειτουργιών I/O στα μέσα αποθήκευσης. Ακόμα και η εξομοίωση ύποπτων προγραμμάτων, που προσφέρουν κάποια συστήματα ασφάλειας, εμφανίζεται σήμερα, σε πολλές περιπτώσεις, να περιορίζεται σε μικρό τμήμα εντολών περί του σημείου εισόδου των προγραμμάτων. Τη στρατηγική αυτή του μειωμένου όγκου της ανίχνευσης ή εξομοίωσης προώθησε, πέρα από την προφανή, συγκριτικά μεγαλύτερη οικονομία πόρων και ταχύτητα που εξασφαλίζει, και η εμφάνιση και αρχική επιτυχία των πρώτων γενεών πολυμορφικών ιών, των οποίων οι μεταλλάξεις δεν άφηναν ιδιαίτερα περιθώρια εύρεσης κοινών τμημάτων κώδικα για ταυτοποίηση οπουδήποτε στο σώμα τους, πρόδιδαν όμως, όπως αποδείχθηκε, την παρουσία του ιού με ύποπτο κώδικα στα σημεία εισόδου. Οι ανιχνευτές κακόβουλου λογισμικού φρόντισαν να αφομοιώσουν τη νέα, αποδοτική τεχνική η οποία αποδείχθηκε ιδιαίτερα επιτυχημένη, καθώς πολλά ήταν τα κακόβουλα

[263] Κύρια, βιβλιογραφική αναφορά: [SZOR-ACVRD].

προγράμματα που αλλοίωναν τη κανονική θέση ή τον κώδικα στο σημείο εισόδου των ξενιστών προκειμένου να αποκτήσουν τον έλεγχο. Το ίδιο έπραξαν και τα συστήματα εξομοίωσης υπολογίζοντας στην ταχύτατη ανάδυση των κακόβουλων εντολών, που θα πυροδοτούσε μια απευθείας ή μια γρήγορη κλήση στον κακόβουλο κώδικα από το σημείο εισόδου του προγράμματος. Η απάντηση όμως από την πλευρά του κακόβουλου λογισμικού δεν άργησε να έρθει, είναι καταλυτική και πολλά υποσχόμενη και λέγεται entry point obfuscation ή obscuring.

v. Άλλες μέθοδοι

Ένα κακόβουλο πρόγραμμα, που κάνει χρήση τεχνικών καμουφλάζ και σίγασης, δεν περιορίζεται στο να αποκρύψει μόνο τον εαυτό του, αλλά προσπαθεί να συγκαλύψει κατά το δυνατόν και την ίδια την προσβολή ενός συστήματος, από τα «μάτια» εχθρικών δυνάμεων.

Μερικά παραδείγματα κατεξοχήν παθητικών stealth μοτίβων δράσης, που ξεφεύγουν από τα πλαίσια της κλασσικής κρυπτογραφίας ή των υπόλοιπων μεθόδων απόκρυψης των αυτοαναπαραγόμενων, κακόβουλων προγραμμάτων, παρουσιάζονται συνοπτικά παρακάτω:

- Ιοί (ή συνδυασμένες απειλές) διατηρούν *αναλλοίωτες τις χρονοσφραγίδες (timestamps)* των αρχείων που μολύνουν, για να μη δείχνουν πρόσφατα τροποποιημένα.[264] Το ίδιο γίνεται και με *τα υπόλοιπα, ταυτοτικά (ιδιο)χαρακτηριστικά των αρχείων πριν τη μόλυνση*, ακόμη και της πληροφορίας του μεγέθους τους, που ενδέχεται τις πιο πολλές φορές να αλλάζει λόγω της παρεμβολής του ιομορφικού κώδικα.
- Δικτυακή επικοινωνία εκτελείται μόνο με *χρήση επιτρεπόμενων πρωτοκόλλων και θυρών επικοινωνίας, ώστε η παραγόμενη κίνηση να μην κινεί υποψίες στα υπό επίθεση συστήματα.*[265] Όσο πιο συνηθισμένος και διαδεδομένος ο τύπος επικοινωνίας που χρησιμοποιείται, τόσο μεγαλύτερος ο βαθμός απόκρυψης της κακόβουλης δραστηριότητας.

[264] Η πρακτική αυτή εξασφαλίζει προστασία έναντι των απλούστερων εκδοχών ελεγκτών ακεραιότητας, που δεν κάνουν χρήση κρυπτογραφικής σύνοψης όλου του όγκου των αρχείων, που θα φανέρωνε ή έστω υποψίαζε για μια αλλοίωση, όσο κρυμμένα και αν ήταν τα χαρακτηριστικά της. Περισσότερα για τους integrity checkers, στο εδάφιο 4.1.4 του τέταρτου μέρους.

[265] Με τρόπο παραπλήσιο στη λογική με εκείνον που είδαμε πως χρησιμοποιούν τα παθητικά ή παθητικής ανίχνευσης σκουλήκια, στο εδάφιο 3.2.2.

- Γίνεται ευρεία *χρήση κρυφών και διακριτικών καναλιών (covert channels)* διάδοσης και επικοινωνίας καθώς και των λοιπών διευκολύνσεων που προσφέρουν οι διάφορες, στεγανογραφικές μέθοδοι[266].

2. Θωράκιση (Armoring)

Η θωράκιση ως μέθοδος προστασίας επιτρέπει στο κακόβουλο, αυτοαναπαραγόμενο λογισμικό να προβάλλει ισχυρή, παθητικού τύπου, αντίσταση στις διάφορες προηγμένες μεθόδους ανίχνευσης, που κατά καιρούς επιχειρεί, *πέραν της αναγκαίας και τυπικής σάρωσης*, να του αντιπαραθέσει η αντιϊομορφική βιομηχανία και τεχνολογία. Μην ξεχνάμε, άλλωστε, πως κατεξοχήν τρόπους αντιμετώπισης μιας απλής σάρωσης προσφέρουν άφθονους και επιτυχημένους και οι τεχνικές απόκρυψης, που προηγήθηκαν. Εδώ, όμως, υφίσταται ανάγκη για κάποιο μέτρο προστασίας που να έρχεται ως απευθείας απάντηση παθητικής άμυνας, κόντρα στις συγκεκριμένες, τεχνολογικές καινοτομίες.

Ανατρέχοντας στο Κεφάλαιο 2[267], διαπιστώνει κανείς πως οι πλέον βασικές από τις προσεγγίσεις, που ακολουθούν πιο συχνά τα προγράμματα και τα υλισμικά ασφάλειας στη μάχη για την έγκαιρη διάγνωση και αναγνώριση μιας μόλυνσης από κακόβουλα όπλα και που ξεφεύγουν από τα συνηθισμένα πλαίσια μιας απλής σάρωσης, είναι οι ακόλουθες πέντε:

Α. Ευριστική σάρωση και ανάλυση.

Β. Εξομοίωση.

Γ. Αποσφαλμάτωση προγράμματος.

Δ. Αποσυναρμολόγηση κώδικα.

Ε. Τεχνικές προσέλκυσης και παγίδευσης κακόβουλης απειλής.

Αποτέλεσμα της εισαγωγής των μεθόδων αυτών στο σκηνικό του εντοπισμού κακόβουλων προγραμμάτων ήταν η ανάπτυξη ευφυών αντιδράσεων στους κόλπους του κακόβουλου προγραμματισμού, που στόχο είχαν τη δημιουργία κατάλληλων, νέων προκλήσεων, που αποτελεσματικά θα απαντούσαν με αντισταθμιστικό τρόπο στις τεχνικές αυτές. Για παράδειγμα, αναφέρουμε τον θωρακισμένο ιό W95/Vulcano[268] που χρησιμοποιούσε τη μη τεκμηριωμένη εντολή SALC των επεξεργαστών μάρκας Intel στο

[266] Περισσότερος λόγος για την προσέγγιση αυτή γίνεται και στο Κεφάλαιο 5, στο ξεχωριστό εδάφιο 5.1.1.

[267] Στο εισαγωγικό εδάφιο 2.4.4

[268] Κύρια, βιβλιογραφική αναφορά: [SZOR-ACVRD].

τμήμα αποκρυπτογράφησης του πολυμορφικού του σώματος, ως αποδοτικό τρόπο αντιμετώπισης των μηχανών εξομοίωσης ορισμένων, αντιϊομορφικών συστημάτων που δεν την αναγνώριζαν και έτσι δεν μπορούσαν να τη χειριστούν (κάποιοι εξομοιωτές «κόλλαγαν» στην εντολή, ενώ άλλοι που απλά την προσπερνούσαν δεν κατάφερναν να ταυτοποιήσουν τον ιό). Ως αποτέλεσμα, ο ιός Vulcano άδραξε την ευκαιρία που του παρείχε ο εγγενής μηχανισμός αντιεξομοίωσης και έδρασε ανεξέλεγκτα (in the wild) για αρκετό διάστημα.

Η θωράκιση αφορά στην ανθεκτικότητα ή παθητική αντίσταση που προσφέρουν ορισμένες ρουτίνες αυτοάμυνας, απέναντι στις διαφορετικές, αντιϊομορφικές και γενικότερα αντικακόβουλες «απειλές», που αναφέρθηκαν προηγουμένως.

i. Αποφυγή εξομοίωσης (Anti-emulation)[269]

Όπως ήδη είδαμε, οι EPO τεχνικές μπορούν να τείνουν χείρα βοηθείας στην παθητική αντιμετώπιση λογισμικού εξομοίωσης με την καθυστέρηση στη φόρτωση του ιομορφικού κώδικα, που εν γένει τις διακρίνει.

Από την άλλη, οι διάφορες μέθοδοι εισαγωγής «άχρηστου» κώδικα, γνωστές και στις πολυμορφικές ή μεταμορφικές μεταλλάξεις, μπορούν επίσης να φανούν χρήσιμες στην παρακώλυση μιας εξομοίωσης ενός κακόβουλου προγράμματος. Ο πρόσθετος, άσχετος κώδικας πρέπει να έχει ικανό μέγεθος και ζητούμενη λειτουργικότητα, ώστε να καταλαμβάνει μεγάλο χρόνο επεξεργασίας, οδηγώντας ιδανικά σε εγκατάλειψη λόγω υπερβάσης χρονικών ορίων τερματισμού την όποια απόπειρα εξομοίωσης. Η λειτουργία που αυτός επιτελεί δεν πρέπει να φέρει ίχνος κακόβουλης ενέργειας, το αντίθετο μάλιστα να φέρεται ως χρήσιμη επεξεργασία και να μην κινεί υποψίες.

Ακόμη, η χρήση κρυπτογραφίας μπορεί να αποτελέσει σύμμαχο στην αντι-εξομοίωση, αρκεί ο μηχανισμός (από)κρυπτογράφησης να είναι όσο το δυνατόν τυχαιώδης όπως λ.χ. συμβαίνει με κάποια είδη malware που χρησιμοποιούν μεθοδολογία λάθους-και-επανάληψης για να εντοπίσουν τα κατάλληλα κλειδιά αποκρυπτογράφησης (brute-force decryption) ή εξοντωτικός π.χ. περιλαμβάνοντας ακολουθιακά πολλαπλούς decryptors ή εκτεινόμενος σε μεγάλο εύρος κώδικα.

Μια άλλη (έξυπνη) ιδέα για την αποφυγή της εξομοίωσης είναι να καταφεύγει κανείς σε μοντέλα κακόβουλου κώδικα που δεν εκτελείται πάντοτε και η εκτέλεση του οποίου αποτελεί τυχαία μεταβλητή, που ακολουθεί συγκεκριμένη κατανομή πιθανότητας. Η κακόβουλη δράση και η αναπαραγωγή σε ένα τέτοιο πρόγραμμα άλλοτε θα

[269] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM], [SZOR-ACVRD].

ενεργοποιούνται και άλλοτε όχι, με βάση κάποιο πείραμα τύχης ή μια συγκεκριμένη πιθανότητα εκτέλεσης (τυχαία μετάπτωση σε φάση λειτουργίας).[270] Έτσι, ο μηχανισμός εξομοίωσης φαίνεται «καταδικασμένος» να «χάσει» κάποια αντίγραφα ή στιγμιότυπα κακόβουλης απειλής, μόνο και μόνο επειδή αυτά δεν ενεργοποιήθηκαν και δεν έτρεξαν.

Επιπρόσθετα, μια πολυνηματική δόμηση (multithreaded design) ενός ιού ή σκουληκιού δύναται να εξαντλεί τους απαιτούμενους συστημικούς πόρους (CPU, RAM) για μια επιτυχημένη εξομοίωση.

Πολύ σημαντική συνδρομή στην αντίσταση ενάντια στη δράση ενός εξομοιωτή παρέχει και η χρήση μη επαρκώς τεκμηριωμένων ή μη συχνά χρησιμοποιούμενων και απίθανων να προσομοιώνονται στα λογισμικά εξομοίωσης CPU εντολών (όπως η εντολή MMX των Pentium) ή ακόμα και εντολών που δεν αφορούν την κεντρική μονάδα επεξεργασίας, αλλά «τρέχουν» σε άλλες επεξεργαστικές μονάδες όπως οι FPUs (coprocessor), οι GPUs (γραφικά), και πιο πρόσφατα οι PPUs (νόμοι φυσικής).[271] Σε τέτοιες συνθήκες, η εξομοίωση αποτυγχάνει και το κατά τα άλλα καθόλα κακόβουλο πρόγραμμα μπορεί να περαστεί για νόμιμο.

Η ίδια λογική ισχύει και στην περίπτωση προγραμματιστικών βιβλιοθηκών ή αρθρωμάτων ή κλήσεων στο Λ/Σ, που μπορεί να προέρχονται από το εξωτερικό ενός συστήματος (μη εξομοιώσιμο) ή να μην είναι επαρκώς γνωστές και τεκμηριωμένες (και σε κάθε περίπτωση να μην είναι χρησιμοποιούμενες από το περιβάλλον εξομοίωσης).[272] Σε αυτές τις καταστάσεις, η κακόβουλη δράση ξεφεύγει του ορίζοντα της εξομοίωσης και το επιβλαβές λογισμικό μπορεί ανενόχλητο π.χ. να κατεβάζει πληροφορίες από μια ιστοσελίδα ή να κάνει χρήση μιας σχετικά άγνωστης μεθόδου του NT Kernel, χωρίς αυτό να παρατηρηθεί σε κάποια φάση εξομοίωσης του εν λόγω προγράμματος.

Τέλος, η ανίχνευση κάποιου εξομοιωτή στο δείνα σύστημα μπορεί να πυροδοτήσει κάποιον εξειδικευμένο μηχανισμό μετάπτωσης ή/και μετάλλαξης-εξέλιξης, που να εξασφαλίζει την ποθητή προστασία.

ii. Αντίσταση στις ευριστικές τεχνικές (Anti-heuristics)[273]

Οι ευριστικές τεχνικές αποτελούν την καρδιά κάθε σύγχρονης σάρωσης, αλλά και αναπόσπαστο συνοδευτικό στοιχείο για μια εμπεριστατωμένη απόπειρα διάγνωσης και

---

[270] Κύρια, βιβλιογραφική αναφορά: [SZOR-ACVRD].

[271] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM], [SZOR-ACVRD].

[272] Κύρια, βιβλιογραφική αναφορά: [SZOR-ACVRD].

[273] Όπως στην προηγούμενη υποσημείωση.

αναγνώρισης μια κακόβουλης μόλυνσης. Τα anti-heuristics εστιάζουν στην αντιμετώπιση των τεχνικών αυτών από την πλευρά ιών, σκουληκιών και άλλων κακόβουλων απειλών.

Στην κατηγορία αυτή των μεθόδων, που προστατεύουν από τις ευριστικές τεχνοτροπίες των συστημάτων ασφάλειας, ανήκουν όλες οι τεχνικές απόκρυψης, αλλά κυριότερα εκείνες της σύνθετης κρυπτογράφησης και της θόλωσης του σημείου εισόδου παρέχουν τα εχέγγυα καταλληλότερης αντίστασης. Οι υπόλοιπες επιλογές απόκρυψης αποτελούν λύσεις λιγότερο ορθόδοξες για την προστασία από τις ευριστικές μεθόδους και τα όποια καλά αποτελέσματα δεν έρχονται τόσο ανέξοδα. Στην ίδια κατηγορία θετικής επίδρασης εμπίπτουν και οι γνωστές μεθοδολογίες και πρακτικές τροποποίησης του κακόβουλου κώδικα, που συναντήσαμε και στις πολυμορφικές και μεταμορφικές μηχανές μετάλλαξης. Σε αυτές, οι (συνεχείς) παραλλαγές του κώδικα αποτελούν το κλειδί για την επιθυμητή αντοχή στις ευριστικές ανιχνεύσεις.

Η διατήρηση ποιοτικών χαρακτηριστικών ακεραιότητας του προσβληθέντος αρχείου (π.χ. μέγεθος, χρονοσφραγίδα τροποποίησης, CRC checksum) ή συστήματος (π.χ. επίπεδα CPU και RAM, εγγραφές security audit logs) στις φυσιολογικές προ μόλυνσης τιμές ή επίπεδά τους παρέχει μια ακόμη δυνατή προσέγγιση προς την επιθυμητή κατεύθυνση.

Ακόμη, η αποφυγή διαδεδομένων και πολύ ντετερμινιστικών μοτίβων κακόβουλης δράσης (π.χ., API αλφαριθμητικά, κώδικας σε γνωστά ή μοναδικά τμήματα κάποιου προγράμματος) και η εισαγωγή αντίστοιχων καινοτομικών ή τυχαιωδών λειτουργιών (αντίστοιχα, CRC32 checksum ενός αλφαριθμητικού, τυχαία ή άγνωστα και μη μοναδικά τμήματα για την εισαγωγή κακόβουλου κώδικα) προστατεύει περαιτέρω από την έκθεση του ιού ή σκουληκιού σε ευριστικές τεχνικές εντοπισμού.

Τέλος, η χρήση της στοίβας (stack)[274] για την κατασκευή κακόβουλου κώδικα, αλλά και την (απο)κρυπτογράφηση αυτού, μπορεί να αποδειχθεί μια εναλλακτική, ιδιαίτερα ισχυρή μέθοδος προστασίας, τόσο στην αντι-ευριστική περίπτωση, όσο και στην πλειονότητα, όπως θα διαπιστώσουμε τελικά, των τεχνικών θωράκισης.

[274] Η στοίβα αποτελεί μια δομή δεδομένων τύπου LIFO, που μοντελοποιείται στη βάση καταχωρητών επεξεργασίας (CPU registers) και έχει άμεση αναφορά στην κύρια μνήμη, είναι δε ευρέως χρησιμοποιούμενη κατά τη φάση προγραμματισμού και εκτέλεσης εφαρμογών από τα συστήματα επεξεργασίας. Ως τέτοια, παρέχει σε καλοπροαίρετους και κακόβουλους συγγραφείς κώδικα τα απαραίτητα μέσα για την κατασκευή ιδιαίτερα εκλεπτυσμένου κώδικα.

iii. Προστασία από αποσφαλμάτωση (Anti-debugging)[275]

Η *μετατροπή της δυναμικής ανάλυσης ενός κακόβουλου προγράμματος μέσω αποσφαλμάτωσης σε επίπονη διεργασία* είναι το ζητούμενο από τις τεχνικές anti-debugging.

Ακολουθώντας τον εντοπισμό (μέσω ανίχνευσης για την ιδιαίτερη ιδιοσυγκρασία του εκάστοτε debugger, των εισαγόμενων από αυτόν σημείων ελέγχου (breakpoints) ή/και της single-stepping λειτουργικότητας των CPUs της οποίας κάνει χρήση) από μέρους ενός ιού ή σκουληκιού κάποιου (ενδεχομένως γνωστού) αποσφαλματωτή σε ένα σύστημα ή εκ των προτέρων μπορεί ένα τέτοιο, κακόβουλο πρόγραμμα να προχωρήσει στην *εφαρμογή κάποιων μεταπτωτικών στρατηγικών ή/και μιας επιλογής ενός συνδυασμού από τις ακόλουθες μεθόδους*, που με τον ένα ή τον άλλο τρόπο προστατεύουν παθητικά από την παρουσία και τη δράση των περισσότερων αποσφαλματωτών:

- Καθαρισμός ή χρήση των ειδικών καταχωρητών αποσφαλμάτωσης ή debug registers της CPU και του εκάστοτε Λ/Σ.
- Προηγμένες EPO τεχνικές.
- Τροποποίηση κώδικα, στη λογική των μηχανών μετάλλαξης (code confusion).
- Βρόχοι αποκρυπτογράφησης αντίστροφης φοράς (backward decryption loops).
- Χρήση της στοίβας (stack) για την κατασκευή κακόβουλου κώδικα, ακόμα και μηχανισμών (απο)κρυπτογράφησης· μια γενικευμένη προώθηση (push) και εξαγωγή (pop) δεδομένων από τη στοίβα μπορεί να προκαλέσει δυσχέρεια στη λειτουργία των περισσότερων αποσφαλματωτών.

Οποιαδήποτε από τις παραπάνω τεχνικές αποτελεί λύση από την οποία μπορεί να επωφεληθεί μια anti-debugging προσέγγιση, σε μια προσπάθεια να παρέχει ολοκληρωμένη προστασία από τον κίνδυνο και την πρακτική της αποσφαλμάτωσης.

iv. Προστασία από αποσυναρμολόγηση (Anti-disassembly)[276]

Όλες οι γνωστές τεχνικές τροποποίησης κώδικα (code confusion-obfuscation), που χρησιμοποιούν οι πολυμορφικές, μεταμορφικές και ενδεχομένως και άλλες εξελικτικές τεχνοτροπίες, μπορούν να δράσουν ως μέτρα αντίστασης του κακόβουλου

[275] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM], [SZOR-ACVRD].

[276] Όπως στην προηγούμενη υποσημείωση.

προγραμματιστή στην αποσυναρμολόγηση ιών και σκουληκιών, αλλά με μια σχετικά ασθενή έννοια.

Οι *στόχοι για μια πιο ισχυρή, αυθεντική προστασία* ιών και σκουληκιών από την αποσυναρμολόγηση είναι κυρίως οι ακόλουθοι 2:[277]

- *Η αποσυναρμολόγηση δεν πρέπει να είναι εύκολα αυτοματοποιήσιμη* (να πραγματοποιείται μόνο από λογισμικό)· ο πολύτιμος (και ακριβός) χρόνος και η επιτηδευμένη γνώση ενός εξειδικευμένου εμπειρογνώμονα ανθρώπου θα πρέπει πάντα να απαιτούνται για τη σωστή εφαρμογή της διαδικασίας και για να γίνει κατανοητός ο αποσυναρμολογημένος κώδικας.
- *Ο πλήρης κώδικας δε θα πρέπει να γίνεται διαθέσιμος, πριν η κακόβουλη απειλή καταφέρει να εκτελεστεί έστω και μια φορά με επιτυχία*.

Η πρώτη σκοπιμότητα ικανοποιείται με την ευρύτερη ανάμιξη των διακριτών τμημάτων κώδικα και δεδομένων των κακόβουλων προγραμμάτων, σε βαθμό που να μη γίνεται εύκολος ο διαχωρισμός τους π.χ. με τη χρήση εντολών ως τιμών δεδομένων και αντίστροφα και τη βοήθεια της στοίβας.

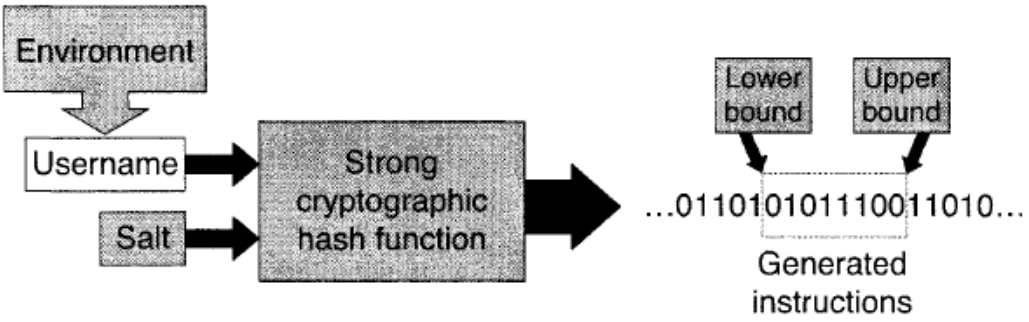
Η δεύτερη προϋπόθεση για μια αποτελεσματική αντιμετώπιση της αποσυναρμολόγησης μπορεί να εκπληρωθεί με *χρήση μιας σειράς από διαφορετικές τεχνικές*, όπως π.χ. οι παρακάτω:[278]

1) Ο κώδικας μπορεί να είναι δυναμικά παραγόμενος (στη λογική των JIT compilers) ή/και τροποποιήσιμος, κατά τη φάση εκτέλεσης του κακόβουλου προγράμματος.

2) Κρυπτογράφηση με τη βοήθεια συναρτήσεων κατακερματισμού (hash functions) και παραμέτρων του περιβάλλοντος εκτέλεσης (όπως στην περιβαλλοντική δημιουργία κλειδιού) για τη δυναμική παραγωγή κώδικα, όπως στο ακόλουθο σχήμα:

[277] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM].

[278] Όπως στην προηγούμενη υποσημείωση.



Σχήμα 19: Έξυπνη κρυπτογράφηση με τη βοήθεια συναρτήσεων σύνοψης για την αντιμετώπιση της αποσυναρμολόγησης

3) Παρεμβολή δεκαεξαδικών αλφαριθμητικών (hex strings) στον κώδικα, ώστε να αντιστοιχούν στο άθροισμα ελέγχου (π.χ. CRC32 checksum) γνωστών API κλήσεων και μεθόδων, που είναι τελείως άσχετες με την όποια κακόβουλη λειτουργία ή απολύτως άχρηστες.

4) Κατ' απαίτηση -και μόνο όταν είναι αναγκαίο- αποκρυπτογράφηση μιας κρυπτογραφημένης απειλής.

5) Μια πολύ εξεζητημένη προσέγγιση βασίζεται στην σύμπραξη 2 ξεχωριστών νημάτων (threads), ενός για την αποκρυπτογράφηση του επόμενου του δείκτη ροής εκτέλεσης (program counter) μπλοκ εντολών και ενός άλλου για την κρυπτογράφηση του αμέσως προηγούμενου. (Η μέθοδος αυτή αποτελεί ταυτόχρονα anti-debugging και anti-emulating τεχνική)

Οι τεχνικές κατά της αποσυναρμολόγησης μπορούν να «αναστείλουν» τη δράση επιτυχημένων προϊόντων και εργαλείων ασφάλειας και να εκνευρίσουν και τον πιο επίμονο και υπομονετικό ερευνητή-εργαζόμενο.

v. Τεχνικές αποφυγής παγίδων (Anti-goat, Anti-honeypot)

Οι δύο μεγαλύτερες απειλές προσέλκυσης και παγίδευσης για το κακόβουλο, αυτοαναπαραγόμενο λογισμικό, που συναντά κανείς στις μέρες μας, είναι όσον αφορά τους ιούς η παρουσία goat αρχείων και η δράση των honeypots για τα σκουλήκια:

- Οι ερευνητές ιών υπολογιστών και τα συστήματα προστασίας δημιουργούν χαρακτηριστικά goat (εκ του αποδιοπομπαίου τράγου) αρχεία για να εντοπίσουν

και να καταλάβουν καλύτερα τη στρατηγική μόλυνσης ενός ιδιαίτερου ιού.[279] *Η μόλυνση ενός τέτοιου αρχείου διευκολύνει την ανάλυση των ιών* επειδή χωρίζει οπτικά το γνωστό περιεχόμενο του ξενιστή από το κατεξοχήν ιομορφικό σώμα. Τα goat αρχεία περιέχουν ειδικές μη παραγωγικές εντολές (όπως οι NOPs) και επιστρέφουν στο λειτουργικό σύστημα, χωρίς να εμφανίζουν οποιαδήποτε χρήσιμη λειτουργικότητα. Τα αρχεία αυτά δημιουργούνται σε διάφορα συστήματα αρχείων και διαθέτουν ποικιλία στο μέγεθος και την εσωτερική τους δομή ανάλογα με το εκάστοτε είδος ιού, στο οποίο στοχεύουν.

Οι ιοί που εφαρμόζουν antigoat θωράκιση χρησιμοποιούν ευριστικούς κανόνες για να ανιχνεύσουν πιθανά αρχεία goat.[280] Παραδείγματος χάριν, ένας ιός μπορεί να είναι έτσι σχεδιασμένος ώστε να αποφεύγει να μολύνει ένα αρχείο, όταν αυτό είναι πάρα πολύ μικρό ή/και περιέχει έναν μεγάλο αριθμό από άχρηστες-μη λειτουργικές οδηγίες, ή ακόμα εάν το όνομα, το μέγεθος και τα περιεχόμενα ενός αρχείου συμφωνούν με κάποια γνωστά και προφορτωμένα στον ιό goat πρότυπα. Η ειδική προτίμηση στην προσβολή, που αναπτύσσει και εκδηλώνει ένας antigoat ιός, είναι μια μορφή παραλλαγής της τεχνικής της μετάπτωσης και τον προστατεύει από το να «τσιμπήσει» διάφορα ανεπιθύμητα, αντιϊομορφικά δολώματα παρέχοντας του έτσι ένα προστατευτικό (χρονικό) παράθυρο αποφυγής εντοπισμού και ανάλυσης.

- Η προσπάθεια παγίδευσης σκουληκιών εμπλέκει και αυτή κάποιας μορφής εξιλαστήρια θύματα. Ένα *honeypot* («δοχείο με μέλι») είναι *"ένα δικτυοκεντρικό σύστημα ηλεκτρονικών υπολογιστών, που είναι εξαρχής στημένο για να προσελκύσει και να «παγιδέψει» -ενεργητικά μέσω επιβολής αντιμέτρων ή παθητικά μέσω ανάλυσης των δραστηριοτήτων- ανθρώπους ή λογισμικό που προσπαθούν να υπονομεύσουν ή να εισβάλλουν παράνομα σε ΠΣ, στα οποία δεν έχουν τέτοια δικαιοδοσία"*.[281] Τα honeypots είναι συνήθως *επίτηδες απροστάτευτα και χωρίς μηχανισμούς ασφάλειας*, ενώ επίσης έχουν επίτηδες έτσι σχεδιαστεί, ώστε να μη διαθέτουν ή πραγματοποιούν καμία άλλη χρήσιμη, υπολογιστική δραστηριότητα, πέραν του να *υποδύονται συγκεκριμένες, δικτυακές υπηρεσίες ή προγραμματιστικές εφαρμογές* (ακόμα και Λ/Σ), προσομοιώνοντας έτσι υποτιθέμενα, πραγματικά συστήματα, πιθανά θύματα χάκερ ή κακόβουλων προγραμμάτων. Ειδικά για τα σκουλήκια και τα στιγμιότυπά τους, αποτελούν ένα

[279] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM].

[280] Κύρια, βιβλιογραφική αναφορά: [SZOR-ACVRD].

[281] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM], [SZOR-ACVRD].

κατά τα άλλα «νόστιμο» (λόγω της μη προστασίας) στόχο, που μπορεί να γίνει όμως ο δήμιός τους.

Σκουλήκια με παθητικές antihoneypot δυνατότητες χρησιμοποιούν ευρέως εξειδικευμένα εργαλεία εντοπισμού τέτοιων δολωμάτων (όπως π.χ. το περίφημο Honeypot Hunter της εταιρείας Send-Safe, που μπορεί κανείς να αποκτήσει μέσω της ιστοσελίδας www.send-safe.com/honeypot-hunter.html) και ειδικούς αλγορίθμους ανίχνευσής τους (υπάρχουν αρκετοί στο Διαδίκτυο, γραμμένοι σε διάφορες γλώσσες προγραμματισμού)[282], ώστε να αντιλαμβάνονται έγκαιρα μια σχετική κατάσταση και να αποφεύγουν την επίθεση σε τέτοια συστήματα (και εδώ πρόκειται για κάτι σαν μια επιλεκτική μετάπτωση).

Η παθητική αποφυγή μιας κακοτοπιάς, που οφείλεται σε κάποια προηγμένη μέθοδο εντοπισμού, είναι ο ένας -και ο πλέον ήπιος- δρόμος αντίδρασης για τον κακόβουλο, αυτοαναπαραγόμενο κώδικα και η θωράκιση είναι το κατάλληλο μέσο. Μια άλλη, πιο αντιδραστική προσέγγιση μπορεί να περιλαμβάνει και τη πιο άμεση και βίαιη καταστολή ή υποβάθμιση της λειτουργίας των εκάστοτε εκφραστών και εκτελεστικών οργάνων των εν λόγω μεθόδων (δηλαδή των διαφόρων συστημάτων ασφάλειας) ή την μετατροπή τους σε πειθήνια υποχείρια του επιτιθέμενου λογισμικού· αυτή είναι όμως μια υπόθεση καθαρά ενεργητικής, τακτικής αυτοάμυνας και θα περιγραφεί και μελετηθεί σε παρακάτω σκέλος, του τρέχοντος εδαφίου.

3. Μετάλλαξη - Εξελικτικός κώδικας (Mutation & Evolution)

Η έννοια της εξέλιξης στον κακόβουλο, αυτοαναπαραγόμενο κώδικα αναφέρεται στο φαινόμενο εμφάνισης και τη διαδικασία παραγωγής «γενετικών» τροποποιήσεων στον κώδικα μεταξύ διαφορετικών γενεών αντιγράφων ή στιγμιοτύπων ενός κακόβουλου προγράμματος. Η αντίληψη ότι *η εξέλιξη του (αυτοαναπαραγόμενου, κακόβουλου) κώδικα αποτελεί ένα ισοδύναμο της δαρβινικής εξέλιξης των έμβιων όντων*[283], που κυβερνάται από τις επαναλαμβανόμενες διαδικασίες της τυχαίας παραλλαγής ή μετάλλαξης (random mutation or variation) και της φυσικής επιλογής (natural selection) είναι ιδιαίτερα διαδεδομένη εδώ και αρκετά χρόνια και σήμερα φαίνεται να «κερδίζει ακόμα περισσότερους πόντους» από τους διάφορους μυημένους και μύστες του

[282] Οι αλγόριθμοι αυτοί βασίζονται στην ύπαρξη ευπαθειών στα πλέον δημοφιλή honeypot συστήματα, όπως το Sebek, το honeyd και το λογισμικό εικονικοποίησης VMWare και την άμεση εκμετάλλευσή αυτόν προς εντοπισμό και αποφυγή ή αχρήστευση της παγίδας.

[283] Κύρια, βιβλιογραφική αναφορά: [LUDWIG-GBBCV], [LUDWIG-CVALE], [JOHANSSON-CVTEALF], [SPAFFORD-CVAL].

ιδιαίτερου αυτού συλλογισμού και των σημασιολογικών συνεπαγωγών του. Στην πραγματικότητα, βέβαια, όπως θα δούμε, η εξελικτική διαδικασία που προκύπτει στους κόλπους του αυτοαναπαραγόμενου, κακόβουλου λογισμικού ίσως θυμίζει περισσότερο μια κατάσταση «νοήμονος σχεδιασμού» ή τεχνητής επιλογής, στην οποία μια εξωτερική, ισχυρή οντότητα (ανθρωπότητα) παρεμβαίνει στη διαδικασία της επιβίωσης των διαφόρων ειδών και της εξέλιξης τους και επηρεάζει την τύχη και την πορεία τους όπως βουλεύεται, παρά μια κλασσική, δαρβινική θεώρηση της μέσω φυσικής επιλογής εξέλιξης, που την θέλει αυτόνομη και αφημένη στους αυτόματους νόμους του γονιδιώματος (κώδικας), των περιβαλλοντικών πιέσεων και του «ανταγωνισμού των ειδών», που ανήκουν στο ίδιο περιβάλλον, και της επιβίωσης του «ισχυρότερου».

Από μια άποψη και μια γενική σκοπιά του θέματος, η διαδικασία της εξέλιξης είναι διάχυτη στο λογισμικό με τον ίδιο τρόπο που είναι και σε οποιοδήποτε άλλο εξάλλου τεχνολογικό πόνημα του ανθρώπου. Διάφορες παράμετροι διαμορφώνουν την επικράτηση ή αποδοχή και συνάμα την επιβίωση μιας τεχνολογίας. Διαφορετικοί παράγοντες πυροδοτούν την εμφάνιση παραλλαγών στα όποια κεντρικά αυτά επικρατούντα μοτίβα, που με τη σειρά τους, ανάλογα και με τις συνθήκες, πετυχαίνουν να επιβιώσουν ή χάνονται από το προσκήνιο της εξέλιξης και η διαδικασία αυτή συνεχίζεται επαναληπτικά και αενάως. Προκειμένου για το σύνολο του κακόβουλου λογισμικού από σύλληψης του μέχρι σήμερα, η εξέλιξη αφορά στην ιστορική του πορεία και τις διαφορετικές υποστάσεις και χαρακτηριστικά που έχει εκλάβει ή απωλέσει μέσα σε αυτήν, εμφανίζοντας μάλιστα και μια ιδιαίτερη «βιοποικιλότητα», όπως η σημερινή. Αυτού του είδους η εξέλιξη είναι το αποτέλεσμα της *χρόνιας τριβής και διαπάλης των σχεδιαστών κακόβουλου λογισμικού με τους αντίστοιχους κατασκευαστές Λ/Σ, εφαρμογών, υλικού και συστημάτων ασφάλειας μέσα στο ευρύτερο, ευμετάβλητο, πληροφοριακό οικοσύστημα*. Ο συνεχής ανταγωνισμός μεταξύ τους και οι όποιες ριζικές καινοτομίες προέκυπταν ήταν η κινητήριος δύναμη για συνεχείς εφευρέσεις, τροποποιήσεις και απομακρύνσεις διαφορετικών προσεγγίσεων και οδήγησε (και θα οδηγεί, όπως όλα δείχνουν) την ιστορική αυτή διαδρομή. Αυτή η θεώρηση της εξέλιξης έχει απλά αξία ως αναδρομή και επισκόπηση των κατά καιρούς εκφάνσεων κακόβουλου κώδικα και των λόγων ή συνθηκών που οδήγησαν στην όποια επιτυχία ή αποτυχία τους, χωρίς να αποτελεί μια πρακτική μέθοδο, που το ίδιο το κακόβουλο λογισμικό μπορεί να θέσει σε εφαρμογή, για να εξυπηρετήσει τα ιδιαίτερα συμφέροντά του με πιο αποτελεσματικό τρόπο.

Από μια άλλη ματιά, η εξέλιξη μπορεί να αποτελέσει και εργαλείο για μεγαλύτερη ενίσχυση της αυτοάμυνας του κακόβουλου, αυτοαναπαραγόμενου κώδικα, με τρόπο προγραμματιστικό. Ο κακόβουλος κώδικας μπορεί να περιέχει εκείνες τις ρουτίνες που

σκόπιμα θα παράγουν, με τυχαιώδη τρόπο, τροποποιημένες εκδοχές του (μεταλλάξεις), κατά τη φάση της αναπαραγωγής, έτσι ώστε καινούριες γενιές του κακόβουλου προγράμματος να διαφέρουν σχεδόν πάντοτε από τις προηγούμενες. Σ' αυτό το σημείο, ακριβώς, έχουμε τη θεμελίωση της «τυχαίας παραλλαγής», στην υπόδειγμα της εξέλιξης των κακόβουλων προγραμμάτων. Από την πλευρά της «φυσικής επιλογής», είναι γενικά παραδεκτή η εικόνα επιβίωσης-επικράτησης της ισχυρότερης και ανθεκτικότερης, κακόβουλης μετάλλαξης στην κόντρα με τα διάφορα συστήματα ασφάλειας που εχθρεύονται και απειλούν ιούς και σκουλήκια. Με αυτήν την έννοια, θεωρεί κανείς την μετάλλαξη-εξέλιξη και ως μέσο και εχέγγυο αυτοπροστασίας των κακόβουλων αυτών όπλων.

Οι πλέον απλές, πλην δημοφιλέστατες, προγραμματιστικές, εξελικτικές ρουτίνες είναι οι πολυμορφικές και μεταμορφικές μηχανές μετάλλαξης, που συζητήθηκαν στο κομμάτι των μεθόδων απόκρυψης[284]. Πέρα από το καμουφλάζ της κρυπτογράφησης και των άλλων βοηθημάτων προστασίας, που παρέχουν ο πολυμορφισμός και ο μεταμορφισμός, κρύβεται στις τεχνικές αυτές και ένας βαθιά εξελικτικός χαρακτήρας, που εκδηλώνεται με τη μεγάλη «βιοποικιλομορφία» των γεννημάτων, με τις διάφορες νέες γενιές να είναι σχεδόν πάντα σημαντικά διαφοροποιημένες από τις παλαιότερες. Οι ριζικές και ανεξέλεγκτες μεταλλάξεις, εν γένει, δυσκολεύουν το έργο της αναγνώρισης και ταυτοποίησης του είδους μιας απειλής μέσω υπογραφών κακόβουλου κώδικα, αφού διαφορετικοί ξενιστές ιών και στιγμιότυπα σκουληκιών, πολυμορφικού ή μεταμορφικού τύπου, εμφανίζουν τυχαίες, δραστικές τροποποιήσεις στη θέση και τη μορφή (και πολύ σπανιότερα και τη λειτουργία) του κακόβουλου κώδικα. Έτσι, η αυτοάμυνα της απόκρυψης πλαισιώνεται και ενισχύεται παραπάνω από την πρόσθετη προστασία της δραστικής μετάλλαξης.

Η προγραμματιστική μετάλλαξη-εξέλιξη, όμως, μπορεί να είναι περισσότερη πολύπλοκη και πιο αποδοτική από την παραπάνω προσέγγιση και να απεμπλέκει εντελώς τόσο το σχεδιασμό του αμυντικού μηχανισμού του κακόβουλου προγράμματος από την απαραίτητη παρουσία κρυπτογραφίας, με σκοπό την παροχή υψηλού βαθμού προστασίας αυτού, όσο και τη μετάλλαξη από το να είναι αποκλειστικότητα της φάσης αναπαραγωγής. Φορέας βελτιστοποίησης είναι πρωτίστως ένα *σύνολο από αλγορίθμους απόφασης για μετάλλαξη*, που την προικοδοτούν με έναν στοιχειώδη μηχανισμό (αυτό)ελέγχου, που εκλείπει από τις συνηθισμένες πολυμορφικές-μεταμορφικές μηχανές

[284] Κύρια, βιβλιογραφική αναφορά: [SZOR-ACVRD].

μετάλλαξης (σε αυτές η μετάλλαξη είναι συνήθως ανεξέλεγκτη, καταναγκαστική προοπτική).[285] Η απόφαση για μετάλλαξη λαμβάνεται:

- είτε ως πείραμα τύχης με συγκεκριμένη, ρυθμιζόμενη κατανομή πιθανότητας για μετάλλαξη ή μη
- είτε με βάση κάποια λογική συνθήκη (τύπου trigger), που πρέπει να ικανοποιείται πρώτα για να πυροδοτεί μια μετάλλαξη

και μια μετάλλαξη μπορεί να λάβει χώρα:

- τόσο κατά τη φάση αναπαραγωγής,
- όσο και οποιαδήποτε άλλη περίοδο κατά τη διάρκεια του κύκλου ζωής (ή του αντίστοιχου μικρότερου της εκτέλεσης) ενός κακόβουλου προγράμματος.

Ο «έλεγχος» των ευρύτερων συνθηκών για μετάλλαξη, που προκύπτει μέσω του προαναφερόμενου σχετικά απλού στη σύλληψη και υλοποίηση μηχανισμού, παράγει:

α) πραγματικά τυχαίες (και όχι μόνο τυχαίου περιεχομένου) παραλλαγές του κακόβουλου κώδικα {τυχαίο πείραμα},

β) υπό συνθήκη μεταλλάξεις {λογική συνθήκη} και

γ) κατ' απαίτηση ή κατ' επιθυμία (on demand, on wish) τροποποιήσεις και όχι απαραίτητα μόνο κατά τη φάση της παραγωγής ενός αντιγράφου ή στιγμιοτύπου (όπως συμβαίνει με τον πολυμορφικό ή μεταμορφικό τρόπο εξέλιξης).

Τα παραπάνω μπορούν να συνθέσουν μια πολύ κομψή δικλείδα ασφάλειας για μια δυναμική αυτοάμυνα· η ανά πάσα στιγμή δυνατότητα ρύθμισης της πιθανότητας μετάλλαξης ή προσεκτικής επιλογής των λογικών συνθηκών πυροδότησής της, μπορούν να φανούν ιδιαίτερα χρήσιμες στην αντιμετώπιση των διαφορετικών, πιθανών, περιβαλλοντικών προκλήσεων, που ενδεχομένως αναδύονται κάθε στιγμή, αντικατοπτρίζοντας μια αντίδραση του κακόβουλου προγράμματος στις συνήθως

[285] Κύρια, βιβλιογραφική αναφορά: [LUDWIG-GBBCV], [LUDWIG-CVALE].

διαρκείς (εν)αλλαγές -και κυρίως τις νέες απειλές- του φυσικού του περιβάλλοντος π.χ. εμφάνιση αντιϊομορφικής δραστηριότητας[286].

Στην κατεύθυνση μιας ακόμη πιο εμπεριστατωμένης, εξελικτικής μεθόδου, συνδράμει και η δυνατότητα μετάλλαξης με τροποποίηση λειτουργικών τμημάτων του κακόβουλου κώδικα και όχι μόνο της μορφής ή της ιδιαίτερης θέσης του. Οι λειτουργικές αυτές παραλλαγές αυτές μπορούν να αφορούν πρακτικά το ο,τιδήποτε, από εναλλακτικές κεφαλές και φορτία, μέχρι διαφορετικές συνταγές κρυπτογράφησης, θωράκισης ή υπονόμευσης διαφόρων Λ/Σ, και να εισάγονται εν ώρα δράσης, όποτε είναι επιθυμητό ή ανάλογα με επικρατούσες συνθήκες π.χ. μέσω εξωτερικής πρόσληψης ή απομακρυσμένου ελέγχου του λογισμικού ή να αφαιρούνται από τον κώδικα με τυχαίο τρόπο ή πάλι με εξωτερική παρέμβαση, με βάση επιθυμίες ή εκάστοτε περιβαλλοντικές περιστάσεις. Αυτού του είδους η εξέλιξη βασίζεται με τον ένα ή τον άλλο τρόπο στην ύπαρξη κάποιου «καναλιού» επικοινωνίας του κακόβουλου προγράμματος με κάποια εξωτερική του κακόβουλη, διαχειριστική οντότητα (άνθρωπος ή μηχανή) από την οποία και λαμβάνει οδηγίες και υλικό μετάλλαξης.

Όπως εύκολα διαπιστώνει κανείς, *η μετάλλαξη (και εξέλιξη) του κακόβουλου, αυτοαναπαραγόμενου κώδικα δεν είναι απλά μια αναπόφευκτη δραστηριότητα στο διηνεκές της τεχνολογικής προόδου, αλλά και μια τεχνική που σκόπιμα και προγραμματιστικά μπορεί να αναζητήσουν και να ακολουθήσουν οι σχεδιαστές κακόβουλων προγραμμάτων, προκειμένου να επιτύχουν για το λογισμικό τους υψηλούς βαθμούς προστασίας και αντοχής στις εκάστοτε -και πιθανώς αφιλόξενες- συνθήκες*.

Ο συνιστάμενος βαθμός δυσκολίας στον εντοπισμό και την αναγνώριση ενός κακόβουλου όπλου, σε συνδυασμό με την εμφανή υπερπήδηση προληπτικών μηχανισμών, που εισάγουν οι τεχνικές του καμουφλάζ, της θωράκισης και της μετάλλαξης, με απλό και ταυτόχρονα παθητικό τρόπο, μπορεί να οδηγήσει ουσιαστικά στη ματαιότητα την παρουσία σύγχρονων μηχανισμών ασφάλειας, είτε βρίσκονται εντός πληροφοριακών κόμβων είτε περιμετρικά αυτών. Άλλοτε οι μεγάλες απαιτήσεις σε χρόνο και άλλοτε το υπερβολικό κόστος της κατανάλωσης διαφόρων πόρων, προκειμένου να εντοπιστούν και αναγνωριστούν επιτυχώς οι όποιες απειλές κάνουν χρήση παθητικών μεθόδων αυτοπροστασίας, μπορούν πρακτικά να «αχρηστεύσουν» και το πιο προηγμένο σύστημα ασφάλειας ΠΣ, αν δεν υπάρξει ουσιαστική πρόνοια για μια ειδική αντιμετώπιση των απειλών αυτού του τύπου και των ενδεχόμενων δυσάρεστων συνεπειών τους. Στο Κεφάλαιο 4, παρουσιάζονται ενδελεχώς οι διάφοροι τρόποι αντιμετώπισης, που μπορεί η αμυνόμενη οντότητα να αντιπαρατάξει. Ακόμη, στο Κεφάλαιο

[286] Βλέπε και ενότητα ευφυούς προσαρμογής παρακάτω, εδάφιο 3.2.6.

5, σχολιάζονται κάποιες σχετικές, πιο πρόσφατες και ελπιδοφόρες προσεγγίσεις στο χώρο της προστασίας της πληροφορίας από τις κακόβουλες εκθέσεις.

Β) Ενεργητικές μέθοδοι (attack on security or operating systems)

Οι ενεργητικές μέθοδοι περικλείουν και ορίζουν έναν *εμφανώς επιθετικότερο χαρακτήρα για την αυτοάμυνα των κακόβουλων όπλων* και διακρίνονται ανάλογα με τον στόχο της επιθετικής αυτής άμυνας. Έτσι, στην περίπτωση που ένας ιός ή σκουλήκι επιχειρεί την ενεργητική καταστολή των συστημάτων ασφάλειας Η/Υ έχουμε να κάνουμε με δείγμα ρετροϊομορφισμού, ενώ όταν στόχος των ιών ή των σκουληκιών γίνεται το ίδιο το λειτουργικό σύστημα των Η/Υ μιλάμε για τη μέθοδο της υπονόμευσης Λ/Σ. Τέλος, μια ενδιαφέρουσα, ενδιάμεση, υβριδική κατάσταση με ιστορία αρκετών ετών αποτελούν οι λεγόμενες τεχνικές σήραγγας (tunneling), όπου ιοί και σκουλήκια «γαντζώνονται» σε εν γένει χαμηλού επιπέδου και άλλοτε ζωτικής σημασίας κλήσεις API του Λ/Σ (όπως π.χ. interrupts), σε μια προσπάθεια να αποφύγουν τον εντοπισμό, παρακάμπτοντας με όσο το δυνατόν διακριτικότερο τρόπο τα όποια, εγκατεστημένα συστήματα ασφάλειας.

Πρώτο μέλημα του αυτοαναπαραγόμενου όπλου στις ενεργητικές μεθόδους αυτοάμυνας δεν είναι να κάνει απλά δύσκολους τον εντοπισμό και την αναγνώρισή του από τους εγγενείς μηχανισμούς προστασίας του Λ/Σ ή από εκείνους των πρόσθετων συστημάτων ασφάλειας ή/και να ξεπεράσει παθητικά την εκάστοτε περιοριστική, προληπτική δράση τους, με την εφαρμογή τεχνικών καμουφλάζ, θωράκισης ή μετάλλαξης, αλλά *να επιτεθεί με την καταστολή των πρόσθετων/παρένθετων συστημάτων ασφάλειας ή/και την υπονόμευση ενός Λ/Σ απευθείας στην καλή και ορθή λειτουργία του όλου οικοδομήματος της ασφάλειάς τους* (πρόληψη, διάγνωση, θεραπεία) παρεμποδίζοντάς την ενεργητικά και εκθέτοντας παράλληλα σε περαιτέρω κινδύνους το ήδη μολυσμένο σύστημα πληροφοριών.

Στις ενεργητικές μεθόδους αυτοάμυνας, *δεν προλαμβάνονται ή περιορίζονται εκ των προτέρων, ούτε μετατρέπονται σε απλά επίπονη διαδικασία*, η σάρωση, η αποσφαλμάτωση, η αποσυναρμολόγηση, η εξομοίωση, ο έλεγχος ακεραιότητας και ύποπτης συμπεριφοράς και οι διάφορες ευριστικές μέθοδοι εντοπισμού και αναγνώρισης των κακόβουλων απειλών και δεν ξεπερνώνται πλέον με παθητικό τρόπο οι ύφαλοι και σκόπελοι που εισάγουν οι όποιες εγγενείς δικλείδες και πολιτικές ασφάλειας των Λ/Σ ή τα εξωγενή συστήματα προστασίας· αντιθέτως *παραβιάζονται, παρακάμπτονται ή εξουδετερώνονται στην καρδιά της ύπαρξής και τον πυρήνα της λειτουργίας τους με στοχευμένο, αντιδραστικό και επιθετικό τρόπο*.

Αυτή είναι και η ειδοποιός διαφορά με τις παθητικές μεθόδους αυτοπροστασίας.

Ρετροϊομορφισμός

Ακριβώς όπως ένας βιολογικός ρετροϊός (όπως π.χ. ο ιός HIV ή ο Embola) επιτίθεται στην επάρκεια της λειτουργίας ενός ανοσοποιητικού συστήματος, έτσι και ένας ψηφιακός ρετροϊός ή ένα ρετροϊομρφικό σκουλήκι *προσπαθεί συγκεκριμένα να παρακάμψει ή να εμποδίσει τη λειτουργία ενός αντιϊομορφικού συστήματος, ενός τείχους αντιπυρικής προστασίας και όποιων άλλων πρόσθετων προγραμμάτων ασφάλειας Η/Υ με ενεργητικό, επιθετικό τρόπο*.

Το επιθετικό, ρετροϊομορφικό λογισμικό (retaliating or retroviral malware) ακολουθεί, συχνά, κάποιες από τις ακόλουθες οδούς, όταν εκτελείται:[287]

- Θέτει εκτός λειτουργίας ή «σκοτώνει» συγκεκριμένα, αντιϊομορφικά προγράμματα στη μνήμη ή/και στο δίσκο.
- Θέτει εκτός λειτουργίας ή παρακάμπτει ορισμένα προϊόντα παρεμπόδισης ύποπτης συμπεριφοράς (behavior blockers).
- Παρακάμπτει ή «σκοτώνει» λογισμικό προσωπικού τείχους αντιπυρικής προστασίας.
- Αλλοιώνει ή διαγράφει τα αρχεία βάσεων δεδομένων προγραμμάτων ελέγχου ακεραιότητας.
- Εντοπίζει και αφαιρεί τυχόν πρόσθετο κώδικα ακεραιότητας από εκτελέσιμα αρχεία.
- Αναστέλλει με επιθετικό τρόπο τη δράση στοχευμένων εργαλείων ανάλυσης κακόβουλου λογισμικού, όπως debuggers, disassemblers, honeypots, port scanners και sniffers, μπορεί δε εφόσον τα εντοπίσει να τα υπονομεύσει θέτοντας τα στην υπηρεσία της κακόβουλης απειλής (π.χ. χρήση των disassemblers για τη δημιουργία ή/και λειτουργία μιας μεταμορφικής μηχανής μετάλλαξης).
- Ανιχνεύει την εκτέλεση ρουτινών ανοσοποίησης ή ελέγχου μόλυνσης (π.χ. σάρωση, έλεγχος ακεραιότητας) και αντεπιτίθεται με οποιονδήποτε τρόπο, είτε απευθείας στο σύστημα ασφάλειας είτε γενικότερα με την απελευθέρωση κάποιου ωφέλιμου φορτίου.
- Μολύνει τα αρχεία δεδομένων των συστημάτων ή εργαλείων ασφάλειας, ώστε αυτά να περιέχουν ιομορφικό κώδικα ή όταν εκτελούνται να απελευθερώνουν κάποιο σκουλήκι ή τέλος να ενεργοποιούν κάποιας άλλης μορφής κακόβουλες εντολές.
- Ανιχνεύει και επιτίθεται σε δικτυακό υλισμικό προστασίας προσπαθώντας να υποβαθμίσει κυρίως τη διαθεσιμότητά του ή την ακεραιότητα των δεδομένων του.

[287] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM], [SZOR-ACVRD], [LUDWIG-GBBCV].

- Προκαλεί και διατυμπανίζει ορισμένες, εικονικές μολύνσεις (decoys)[288], αποπροσανατολίζοντας και οδηγώντας σε λάθος συμπεράσματα και συναγερμούς τα συστήματα ασφάλειας.
- Αποτρέπει τα μολυσμένα συστήματα από το να συνδεθούν και να «κατεβάσουν» κρίσιμες ενημερώσεις ασφάλειας (π.χ. νέες υπογραφές ιών κτλ) και άλλο λογισμικό αναβάθμισης και διόρθωσης από τους ιστοχώρους των προμηθευτών των συστημάτων ασφάλειας.
- Απενεργοποιεί ή/και καταστρέφει βασικό, πληροφοριακό, υλικό εξοπλισμό αλληλεπίδρασης χρήστη (μηχανήματα εισόδου-εξόδου (I/O) όπως δίσκους, οθόνες, πληκτρολόγια, εκτυπωτές κτλ) προκειμένου να αποπροσανατολίσει ή να εμποδίσει μια προσπάθεια εντοπισμού και εξουδετέρωσής του.

Ως παράδειγμα ρετροϊομορφικής δράσης αναφέρουμε τη συνδυασμένη απειλή με το κωδικό όνομα Ganda[289], η οποία σκοτώνει τις διαδικασίες που εμφανίζονται ως λογισμικό προστασίας, χρησιμοποιώντας μια λίστα γνωστών, αντιϊομορφικών προγραμμάτων· εξετάζει επίσης τα προγράμματα που αρχίζουν τη δράση τους, με την εκκίνηση ενός υπολογιστικού συστήματος (startup programs)[290], ψάχνοντας για συναφές λογισμικό και χρησιμοποιώντας τον ίδιο κατάλογο ονομάτων. Εάν το πρόγραμμα Ganda εντοπίσει το αναζητούμενο λογισμικό, κατά τη διάρκεια αυτής της εξέτασης, ανιχνεύει την εκτελέσιμη εικόνα τους στο δίσκο και αντικαθιστά την πρώτη οδηγία της με μια οδηγία τύπου RET. Αυτό αναγκάζει το αντιϊομορφικό πρόγραμμα να τερματίζει, αμέσως αφού εκκινεί.

Συνήθως, *ο ρετροϊομορφισμός εκδηλώνεται ως μια βίαιη, ωμή μέθοδος αυτοάμυνας*,[291] τα σημάδια της οποίας στα προσβεβλημένα συστήματα πλην ελαχίστων εξαιρέσεων είναι έκδηλα και εμφανή, συνεπώς μπορούν να γίνουν γρήγορα και εύκολα αντιληπτά από εξοικειωμένο-εξειδικευμένο προσωπικό ή/και ανθεκτικά στον ρετροϊό ή το ρετροσκουλήκι, ευφυή συστήματα ασφάλειας. Παρόλ' αυτά, δεν παύει να αποτελεί μια *εξαιρετικά επικίνδυνη πρακτική, που δύναται να προκαλέσει με άμεσο ή έμμεσο τρόπο αναρίθμητα προβλήματα στα*

---

[288] Σε μια λογική παγίδευσης όμοια με ενός goat file, αλλά με αντιστροφή των ρόλων. Στην ουσία, τα εν λόγω παραπλανητικά τεχνάσματα επιτρέπουν ένα αξιόλογο αντιπερισπασμό για την κύρια δράση του κακόβουλου κώδικα, στρέφοντας την προσοχή των διωκτών τους σε άλλα σημεία και προκαλώντας πιθανώς σύγχυση και περαιτέρω αναστάτωση με τους λάθος συναγερμούς που ίσως ενεργοποιηθούν.

[289] Πηγή: Διαδίκτυο, ιστοχώρος της online «εγκυκλοπαίδειας» ιομορφικού και άλλου κακόβουλου λογισμικού VirusList, http://www.viruslist.com/en/viruslist.html?id=59937.

[290] Είναι σύνηθες για τα προγράμματα προστασίας να «φορτώνονται» στη μνήμη με την εκκίνηση των υπολογιστικών συστημάτων, προκειμένου να εντοπίσουν και να προλάβουν τη δράση κάποιας κακόβουλης εφαρμογής, όπως π.χ. την εκτέλεση στη μνήμη ενός ιού τομέα εκκίνησης ή την εγκατάσταση ενός rootkit σε μια «πυρηνική» διεργασία.

[291] Στη λογική του «η καλύτερη άμυνα είναι η επίθεση».

υπό επίθεση συστήματα, κυρίως όμως να υποβαθμίσει σημαντικά, έστω και αν γίνει αμέσως αντιληπτή λόγω των δραστικών αποτελεσμάτων της, για κάποιο χρονικό διάστημα την ασφάλειά τους.

Στο διάστημα αυτό, για παράδειγμα, που το ρετροϊομορφικό λογισμικό καταστέλλει την πρόσθετη άμυνα ενός πληροφοριακού συστήματος, είναι ενδεχομένως ανοιχτός ο δρόμος και σε άλλο, κακόβουλο κώδικα ή λογισμικό υπολογιστών, που είναι ειδάλλως γνωστά και εύκολα αντιμετωπίσιμα από το εκάστοτε εγκατεστημένο λογισμικό προστασίας ή τις όποιες, υλισμικές λύσεις ασφάλειας. Ακόμη, ο ίδιος ο ρετροϊός ή ρετροσκώληκας μπορεί με άμεσο τρόπο να εκμεταλλεύεται την υποβάθμιση ασφάλειας, που προξένησε σε κάποιο σύστημα, για να εξυπηρετήσει καλύτερα τους προσωπικούς του στόχους διάδοσης ή/και παράδοσης ωφέλιμου φορτίου. Τέλος, η απώλεια ή δυσλειτουργία κάποιων συστημάτων ασφάλειας μπορεί για προληπτικούς λόγους να πυροδοτήσει ενδογενείς ή εξωγενείς μηχανισμούς απομόνωσης για τα υπολογιστικά συστήματα (καραντίνας), που επιφέρουν ταυτόχρονα και κάποιους περιορισμούς στη διαθεσιμότητά τους, με ό,τι επιζήμιο μπορεί αυτό να συνεπάγεται. Άρα, *η πλήρης θεραπεία και επανόρθωση στην περίπτωση έκθεσης σε ρετροϊομορφική επίθεση, όσο και αν η διάγνωση και αναγνώριση μιας τέτοιας απειλής φαίνεται από πρώτης άποψης απλή υπόθεση, μπορεί να γίνει ιδιαίτερα περίπλοκη και περιπαθής*.

Υπονόμευση Λ/Σ (attack on host OS)[292]

Η υπονόμευση σκοπό έχει *να «γκρεμίσει» τις εγγενείς, αμυντικές οχυρώσεις που ένα Λ/Σ προσφέρει ή να ανοίξει ρωγμές ασφάλειας στις λειτουργίες που αυτό επιτελεί*. Η τεχνική αυτή προϋποθέτει μια χαμηλού επιπέδου μόλυνση σε βασικά, συστατικά στοιχεία (αρχεία ή υπηρεσίες) ενός Λ/Σ, που *συνήθως είναι αδιόρατη στα μάτια ενός απλού χρήστη*, ή μια επίμονη μέθοδο παραμονής μιας προσβολής στο σύστημα, με χρήση βασικών, συστατικών μερών των Λ/Σ. Στη διάρκεια επιθέσεων υπονόμευσης εναντίον των Λ/Σ, τα αυτοαναπαραγόμενα όπλα επικαλούνται συχνά και τη *βοήθεια πολλών, απευθείας, προγραμματιστικών κλήσεων μη επαρκώς τεκμηριωμένων ή/και χαμηλού εν γένει επιπέδου ρουτινών διεπαφής με το Λ/Σ*, που (όπως π.χ. είδαμε και στις περιπτώσεις αντιεξομοίωσης) προσδίδουν στον κακόβουλο κώδικα ακόμη μεγαλύτερη παθητικού τύπου προστασία έναντι στα εκάστοτε συστήματα ασφάλειας[293].

Το κακόβουλο, αυτοαναπαραγόμενο λογισμικό μπορεί στα πλαίσια αυτής της υπονόμευσης εναλλακτικά ή συνδυαστικά να:[294]

---

[292] Κύρια, βιβλιογραφική αναφορά: [BUTLER_HOGLUND-ROOTKITS], [RUTKOWSKA-RSbDM].

[293] Κύρια, βιβλιογραφική αναφορά: [KALYANI-AVA].

[294] Κύριο, βιβλιογραφική: [SYMANTEC-WMMR].

- Εκμεταλλεύεται την ύπαρξη ή εγκαθιστά το ίδιο rootkits[295] και άλλο κακόβουλο λογισμικό στο επίπεδο των χρηστών (user-mode ή CPU ring3 malware) ή κυρίως σε βάθος πυρήνα του Λ/Σ (kernel-mode ή CPU ring0 malware), για την αχρήστευση των ιδιαίτερων λειτουργιών ασφάλειας ενός Λ/Σ (π.χ. λογισμικό αυτόματων ενημερώσεων ασφάλειας, αναβαθμίσεων και διορθώσεων των κατασκευαστών του Λ/Σ), την απόκρυψη εαυτού (και των τεκμηρίων) της δράσης του, αλλά αντίστοιχα και ομολόγων του (άλλων κακόβουλων προγραμμάτων), από χρήστες ή/και συστήματα ασφάλειας (με ενεργητικές μεθόδους καμουφλάζ) και την παροχή διακριτικών καναλιών απομακρυσμένης διαχείρισης στους επιτιθέμενους[296]. Σε αυτές τις συνθήκες, ένας Η/Υ δεν είναι παρά έρμαιο των ορέξεων του μολυσμένου Λ/Σ, οι διαχειριστικές εντολές του οποίου (αυτές δηλαδή που μπορούν να επηρεάσουν καθολικά, αλλά με σχεδόν ή ακόμα και εντελώς αφανή τρόπο, και κάποιες φορές ίσως ανεπανόρθωτα τη συμπεριφορά κάποιου Η/Υ) αντικατοπτρίζουν πλέον τις επιθυμίες κάποιας κακόβουλης οντότητας, της οποίας έχει γίνει υποχείριο.
- Παρεμποδίζει την εκκίνηση των συστημάτων σε κατάσταση ασφαλούς λειτουργίας (safe-booting) με τη χρήση π.χ. κακόβουλων ή ακατάλληλων οδηγών συσκευών και άλλων φαντασμάτων.[297]
- Παραμένει σε σκιώδη αντίγραφα ασφάλειας του Λ/Σ προκειμένου να επαναμολύνει το σύστημα, όταν ο χρήστης επιχειρεί αυτοματοποιημένη επαναφορά συστήματος σε κατάσταση καλής λειτουργίας, με αναδρομή σε κάποιο παλαιότερο σημείο αναφοράς (system restore infection).[298]

---

[295] Περισσότερα για την κακόβουλη δυναμική των rootkits «φαντασμάτων», αλλά και εν γένει της σε βάθος υπονόμευσης των Λ/Σ στο κεφάλαιο 5 (5.1.2).

[296] Π.χ. μέσω της εγκατάστασης κάποιου backdoor ή της ενεργοποίησης ενός «κρυφού καναλιού» στεγανογραφικής φύσεως (βλέπε σχετικά 5.1.1).

[297] Η εκκίνηση σε κατάσταση ασφαλούς λειτουργίας είναι μια από τις παλαιότερες, μα συνάμα τελευταίες γραμμές άμυνας των σύγχρονων Λ/Σ έναντι σε προβληματική λειτουργία τους. Στην κατάσταση ασφαλούς λειτουργίας, ο υπολογιστής χρησιμοποιεί ένα μίνιμουμ εντολών πυρήνα και διεπαφών χρήστη, απενεργοποιώντας μεγάλο μέρος της παρεχόμενης λειτουργικότητας για λόγους επιθεώρησης και επίλυσης προβλημάτων (troubleshooting). Σε safe-mode, δε φορτώνεται στη μνήμη τίποτε άλλο, παρά μόνο ο πλέον απαραίτητος κώδικας λειτουργίας του Η/Υ, εκτός και αν κάποιο κακόβουλο λογισμικό εισχωρήσει σε μεγάλο «πυρηνικό» βάθος, «διαβάλλοντας» και τις πιο σημαντικές λειτουργίες του συστήματος. Επειδή κάτι τέτοιο είναι εξεζητημένη περίπτωση, είναι πιο εύκολο για έναν κακόβουλο συγγραφέα να εμποδίζει/αποτρέπει προγραμματιστικά την εκκίνηση σε safe-mode, απλά υπονομεύοντας σε μικρότερο βάθος το Λ/Σ.

[298] Πολλά Λ/Σ παρέχουν μεθόδους λήψης αντιγράφων ασφάλειας της τρέχουσας κατάστασης (δεδομένα, προγράμματα, παραμετροποίηση) ενός Η/Υ, προκειμένου οι χρήστες να προβαίνουν σε αναδρομή σε πρότερες περιόδους λειτουργίας, σε περίπτωση που το επιθυμούν ή κρίνουν αναγκαίο. Σε περίπτωση μόλυνσης π.χ. από κάποιο, κακόβουλο πρόγραμμα κάτι τέτοιο είναι πολύ χρήσιμο, καθώς επιτρέπει την επιστροφή σε παλαιότερη, «άνοση» κατάσταση. Η υπονόμευση του system restore

Οι παραπάνω τρεις προσεγγίσεις μπορεί να βρεθούν σε κάποιο μικρό ή μεγαλύτερο βαθμό να επικαλύπτονται, μπορούν όμως να αποτελούν και σαφώς διακριτές διαφοροποιήσεις της τεχνικής της υπονόμευσης των Λ/Σ, που είναι δυνατόν να χρησιμοποιούν τα αυτοαναπαραγόμενα, κυβερνοόπλα λογισμικού.

Η χρήση μεθοδικής υπονόμευσης Λ/Σ από ιούς ή σκουλήκια φαντάζει ιδανική πρακτική, καθώς μπορεί να αποβεί εξαιρετικά καρποφόρα για τους σκοπούς μιας κακόβουλης επίθεσης, ενώ από την πλευρά του εκτεθειμένου μέρους *περιμένει κανείς πως θα απαιτηθεί επίπονη προσπάθεια και θα δαπανηθούν σημαντικοί πόροι για την ανάνηψη ΠΣ από μολύνσεις σε επίπεδο Λ/Σ*.

Τεχνικές Σήραγγας (Tunneling)[299]

Οι τεχνικές σήραγγας είναι ένα σύνολο μεθόδων γνωστών από την εποχή των πρώτων ιών για το DOS της Microsoft και ουσιαστικά αποτελούν μια τομή, έναν συνδυασμό των παραπάνω 2 προσεγγίσεων, δηλαδή του ρετροϊομρφισμού και της υπονόμευσης των Λ/Σ.

Όταν ένα κακόβουλο, αυτοαναπαραγόμενο πρόγραμμα ανιχνεύει κάποιας μορφής έλεγχο από λογισμικό προστασίας Η/Υ, οι τεχνικές σήραγγας του επιτρέπουν να τον παρακάμπτει προγραμματιστικά. Το αντιϊομορφικό λογισμικό και όλα τα συναφή προγράμματα ασφάλειας Η/Υ μπορούν να παρακολουθούν τις κλήσεις στο API του λειτουργικού συστήματος, ώστε να ελέγχουν για τυχόν ύποπτη δραστηριότητα. Επιβλαβές λογισμικό αυτού του τύπου προσπαθεί, όσο πιο «αθόρυβα» μπορεί, να έρθει πρώτο σε μια αλυσίδα κλήσης διακοπτών (interrupt requests ή απλά interrupts) ή άλλων κύριων συστατικών του API ενός Λ/Σ, εγκαθιστώντας τον εαυτό του πριν από άλλες διαμένουσες στην κύρια μνήμη εφαρμογές, με σκοπό να καλέσει τους διακόπτες ή τα συστατικά αυτά στο ακριβές σημείο εισόδου των αρχικών χειριστών τους (handlers). Η διαδικασία αυτή είναι ευρύτερη γνωστή με το όνομα «γάντζωμα» (hook) και όσο πιο χαμηλού επιπέδου και διαφανής, τόσο μεγαλύτερη η υπονόμευση του Λ/Σ που απαιτεί (*χαρακτήρας υπονόμευσης Λ/Σ*). Κατ' αυτόν τον τρόπο, ο έλεγχος φτάνει πρώτα στο κακόβουλο πρόγραμμα, προτού προλάβουν να τον αποκτήσουν οι τρέχουσες διεργασίες των προγραμμάτων ασφάλειας, πράγμα που θα σήμαινε και πιθανό εντοπισμό της επίβουλης απειλής. Στη συνέχεια, κατόπιν της όποιας, κακόβουλης δράσης του, ο ιός ή το σκουλήκι προχωρά στην εκτέλεση του αρχικού χειριστή δίνοντας τη σκυτάλη

μπορεί να αναπαράγει την κακόβουλη προσβολή σε όλες τις πρότερες και μετέπειτα ληφθείσες καταστάσεις, για αυτό κα αποτελεί ιδανικό τέχνασμα για τους κατασκευαστές οπλολογισμικού.

[299] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM], [SZOR-ACVRD], [LUDWIG-GBBCV].

και παραδίνοντας συνάμα τον έλεγχο στο εκάστοτε λογισμικό προστασίας, ουσιαστικά παρακάμπτοντάς το με έναν ιδιαίτερα αποτελεσματικό τρόπο (*ρετροϊομορφικός χαρακτήρας*).

Ο Βουλγαρικής καταγωγής ιός με την κωδική ονομασία Yankee_Doodle ήταν ένα από τα αξιοσημείωτα, αυτοαναπαραγόμενα όπλα που υλοποιούσαν μια τεχνική σήραγγας για την προστασία τους από τα συστήματα ανίχνευσης και δίωξης κακόβουλου κώδικα, γαντζώνοντας το διακόπτη INT_1 στο DOS[300].

Η μέθοδος αυτοάμυνας με χρήση τεχνικών σήραγγας αποτελεί μια *εκλεπτυσμένη εκδοχή ρετροϊομορφικής προσέγγισης*, που αντλεί τη δύναμή της από την εκμετάλλευση του πιο σημαντικού πλεονεκτήματος της υπονόμευσης ενός Λ/Σ, τη *μεγαλύτερη διακριτικότητα και διαφάνεια* που αρχίζει να χαρακτηρίζει τη δράση μιας κακόβουλης μόλυνσης, όσο αυτή πλησιάζει πιο κοντά στον πυρήνα του Λ/Σ. Ουσιαστικά, το κατά τα άλλα ευρύ πεδίο χρήσης ενός υπονομευμένου Λ/Σ (π.χ. απομακρυσμένη διαχείριση, παράνομη παρακολούθηση/υποκλοπή, υποβάθμιση εγγενούς ασφάλειας Λ/Σ κτλ) βρίσκει μοναδική εφαρμογή στην εξουδετέρωση ή παράκαμψη του όποιου πρόσθετου λογισμικού προστασίας Η/Υ, με την παραδοχή ότι αυτό θα χρησιμοποιεί πάντοτε κάποιες κλήσεις συστήματος χαμηλού επιπέδου. Η υπονόμευση ενός Λ/Σ τίθεται στην υπηρεσία του ρετροϊομορφισμού, αλλά με τρόπο μη βίαιο, με λειτουργίες όσο γίνεται πιο «υπόγειες» και αποτελέσματα κατά το δυνατόν λιγότερο αντιληπτά.

Προφανώς, η υπονόμευση μπορεί να χρησιμεύσει και σε μια ακόμη πιο επιθετική ρετρο-αχρήστευση των συστημάτων ασφάλειας, αλλά τότε πρώτον δεν θα είχαμε να κάνουμε με τεχνικές σήραγγας και δεύτερον θα υπήρχε απώλεια του σημαντικού πλεονεκτήματος που διαχωρίζει τις τεχνικές αυτές από οποιεσδήποτε, άλλες, κλασσικές, ρετροϊομορφικές προσεγγίσεις[301], που σπάνια δεν αφήνουν πρόδηλα σημάδια κακόβουλης δράσης. Οι περιπτώσεις, πάντως, όπου ιοί ή σκουλήκια καταφεύγουν σε χρήση τεχνικών υπονόμευσης του Λ/Σ, για να καταφέρουν και κλασσικότερες και ωμότερες, ρετροϊομορφικές επιθέσεις είναι άφθονες.

Η ενδεχόμενη απουσία ισχυρής προστασίας μεταξύ πεδίου χρηστών (user space) και χώρου πυρήνα (kernel space) στη μνήμη κάποιων Λ/Σ, η ύπαρξη πληθώρας μη επαρκώς τεκμηριωμένων μεθόδων στα περισσότερα API των Λ/Σ και η ωρίμανση της τεχνολογίας των rootkits συμβάλλουν αποφασιστικά στη διάδοση και την επιτυχία των σύγχρονων τεχνικών σήραγγας, όπως αντίστοιχα συμβαίνει και για το υπερσύνολο των τεχνικών υπονόμευσης των Λ/Σ.[302]

---

[300] Κύρια, βιβλιογραφική αναφορά: [SZOR-ACVRD].

[301] Όπως αυτές που συζητήθηκαν προηγούμενα στο ομώνυμο σκέλος.

[302] Τα θέματα αυτά θα προσεγγίσουν και τα Κεφάλαια 4, 5 από διαφορετικές αφετηρίες σκέψης και ανάλυσης.

Η ευρύτερη χρήση από τα αυτοαναπαραγόμενα όπλα των τεχνικών υπονόμευσης των Λ/Σ, είτε αυτόνομα είτε στη μορφή τεχνικών σήραγγας, ώστε να υποβαθμίζεται η εσωτερική - εγγενής και πρόσθετη- ασφάλεια των κόμβων, σε συνδυασμό με επιλεκτική, ωμή ρετροϊομορφική δράση κατά δικτυακών κυρίως συστημάτων ασφάλειας έχει τη δυνατότητα να προκαλέσει πανωλεθρία στην ασφάλεια ΠΣ, έτσι όπως αυτή νοείται σήμερα και εκφράζεται μέσα από τα διαφορετικά συστήματα προστασίας (host-based, network-based). Συγκεκριμένα μέτρα είναι αναγκαίο να λαμβάνονται, προκειμένου να αποφεύγονται τα πλέον δυσάρεστα ενδεχόμενα λόγω προσβολής από λογισμικό αυτοαναπαραγωγής, που κάνει χρήση των ενεργητικών μεθόδων αυτοάμυνας. Περισσότερα για το θέμα αυτό μπορεί να βρει κανείς στην ανάλυση των κεφαλαίων 4 και 5 περί των βέλτιστων, τρεχουσών και νεωτεριστικών μεθόδων προστασίας και πολιτικών ασφάλειας.

3.2.5 Αυτοματοποιημένες γεννήτριες (Construction Kits)

Εξαιρετικά χρήσιμη είναι η *δυνατότητα δημιουργίας προγραμμάτων που παράγουν με αυτόματο τρόπο μέρος ή το σύνολο του κώδικα* ενός ιού ή σκουληκιού. Τα προγράμματα αυτά ονομάζονται *γεννήτριες ή σετ εργαλείων κατασκευής (construction generators or kits)* και φέρουν την ιδιότητα ότι μπορούν να χρησιμοποιηθούν πρακτικά από οποιονδήποτε χειριστή Η/Υ με κακόβουλες προθέσεις, χωρίς αυτός να πρέπει πρώτα να έχει εντρυφήσει στην απόκρυφη και δύσκολη τέχνη της συγγραφής επιβλαβούς λογισμικού[303]. Η ύπαρξη, λοιπόν, των αυτοματοποιημένων γεννητριών κατασκευής εύκολα καταλαβαίνει κανείς πως είναι γεγονός ιδιαίτερα βολικό για κάποιον επίδοξο επιτιθέμενο και αρκετά επικίνδυνο για τους αντιπάλους αυτού.

Τα σύγχρονα σετ εργαλείων κατασκευής παρουσιάζουν *αξιοσημείωτη ποικιλία διεπαφών χρήστη* (γραμμή εντολών, σύνθετα μενού, γραφικά περιβάλλοντα χρήσης) που απευθύνονται και εξυπηρετούν διαφορετικές μερίδες χρηστών, ανάλογα με το βαθμό λεπτομέρειας και επεξήγησης που απαιτείται.[304]

Στηριζόμενες σε *συγκεκριμένα, βασικά, στοιχειώδη πρότυπα* πάνω στα οποία θα «χτιστούν» όποιες πρόσθετες λειτουργίες και δυνατότητες και με τη συνδρομή της τυχαιότητας αλλά και της αλληλεπιδραστικής ανάδρασης του χρήση, όσον αφορά τα επιθυμητά χαρακτηριστικά του υπό παραγωγή ιού ή σκουληκιού, οι γεννήτριες κατασκευής δομούν εξολοκλήρου *νέα και*

[303] Κύρια, βιβλιογραφική αναφορά: [BILAR-IM].

[304] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM].

διαφορετικά, επιβλαβή παράγωγα.[305] Μια *πληθώρα επιλογών κεφαλής, αυτοάμυνας ακόμα και ωφέλιμου φορτίου* υπάρχει για να καλύψει πολύπλευρες και διαφορετικές ανάγκες, μετατρέποντας παράλληλα σε παιχνίδι για τον επιτιθέμενο την παραγωγή του οπλοστασίου του. Λόγου χάριν η παροχή και κατάλληλη χρήση μηχανών μετάλλαξης μπορεί να προσδώσει τον απαιτούμενο πολυμορφισμό ή μεταμορφισμό στις γενιές των ιών και σκουληκιών που θα παραχθούν, ενώ αντίστοιχα ο εφοδιασμός με κάποιες, σύνθετες τεχνικές θωράκισης[306] μπορεί να προστατεύσει τα κακόβουλα προϊόντα μιας γεννήτριας από διάφορες ευριστικές και άλλες στοχαστικές, έμμεσες μεθόδους εντοπισμού.

Examples of Virus Generator Kits

Name of Generator Kit	Description
NRLG (NuKE's Randomic Life Generator)	Released in 1994 by the virus writer Azrael. Very similar to VCL.
OMVCK (Odysseus Macro Virus Construction Kit)	This kit was released in early 1998. It can generate Word Basic macro-virus source code.
SSIWG (Senna Spy Internet Worm Generator)	Released in 2000 in Brazil. This generator supports the creation of VBS worms.
NEG (NoMercy Excel Generator)	This was the first Excel macro virus generator kit (1998). It creates .bas files.
VBSWG (VBS Worm Generator)	Released in 2000 by [K]Alamar. Generates various script worms.
AMG (Access Macro Generator)	Created in 1998 by the virus writer Ultras to generate Access97 macro viruses.
DREG (Digital Hackers' Alliance Randomized Encryption Generator)	Released in 1997 by Gothmog. Supports advanced code morphing and antiheuristics.

Σχήμα 20: Παραδείγματα γεννητριών κακόβουλου, ιομορφικού και άλλου, αυτοαναπαραγόμενου κώδικα

Η μεγάλη αυτή ποικιλομορφία λύσεων, που προσφέρει ένα σετ εργαλείων κατασκευής, μπορεί να αποτελέσει *μεγάλο πονοκέφαλο για τους υπερασπιστές της ασφάλειας* συστημάτων, αφού η δυσκολία στον εντοπισμό και την αναγνώριση όλων των πιθανών παραγώγων ενδέχεται να είναι αρκετά σημαντική.[307] Η γνώση αυτού του κινδύνου, σε συνδυασμό με την

[305] Κύρια, βιβλιογραφική αναφορά: [SZOR-ACVRD].

[306] Προστασία από debuggers, disassemblers, emulators, σύνθετα heuristics, goat files, honeypots κτλ, όπως την αναλύσαμε στο σχετικό εδάφιο 3.2.4.

[307] Πηγή: "Virii Generators: Understanding the Threat", James Tarala, 2002, διαθέσιμο από το δεσμό http://vx.netlux.org/lib/ajt00.html.

όποια *ευκολία χρήσης* και τις *δυνατότητες παραμετροποίησης*, που διακρίνουν εν γένει τις γεννήτριες κατασκευής, τις καθιστά ανάρπαστες και περιζήτητες στους κόλπους επίβουλων δυνάμεων.[308] Όσο μεγαλύτερη, βέβαια, δημοφιλία απολαμβάνει ένα πρόγραμμα αυτοματοποιημένης παραγωγής αυτοαναπαραγόμενου κακόβουλου λογισμικού, τόσο περισσότερες είναι οι πιθανότητες να έχει προσελκύσει την προσοχή και να έχει γίνει αντικείμενο έρευνας, ώστε να είναι ενημερωμένα τα τρέχοντα συστήματα ασφάλειας και να παρέχουν έτοιμες λύσεις προστασίας και τις μεθόδους εντοπισμού, τόσο του ίδιου όσο και των γεννημάτων του. Για αυτό το λόγο, παρατηρείται μια συνεχής δραστηριότητα συγγραφής νέων ή τροποποίησης, αναθεώρησης και αναβάθμισης υπαρχόντων σετ εργαλείων αυτοματοποιημένης κατασκευής, που φιλοδοξούν να δράσουν ανενόχλητα, ωσότου και αυτά με τη σειρά τους υποπέσουν στην αντίληψη και εντοπιστούν από κάποιον χρήστη, ερευνητή ή ευριστικό σύστημα ασφάλειας. Αυτός ο κύκλος δε φαίνεται να έχει, τουλάχιστον προς το παρόν, κάποιο προφανές σημείο εξόδου και η προκαλούμενη ανησυχία στις τάξεις των φρουρών της ασφάλειας διαρκώς μεγαλώνει.

3.2.6 Ευφυής Προσαρμογή

Μια ιδιαίτερα σύγχρονη και πλέον επιτυχημένη προσέγγιση στις επιθέσεις με κακόβουλο, αυτοαναπαραγόμενο λογισμικό εξοπλίζει ιούς και σκουλήκια με κατάλληλους μηχανισμούς προσαρμογής στο εκάστοτε περιβάλλον τους. Ένα προσαρμοστικός, κακόβουλος κώδικας παρέχει τη *δυνατότητα αναγνώρισης των διαφόρων, περιβαλλοντικών προκλήσεων και κατάλληλης ανταπόκρισης σε αυτές* και αυτό μπορεί να είναι κάτι ιδιαίτερα σημαντικό για την όλη διαδικασία διάδοσης.[309]

Ουσιαστικά, οι ιοί και τα σκουλήκια αποκτούν, ούτε λίγο ούτε πολύ, ένα δικό τους εκλεπτυσμένο σύστημα παρακολούθησης, διάγνωσης και αναγνώρισης (MDI system)[310] των βασικών συστατικών του περιβάλλοντός τους. *Με την παρουσία και βοήθεια συγκεκριμένων αισθητηρίων οργάνων (sensors)*, αλλά και την *εφαρμογή διαφόρων ευριστικών αλγορίθμων*, το επιβλαβές, αυτοαναπαραγόμενο λογισμικό *δύναται να αντιληφθεί πλήθος περιβαλλοντικών συνθηκών και συνιστωσών, καθώς και τις όποιες μεταβολές αυτών*, όπως π.χ.:

---

[308] Δεν είναι και ιδιαίτερα δύσκολο πλέον να αποκτήσει κανείς σήμερα μια τέτοια γεννήτρια. Η διαθεσιμότητα αυτών των προγραμμάτων αυξάνεται ολοένα στο χώρο του Διαδικτύου, από όπου είτε υπογείως είτε απροκάλυπτα, άλλοτε μέσω αμοιβής και άλλοτε χωρίς τίμημα, μπορεί κάποιος να τα προμηθευτεί.

[309] Η δυνατότητα προσαρμογής εξασφαλίζει ουσιωδώς μεγαλύτερες πιθανότητες επιβίωσης για το οπλολογισμικό και το φορτίο αυτού από μια απλή μέθοδο αυτοάμυνας, που δεν μπορεί να προβλέψει το είδος και την πολυπλοκότητα των περιβαλλοντικών συνθηκών, ούτε μπορεί να ανταποκριθεί το ίδιο αποτελεσματικά σε όλες τις πιθανές αλλαγές.

[310] Με την έννοια και τον τρόπο λειτουργίας που περιγράψαμε στο εδάφιο 2.2.8.

1. Παρουσία και δράση μηχανισμών προστασίας και συστημάτων ασφάλειας (host- ή network-based).
2. Δικτυακή Κίνηση/Συμφόρηση.
3. Παρουσία και δράση κακόβουλου λογισμικού σε σύστημα-στόχο.
4. Είδος και Παραμετροποίηση Λ/Σ στόχου.
5. Δυνατότητες υλικού στόχου (Επεξεργαστής, Μνήμη, Δίσκος, Δικτυακή Υποδομή).

Με οδηγό τις βασικές αυτές αισθήσεις, μπορεί ένας ιός ή ένα σκουλήκι *δυναμικά και σκόπιμα να προσαρμόζει, με συγκεκριμένο τρόπο, τον κώδικά του και αναλόγως να προσλαμβάνει ή αποβάλλει ορισμένα χαρακτηριστικά στη συμπεριφορά και να εφαρμόζει αντίστοιχα πρότυπα στη δράση του, έτσι ώστε να εκμεταλλεύεται με τον καλύτερο τρόπο την όποια συγκυρία στις προσλαμβάνουσες παραστάσεις ή/και να εξυπηρετεί πιο αποτελεσματικά τις ιδιαίτερες απαιτήσεις μιας επίθεσης, παρουσία συγκεκριμένων συνθηκών*. Η παραπάνω προσαρμογή μπορεί να γίνεται με *ενδογενή, αυτόματο τρόπο* ή/και *χειροκίνητα κατόπιν επικοινωνίας και κατάλληλης καθοδήγησης από κάποιο απομακρυσμένο κέντρο συντονισμού και λήψης αποφάσεων (command and control entity)*[311], που είναι υπεύθυνο για την παροχή εναλλακτικών σχεδίων δράσης. Η ενσωμάτωση ή και εξωτερική κλήση σετ εργαλείων αυτοματοποιημένης κατασκευής κώδικα παρέχει ένα ακόμη ισχυρό και ιδιαίτερα ανεπτυγμένο σύμμαχο, καθώς μπορεί να διευκολύνει και να επιταχύνει την όλη διαδικασία.

Το κακόβουλο λογισμικό αυτοαναπαραγωγής, στα πλαίσια ενός μηχανισμού ευφυούς προσαρμογής, μπορεί να αποφαίνεται στις εκάστοτε συνθήκες και συνιστώσες με μια ποικιλία από διαφορετικές λειτουργίες, καθώς και με συνδυασμούς αυτών. Παρακάτω, συνοψίζονται ορισμένα από τα πλέον κεντρικά μοτίβα:

- *Αυξομειώσεις μεγέθους κώδικα*:

  Ένας απλός τρόπος κάλυψης ή μια ενίσχυση με τις απαραίτητες λειτουργίες, όταν συγκεκριμένες παραστάσεις του περιβάλλοντος το επιτρέπουν, το υπαγορεύουν, το ευνοούν.

- *Μεταβολές κινητικότητας*:

  Το κακόβουλο λογισμικό αναστέλλει ή επιταχύνει, κατά βούληση και σε εναρμόνιση με τις επικρατούσες συνθήκες, την ταχύτητα διάδοσής του και αντίστοιχα περιορίζει ή βιάζει τη διεισδυτικότητα και τη διασπορά του.

- *Μεταπτώσεις* από και σε λανθάνουσα κατάσταση.

  Η τέχνη του «κρυφτού» στην υπηρεσία της ευφυούς, δυναμικής προσαρμογής.

- *Προσαρμογή δικτυακών επικοινωνιών*:

  Ο κακόβουλος κώδικας –κυρίως στα σκουλήκια- μπορεί να μεταβάλλει κάθε στιγμή το είδος και το μέγεθος της δικτυακής κίνησης με βάση τα ιδιαίτερα περιβαλλοντικά χαρακτηριστικά. Π.χ. η παρουσία ενός NIDS μπορεί να σημάνει συναγερμό σίγασης για ένα σκουλήκι, ενώ η αναγνώριση μιας «τρύπας» σε κάποιον HTTP εξυπηρετητή μπορεί να αποτελεί υπόδειξη επιλογής κα χρησιμοποίησης TCP πακέτων υπονόμευσης από μια δεξαμενή πιθανών κεφαλών.

- *Καταστολή μηχανισμών προστασίας και ασφάλειας συστημάτων-στόχων*:

  Το κακόβουλο λογισμικό καταφεύγει σε ρετροϊομορφικές και άλλες ενεργητικές στρατηγικές, κατόπιν εντοπισμού πιθανών εχθρών του.

- *Σκόπιμες μεταλλάξεις*:

  Επιστρατεύονται πολυμορφικές, μεταμορφικές και άλλες εξελικτικές τεχνοτροπίες, για να παράγουν «δαρβινικά» ισχυρότερες γενιές κώδικα, ενώπιον συγκεκριμένων, περιβαλλοντικών προκλήσεων και περιστάσεων, που επιβάλλουν ή πριμοδοτούν τον καλύτερα προστατευμένο κώδικα.

- *«Κατά παραγγελία» πλάνα δράσης*:

  Ίσως το μεγαλύτερο κληροδότημα του μηχανισμού της προσαρμογής. Οι εκάστοτε παραμετροποιήσεις των συστημάτων-στόχων μαζί με τις λοιπές περιβαλλοντικές συνιστώσες τροφοδοτούν μια ευρύτερη και αδιάκοπη διαδικασία:

  --δυναμικής βελτιστοποίησης υπαρχόντων χαρακτηριστικών του κώδικα του κακόβουλου λογισμικού,

  --επιλογής των εντός-κώδικα κάλλιστων εναλλακτικών και

  --κατ' απαίτηση κατάστρωσης ή εξωτερικής πρόσληψης νέων σχεδίων.

  Τελική έξοδος της διαδικασίας αυτής είναι κάθε φορά μια στρατηγική πλήρως προσανατολισμένη στον τρέχοντα στόχο και εναρμονισμένη ιδανικά με τις υπόλοιπες, υπάρχουσες συνθήκες.

- *Μνήμη και Μάθηση*:

---

[311] Κύρια, βιβλιογραφική αναφορά: [FERNANDEZ_BUREAU-OM].

Ορισμένες φορές στα συστήματα προσαρμογής συναντάται η ύπαρξη και κάποιου στοιχείου ή μηχανισμού μνήμης ή μάθησης, που σκοπό έχει να αυξήσει την ταχύτητα και την αποτελεσματικότητα της ανταπόκρισης, σε γνωστές συγκυρίες και συνθήκες, και προσδίδει, άλλωστε, περισσότερο κύρος και ευφυΐα στην όλη διαδικασία της προσαρμογής. Στην περίπτωση του κακόβουλου, αυτοαναπαραγόμενου λογισμικού, η υλοποίηση με τη βοήθεια γενετικών αλγόριθμων είναι η πλέον συνηθισμένη πρόταση για τον εν λόγω μηχανισμό μνήμης και μάθησης.

Γενικότερα, η παρουσία του συστήματος προσαρμογής στο σώμα ενός ιού ή σκουληκιού προσδίδει ένα *πολύ σημαντικό βαθμό ευελιξίας στον κακόβουλο κώδικα* και αποδεικνύεται πολύ χρήσιμο εργαλείο στη σχετική επιτυχία μιας επίθεσης με οπλολογισμικό.

3.3 Ταξινομία του οπλοστασίου

Το αυτοαναπαραγόμενο, επιβλαβές λογισμικό, όταν βρίσκεται στην υπηρεσία πληροφοριακής εχθροπραξίας, όπως είδαμε, διακρίνεται από τη δυνατότητα παρουσίας ιδιαίτερα χρήσιμων στον επιτιθέμενο ιδιοτήτων, που το καθιστούν ένα πραγματικό υπερόπλο.

Τα χαρακτηριστικά αυτά που κάλλιστα θα μπορούσαν να αποτελούν γενικά παραδεκτές, επιθυμητές ιδιότητες οποιουδήποτε οπλικού συστήματος, παρουσιάστηκαν και αναλύθηκαν επισταμένως σε διαφορετικά σημεία και πρότερα εδάφια του κεφαλαίου τούτου και συνοψίζονται παρακάτω:

- **Αξιοπιστία όπλου (Reliability):** Οι ιοί και τα σκουλήκια αποτελούν αξιόλογα όπλα «κυβερνετικού πολέμου», πάνω στα οποία μπορεί να «χτιστεί» μια ικανοποιητικά ελεγχόμενη, επιθετική επιχείρηση. Μια κακόβουλη οντότητα μπορεί να κάνει χρήση και συμβιβασμό των προτερημάτων των ακόλουθων μηχανισμών για να πετυχαίνει μεγάλο βαθμό υπακοής και καθοδήγησης της συμπεριφοράς του οπλικού της συστήματος:

    - Αυτοματισμός (Automation): Μεγάλο μέρος του κώδικα του οπλολογισμικού μπορεί να παραχθεί με αυτόματο τρόπο (π.χ. μέσω generation kits), ενώ και στο ίδιο το πρόγραμμα μπορεί να δοθεί σημαντικός βαθμός αυτονομίας στη δράση (απουσία απευθείας αλληλεπίδρασης και παρέμβασης).

- Απομακρυσμένη διαχείριση – Τηλεκατεύθυνση (Remote Control): Πολλοί τρόποι υπάρχουν για τη σύναψη σχέσεων και διόδων παρακολούθησης και διαχείρισης (rootkit, backdoors, κανάλια IRC) της δράσης του οπλολογισμικού, καθ' όλη τη διάρκεια των επιθετικών ενεργειών.

- **Ανωνυμία πηγής (Source Anonymity):** Η εισβολή και υπονόμευση των αντίπαλων ή παράπλευρων συστημάτων απαιτεί συνήθως μεγάλη διακριτικότητα και την καλύτερη δυνατή απόκρυψη της πηγής του προβλήματος. Τα αυτοαναπαραγόμενα όπλα καλύπτουν αυτές τις απαιτήσεις με μια σειρά από εξαιρετικά, χαρακτηριστικά γνωρίσματα, που θίξαμε κατά μήκος αυτού του κεφαλαίου και επαναλαμβάνουμε εδώ για λόγους εξυπηρέτησης της τρέχουσας επιχειρηματολογίας:

  - Γαμψή εισβολή: Άμεσο, καίριο «χτύπημα» στο πλέον αδύναμο σημείο των στόχων.
  - Έμμεση στόχευση: Ο δράστης μπορεί να «κρυφτεί» με εύκολο τρόπο πίσω από άλλες, τρίτες οντότητες (όπως π.χ. zombies, επιθέσεις DDoS), για να πλήξει με μη ανιχνεύσιμο τρόπο τον βασικό του στόχο.
  - Μη ανιχνεύσιμη προσβολή και εμφύτευση: Η αρχική διοχέτευση ιών και σκουληκιών γίνεται με τη βοήθεια μεθόδων, που παρέχουν σημαντική ανωνυμία στον δράστη.
  - Κρυφά κανάλια επικοινωνίας και ελέγχου: Η λήψη δεδομένων από τα μολυσμένα συστήματα και αντίρροπα η παροχή πληροφοριών καθοδήγησης στο αυτοαναπαραγόμενο όπλο μπορεί να γίνεται με τη βοήθεια διακριτικών καναλιών επικοινωνίας (π.χ. συγκαλυμμένα κανάλια[312], ανώνυμη ηλεκτρονική αλληλογραφία κ.ά.), ώστε να προστατεύεται η ταυτότητα του δράστη.

- **Κλιμακωσιμότητα**: Το απαιτούμενο εύρος εξάπλωσης, τα κίνητρα και τα ποθούμενα αποτελέσματα, η επιθυμητή ταχύτητα στην μετάδοση και την υπονόμευση, όλα αποτελούν ζητούμενα που πρέπει να ρυθμίζει και να ικανοποιεί ένα οπλικό σύστημα. Στα πλαίσια αυτά, οι ιοί και τα σκουλήκια επιτρέπουν μια μεγάλη κλιμακωσιμότητα (σε είδος, εύρος και αποτελέσματα) των επιθέσεων, χάρη κυρίως στους ακόλουθους μηχανισμούς:

[312] Για τα συγκεκριμένα θα μιλήσουμε πιο αναλυτικά στο πέμπτο κεφάλαιο της εργασίας (5.1.1).

- Τύπος «ωφέλιμου» φορτίου (Payload Genre): Το είδος του φορτίου στα κυβερνοόπλα αντικατοπτρίζει αμφιμονοσήμαντα τις επιθυμίες του συγγραφέα τους, αλλά και του δράστη μιας επίθεσης με αυτά. Η ύπαρξη του εν λόγω χώρου στον κώδικα υπάρχει ακριβώς για να παρέχει στους δράστες το μέσο για τη μελέτη μιας ποικιλίας διαφορετικών προσεγγίσεων, μεθοδολογιών, αλλά και πιθανών αποτελεσμάτων και συνεπώς την κατάστρωση διαφορετικών σχεδίων δράσης και τη χάραξη της επιθυμητής στρατηγικής.
- Αυτοματοποιημένες γεννήτριες κακόβουλου κώδικα: Όλη η επιχειρησιακή λογική μιας επίθεσης μπορεί να παραχθεί κατά παραγγελία από έξυπνες γεννήτριες κώδικα, οι οποίες επιδέχονται σημαντικής παραμετροποίησης των παραγόμενων όπλων, ώστε αυτά να ταιριάζουν περισσότερο στις ανάγκες του κάθε δράστη.
- Κινητικότητα/Ευκινησία (Cruising, Mobility): Το οπλολογισμικό σήμερα ρέει στις ταχύρρυθμες, δικτυακές αρτηρίες και ταξιδεύει μέχρι τα πέρατα της Γης και του κάθε ΠΣ, πολύ πιο συχνά από την εποχή των πρώτων γενεών κακόβουλων προγραμμάτων, δίνοντας τη δυνατότητα εύρεσης και στόχευσης και του πιο απομακρυσμένου, επιθυμητού σημείου. Η ολοένα αυξανόμενη, παρατηρούμενη κινητικότητα του κακόβουλου, αυτοαναπαραγόμενου κώδικα είναι ίσως από τα πιο ενδιαφέροντα, τρέχοντα χαρακτηριστικά του και αποτελεί το θεμελιώδες «κύτταρο» της κλιμακωσιμότητάς των παραγώγων και εκπροσώπων του.

- **Αντοχή (Endurance)**: Όλοι οι προαναφερόμενοι μηχανισμοί αυτοάμυνας, αλλά και η ίδια η ιδιότητα της παραμένουσας μόλυνσης συνθέτουν ένα ιδιαίτερα ανθεκτικό στις έξωθεν «πιέσεις» όπλο. Συνοψίζουμε παρακάτω τους θεμέλιους λίθους της ανθεκτικότητας ιών και σκουληκιών:

  - Παραμονή: Συνέχιση της παρουσίας και δράσης μιας προσβολής, αν και εφόσον δεν αφαιρεθεί πλήρως από κάποιο, μολυσμένο σύστημα.
  - Μετάπτωση: Λειτουργία ή Αεργία, ανάλογα με το ενδεχόμενο ή τον εντοπισμό κινδύνου.
  - Απόκρυψη ή Θωράκιση (Stealth or Armoring): Καμουφλάρισμα και παθητικού τύπου προστασία από τους μηχανισμούς άμυνας των ΠΣ.
  - Εξέλιξη/Μετάλλαξη (Evolution/Mutation): Τυχαίου τύπου παραλλαγή του κώδικα και των ιδιοτήτων των προγραμμάτων, με σκοπό τη μεγαλύτερη

δυνατή «ταλαιπωρία» των συστημάτων προστασίας των ΠΣ και την επιβίωση των δυνατότερων γενεών.

- Ρετροϊομορφισμός – Retroviral property: Επιθετική αχρήστευση εγγενών και παρένθετων συστημάτων ασφάλειας.
- Υπονόμευση Λ/Σ → Τεχνικές σήραγγας: Όσο γίνεται πιο διακριτική κατάληψη και χειραγώγηση των μηχανισμών λειτουργίας ή/και ασφάλειας των συστημάτων.

- **Προσαρμοστικότητα και ευελιξία**: Οι σύγχρονες εκφάνσεις οπλολογισμικού, όπως είδαμε γίνονται σταδιακά όλο και πιο ευέλικτες στο χειρισμό των λιγότερο ή περισσότερο απότομων αλλαγών του περιβάλλοντος τους, στο οποίο «μαθαίνουν» να ανταποκρίνονται με μεγαλύτερη αποτελεσματικότητα. Οι μηχανισμοί που κρύβονται πίσω από τη συγκεκριμένη, εξελικτική πορεία και εγγυώνται την μακροημέρευση ιών και σκουληκιών υπενθυμίζουμε πως είναι:

  - Προσαρμογή (Adaptation/Adaptivity): Δυναμική μεταβολή των ιδιοτήτων και του κώδικα, ανάλογα με το περιβάλλον αναφοράς και τις εκάστοτε, επικρατούσες συνθήκες.

Η επιτυχία -θεωρούμενη με την ευρεία έννοια της ικανοποίησης στρατηγικών σκοπών και στόχων- μιας συγκεκριμένης πληροφοριακής επίθεσης είναι, συνήθως, άμεση συνάρτηση των παραπάνω παραγόντων. Τα γνωρίσματα αυτά είναι τόσο σημαντικά, ώστε να αποτελούν καθοριστικές προϋποθέσεις για την εξασφάλιση ορισμένων κατεξοχήν κρίσιμων και αρκετά διαφορετικών μεταξύ τους στόχων του επιτιθέμενου, όπως:[313]

1. **Αξιοπιστία επίθεσης**: Αναφερόμαστε στην ανάγκη για αποτελεσματικό έλεγχο επί του τρόπου εκτέλεσης και των ιδιαίτερων επιπτώσεων μιας επίθεσης.
2. **Ανωνυμία κι μη ανιχνευσιμότητα επιτιθέμενης οντότητας**: Έχει να κάνει με τη διαβεβαίωση πως ο επιτιθέμενος δε θα θεωρηθεί ή αποδειχθεί με συγκεκριμένα και ευσταθή πειστήρια υπαίτιος/υπεύθυνος μιας εχθροπραξίας.
3. **Ταχύτητα εκδήλωσης και εξάπλωσης**: Κάθε επίθεση έχει και διαφορετική αντίληψη του χρόνου· έτσι κάποιες φορές υπάρχει η ανάγκη για γρήγορη και πολύ

[313] Οι στόχοι αυτοί είναι οι πλέον προφανείς για κάθε κακόβουλο συγγραφέα και επιτιθέμενο ιδίως στην περιοχή δράσης που ορίζει μια πληροφοριακή εχθροπραξία, αλλά και γενικότερα -ούτε λίγο ούτε πολύ- σε κάθε έκφανση επίθεσης με κακόβουλο κώδικα.

κινητική δράση και άλλες πάλι για αργή, διακριτική εξέλιξης και μετακύλησης των τεκταινόμενων.

4. **Εύρος και εμβέλεια**: Μιλάμε για τις απαιτήσεις διείσδυσης, διάδοσης και διασποράς στις διάφορες αρχιτεκτονικές και πλατφόρμες ΠΣ, που έχει προδιαγράψει και καλείται να ικανοποιήσει ο επιτιθέμενος.
5. **Επιτυχία παράδοσης φορτίου**: Ο σημαντικότερος ίσως και αρκετά πρόδηλος στόχος είναι η μεγαλύτερη δυνατή εξασφάλιση της επιτυχίας στην εκτέλεση του σκοπού που «κρύβεται» σχεδόν πάντα εντός του «ωφέλιμου» φορτίου του κακόβουλου όπλου.

Η αποτελεσματικότητα ικανοποίησης των παραπάνω, στρατηγικών στόχων εξαρτάται από τον ιδιαίτερο βαθμό εμφάνισης εκείνων των (σχεδιαστικών απαιτήσεων και) παραγόντων, οι οποίοι παίζουν σημαντικό ρόλο κάθε φορά και συντελούν στην εκπλήρωση των εκάστοτε αυτών στόχων. Στην εν λόγω εργασία, θα σταθούμε αφενός μεν στην επιθεώρηση και επισήμανση του ιδιαίτερου ρόλου της ανωνυμίας πηγής και της αξιοπιστίας του μεταχειριζόμενου όπλου, αφετέρου δε θα θίξουμε τα πολλαπλά οφέλη μιας ισορροπημένης σχέσης μεταξύ ανθεκτικότητας και κινητικότητας του αυτοαναπαραγόμενου, επιβλαβούς κώδικα και, τέλος, θα αναδείξουμε ως μείζον θέμα επιτυχίας, «προόδου» και περαιτέρω όξυνσης των πληροφοριακών επιθέσεων με οπολολογισμικό, την παρουσία και ενεργοποίηση στις διάφορες, κλασσικές, ιομορφικές και στις άλλες, πιο δικτυοστρεφείς, υποστάσεις του, εξειδικευμένων μηχανισμών για την καλύτερη προσαρμογή τους, στις επιταγές του πιθανού οικοσυστήματος, στο οποίο αυτές κάθε φορά οργανώνονται και καλούνται, ανάλογα και με τους εκάστοτε στόχους, να δράσουν και να «επιβιώσουν»/εξαπλωθούν.

Με βάση την αναγκαιότητα ύπαρξης, το βαθμό και τον τρόπο επίδρασης καθενός εκ των παραπάνω χαρακτηριστικών στην αποτελεσματικότητα των τυχόντων στόχων μιας επίθεσης μπορεί κανείς να ταξινομήσει το αυτοαναπαραγόμενο, κακόβουλο λογισμικό σε 4 κύρια είδη. Τα είδη αυτά στην παρόν έργο αποτελούν προϊόντα πρωτογενούς στοχασμού, ανάλυσης και συνεκτίμησης και καινοφανούς παρουσίασης των υπό συζήτηση παραγόντων, με απώτερο στόχο τη *θεμελίωση ενός νέου σημείου αναφοράς και αφετηρίας έρευνας για την καλύτερη αξιολόγηση και μεγαλύτερη επίγνωση/αντίληψη του ιδιαίτερου χαρακτήρα και των γνωρισμάτων κάθε πληροφοριακής επίθεσης με χρήση οπλολογισμικού*. Ας παρουσιάσουμε και σχολιάσουμε, τώρα, τις 4 τον αριθμό προτεινόμενες κατηγορίες.

3.3.1 Α' Είδος: Αξιοπιστία-Ανωνυμία Πηγής

Στην περίπτωση αυτή, κύριο μέλημα του επιτιθέμενου είναι να εκδηλώσει μια κατά το δυνατόν αξιόπιστη επίθεση, που να διατηρεί την ταυτότητα του επιτιθέμενου όσο γίνεται πιο ασφαλή από τον αντίπαλο. Υποθέτουμε ότι οι υπόλοιποι στόχοι είναι αμελητέας προτεραιότητας σε σχέση με την παραπάνω απαίτηση.

Η κατηγορία αυτή (Type 0) αποτελεί τον ελάχιστο συνδυασμό απαιτούμενων ιδιοτήτων του κακόβουλου, αυτοαναπαραγόμενου όπλου, η ύπαρξη των οποίων εξασφαλίζει ικανοποιητικό βαθμό αποτελεσματικότητας στην εξυπηρέτηση των δύο αυτών, πλέον βασικών στρατηγικών στόχων του επιτιθέμενου.

Εφόσον είναι λογικό κάθε επιτιθέμενος να επιθυμεί την επιτυχή ολοκλήρωση της επίθεσης του με την παράδοση του όποιου φορτίου, εύκολα διαπιστώνει κανείς πως η συγκεκριμένη κατηγορία είναι μάλλον κάπως εκφυλισμένη, μιας και στερείται πρακτικού νοήματος. Μια πληροφοριακή επίθεση, που δεν φροντίζει έστω υποτυπωδώς για την επιτυχία παράδοσης του φορτίου της, δεν ανήκει και τόσο στη σφαίρα της πραγματικότητας και δεν πρέπει να νοείται ως κανονική επίθεση. Παρόλ' αυτά, σκοπός παράθεσης του συγκεκριμένου είδους είναι η ανάδειξη της αναγκαιότητας εκπλήρωσης των 2 υπό εξέταση, εξαιρετικά σημαντικών και πολύτιμων, ιδιοτήτων, σε κάθε απόπειρα ουσιαστικής, πληροφοριακής επίθεσης:

- *Αξιοπιστία*, για να μην ξεφεύγει μια επίθεση από τον έλεγχο του επιτιθέμενου ή να μην προκαλεί αποτελέσματα που ο επιτιθέμενος δεν έχει προβλέψει και σχεδιάσει ή ακόμα περισσότερο δεν επιθυμεί, ανεξάρτητα από την επιτυχία στην παράδοση του φορτίου. Η δυνατότητα αυτοματοποίησης και απομακρυσμένης διαχείρισης του ολπολογισμικού παρέχουν τα πλαίσια της αξιοπιστίας αυτής.
- *Ανωνυμία Πηγής*, ώστε να εξασφαλίζεται στον επιτιθέμενο, τόσο στην περίπτωση αποτυχίας όσο και στην αντίστοιχη επιτυχίας παράδοσης του φορτίου, ένα είδος επιθυμητού άλλοθι ή ένας σημαντικός βαθμός μη ανιχνευσιμότητας.

Οποιαδήποτε πραγματική επίθεση, που πετυχαίνει τρόπον τινά ή έστω αποπειράται την παράδοση κάποιου φορτίου πρέπει προηγουμένως να έχει φροντίσει να πληροί τις προϋποθέσεις αξιοπιστίας και ανωνυμίας.

Ιοί και σκουλήκια τύπου 0 είναι όσα στερούνται βασικών μηχανισμών ταχείας ή ευρείας διάδοσης, αυτοάμυνας και προσαρμογής, αλλά διαθέτουν και χρησιμοποιούν βασικούς ή ανεπτυγμένους μηχανισμούς αξιοπιστίας και ανωνυμίας πηγής.[314] Τέτοιοι ιοί ή σκουλήκια

[314] Τη λογική και μορφολογία αυτού του είδους αποτυπώνουμε γλαφυρά στο Σχήμα 21, που ακολουθεί παρακάτω.

στα πλαίσια πληροφοριακής εχθροπραξίας δεν απασχολούνται με την ταχύτητα ή την εμβέλεια μιας πληροφοριακής επίθεσης, ούτε καν με αυτή καθαυτή την επιτυχία παράδοσης του «ωφέλιμου» φορτίου, αλλά μόνο με την ανωνυμία της πηγής και την αξιοπιστία της επίθεσης. Λογισμικό τύπου 0 θα μπορούσε να μη φέρει καθόλου φορτίο. Σε περίπτωση ύπαρξης φορτίου, οι επιτιθέμενοι με λογισμικό αυτού του τύπου θα πρέπει να γνωρίζουν πως αφήνουν την επίθεση να εξελιχτεί με αδιάφορο και ελαφρώς τυχαίο τρόπο, όσον αφορά την ταχύτητα εκδήλωσης και εξάπλωσης και το εύρος διάδοσής της, αλλά ακόμα και την ίδια την παράδοση του φορτίου. Ο τυχαίος χαρακτήρας εξέλιξης δεν εγκυμονεί κίνδυνο ούτε έρχεται σε σύγκρουση με την απαιτούμενη αξιοπιστία ή την ανωνυμία της επίθεσης με λογισμικό τύπου 0, εφόσον θεωρούμε πως:

- η επιλογή χρήσης του λογισμικού αυτού είναι σκόπιμη και γίνεται από εχέφρονα επιτιθέμενο,
- το λογισμικό ελέγχεται ή έχει έτσι σχεδιαστεί, ώστε τα όποια αποτελέσματα της επίθεσης όσο τυχαία και αν έρθουν είναι γνωστά ή προβλεπόμενα και δεν αποτελούν μη αναμενόμενη, ανεπιθύμητη ή δυσμενή για αυτόν κατάληξη και
- η δράση του λογισμικού είναι κάθε φορά τέτοια, που δεν διακυβεύεται η αποκάλυψη της ταυτότητας ή της εμπλοκής του επιτιθέμενου στην επίθεση.

Όσο μεγαλύτερος ο βαθμός αξιοπιστίας και ανωνυμίας, που προσφέρει ένας ιός ή ένα σκουλήκι που ανήκει στην κατηγορία αυτή, τόσο πιο αποτελεσματικά εξυπηρετεί τους τρέχοντες στόχους ενός επιτιθέμενου, που όπως είπαμε αποτελούν τους πλέον πρωταρχικούς στόχους οποιασδήποτε σοβαρής πληροφοριακής επίθεσης και δεν είναι άλλοι από την εξαπόλυση μιας όσο το δυνατόν ανώνυμης και αξιόπιστης επίθεσης, ανεξάρτητα από το εύρος και το χρόνο διάδοσής της και την επιτυχία παράδοσης του φορτίου της.

3.3.2 Β' Είδος: Κινητικότητα ή Αντοχή;

Η κινητικότητα και η ανθεκτικότητα ενός ιού ή σκουληκιού είναι πολλές φορές ιδιότητες αλληλοσυγκρουόμενες. Η παρουσία πολύπλοκων ρουτινών κινητικότητας, για την κάλυψη των ιδιαίτερων απαιτήσεων μιας επίθεσης, πολλές φορές οδηγεί αναπόφευκτα και σε κάποια αύξηση του συνολικού όγκου του λογισμικού. Η πιθανή, παράλληλη ύπαρξη ανεπτυγμένων μηχανισμών άμυνας και αυτοπροστασίας σίγουρα ενισχύει την επιβίωση του λογισμικού και συνάμα του φορτίου αυτού, παρέχοντας τις προϋποθέσεις για επιτυχημένη παράδοσή του, αλλά μπορεί να επιβαρύνει επιπλέον το μέγεθός του. Μια υπέρογκη αύξησή του ενδέχεται, εν

τέλει, αντί να συμβάλλει θετικά λόγω της παρουσίας επισταμένων μεθόδων, να προκαλεί προβλήματα και να δυσχεράνει την ικανοποίηση ορισμένων στόχων κινητικότητας ιών και σκουληκιών. Η κινητικότητα από τη μεριά της μπορεί να προδώσει λόγω π.χ. υπερβολικής ταχύτητας, διεισδυτικότητας και διασποράς την παρουσία του οπλολογισμικού και να το εκθέσει σε κίνδυνο δοκιμάζοντας τα όρια της αντοχής του. Γενικότερα, *οι δράσεις των ξεχωριστών λειτουργιών αντοχής και κινητικότητας είναι δυνατόν να αποτελέσουν τροχοπέδη η μία για την άλλη. Οι στρατηγικές επιθυμίες του επιτιθέμενου είναι αυτές που θα καθορίσουν τελικά την όποια ισορροπία μεταξύ των δύο αυτών ιδιοτήτων*.

Όταν οι απαιτήσεις για επιτυχημένη παράδοση του φορτίου ξεπερνούν σε μεγάλο βαθμό αυτές για ευρεία ή ταχεία διάδοση ή όταν ο επιτιθέμενος επιθυμεί κατά κύριο λόγο την επιτυχημένη παράδοση του φορτίου, χωρίς να τον απασχολούν ιδιαίτεροι στόχοι ταχύτητας εκδήλωσης και εξάπλωσης και εμβέλειας δράσης του οπλολογισμικού, η αντοχή του λογισμικού προβάλλει ως σημαντικότερη ιδιότητα σε σχέση με την κινητικότητα. Σε τέτοιες συνθήκες βρίσκουν εφαρμογή ιοί και σκουλήκια που κατατάσσονται στο α' υποείδος τύπου I (Type Ia).[315] Το οπλολογισμικό αυτού του τύπου συνήθως φέρει ένα σύνθετο σύστημα αντοχής για να του εξασφαλίζονται οι μέγιστες πιθανότητες επιτυχίας στην παράδοση του φορτίου, ενώ οι ρουτίνες διάδοσης και διεύρυνσης είναι σημαντικά πιο στοιχειώδεις. Ταυτόχρονα, δίνεται προσοχή, ώστε η όποια, βασική κινητικότητά του να μην εκθέσει την ανθεκτικότητά του ή να προκαλέσει οποιαδήποτε ανεπιθύμητα προβλήματα στον περισσότερο σημαντικό στόχο της παράδοσης του φορτίου.

Αν πάλι η επιτυχημένη παράδοση του φορτίου απασχολεί λιγότερο σε σχέση με την ευρύτητα και την ταχύτητα εκδήλωσης και εξάπλωσης της επίθεσης, τότε οι μηχανισμοί αντοχής είναι σαφώς πιο υποτυπώδεις από του προηγούμενου υποείδους και δίνεται ιδιαίτερο βάρος, ώστε να μην παρακωλύουν την επιθυμητή κινητικότητα. Ο επιτιθέμενος στις περιπτώσεις αυτές είτε:

- δεν επιθυμεί να εξαπολύσει κάποιο φορτίο (τετριμμένη περίπτωση) είτε
- ενδιαφέρεται πολύ περισσότερο να ικανοποιήσει κάποια χρονοδιαγράμματα και σχέδια εμβέλειας της επίθεσής του και είναι διατεθειμένος να ρισκάρει στην παράδοση του φορτίου προκειμένου να το επιτύχει (τυχαιότητα στην παράδοση του φορτίου) – η παράδοση του φορτίου, αν τελικά πραγματοποιηθεί, θα πρέπει να συμβεί στον χρόνο και το εύρος που τέθηκαν ως στόχοι της επίθεσης.

[315] Φαίνεται στο επάνω τμήμα του δεύτερου «παραθύρου» του Σχήματος 21.

Λογισμικό αυτού του τύπου ανήκει στο β' υποείδος (Type Ib).[316] Οι ρουτίνες κινητικότητας στα μέλη αυτής της υποκατηγορίας σαφώς υπερτερούν των αντίστοιχων της αυτοάμυνας και αυτοπροστασίας τους. Οι ιοί και τα σκουλήκια, που ανήκουν στον τύπο Ib, διαθέτουν τις απαραίτητες, κωδικοποιημένες, σύνθετες λειτουργίες διάδοσης και διεύρυνσης και το κατάλληλο μέγεθος, που θα τους επιτρέψουν να κινηθούν με βάση το επιθυμητό σχέδιο, ενώ λειτουργίες αντοχής είτε απουσιάζουν εντελώς (εκφυλισμένη κατάσταση) είτε υπάρχουν στοιχειωδώς και παρουσιάζονται σε τέτοιο βαθμό, που να μην αποτελούν εμπόδιο στην ποθούμενη κινητικότητα.

Πρέπει να τονιστεί ότι και τα 2 υποείδη αυτού του τύπου θεωρείται ότι παρέχουν άνευ όρων στον επιτιθέμενο τις πλέον βασικές, τύπου Ι ιδιότητες, αξιοπιστία δηλαδή της επίθεσης και ανωνυμία πηγής. Χωρίς αυτές, όπως εξηγήθηκε προηγούμενα, δεν εκπληρώνονται πρωταρχικότατοι στόχοι του επιτιθέμενου.

3.3.3 Γ' Είδος: Κινητικότητα και Αντοχή!

Η τρίτη κατηγορία (Type II) αποτελεί ουσιαστικά την ένωση των δύο υποειδών τύπου Ι.[317] Στην πράξη υπάρχουν σενάρια πληροφοριακής εχθροπραξίας που υπαγορεύουν την *ταυτόχρονη συνύπαρξη κινητικότητας και αντοχής ως απαιτήσεις για αποτελεσματική ικανοποίηση των στόχων της επιτιθέμενης οντότητας*. Πέρα από τη διαφύλαξη της ανωνυμίας του και την επιταγή για αξιόπιστη επίθεση, ο επιτιθέμενος πλέον θέτει ξεκάθαρους στόχους για την ταχύτητα εκδήλωσης και εξάπλωσης της επίθεσης και επιθυμεί την πραγμάτωση συγκεκριμένου πλάνου διείσδυσης και διασποράς της επίθεσης. Η επιτυχημένη παράδοση του φορτίου θεωρείται, επίσης, αδιαμφισβήτητη αναγκαιότητα της επίθεσης. Στις καταστάσεις αυτές, μας ενδιαφέρει εξίσου τόσο η κινητικότητα όσο και η ανθεκτικότητα του αυτοαναπαραγόμενου όπλου· η κινητικότητα για την εκπλήρωση των ιδιαίτερων χρονοδιαγραμμάτων και πλάνων διείσδυσης και διασποράς και η αντοχή ως ικανή και αναγκαία συνθήκη για την επιτυχία παράδοσης του φορτίου. Μας ενδιαφέρουν δε με τέτοιο τρόπο που να συμβιβάζονται και όχι να αλληλοαναιρούνται οι δράσεις τους λόγω π.χ. ακατάλληλου μεγέθους ή όγκου του όπλου ή ακόμα και απρόσεκτης και ή/και υπέρμετρης εκδήλωσης, εξάπλωσης και διεύρυνσης.

Ιοί και σκουλήκια του τύπου ΙΙ περιέχουν, συνήθως, λειτουργίες αυτοάμυνας που ενισχύουν την αντοχή τους, ώστε να παραδώσουν επιτυχώς το φορτίο του, και είναι δυνατόν να

[316] Που απεικονίζεται στο δεύτερο «παράθυρο» του Σχήματος 21.

[317] Βλέπε και το Σχήμα 21, λίγο πιο κάτω.

χρησιμοποιούν πολλές και διάφορες τεχνικές διάδοσης και εξάπλωσης[318], για την ικανοποίηση των ιδιαίτερων απαιτήσεων κινητικότητας που έχει θέσει η κάθε επίθεση. Η παρουσία των λειτουργιών αντοχής δε θα πρέπει σε καμία περίπτωση να δυσκολεύει την απαιτούμενη κινητικότητα, όμως, και η όποια ευκινησία να μην προδίδει τη μυστικότητα ή να μην περιορίζει την αντιδραστικότητα που προσφέρουν οι μέθοδοι αυτοπροστασίας. Το μέγεθος των προγραμμάτων της εν λόγω κατηγορίας πρέπει να είναι τέτοιο, ώστε να εξασφαλίζει τον κατάλληλο και απαιτητό μηχανισμό αντοχής, χωρίς όμως να παρεμποδίζεται η επιθυμητή κινητικότητα.

Όπως και στο β' είδος έτσι και εδώ η ικανοποίηση των πρωτογενών απαιτήσεων του επιτιθέμενου για ανωνυμία πηγής και αξιοπιστία της επίθεσης πρέπει να θεωρείται δεδομένη.

3.3.4 Δ' Είδος: Προσαρμογή στις εκάστοτε συνθήκες

Ο τέταρτος τύπος (Type III) αυτοαναπαραγόμενου, κακόβουλου λογισμικού αποτελεί την πλέον σύνθετη κατηγορία ιών και σκουληκιών. Ουσιαστικά, το τρίτο είδος *ενισχύεται περαιτέρω με την καθ' όλα σημαντική ιδιότητα της προσαρμογής*. Η προσαρμογή ως οπλικό σύστημα ενδυναμώνει περαιτέρω το αυτοαναπαραγόμενο, κακόβουλο λογισμικό του προηγούμενου τύπου, με εκείνες τις λειτουργίες που θα του επιτρέψουν να ικανοποιήσει πληθώρα από περίπλοκα μεταβαλλόμενες ή φαινομενικά αντικρουόμενες απαιτήσεις και να φέρει έτσι σε πέρας περίτεχνες επιθέσεις πληροφοριακής εχθροπραξίας.

Οι στόχοι του επιτιθέμενου και σε αυτήν την περίπτωση παραμένουν αδιαπραγμάτευτοι. Η μεγιστοποίηση της ανωνυμίας και της αξιοπιστίας της επίθεσης, καθώς και η εκπλήρωση των απαιτήσεων χρόνου, επιθυμητής εμβέλειας και επιτυχημένης παράδοσης του φορτίου είναι το ποθούμενο. Μόνο που, στην περίπτωση αυτή, το λογισμικό αυτοπροσαρμόζεται στις εκάστοτε συνθήκες, που συναντά στην χωροχρονική του πορεία μέχρι την παράδοση του φορτίου του, προκειμένου να ανταποκριθεί με τον καλύτερο τρόπο στην ικανοποίηση των προαναφερόμενων στόχων. Κάτι τέτοιο ουσιαστικά μπορεί να επιτρέπει στο κακόβουλο λογισμικό να «συναισθάνεται» κάθε φορά το εκάστοτε περιβάλλον του και αναλόγως με το αν κρίνει ότι κάποιες συνθήκες είναι αρκούντως ευνοϊκές ή αντίστοιχα δυσμενείς να μεταβάλλει κατάλληλα και σε προσωρινό ορίζοντα (fine tuning) τον τρέχοντα βαθμό κινητικότητας, αντοχής, ακόμα και ανωνυμίας ή αξιοπιστίας προκειμένου να βελτιστοποιήσει (optimization) ορθολογικά τη συνολική διαδικασία εξυπηρέτησης των στόχων της επίθεσης. Κάθε μια από τις 4 ιδιότητες του λογισμικό τύπου ΙΙ περιβάλλεται

[318] Σαν αυτές που παρουσιάστηκαν κα για τις οποίες έγινε εκτενής λόγος στο παρόν κεφάλαιο.

πλέον από το υπερκείμενο, εξωτερικό στρώμα της προσαρμογής[319], στης οποίας τις διαρκείς, διορθωτικές ρυθμίσεις ανά πάσα στιγμή υπόκειται. Αυτή είναι η εξαιρετικά χρήσιμη ικανότητα της προσαρμογής.

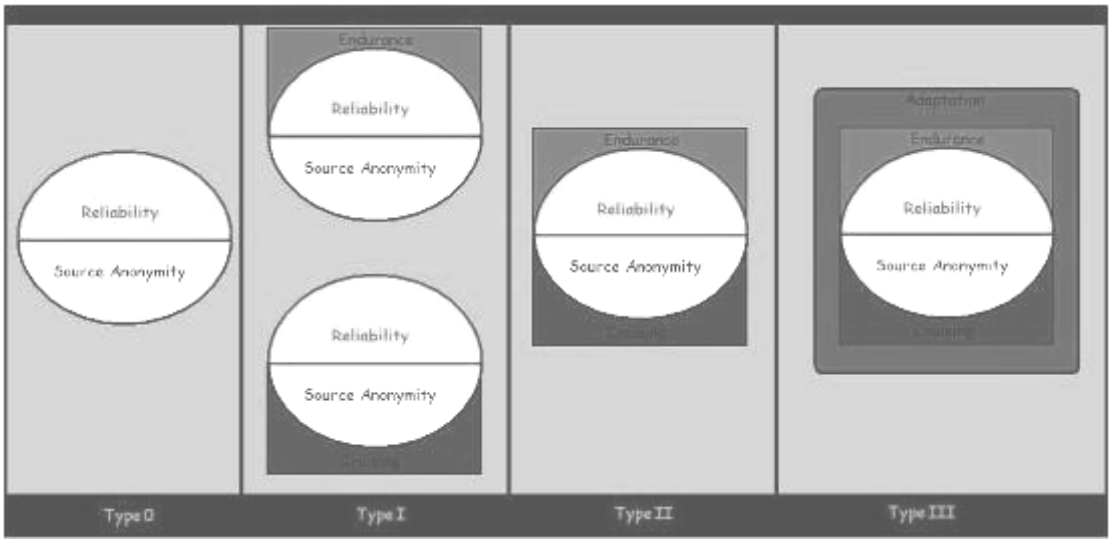
Ο τύπος αυτός λογισμικού είναι ο κατάλληλος για καταστάσεις, όπου το λογισμικό επίθεσης καλείται να βρεθεί σε πλήθος διαφορετικών συστημάτων και να ανταπεξέλθει σε ποικιλία συνθηκών και παραμετροποιήσεων, προκειμένου να ολοκληρώσει την αποστολή πληροφοριακής εχθροπραξίας που ανέλαβε. Σε καταστάσεις αυτού του είδους, τόσο η επιτυχής παράδοση ενός φορτίου, η επιθυμητή αξιοπιστία και εμβέλεια μιας επίθεσης και οι απαιτούμενοι χρόνοι εκδήλωσης και εξάπλωσης της, όσο και η ανωνυμία πηγής που αυτή οφείλει να προσφέρει, μπορούν να αποτελέσουν ακατόρθωτες «χίμαιρες», αν δεν υφίσταται κάποιος μηχανισμός που να προσδίδει στο οπλολογισμικό την απαραίτητη ευελιξία και να του επιτρέπει να αναπτύξει εκείνο το βαθμό προσαρμοστικότητας στο εκάστοτε περιβάλλον, που θα το συνδράμει στην πορεία εξέλιξης της επίθεσης, έτσι ώστε να τελεσφορήσει αποτελεσματικά τους στόχους αυτούς. Τα καθήκοντα του μηχανισμού αυτού έρχεται να επιτελέσει η ιδιότητα της προσαρμογής[320].

Η λογική που ακολουθήθηκε στην προηγούμενη ταξινόμηση ομοιάζει εκείνης της Joanna Rutkowska, που κατέταξε το κακόβουλο λογισμικό σε 4 τύπους από Type 0 έως Type III με βάση το μεγαλύτερο βαθμό υπονόμευσης του Λ/Σ[321], που τα διάφορα είδη είναι δυνατόν να επιτύχουν. Στην παρούσα περίσταση, το αντικείμενο υπήρξε ο μεγαλύτερος βαθμός εξυπηρέτησης των στόχων του επιτιθέμενου κατά τη διάρκεια πληροφοριακής εχθροπραξίας με αυτοαναπαραγόμενο, επιβλαβές λογισμικό. Οι 4 δυνατές κατηγορίες του λογισμικού που προέκυψαν φαίνονται σχηματικά παρακάτω:

[319] Όπως φαίνεται χαρακτηριστικά στο Σχήμα 21.

[320] Μια έκφανση του μηχανισμού της προσαρμογής μελετήσαμε μεθοδικά στο εδάφιο 3.2.6, στα πλαίσια των Βέλτιστων Πρακτικών του οπλολογισμκού.

[321] Κύρια, βιβλιογραφική αναφορά: [RUTKOWSKA-ISMT], [RUTKOWSKA-FSMTVOS].



Σχήμα 21: Πρότυπη ταξινόμηση των αυτοαναπαραγόμενων όπλων λογισμικού της πληροφοριακής εχθροπραξίας, με βάση αρχετυπικά χαρακτηριστικά τους, που θεωρούνται εγγυητές και απαραίτητοι όροι για την επιτυχία μιας κακόβουλης, κυβερνετικής επίθεσης

4 *Ασφάλεια και Προστασία πληροφορίας από επιθέσεις τύπου αυτοαναπαραγόμενου, επιβλαβούς λογισμικού*

Στο κεφάλαιο τούτο, γίνεται μια προσπάθεια ανάγλυφης παρουσίασης και περιγραφής των βασικότερων τεχνολογιών, διαδικασιών, κανόνων και μεθοδολογιών (αναφέρονται λύσεις αιχμής, μα και άλλες πιο διαχρονικές) που μπορούν να ενσωματωθούν στις τάξεις των ΠΣ, σήμερα, προκειμένου να τα καταστήσουν περισσότερο ανθεκτικά ή λιγότερο ευάλωτα στις πληροφορικές επιθέσεις μέσω ιών και σκουληκιών, των οποίων η σχετική δυναμική αναλύθηκε στο αμέσως προηγούμενο κεφάλαιο αφήνοντας έκδηλα υπονοούμενα για το μέγεθος των πιθανών, αρνητικών επιπτώσεων τους για τα στοχευμένα συστήματα. Τα κράτη, οι οργανισμοί, οι επιχειρήσεις και όλοι όσοι ενδιαφέρονται για την ασφάλεια των προσφιλών τους ΠΣ καλούνται να ενδυναμωθούν και να εξοπλιστούν καταλλήλως, αλλά και να προωθήσουν ευρύτερες, συνεργατικές δράσεις, προκειμένου να αντέξουν την αναμενόμενη, αλλά και μεγαλύτερη ίσως σφοδρότητα, και εδώ θα δούμε τι μπορούν να πράξουν και πώς δύνανται να το πραγματοποιήσουν για να εξασφαλίσουν αποτελεσματική οχύρωση και προστασία.

Με λίγα λόγια, ξεκινά από το σημείο αυτό η διατύπωση και ανάλυση των ενδεδειγμένων, περισσότερο ή λιγότερο αξιόπιστων, τρόπων άμυνας κόντρα στο αυτοαναπαραγόμενο οπλολογισμικό.

4.1 Βιομηχανία αντι-ιομορφικού λογισμικού/Υλισμικές λύσεις προστασίας

Η πρωταρχική, αμυντική απάντηση στα ποικίλα προβλήματα που φέρνει στην επιφάνεια το οπλολογισμικό και η μέσω αυτού κακόβουλη δράση δίνεται κυρίως από κατάλληλα, επιπρόσθετα στο υπάρχον ΠΣ, συστήματα υλικού και λογισμικού, όπως τα εμπεριστατωμένα εμπορικά προϊόντα της ευρύτερης βιομηχανίας προγραμμάτων κατά των ιών και σκουληκιών (antivirus industry), αλλά και τα αντίστοιχα, τεχνολογικά μέσα (firewalls, IDS/IPS κτλ) που προστατεύουν από γενικότερες επίβουλες και υπονομευτικές ενέργειες, εμποδίζοντας την παράνομη πρόσβαση και εκμετάλλευση των ΠΣ. Όσοι επιθυμούν τη μεγαλύτερη διαβεβαίωση από πλευράς λειτουργικής σταθερότητας και ανοσίας των κρίσιμων συστημάτων τους πρέπει να χαράξουν τη στρατηγική τους όσον αφορά την ασφάλεια πληροφοριών, ξεκινώντας από και στηριζόμενοι κατά μείζονα λόγο στις λύσεις αυτές, ενώ σκόπιμο κρίνεται να προσπαθούν διαρκώς να τις βελτιστοποιήσουν, διερευνώντας και σχεδιάζοντας με φειδώ τους τρόπους αποτελεσματικότερης υλοποίησης, εγκατάστασης και διαχείρισης τους.

Παρακάτω, στεκόμαστε με σχετικό βάθος στους βασικούς εκφραστές προστατευτικής δραστηριότητας που εμπίπτουν στην επαρκώς εγνωσμένη αυτή κατηγορία.

4.1.1 Σαρωτές

Οι σαρωτές κακόβουλου λογισμικού είναι η πλέον γνωστή κατηγορία λογισμικού κατά των ιών και των σκουληκιών, μια τεχνολογία που συνοδεύει τα επιβλαβή αυτά προγράμματα από την πρώτη περίοδο δράσης τους στο χώρο της πληροφορικής. Τα συστήματα σάρωσης (malware scanners) κακόβουλου λογισμικού *αποτελούν τον πυρήνα για πολλές εμπορικές και βιομηχανικές λύσεις* (τόσο ως καθαρά πακέτα λογισμικού, όσο και ενσωματωμένα σε υλισμικά προϊόντα όπως τα IDS/IPS[322]) στο χώρο της ασφάλειας δικτύων (και) δεδομένων.

Όσον αφορά τη σχεδιαστική τους νοοτροπία, οι σαρωτές είναι προγράμματα που επιτρέπουν *2 μορφές (τόπους και τύπους) ανίχνευσης*· πρώτον *στο επίπεδο φυσικού αρχείου ή κατάτμησης ή τομέα στο δίσκο* (με στόχο το λανθάνον ή boot-sector malware) και δεύτερον *στο επίπεδο διεργασιών και εν γένει σελίδων της κύριας μνήμης* (με στόχο το στιγμιαία ενεργό ή παραμονεύον ή τις περιπτώσεις TSR malware, αλλά και άλλα -φαινομενικά σκουπίδια-

[322] Βλέπε σχετικό εδάφιο 4.1.6.

κατάλοιπα/τεκμήρια επιβλαβούς δράσης κακόβουλων προγραμμάτων, όπως αυτά περιγράφηκαν στα εδάφια του 3ου Κεφαλαίου).

Επίσης *2, είναι και οι προσφερόμενοι από το λογισμικό σάρωσης δυνατοί τρόποι λειτουργίας*:[323]

- **Κατ' απαίτηση σάρωση (on-demand)**

  Στην κατ' απαίτηση σάρωση το πρόγραμμα του σαρωτή ενεργοποιείται *κατ' εντολή του χρήστη ή διαχειριστή ενός υπολογιστικού συστήματος*, υπακούοντας σε κατάλληλα εκπεφρασμένη και διαμορφωμένη αίτηση ανίχνευσης από μέρους τους.

- **Μόνιμη (resident) ή τη στιγμή της πρόσβασης (on-access) σάρωση**

  Στη μόνιμη ή στη στιγμή της πρόσβασης σάρωση το υπεύθυνο λογισμικό παραμένει *μόνιμα σε λειτουργία στο παρασκήνιο* (π.χ. στην κύρια μνήμη του προστατευόμενου συστήματος, όταν τρέχει ως διεργασία σε μεμονωμένο κόμβο, ή ευθύγραμμα στη διεύθυνση επικοινωνίας με το εξωτερικό περιβάλλον, όταν εδρεύει σε κάποια υλισμικού τύπου, δικτυακού προσανατολισμού συσκευή προστασίας), όπου και *δρα με αυτόματο τρόπο*, σαρώνοντας είτε συνεχώς κάθε πιθανή πηγή απειλής (δηλαδή αρχεία, τρέχουσες διεργασίες, σελίδες στη μνήμη, τομείς και κατατμήσεις στο δίσκο) είτε, σπανιότερα και πάντα σε συνδυασμό με άλλες, πιο αντιδραστικές, λύσεις ασφάλειας (όπως τα συστήματα IPS), κατά περίσταση ανταποκρινόμενο σε εξωτερικά ερεθίσματα (δικτυακά μηνύματα και πακέτα δεδομένων) και ανιχνεύοντας το περιεχόμενό τους για κακόβουλα ίχνη.

Δύο είναι τέλος και οι βασικές προσεγγίσεις των σαρωτών στο θέμα του εντοπισμού και της επιβεβαίωσης κακόβουλου κώδικα: *από τη μια η μέθοδος των υπογραφών και από την άλλη οι στατικές, ευριστικές μέθοδοι*.[324] Πιο κάτω αναλύονται τα χαρακτηριστικά και η φιλοσοφία λειτουργίας των προσεγγίσεων αυτών:

1. **Υπογραφές και βάσεις δεδομένων υπογραφών κακόβουλου κώδικα**

   Στην κλασσική αυτή αντιμετώπιση της σάρωσης, *κάθε κακόβουλο πρόγραμμα αντιπροσωπεύεται από ένα ή περισσότερα μοτίβα-τμήματα κώδικα, ή αλλιώς υπογραφές*, που δεν είναι παρά *ακολουθίες bytes, που (ενδεχομένως) χαρακτηρίζουν μοναδικά το κάθε*

[323] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM].

[324] Κύρια, βιβλιογραφική αναφορά: [LUDWIG-GBBCV].

επιβλαβές δημιούργημα.[325] Οι υπογραφές καλούνται μερικές φορές και αλφαριθμητικά ανίχνευσης (scan strings) και δεν χρειάζεται να είναι σταθερές συμβολοσειρές. Πολλοί σαρωτές παρέχουν *υποστήριξη για σύμβολα-μπαλαντέρ (wildcards)* που χρησιμοποιούνται εντός των υπογραφών για να ταιριάξουν με κάποιο αυθαίρετο byte, με κάποιο τμήμα ενός byte ή ακόμα με κανένα ή με περισσότερα του ενός bytes του κακόβουλου κώδικα. Με τη βοήθεια των υπογραφών αυτών *εντοπίζονται, απομονώνονται και ταυτοποιούνται/αναγνωρίζονται (σε ιδιαίτερο είδος και ενδεχομένως οικογένεια*) τα διάφορα περιστατικά κακόβουλου λογισμικού (*είτε βρίσκονται σε εργώδη είτε σε άεργη φάση*).

Ο πάροχος του οιουδήποτε λογισμικού σάρωσης καλείται συνήθως να ανταπεξέλθει σε 2 ισότιμα «συναρπαστικές» και, παράλληλα, λειτουργικά απαραίτητες προκλήσεις:

Α) Τη διατήρηση των επιπέδων κατανάλωσης συστημικών πόρων κατά την *ποροβόρο φάση του ταιριάσματος κώδικα-υπογραφών* (μην ξεχνάμε πως ειδικά σήμερα δεν είναι και λίγες οι υπογραφές αυτές[326]) σε ανεκτά επίπεδα, χωρίς να υποβαθμίζεται η δραστηριότητα του σαρωτή, μέσω ευφυών αλγορίθμων και προσεκτικού σχεδιασμού.[327]

Β) Τη *συντήρηση και ενημέρωση/αναβάθμιση εξειδικευμένων βάσεων δεδομένων* φύλαξης του αβίαστα ογκώδους πλήθους των σύγχρονων υπογραφών καθώς και τη μέριμνα για την υλοποίηση κάποιου στοιχειώδους μηχανισμού (αυτοματοποιημένου ή χειροκίνητου) για την απόκτηση των πλέον επίκαιρων, ενημερωμένων εκδόσεων των υπογραφών από πλευράς των τελικών χρηστών των συστημάτων σάρωσης.[328]

Όσο καλύτερα ικανοποιούνται οι παραπάνω 2 απαιτήσεις καλής λειτουργίας του προγράμματος σάρωσης, τόσο πιο ιδανικές διαμορφώνονται οι συνθήκες για την

---

[325] Κύρια, βιβλιογραφική αναφορά: [SZOR-ACVRD], [LUDWIG-GBBCV], [RABAIOTTI-CIS].

[326] Λόγω της ραγδαίας αύξησης και εξάπλωσης του κακόβουλου λογισμικού.

[327] Η βελτιστοποίηση των αλγορίθμων σάρωσης όσον αφορά τη συστημική επιβάρυνση είναι ολόκληρος, ξεχωριστός κλάδος, τόσο για την επιστήμη και την τεχνολογία κατά του κακόβουλου λογισμικού, όσο και για τη βιομηχανία παραγωγής αντιϊομορφικών προϊόντων. Ένας προσεκτικός, αποδοτικός και αξιόπιστος αλγόριθμος, που οδηγεί σε φιλικά προς τους πόρους προγράμματα σάρωσης, τα καθιστά συνήθως, ευρείας αποδοχή από χρήστες και οργανισμούς.

[328] Το ζήτημα της συντήρησης, παροχής και συμπερίληψης συναφών και συμβατών με τις εξελίξεις υπογραφών κακόβουλου κώδικα καθορίζει σε μεγάλο βαθμό το αποτέλεσμα των εκάστοτε μαχών με τα αυτοαναπαραγόμενα όπλα. Η διατήρηση, εκ μέρους των εταιρειών κατασκευής προγραμμάτων σάρωσης, τέτοιων, επικαιροποιημένων βάσεων δεδομένων και πληροφοριών είναι δείγμα της ποιότητας της έρευνας και των προϊόντων τους και καθοριστικός παράγοντας για την εμπορική τους αποδοχή.

αξιοπιστία, την απόδοση και την επίδοση στην επιτέλεση του σκοπού του, βασικοί συνολικοί δείκτες για την αξιολόγηση της προσφερόμενης από αυτό προστασίας.

2. Στατικές, ευριστικές τεχνικές

Ο Fred Cohen στη διδακτορική του διατριβή (το 1986)[329] απέδειξε με μαθηματικό τρόπο την *εγγενή, γενική αδυναμία για βεβαιότητα στην ανίχνευση ιομορφικού κώδικα, στη βάση της θεωρίας του Kurt Goedel περί μη πληρότητας (incompletness theorems)*. Γενικά, επεκτείνοντας το συμπέρασμα/θεώρημα αυτό της μη τελειότητας, μπορούμε να πούμε πως οι λύσεις προστασίας, που βασίζουν την ανίχνευση επιβλαβών προγραμμάτων στην *απλοϊκή θεώρηση (μονομερούς συνήθως πληροφόρησης και) ντετερμινιστικής απάντησης «ΝΑΙ» ή «ΟΧΙ», στην ερώτηση αν ένα σύστημα πληροφοριών έχει υπονομευτεί ή όχι*, πάσχουν ενδογενώς[330] από την αποδεδειγμένη δυνατότητα κατασκευής, έστω και ενός, υποδείγματος κακόβουλου κώδικα για το οποίο καμιά από τις 2 απαντήσεις δε θα ευσταθεί με απόλυτη ακρίβεια, οδηγώντας αναπόφευκτα το σύστημα σε αποφάσεις που παράγουν σε σημαντικούς αριθμούς *κακώς επιτυχημένες (FalsePositive, FP)* και *κακώς αποτυχημένες (FalseNegative, FN) διαγνώσεις*. Επάνω στο συμπέρασμα αυτό ακριβώς τεκμηριώνεται και στοιχειοθετείται η *ανάπτυξη των πιο ευριστικών (στατικών και δυναμικών) αλγορίθμων και μεθόδων απόφασης*, που ανάγουν την ανίχνευση σε *στατιστικού τύπου υπέρθεση και σύγκριση της συλλογικής συνεισφοράς πολλαπλών, διαφορετικών, χαρακτηριστικών παραμέτρων και παραγόντων, ισχυρά συσχετισμένων με γνωστές και επιβεβαιωμένες καταστάσεις πλήρους μόλυνσης ή ιδανικής ανοσίας*. Η τελική απόφαση είναι πιο σταθμισμένη, αντικειμενική και ρεαλιστική[331], καθώς λαμβάνεται με κριτήρια τη *μεγαλύτερη από τις υπολογισμένες, από το εκάστοτε ευριστικό μοντέλο πρόβλεψης, πιθανότητες των 2 διακριτών ενδεχομένων (παρουσία μόλυνσης/μη μόλυνση)* και την *κατάλληλη επιλογή κατωφλίων αποδοχής/απόρριψής της υπόθεσης ύπαρξης ή όχι μιας μόλυνσης* (με την έννοια της στατιστικά παρεχόμενης βεβαιότητας) και όχι με απόλυτο και καταδικασμένο εξαρχής, σε περισσότερα λάθη και αποτυχίες (FP, FN) στην προσπάθεια εντοπισμού, τρόπο.

Οι στατικού τύπου ευριστικές τεχνικές, τώρα, μπορούν να ιδωθούν και ως ένας τρόπος να μειωθούν κάπως και οι κατά τα άλλα υψηλές απαιτήσεις σε πόρους των σαρωτών. Οι

---

[329] Κύρια, βιβλιογραφική αναφορά: [COHEN-CV].

[330] Στην κατηγορία αυτή ανήκουν οι περισσότεροι μηχανισμοί απλής ανίχνευσης κακόβουλων προγραμμάτων, όπως π.χ. σαρωτές με υπογραφές, στοιχειώδεις ελεγκτές της ακεραιότητας, μη ευριστικού τύπου παρεμποδιστές και άλλοι παρόμοιας λογικής, που θα συναντήσουμε και περιγράψουμε σε όλη την ενότητα αυτή (4.1) του τρέχοντος κεφαλαίου.

[331] Χωρίς αυτό να σημαίνει πως εκλείπουν τα FPs και FNs, αλλά μάλλον πως είναι σημαντικά πιο ελαττωμένα· η μέθοδος απόφασης πάντως είναι ουσιωδώς πιο αξιόπιστη.

πλήρεις υπογραφές κακόβουλου κώδικα αντικαθίστανται από *ένα σύνολο μικρών και γενικού τύπου, στατικών ευριστικού τύπου υπογραφών*. Ένα πρόγραμμα σάρωσης μπορεί να ψάχνει πρώτα για αυτές τις συντομότερες υπογραφές κώδικα και μόνο στην περίπτωση που βρίσκεται μια αντιστοιχία να φορτώνει το σχετικό σύνολο των πληρέστερων υπογραφών. Αυτό ανακουφίζει από την ανάγκη να κρατώνται οι πλήρεις υπογραφές στη μνήμη καθ' όλο το χρόνο εκτέλεσης του αλγορίθμου σάρωσης.

Στην ουσία, οι σαρωτές ρυθμίζονται έτσι, ώστε αντί να ψάχνουν για συγκεκριμένες υπογραφές να αναζητούν εναλλακτικά και σε πρώτη φάση τμήματα κώδικα που στοιχειοθετούν «ομοιάζουσα με κακόβουλη» συμπεριφορά. Ο στατικός χαρακτήρας, βέβαια, σημαίνει πως *η ανίχνευση περιορίζεται σε ύποπτο κώδικα, που δεν εκτελείται εκείνη τη στιγμή,* είτε αυτός εντοπίζεται σε κάποια συσκευή αποθήκευσης, είτε περιφέρεται άεργος στη μνήμη -είτε ακόμη ευρίσκεται εντός πακέτου δικτυακής επικοινωνίας, αν πραγματοποιούνται τέτοιου είδους έλεγχοι με την πρόσθετη συνέργεια άλλων προστατευτικών μονάδων. Η ευριστική τεχνοτροπία περιλαμβάνει και ολοκληρώνεται σε 2 στάδια:[332]

- **Στάδιο συλλογής δεδομένων**

  Ο σαρωτής ανιχνεύει την *παρουσία ενδείξεων (ή διαφορετικά μικρών υπογραφών) ύποπτου κώδικα -των λεγόμενων boosters-* για παράδειγμα «άχρηστο» κώδικα, βρόχους (από)κρυπτογράφησης, μεταλλασσόμενο κώδικα, μη επαρκώς τεκμηριωμένες API κλήσεις, αλλοίωση/εκμετάλλευση/«γάντζωμα» στοιχείων του Λ/Σ, ασυνήθιστες εντολές, προφανή αλφαριθμητικά-μανιφέστα του κακόβουλου συγγραφέα κ.ά. Ταυτόχρονα ελέγχει για την *ύπαρξη τεκμηρίων -γνωστών ως stoppers- φυσιολογικού και νόμιμου κώδικα* και εντολών που γενικά αποφεύγονται ή δε χρησιμοποιούνται από τους συγγραφείς επιβλαβών προγραμμάτων. Τέλος, πραγματοποιούνται κάποιοι πιο σύνθετοι υπολογισμοί που αφορούν το σύνολο του κώδικα όπως φασματική ανάλυση (spectral analysis), μετρήσεις μεγέθους συστατικών μερών του υπό σάρωση αντικειμένου, στατιστική ανάλυση με βάση πρότυπα, μαθηματικοποιημένα, θεωρητικά μοντέλα κακόβουλης εξάπλωσης και δράσης και διάφοροι έλεγχοι πλεονασμού.[333]

  Στο τέλος του σταδίου συλλογής οι παραπάνω πληροφορίες έχουν συγκεντρωθεί και ταξινομηθεί στις ανήκουσες κατηγορίες και κατόπιν τροφοδοτούνται ως «είσοδος» στο στάδιο ανάλυσης.

---

[332] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM], [RABAIOTTI-CIS].

[333] Κύρια, βιβλιογραφική αναφορά: [WEBSTER_MALCOLM-DMCVAS], [LUDWIG-GBBCV].

- **Στάδιο ανάλυσης δεδομένων**

  Στη φάση αυτή *αφού δοθεί το κατάλληλο ειδικό βάρος στους διάφορους boosters (θετικό πρόσημο) και stoppers (αρνητικό πρόσημο) υπολογίζεται κάποιο αποτέλεσμα απόφασης*, η τιμή του οποίου, εφόσον ξεπερνά κάποιο δεδομένο κατώφλι, τότε το υπό σάρωση αντικείμενο θεωρείται κακόβουλο. Στο στάδιο αυτό έχουν θέση και βρίσκουν εφαρμογή ακόμα και ιδιαίτερα ενδιαφέρουσες και αξιοπρόσεκτες τεχνολογίες, όπως τα νευρωνικά δίκτυα (neural nets), τα ευφυή συστήματα (cognitive systems) και οι τεχνικές εξόρρυξης δεδομένων (data mining techniques)[334].

Μόλις περατωθεί ο εντοπισμός κάποιας κακόβουλης οντότητας και αναγνωριστεί το ιδιαίτερο της είδος με τη βοήθεια των κλασσικών υπογραφών, αλλά και των πιο ευέλικτων ευριστικών μεθόδων, τα προγράμματα σάρωσης αναλαμβάνουν επιπλέον να εκτελέσουν και κάποιες σημαντικές, *πρόσθετες εργασίες για την ασφάλεια, όπως το να καταγράψουν το συμβάν και να ειδοποιήσουν έπειτα με τα ανάλογα επεξηγηματικά μηνύματα τους ιδιοκτήτες/διαχειριστές των συστημάτων* για την επίθεση-εισβολή και τον εντοπισμό αυτής, καθώς ακόμα και το *να προχωρήσουν με ή χωρίς την ανθρώπινη καθοδήγηση στη λήψη των απαραίτητων μέτρων για την απομάκρυνση ή τον περιορισμό του κινδύνου*. Για τον τελευταίο σκοπό ειδικά, *συνηθίζεται στην κάθε υπογραφή να αντιστοιχίζονται και κάποιες πληροφορίες για την αφαίρεση της εκάστοτε περιγραφόμενης μόλυνσης (disinfection),* που μπορεί να είναι τόσο απλές και γενικές όσο η φυσική διαγραφή της ευρεθείσας ως κακόβουλης διεργασίας, αλλά μπορεί και πιο σύνθετες και εξαρτημένες από την κάθε περίπτωση· τα στοιχεία αυτά φυλάσσονται είτε τοπικά στη βάση δεδομένων των υπογραφών και ανακαλούνται από εκεί μόλις ταυτοποιηθεί το είδος του κακόβουλου κώδικα είτε μεταφορτώνονται δυναμικά από κάποιον κεντρικό εξυπηρετητή π.χ. στο Διαδίκτυο τη στιγμή του χαρακτηρισμού της απειλής. Επίσης, στο ίδιο σκεπτικό, οι σαρωτές σχεδιάζονται έτσι ώστε να παρέχουν στους χρήστες μια διάφανη απεικόνιση και τη δυνατότητα παραμετροποίησης/αυτοματοποίησης των διαφόρων επιλογών αντιμετώπισης σε κάθε περίπτωση εντοπισμού φορέα υπονόμευσης. Οι επιλογές που δίδονται κατά περίσταση, τελικά, είναι συνήθως οι εξής 4:[335]

-- Εκκαθάριση της μόλυνσης, χωρίς απώλεια πληροφορίας.

-- Επαναφορά σε πρότερη, άνοση κατάσταση.

---

[334] Κύρια, βιβλιογραφική αναφορά: [RABAIOTTI-CIS].

-- Επιβολή καραντίνας στο αίτιο της απαράδεκτης συμπεριφοράς.

-- Ολοκληρωτική διαγραφή της πρόκλησης και του προβληματικού επίκεντρου, με πιθανή απώλεια χρήσιμης πληροφορίας[336].

Με τις παραπάνω διαδικασίες ολοκληρώνεται και ο κύκλος της μοναδιαίας λειτουργίας ενός σαρωτή, που όπως είδαμε περιλαμβάνει μια σχετικά πλήρη στρατηγική άμυνας και προστασίας, με ξεκάθαρες και ενδελεχείς τις φάσεις της παρακολούθησης, διάγνωσης και αναγνώρισης κινδύνου, αλλά και της ανταπόκρισης, θεραπείας και επανόρθωσης[337].

Κλείνοντας το παρόν σκέλος, θα μπορούσαμε να πούμε πως *το λογισμικό σάρωσης αποτελεί την αρχαιότερη, μα συνάμα και την περισσότερο ώριμη, αμυντική λύση* των υπολογιστικών και πληροφοριακών συστημάτων, κόντρα στο επίβουλο λογισμικό και τους κυβερνοκακοποιούς «σπόνσορές» του. Χρόνια και επενδύσεις συνεχιζόμενης έρευνας και παραγωγής έχουν δαπανηθεί και δαπανώνται ακόμα προκειμένου το λογισμικό κατά των ιών και του υπόλοιπου, κακόβουλου διάκοσμου να συμβαδίζει με τις εκάστοτε, επίκαιρες εξελίξεις προστατεύοντας ει δυνατόν με τη μεγαλύτερη αποτελεσματικότητα από τις εχθροπραξίες και τις επιθέσεις με φορείς τα συγκεκριμένα όπλα. Ο *βαθμός εξοικείωσης χρηστών και χειριστών με τα εν λόγω συστήματα είναι επίσης μεγάλος* -λόγω της εκτεταμένης προϊστορίας και της αδιάλειπτης υποστήριξης και τεκμηρίωσης- καθιστώντας τα άμυνα γενικής αποδοχής και εφαρμογής. Αυτό καμιά φορά λειτουργεί και εις βάρος της ασφάλειας των ΠΣ, εφόσον περιοριστούν στη χρήση μόνο αυτού του τύπου της αμυντικής θωράκισης, αν αναλογιστεί κανείς, μάλιστα, πως το επίπεδο σπουδής της υλοποίησης και του τρόπου λειτουργίας και των ενδεχόμενων αδυναμιών/παραβλέψεων αυτών, προκειμένου για την τεχνολογία των σαρωτών, είναι *για παρόμοιους λόγους εξίσου υψηλό και για τους επίδοξους κυβερνοεγκληματίες* (εμπνευστές, συγγραφείς και δράστες κακόβουλων σχεδίων). Φυσικά, κάτι τέτοιο δεν υποβαθμίζει τη συνολικά σημαντική προσφορά (έρευνα, δράση και αποτέλεσμα) των προγραμμάτων σάρωσης -αλλά και της υπερκείμενης «αντιϊομορφικής» βιομηχανίας, της οποίας και αποτελούν το βασικότερο/γνωστότερο προϊόν- στην καταπολέμηση κάθε είδους κακόβουλου κώδικα που απειλεί να εισέλθει/δράσει εντός των τειχών των πληροφοριακών κέντρων. Η παρουσία τους, πέρα από συνηθισμένη/καθιερωμένη, αποδεικνύεται στην πράξη ουσιώδης, πολύτιμη και τελικά απαραίτητη προστατευτική

---

[335] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM].

[336] Εφόσον δεν υπάρχει άλλη επιλογή η πιθανή, αναγκαστική απώλεια δεδομένων ή άλλων συστημικών ιδιοτήτων μπορεί να καλυφθεί με την ανάκτηση/επαναφορά μέσω κατάλληλων, αντιγράφων ασφάλειας, που θα έχει φροντίσει να λαμβάνει και να διατηρεί ο εκάστοτε χρήστης ή διαχειριστής ενός ΠΣ.

[337] Όπως την προσεγγίσαμε και μελετήσαμε στο εδάφιο του υποβάθρου 2.2.8.

μέριμνα, αποτελώντας τη *βάση της πυραμίδας στο «χτίσιμο» της ασφάλειας των σύγχρονων ΠΣ*.

4.1.2 Εξομοιωτές

Τα συστήματα εξομοίωσης *επιτρέπουν την ανάλυση κακόβουλου κώδικα και προγραμμάτων σε ένα προστατευμένο, εικονικό περιβάλλον επεξεργασίας και δικτυακής διασύνδεσης με την ελπίδα ένας ιός ή κάποιο σκουλήκι να καταδείξει την ποιοτική του υφή, το διακριτικό του μοτίβο κακόβουλης δράσης και τα άλλα ειδοποιά χαρακτηριστικά διάδοσης που θα επιτρέψουν τον εντοπισμό και την ταυτοποίησή του, χωρίς την ανάγκη οιασδήποτε, επιβλαβούς αλληλεπίδρασής με πραγματικού τύπου ΠΣ*[338]. Τα συστήματα αυτά ήρθαν στο προσκήνιο, στην προσπάθεια αντιμετώπισης των πρώτων πολυμορφικού τύπου προγραμμάτων και των πολύπλοκων/απρόσιτων, για τα τότε δεδομένα της απλής σάρωσης, μηχανών μετάλλαξης, που χρησιμοποιούσαν[339]. Με την προσθήκη του περιβάλλοντος και των μηχανισμών εξομοίωσης (όπως η γενικής φύσεως αποκρυπτογράφηση (generic decryption) και η δυναμική, ευριστική ανάλυση (dynamic heuristics)) η ανίχνευση και ταυτοποίηση παρόμοιων απειλών έγινε ευκολότερη και ο περιορισμός της ανεξέλεγκτής τους πορείας πραγματικότητα. Σήμερα, εξακολουθούν να αποτελούν τον *κύριο αντίπαλο για τα εξελίξιμα, αυτοαναπαραγόμενα όπλα*[340] *και τις τεχνικές της μετάλλαξης*, κυρίως λόγω της προσφερόμενης ικανότητας για δυναμική ανάλυση και εξακρίβωση της όποιας, ύποπτης συμπεριφοράς και δράσης, καθώς και της όποιας παραλλαγής σε αυτές, σε περιορισμένο, προστατευμένο περιβάλλον.

Η ανατομία ενός εξομοιωτή περιλαμβάνει τα 5 ακόλουθα μέρη:[341]

1. Εξομοίωση επεξεργαστικής μονάδας.
2. Εξομοίωση κύριας μνήμης.
3. Εξομοίωση περιφερειακού υλικού και Λ/Σ.
4. Ελεγκτής εξομοίωσης, που καθορίζει το πότε και το πώς θα σταματήσει μια εξομοίωση, αλλά και τις παραμέτρους του χρόνου εκτέλεσης.

---

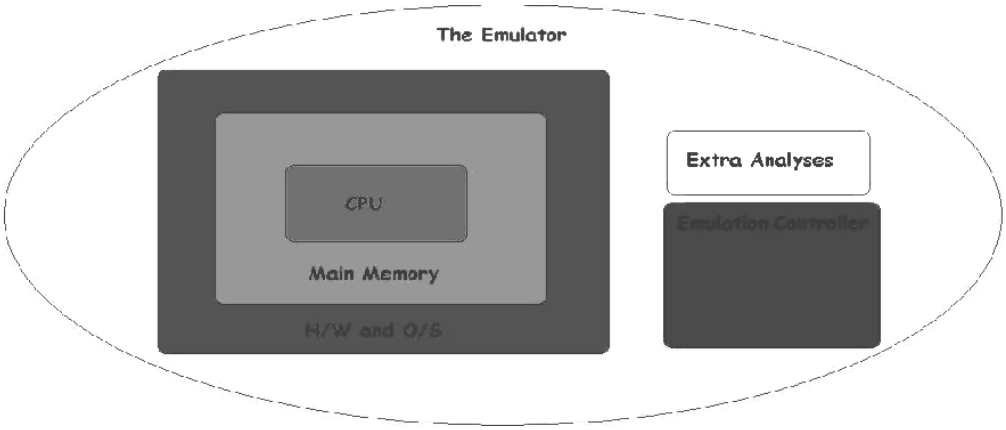
[338] Κύρια, βιβλιογραφική αναφορά: [SZOR-ACVRD].

[339] Κύρια, βιβλιογραφική αναφορά: [PEARCE-VP].

[340] Όπως τα εννοήσαμε στο εδάφιο 3.2.4 του 4ου κεφαλαίου.

[341] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM].

5. Πρόσθετη ανάλυση π.χ. μέσω συλλογής στατιστικών, επιθεώρησης φασματικού αποτυπώματος, επεξεργασίας αρχείων goat κτλ.



Σχήμα 22: Ανατομία ενός συστήματος εξομοίωσης

Η εξομοίωση εμφανίζεται και εφαρμόζεται με 2 κυρίως τακτικές δράσης κόντρα στον κακόβουλο κώδικα:[342]

- **Δυναμικές, ευριστικές μέθοδοι**, με τις οποίες *συλλέγονται κατά το χρόνο εξομοίωσης* διάφορες *πληροφορίες όμοιας λογικής και χρησιμότητας με αυτές στις στατικές, ευριστικές μεθόδους* και αξιολογούνται ως προς το αν και κατά πόσο μπορούν να αποτελέσουν τεκμήρια κακόβουλης μόλυνσης (π.χ. η χρήση μεταλλακτικού κώδικα ή μη επαρκώς τεκμηριωμένων κλήσεων API αναμένεται να λάβει «υψηλή βαθμολογία» στην αποτίμηση μιας «υποψήφιας» ως ενσάρκωσης κακόβουλου κώδικα εφαρμογής, που καταφεύγει σε αυτές τις κατεξοχήν ύποπτες δράσεις).
- **Γενικής φύσεως αποκρυπτογράφηση**, χάρη στην οποία με ευριστικό τρόπο επιτυγχάνεται *«σκιώδης» αποκρυπτογράφηση μιας κρυπτογραφημένης απειλής*· σε αυτό το πλαίσιο για να είμαστε πιο συγκεκριμένοι είναι δυνατόν με τη βοήθεια του εξομοιωτή:

    - να εντοπίζονται (στη μνήμη) οι αποκρυπτογραφημένες εκδοχές του ιού ή του σκουληκιού, τη στιγμή αμέσως μετά την έτσι και αλλιώς οικειοθελή αποκρυπτογράφηση του σώματος από μέρους του κακόβουλου κώδικα, που

[342] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM], [SYMANTEC-STRIKER].

ούτως ή άλλως συμβαίνει και όχι κατόπιν απόπειρας «σπασίματος» του κρυπτογραφήματος από μέρους του λογισμικού προστασίας και

- να ανιχνεύονται (στη μνήμη ή στο υπόλοιπο αποθηκευτικό περιβάλλον), π.χ. με αναζήτηση για μεγάλου μήκους αλφαριθμητικά (string search), πληροφορίες σχετικές με την αποκρυπτογράφηση του σώματος, όπως λ.χ. κλειδιά ή μέρη/συνιστώσες αυτών.

Το ξεκάθαρο όφελος από τη χρήση τεχνικών εξομοίωσης στα συστήματα ασφάλειας των σύγχρονων, πληροφοριακών οχυρών είναι σίγουρα η μη αναγκαιότητα επαφής με πραγματικά συστήματα και πρότερης ή τρέχουσας σε αυτά επιμολυντικής δράσης, προκειμένου να εντοπιστεί και να αναγνωριστεί μια απειλή οπλολογισμικού τύπου.[343] Στα συν, επίσης, της συγκεκριμένης τεχνολογίας και η *δυνατότητα για «εύρεση» εντελώς νέων και άγνωστων μορφών πληροφοριακών όπλων λογισμικού*. Βέβαια, η ίδια η εξομοίωση από μόνη της δεν παρέχει παρά μόνο εντοπισμό ενδείξεων και ανεπιθύμητων ή μη αναμενόμενων αποτελεσμάτων από την εκτέλεση/δράση ενός προγράμματος στο περιβάλλον εικονικοποίησης· η συνεργασία, όμως, με έναν επικαιροποιημένο σαρωτή μπορεί να αποδώσει υψηλά επίπεδα αναγνώρισης του είδους της απειλής, χωρίς τους κινδύνους της πρότερης ή τρέχουσας εκτέλεσης στα πραγματικά ΠΣ, και για αυτό οι εξομοιωτές απαντώνται συχνά σε συνδυασμό με συστήματα κατ' απαίτηση σάρωσης κώδικα/δεδομένων. Τέλος, *όπως κάθε δυναμική μέθοδος της βιομηχανίας προστασίας από το κακόβουλο λογισμικό, έτσι και η εξομοίωση, αποδεικνύεται ιδιαιτέρως ακριβή σε συστημικούς πόρους*, ενώ δεν παύει να *εμφανίζει και λειτουργικές ατέλειες*, όπως η μειωμένη ταχύτητα, η εξάρτηση της διάγνωσης από το μέγιστο χρόνο εξομοίωσης και οι όποιες αδυναμίες παροχής ενός τέλεια εξομοιωμένου περιβάλλοντος, που μπορούν να αποτελέσουν τροχοπέδη για μια επιτυχημένη διάγνωση, αλλά ταυτόχρονα και πηγή ευπαθειών. Παρόλ' αυτά, η σημερινή παρουσία των εξομοιωτών είναι μια εγνωσμένης αξίας πραγματικότητα, που διαρκώς αποπνέει αυξημένη δυναμική -στα πλαίσια των ευρύτερων υποσχέσεων της εικονικοποίησης[344]- επιτυχίας στις απόπειρες προστασίας των πληροφοριακών κέντρων της εποχής μας.

4.1.3 Κλασσικές λύσεις τειχών αντιπυρικής προστασίας

Ένα τείχος πυροπροστασίας ή αντιπυρικής προστασίας (πλέον γνωστό με τον αγγλικό όρο firewall) είναι *"μια εξειδικευμένη συλλογή συσκευών συνοδευόμενων από το κατάλληλο*

[343] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM].

[344] Περισσότερα για το θέμα στο εδάφιο 5.2.1.

λογισμικό οδήγησης, λειτουργίας και παραμετροποίησης των ή ένα μεμονωμένο πρόγραμμα για Η/Υ, που σκοπό έχει να διαπραγματεύεται και να διαφεντεύει την πρόσβαση μεταξύ διαφορετικών τομέων ή επιπέδων ασφάλειας".[345] Όλη η δικτυακή κίνηση ανεξαρτήτου κατεύθυνσης (από ή προς κάποιον τομέα) επιθεωρείται και ελέγχεται ιδανικά από το εν λόγω υλισμικό στα πλαίσια των ορίων ασφάλειας (security boundaries) των διαφορετικών τομέων, που ορίζονται κατά μήκος των διαφόρων ΠΣ. Τα συστήματα αυτά βρίσκουν θέση, τόσο περιμετρικά του ΠΣ, όσο και εντός των κόμβων αυτού.

Ο τυπικός ρόλος κάθε τέτοιου τείχους είναι η *αυτοματοποιημένη αποδοχή ή απόρριψη των εκφάνσεων της λεγόμενης, δικτυακής κίνησης* με άμεση αναφορά στην τιμή των κυρίων εκπροσώπων της, δηλαδή των διευθύνσεων πηγής-προορισμού, των εκατέρωθεν συνδέσεων και του εκάστοτε, ειδικού χαρακτήρα (μέγεθος, τύπος, διάρκεια κτλ) των διακινούμενων ρευμάτων/μηνυμάτων (πιο γνωστά πακέτων) δεδομένων.[346] Η απόφαση για αποδοχή ή απόρριψη λαμβάνεται *με τη βοήθεια προγραμματιστικών κανόνων στατικού/σταθερού ή δυναμικού/προσαρμόσιμου χαρακτήρα*, που μπορούν να περιέχουν ως μεταβλητές οποιεσδήποτε από τις προαναφερόμενες πληροφορίες κίνησης.[347] Τα στατικά σετ κανόνων παραμένουν αμετάβλητα τουλάχιστον για όσο χρόνο δεν επεμβαίνει με αναθεωρητικό πνεύμα επεξεργασίας κάποιο ανθρώπινο στοιχείο, ενώ τα αντίστοιχα δυναμικά παράγονται (και αναλώνονται) με πιο αυτόματο τρόπο και εν ώρα ανάγκης από το ίδιο το λογισμικό του τείχους προστασίας όπως π.χ. μπορεί να συμβεί με τη συνεργασία/συντονισμό του τείχους με κάποιο ολοκληρωμένο σύστημα διάγνωσης/αποτροπής, ως ανάδραση σε μια εν εξελίξει επίθεση[348]. Τέλος, *τα περισσότερα firewalls υποστηρίζουν ενδογενώς αμιγείς και εκτεταμένες υπηρεσίες AAA*, ακριβώς λόγω του κρίσιμου και σπουδαίου στόχου που καλούνται να διεκπεραιώνουν με ασφάλεια και επιτυχία· ειδικά τα αρχεία καταγραφής (firewall audit logs) ενός τείχους προστασίας αποτελούν πολύτιμες πηγές γνώσης για την κατάσταση και την ποιότητα ασφάλειας ενός δικτύου πληροφοριών.

Στην πορεία των ετών της τεχνολογικής εξέλιξης στην πληροφορική και την ασφάλεια των συστημάτων, η εννοιολογική σύλληψη και τεχνολογική υλοποίηση του αντιπυρικού τείχους προστασίας διήλθε από διάφορες φάσεις αναθεώρησης και καινοτομίας και σήμερα συναντάται κυρίως σε 5 υποστάσεις, που διακρίνονται μεταξύ τους ανάλογα με την πολυπλοκότητα και την ευαισθησία τους στην ανάλυση της δικτυακής κίνησης· οι κάτωθι 5 μορφές αποτελούν λογικά διακριτούς, μα όχι αλληλοαποκλειόμενους, ρόλους για μια

---

[345] Κύρια, βιβλιογραφική αναφορά: [FFIEC-IS].

[346] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM].

[347] Οι κανόνες αυτοί ονομάζονται λίστες ελέγχου δικτυακής πρόσβασης ή network access control lists (NACLs).

[348] Βλέπε σχετικό εδάφιο 4.1.6 για τα IDS/IPS, παρακάτω.

συσκευή ή πρόγραμμα αντιπυρικής προστασίας και συχνό είναι το φαινόμενο μια εμπορική λύση να αναλαμβάνει-επιτελεί περισσότερες της μιας από τις ακόλουθες «υποσχέσεις»:

Α. Βασικό Φιλτράρισμα πακέτων (packet filtering)[349]

Το φιλτράρισμα αφορά ακριβώς στη διαδικασία διαχωρισμού της «νόμιμης» από τη μη επιτρεπόμενη κίνηση με βάση ήδη θεσπισμένους ή κατ' απαίτηση παραγόμενους κανόνες. Στη βασική του μορφή, το φιλτράρισμα αφορά τα στρώματα 3 και 4 του μοντέλου OSI του οργανισμού ISO, το στρώμα δηλαδή του δικτύου και εκείνο της μεταφοράς, όπου οι ανταλλασσόμενες, διακινούμενες μονάδες επικοινωνίας είναι τα λεγόμενα πακέτα δεδομένων.

Οι αντιπυρικές ζώνες φιλτραρίσματος πακέτων *αξιολογούν τις επικεφαλίδες και τις εκεί κωδικοποιημένες ιδιότητες κάθε εισερχόμενου και εξερχόμενου πακέτου* για να εξασφαλίσουν ότι έχει μια έγκυρη, εσωτερική διεύθυνση, προέρχεται από μια επιτρεπόμενη, εξωτερική διεύθυνση, συνδέεται με ένα εξουσιοδοτημένο πρωτόκολλο ή μια «νόμιμη» υπηρεσία και περιέχει έγκυρες, βασικές οδηγίες στην επικεφαλίδα (header) του.[350] Εάν το πακέτο δεν ταιριάζει με την προκαθορισμένη πολιτική για την δικτυακή κυκλοφορία, το τείχος (απορ)ρίπτει (drops) το πακέτο. Τα φίλτρα πακέτων στην πλειονότητα τους *δεν αναλύουν το περιεχόμενο των πακέτων πέρα από την κεφαλή αυτών* εξ ου και προκύπτει η ανωτερότητά τους όσον αφορά την *ταχύτητα επεξεργασίας* σε σχέση με τις υπόλοιπες λύσεις της οικογένειας πυροπροστασίας, που εγκολπώνουν πολυπλοκότερες ρουτίνες παρακολούθησης και ανάλυσης της κίνησης, απαιτώντας, συνήθως, μεγαλύτερο χρόνο επεξεργασίας και οδηγώντας σε κάπως βραδύτερο δίκτυο.

Το επίπεδο ασφάλειας που παρέχουν τα τείχη φιλτραρίσματος πακέτου θεωρείται από τους ειδήμονες *το ελάχιστο επιθυμητό και το πλέον ουσιώδες σε καθημερινά, πληροφοριακά περιβάλλοντα* (όπως π.χ. το οικιακό ή αυτό ενός μικρού γραφείου-επιχείρησης), ενώ οι κρισιμότερες υποδομές και οργανισμοί πρέπει οπωσδήποτε να περιστοιχίζονται και από πρόσθετα και πιο ενδελεχή, αντιπυρικά συστήματα, σαν αυτά που ακολουθούν.

Β. Επιθεώρηση πακέτων με βάση την κατάσταση TCP σύνδεσης (SPI)[351]

Η επιθεώρηση με βάση την κατάσταση προεκτείνει το απλό φιλτράρισμα πακέτων (stateless filtering) προσθέτοντας *λειτουργίες που ελέγχουν ειδικότερα την κατάσταση (state) των TCP συνδέσεων*. Κάθε σύνοδος TCP αρχίζει με μια "χειραψία" που επικοινωνείται μέσω των

[349] Κύρια, βιβλιογραφική αναφορά: [FFIEC-IS].

[350] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM].

[351] Κύρια, βιβλιογραφική αναφορά: [FFIEC-IS].

σημαιών/σημάνσεων TCP (TCP flags) στις πληροφορίες επικεφαλίδας. Όταν μια σύνδεση εγκαθίσταται, το τείχος αντιπυρικής προστασίας τοποθετεί αυτές τις πληροφορίες σύνδεσης σε έναν πίνακα κατάστασης (State Table).[352] Το τείχος μπορεί κατόπιν να συγκρίνει τα μελλοντικά πακέτα με τα περιεχόμενα του πίνακα σύνδεσης ή κατάστασης (Stateful Packet Inspection). Αυτό, ουσιαστικά, *διασφαλίζει ότι η όποια, εισερχόμενη κίνηση έρχεται πάντοτε ως απάντηση σε αιτήματα που αρχίζουν από μέσα από την αντιπυρική ζώνη*.

Γ. Εκτενής επιθεώρηση πακέτων (DPI)[353]

Η σε βάθος επιθεώρηση πακέτων (Deep Packet Inspection) είναι μια μορφή φιλτραρίσματος πακέτων, που *εξετάζει και το πεδίο δεδομένων και το μέρος της επικεφαλίδας ενός πακέτου*, καθώς αυτό περνά από ένα σημείο επιθεώρησης, αναζητώντας μη συμμόρφωση σε πολιτικές, όσον αφορά τα χρησιμοποιούμενα πρωτόκολλα, τους ιούς, την ανεπιθύμητη αλληλογραφία, τις παράνομες παρεισφρύσεις ή άλλα προκαθορισμένα κριτήρια, με τελικό σκοπό να αποφασιστεί εάν το εν λόγω πακέτο μπορεί να διέλθει του σημείου αυτού ή εάν πρέπει να απορριφθεί ή να καθοδηγηθεί σε έναν διαφορετικό προορισμό. Ο όρος επινοήθηκε για να έρχεται σε αντίθεση με τη «ρηχή» επιθεώρηση πακέτων (συνήθως αποκαλούμενη απλώς επιθεώρηση πακέτων[354]), που ελέγχει μόνο την περιοχή της επικεφαλίδας ενός πακέτου.

Η σε βάθος επιθεώρηση των πακέτων συνδυάζει τη λειτουργία ενός συστήματος ανίχνευσης (IDS) και ενός πρόληψης (IPS) εισβολών και παρεισφρύσεων, με ένα παραδοσιακό stateful firewall[355]. Αυτός ο συνδυασμός καθιστά πιθανό να ανιχνευτούν και περιοριστούν ορισμένες επιθέσεις που, ούτε τα IDS/IPS ούτε οι stateful αντιπυρικές ζώνες, δεν μπορούν να εντοπίσουν από μόνα τους.

Τα DPIs χρησιμοποιούνται για να αποτρέψουν επιθέσεις από ιούς και σκουλήκια με μεγάλες ταχύτητες. Πιο συγκεκριμένα, ένα DPI μπορεί να είναι αποτελεσματικό ενάντια σε επιθέσεις υπερχείλισης καταχωρητών (buffer overflows), άρνησης υπηρεσιών (DoS), περίπλοκων παρεισφρύσεων και ενός μικρού ποσοστού των σκουληκιών που εδρεύουν μέσα σε ένα μόνο πακέτο.

Οι συσκευές DPI έχουν τη δυνατότητα να εξετάσουν τα στρώματα 2 μέχρι και 7 του προτύπου OSI. Αυτό περιλαμβάνει τις επικεφαλίδες και δομών δεδομένων των χρησιμοποιούμενων πρωτοκόλλων, καθώς επίσης και το πραγματικό «ωφέλιμο φορτίο» κάθε

---

[352] Πηγή: Διαδίκτυο, ιστοχώρος της online εγκυκλοπαίδειας WikiPedia, http://en.wikipedia.org/wiki/Stateful_firewall.

[353] Πηγή: Διαδίκτυο, ιστοχώρος της online εγκυκλοπαίδειας WikiPedia, http://en.wikipedia.org/wiki/Deep_packet_inspection.

[354] Που αναλύσαμε ευθύς προηγουμένως.

[355] Πηγή: "Firewall Evolution - Deep Packet Inspection", Ido Dubrawsky, 2003, διαθέσιμο από το δεσμό http://www.securityfocus.com/infocus/1716.

μηνύματος. Το DPI σύστημα θα εξετάσει, προσδιορίσει και ταξινομήσει την κυκλοφορία στηριζόμενο σε μια *βάση δεδομένων υπογραφών*[356] *που περιλαμβάνει κακόβουλες πληροφορίες που μπορούν να εισαχθούν στα φορτία των πακέτων*, πράγμα που επιτρέπει πιο *ραφιναρισμένο και σημασιολογικότερο έλεγχο* από μια ανίχνευση απειλών και επιθέσεων βασισμένη μόνο στις πληροφορίες των επικεφαλίδων.

Τα συστήματα του αυτού είδους εκτελούν μια τόσο *άνευ όρων και άκρως διεισδυτική επέμβαση στον ιδιαίτερο χαρακτήρα και τις ποιότητες των διακινούμενων μηνυμάτων και πληροφοριών*, που φτάνει μέχρι και το τελευταίο, πλέον ανθρωπίνως αισθητό, στρώμα του OSI μοντέλου[357], απειλώντας δυνητικά, με άμεσο τρόπο, την ιδιωτικότητα των εμπλεκόμενων οντοτήτων, είτε κακόβουλων είτε μη.

Δ. Πυροπροστασία εντός διαμεσολαβητών (Proxy Server firewalls)[358]

Οι διακομιστές μεσολάβησης ή διαμεσολαβητές, πέραν του γνώριμου, πρωτεύοντος ρόλου τους να εξυπηρετούν με διαφάνεια και διαφύλαξη της ιδιωτικότητας μεγάλες ομάδες χρηστών και μηχανημάτων, εξοπλίζονται πλέον, όλο και συχνότερα, *με εξειδικευμένες λειτουργίες πυροπροστασίας*, ενσωματώνοντας λογισμικό ή ρουτίνες φιλτραρίσματος, *τόσο στα επίπεδα δικτύου και μεταφοράς, όσο και στο επίπεδο εφαρμογής*, και παρέχοντας ιδιαίτερα παραμετροποιήσιμο και λεπτομερή έλεγχο πρόσβασης (πάντα μαζί με την απαραίτητη αυθεντικοποίηση και καταγραφή δράσης).

Ε. Πυροπροστασία στο Επίπεδο Εφαρμογής (Application-Level firewalling)[359]

Το επίπεδο εφαρμογής αποτελεί το τελευταίο στάδιο της ιεραρχίας OSI και ταυτόχρονα τον *πραγματικό χώρο της εξέλιξης κάθε ανθρωπίνως αντιληπτής, πληροφοριακής δραστηριότητας* - ωφέλιμης ή κακόβουλης. Εδώ, χτυπά η καρδιά της ηλεκτρονικής επικοινωνίας, συνεννόησης και συνεργασίας, εδώ είναι και η ευκαιρία να προστατευτούμε από την εχθροπραξία εν τη γενέσει της.

Τα firewalls του αυτού επιπέδου *επεκτείνουν και εξειδικεύουν* (το βάρος των ελέγχων δίδεται *στο στρώμα εφαρμογής* και λιγότερο ή/και καθόλου στο στρώμα δικτύου) τις λειτουργίες φιλτραρίσματος πακέτων και διαμεσολάβησης με επιπρόσθετες παρακολούθησης-

---

[356] Οι υπογραφές αυτές χρησιμοποιούνται, όπως από τα συστήματα σάρωσης ή τα IDS/IPS, για την ταυτοποίηση των κακόβουλων προγραμμάτων ή περιστατικών.

[357] Η ειδοποιός διαφορά με τα στενά συγγενή σε φιλοσοφία σχεδιασμού και λειτουργίας application-level firewalls είναι η εκτεταμένη παρουσία και χρήση των IDS-τύπου υπογραφών κακόβουλης συμπεριφοράς.

[358] Κύρια, βιβλιογραφική αναφορά: [FFIEC-IS].

[359] Πηγή: Διαδίκτυο, ιστοχώρος της online εγκυκλοπαίδειας WikiPedia, http://en.wikipedia.org/wiki/Application_layer_firewall.

επικύρωσης του περιεχομένου των πακέτων (εφαρμόζοντας DPI μεθόδους[360]) και των αιτημάτων εξυπηρέτησης, ανάλογα με την εκάστοτε εφαρμογή, παρέχοντας έτσι μια ακόμη βαθμίδα ελέγχου και προστασίας από κακόβουλες ή εν γένει ανεπιθύμητες ενέργειες ή καταστάσεις, με *τίμημα μια μικρή επιβράδυνση των επικοινωνιών* εξαιτίας του μεγαλύτερου, σε σχέση με τα απλά packet filters, χρόνου επεξεργασίας ενός πακέτου. Επιπλέον, είναι δυνατόν να καθορίζονται πολιτικές και δικαιώματα πρόσβασης για τις διάφορες εφαρμογές και τα πρωτόκολλα του εν λόγω OSI στρώματος, ανάλογα με την περίσταση και τις επιχειρησιακές ανάγκες. Βέβαια, ο ρυθμός ανάπτυξης νέων και εξέλιξης των υπαρχουσών εφαρμογών, πολλές φορές, τείνει να καθιστά τις λύσεις αυτού του είδους, αν όχι ανεπίκαιρες, σίγουρα ελλιπείς,[361] χωρίς αυτό να υποβαθμίζει τη σχετική τους σημαντικότητα και την ευεργετική δράση που επιδεικνύουν, ιδιαίτερα σε συνδυασμό με τις συγγενείς τους λύσεις IDS/IPS, που θα εξετάσουμε παρακάτω, ή συμπληρωματικά με τις προηγηθείσες τεχνολογίες πυροπροστασίας.

Τα μηχανήματα ή προγράμματα τειχών προστασίας έχουν εξελιχθεί τόσο, ώστε να αποτελούν το κατεξοχήν, πλέον απαραίτητο μέτρο ασφάλειας, για κάθε σύστημα που επιθυμείται να θεωρείται αξιόπιστο. Ειδικά, όσον αφορά το κακόβουλο λογισμικό, *η δράση των συστημάτων αντιπυρικής προστασίας είναι διττώς προληπτική* καθώς:

- Θωρακίζει από την έξωθεν πολιορκία ιών και ακόμα περισσότερο σκουληκιών.
- Αποτρέπει την σκόπιμη διαρροή πληροφοριών ή την εκκίνηση μη εξουσιοδοτημένης (δικτυακής) κίνησης προς το εξωτερικό περιβάλλον, που επιστρατεύουν ολοένα και πιο συχνά οι σύγχρονες ενσαρκώσεις των αυτοαναπαραγόμενων -και μη- όπλων λογισμικού.

Όλα τα τείχη πυροπροστασίας είναι *επισφαλή σε λογής επιθέσεις* (με τη βοήθεια και του κακόβουλου λογισμικού π.χ. «μασκάρεμα» των IP διευθύνσεων ή των DNS ονομάτων (υπόδυση ρόλου τύπου spoofing ή masquerading), επιθέσεις άρνησης εξυπηρέτησης, επιθέσεις βασισμένες σε ευπάθειες του υλισμικού ή ατέλειες παραμετροποίησης κτλ[362]) και όλα τους ανεξαιρέτως *ενδεχομένως να εμφανίζουν κάποιες, τεχνικές ατέλειες*, που μπορούν να τα καταστήσουν ανεπιτυχή[363] ή να τα οδηγήσουν σε βλάβη/δυσλειτουργία[364]. Ειδικά στην

[360] Χωρίς, όμως, να διαθέτουν και τις IDS υπογραφές των αντίστοιχων DPI λύσεων.

[361] Κύρια, βιβλιογραφική αναφορά: [FFIEC-IS].

[362] Όπως στην προηγούμενη υποσημείωση.

[363] Με την έννοια της αποτυχίας στην πρόληψη μιας εισβολής ή άλλης ανεπιθύμητης επικοινωνίας.

περίπτωση βλαβών ή παρατεταμένης δυσλειτουργίας, κατάλληλη μέριμνα πρέπει να έχει ληφθεί, ώστε οι συσκευές αυτές να λειτουργήσουν μάλλον ως «ανοιχτοί διακόπτες» μπλοκάροντας όλη τη διερχόμενη κίνηση, παρά σα δίοδοι ελεύθερης και άνευ εξουσιοδότησης πρόσβασης[365].

Από πλευράς σημαντικότητας και αξιοπιστίας, πάντως, θα μπορούσε να πει κανείς πως τα αντιπυρικά τείχη έχουν καταλήξει να θεωρούνται από τους περισσότερους στο χώρο ως ο *κύριος κορμός, πάνω στον οποίο πρέπει να αναπτύσσεται και να εξελίσσεται κάθε σοβαρή προσπάθεια αξιοπρεπούς οχύρωσης* των πληροφορικών δομών των σύγχρονων ψηφιακών μέσων και συστημάτων μαζικής επεξεργασίας, επικοινωνίας, συνεννόησης και συνεργασίας. Αυτή η παραδοχή τα καθιστά αναπόσπαστο και επιβεβλημένο κομμάτι στις προετοιμασίες, το σχεδιασμό και την υλοποίηση των πλάνων άμυνας κάθε τέτοιου συστήματος, απέναντι στο χάος των σημερινών, πληροφοριακών, επιθετικών ενεργειών.

4.1.4 Συστήματα ελέγχου ακεραιότητας

Οι ιοί και τα σκουλήκια, σε πλείστες των περιπτώσεων, καταλήγουν να μεταβάλλουν αρχεία ή άλλες πληροφορίες και ιδιότητες[366] των συστημάτων που μολύνουν, είτε προκειμένου να διαδοθούν είτε ως παράπλευρη απώλεια. Ειδικά συστήματα, που *παρακολουθούν για* τέτοιες *μη εξουσιοδοτημένες ή ύποπτες αλλαγές σε αρχεία και δεδομένα πληροφοριακών κόμβων*, μπορούν να *χρησιμοποιηθούν για τον εντοπισμό κακόβουλων προγραμμάτων και επιθέσεων*.

Τα συστήματα ελέγχου ακεραιότητας βασίζονται θεμελιωδώς στην *ύπαρξη ενός τέλεια «καθαρού» συστήματος*, που τα μέρη αυτού βρίσκονται σε ιδανικά άνοση κατάσταση, καθώς αυτό θα *αποτελεί το μέτρο σύγκρισης* για τα υπονομευμένα συστήματα. Πάνω στο σύστημα αυτό υπολογίζονται και φυλάσσονται αποτελέσματα ελέγχου ακεραιότητας των δομικών μερών και των δεδομένων σε μορφή *αθροισμάτων ελέγχου (checksums) και κρυπτογραφικής σύνοψης (hashes)*, που αντιπαραβάλλονται σε αντίστοιχες εκδοχές των πιθανώς μολυσμένων κόμβων και των περιεχομένων πληροφοριών τους.[367] Με τη λογική αυτή, *οποιαδήποτε παρέκκλιση από τις υπολογισμένες τιμές στην «καθαρή» κατάσταση εγείρει συναγερμό από*

---

[364] Εννοώντας μια πλήρη αποδιοργάνωση και εσφαλμένη λειτουργία του υλισμικού τους.

[365] Όταν ένα τείχος καταρρεύσει μηχανικά (λόγω προβλημάτων υλικού ή λογισμικού του) και ειδικότερα όταν αποτελεί μοναδικό σημείο αστοχίας (SPOF) καλό είναι να λειτουργεί πάντοτε ως φράγμα μεταξύ του υποκείμενου συστήματος πληροφοριών και του εξωτερικού κόσμου και να μην δρομολογεί μη ελεγχόμενη κίνηση εντός ή εκτός. Αυτό εν πολλοίς είναι θέμα σχεδιασμού και ρύθμισης των firewalls.

[366] Όπως μέγεθος, χρόνο τελευταίας τροποποίησης, πληροφορίες ιδιοκτησίας, ακόμα και πρότερα δεδομένα (όπως συμβαίνει στις τεχνοτροπίες για τις οποίες μιλήσαμε στους overwriters ιούς).

[367] Κύρια, βιβλιογραφική αναφορά: [COHEN-SCCV], [LUDWIG-GBBCV], [TANENBAUM-MOS9], [RABAIOTTI-CIS].

μέρους του ελεγκτή ακεραιότητας. Ο χρήστης, διαχειριστής ή υπεύθυνος ασφάλειας του Λ/Σ ή των εφαρμογών του κόμβου τελικά καλείται να αποφασίσει, αν μια τροποποίηση εντοπισμένη από το σύστημα ελέγχου ακεραιότητας είναι μη αναμενόμενη, μη αποδεκτή και όντως συνιστά παραβίαση ασφάλειας και να τροφοδοτήσει τον ελεγκτή με την κατάλληλη πληροφόρηση/απόφαση.[368] Κάτι τέτοιο μπορεί και να αυτοματοποιηθεί στη μορφή παραμετροποιήσιμων συνθηκών και πολιτικών, πάνω στις οποίες θα βασίσει το σύστημα ελέγχου της ακεραιότητας τις αποφάσεις και ενέργειές του, στα πλαίσια αποκάλυψης των εκάστοτε αποκλίσεων.

Ο έλεγχος ακεραιότητας μπορεί να συντελείται συνήθως με 4 διαφορετικούς τρόπους και τις αντίστοιχες φάσεις λειτουργίας:[369]

- *Σε κατάσταση «εκτός λειτουργίας» (offline)* και με τη βοήθεια εξωτερικών, «καθαρών» μέσων και την απευθείας σύγκριση με αυτά.
- *Με αυτό-έλεγχο των εκτελέσιμων προγραμμάτων* (και ιδιαίτερα του λογισμικού προστασίας από κακόβουλες δράσεις), όσο αυτά εκτελούνται από τα συστήματα επεξεργασίας· η απειλή του ρετροϊομορφισμού, όπως είδαμε άλλωστε, δεν είναι και μικρή.
- *Με τη στιγμή της πρόσβασης δράση από ξεχωριστά κελύφη Λ/Σ* (integrity shells)[370], ειδικά σχεδιασμένα για την ακεραιότητα, που σε πραγματικό χρόνο διαβεβαιώνουν για την πιστότητα και μη υπονόμευση των εφαρμογών του πυρήνα αλλά και άλλων κρίσιμων (εκτελέσιμων) προγραμμάτων· η θετική συμβολή από λειτουργίες σαν της επιβεβαίωσης συζητώνται και στο Κεφάλαιο 5.
- *Κατ' απαίτηση μέσω κατάλληλων, υπεύθυνων ρουτινών και διεπαφών χρήστη* των εξειδικευμένων εφαρμογών ελέγχου ακεραιότητας.

Πρέπει να σημειωθεί πως πέραν του εντοπισμού μιας ύποπτης μεταβολής στις τιμές ακεραιότητας, ένας ελεγκτής ακεραιότητας δεν παράγει άλλο, χρήσιμο, αντι-κακόβουλο

---

[368] Υπάρχει, βέβαια, η εγγενής αδυναμία που προκύπτει από τη διαπίστωση πως κάποιες αλλαγές στην ακεραιότητα εκ των πραγμάτων μπορεί να προέρχονται από κατά τα άλλα νόμιμα στοιχεία και ενέργειες εντός των ΠΣ. Αυτό δυσκολεύει τις αποφάσεις χρηστών και συστημάτων προστασίας, παράγοντας και πολλά false positives στην ανίχνευση.

[369] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM], [SZOR-ACVRD].

[370] Ο όρος integrity shell πρωτοχρησιμοποιήθηκε από τον Fred Cohen για να ονοματίσει το πρωτοπόρο και επαναστατικό, πρότυπο σύστημα ελέγχου ακεραιότητας, που κατασκεύασε το 1985 για το Λ/Σ UNIX.

έργο.[371] Για παράδειγμα, *δεν παρέχει ρουτίνες επιδιόρθωσης-ανοσοποίησης* ενός πιθανώς μολυσμένου συστήματος, αλλά επίσης *δε διαθέτει και κανένα μέσο για την αναγνώριση τους είδους και του γενεσιουργού αιτίου της εντοπισμένης παρεκτροπής*. Αποτελούν, όμως παράλληλα, οι λύσεις αυτές *μέτρα προστασίας τάχιστης απόκρισης με μικρές απαιτήσεις σε συστημικούς πόρους, που μπορούν να εντοπίσουν με ακρίβεια τις (παρ)ενέργειες γνωστών, αλλά και αγνώστων προϊόντων, κακόβουλης πρόθεσης*, και για αυτό χρησιμοποιούνται ευρέως, σε συνδυασμό και με το υπόλοιπο οπλοστάσιο της βιομηχανίας κατά του κακόβουλου λογισμικού[372].

4.1.5 Συστήματα παρεμπόδισης ύποπτης συμπεριφοράς

Τα συστήματα παρεμπόδισης ύποπτης συμπεριφοράς *παρακολουθούν τη συμπεριφορά προγραμμάτων και εφαρμογών, σε πραγματικό χρόνο, ελέγχοντάς τη για τυχόν ύποπτες δραστηριότητες*. Σε περίπτωση εμφάνισης/επιβεβαίωσης μιας παρόμοιας συμπεριφοράς, το σύστημα παρεμπόδισης εξουσιοδοτείται να αντιδρά με κωδικοποιημένα τα κατά συνθήκη αντίμετρα και π.χ. να προλαμβάνει τοιουτοτρόπως την επιτυχημένη εκτέλεση μιας ανεπιθύμητης εντολής ή να τερματίζει το ύποπτο, καλόν πρόγραμμα ή ακόμα να περιμένει ζητώντας τον καθορισμό κατάλληλου πλαισίου δράσης από τον άνθρωπο-χειριστή.[373]

Ο ορισμός της «καλής» ή «κακής» συμπεριφοράς τροφοδοτείται εξαρχής στο σύστημα παρακολούθησης και παρεμπόδισης, με τη μορφή πολιτικών ασφάλειας επιτρεπόμενων και ανεπίτρεπτων/ανεπιθύμητων ή μη αναμενόμενων ενεργειών και μπορεί να περιλαμβάνει και κάποιους ευριστικού τύπου κανόνες για ανώμαλη δραστηριότητα. Οι πολιτικές αυτές μπορούν στη συνέχεια και κατά την πορεία δράσης του παρεμποδιστή να τροποποιούνται με *μεγάλο βαθμό ευελιξίας* (αναβάθμιση, «σκλήρυνση», «χαλάρωση», προσθήκη, αφαίρεση) για να ικανοποιούν καλύτερα τις ανάγκες και τις παραμέτρους των εκάστοτε, υποστηριζόμενων πληροφοριακών δομών. Η *φυσιολογική συμπεριφορά* μοντελοποιείται σχεδόν πάντοτε ως *συνδυασμός μη απομάκρυνσης από τις εγκεκριμένες και αποφυγής των ανώμαλων δραστηριοτήτων*.[374] Σε διαφορετική περίπτωση, γίνεται λόγος αντίστοιχα για θετική ή αρνητική διάγνωση αφύσικης συμπεριφοράς, που προκύπτει κάθε φορά από τη μη

---

[371] Παρόλ' αυτά, ο Fred Cohen το 1994, στο βιβλίο του "A Short Course on Computer Viruses", επέδειξε πώς ο έλεγχος ακεραιότητας είναι η πιο αποδοτική γενικής φύσεως στρατηγική κατά των δράσεων του κακόβουλου κώδικα. Κύρια, βιβλιογραφική αναφορά: [COHEN-SCCV].

[372] Πολύ συχνά συναντάμε εξειδικευμένους ελέγχους ακεραιότητας στην πλειοψηφία των διακριτών προϊόντων προστασίας των ΠΣ.

[373] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM], [LUDWIG-GBBCV], [TANENBAUM-MOS9], [RABAIOTTI-CIS].

[374] Στη λογική των boosters και των stoppers, που συναντήσαμε στις ευριστικές τεχνικές του εδαφίου 4.1.1.

ικανοποίηση των κωδικοποιημένων, θετικού τύπου συνθήκης (allow) στην μια περίπτωση ή αρνητικού στην άλλη (forbid/block), προτύπων συμπεριφοράς.

Κρίνοντας τα συστήματα παρεμπόδισης με βάση τη σχετική τους επιτυχία πιο συγκεκριμένα στην αντιμετώπιση ιών και σκουληκιών μπορούμε να επισημάνουμε τη *δυναμική εντοπισμού γνωστών και αγνώστων τύπων απειλών* που είδαμε και στα συστήματα ελέγχου ακεραιότητας, με μεγαλύτερη όμως παροχή γνώσης που αφορά την πηγή και αιτία του προβλήματος από ό,τι σε εκείνα.[375] Παραμένει, ωστόσο, και εδώ -ελλείψει σάρωσης και κακόβουλων υπογραφών- η γνωστή *αδυναμία αναγνώρισης του είδους του κακόβουλου προγράμματος* και η *απουσία συγκεκριμένων ρουτινών κάθαρσης/επαναφοράς* από μια μόλυνση, απουσία που συναντήθηκε επίσης στους ελεγκτές ακεραιότητας, ευρισκόμενες παράλληλα σε συνδυασμό και με *κάποιες εγγενείς αδυναμίες όπως των κακώς επιτυχημένων (false positives[376]) -θετικών και αρνητικών- διαγνώσεων, της λειτουργικής επιβάρυνσης στην κατανάλωση συστημικών πόρων και της αναγκαιότητας για μια έστω και μικρής διάρκειας προηγηθείσα ή τρέχουσα δράση του ιού ή του σκουληκιού, προκειμένου να εντοπιστεί η κακόβουλη συμπεριφορά του*. Μια τέτοια απειλή αντιμετωπίζεται, πάντως εν τέλει, από τους παρεμποδιστές με συνδυασμούς καίριων, *στοιχειωδών προληπτικών-αποτρεπτικών (αντι)μέτρων*, όπως π.χ. με περιορισμό της ακτίνας δράσης και μετάδοσής της, αποτροπή της επιπλέον εκτέλεσης ή παραμονής στη μνήμη, διαγραφή/αποκοπή της πηγής των προβλημάτων ή/και ειδοποίηση-έκκληση στον άνθρωπο-χειριστή για περαιτέρω ενέργειες[377], που δεν στοιχειοθετούν όμως σαφή απομάκρυνση της πραγματικής πηγής του προβλήματος, παρά στρέφονται μόνο στον αισθητό μετριασμό της επιζήμιάς του δράσης.

4.1.6 Προηγμένα Συστήματα IDS/IPS

Τα συστήματα IDS/IPS αποτελούν την *επιτομή της τεχνολογίας ασφάλειας* απέναντι στο επιβλαβές λογισμικό και εν γένει τις κακόβουλες, πληροφοριοθηρικές επιδρομές. Κάθε τέτοιο σύστημα διατείνεται πως μπορεί να χρησιμοποιηθεί για τον έγκαιρο εντοπισμό και αναγνώριση εκείνων των συμπεριφορών και καταστάσεων που υποβαθμίζουν την ασφάλεια και υπονομεύουν την αξιοπιστία ενός ΠΣ, παρέχοντας ενδεχομένως και τη δυνατότητα για ανάληψη ανταπαντητικής δράσης. Στην ουσία, φιλοδοξούν να αποτελέσουν ένα πρότυπο,

---

[375] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM].

[376] Το πρόβλημα μιας κακώς επιτυχημένης διάγνωσης ταλανίζει εγγενώς όλα τα γνωστά συστήματα προστασίας, εδώ όμως, λόγω του ιδιαίτερα αφηρημένου χαρακτήρα της μοντελοποίησης μιας ύποπτης ή μη συμπεριφοράς (χωρίς υπογραφές ή κανόνες πρόσβασης), η επενέργεια των πάντοτε χαοτικών, συστημικών γεγονότων και περιστατικών μπορεί να παράγει πολύ περισσότερες λάθος επισημάνσεις.

[377] Ο χρήστης ειδοποιείται με κατάλληλα μηνύματα για τον εντοπισμό μιας τεκμηριωμένα ύποπτης συμπεριφοράς

ευφυές και ολοκληρωμένο, «ανοσοποιητικό σύστημα» για τα υπολογιστικά συστήματα και τα δικτυώματά τους.

Δύο είναι οι βασικές υλοποιήσεις: *τα παθητικά συστήματα εντοπισμού εισβολών ή αμιγή IDS* και *τα ενεργητικά-αντιδραστικά συστήματα «πρόληψης» εισβολών ή συντομότερα IPS*.[378] Τα μεν πρώτα ειδικεύονται στην παρακολούθηση-ανίχνευση κακόβουλων παρεισφρύσεων, με παράλληλη καταγραφή τους και ενεργοποίηση κατάλληλων συναγερμών ή αποστολή ανάλογων ειδοποιήσεων στο διαχειριστικό προσωπικό, ενώ τα δεύτερα δεν περιορίζονται σε αυτές τις λειτουργίες, αλλά τις προχωρούν ένα βήμα παραπάνω ανταποκρινόμενα -όπου χρειάζεται και είναι εφικτό- με αυτόματο, αποτρεπτικό τρόπο στις διάφορες προκλήσεις επιδιώκοντας τον περιορισμό και ει δυνατόν την εξάλειψή τους. Τα συστήματα αυτά εξετάζονται μαζί, τόσο γιατί αποτελούν το ένα φυσική επέκταση του άλλου, όσο και γιατί ο συνδυασμός της δράσης τους προβάλλει ως εξαιρετικά ολοκληρωμένη πρακτική και εποικοδομητική πολιτική προστασίας, στη μάχη με πάσης φύσεως απειλές κατά της ασφάλειας πληροφοριών και ιδιαίτερα όσες εδρεύουν ή χρησιμοποιούν τις δικτυακές συνδέσεις των ΠΣ (σκουλήκια, συνδυασμένες απειλές, ιομορφικό περιεχόμενο σε μηνύματα και αιτήσεις εξυπηρέτησης).

Ένα τυπικό IDS/IPS σύστημα αποτελείται από τα ακόλουθα συστατικά:[379]

1. **Διάφορους αισθητήρες (sensors)** που παρακολουθούν το υποστηριζόμενο σύστημα, συλλαμβάνουν τις όποιες «διεγέρσεις» του και παράγουν τα γεγονότα/περιστατικά ασφάλειας (security events).

2. **Μια κονσόλα (console)** επιτήρησης των γεγονότων και των συναγερμών και ελέγχου των αισθητήρων.

3. **Μια κεντρική μηχανή (alert/notification engine)**, που καταγράφει τα γεγονότα που παρατηρούνται από τους αισθητήρες σε μια βάση δεδομένων και χρησιμοποιεί ένα σύστημα κανόνων (π.χ. υπογραφές κακόβουλου λογισμικού, λίστες πρόσβασης και άλλες ρητές πολιτικές ασφάλειας και ελέγχου συμπεριφοράς, ευριστικές μέθοδοι για «ανώμαλη» συμπεριφορά) για να παραχθούν κατόπιν επεξεργασίας (π.χ. σάρωση δεδομένων για κακόβουλο περιεχόμενο, απλός ή σε βάθος (DPI) έλεγχος εγκυρότητας δικτυακής κίνησης, επιβεβαίωση συμπεριφορικής νομιμότητας, δυναμική, με βάση δοκιμές αποκρυπτογράφηση) οι κατάλληλοι συναγερμοί και ειδοποιήσεις από τα λαμβανόμενα γεγονότα ασφάλειας.

4. **Ένα σύνολο κανόνων αντίδρασης ή αυτοάμυνας (response ruleset)** και ένα σύνολο διεπαφών με το Λ/Σ τυχόν φέροντα κόμβου, την υπόλοιπη υποδομή ασφάλειας (π.χ. τείχη

---

[378] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM].

[379] Πηγή: Διαδίκτυο, ιστοχώρος της online εγκυκλοπαίδειας WikiPedia, http://en.wikipedia.org/wiki/Intrusion-detection_system.

πυροπροστασίας, παρεμποδιστές κτλ), αλλά και τους δικτυακούς διαύλους (κάρτες δικτύου, sockets στον πυρήνα του Λ/Σ), βάσει των οποίων μπορεί ένα IPS να συντονίζει τις προληπτικές του ενέργειες («φιλτράρισμα», περιορισμός/τερματισμός συνδέσεων κτλ).

Υπάρχουν διάφοροι τρόποι να ταξινομηθεί ένα IDS/IPS, ανάλογα με τον τύπο και τη θέση των αισθητήρων και της μεθοδολογίας που χρησιμοποιείται από τη μηχανή για να παραγάγει τις ειδοποιήσεις και τους συναγερμούς. Σε πολλές, απλές εφαρμογές IDS/IPS τα τέσσερα προηγούμενα συστατικά στοιχεία συνδυάζονται είτε σε μια *ενιαία συσκευή ή μηχάνημα (HW-based)* είτε υλοποιούνται *εντός αυτόνομων προγραμμάτων, λογισμικών πακέτων και βιβλιοθηκών (SW-based)*.[380]

Ανάλογα, επίσης, με την ιδιαίτερη θέση τους στο δικτυακό, πληροφοριακό περιβάλλον τα εν λόγω IDS/IPS συστήματα μπορούν να διαχωριστούν στις παρακάτω λύσεις:

Επιπέδου κόμβου (host-based)

Τα συστήματα αυτά (είτε σε IDS είτε σε IPS λειτουργία) εδρεύουν εντός συγκεκριμένου κόμβου και σκοπό έχουν να προστατεύουν αυτόν και μόνο από επίβουλες προσπάθειες υπονόμευσής του. Ως υλοποιήσεις και δραστηριότητες εξαρτώνται σε μεγάλο βαθμό από το είδος του Λ/Σ και των εφαρμογών των κόμβων που καλούνται να περιφρουρήσουν. Στην πλειοψηφία τους είναι προϊόντα λογισμικού, που τρέχουν ως αυτόνομες διεργασίες στο στοχευμένο Λ/Σ (στο επίπεδο πυρήνα ή, αν και πλέον όχι και τόσο συχνά, στο επίπεδο χρήστη) του δεδομένου κόμβου, που τα φιλοξενεί και τον οποίο καλούνται να υπηρετούν και επιτηρούν.[381]

A. hIDS

Αποτελούνται από πράκτορες λογισμικού (software agents) που εγκαθίστανται σε μεμονωμένους υπολογιστές μέσα στο πληροφοριακό σύστημα, που ενδιαφέρει. Τα hIDS αναλύουν κατά κύριο λόγο την κυκλοφορία από και προς το συγκεκριμένο υπολογιστή, στον οποίο το λογισμικό ανίχνευσης εισβολής εγκαθίσταται. Γενικότερα, όμως, είναι σε θέση να παρακολουθούν τις δραστηριότητες που μόνο ένας διαχειριστής θα μπορούσε να επιτελεί και

[380] Που ενδέχεται άλλοτε να δρουν εντελώς ανεξάρτητα και άλλοτε να ορίζονται, κατευθύνονται και ενορχηστρώνονται από κάποιον, κεντρωμένο «νου», στη μορφή υλισμικού.

[381] Χωρίς όμως να αποκλείεται σε κάποιες περιπτώσεις -ειδικά hIDS- ο συντονισμός, η καθοδήγηση και η επεξεργασία της δραστηριότητας των διαφόρων πρακτόρων λογισμικού των κόμβων να επιτελείται συνολικά από κάποιο, κεντρικό μηχάνημα/υλισμικό.

να επιβλέπει εντός του Λ/Σ του κόμβου που επιθεωρούν.[382] Είναι ικανά π.χ. να ελέγχουν για αλλαγές σε βασικά αρχεία των συστημάτων, καθώς και για οποιαδήποτε προσπάθεια να επικαλυφθούν αυτά τα αρχεία ή ακόμα να ειδοποιούν -με τη βοήθεια ταιριάσματος γνωστών υπογραφών και παραβίασης θεσπισμένων κανόνων ασφάλειας- για απόπειρες να εγκατασταθεί πάσης φύσεως κακόβουλο λογισμικό εντός συστήματος. Σε αντίθεση με τα δικτυακά IDS (nIDS), δεν προσφέρουν αληθινή σε πραγματικό χρόνο ανίχνευση, παρά μόνο εάν παραμετροποιηθούν σωστά, οπότε πλησιάζουν πιο πολύ τον πραγματικό χρόνο.[383] Η καλή τους λειτουργία εξαρτάται σε μεγάλο βαθμό από τις επεξεργαστικές δυνατότητες του φέροντα κόμβου και από την πυκνή ενημέρωση των υπογραφών ασφάλειας.

B. hIPS

Χρησιμοποιούνται για να προστατεύσουν τόσο κεντρικούς εξυπηρετητές όσο και τερματικούς σταθμούς ενός ΠΣ, μέσω λογισμικού που «τρέχει» μεταξύ συστημικών εφαρμογών και πυρήνα του Λ/Σ των κόμβων. Το λογισμικό αυτό επιτηρεί, συνήθως, κανόνες προστασίας βασισμένους σε υπογραφές παρείσφρυσης ή/και επίθεσης, καθώς και σε άλλους μηχανισμούς ελέγχου ύποπτης συμπεριφοράς. Τα hIPS «συλλαμβάνουν»[384] την τυχόν ύποπτη δραστηριότητα στο σύστημα και έπειτα, ανάλογα με τους προκαθορισμένους κανόνες, είτε παρεμποδίζουν (με τη βοήθεια του Λ/Σ) είτε επιτρέπουν στο όποιο γεγονός να συμβεί. Τα συστήματα αυτά μεταξύ άλλων παρακολουθούν δραστηριότητες, όπως αιτήματα για εφαρμογές ή δεδομένα, προσπάθειες δικτυακής σύνδεσης, απόπειρες ανάγνωσης/εγγραφής κ.ά..

Τα hIPS σε κάθε ευρισκόμενο σύστημα πρέπει πάση θυσία να ενημερώνονται συχνά, για να εξασφαλιστεί ότι οι υπογραφές εισβολής/επίθεσης δε θα είναι ποτέ ανεπίκαιρες ή/και κακώς εφαρμόσιμες, ενώ και οι απαιτήσεις σε συστημικούς πόρους για την εκτέλεση των ελέγχων συμμόρφωσης στο παρασκήνιο του Λ/Σ ίσως να εγείρει περιορισμούς για το υλικό και το λογισμικό των φερόντων κόμβων.

Ενώ τα hIPS θεωρείται πως παρέχουν πληρέστερη[385] (αλλά και πιο κατανεμημένη) ασφάλεια από τα αδελφά τους δικτυακά συστήματα πρόληψης εισβολής (nIPS), η διαδικασία του να

---

[382] Πηγή: Διαδίκτυο, ιστοχώρος της online εγκυκλοπαίδειας WikiPedia, http://en.wikipedia.org/wiki/Host_based_intrusion_detection_system.

[383] Πηγή: "Intrusion Detection & Prevention: All About IPS & IDS", Vangie 'Aurora' Bell, 2005, διαθέσιμο από το δεσμό http://www.webopedia.com/DidYouKnow/Computer_Science/2005/intrusion_detection_prevention.asp.

[384] Σε πραγματικό χρόνο με τη βοήθεια των Λ/Σ.

[385] Για παράδειγμα μπορούν να αναλύσουν τα περιεχόμενα μια κρυπτογραφημένης συνόδου, εφόσον αυτή τελικά αποκρυπτογραφείται εντός κόμβου, πράγμα που τα δικτυακά ευρισκόμενα nIPS δεν μπορούν να πραγματοποιούν χωρίς επιτυχημένη εφαρμογή μεθόδων ωμής ή λεξικογραφικής επίθεσης στο κρυπτογραφημένο περιεχόμενο.

εγκαταστήσει κανείς το απαραίτητο λογισμικό σε κάθε μηχάνημα, εντός δοθέντος ΠΣ, μπορεί να είναι αρκετά δαπανηρή από πάσης άποψης[386] και εμπεριέχει κινδύνους σχεδιαστικών ατοπημάτων ή παραβλέψεων.

Επιπέδου δικτύου (network-based)

Σε αντίθεση με την παραπάνω κατηγορία, τα IDS/IPS αυτού του τύπου κατέχουν περιμετρικές ή άλλες εποπτικές του δικτύου θέσεις-κλειδιά στο πληροφοριακό οικοδόμημα, που καλούνται να προστατεύσουν συνολικά και χωρίς εξαιρέσεις.[387] Η υλοποίηση τους εμπλέκει, συνήθως, σύνθετο υλισμικό (συσκευές με το οδηγούν λογισμικό τους) και η φιλοσοφία κατασκευής και τοποθέτησής τους ομοιάζει των «κλασσικών» τειχών πυροπροστασίας υλισμικού τύπου, χωρίς να αποκλείονται σπανιότερα και λύσεις αμιγώς λογισμικού τύπου, όπου κάποιος κεντρικός εξυπηρετητής/σταθμός εργασίας/δικτυακός κόμβος αναλαμβάνει να εκτελεί το IDS/IPS πρόγραμμα ως υπηρεσία για λογαριασμό ολόκληρου του δικτυοκεντρικού ΠΣ.

A. nIDS

Είναι συχνά αυτόνομες συσκευές υλικού, που περιλαμβάνουν ικανότητες ανίχνευσης παρείσφρυσης δικτύων. Αποτελούνται, συνήθως, από αισθητήρες υλικού που βρίσκονται διάσπαρτοι σε διάφορα κρίσιμα σημεία κατά μήκος του δικτύου ή από τμήματα λογισμικού[388] που εγκαθίσταται στους υπολογιστές του πληροφοριακού δικτύου και που αναλύουν τα πακέτα δεδομένων που εισχωρούν ή εγκαταλείπουν το δικτυακό ιστό του ΠΣ.

Η λογική ανάλυσης που διέπει τα εν λόγω συστήματα δε διαφέρει από τα hIDS με την έννοια ότι το ζητούμενο είναι εκ νέου ο εντοπισμός, με τη βοήθεια κατάλληλων (και επίκαιρων) υπογραφών αλλά και άλλων πολιτικών ασφάλειας, των διαφόρων επίβουλων υπονομεύσεων. Το συγκριτικό τους πλεονέκτημα είναι ο αισθητά μικρός χρόνος απόκρισης σε περίπτωση εισβολής, που όμως ισοσκελίζεται κάπως από τον περιορισμό του εύρους ευθύνης στη δικτυακή κίνηση (κυρίως πακέτα) και μόνο, σε σχέση πάντα με τα αδελφά hIDS. Αν και εξαρτάται σημαντικά από το μέγεθος του δικτύου και τον αριθμό των μεμονωμένων κόμβων

---

[386] Ειδικά αν το δικτύωμα αναφοράς έχει πολλούς κόμβους για εποπτεία, η απαιτούμενη κατανάλωση σε ανθρώπινους και οικονομικούς πόρους για την προμήθεια, εγκατάσταση, παραμετροποίηση, συντήρηση και λειτουργία hIPSs είναι ένα αδιαμφισβήτητο πρόβλημα.

[387] Τα επιπέδου δικτύου συστήματα προστασίας είναι node platform agnostic, δηλαδή δεν περιορίζεται η δράση τους από τα Λ/Σ και τις εφαρμογές που εκτελούνται στους πληροφοριακούς κόμβους, που καλούνται να προστατεύσουν.

[388] Στη μορφή και λειτουργία πρακτόρων λογισμικού (software agents), που εγκαθίστανται σε κάθε μηχανή που χρήζει εποπτείας, και επικοινωνούν/συνεργάζονται μεταξύ τους και με το κεντρικό IDS μηχάνημα για την ανίχνευση προβλημάτων και την παραγωγή ειδοποιήσεων.

που το απαρτίζουν, τα nIDS είναι συνήθως φθηνότερη λύση από τα hIDS[389] και απαιτούν λιγότερους πόρους από άποψη διαχείρισης και κατάρτισης των χρηστών. Στην πράξη, όμως, δεν είναι ούτε τόσο ευέλικτα ούτε τόσο εύκαμπτα από πλευράς ρύθμισης και αναβάθμισης, όπως τα επιπέδου κόμβου ανάλογά τους, ενώ επίσης παύουν να παρέχουν οποιαδήποτε προστασία, αν η δικτυακή δομή καταρρεύσει και αποτελούν μοναδικά σημεία αστοχίας/αποτυχίας (Single Points Of Failure, SPOF) για συστήματα άμυνας, που βασίζονται κυρίως σε αυτά.[390] Τέλος, μην ξεχνάμε πως εισάγουν εκ των πραγμάτων μια πρόσθετη, δικτυακή επιβάρυνση (λόγω της επιθυμητής επεξεργασίας της κίνησης των πακέτων) στο σύστημα που υποστηρίζουν.

Β. nIPS

Τα συχνά αποκαλούμενα ευθύγραμμα συστήματα πρόληψης είναι μια κεντρωμένη λύση, για βασισμένη στο δίκτυο ασφάλεια, με τη βοήθεια εξειδικευμένου υλισμικού ή αλλιώς «αφοσιωμένου» μηχανήματος. Τα nIPS παρεμβάλλονται σε όλη την κυκλοφορία των δικτύων και την ελέγχουν για την πάσα ύποπτη δραστηριότητα, αναζητώντας και απομονώνοντας γεγονότα «ανώμαλης» συμπεριφοράς, με στόχο την παρεμπόδιση των όσων κριθούν ακατάλληλα και το μικρότερο δυνατό κόστος για την ταχύτητα και επιτυχία διέλευσης της νόμιμης κίνησης.

Η δομή και δραστηριότητά τους πλησιάζει πολύ τις αντίστοιχες των τειχών πυροπροστασίας επιπέδου εφαρμογής μιας και οι έλεγχοι για αποδοχή/απόρριψη των πακέτων δεδομένων και μηνυμάτων υπηρεσιών είναι σχεδόν πανομοιότυποι, χωρίς όμως αυτό να είναι αρκετό για να χαρακτηριστούν τέτοια.[391] Άλλωστε, τα nIPS προχωρούν ένα βήμα παραπάνω δρώντας αποτρεπτικά (σε συνεργασία ενδεχομένως και με υπάρχοντα αντιπυρικά τείχη που υποστηρίζουν δυναμικούς κανόνες φιλτραρίσματος) στην περαιτέρω εξάπλωση/διείσδυση μιας επιβεβαιωμένης, παρατηρούμενης υπονόμευσης-παραβίασης, που δεν μπορούσε να υπαχτεί σε κάποιον προμελετημένο κανόνα, αλλά κρίθηκε παρόλ' αυτά επικίνδυνο γεγονός χάρη στους ευριστικού τύπου μηχανισμούς ανακάλυψης ύποπτων συμπεριφορών. Ακόμα, εμφανίζονται πιο ευέλικτα από τα «ξαδέλφια» τους αντιπυρικά τείχη, καθώς η αυστηρότητα της επιβαλλόμενης πολιτικής ασφάλειας στη δικτυακή κίνηση μπορεί εν γένει να «σφίγγει» ή

---

[389] Δεν ισχύει από οικονομικής απόψεως πάντα και για όλες τις προσφερόμενες από την εν λόγω αγορά λύσεις, αλλά διαχειριστικά τουλάχιστον (σε δείκτες ολικού κόστους ιδιοκτησίας ή TCO) μια δικτυακού τύπου λύση προστασίας παρουσιάζεται πολύ περισσότερο ανεκτή ή συμφέρουσα σε σχέση με μια εντός κόμβων προσέγγιση.

[390] Πηγή: "Host-Based IDS vs Network-Based IDS", Ricky Magalhaes, 2006, διαθέσιμο από το δεσμό http://www.windowsecurity.com/articles/Hids_vs_Nids_Part1.html.

[391] Πηγή: Διαδίκτυο, ιστοχώρος της online εγκυκλοπαίδειας WikiPedia, http://en.wikipedia.org/wiki/Intrusion-prevention_system#IPS.2C_Application_Firewalls.2C_Unified_Threat_Management_.26_Access_Control.

να «χαλαρώνει» κατάλληλα και με δυναμικό τρόπο για να προσαρμόζεται πιο αποτελεσματικά στις επιταγές του περιβάλλοντος και των προκλήσεων αυτού. Τέλος, έχουν εξαρχής σχεδιαστεί για να είναι πρακτικά «αόρατα» από το τμήμα του δικτύου που επιβλέπουν (δε διαθέτουν IP διεύθυνση ανήκουσα στο εν λόγω τμήμα του δικτύου ή δεν απαντούν σε αιτήσεις εξυπηρέτησης προερχόμενες από το τμήμα αυτό), πράγμα που έρχεται σε πλήρη αντίθεση με οποιαδήποτε υπόσταση αντιπυρικού τείχους.

Στα θετικά των nIPS, η υποσχόμενη, κεντρικού τύπου προστασία[392], στα αρνητικά, η έτσι και αλλιώς αδυναμία σε βάθος ελέγχου των εντός των κόμβων τεκταινόμενων πέραν της εγκυρότητας των αιτημάτων και απαντήσεων εξυπηρέτησης, η συχνά παρουσιαζόμενη δικτυακή επιβράδυνση που τα συνοδεύει και το αυξημένο κόστος από τις λάθος διαγνώσεις και παρακωλύσεις μιας κατά τα άλλα νόμιμης επικοινωνίας[393]. Η αναγκαιότητα για τακτή ενημέρωση των υπογραφών ασφάλειας και για μεθοδική παραμετροποίηση είναι για άλλη μια φορά υψίστης σημασίας -εδώ μάλιστα ένα σκαλί παραπάνω λόγω του συγκεντρωτικού και οικουμενικού χαρακτήρα της λύσης- προκειμένου να αποφεύγονται ανεπιθύμητες εμπλοκές.

Όλα τα IDS/IPS, ανεξαιρέτως, εμφανίζουν σημαντική συνάφεια στη λειτουργία τους με τα, σε προηγούμενο εδάφιο, αναφερόμενα τείχη πυροπροστασίας επιπέδου εφαρμογής, με την έννοια ότι και οι 2 λύσεις ασκούν πληθώρα ελέγχων στο στρώμα εφαρμογής του προτύπου OSI με ό,τι οφέλη και αδυναμίες αυτό συνεπάγεται· η ουσιώδης όμως διαφορά τους και συνάμα ένα μέτρο για την πολυσήμαντη αξία τους είναι πως τα διάφορα συστήματα εντοπισμού ή πρόληψης εισβολών εξετάζουν, επιβάλλουν και περιφρουρούν σημαντικά μεγαλύτερο αριθμό λογικών συνθηκών και πολιτικών ασφάλειας, από μοναχά τη στενή παρακολούθηση της δικτυακής κίνησης, συμπεριλαμβανομένου εκτός των άλλων ελέγχων συμμόρφωσης σε επίπεδο Λ/Σ και διεργασιών, συσκευών αποθήκευσης, μνήμης και επεξεργασίας, ενώ παράλληλα διακρίνονται και από τη μεγαλύτερη δυνατότητα παραμετροποίησης, καθώς τέλος και από έναν ξεκάθαρα υπέρτερο μηχανισμό υπευθυνότητας με λεπτομερή καταγραφή συμβάντων, ενεργοποίηση συναγερμών και αποστολή ειδοποιήσεων ασφάλειας. Ειδικά, ο τελευταίος, αυτοματοποιημένος μηχανισμός είναι και ένας από τους κατεξοχήν λόγους δημιουργίας και καθοριστικός παράγοντας επιτυχίας-διάδοσης των συστημάτων αυτών.

Ως βασικά προβλήματα, που ταλανίζουν τα υπό συζήτηση συστήματα, αναφέρουμε ενδεικτικά την *αυξημένη, διαχειριστική πολυπλοκότητα τους και την επεξεργαστική ή δικτυακή*

[392] Η οποία, όπως και στα nIDS, όμως, σημαίνει ταυτόχρονα και SPOF πρόβλημα.

[393] Πηγή: "Intrusion Detection & Prevention: All About IPS & IDS", Vangie 'Aurora' Bell, 2005, διαθέσιμο από το δεσμό http://www.webopedia.com/DidYouKnow/Computer_Science/2005/intrusion_detection_prevention.asp.

επιβάρυνση (latency) εξαιτίας των εφαρμοζόμενων, ενδελεχών ρουτινών ελέγχου, ενώ πεδία επίκαιρης, ερευνητικής και βιομηχανικής δραστηριότητας βελτιστοποίησης αποτελούν οι στόχοι περαιτέρω αύξησης του ρυθμού *απόκρισης και απόδοσης (throughput)* και παράλληλης μείωσης των *μη αμελητέων* -αλλά κατά γενική ομολογία ήδη χαμηλών- επιπέδων διακύμανσης των *κακώς επιτυχημένων και αποτυχημένων (false positives and negatives)* διαγνώσεων, συναγερμών και ειδοποιήσεων.[394]

Σε γενικές γραμμές, πάντως, η δυνατότητα για έγκυρο και έγκαιρο εντοπισμό κακόβουλων ή ανεπιθύμητων ενεργειών, που οδηγούν σε παραβιάσεις και άλλες υποβαθμίσεις αξιοπιστίας, σε συνδυασμό με την παροχή δυνατοτήτων απομάκρυνσης του εμφανιζόμενου κινδύνου, στα πρώτα στάδια εξέλιξής του, αλλά και με την υποστήριξη της διαλειτουργικότητας και συνεργασίας με άλλα υπάρχοντα συστήματα ασφάλειας, έχουν καθιερώσει τα IDS/IPS ως τις πλέον ολοκληρωμένες λύσεις προστασίας και ως τα πιο επιπρόσθετα αναγκαία μέτρα πρώτης γραμμής στο πεδίο μάχης μιας πολύτροπης και ουσιαστικής διαφύλαξης των σύγχρονων και κρίσιμων ΠΣ και ιδιαίτερα στον αγώνα κατά της εχθροπραξίας μέσω αυτοαναπαραγόμενου οπλολογισμικού.

4.1.7 Εργαλειοθήκες ασφάλειας

Πέρα από τους προαναφερόμενους και πλέον γνωστούς εκπροσώπους της βιομηχανίας προστασίας από τα κακόβουλα προγράμματα και την ανάλογη δράση υπάρχει και μια *σειρά εξειδικευμένων προϊόντων* του αυτού προσανατολισμού που επιτελούν πρόσθετο ρόλο ασφάλειας ή συνεπικουρούν το προσωπικό και τα μεγαλύτερα συστήματα ασφάλειας, χωρίς να ανήκουν όμως ξεκάθαρα σε κάποια από τις παραπάνω κατηγορίες λογισμικού ή υλισμικού.

Σήμερα, παρατηρείται πληθώρα τέτοιων εργαλείων πολλά από τα οποία γίνονται διαθέσιμα απευθείας μέσω του Διαδικτύου με απλή μεταφόρτωση λογισμικού. Στο είδος αυτό ανήκουν π.χ. προγράμματα όπως:

- **Κρυπτογραφικές βιβλιοθήκες και λογισμικό**, όπως π.χ. το CryptoAPI της Microsoft ή οι ευρέως χρησιμοποιούμενες OpenSSL βιβλιοθήκες.
- **Αναλυτές δικτυακής κίνησης και επικοινωνίας (sniffers, dumpers),** όπως τα πασίγνωστα WireShark, tcpdump και TCPView.

[394] Κύρια, βιβλιογραφική αναφορά: [ZANERO-FFEIIT].

- **Αναλυτές αρχείων καταγραφής**, όπως π.χ. οι syslog «δαίμονες» των συστημάτων UNIX ή το EventViewer των Windows.
- **Αναλυτές διεργασιών** (παρακολούθηση/μετατροπή αναγκών και λειτουργιών επεξεργασίας, μνήμης, μητρώου, δίσκων κ.ά.), όπως είναι για παράδειγμα οι εφαρμογές της SysInternals Process Explorer, RegMon και Process Monitor.
- **Αποσφαλματωτές/Αποσυναρμολογητές κώδικα**, όπως τα προγράμματα SoftICE ή OllyDbg.

Τα παραπάνω προγράμματα και συστήματα μπορούν να αποτελέσουν *πολύτιμες εργαλειοθήκες* για την ασφάλεια και την προστασία των ΠΣ, καθώς παρέχουν στο υπεύθυνο προσωπικό και τα ανάλογα συστήματα χρήσιμες πληροφορίες και ενδείξεις για τη συμπεριφορική κατάσταση των εκτελέσιμων εφαρμογών, του Λ/Σ, των διαφόρων κόμβων ή του όλου δικτύου και ειδικά όσον αφορά σημάδια εμφάνισης και δράσης κακόβουλου λογισμικού. Στα χέρια ικανών επιτήδειων τα εν λόγω σετ εργαλείων, που κυρίως εξυπηρετούν διαδικασίες ενίσχυσης, παρακολούθησης, σήμανσης και ανάλυσης, μπορούν να διευκολύνουν με πολύ αποτελεσματικό τρόπο τις προσπάθειες πρόληψης, όμως κατά μείζονα λόγω υποβοηθούν εκείνες του εντοπισμού, αλλά υπό προϋποθέσεις ακόμα και της αφαίρεσης των κακόβουλων απειλών, χωρίς αυτό να σημαίνει πως δεν μπορούν -άμεσα ή έμμεσα- να εξυπηρετήσουν ταυτόχρονα και τους σκοπούς των κακόβουλων οντοτήτων[395]. Η τεχνολογία, εξάλλου, τις περισσότερες φορές είναι κάτι το ουδέτερο, η χρήση αυτής και οι επιπτώσεις από αυτήν την χρήση είναι που πρέπει να χαρακτηρίζονται ως επωφελείς ή επιζήμιες.

4.2 Λειτουργικά Συστήματα

Τα λειτουργικά συστήματα αποτελούν *το «νου» κάθε υπολογιστικού κόμβου* ενός δικτυοκεντρικού ΠΣ. Η καλή και αναμενόμενη λειτουργία των κόμβων (άρα και του συνόλου του πληροφοριακού οικοδομήματος) στα σημερινά περιβάλλοντα των πολύπλοκων κακόβουλων απειλών βασίζεται σε μεγάλο μέρος στην ύπαρξη και εφαρμογή πολύ συγκεκριμένων μέτρων προστασίας σε επίπεδο Λ/Σ. Η τάση αυτή για εντός των τειχών προστασία είναι πλέον ιδιαίτερα διαδεδομένη στους κόλπους της ασφάλειας, τόσο που έχει

[395] Παραδείγματος χάριν οι κρυπτογραφικές βιβλιοθήκες αποτελούν άμεσο όχημα για την επιτυχή εκδήλωση κρυπτοϊομορφικών επιθέσεων, ενώ ο μεταμορφισμός χρειάζεται τους αποσυναρμολογητές για να μεταφράζει δυναμικά και να μεταλλάσει τον κώδικα του στη μνήμη. Όσο δε για τους sniffers, τους debuggers ή τα υπόλοιπα είδη και συστήματα εξειδικευμένων εργαλείων προστασίας, όλα τους ανεξαιρέτως έχουν θέση στο οπλοστάσιο του κακόβουλου προγραμματιστή ή εισβολέα.

αρχίσει να καθορίζει τις μελλοντικές εξελίξεις στα πεδία μάχης των πληροφοριακών αντιπάλων[396].

Ένα Λ/Σ παρέχει τόσο τη δυνατότητα για την αποτροπή μολύνσεων, αλλά και για τον έγκαιρο εντοπισμό μιας υποβάθμισης στην ασφάλεια, όσο και τα «μέσα» για μια ισχυρή (σε βάθος) υπονόμευση ενός κόμβου, σε σημείο που οι κακόβουλες ενέργειες να μην είναι αναγνωρίσιμες[397]. Η διττή αυτή φύση, υπό το πρίσμα αντιμετώπισης των σύγχρονων ιών και σκουληκιών, υποχρεώνει κατασκευαστές και χρήστες των Λ/Σ να ενδιαφέρονται πλέον περισσότερο για μια ουσιαστική ενίσχυση των ιδίων, αλλά και των εγγενών μηχανισμών προστασίας που αυτά προσφέρουν, με σκοπό τον ευρύτερο περιορισμό της δραστηριότητας του οπλολογισμικού.

4.2.1 Εγγενείς πολιτικές ασφάλειας

Τα περισσότερα Λ/Σ παρέχουν την απαραίτητη προστασία από τις απειλές του κακόβουλου λογισμικού βασιζόμενα σε εσωτερικούς μηχανισμούς σχεδιασμένους για να παρέχουν υπηρεσίες ασφάλειας.

- Τα *συστήματα αυθεντικοποίησης, εξουσιοδότησης και υπευθυνότητας (ΑΑΑ)* αποτελούν τη ραχοκοκκαλιά της εγγενούς προστασίας των Λ/Σ.
- Κάθε φυσικός χρήστης ή διεργασία ενός Λ/Σ και κάθε εγκεκριμένο, συναλλασσόμενο με αυτό μηχάνημα διαθέτουν *μοναδικό συνδυασμό ονόματος/αναγνωριστικού και (κρυπτογραφημένου) κωδικού ασφάλειας*, μέσω του οποίου αυθεντικοποιούνται στο σύστημα, ενώ ο κάθε τέτοιος λογαριασμός αναλαμβάνει συγκεκριμένο ρόλο με δικαιώματα, δεδομένα και ανυπέρβλητα, δημιουργώντας έτσι κάποια επίπεδα ασφάλειας για την εξουσιοδοτημένη και υπεύθυνη πρόσβαση στις πληροφορίες και τις λειτουργίες του συστήματος.[398] Στην πλέον εκλεπτυσμένη του μορφή, στα σύγχρονα Λ/Σ, ο παραπάνω μηχανισμός λειτουργεί σύμφωνα με τις επιταγές του εγνωσμένου μοντέλου RBAC (Role-Based Access Control).

---

[396] Για την νεωτεριστική αυτή αντιμετώπιση στην ασφάλεια πληροφοριών θα μιλήσουμε πιο αναλυτικά και στο εδάφιο 5.2.5 του πέμπτου κεφαλαίου.

[397] Όπως είδαμε χαρακτηριστικά στο Κεφάλαιο 3 και θα επισημάνουμε πολύ περισσότερο στο πέμπτο μέρος της εργασίας.

[398] Πηγή: "Authorization Manager and Role-Based Administration in Windows Server 2003", Deb Shinder, 2005, διαθέσιμο από το δεσμό http://www.windowsecurity.com/articles/Authorization_Manager_Role_Based_Administration_Windows_Server_2003_Part1.html.

- Τα *ενσωματωμένα συστήματα καταγραφής συμβάντων (audit logging/event logging/system logging)* αποτελούν δικλείδες ασφάλειας[399], καθώς αποτυπώνουν κάθε σημαντική μεταβολή και περιστατικό στις συνισταμένες του χώρου εποπτείας και δράσης ενός Λ/Σ, περιέχοντας έτσι χρήσιμες πληροφορίες για τη γενικότερη ασφάλεια ενός συστήματος. Με τη βοήθεια αυτής της καταγραφής μπορεί κάλλιστα να εντοπιστούν σημάδια μια τρέχουσας μόλυνσης και να διακριβωθεί η ιδιαίτερη συμπεριφορά της.
- Οι εμφανώς συσχετισμένοι μηχανισμοί μη αποποίησης (binding) και υπευθυνότητας (accountability) συνεργάζονται άμεσα με τα 2 παραπάνω συστήματα, με σκοπό όπου είναι εφικτό να μετατρέψουν την *κάθε, μοναδιαία πράξη εντός του Λ/Σ σε καταγεγραμμένη, αναγνωρίσιμη ενέργεια συγκεκριμένου λογαριασμού χρήσης*, που δεν οφείλεται σε τυχαία απόφαση, αλλά σε σκοπιμότητα.
- Το ιδιαίτερο σύστημα αρχείων του κάθε Λ/Σ εκμεταλλεύεται τους παραπάνω μηχανισμούς ΑΑΑ, για να αποδώσει βασισμένα σε ρόλους δικαιώματα (με τη μορφή λιστών ελέγχου πρόσβασης ή ACLs) ανάγνωσης, εγγραφής, εκτέλεσης, διαγραφής κ.ά. στα διάφορα αρχεία δεδομένων, προφυλάσσοντας τα έτσι από ακατάλληλη χρήση.[400] Τα βασισμένα στο UNIX π.χ. Λ/Σ φημίζονται και διακρίνονται για την ικανότητά τους να παρέχουν *ραφιναρισμένη, ελεγχόμενη πρόσβαση στα αρχεία δεδομένων*, μέσω του ιδιαίτερου συστήματος αρχείων και των δικαιωμάτων που αυτό παρέχει στους χρήστες.

4.2.2 Ενδυνάμωση Λ/Σ

Η ενδυνάμωση των Λ/Σ είναι σημαντική διαδικασία, καθώς ένας μεγάλος αριθμός συστημάτων έρχονται εκ κατασκευής παραμετροποιημένα με το βλέμμα στραμμένο περισσότερο στην ευχρηστία και μετά στην ασφάλεια. Η *διαδικασία ενδυνάμωσης (OS hardening) είναι μια διαρκής προσπάθεια* -περαιτέρω της εγγενούς- *θωράκισης* των Λ/Σ των υπολογιστικών κόμβων *μέσω συνδυασμένης δράσης και συνέργειας χρηστών, διαχειριστών και εταιρειών κατασκευής* και επιτυγχάνεται, στην ουσία, με 5 κυρίως τρόπους:

---

[399] Πηγή: "The Importance of Audit Logs", George Spafford, 2006, διαθέσιμο από το δεσμό http://itmanagement.earthweb.com/columns/article.php/3578916.

[400] Πηγή: Διαδίκτυο, ιστοχώρος της online εγκυκλοπαίδειας WikiPedia, α)http://en.wikipedia.org/wiki/Access_control_list#File_system_ACLs, β)http://en.wikipedia.org/wiki/File_system_permissions.

1. Εφαρμόζοντας την *αρχή του μινιμαλισμού (minimalism)*.[401] Η αποφυγή ύπαρξης περίσσειας από πλευράς αναγκαιότητας στις υπάρχουσες πληροφορίες και στις παρεχόμενες υπηρεσίες και εφαρμογές ενός Λ/Σ μπορεί να προστατεύσει από μια μόλυνση ή υπονόμευση. Είναι συχνά διαπιστωμένο πως όσο περισσότερες είναι οι διαθέσιμες πληροφορίες, υπηρεσίες και εφαρμογές (γενικού χαρακτήρα), τόσο μεγαλύτερη είναι η πιθανότητα ύπαρξης τεχνικών και μη ευπαθειών στους κόλπους αυτών, που θα μπορούσε να εκμεταλλευτεί για τη διάδοσή του το κακόβουλο, αυτοαναπαραγόμενο λογισμικό. Η υπερβολή στις παρεχόμενες υπηρεσίες και εφαρμογές θα επιφέρει αναπόφευκτα μια αύξηση των κρουσμάτων και της προσιτότητας από μεριάς των κυβερνοόπλων. Το Λ/Σ πρέπει, λοιπόν, να παρέχει στους χρήστες ιδανικά μονάχα εκείνα τα συστατικά, που διατελούν σε αναλογία με τις εκάστοτε ανάγκες και τη λειτουργικότητα (τον ειδικό χαρακτήρα) της σφαίρας του ΠΣ που εξυπηρετεί, και όχι παραπανίσια ή/και αχρείαστα και μάλιστα με τρόπο που δε διατυμπανίζει απροκάλυπτα τις παρεχόμενες διεπαφές. Στην ίδια λογική και σε παρόμοιο πνεύμα, βρίσκεται και η *αρχή των ελαχίστων δικαιωμάτων χρήσης/προσπέλασης (least privilege)*[402]· οι ενεργούσες πάνω στο ΠΣ οντότητες δε θα πρέπει να διαθέτουν περισσότερα δικαιώματα από όσα χρειάζονται, για να πραγματοποιούν τις επιθυμητές και εγκεκριμένες, χρήσιμες δραστηριότητές τους.

   Η εφαρμογή της εν λόγω αρχής μπορεί να γίνει με σκόπιμη αφαίρεση ή διακοπή εκείνων των διαθέσιμων υπηρεσιών και εφαρμογών των Λ/Σ από την ύπαρξη των οποίων δεν εξαρτάται άμεσα η επιθυμητή λειτουργία του υπερκείμενου ΠΣ και από την απουσία των οποίων δεν επηρεάζονται αρνητικά οι στρατηγικοί στόχοι αυτού.

2. Σχεδιάζοντας και επιβάλλοντας συγκεκριμένες πολιτικές ασφάλειας (π.χ. παρακολούθηση, καταγραφή, περιορισμοί πρόσβασης κ.ά.) με βάση το εκάστοτε περιβάλλον και τις ανάγκες του ΠΣ[403], που ενδιαφέρει. Η *επιβολή πολιτικών ειδικού χαρακτήρα* εγγυάται την παροχή της κατάλληλης, απαραίτητης προστασίας για την κάθε περίπτωση, ανάλογα με την εκάστοτε παραμετροποίηση (αριθμός χρηστών, ανάγκες διαθεσιμότητας, κρισιμότητα δεδομένων), τις υπηρεσίες που επιτελούνται και τις απειλές που αναμένονται να εκδηλωθούν και των οποίων επιθυμείται η

---

[401] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM].

[402] Πηγή: Διαδίκτυο, ιστοχώρος της online εγκυκλοπαίδειας WikiPedia, http://en.wikipedia.org/wiki/Principle_of_least_privilege.

[403] Η παροχή «κουστουμαρισμένων» (customized) ή κατ' απαίτηση λύσεων στα Λ/Σ, σε συνδυασμό με τη δυνατότητα για εύκολη και εκτεταμένη παραμετροποίησή τους, είναι μοναδικής αξίας. Ο κάθε οργανισμός ανάλογα με τους στρατηγικούς του στόχους και με τις εκάστοτε, περιβαλλοντικές συνθήκες έχει και διαφορετικές ανάγκες λειτουργικότητας και ασφάλειας, με ευαίσθητη, μεταξύ τους, ισορροπία και χρονική εξάρτηση. Τα Λ/Σ πρέπει να ενδυναμώνονται έτσι, ώστε να αντανακλούν και να εξυπηρετούν αυτές τις απαιτήσεις.

αναστολή δράσης. Τα Λ/Σ μπορούν να σχεδιαστούν με τέτοιο τρόπο, ώστε να παρέχουν *μεγάλο βαθμό εναλλακτικών επιλογών και ευελιξίας, με τις επιβαλλόμενες πολιτικές ασφάλειας να είναι ικανώς παραμετροποιήσιμες από τους διαχειριστές, ώστε να αντανακλούν την όποια, επιχειρησιακή λογική* στα πλαίσια ενός ΠΣ και των γεγονότων που λαμβάνουν χώρα στη σφαίρα επιρροής του και γενικότερα στο περιβάλλον του.

3. Ενσωματώνοντας εκ κατασκευής και φιλοσοφίας σχεδιασμού *λειτουργίες αναβάθμισης και «υποστήριξης» του παρεχόμενου λογισμικού*. Οι μηχανισμοί διόρθωσης ατελειών, σφαλμάτων και κενών ασφάλειας (που συζητώνται παρακάτω και ως γενικότερες αρχές κατασκευής ασφαλούς λογισμικού[404]) έχουν τη δυναμική να προλαμβάνουν και να αποτρέπουν εκδηλώσεις ιών και σκουληκιών, που εκμεταλλεύονται την ύπαρξη των όποιων αδυναμιών, παραλείψεων ή σχεδιαστικών λαθών στο Λ/Σ, για να επιτύχουν τη διάδοσή τους. Οι χρήστες και διαχειριστές των συστημάτων είναι αντίστοιχα υπεύθυνοι για την τήρηση τακτής και αδιάκοπης πολιτικής εγκατάστασης των απαραίτητων ενημερώσεων και αναθεωρήσεων.

4. Παρέχοντας *δυνατότητες για (σκιώδη ή εμφανή) λήψη αντιγράφων ασφάλειας των κρίσιμων δεδομένων και των συστατικών τους μερών*[405], ώστε να είναι εύκολη και εφικτή, στην περίπτωση που θα χρειαστεί, η επιστροφή του συστήματος σε μια, πρότερη μιας μόλυνσης ή υπονόμευσης, «καθαρή» κατάσταση.

5. Ακολουθώντας *συνεπή πολιτική στην κατασκευή, διάθεση και εγκατάσταση νέων εκδόσεων*, που θα αντιμετωπίζουν συγκεντρωτικά τις επικρατούσες εκδηλώσεις κακόβουλου λογισμικού καθορίζοντας παράλληλα κατά το δυνατόν ένα εντελώς καινούριο, αρχικά ξένο περιβάλλον για το λογισμικό αυτό και για τους συγγραφείς του. Μια τέτοια δράση μπορεί να περιορίσει αποτελεσματικά τις ευκαιρίες εξάπλωσης για τους ιούς και τα σκουλήκια, που θα πρέπει εκ των πραγμάτων να παρακολουθούν από κοντά τις εξελίξεις και τις όποιες αλλαγές στα Λ/Σ και να προσαρμόζονται σε αυτές, αν θέλουν να συνεχίζουν να διαδίδονται.

---

[404] Στο σχετικό εδάφιο 4.5.

[405] Η σημασία του backup των δεδομένων, της παραμετροποίησης, αλλά ακόμη-ακόμη και τις ίδιας της τρέχουσας κατάστασης (state) των συστημάτων, αποδεικνύεται ολοένα και πιο σημαντική στο περιβάλλον των πληροφοριακών εχθροπραξιών. Οι προκύπτουσες δυνατότητες ανάκτησης απωλεσθέντων στοιχείων ή/και επαναφοράς σε μια επιθυμητή, πρότερη κατάσταση αποτελούν πολύτιμη βοήθεια στον αγώνα επιβίωσης των ΠΣ. Έτσι, οι κατασκευαστές των Λ/Σ οφείλουν να ενσωματώνουν τέτοιες λειτουργίες και οι χρήστες να σχεδιάζουν, εφαρμόζουν και ακολουθούν διαδικασίες σχετικής διαχείρισης.

4.2.3 Ισχυρά Λ/Σ

Τα ισχυρά Λ/Σ προχωρούν ένα βήμα παραπάνω, καθώς δεν παρέχουν απλά κάποια εχέγγυα περιορισμού ή εντοπισμού μιας κακόβουλης δραστηριότητας, αλλά *προχωρούν σε πιο προηγμένες μεθόδους αποτροπής* μιας τέτοιας απειλής, *ενσωματώνοντας κατάλληλους μηχανισμούς* (ειδικά σχεδιασμένες ρουτίνες πυρήνα και διεπαφές εφαρμογών) και *εκμεταλλευόμενα την παρουσία υποδομών ασφαλούς επεξεργασίας και αρχιτεκτονικής υλικού*[406], ώστε να:[407]

- αναγνωρίζουν δυναμικά εν εξελίξει κακόβουλο ή μη αναμενόμενο κώδικα και αναστέλλουν την εκτέλεσή του ή/και διορθώνουν τα κακώς κείμενα σε αυτόν και να
- διαχωρίζουν, απομονώνουν και θωρακίζουν επαρκώς το χώρο δράσης του χρήστη (user-space) από το χώρο δράσης του πυρήνα του Λ/Σ (kernel-space) και αντίστροφα, ενώ παράλληλα προστατεύουν με αποτελεσματικότητα και από μη εξουσιοδοτημένες «μεταναστεύσεις» ή τροποποιήσεις κώδικα στην κύρια μνήμη (π.χ. με αυστηρά ελεγχόμενο Kernel Patching και Inter-Process Communication).

Ενδεικτικά παραδείγματα τέτοιων μηχανισμών, που επιτελούν τον πρώτο στόχο, αποτελούν τα συστήματα DEP (Data Execution Prevention) και PatchGuard (Kernel Patch Protection) της Microsoft[408], που ενσωματώνονται ήδη ή θα ενσωματωθούν σε προϊόντα Λ/Σ της εταιρείας.

Ο δεύτερος στόχος είναι σαφώς πιο φιλόδοξος από τον πρώτο και σημαντικά πιο δύσκολα επιτεύξιμος. Η διαχείριση της κύριας μνήμης εξακολουθεί να γίνεται σήμερα με τρόπο που δεν εξασφαλίζει 100% αποτροπή υπονόμευσης (απουσία ίσως και του κατάλληλου, ασφαλούς πλαισίου επεξεργασίας και ευρύτερου, αξιόπιστου σχεδιασμού του hardware[409]) από κακόβουλο κώδικα και μάλιστα, στην περίπτωση που η υπονόμευση αυτή πραγματοποιηθεί, τα πιθανά προβλήματα που ελλοχεύουν είναι μεγάλης δυναμικότητας. Περισσότερα για το θέμα αυτό θα δούμε και στο Κεφάλαιο 5.

---

[406] Σαν αυτές που συζητώνται μετέπειτα στο εδάφιο 4.3.

[407] Πηγή: Διαδίκτυο, ιστοχώρος της online εγκυκλοπαίδειας WikiPedia, http://en.wikipedia.org/wiki/Computer_security#Secure_operating_systems.

[408] Μπορεί κανείς να ενημερωθεί περισσότερο μέσω του ιστοχώρου της Microsoft και του σχετικού δεσμού http://www.microsoft.com/servers/64bit/x64/benefits.mspx.

[409] Όπως περιγράφεται στο αμέσως επόμενο εδάφιο 4.3.

4.2.4 Πλουραλισμός Λ/Σ / Χρήση εναλλακτικών από τις επικρατούσες τάσεις

Στη βιολογία, όταν όλα τα μέλη ενός είδους είναι πανομοιότυπα (σε γονότυπο και φαινότυπο) αυτό αποτελεί ενδεχόμενη θανάσιμη απειλή για το είδος, καθώς μια συγκεκριμένη νόσος μπορεί να το εξαλείψει ολοκληρωτικά.[410] Με παρόμοιο τρόπο και η καθολική αποδοχή και χρήση ενός συγκεκριμένου τύπου ή οικογένειας Λ/Σ (π.χ. MS Windows, UNIX, Linux, BSD) μπορεί να αποτελέσει εξίσου επικίνδυνη πρακτική, καθώς ιοί και σκουλήκια θα μπορούσαν να μολύνουν πιο αποδοτικά και αποτελεσματικά τα διάφορα δικτυοκεντρικά ΠΣ, αν αυτά βασιστούν σε μεγάλο βαθμό στην ίδια υποδομή Λ/Σ.[411]

Η *χρησιμοποίηση διαφορετικών μεταξύ τους Λ/Σ*, έτσι και αλλιώς, εγγυάται μια ισχυρή παρεμπόδιση στη διάδοση και εξάπλωση μιας κακόβουλης υπονόμευσης, καθώς το φράγμα που θέτει η σχεδίαση του καθενός Λ/Σ είναι σημαντικά μεγάλο, για να μπορεί εύκολα ένα συγκεκριμένο είδος κακόβουλου, αυτοαναπαραγόμενου λογισμικού να το υπερπηδήσει κατά τη διάρκεια μιας επίθεσης. Από την άλλη, η καθιέρωση μιας συγκεκριμένης κουλτούρας στο Λ/Σ σημαίνει ταυτόχρονα και μια αντίστοιχη στοχοθέτηση από την πλειοψηφία των κακόβουλων συγγραφέων και δραστών,[412] με αποτέλεσμα η χρήση εναλλακτικών Λ/Σ να προστατεύει από το μεγάλο αυτό ποσοστό των εκάστοτε τρεχουσών απειλών για την επικρατούσα μορφή Λ/Σ (π.χ. MS Windows - Linux). Τέλος, η *αποφυγή της μονολιθικότητας, των μονοπωλίων και των μονοκαλλιεργειών (monocultures)*[413], που αποτελούν έναν τόσο ισχυρό παράγοντα όξυνσης για τις περισσότερες παθογένειες, μπορεί να επιτευχθεί και από μια συνεχή διαδικασία αναβάθμισης του κάθε ιδιαίτερου είδους Λ/Σ (π.χ. ενημερώσεις ασφάλειας, διορθώσεις bugs, νέες εκδόσεις), ώστε τα νέα χαρακτηριστικά να καθιστούν άχρηστες τις παλαιότερες, δοκιμασμένες κακόβουλες απειλές και να διαφοροποιούν ουσιαστικά το Λ/Σ, σε βαθμό που ένας κακόβουλος συγγραφέας ή δράστης να πρέπει να δαπανήσει εκ νέου πόρους για την κατασκευή και χρήση νέων απειλών για αυτό[414].

---

[410] Πηγή: "Warning: Microsoft 'Monoculture'", The Associated Press, 2004, διαθέσιμο από το δεσμό http://www.wired.com/politics/security/news/2004/02/62307.

[411] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM].

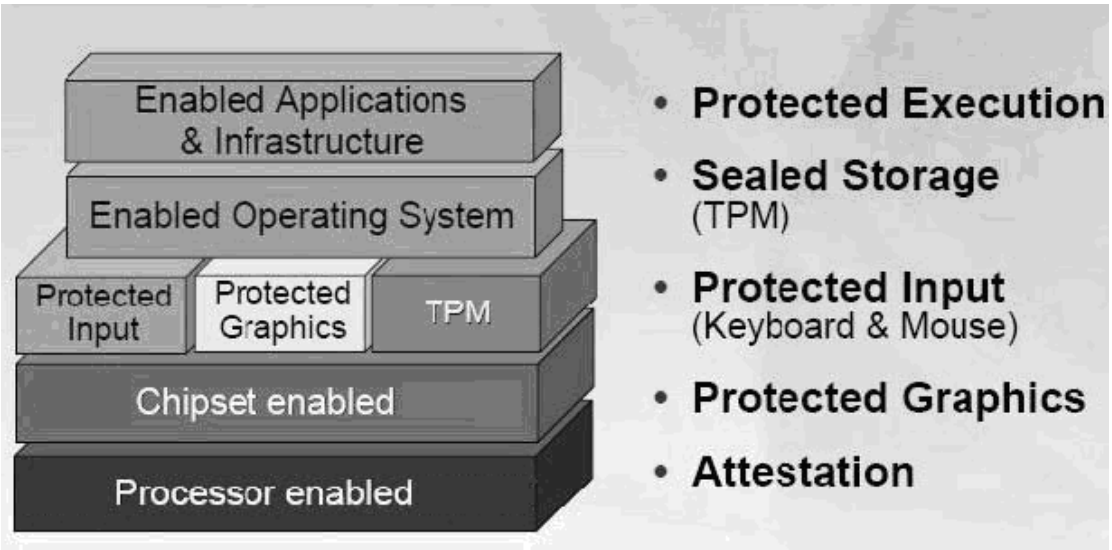
[412] Δεν είναι τυχαίο πως το μεγαλύτερο ποσοστό των σύγχρονων, αναγνωρισμένων κακόβουλων απειλών στρέφεται ενεργά κατά συστημάτων που κάνουν χρήση λογισμικού της Microsoft, που διατηρεί τα ηνία στο χώρο των Λ/Σ, τουλάχιστον όσον αφορά τους βασικούς και απλούστερους, υπολογιστικούς κόμβους.

[413] Κύρια, βιβλιογραφική αναφορά: [WEAVER_PAXSON-TCW].

[414] Στην ουσία, μια αναβαθμισμένη έκδοση του ίδιου είδους Λ/Σ (ίδια οικογένεια) μπορεί, από πλευράς κακόβουλης μολυσματικότητας, να μη διαφέρει ποιοτικά (μικρότερη αποτελεσματικότητα-αποτυχία) από τη χρήση κάποιου εντελώς διαφορετικού Λ/Σ (άλλης οικογένειας).

4.3 Αρχιτεκτονική έμπιστου υλικού - Πλατφόρμες ασφαλούς επεξεργασίας

Η επιστράτευση του υλικού των υπολογιστικών συστημάτων (system(s)-on-chip(s), SoC)[415] στην ευρύτερη προσπάθεια θωράκισης μπορεί να αποδειχθεί στην πράξη ιδιαίτερα επωφελής. *Το υλικό ενός Η/Υ δύναται να αποτελέσει ιδανική «κρυψώνα» για πάσης φύσεως μυστικά που είναι ευκολότερα ανιχνεύσιμα όντας εντός λογισμικού, ενώ παρέχει συνάμα μεγαλύτερη ανθεκτικότητα από παραποίηση (tamper-resistance)*. Τέλος, χάρη σε υλικού τύπου λύσεις ασφάλειας επιτυγχάνεται με άμεσο τρόπο ένας μεγαλύτερος βαθμός αξιόπιστης προστασίας από τη φόρτωση στην κύρια μνήμη ανεπιθύμητων (συμπεριλαμβανομένου των κακόβουλων) εντολών/λειτουργιών ή/και την εκτέλεση τους από μέρους των επεξεργαστικών μονάδων που γίνονται καθ' οδηγία των διαφόρων Λ/Σ των πληροφοριακών κόμβων.



Σχήμα 23: Σκιαγράφηση της δομής μιας ασφαλούς υπολογιστικής μονάδας

4.3.1 Επεξεργαστής και Κύρια Μνήμη

Πρέπει να λαμβάνουμε υπόψιν μας πως το σημερινό σχέδιο μικροεπεξεργαστή για Η/Υ κρατά από τη δεκαετία του '80. Εκείνη την περίοδο, αυτοί οι μικροεπεξεργαστές σχεδιάστηκαν για να κάνουν την εργασία τους παρά τους όποιους έμφυτους περιορισμούς στην αρχιτεκτονική του υλικού τους. Αυτό το σχέδιο υλικού ήταν αρκετά διαφορετικό από αυτό που χρησιμοποιήθηκε για τους μινικομπιούτερς ή τα μεϊνφρέιμς

[415] Που αποτελεί την «καρδιά» κάθε ΠΣ.

(minicomputrers/mainframes, παλαιότερες του PC γενιές αρχιτεκτονικής υπολογιστών). Παραδείγματος χάριν, η προστατευμένη εκτέλεση υπήρξε για χρόνια ένα κλασικό μοτίβο στην πληροφορική, καθώς αποτρέπει επιθέσεις τύπου DoS (μέσω υπονομεύσεων της στοίβας ή άλλων υπερχειλίσεων καταχωρητών) και όχι μόνο από το να είναι επιτυχείς. Μολαταύτα οι αρχικές γενιές μικροεπεξεργαστών για λόγους αποτελεσματικότερης λειτουργίας δεν την ενσωμάτωναν σε ικανοποιητικό βαθμό. Σήμερα, καλούμαστε να επαναφέρουμε τα οφέλη ενός πλήρως λειτουργικού και αρκούντως προστατευτικού αρχιτεκτονικού σχεδίου υλικού για τη μονάδα (διαχείρισης) μνήμης και τη μονάδα επεξεργασίας του προσωπικού Η/Υ, που είναι άλλωστε και ο κύριος δομικός λίθος της πλειοψηφίας των δικτυοκεντρικών ΠΣ.

Οι προσεγγίσεις προς μια ασφαλέστερη εκδοχή των μονάδων επεξεργασίας και κύριας μνήμης ποικίλλουν κατέχουν όμως κάποιες κοινές ιδιότητες μέσα από τις οποίες επιδιώκουν την ισχυροποίηση. Το υλικό πρέπει να είναι έτσι σχεδιασμένο, ώστε το υπερκείμενο Λ/Σ, εφόσον παραμετροποιηθεί καταλλήλως να υποστηρίζεται από τους ακόλουθους -κατά κύριο λόγο και γενική ομολογία υπέρτατης αξίας- μηχανισμούς:

1. *Ύπαρξη κάποιου «θησαυροφυλακίου» προστασίας*[416], και προτεραιότητας για τον πυρήνα του Λ/Σ και τις κρίσιμες εφαρμογές. Οι υπόλοιπες εφαρμογές της ακτίνας δράσης του χρήστη (user-land) τοποθετούνται σε χώρους πάντα ελεγχόμενης μα ευκολότερης, δημόσιας ή/και κοινής διάθεσης/πρόσβασης.
2. *Επαρκής διαχωρισμός και απομόνωση (isolation) των διεργασιών και των σελίδων* (ελαχιστοποίηση αλληλεπικαλυπτόμενων μερών).
3. *Αποτροπή μη εξουσιοδοτημένης πρόσβασης* (ανάγνωση, τροποποίηση) *στα δεδομένα (data segment) και τον κώδικα (code segment) ξένων διεργασιών* στην κύρια μνήμη με τη βοήθεια π.χ. HW κρυπτογραφίας[417] – μόνο κατόπιν επιτυχημένης AAA διαδικασίας διαπίστευσης να επιτρέπονται τέτοιες ενέργειες. Η διεπικοινωνία μεταξύ διεργασιών (IPC)[418] πρέπει να γίνεται σε βάσεις που να εξασφαλίζουν την εμπιστευτικότητα και την ακεραιότητα της περιοχής μνήμης της κάθε εμπλεκόμενης διεργασίας.

   (Τα 2,3 αναφέρονται και ως δημιουργία διαμερισμάτων (compartment implementation[419]), ενώ οι *διακριτές περιοχές της μνήμης που παρέχουν ανοσία στις αναρμόδιες παρατηρήσεις και μεταβολές καλούνται διαμερίσματα (compartments)*.)

---

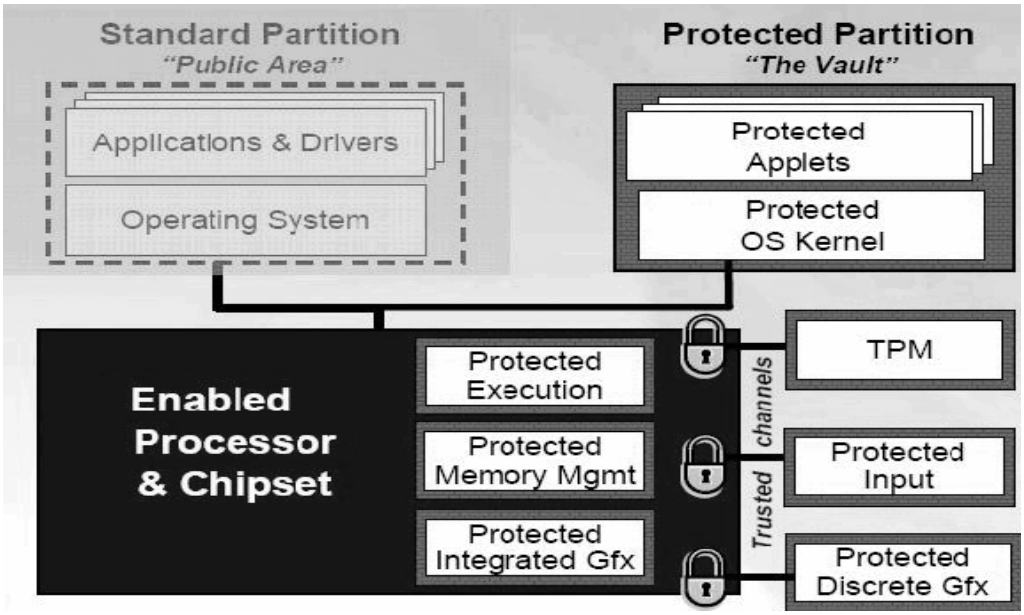
[416] Κύρια, βιβλιογραφική αναφορά: [KOEHLER-TCTP].

[417] Λόγου χάριν με τη βοήθεια των ειδικά για αυτό το σκοπό σχεδιασμένων TPM τσιπς, που θα δούμε πιο κάτω (4.3.2).

[418] Κύρια, βιβλιογραφική αναφορά: [ISG-CCTC].

[419] Κύρια, βιβλιογραφική αναφορά: [LIE-IUOSTH].

4. *Αισθητός και καλοσχεδιασμένος διαχωρισμός των 2 διακριτών τμημάτων κώδικα και δεδομένων* κάθε προγράμματος μεταξύ τους.[420]
5. *Αποτροπή εκτέλεσης δεδομένων ή εκτελέσιμου κώδικα*, που δε φέρουν κάποια κατάλληλη σήμανση (π.χ. executable bits ή tags) ή/και άλλη εξουσιοδότηση.[421]
6. *Αποφυγή των DMA προσβάσεων* συσκευών υλικού στη φυσική μνήμη, χωρίς την παρεμβολή εξειδικευμένων, ολοκληρωμένων συστημάτων διαχείρισης και προστασίας της μνήμης[422].



Σχήμα 24: Μοντέλο Ασφαλούς Επεξεργασίας

Η δυναμική που προκύπτει από μια ασφαλέστερη διαχείριση της μνήμης, αλλά και της ίδιας της επεξεργασίας των δεδομένων, είναι πράγματι τεράστια, ιδιαίτερα αν την εξετάσουμε από τη σκοπιά της προστασίας από κακόβουλες απειλές. Δεν είναι μόνο η αποφυγή επιθέσεων άρνησης υπηρεσίας είναι σύσσωμη η αντιμετώπιση των κακόβουλων/αναρμόδιων ή μη επιθυμητών ενεργειών/λειτουργιών σε μνήμη και επεξεργαστή που «βρίσκεται στο σφυρί» και αυτό είναι κάτι που δεν πρέπει με τίποτε να παραγνωριστεί.

Όπως θα δούμε παρακάτω στο Κεφάλαιο 5, υπάρχουν πάντα κάποιοι περιορισμοί και προβλήματα, αλλά εκ των πραγμάτων η απουσία κάποιας υποδομής -σαν αυτή- ουσιαστικής

[420] Μια τέτοια πρακτική πρόληψης έγκειται στα πλαίσια της συγγραφής ασφαλών προγραμμάτων και εφαρμογών, για αυτό και είναι εξαιρετικής σημασίας να υποστηρίζεται εγγενώς από τα συστήματα επεξεργασίας των ΠΣ.

[421] Κύρια, βιβλιογραφική αναφορά: [GRASSER-SSCSTTDESABOA].

[422] Όπως οι συσκευές IOMMU που περιγράφονται σε ακόλουθο εδάφιο (4.3.3).

επιβεβαίωσης για τις εκτελούμενες διεργασίες συνιστά σχεδόν πάντοτε πηγή κακόβουλων ή άλλων ανεπιθύμητων γεγονότων, πολλές φορές διόλου αμελητέας σοβαρότητας.

Οι παραπάνω αρχιτεκτονικές μακέτες ασφαλών συστημάτων επεξεργασίας και κύριας μνήμης για τους πληροφοριακούς κόμβους έχουν πλέον αρχίσει δειλά να υλοποιούνται και να βελτιστοποιείται η δομή τους, καθώς σήμερα είναι περισσότερο από επιβεβλημένο να προωθηθεί εκτενώς η παραγωγή και χρήση τους. Ήδη έχουν αρχίσει να διαφαίνονται κάποια πρώτα αποτελέσματα από τη χρησιμοποίηση ορισμένων πρωτοτύπων ή πρωτοποριακών προϊόντων (κυρίως από τους 2 μεγάλους εκπροσώπους του χώρου, όπως η Intel και η AMD) και η έρευνα σε πανεπιστημιακό και βιομηχανικό επίπεδο συνεχίζεται με πυρετώδη ρυθμό.

4.3.2 Ειδικές Μονάδες ασφαλούς επεξεργασίας (Trusted Platform Units/Modules)

Η μονάδα ασφαλούς επεξεργασίας TPM είναι *"μια δημοσιευμένη προδιαγραφή για έναν ασφαλή κρυπτοεπεξεργαστή (cryptoprocessor), που μπορεί να αποθηκεύει και να πραγματοποιεί ελέγχους επικύρωσης σε κρίσιμες πληροφορίες, καθώς επίσης και το γενικό όνομα των υλοποιήσεων αυτής της προδιαγραφής, αποκαλούμενων συχνά "TPM τσιπ", "Fritz τσιπ" ή "συσκευή ασφάλειας TPM" (Dell)"*.[423] Η προδιαγραφή TPM αποτελεί εργασία της ομάδας TGC (Trusted Computing Group). Η τρέχουσα έκδοση της προδιαγραφής TPM είναι η 1.2 αναθεώρηση 103 και δημοσιεύτηκε στις 9 Ιουλίου 2007.

Ένα TPM μικροτσίπ είναι ένα κύκλωμα σιλικόνης που προσφέρει τις κατάλληλες υποδομές μεταξύ άλλων για ασφαλή παραγωγή κρυπτογραφικών κλειδιών (RSA Engine), δυνατότητα να περιοριστεί η πρόσβαση και χρήση των κρυπτογραφικών κλειδιών (PCR καταχωρητής), καθώς επίσης και μιας γεννήτρια τυχαίων αριθμών (Random Number Generator) μέσω υλικού.[424] Περιλαμβάνει και προσδίδει επίσης ικανότητες, όπως η απομακρυσμένη επιβεβαίωση (remote attestation), η δέσμευση (binding) και η σφραγισμένη αποθήκευση (sealed storage on NV-Storage)[425].

Οι κύριες λειτουργίες/ευθύνες του TPM είναι:[426]

- Τήρηση μυστικότητας για πληροφορίες όπως π.χ. κωδικοί πρόσβασης και κλειδιά και προστασία τους από την ευρύτερη επιρροή των επιθέσεων μέσω ή εναντίον λογισμικού.

---

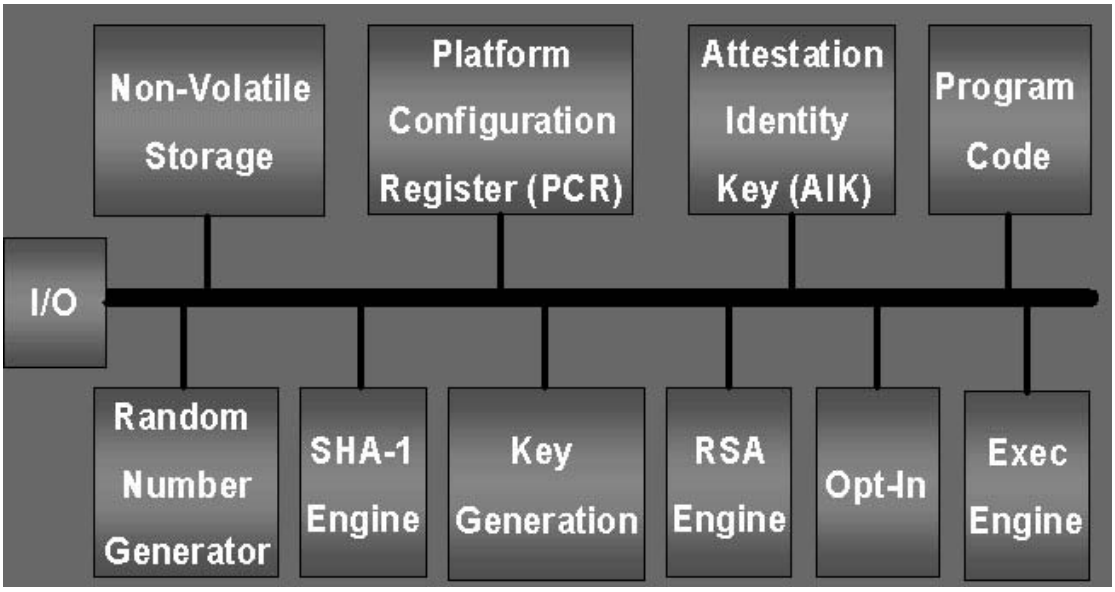
[423] Πηγή: Διαδίκτυο, ιστοχώρος της online εγκυκλοπαίδειας WikiPedia, http://en.wikipedia.org/wiki/Trusted_Platform_Module.

[424] Κύρια, βιβλιογραφική αναφορά: [NILSSON-TPMHbS].

[425] Κύρια, βιβλιογραφική αναφορά: [ISG-CCTC].

[426] Κύρια, βιβλιογραφική αναφορά: [KOEHLER-TCTP].

- Παραγωγή κλειδιών υψηλής ποιότητας, με χρήση της HW γεννήτριας τυχαίων αριθμών.
- Επεξεργασία ιδιωτικών κλειδιών, μέσα στα όρια της μονάδας.
- Αποθήκευση μετρήσιμων δεδομένων.



Σχήμα 25: Το εσωτερικό ενός TPM αρθρώματος

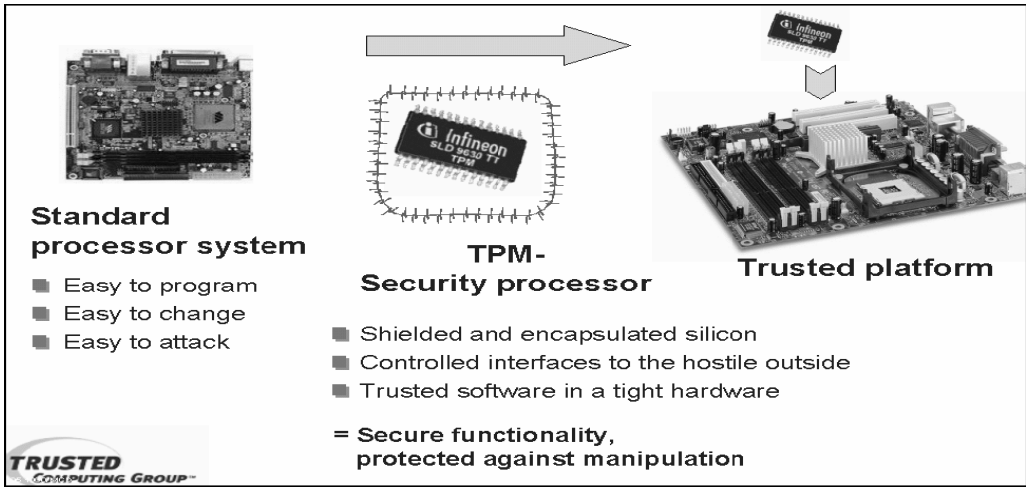
Η *απομακρυσμένη επιβεβαίωση* δημιουργεί μια σχεδόν μη τροποποιήσιμη/παραχαράξιμη τιμή σύνοψης (hash summary value) του υλικού και του λογισμικού ενός Η/Υ. Μέχρι ποιο σημείο το λογισμικό συνοψίζεται, αποφασίζεται από το ίδιο το λογισμικό που κρυπτογραφεί τα δεδομένα. Αυτό επιτρέπει σε κάποιον τρίτο να ελέγξει/επιβεβαιώσει προγραμματιστικά ότι στοιχεία του δείνα λογισμικού (π.χ. του Λ/Σ) δεν έχουν αλλάξει/μεταβληθεί[427]. Η *δέσμευση* κρυπτογραφεί τα δεδομένα χρησιμοποιώντας το κλειδί επικύρωσης του TPM -ένα μοναδικό κλειδί RSA, που «καίγεται» επάνω στο μικροτσίπ κατά τη διάρκεια της παραγωγής του[428]- ή ένα άλλο εμπιστευόμενο κλειδί. Η *σφράγιση*, τέλος, κρυπτογραφεί δεδομένα κατά τέτοιον τρόπο ώστε να μπορούν να αποκρυπτογραφηθούν, μόνο εάν το TPM απελευθερώσει το σωστό κλειδί αποκρυπτογράφησης, το οποίο συμβαίνει μόνο εάν ακριβώς το ίδιο λογισμικό είναι παρόν, όπως όταν κρυπτογραφήθηκαν τα εν λόγω δεδομένα.

[427] Βλέπε και το σχετικό με την επιβεβαίωση εδάφιο 5.2.2 του Κεφαλαίου 5.

[428] Το κλειδί αυτό ονομάζεται στην αγγλική ορολογία της ομάδας TGC endorsement key (EK).

Ένα TPM μπορεί να χρησιμοποιηθεί επίσης για να επικυρώσει συσκευές υλικού[429]. Δεδομένου ότι σε κάθε τσιπ TPM «καίγεται» ένα μοναδικό και μυστικό κλειδί RSA, κατά τη διάρκεια της παραγωγής, ή/και αποθηκεύονται σε αυτό πρόσθετες και συσχετισμένες με το κλειδί αυτό πληροφορίες πρόσβασης (π.χ. ιδιωτικά κλειδιά, ψηφιακές υπογραφές/πιστοποιητικά), είναι σε θέση να επιτελέσει επικύρωση πλατφορμών (μέσω αυτοαναγνώρισης-επιβεβαίωσης, αυθεντικοποίησης-ταυτοποίησης και ελέγχου επιτρεπτότητας). Παραδείγματος χάριν, μπορεί να χρησιμοποιηθεί για αυτοεντοπισμό του τρέχοντος συστήματος (αυτοαναγνώριση) ή για να ελέγξει κανείς ότι το σύστημα που επιδιώκει την πρόσβαση είναι το αναμενόμενο σύστημα (αυθεντικοποίηση) ή ακόμα περισσότερο για να επιβεβαιωθεί/επιτραπεί η δυνατότητα επικοινωνίας μεταξύ συστημάτων (επιτρεπτότητα). Άλλες χρήσεις της TPM τεχνολογίας αφορούν συστήματα κρυπτογράφησης διαμερισμάτων και δίσκων (π.χ. το BitLocker της MS και άλλες λύσεις bulk encryption) ή πιο γενικούς και σύνθετους μηχανισμούς AAA (π.χ. το Linux Enforcer, τα encrypted συστήματα αρχείων κτλ)[430], όπου εξασφαλίζεται πως, εν απουσία του TPM που χρησιμοποιήθηκε κατά την κρυπτογράφηση ή σε περίπτωση αποτυχίας παροχής των κατάλληλων, απαραίτητων, ισχυρών κλειδιών, η πιθανότητα προσπέλασης είναι μηδαμινή.

Το TPM ως επί το πλείστον είναι ένα μεμονωμένο σύστημα που τυπώνεται πάνω στη μητρική κάρτα του Η/Υ και ενώνεται με ειδικούς διαύλους (π.χ. τον FSB) προς το BIOS, τη μνήμη και τη CPU ή/και τα άλλα περιφερειακά συστήματα.



Σχήμα 26: Η διαφορά στην ασφάλεια που κομίζει το TPM

[429] Η τεχνοτροπία αυθεντικοποίησης συσκευών είναι μια ιδιαίτερα καινοτομική τάση στην ασφάλεια συστημάτων και πληροφοριών, που γίνεται αντικείμενο ξεχωριστής αναφοράς στο εδάφιο 5.2.3.

[430] Πηγή: Διαδίκτυο, ιστοχώρος της online εγκυκλοπαίδειας WikiPedia, http://en.wikipedia.org/wiki/Full_disk_encryption.

Συνοψίζοντας, η τεχνολογία TPM είναι μια *αξιόπιστη λύση ασφάλειας που παρέχει ένα αφοσιωμένο, υλικό μέσο κρυπτογράφησης και προστατευμένης αποθήκευσης και επεξεργασίας* κρίσιμων, χαρακτηριστικών πληροφοριών του φέροντος συστήματος με πολλά πρόσθετα οφέλη ασφάλειας και όχι μόνο (μεγάλου μήκους και ισχυρή κρυπτογράφηση, επιτρεπτότητα, αυτοματοποιημένο και ασφαλές single-sign-on). Αν μάλιστα συνδυαστεί με τις προαναφερόμενες και ακόλουθες τεχνικές για τη διασφάλιση των υπολοίπων, συστατικών τμημάτων ενός Η/Υ, μπορεί να αποδώσει εξαιρετικά συνεισφέροντας σε υψηλότατους βαθμούς προστασίας από κακόβουλες ή άλλες εν γένει μη επιθυμητές ενέργειες.

4.3.3 Ειδική μονάδα ασφαλούς διαχείρισης της μνήμης (Input-Output Memory Management Units)

Τα εν λόγω συστήματα είναι συσκευές υλικού (τσιπς) που -σε αναλογία με τις κλασσικές μονάδες διαχείρισης της μνήμης (MMUs)- μεταφράζουν εικονικές διευθύνσεις, απευθείας προσπέλασης της μνήμης (DMA), των συσκευών με τέτοιες δυνατότητες, σε φυσικές διευθύνσεις μνήμης, σε αντίθεση με τα καθιερωμένα συστήματα DMA που βασίζονται και χρησιμοποιούν απευθείας φυσική διευθυνσιοδότηση της μνήμης.[431] Με τον τρόπο αυτό παρέχουν έναν, πιο προσεγμένο από πλευράς ασφάλειας, μηχανισμό σύνδεσης μιας τέτοιας συσκευής με την κύρια μνήμη και τον επεξεργαστή.

Τα IOMMUs εκτελούν πολύτιμες υπηρεσίες ασφάλειας, *αποτρέποντας τις συσκευές «απατεώνων» από την εκτέλεση «παρεξηγίσιμων» ή κακόβουλων, απευθείας προσπελάσεων της μνήμης*, με αυτόν τον τρόπο αυξάνοντας αισθητά την αξιοπιστία και τη διαθεσιμότητα των συστημάτων επεξεργασίας. Χωρίς ένα τέτοιο σύστημα διαχείρισης, μια συσκευή με DMA δυνατότητες θα μπορούσε να προγραμματιστεί για να επικαλύψει/αλλοιώσει οποιοδήποτε μέρος της μνήμης του συστήματος, με καταστροφικά αποτελέσματα[432]. Ένα IOMMU μπορεί να είναι ικανό για *κατάλληλη απομόνωση-προστασία της μνήμης*, καθώς περιορίζει μια τέτοια συσκευή έτσι, ώστε να μπορεί να έχει πρόσβαση μόνο σε περιοχές της μνήμης, όπου της έχουν χορηγηθεί ρητά τα σχετικά δικαιώματα. Τα λειτουργικά συστήματα μπορούν να χρησιμοποιούν τα τσιπς αυτά για να απομονώνουν τους οδηγούς συσκευών

[431] Πηγή: Διαδίκτυο, ιστοχώρος της online εγκυκλοπαίδειας WikiPedia, http://en.wikipedia.org/wiki/IOMMU.

[432] Η απευθείας, προγραμματιστική πρόσβαση στην κύρια μνήμη επιτρέπει μια σειρά από επιθέσεις (άρνηση εξυπηρέτησης, αντικατάσταση, εξαπάτηση) εκ μέρους των κακόβουλων κυβερνοόπλων, για τις οποίες γίνεται ιδιαίτερη μνεία στο εδάφιο 5.1.3 του 5ου κεφαλαίου.

(device drivers)[433], ενώ οι hypervisors[434] για να χορηγούν ασφαλή, άμεση πρόσβαση υλικού στις εικονικές μηχανές, που διαχειρίζονται.

Με την πρόσφατη εισαγωγή από την πλευρά της Intel και της AMD ικανών για απομόνωση IOMMUs σε όλους τους νέους τύπους συστημάτων επεξεργασίας για διακομιστές, τα IOMMUs αναμένεται γίνουν πανταχού παρόν. Προς το παρόν, πάντως, απουσιάζουν και για αρκετό καιρό ακόμη η πλειοψηφία των ΠΣ προβλέπεται πως θα στερείται αναπόφευκτα των πολύτιμων υπηρεσιών τους, μέχρι τουλάχιστον να ωριμάσει κάπως η τεχνολογία που τα ορίζει και διακατέχει.

4.3.4 Περιφερειακές μονάδες

Πάσης φύσεως περιφερειακές του κεντρικού επεξεργαστή και της κύριας μνήμης μονάδες μπορούν να χρησιμεύσουν περαιτέρω στην επίπονη προσπάθεια προστασίας από κακόβουλα προγράμματα, αλλά και γενικότερης ενίσχυσης της ασφάλειας ενός Η/Υ:

1. Έξυπνες κάρτες (Smart cards) ή άλλα «έξυπνα» μέσα (security tokens, smart media) για την αποθήκευση/ανάκτηση/κρυπτογράφηση κρίσιμης πληροφορίας.[435]
2. PCI ή εξωτερικού τύπου υλοποιήσεις κρυπτογραφικών αρθρωμάτων υλικού υπεύθυνων για την ασφάλεια ενός υπολογιστικού κόμβου.[436]
3. Ασφαλείς κάρτες δικτύου (με εξολοκλήρου δικά τους ολοκληρωμένα κυκλώματα κρυπτογράφησης).[437]
4. PCI ή εξωτερικού τύπου συσκευές ανίχνευσης ή «κλειδώματος» μνήμης (π.χ. μέσω DMA) RAM.[438]

---

[433] Οι σύγχρονες επιθέσεις μέσω rootkits βασίζονται εν πολλοίς στην απευθείας εμφύτευση κακόβουλων οδηγών συσκευών στο επίπεδο του πυρήνα. Η απομόνωση αφορά στην προσπάθεια περιορισμού των παρεμβάσεων του κώδικα των οδηγών και των επιπτώσεων (π.χ. kernel crashes) που αυτές έχουν στο νόμιμο κώδικα του πυρήνα. Διαβάζει κανείς σχετικά στην ενδιαφέρουσα παρουσίαση του Hebrew University, που είναι διαθέσιμη από το δεσμό http://httpdyn.cs.huji.ac.il/moodle/file.php?file=/33/osa-seminar.ppt.

[434] Οι hypervisors θα μελετηθούν σε ξεχωριστό εδάφιο (5.2.1) του πέμπτου κεφαλαίου.

[435] Πηγή: Διαδίκτυο, ιστοχώρος της online εγκυκλοπαίδειας WikiPedia, http://en.wikipedia.org/wiki/Security_token.

[436] Πηγή: Διαδίκτυο, ιστοχώρος της online εγκυκλοπαίδειας WikiPedia, http://en.wikipedia.org/wiki/Hardware_Security_Module.

[437] Αντίστοιχες της υλοποίησης από την εταιρεία προϊόντων δικτύωσης 3COM, τα χαρακτηριστικά της οποίας μπορεί κανείς να επιθεωρήσει μέσω της ιστοσελίδας http://www.softchoice.com/catalog/en-us/network-adapters-3com-10100-secure-nic-network-adapter-pci-3CR990B-97-H07713.

[438] Οι συσκευές, για παράδειγμα, που επιτρέπουν διεπαφή μέσω του πρωτοκόλλου επικοινωνίας FireWire, έχουν τη δυνατότητα να παρέχουν απευθείας ανάγνωση (λόγω DMA) και, υπό κατάλληλη παραμετροποίηση, «κλείδωμα» της μνήμης, που μπορούν

5. Εξειδικευμένα μικροτσίπ για την ασφάλεια -μηχανών/επεξεργαστών- πολυμέσων (γραφικών, ήχου, βίντεο).[439]

4.3.5 Πλουραλισμός

Η κατάστρωση, εμπορική διάθεση, επιλογή και χρήση *διαφορετικών αρχιτεκτονικών και λύσεων υλικού (H/W polycultures)* κατά μήκος του σύγχρονου, παγκόσμιου, πληροφοριακού ιστού εγγυάται μια ισορροπημένη αντίσταση, σε απειλές μεγάλης εμβέλειας και αυξημένης, επεκτατικής δυναμικής από πλευράς λογισμικού. Η συγγραφή και δράση κακόβουλου λογισμικού ανεξάρτητου της εκάστοτε αρχιτεκτονικής του υλικού (π.χ. της μάρκας της CPU)[440] είναι ζήτημα με σημαντικές, (οικονομο)τεχνικές δυσκολίες που τις περισσότερες φορές παραμένει απαγορευτικό όνειρο «θερινής νυκτός» για τους επίβουλους κυβερνοκακοποιούς.

Αντιθέτως, η προσκόλληση σε συγκεκριμένες εταιρείες και προϊόντα, ενώ μπορεί σίγουρα να εξυπηρετεί σκοπούς συμβατότητας και αποφυγής πολυπλοκότητας (π.χ. στη συγγραφή επωφελούς λογισμικού), εντούτοις λειτουργεί αρνητικά, γιατί διευκολύνει την αποτελεσματικότερη διάδοση και διείσδυση ιών και σκουληκιών και απαλλάσσει τους κακόβουλους συγγραφείς από όποιο, πρόσθετο κόπο για την ικανοποίηση κάποιων στόχων μόλυνσης πολλαπλών και διαφορετικών αρχιτεκτονικών[441].

4.3.6 Έρευνα και Νέα Τεχνολογία

Η ενίσχυση της ερευνητικής διαδικασίας, για την παραγωγή νέων και ασφαλέστερων αρχιτεκτονικών υλικού και κυρίως όσον αφορά τις μονάδες μνήμης και επεξεργασίας, που αποτελούν τη βασικότερη εξάρτηση για τη συγγραφή κακόβουλων όπλων, πρέπει να αποτελεί βασική προτεραιότητα όλων των εν δυνάμει ενδιαφερόμενων για την προστασία των ΠΣ φορέων. Η συντονισμένη αναβάθμιση σε νέες αρχιτεκτονικές (π.χ. 64-Bit memory,

---

να φανούν ιδιαίτερα χρήσιμες ως λειτουργίες στους αναλυτές και τα συστήματα ασφάλειας. Από την άλλη, μια απευθείας ανάγνωση στη μνήμη μπορεί να εγείρει πολλά προβλήματα λόγω πιθανής υπονόμευσης, πράγμα που θα επισημανθεί και στο τρέχον και στο επόμενο κεφάλαιο.

[439] Κύρια, βιβλιογραφική αναφορά: [XUEMIN-ISMSoC].

[440] Το περιβάλλον επεξεργασίας, όπως έχουμε ξανατονίσει, αποτελεί μέχρι σήμερα φραγμό για την κατασκευή και επέκταση κακόβουλων προγραμμάτων. Η αρχιτεκτονική του υλικού της CPU και της μνήμης χαρακτηρίζει μονοσήμαντα κάθε υπόσταση οπλολογισμικού και προς το παρόν οι «διαρχιτεκτονικές» απειλές και μολύνσεις (cross-platform viral/worm threats) παραμένουν ασήμαντα σπάνιες και θεωρητικής αξίας περιπτώσεις.

[441] Όπως ισχύει αντίστοιχα και στο λογισμικό των πληροφοριακών κόμβων λόγω έλλειψης πλουραλισμού στα Λ/Σ, γεγονός που εξετάσαμε, πιο πριν, στο εδάφιο 4.2.4.

64-Bit CPU, multicore programming) και η πλουραλιστική διασπορά αυτών, με τον τρόπο που αναφέρθηκε στο αμέσως προηγούμενο εδάφιο, μπορεί να εγείρει σημαντικά, τεχνολογικά χάσματα[442] στους κακόβουλους συγγραφείς και δράστες, που σίγουρα θα απαιτήσουν μεγαλύτερη ενασχόληση και κατανάλωση πόρων για την παρασκευή, επαρκώς κατάλληλων για τα νέα δεδομένα, απειλών οπλολογισμικού τύπου. Έτσι, παρέχεται μέσω της ανανεωτικής αυτής διαδικασίας συνολικά ένα χρονικά περιορισμένο, μα ασφαλές περιθώριο για τα ΠΣ να συνέλθουν από τα συνεχή κακόβουλα χτυπήματα και να προετοιμαστούν για τα όποια επόμενα, όσο οι αντίπαλοι ετοιμάζουν τις νέες -προσανατολισμένες στην καινούρια αρχιτεκτονική- τακτικές τους.

4.4 Δίκτυα και πρωτόκολλα δικτυακής επικοινωνίας

Τα δίκτυα, όπως έχουμε ξαναπεί, είναι η *κινητήριος δύναμη της σύγχρονης, πληροφοριακής επανάστασης*[443] και δε θα μπορούσαν παρά να επιτελούν θεμελιώδη ρόλο, τόσο στις δυνατότητες για κακόβουλη δράση, όσο και στην προστασία από αυτή. Χωρίς π.χ. τις ταχύτατες, δικτυακές υποδομές του σήμερα τα άκρως μεταδιδόμενα σκουλήκια θα παρέμεναν επιστημονική φαντασία, ενώ από την άλλη ένας πολύ προσεκτικός σχεδιασμός της εσωτερικής δομής ενός δικτύου πολλές φορές επιβάλλεται για να αντισταθμίζει την εισερχόμενη/εξερχόμενη, πληροφοριακή εχθροπραξία.

Τα πρωτόκολλα επικοινωνίας στα δικτυοκεντρικά συστήματα είναι η τυποποιημένη γλώσσα που ομιλούν οι διάφοροι διασυνδεδεμένοι κόμβοι που επιθυμούν την μεταξύ τους ανταλλαγή δεδομένων ή άλλη μηνυματοδοσία (συναλλαγή). Η γνώση της ιδιαίτερη λειτουργίας αυτών των πρωτοκόλλων ή/και η ενδεχόμενη ύπαρξη κενών ασφάλειας και άλλων τεχνικών αδυναμιών σε αυτά (πράγμα πολύ σύνηθες τα πρώτα χρόνια του Internet) μπορεί υπό προϋποθέσεις να δημιουργεί τις κατάλληλες ευκαιρίες υπονόμευσης των ομιλούντων συστημάτων για τις κακόβουλες οντότητες. Έτσι, σήμερα βάρος δίνεται και σε προσπάθειες μετριασμού του κινδύνου αυτού.

4.4.1 Ασφαλή πρωτόκολλα

Όταν το Internet και η δικτύωση του πρωτοέλαβαν χώρα, η ασφάλεια δεν ήταν πρώτη προτεραιότητα, πέραν ίσως από κάποιες φροντίδες για την αποφυγή επιθέσεων άρνησης

[442] Δυστυχώς βέβαια πάντα θα υπάρχουν κάποιοι που θα τα βλέπουν ως πνευματικές προκλήσεις.

[443] Βλέπε σχετικά εδάφια 2.1 και 2.3 του δεύτερου κεφαλαίου.

εξυπηρέτησης. Με τον καιρό, η δημιουργία και ύπαρξη πολλαπλών συμφερόντων και η είσοδος κρίσιμων και ευαίσθητων πληροφοριών (οικονομοτεχνική εξέλιξη), σε συνδυασμό με την εμφάνιση των πρώτων κρουσμάτων κακόβουλων απειλών και επιθέσεων, κατέστησε σαφές πως μια νέα προσέγγιση, με γνώμονα την ασφάλεια των επικοινωνιών, ήταν αναγκαία.

Στον κόσμο των δικτυοκεντρικών συστημάτων, η επικοινωνία έχει δομηθεί εξαρχής και βασίζεται εξολοκλήρου στα λεγόμενα πρωτόκολλα[444] (τη γλώσσα δηλαδή που χρησιμοποιούν δύο ομότιμες οντότητες του δικτύου για να συνεννοηθούν μεταξύ τους), άρα η ασφάλεια της εξαρτάται και περνά απαραίτητα μέσα από αυτά. Σήμερα, το ζήτημα αυτό αντιμετωπίζεται από 2 διαφορετικές όψεις του:

1. Από τη μία, τα *κρυπτογραφικά πρωτόκολλα ασφάλειας*[445], όπως το SSL, που αποκαλείται στην τελευταία σύγχρονη μορφή του TLS, μαζί με το ειδικό πρωτόκολλο επικοινωνίας SSH, μπορούν να χρησιμοποιηθούν για να ενισχύσουν την ασφάλεια των υπόλοιπων πρωτοκόλλων επικοινωνίας παράγοντας overSSL ή overSSH εκδοχές τους (όπως π.χ. HTTPS, FTPS, SFTP, SCP, SMIME κ.ά.), που είναι σαφώς λιγότερο υπονομεύσιμες.

   Η δράση όλων των εν λόγω πρωτοκόλλων επικεντρώνεται στη χρήση μιας ποικιλίας μεθόδων και μηχανισμών για την αξιόπιστη παροχή κυρίως των παρακάτω υπηρεσιών ασφάλειας:

   - Αυθεντικοποίηση και γενικότερα AAA υπηρεσιών
   - Εμπιστευτικότητα
   - Ακεραιότητα
   - Μη αποποίηση

   Οι τεχνικές που ενσωματώνουν τα εξειδικευμένα πρωτόκολλα ασφάλειας πραγματοποιούν εκτενή χρήση κρυπτογραφικών αλγορίθμων (τόσο με συμμετρικό όσο και με ασύμμετρο τρόπο) και εκμεταλλεύονται την ύπαρξη υποδομών έμπιστων

---

[444] Στους υπολογιστές, ένα πρωτόκολλο είναι η σύμβαση ή τα πρότυπα που περιγράφουν και καθορίζουν τη σύνδεση, την επικοινωνία και τη μεταφορά δεδομένων μεταξύ δύο υπολογιστικών άκρων. Στην απλούστερη μορφή του, ένα πρωτόκολλο μπορεί να οριστεί ως «οι κανόνες που κυβερνούν τη σύνταξη, τη σημασιολογία και το συγχρονισμό της επικοινωνίας». Τα πρωτόκολλα μπορούν να υλοποιούνται και να εφαρμόζονται από το υλικό, το λογισμικό ή από έναν συνδυασμό και των δύο (υλισμικό).

[445] Πηγή: Διαδίκτυο, ιστοχώρος της online εγκυκλοπαίδειας WikiPedia, http://en.wikipedia.org/wiki/Cryptographic_protocol.

τρίτων οντοτήτων (trusted-third-party)[446], για την κατά το δυνατόν καλύτερη υποστήριξη και αποτελεσματικότερη εξυπηρέτηση των ανωτέρω αναφερόμενων υπηρεσιών.

2. Πέρα από τους 2 παραπάνω εγνωσμένους τρόπους ενδυνάμωσης των πρωτοκόλλων επικοινωνίας (που αφορούν κυρίως το στρώμα εφαρμογής του OSI), παρουσιάζεται εδώ και μια δεκαετία περίπου, μια *γενική τάση για αντικατάσταση των παραδοσιακών (δια)δικτυακών πρωτοκόλλων από νέες ασφαλέστερες εκδοχές τους* (καθ' όλο το μήκος της στοίβας της OSI/ISO αρχιτεκτονικής) με την ενσωμάτωση και παροχή μεγάλου πλήθους υπηρεσιών ασφάλειας (ενδεχομένως επιπλέον και των βασικών τριών που αναφέρθηκαν προηγουμένως). Για το λόγο αυτό εκτενής έρευνα διεξάγεται στην κατεύθυνση αυτή, με τους προγραμματιστές και τους οργανισμούς τυποποίησης να προσπαθούν για και να ευελπιστούν σε μια εξαρχής αναθεώρηση, με βάση την ασφάλεια. Ήδη συναντώνται και πολλές φορές έχουν αμέσως τύχει μεγάλης αποδοχής και εφαρμογής οι πρώτοι καρποί αυτής της ευρύτερης δραστηριότητας με τρανότερα παραδείγματα:

- Τα πρωτόκολλα IPsec, DNSsec, που εμπλουτίζουν τις υπηρεσίες και τους ελέγχους ασφάλειας των βασικών αυτών κολώνων της (δια)δικτύωσης.
- Τις αξιόπιστες υποδομές δικτυακής αυθεντικοποίησης οντοτήτων Kerberos και Sesame, που αποτελούν την κορωνίδα προστασίας σε μη ασφαλή περιβάλλοντα επικοινωνίας.
- Το πρωτόκολλο σήραγγας L2TP, που αποτελεί εγγύηση για τις VPN συνδέσεις και επικοινωνίες.
- Τις λύσεις για ασύρματη ασφάλεια της οικογένειας WPA.
- Τις λύσεις αυθεντικοποίησης CHAP, EAP, PEAP.

Όλες οι επιτυχημένες αυτές συνταγές βασίζονται επίσης σε εκτεταμένη χρήση μηχανισμών της κρυπτογραφίας ή/και δικτύων έμπιστων οντοτήτων.

Σε όλα τα νέα αυτά πρωτόκολλα πρώτο μέλημα είναι η ασφάλεια στις επικοινωνίες και σημαντική έμφαση έχει δοθεί ειδικά στην μεγαλύτερη εξασφάλιση προστασίας από

[446] Που πιστοποιούν την αξιοπιστία και αυθεντικότητα ψηφιακών πιστοποιητικών, υπογραφών και άλλων κρυπτογραφημένων, ταυτοτικών στοιχείων, που εξασφαλίζουν την εγκαθίδρυση ασφαλούς προσπέλασης πληροφοριών και ανταλλαγής μηνυμάτων.

κακόβουλες οντότητες και οπλολογισμικό. Η αποδοχή και χρήση λοιπών των λύσεων αυτών στους κόλπους του Internet και των δικτυοκεντρικών ΠΣ έχει την ικανότητα να περιορίζει δραστικά τα περιθώρια εμφάνισης και δράσης κακόβουλων απειλών και να μειώνει τα όποια ενδεχόμενα επιτυχίας τους.

4.4.2 Δράσεις ICANN/IANA/IETF και άλλων καθ' ύλην αρμόδιων, διεθνών οργανισμών

Ευρύτερες ενέργειες από τους *διεθνείς οργανισμούς, που ασχολούνται ειδικά με τη λειτουργία του Διαδικτύου* (κυρίως ICANN/IANA, IETF), είναι διαρκώς αναγκαίες:

- στην πολυαναμενόμενη μετάβαση στη ριζικά μεγαλύτερη ασφάλεια του IPv6,
- στον κρίσιμο τομέα της εύρυθμης και ασφαλούς DNS λειτουργίας με δράσεις όπως αυτή του DNSsec και του προσεκτικού συντονισμού του DNS χώρου διευθύνσεων,
- στην τήρηση και σύννομη δημόσια διάθεση επικαιροποιημένων μητρώων ιδιοκτητών IP διευθύνσεων και στη διαρκή βελτιστοποίηση της διαδικασίας ανάθεσης και παρακολούθησης των IPs από πλευράς ασφάλειας, σε συνεργασία και με τους κατά τόπους παρόχους (ISPs),
- στην ελεγχόμενη ανάθεση νέων θυρών επικοινωνίας,
- στην έγκαιρη επισήμανση ευπαθών πρωτοκόλλων και θυρών επικοινωνίας,
- στην απόσυρση παρωχημένων πρωτοκόλλων και τέλος
- στον τομέα της έρευνας, τυποποίησης και πιστοποίησης της καλής λειτουργίας νέων (και ασφαλέστερων) εναλλακτικών για τη δικτυακή επικοινωνία.

Οι παραπάνω ενέργειες εξασφαλίζουν *μια, σε κεντρικό επίπεδο συντονισμένη, μεγαλύτερη και οικουμενικότερη προστασία* από κακόβουλες δράσεις αποτρέποντας με τον ένα ή τον άλλο τρόπο την εκδήλωση ή εξάπλωσή τους.

4.4.3 Εναλλακτικά δίκτυα δεδομένων (IPX, AppleTalk, DECNET)

Αν και η επικράτηση του TCP/IP μοντέλου θεωρείται πλέον μια αδιαμφισβήτητη πραγματικότητα, παλαιότερα συστήματα και πρωτόκολλα δικτύωσης (επίπεδα δικτύου και μεταφοράς 3,4 του μοντέλου OSI), όπως π.χ. τα Novell IPX/SPX, AppleTalk και DECNET *μπορούν να λειτουργήσουν ως «αντιπλημμυρικά έργα» σε επίπεδο τοπικού δικτύου* (LAN)·

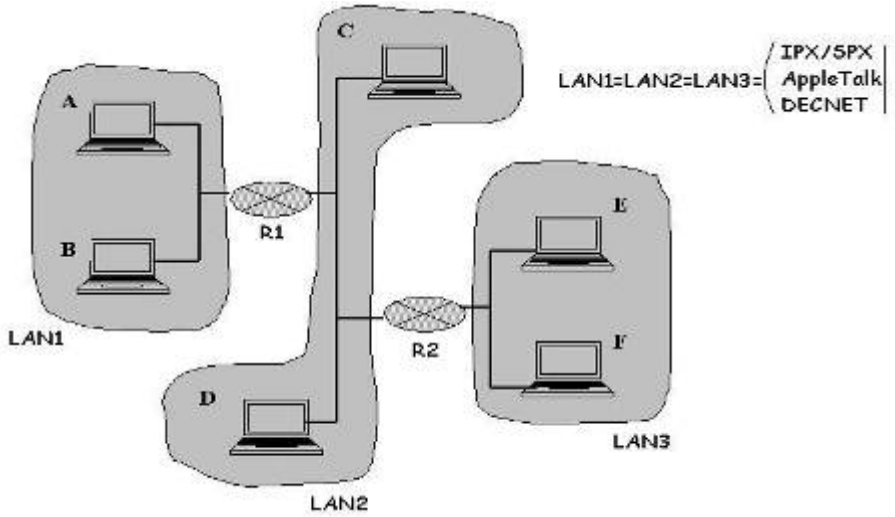
στην ουσία κανένα σκουλήκι ή συνδυασμένη απειλή, που βασίζεται στην TCP/IP στοίβα και τα πρωτόκολλα TCP ή UDP για τη μετάδοση και διασπορά, δε θα μπορεί σε κανονικές συνθήκες να τα διαπεράσει. Βέβαια, τα συστήματα αυτά θεωρούνται και είναι αρκετά παρωχημένα σήμερα και η υποστήριξή τους σημαντικά μικρότερη από την αντίστοιχη του TCP/IP, που είναι και το κατεξοχήν πρωτόκολλο για το Internet, αλλά θα μπορούσαν να χρησιμεύσουν ως «φρουροί» συστημάτων υψίστης σημασίας από τη μόλυνση ιών και σκουληκιών με εξαρτήσεις στην TCP/IP δικτύωση.

Παλαιότερα, όταν τα συστήματα αυτά ήταν κραταιά, ιοί και σκουλήκια ακολουθούσαν τα συγκεκριμένα μοντέλα δικτύωσης. Ο ερχομός του Internet και του TCP/IP με τον επακόλουθο μαρασμό των εν λόγω εναλλακτικών πρωτοκόλλων σήμαινε περιορισμό των δυνατοτήτων διάδοσης για το συγκεκριμένο, κακόβουλο λογισμικό (για παράδειγμα το άλλοτε κραταιό στο DECNET Father Christmas worm του 1988[447] σταδιακά «εξαφανίστηκε» από το προσκήνιο, με την υιοθέτηση της TCP/IP διασύνδεσης) και τη σταδιακή εγκατάλειψη κατασκευής του. Σήμερα, αντιστρέφοντας τη λογική αυτή, η επιστροφή στη χρήση των παλαιότερων πρωτοκόλλων μπορεί κάτω από ορισμένες προϋποθέσεις να αποτελέσει καταφύγιο για κρίσιμα ΠΣ από τις επιδρομές της καθεστηκυΐας τάξης των TCP/IP ιών και σκουληκιών (με πλέον εμφανές όμως κόστος στη διαλειτουργικότητα με τον κόσμο του Internet).

Προφανώς, τα εναλλακτικά δίκτυα δεδομένων (ακόμα και στις πιο σύγχρονες εκδοχές τους) δεν αφορούν τη μεγάλη πλειοψηφία των ΠΣ, που βασίζουν τη λειτουργία τους και οφείλουν την επιτυχία ή την αποτελεσματικότητά τους στην παρουσία τους στο Διαδίκτυο και στην εκμετάλλευση των πολλαπλών δυνατοτήτων του, αλλά έχουν νόημα και θέτουν *υποψηφιότητα για χρήση σε δικτυοκεντρικά ΠΣ μεγάλης κρισιμότητας, που δεν εμφανίζουν άμεση εξάρτηση από το Διαδίκτυο* (π.χ. απόρρητα κυβερνητικά ή στρατιωτικά συστήματα πληροφοριών[448]), προσφέροντας σε αυτά, κατόπιν κατάλληλης διαρρύθμισης, έναν υψηλότερο δείκτη προστασίας, σε σχέση πάντα με το ευάλωτο και στοχευμένο TCP/IP πρότυπο. Παρακάτω φαίνεται κάποιο σχετικό σχηματικό:

[447] Πηγή: "Threat Assessment of Malicious Code and Human Threats", Lawrence Bassham and Timothy Polk, NIST 1994, διαθέσιμο από το δεσμό http://csrc.nist.gov/publications/nistir/threats/threats.html.

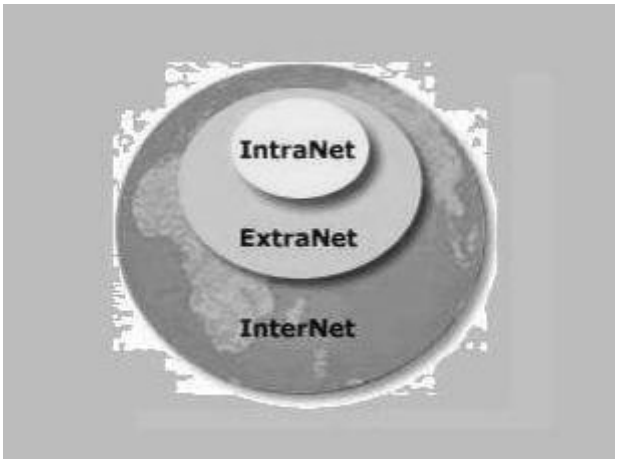
[448] Η χρήση παλιότερων ή/και καινοτόμων, μα απόρρητων, συστημάτων δικτύωσης, διαφορετικών πάντως του TCP/IP, μπορεί να λειτουργήσει προς συμφέρον της φύλαξης και προστασίας των ιδιαίτερα ευαίσθητων ΠΣ.



Σχήμα 27: Εναλλακτική δικτύωση σε LAN επίπεδο

4.4.4 Εσωτερικά συστήματα (IntraNETs) και πολυεπίπεδη, ελεγχόμενη πρόσβαση σε εξωτερικά, δικτυοκεντρικά ΠΣ

Ως γνωστόν ένα ενδοδίκτυο (ή Intranet) είναι *"ένα ιδιωτικό δίκτυο υπολογιστών που χρησιμοποιεί τα ίδια πρωτόκολλα διασύνδεσης και επικοινωνίας με το Διαδίκτυο (κυρίως την TCP/IP στοίβα, αλλά δεν αποκλείεται η χρήση και άλλων εναλλακτικών[449]) για να διαμοιράσει ασφαλώς μέρος των πληροφοριών ή των επιχειρησιακών διαδικασιών ενός οργανισμού στους υπαλλήλους και εργαζομένους αυτού"*[450].



Σχήμα 28: Η συγκριτική θέση και το μέγεθος των ενδοδικτύων στον παγκόσμιο πληροφοριακό χάρτη

[449] Με την όποια ωφέλεια που επισημάνθηκε στο αμέσως προηγούμενο εδάφιο 4.4.3.

Στα πλαίσια των ενδοδικτύων εφαρμόζονται, συνήθως, συνειδητά αυστηρές πολιτικές ασφάλειας καταφεύγοντας, όποτε είναι σκόπιμο και ευκταίο, και στη χρήση συγκεκριμένων προστατευτικών μηχανισμών υλισμικού τύπου. Οι γενικές αρχές που διέπουν την ιδανική οργάνωση ενός ενδοδικτύου είναι οι ακόλουθες:

1. Κάθε εισερχόμενη και εξερχόμενη δικτυακή κίνηση ελέγχεται και φιλτράρεται καταλλήλως με τη βοήθεια τειχών αντιπυρικής προστασίας ή/και συστημάτων IDS/IPS.[451] Συστήματα περιφρούρησης των υπολογιστικών και πληροφοριακών κόμβων, τόσο εντός αυτών όσο και σε πιο κεντρικό επίπεδο, τοποθετούνται κατά μήκος του εσωτερικού δικτύου.
2. Τα πρωτοκόλλα δικτύωσης και επικοινωνίας που εμπλέκονται τείνουν να είναι προτιμητέα στις όσο το δυνατόν ασφαλέστερες εκδοχές τους[452] και τεχνολογίες όπως οι SSH και SSL είναι πανταχού παρούσες.[453] Τα συστήματα λειτουργίας των κόμβων (υλικό και λογισμικό) πληρούν σύγχρονες προϋποθέσεις ασφάλειας.
3. Κάθε ενέργεια, εντός της σφαίρας επιρροής και δράσης που ορίζει ένα ενδοδίκτυο, καταγράφεται και αποτιμάται προγραμματιστικά, αλλά και όχι μόνο, από πλευράς ασφάλειας. Αν δεν ικανοποιεί ή αντιβαίνει σε θεσπισμένες πολιτικές, είτε αποτρέπεται είτε εγείρονται σχετικοί, επιχειρησιακοί «συναγερμοί» και πραγματοποιείται ευρύτερη προσπάθεια επαναφοράς στο επιθυμητό επίπεδο ασφάλειας.
4. Η είσοδος/έξοδος πληροφοριών και η διακίνηση υπηρεσιών από και προς το εξωτερικό περιβάλλον κάποιου οργανισμού πραγματοποιείται ιδανικά από μοναδικό, περιμετρικό σημείο στο δίκτυο, το οποίο αποτελεί τη λεγόμενη πύλη (border gateway)[454] και στην οποία οι έλεγχοι και μηχανισμοί ασφάλειας είναι αισθητά πιο αυξημένοι. *Σε εξαιρετικά κρίσιμα ΠΣ η πύλη αυτή μπορεί να μην υφίσταται καθόλου αποκόβοντας εντελώς το σύστημα από τον έξω κόσμο και το Διαδίκτυο και περιορίζοντας έτσι τις πηγές απειλών και κακόβουλων δράσεων εντός της περιμέτρου*

---

[450] Πηγή: Διαδίκτυο, ιστοχώρος της online εγκυκλοπαίδειας WikiPedia, http://en.wikipedia.org/wiki/Intranet.

[451] Κύρια, βιβλιογραφική αναφορά: [ASHLEY-PISOSAAT].

[452] Βλέπε σχετικό εδάφιο 4.4.1.

[453] Κύρια, βιβλιογραφική αναφορά: [ASHLEY-PISOSAAT].

[454] Δεν πρέπει να τη συγχέουμε με τις διαδικτυακές πύλες (web internet portals), που αφορούν τρόπους επικοινώνησης και διάθεσης πληροφοριών σε μαζικό κοινό μέσω κατάλληλης δόμησης ιστοχώρων. Η πύλη στην περίπτωση που μελετάμε αφορά το μοναδικό, ιδιαίτερο χωρικό σημείο και τα απαραίτητα, τεχνικά μέσα πρόσβασης πολλαπλών υπηρεσιών, πληροφοριών και ανθρώπων από και προς ένα ενδοδίκτυο με πηγή ή προορισμό άλλα ενδοδίκτυα ή το Διαδίκτυο.

αυτού. Στην πλέον συνηθισμένη πρακτική, πάντως, τα σύγχρονα ΠΣ επιτρέπουν προσεγμένη (π.χ. με χρήση διαμεσολαβητών, αντιπυρικών φίλτρων και συστημάτων παρακολούθησης και προστασίας επικοινωνιών[455]) έξοδο συνδέσεων και πληροφοριών και αποδέχονται ελεγχόμενη (με κατάλληλα δικαιώματα χρήσης, που να ικανοποιούν την αρχή του μινιμαλισμού, και με τη βοήθεια κρυπτογραφημένων καναλιών, που να εξασφαλίζουν την υπευθυνότητα στην επικοινωνία[456]) είσοδό τους. Ανάλογα με το είδος του εξωτερικού ΠΣ καθορίζεται και τροποποιείται κατάλληλα ο εκάστοτε βαθμός πρόσβασης και συναλλαγής π.χ. *«γνωστοί»/ταυτοποιημένοι πελάτες και συνεργάτες (προμηθευτές, ανάδοχοι έργων, εμπορικοί εταίροι, φίλιες επιχειρήσεις κτλ) διαμορφώνουν το λεγόμενο εξωδίκτυο ή extranet*[457] ενός οργανισμού που απολαμβάνει ένα ενδιάμεσο επίπεδο ασφάλειας στις δικτυακές επικοινωνίες σε σύγκριση με εκείνο των υπαλλήλων από τη μια πλευρά και στον αντίποδά της αυτό των «αγνώστων» επισκεπτών ή προορισμών.

5. Γίνεται εκτενής χρήση κρυπτογραφίας για την προστασία των ποθητών ιδιοτήτων της ασφάλειας των ΠΣ. Ειδικά στην περίπτωση των ΑΑΑ μηχανισμών, αλλά και στα πλαίσια προστασίας της εμπιστευτικότητας, ενεργοποιούνται εκλεπτυσμένες και ισχυρές, κρυπτογραφικές υποδομές (όπως η υποδομή δημόσιου κλειδιού ή τα συστήματα Kerberos και Sesame), που βασίζονται σε μεγάλο βαθμό στη «γνωμοδότηση» αρχών πιστοποίησης και τρίτων έμπιστων οντοτήτων.[458] Στα πλαίσια της ακεραιότητας δεδομένων, κάθε χρήσιμη/κρίσιμη πληροφορία ευρίσκεται εντός κρυπτογραφημένων βάσεων και αποθηκών και ανακτάται επιτυχώς, μόνο κατόπιν προγραμματιστικής παροχής των απαραίτητων κλειδιών.

6. Το ενδοδίκτυο χωρίζεται τεχνικά σε λογικές ζώνες ασφάλειας.[459] Πρώτ' απ' όλα, *οι κρίσιμες, εξωτερικά διαθέσιμες υπηρεσίες (presentation logic) κάθε ΠΣ (front-end systems) τοποθετούνται για λόγους πρόληψης σε ξεχωριστή, απομονωμένη από το υπόλοιπο δίκτυο ζώνη (DMZ)*[460], κοντά στην πύλη, κυρίως λόγω της αναγκαίας, μεγάλης έκθεσής τους σε έξωθεν απειλές, που δύνανται διαφορετικά να επηρεάσουν όλο την πληροφοριακή υποδομή, αλλά και για να προστατεύονται και εκείνες με τη

---

[455] Όπως τα περιγράψαμε στα εδάφια 4.1.3 και 4.1.6.

[456] Όπως αναλύθηκαν σε πρότερα σκέλη του τρέχοντος κεφαλαίου.

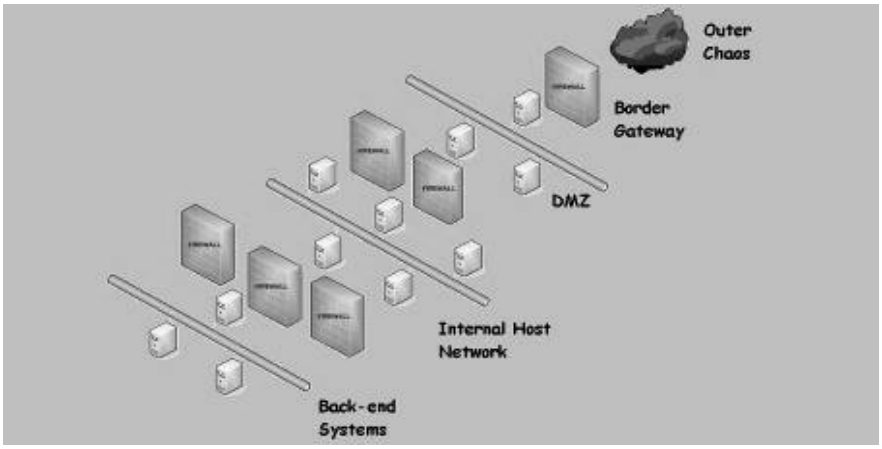
[457] Πηγή: Διαδίκτυο, ιστοχώρος της online εγκυκλοπαίδειας WikiPedia, http://en.wikipedia.org/wiki/Extranet.

[458] Κύρια, βιβλιογραφική αναφορά: [ASHLEY-PISOSAAT].

[459] Πηγή: "The Evolution of Network Security: From DMZ Designs to Devices", Mark Bouchard, MetaGroup 2004, διαθέσιμο από το δεσμό www.juniper.net/solutions/literature/white_papers/200084.pdf.

[460] Η λεγόμενη και αποστρατικοποιημένη ζώνη, ακριβώς επειδή η παρουσία ισχυρών μέτρων και πολιτικών ασφάλειας είναι πιο διακριτική και «χαλαρή», σε σχέση με το υπόλοιπο IntraNET.

σειρά τους από εσωτερικές παραβιάσεις ασφάλειας. Οι σταθμοί εργασίας και τα διάφορα τερματικά οριοθετούν μια ενδιάμεση, δεύτερη ομάδα ασφάλειας, ενώ *η επιχειρησιακή λογική (business logic) και οι ευαίσθητες εσωτερικές πληροφορίες και υπηρεσίες «κρύβονται»* από τους αναρμόδιους και φυλάσσονται σε τρίτο, ειδικά προστατευμένο χώρο (back-end security), ιδανικά αρκετά «μακριά» από την εξωτερική πύλη του ΠΣ.



Σχήμα 29: Το τυπικό, σύγχρονο IntraNET

Οι 3 αυτές ζώνες διαθέτουν μεγάλο βαθμό μεταξύ τους απομόνωσης, με τη βοήθεια συσκευών και εξειδικευμένου λογισμικού φιλτραρίσματος και ελέγχου πρόσβασης, ενώ η αλληλεπικάλυψή τους διατηρείται στο ελάχιστο δυνατό, σχεδόν μηδαμινό, επίπεδο. Η διαβάθμιση αυτή στην εσωτερική δομή του ενδοδικτύου εξασφαλίζει *πολυεπίπεδη προστασία (multilayered)*[461] *του πληροφοριακού ιστού* ενός οργανισμού, τόσο από εσωτερικές (μεταξύ των ζωνών), όσο και από εξωτερικά προερχόμενες (στην ζεύξη από και προς την πύλη) ενδεχόμενες παραβιάσεις ή υποβαθμίσεις ασφάλειας, ενώ υπάρχει ιδιαίτερη φροντίδα, ώστε να μην προκαλείται αισθητός περιορισμός της λειτουργικότητας και της ευχρηστίας λόγω του «σφιχτού» αυτού σχήματος.

7. Ένα ενδοδίκτυο αποδεικνύεται τόσο περισσότερο επιτυχημένο από πλευράς ασφάλειας, όσο πιο τοπικό χαρακτήρα εμφανίζει το εύρος του δικτύου του φέροντα οργανισμού. Σε περίπτωση οργανισμών με WAN αναγκαιότητες[462] οι 5 παραπάνω αρχές οφείλουν να εφαρμόζονται ξεχωριστά και ανεξάρτητα εσωτερικά σε καθένα

[461] Κύρια, βιβλιογραφική αναφορά: [SYMANTEC-EIWLSS].

[462] Είναι πολύ συνηθισμένο πια, στην εποχή του διεθνισμού, οι επιχειρήσεις και οι οργανώσεις να ξεπερνούν ποικίλα γεωγραφικά σύνορα και δρουν ενδεχομένως ακόμα και σε παγκόσμια επίπεδο, προεξαρχόντως των πολυεθνικών εταιρειών και των διακρατικών ενώσεων.

από τα μεμονωμένα LANs που απαρτίζουν το συνολικό δίκτυο. Σε μια τέτοια αναγκαιότητα, τον απαιτούμενο, ικανοποιητικό συμβιβασμό ασφάλειας και επιχειρησιακής λειτουργικότητας παρέχουν λύσεις, όπως τα εικονικά, ιδιωτικά δίκτυα ή VPNs[463], που διασυνδέουν τα οικεία, ενδοδίκτυα του WAN μεταξύ τους. Η πολυπλοκότητα, βέβαια, στη διαχείριση και η συνακόλουθη αβεβαιότητα στην παρεχόμενη ασφάλεια αυξάνονται ευθέως ανάλογα με τις μεταβλητές όγκου (απόσταση, αριθμός εμπλεκόμενων χρηστών και συστημάτων) του κάθε εν λόγω δικτυώματος.

8. Τα IntraNETs λειτουργούν βασιζόμενα σε εμπεριστατωμένα και εκτεταμένα μοντέλα επιχειρησιακών ρόλων-εξουσιοδοτήσεων (business role-based privileges) και στρατηγικών διαδικασιών (mission-critical processes), για να επιβάλλουν κατάλληλα δικαιώματα πρόσβασης/προσπέλασης, αλλά και τις ανάλογες αρμοδιότητες/ευθύνες διαχείρισης και χρήσης, σε κάθε χρήσιμα εμπλεκόμενη οντότητα, ώστε καθ' όλη τη διάρκεια λειτουργίας να διαφυλάσσεται και να εξυπηρετείται η προσπάθεια υλοποίησης των στρατηγικών, επιχειρησιακών στόχων.[464]

Τα ενδοδίκτυα αποτελούν σήμερα το πλέον συνηθισμένο και ενδεδειγμένο υπόδειγμα ενδοεταιρικής οργάνωσης του πληροφοριακού δικτύου ενός οργανισμού, ασχέτως του σχετικού του μεγέθους. Με τη βοήθεια της δομής των ενδοδικτύων και της επιτεύξιμης μέσω αυτών ελεγχόμενης πρόσβασης από και προς εξωτερικά συστήματα πληροφοριών (ανάμεσα τους και το ίδιο το Διαδίκτυο) που δεν βρίσκονται στην άμεση δικαιοδοσία, έλεγχο ή κατοχή, οι οργανισμοί είναι πλέον σε θέση να προστατεύουν αποτελεσματικότερα τα κρίσιμα δεδομένα και λοιπά συστατικά του ιδιόκτητου ΠΣ τους από κακόβουλους κινδύνους πέραν της περιμέτρου τους. Αν μια υποδομή ενδοδικτύου έχει σχεδιαστεί με τεκμαρτή σοβαρότητα (χρονοδιάγραμμα, πρότυπες διαδικασίες και μηχανισμοί, επενδύσεις), τότε είναι δυνατόν να αποτελέσει φραγμό και όνειδος στα όνειρα και τις απόπειρες κακόβουλων κακοποιών.

4.5 Αρχιτεκτονική ασφαλούς λογισμικού εφαρμογών

Το λογισμικό μπορεί να περιέχει από σφάλμα/παράλειψη ή σκόπιμα κώδικα που εισάγει συγκαλυμμένα κανάλια, κερκόπορτες, και άλλες αδυναμίες ασφάλειας στα συστήματα και τις

---

[463] Πηγή: " Issues in Intranet Security: A primer on keeping the keys to the enterprise safe", Stephen Cohn, nCipher, διαθέσιμο από το δεσμό http://www.intranetjournal.com/features/isecurity.shtml.

[464] Πηγή: "Intranet Organization: Strategies for managing change", Steven Telleen, 1996, διαθέσιμο από το δεσμό http://www.iorg.com/intranetorg/.

εφαρμογές. Το κακόβουλο λογισμικό μπορεί να εκμεταλλεύεται τα στοιχεία αυτά, ώστε να αποκτά όπως είδαμε αναρμόδια πρόσβαση στα δεδομένα των ΠΣ ή να παίρνει τον έλεγχο των δικτυακών επικοινωνιών, εισάγοντας παράλληλα κινδύνους υπονόμευσης/παραχάραξης των κόμβων. Άρα, η απαίτηση για ασφαλές λογισμικό εφαρμογών αποτελεί σημαντική προτεραιότητα και προοπτική στον αγώνα για τον περιορισμό της κακόβουλης δράσης ιών και σκουληκιών λόγω της ανακοπής των διαδρόμων μη εξουσιοδοτημένης πρόσβασης και των διανυσμάτων μόλυνσης που ιδανικά υπόσχεται να πραγματώσει.

4.5.1 Ενσωμάτωση υπηρεσιών ασφάλειας και εφαρμογή προτύπων συγγραφής ασφαλούς κώδικα

Πρώτη αναγκαιότητα για τη συγγραφή ασφαλούς λογισμικού και την ανάπτυξη εφαρμογών είναι να ενσωματώνονται στα νέα προγράμματα κατάλληλοι μηχανισμοί ελέγχων και υπηρεσιών ασφάλειας και οι αρχιτέκτονες του λογισμικού να συμμορφώνονται με ευρέως αποδεκτά πρότυπα ασφαλούς κώδικα. Η όλη αυτή ιδέα αποδίδεται με τον ξένο όρο safe programming[465].

Οι περισσότερες εφαρμογές απαιτούν σήμερα την *παρουσία και χρήση ενισχυμένων μεθόδων αυθεντικοποίησης, ελέγχου εξουσιοδοτήσεων και κρυπτογράφησης* για να εξασφαλίσουν την επιθυμητή ακεραιότητα και εμπιστευτικότητα των πληροφοριών. Καθώς ο αριθμός των κρίσιμων συναλλαγών αυξάνεται ολοένα, το εγγενές σχήμα ελέγχου πρόσβασης γενικότερα που παρέχουν τα προγράμματα γίνεται ανάλογα πιο σημαντικό, ώστε να εξασφαλίζεται εκτός των άλλων και η μη αποποίηση των συναλλαγών και η υπευθυνότητα στις όποιες δραστηριότητες εντός της δικαιοδοσίας δοθέντος ΠΣ.

Σε γενικές γραμμές, μια σύγχρονη θεώρηση για την ανάπτυξη ασφαλών εφαρμογών από την άποψη των ενσωματωμένων υπηρεσιών και εφαρμοσμένων προτύπων θα πρέπει να προβλέπει:[466]

1. Ολοκληρωμένο σύστημα ελέγχου πρόσβασης (AAA) χρηστών στην εφαρμογή, όπως π.χ. τα διαδεδομένα μοντέλα RBAC και T-RBAC.
2. Εκτεταμένη κρυπτογραφία για τα κρίσιμα δεδομένα και συνδέσεις.

---

[465] Κύρια, βιβλιογραφική αναφορά: [GRAFF_VANWYK-SCPP].

[466] Πηγές: Διαδίκτυο, προτάσεις και οδηγίες των παγκοσμίου φήμης και αποδοχής εταιρειών λύσεων Πληροφορικής Sun (http://java.sun.com/security/seccodeguide.html) και Microsoft (http://msdn2.microsoft.com/en-us/security/aa570401.aspx) στους προγραμματιστές τους, σχετικά με τις safe-coding πρακτικές.

3. Επιμονή στη χρήση αξιόπιστων και ασφαλών πρωτοκόλλων επικοινωνίας.
4. Πρόνοια για τη μεγαλύτερη δυνατή διαλειτουργικότητα (παροχή διεπαφών) με υπάρχοντες, εξωτερικά προσφερόμενους μηχανισμούς ασφάλειας (π.χ. Λ/Σ, εξειδικευμένου υλισμικού κατά των κακόβουλων απειλών).
5. Επαρκής και εμφανής διαχωρισμός κώδικα εφαρμογής και δεδομένων, που αυτή χρησιμοποιεί, με την προοπτική της εκτέλεσης σε ασφαλή περιβάλλοντα επεξεργασίας[467].
6. Ελέγχους επικύρωσης των εντολών εισόδου/εξόδου δεδομένων (input/ouput validation).
7. Επιλογή τύπων περιγραφής δεδομένων ή μηνυματοδοσίας, όπως π.χ. το πρότυπο XML, που παρέχουν εγγενή και πρόσθετο, επαρκή βαθμό ευελιξίας στην ασφάλεια δικτυοκεντρικών υπηρεσιών (WS-Security[468]) και των υποστηριζόμενων ΠΣ.
8. Ικανοποίηση όσο είναι δυνατόν της αρχής του μινιμαλισμού (KISS[469]) στη λειτουργικότητα. Κάθε πρόγραμμα πρέπει, εν γένει, να αποφεύγει να παρέχει την όποια πρόσθετη από την απαιτούμενη και επιθυμητή λειτουργικότητα ή όταν δεν το κάνει οι προγραμματιστές οφείλουν να έχουν επιληφθεί του όλου θέματος με μεγάλη προσοχή, έχοντας λάβει τα απαραίτητα μέτρα για τον περιορισμό των αυξημένων, επικίνδυνων καταστάσεων.
9. Επισκόπηση της εκάστοτε, τρέχουσας φιλολογίας των απειλών για την αποφυγή εγνωσμένων, προγραμματιστικών αβλεψιών, που αποδεδειγμένα και με πολύ συγκεκριμένους, υλοποιημένους τρόπους εκθέτουν την ασφάλεια του λογισμικού. Π.χ. η αποφυγή επιθέσεων υπερχείλισης καταχωρητών ή ωμών και λεξικογραφικών δοκιμών σπασίματος ξεκινά από την απαραίτητη πρόνοια στη μελέτη και συγγραφή προσεκτικά δομημένου κώδικα.
10. Εντοπισμός και εκτίμηση του μεγέθους και του αντίκτυπου των εξαρτώμενων και προκαλούμενων από την σχεδιαζόμενη εφαρμογή απειλών και ευπαθειών (application-dependent threat and vulnerability modeling). Μια τέτοια αξιολόγηση πρέπει να είναι η απαρχή κάθε στοχευμένης προσπάθειας περιορισμού των κινδύνων μέσω ασφαλούς προγραμματισμού.
11. Παροχή εξειδικευμένου μηχανισμού αυτόματων ενημερώσεων ασφάλειας (βλέπε αναλυτικότερα σε επόμενο εδάφιο) και συστήματος αποστολής ανάδρασης χρηστών

---

[467] Όπως τα αναλύσαμε στο προηγούμενο εδάφιο 4.3.

[468] Κύρια, βιβλιογραφική αναφορά: [HOLGERSSON-WSS].

[469] Πηγή: Διαδίκτυο, ιστοχώρος της online εγκυκλοπαίδειας WikiPedia, http://en.wikipedia.org/wiki/KISS_principle.

π.χ. σε περίπτωση απρόσμενης ενέργειας ή βλάβης της εφαρμογής (πολύ χρήσιμο για αποτελεσματικό debugging/bug fixing).

12. Συμπερίληψη συγκεκριμένου κώδικα με στόχο σαφή, δραστική άμυνα ενάντια σε κάποια είδη κακόβουλης υπονόμευσης (π.χ. αντεπίθεση σε κακόβουλο λογισμικό ή κόμβο, «αυτοκαταστροφή», ενεργοποίηση συναγερμών).
13. Παντελής έλλειψη εντολών «επιθετικού» χαρακτήρα ή οιασδήποτε μορφής κακόβουλου κώδικα (προφανές).
14. Αποφυγή μη επαρκώς τεκμηριωμένων, προγραμματιστικών κλήσεων και επιλογή συνετής χρήσης των τυποποιημένων και πλέον δοκιμασμένων και ανθεκτικών APIs (βλέπε τεκμηρίωση μεθόδων).
15. Προτίμηση στα αξιόπιστα περιβάλλοντα ανάπτυξης, στις προσεγμένες και ευέλικτες γλώσσες προγραμματισμού (π.χ. type-safe languages) και σε νέους, σταθερούς, επαρκώς δοκιμασμένους και ασφαλείς μεταγλωττιστές/διερμηνευτές.
16. Αποτροπή ανεπιθύμητης, μη εξουσιοδοτημένης πρόσβασης/παρέμβασης στη διαδικασία σχεδιασμού κάποιας εφαρμογής.
17. Συμμόρφωση με παγκοσμίως αναγνωρισμένες και αποδεκτές υλοποιήσεις προτύπων καθοδήγησης για ασφαλή προγραμματισμό[470].

Η εκπλήρωση των παραπάνω σημείων αποτελεί πρόκληση για τον κάθε προγραμματιστή, καθώς υπεισέρχονται και άλλα ζητήματα, όπως του μεγέθους ή της ευχρηστίας της παραγόμενης εφαρμογής· δεν παύουν όμως να στοιχειοθετούν ένα εξαιρετικό υπόδειγμα προσέγγισης της *πρακτικής του safe-programming* και εγγυώνται πως, όταν εφαρμόζονται με συνέπεια, αναδεικνύονται σε μια ξεκάθαρη λύση για αποτελεσματική προστασία από τους «στρόβιλους» του κακόβουλου λογισμικού.

4.5.2 Διορθώσεις τεχνικών λαθών και ατελειών (Bug or Flaw Fixing)

Δεύτερη κατά σειρά προϋπόθεση για τη δημιουργία ασφαλούς λογισμικού είναι μια *διαρκής δραστηριότητα εντοπισμού και επιδιόρθωσης τυχόντων τεχνικών λαθών και παραλείψεων (bugs)*, που όχι μόνο αντιστέκονται στην καλή λειτουργία ενός προγράμματος (προβληματίζοντας και τους χρήστες), αλλά δύνανται να το εκθέσουν και σε κακόβουλες

[470] Όπως τα εγνωσμένα πρότυπα, που προβάλλει και προωθεί ο διεθνής, συντονιστικός οργανισμός CERT, μέσα από τις σελίδες και τις επισημάνσεις του ιστοχώρου του, https://www.securecoding.cert.org/confluence/display/seccode/CERT+Secure+Coding+Standards.

απειλές (και μαζί με αυτό ολόκληρο το υπερκείμενο του σύστημα πληροφοριών), παρέχοντας κατάλληλα διανύσματα μόλυνσης στις επίδοξες, επίβουλες οντότητες. Το στάδιο αυτό αποτελεί μέτρο πρόληψης για την εμφάνιση και δράση απειλών, που θα εκμεταλλεύονται υπαρκτές ατέλειες ή σχεδιαστικά λάθη σε εφαρμογές, με σκοπό την επίθεση στην ασφάλεια ενός συστήματος που περιέχει τρόπον τινά αυτές τις εφαρμογές. Έχει αποδειχθεί πως όσο αποτελεσματικότερη η διαδικασία αποσφαλμάτωσης των προγραμμάτων, τόσο μικρότερη είναι η πιθανότητα εμφάνισης ευπαθειών σε αυτά[471]. Θεωρείται δε εκ των ων ουκ άνευ πως η διόρθωση μιας ατέλειας δε θα πρέπει κατά το δυνατόν να εισάγει καινούριες, διότι τότε θα υπήρχε διαιωνισμός και ανακύκλωση των παρακείμενων κινδύνων και δυσκολιών.

Στην όλη διαδικασία της αποσφαλμάτωσης μπορούν να *μετέχουν/συνεισφέρουν ενεργά και οι τελικοί χρήστες* με την (διάφανη ή πιο αδιαφανή) αποστολή συγκεκριμένων στοιχείων στους προγραμματιστές, εν είδη ανάδρασης κατά την αντιμετώπιση/εντοπισμό κάποιου άγνωστου ή μη διορθωμένου bug, στη διάρκεια λειτουργίας μιας εφαρμογής[472].

4.5.3 Ενημερώσεις ασφάλειας-Διορθώσεις ευπαθειών (Security Patching)

Το τρίτο βήμα για την κατασκευή ασφαλούς λογισμικού είναι η ύπαρξη μιας *αδιάλειπτης διαδικασίας αναγνώρισης συγκεκριμένων ευπαθειών στο εκάστοτε πρόγραμμα και παροχής κατάλληλων, ενημερωμένων εκδόσεων αυτού, στις οποίες κάποια από τα υπάρχοντα κενά ασφάλειας έχουν πλέον διορθωθεί-εξαλειφθεί*.[473] Η διαδικασία αυτή έρχεται ως αντίδραση των προγραμματιστών ενός λογισμικού σε επιτυχημένες απόπειρες υπονόμευσής του που οφείλονται σε σχεδιαστικά λάθη ή παραλείψεις, τα οποία οδηγούν σε ευπάθειες. Όσο πιο έγκαιρη, έγκυρη και αποτελεσματική είναι η προσπάθεια «πατσαρίσματος» του λογισμικού έναντι εκδηλωμένων προβλημάτων ασφάλειας, τόσο πιο μεγάλες είναι οι πιθανότητες περιορισμού της επέκτασης μιας σχετικής κακόβουλης απειλής και πρόληψης νέων ανάλογων κρουσμάτων ή περιπτώσεων. Σε διαφορετική περίπτωση (άκαιρη και προβληματική ενημέρωση) το πρόβλημα παραμένει ή μπορεί να γίνει και ακόμη οξύτερο.

Στα πλαίσια των διορθώσεων ασφάλειας, η «εκμετάλλευση» της συνεισφοράς -μέσω της επισήμανσης καίριων προβλημάτων- της κοινότητας των χρηστών, που υπογραμμίστηκε και στο κομμάτι του bug fixing, και οι σκόπιμες, τεχνικές δοκιμές ασφάλειας του λογισμικού,

---

[471] Για την αντίστοιχη διαδικασία για τις ευπάθειες προγραμμάτων, δείτε στο αμέσως επόμενο εδάφιο 4.5.3.

[472] Ένα πολύ δημοφιλές σύστημα «καταγγελίας» και διαχείρισης λαθών και ατελειών είναι το περίφημο BugZilla (http://www.bugzilla.org/), που αφορά τα έργα του ιδρύματος Mozilla και στη λογική του οποίου κινούνται και λοιπά, παρόμοια συστήματα.

[473] Πηγή: Διαδίκτυο, ιστοχώρος της online εγκυκλοπαίδειας WikiPedia, http://en.wikipedia.org/wiki/Patch_(computing)#Security_patches.

που συζητούνται σε επόμενο σκέλος, είναι κύριοι σύμμαχοι και καλές πρακτικές για τους προγραμματιστές.

Βέβαια, η παροχή των όποιων ενημερώσεων ασφάλειας, που βαραίνει εξολοκλήρου τους κατασκευαστές/προμηθευτές κάθε λογισμικού, δεν αρκεί από μόνη της για την εξασφάλιση επίκαιρης προστασίας, καθώς η *εφαρμογή των ενημερωμένων εκδόσεων/διορθώσεων* από μεριάς των ιδιοκτητών και (δια)χειριστών των συστημάτων πληροφοριών είναι εξίσου, αν όχι περισσότερο, σημαντική.[474] Αν για τον οποιοδήποτε λόγο (αμέλεια, στρατηγική απόφαση κτλ) μια διόρθωση ή ενημέρωση ασφάλειας δεν εφαρμοστεί σε επίπεδο χρήστη του λογισμικού, το κενό στην ασφάλεια θα παραμένει με ό,τι εγνωσμένο κίνδυνο αυτό συνεπάγεται από πλευράς δυνατοτήτων κακόβουλης δράσης.

4.5.4 Τεκμηρίωση μεθόδων (Documentation)

Προτελευταίο στάδιο στη διαδικασία κατασκευής λογισμικού συντονισμένου στον ποθούμενο δείκτη ασφάλειας είναι η *συγγραφή/παροχή κατάλληλης (και όσο γίνεται πιο πλήρους) τεκμηρίωσης λειτουργίας (και εγχειριδίων χρήσης)*. Πέρα από την προφανή ευκρίνεια και ευκολία, που προσφέρει η τεκμηρίωση στο χειρισμό του κάθε προγράμματος από τον εκάστοτε, τελικό του χρήστη, είναι σημαντική για την προστασία από το κακόβουλο λογισμικό για τρεις κυρίως ακόμη, σχετικά συγγενείς, λόγους:[475]

- Η σχολαστική τεκμηρίωση όλων των χρησιμοποιούμενων από την εφαρμογή μεθόδων, καταρχάς, απαλλάσσει το διαχειριστή ή τον επαγγελματία της ασφάλειας από άσκοπες, περιττές και χρονοβόρες, τεχνικές ενέργειες στην προσπάθεια να αποσφαλματώσει/διαγνώσει την (καλή ή κακή) λειτουργία ενός προγράμματος.
- Κατά δεύτερο λόγο, η τεκμηρίωση λειτουργεί σα μηχανισμός μνήμης για τον δημιουργό ενός προγράμματος, επιτρέποντάς του να μπορεί να βρίσκεται σε θέση να παρέχει καλύτερη και μακροπρόθεσμη υποστήριξη, όποτε και με όποιο τρόπο αυτό χρειάζεται. Το ίδιο σκεπτικό ισχύει και για τους φέροντες οργανισμούς, που εφόσον διαθέτουν την απαραίτητη τεκμηρίωση, μπορούν ανά πάσα χρονική στιγμή επιθυμούν να προσεγγίζουν με ουσιαστικό και έγκυρο τρόπο τα χαρακτηριστικά δημιουργίας, εγκατάστασης και παραμετροποίησης ενός αποκτηθέντος προγράμματος.

---

[474] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM].

[475] Πηγή: "Documentation is Important", Curtis Cook and Marcello Visconti, 1994, διαθέσιμο από το δεσμό http://www.stsc.hill.af.mil/crosstalk/1994/11/xt94d11j.asp.

- Η τεκμηρίωση είναι οδηγός για τη βελτιστοποίηση και αναβάθμιση της λειτουργικότητας και της ασφάλειας των προγραμμάτων, καθώς παρουσιάζει με γλαφυρό τρόπο τις υπαρκτές ελλείψεις, παραλείψεις, παρανοήσεις, αδυναμίες και ατέλειες των εφαρμογών, από πλευράς επιχειρησιακών απαιτήσεων και επιθυμιών.

Σαν μια τρίτη παρατήρηση, οφείλουμε να τονίσουμε την εμμονή πολλών κακόβουλων συγγραφέων, στις μέρες μας, στο να καταφεύγουν στη χρήση μη επαρκώς τεκμηριωμένων μεθόδων των προγραμμάτων προκειμένου να τα υπονομεύσουν ή να τα χρησιμοποιήσουν σε κακόβουλες ενέργειες εναντίον άλλων[476]. Με τον τρόπο αυτό, ευελπιστούν σε μεγαλύτερη δυνατή απόκρυψη (άρα και αντοχή-«διάρκεια») της κακόβουλης δραστηριότητας.

Για όλους αυτούς τους λόγους μαζί αλλά και για κάθε έναν ξεχωριστά, η τεκμηρίωση φαντάζει επιβεβλημένη διαδικασία στην κατεύθυνση της αρχιτεκτονικής ασφαλούς λογισμικού και εμφανίζεται να διαδραματίζει ιδιαίτερα εποικοδομητικό ρόλο στην πρόληψη της δράσης/επέκτασης ιών και σκουληκιών.

4.5.5 Έλεγχοι-Δοκιμές ασφάλειας

Πριν τη διάθεση της δείνα εφαρμογής για ευρεία χρήση, σκόπιμο είναι οι προγραμματιστές αυτής να καταφεύγουν και σε *κάποιου είδους δοκιμές ασφάλειας*, παράλληλα με τους όποιους ελέγχους καλής λειτουργίας της (σε επίπεδο τουλάχιστον πρωτοτύπου)[477]. Οι δοκιμές αυτές θα μπορούσαν να συμπεριλαμβάνουν γνωστές και συνηθισμένες τον καιρό της δημιουργίας της εφαρμογής επιθέσεις, με σκοπό την μόλυνση και υπονόμευση αυτής ή την υποβάθμιση των υπηρεσιών ασφάλειας που παρέχει.[478] Η λογική των δοκιμών και των ελέγχων μπορεί να επεκταθεί και στη φάση λειτουργίας του τελικού προγράμματος, ως μέρος μιας διαρκούς διαδικασίας αποτίμησης-αναβάθμισης[479]. Η σχετική επιτυχία των καλοπροαίρετων αυτών «επιθέσεων» και τα όποια συμπεράσματα από τις δοκιμές μπορούν να χρησιμοποιηθούν για την αναγνώριση των αδυναμιών ασφάλειας του υπό παραγωγή προγράμματος και ακολούθως

---

[476] Αυτή είναι μια πολύ συνηθισμένη και αποδοτική τακτική στους χώρους της κατασκευής επιβλαβών προγραμμάτων, που θα επισημάνουμε πολλές φορές στη διάρκεια της διπλωματικής (ιδίως στα τμήματα που έχουν σχέση με σε βάθος υπονόμευση Λ/Σ). Η επιτυχία της βασίζεται ακριβώς στην απουσία γνώσης πάνω στις χρησιμοποιούμενες μεθόδους προσβολής και στην συνακόλουθη αδυναμία των μηχανισμών άμυνας να δράσουν έχοντας κάποια, τεκμηριωμένη καθοδήγηση.

[477] Οι έλεγχοι αυτοί αποτελούν αποδείξεις μετρήσιμης ποιότητας, για αυτό και έχουν καθιερωθεί ευρέως από τους κατασκευαστές λογισμικού, σε μια προσπάθεια να «πείσουν» τον όποιο συμβαλλόμενο για την αξιοπιστία και ασφάλειας του παρεχόμενου προϊόντος ή της προσφερόμενης υπηρεσίας.

[478] Κύρια, βιβλιογραφική αναφορά: [MCGRAW-SST].

[479] Όπως στην προαναφερόμενη (4.5.3) περίπτωση της παροχής ενημερωμένων εκδόσεων ασφάλειας.

την σχεδιαστική βελτιστοποίηση/αναθεώρηση των χαρακτηριστικών του, στην κατεύθυνση του όποιου, επιθυμητού ή αναγκαίου επιπέδου ασφάλειας.

4.6 Φυσικού Τύπου Προστασία

Η καλύτερη προστασία από την δράση του κακόβουλου, αυτοαναπαραγόμενου λογισμικού πολλές φορές προϋποθέτει και την ύπαρξη κάποιου επιτηδευμένου μηχανισμού φύλαξης και παρακολούθησης ή/και αυθεντικοποίησης, εξουσιοδότησης και υπεύθυνης, καταγεγραμμένης πρόσβασης (υπηρεσίες ΑΑΑ), που να βασίζεται στην φυσική ταυτοποίηση των οντοτήτων που ευρίσκονται σε δεδομένο χώρο κρίσιμο για τη λειτουργία κάποιου ΠΣ. Δεν είναι λίγες οι περιπτώσεις που ένας ιός ή κάποιο σκουλήκι ξεκίνησε τη μολυσματική του περιπέτεια μέσα από τους κόλπους κάποιου οργανισμού για να διαδοθεί και να υπονομεύσει τον ίδιο ή/και άλλους, έχοντας κυριολεκτικά τοποθετηθεί με φυσικό τρόπο από κάποια κακόβουλη οντότητα που εκμεταλλεύτηκε τις διάφορες, ανεπαρκώς φυλασσόμενες υποδομές και κρίσιμους χώρους εντός των ιδιαίτερων ορίων του υπό συζήτηση οργανισμού.

Η χρήση κατάλληλων αισθητήρων και εξελιγμένων συστημάτων και κυκλωμάτων παρακολούθησης και διαπίστευσης οντοτήτων, σε συνδυασμό με ανθρώπινη ανάλυση και διαχείριση των πληροφοριών που προκύπτουν, μπορεί να προφυλάσσει δυναμικά και ικανοποιητικά από μη εξουσιοδοτημένη ή παράνομη πρόσβαση απαγορεύοντάς την ή προκαλώντας την ενεργοποίηση κάποιου γενικότερου, κατάλληλου «συναγερμού» ασφάλειας.

Όπως και να ’χει, *η παρουσία μηχανισμών φυσικού τύπου προστασίας δρα αποτρεπτικά για κακόβουλα εγχειρήματα εντός της φυσικής περιμέτρου ενός ΠΣ* και χρήσιμο είναι τέτοια μέτρα να υφίστανται και να εφαρμόζονται σε όλους τους ευαίσθητους, φυσικούς χώρους, αλλά και κατά μήκος της περιμέτρου, ειδικά αν τα ΠΣ που διακυβεύονται είναι μεγάλης σημασίας. Η φυσική ταυτοποίηση και εξουσιοδότηση θα μπορούσε εξάλλου να εμπεριέχει ή να συνεπάγεται έμμεσα και την περαιτέρω ικανοποίηση/ενίσχυση μιας ακόμη σημαντικότατης υπηρεσίας ασφάλειας κοντινής στο καθιερωμένο σχήμα ΑΑΑ· της μη αποποίησης μιας δράσης κατά τη διάρκεια της πρόσβασης, που είναι δυνατόν να χρησιμοποιηθεί εκτός των άλλων και για τη νομική κατηγορία και τιμωρία κακόβουλων δραστών, παρέχοντας στοιχεία και πειστήρια υπευθυνότητας/υπαιτιότητας. Όλα αυτά συντηρούν και δικαιολογούν την ολοένα αυξανόμενη δυναμική των φυσικών μεθόδων προστασίας.

4.6.1 Συστήματα ελέγχου φυσικής πρόσβασης και παρακολούθησης ανθρώπινης δραστηριότητας σε φυλασσόμενους χώρους

Οι *συνήθεις μηχανισμοί φύλαξης και διαπίστευσης ατόμων* (φύλακες, συναγερμοί, κλειδαριές, μαγνητικές κάρτες και ταυτότητες, «εισιτήρια», PINs και άλλα συνθηματικά με την ευρεία έννοια, σημεία και πύλες επίδοσης, ελέγχου και εξακρίβωσης στοιχείων και διαπιστευτηρίων κτλ)[480], προκειμένου να αποφευχθεί μια μη εξουσιοδοτημένη πρόσβαση σε χώρους με υψηλές απαιτήσεις ασφάλειας, μπορούν να βρουν εφαρμογή και στην περίπτωση προστασίας από τη δράση κακόβουλου λογισμικού, όταν αυτή απαιτεί τη φυσική παρουσία κάποιας οντότητας σε αυτούς τους χώρους.

Επιπρόσθετα, τα *κλασσικά συστήματα παρακολούθησης* (surveillance or monitoring systems) π.χ. μέσω κυκλωμάτων ασφάλειας (κάμερες) στους ιδιαίτερα κρίσιμους χώρους (backend systems' rooms, computer rooms) ενισχύουν την πιθανότητα αποφυγής κακόβουλων ενεργειών στο βαθμό που αυτές απαιτούν φυσική παρουσία κάποιας οντότητας σε κάποια φάση της επιβλαβούς δράσης.

Όταν ένας χώρος ιδιαίτερης φυσικής σημασίας για κάποιο ΠΣ φυλάσσεται επαρκώς και παρακολουθείται καταλλήλως με τη *συμμετοχή του ανθρώπου*, αλλά και ολοκληρωμένων συστημάτων φυσικής διαπίστευσης (για παράδειγμα τα βιομετρικά συστήματα, για τα οποία θα πούμε ευθύς παρακάτω, ή άλλα, όπως τα αμφιλεγόμενα RFID συστήματα[481]), αποτρέπεται σε σημαντικό βαθμό η επιτόπου δράση κακόβουλων οντοτήτων με σκοπό π.χ. την μόλυνση με ιούς ή την έγχυση κάποιου σκουληκιού.

4.6.2 Βιομετρικά συστήματα αυθεντικοποίησης, εξουσιοδότησης και καταγραφής

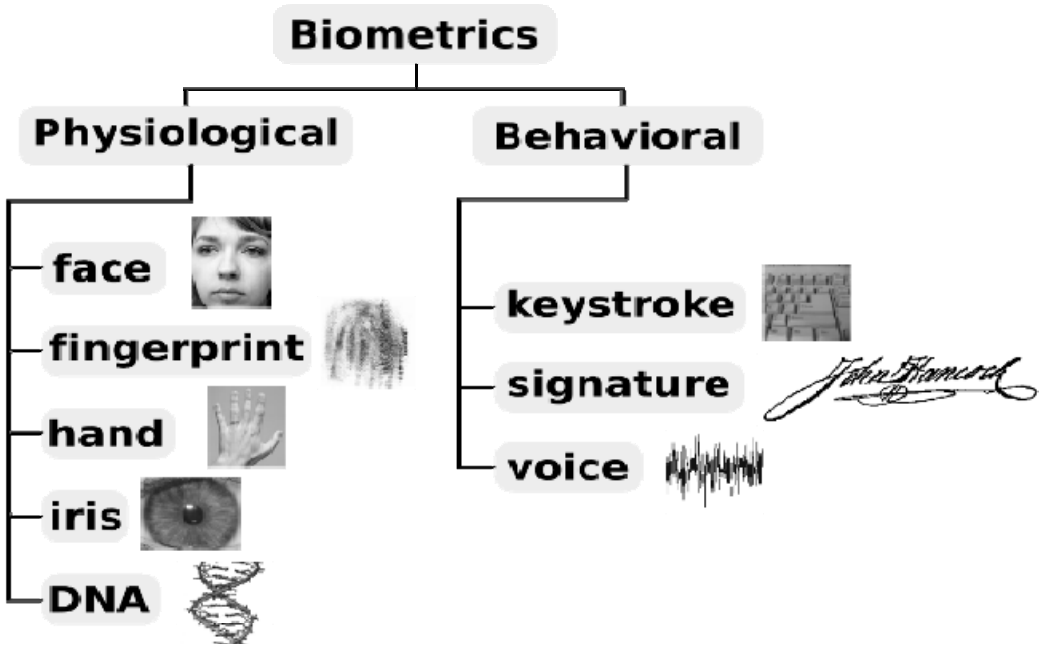
Η *βιομετρία ή τηλεβιομετρία* αφορά στη *"συλλογή και επεξεργασία ιδιοχαρακτηριστικών της ανθρώπινης φυσιολογίας ή συμπεριφοράς, με σκοπό την επαλήθευση της αυθεντικότητας ενός φυσικού προσώπου και τον συνακόλουθο έλεγχο των εξουσιοδοτήσεων αυτού"*[482].

---

[480] Πηγή: Διαδίκτυο, ιστοχώρος της online εγκυκλοπαίδειας WikiPedia, http://en.wikipedia.org/wiki/Access_control#Physical_access.

[481] Συζητώνται ως καινοτομία στην ασφάλεια στο εδάφιο 5.2.3 του Κεφαλαίου 5.

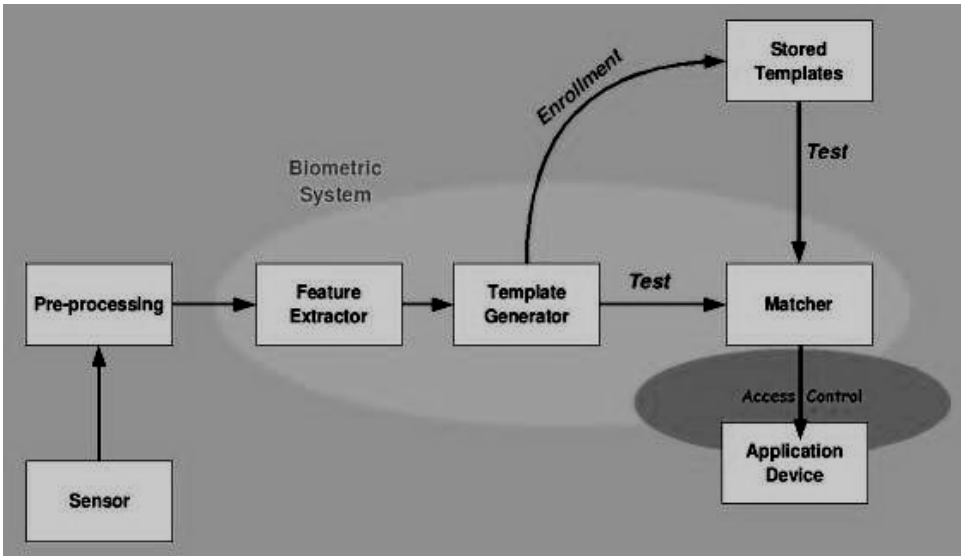
[482] Πηγή: Διαδίκτυο, ιστοχώρος της online εγκυκλοπαίδειας WikiPedia, http://en.wikipedia.org/wiki/Biometrics.



Σχήμα 30: Η οικογένεια των βιομετρικών μεθόδων ταυτοποίησης

Η χρήση των βιομετρικών συστημάτων στα σύγχρονα, δικτυοκεντρικά ΠΣ, σε συνδυασμό πάντα με τις πιο παραδοσιακές ΑΑΑ μεθόδους (π.χ. κωδικοί πρόσβασης, βάσεις δεδομένων εξουσιοδοτήσεων), μπορεί να δημιουργήσει ένα *ισχυρό πλέγμα προστασίας από κακόβουλες ενέργειες*. Ειδικά σε κρίσιμα σενάρια, όπως π.χ. η όπλιση πολεμικών όπλων ή η πρόσβαση σε άκρως απόρρητες πληροφορίες ή ακόμα-ακόμα η είσοδος σε κτίρια ή/και χώρους υψηλού κινδύνου κ.ό.κ., η βιομετρία μπορεί να καταστήσει, σε πολλές περιπτώσεις, το συνηθισμένο, αυτοαναπαραγόμενο οπλολογισμικό ανίκανο να αποτελέσει από μόνο του, χωρίς δηλαδή την παράλληλη δράση κάποιας φυσικής, κακόβουλης οντότητας, σοβαρή απειλή. Στην ουσία, δημιουργείται *ένα επιπλέον επίπεδο ασφάλειας, που προσαρτάται σε μια πλήρως αυτοματοποιημένη και προγραμματίσιμη ΑΑΑ δραστηριότητα*, διευρύνοντάς την με την προσθήκη και του καθαρά ανθρώπινου στοιχείου της -διαμέσω ειδοποιών ιδιοχαρακτηριστικών- θετικής, μοναδικής ταυτοποίησης της φυσικής οντότητας[483], που υπό κανονικές συνθήκες δεν μπορεί να γίνει με αυτόματο, μηχανιστικό τρόπο, αλλά μόνο κατόπιν εξέτασης και εξακρίβωσης της αυθεντικότητας, νομιμότητας και καταλληλότητας του φυσικού υποκειμένου που επιθυμεί την πρόσβαση.

[483] Κύρια, βιβλιογραφική αναφορά: [LEHTINEN-CSB].



Σχήμα 31: Η λειτουργία ενός βιομετρικού συστήματος

Βέβαια, και τα ίδια τα βιομετρικά συστήματα, ακριβώς επειδή βασίζονται στο λογισμικό και ελέγχονται από αυτό, φέρουν θεωρητικά όλες τις πιθανές αδυναμίες, που αυτό μπορεί να έχει, με αποτέλεσμα είτε να μπορούν να παρακαμφθούν/παραπλανηθούν (bypass/deception) είτε να υπονομευθούν (subversion), απειλώντας πολλές φορές έτσι να δημιουργήσουν νέες εστίες κινδύνου για τον οργανισμό που προστατεύουν, αν π.χ. τελικά λειτουργήσουν προς όφελος μιας κακόβουλης οντότητας (άρνηση εξυπηρέτησης, επηρεασμός/αποκλεισμός νόμιμων χρηστών και δραστηριοτήτων, πλαστοπροσωπία & υπόδυση ρόλων)[484]. Ειδικά σχεδιασμένοι ιοί και σκουλήκια μπορούν να στοχεύουν στο να ρετρο-αχρηστεύουν ή να ξεγελούν ή να χειραγωγούν τα συστήματα αυτά εκμεταλλευόμενοι (-α) τις διάφορες τεχνικές ατέλειες ή παραλείψεις ή ευπάθειες τους. Αποδεικνύεται, λοιπόν ξανά, και μάλιστα με περίτρανο τρόπο, πως οι όποιες νέες προσθήκες στα υπάρχοντα συστήματα ασφάλειας, αν και καλοδεχούμενες, πρέπει να γίνονται με γνώμονα την περαιτέρω μείωση του κινδύνου και όχι τη μετατόπισή του σε καινούρια, ανεξερεύνητα πεδία. Για την αποφυγή τέτοιων εφιαλτικών σκηνικών είναι σημαντική και συχνά επιβεβλημένη η υποβοήθηση της βιομετρικής αναγνώρισης μέσω *επίβλεψης και επαλήθευσης της σωστής δράσης των εν λόγω συστημάτων από ανθρώπους*-χειριστές (όπως άλλωστε συμβαίνει και για τα συστήματα ελέγχου φυσικής πρόσβασης και παρακολούθησης ανθρώπινης δραστηριότητας, που εξετάστηκαν ακριβώς παραπάνω). Για μια ακόμη φορά, ένα σκαλοπάτι ανθρώπινου ελέγχου σε κάποια κατά τα άλλα σχετικά αυτοματοποιημένη διαδικασία μπορεί να λειτουργήσει εξαιρετικά προστατευτικά ενάντια στις κακόβουλες δράσεις, αν και εφόσον φυσικά τα εμπλεκόμενα άτομα δρουν ευσυνείδητα και περιορίζουν στο ελάχιστο τις πιθανότητες ανθρώπινου λάθους.

---

[484] Κύρια, βιβλιογραφική αναφορά: [TAKASHI-ISVSPSVTBBA].

4.7 Νομικό Πλαίσιο

Αν και η συγκεκριμένη εργασία δε θα σταθεί εξονυχιστικά στις νομικές λεπτομέρειες που διέπουν τη συγγραφή, διάθεση και χρησιμοποίηση κακόβουλου λογισμικού για την εκδήλωση πληροφοριακών επιθέσεων, η παρούσα μελέτη θα ήταν ελλιπής, χωρίς μια σύντομη περιγραφή της λογικής που χαρακτηρίζει το κάθε εν λόγω θεσμικό πλαίσιο, της παρουσίας και εφαρμογής του σε παγκόσμιο επίπεδο (π.χ. ποιες χώρες διαθέτουν ξεκάθαρες, συντεταγμένες πολιτικές, ποιοι οργανισμοί συντονίζουν και ρυθμίζουν τις κατάλληλες δράσεις) και της αποτελεσματικότητας που αυτό εμφανίζει.

Ο *αυξανόμενος κίνδυνος από τα εγκλήματα που διαπράττονται ενάντια στους υπολογιστές*, ή ενάντια στις πληροφορίες των υπολογιστών, αρχίζει να κερδίζει την προσοχή σε εθνικό και σε οικουμενικό επίπεδο. Σε πολλές χώρες σε όλο τον κόσμο, εντούτοις, οι υφιστάμενοι νόμοι είναι πιθανό να παραμένουν ανενεργοί/ανεφάρμοστοι ενάντια σε τέτοια εγκλήματα. Αυτή η έλλειψη νομικής προστασίας σημαίνει ότι επιχειρήσεις και κυβερνήσεις πρέπει να στηρίζονται, σε μεγάλο βαθμό, κυρίως στα δικά τους τεχνικά μέτρα για να προστατευθούν από εκείνους που θα έκλεβαν, θα αρνούνταν την πρόσβαση, ή θα κατέστρεφαν τις πολύτιμες πληροφορίες τους.

Η *ανάγκη για μελετημένες, νομικές δράσεις και παρεμβάσεις για την κυβερνοασφάλεια και μάλιστα σε υπερεθνικό επίπεδο* κορυφώνεται, καθώς με μεγάλο ρυθμό σήμερα διάφοροι επιτήδειοι, με (ή χωρίς) τη βοήθεια και του κακόβουλου λογισμικού, θέτουν σε σοβαρή διακύβευση, όπως είδαμε, τις πληροφοριακές υποδομές χρηστών, οργανισμών και κρατών ή διαπράττουν άλλα ειδεχθή εγκλήματα (παιδική πορνογραφία) και παρανομίες (πνευματικά δικαιώματα, παρεμπόριο).

Όπως και να ’χει, είναι γενικά αποδεκτό πως η παρουσία διεθνώς αναγνωρισμένων, δυναμικών, θεσμοθετημένων κανόνων αποτελεί μια ουσιαστική εγγύηση προστασίας από πληροφοριακές επιθέσεις με αυτοαναπαραγόμενο, επιβλαβές λογισμικό και από άλλα υστερόβουλα ηλεκτρονικά εγκλήματα, καθώς μπορεί να δράσει παραδειγματικά σε πράξεις και ανασταλτικά σε φιλοδοξίες των κακοποιών.

4.7.1 Ουσία του Νόμου

Στην παγκόσμια νομοθεσία, η δεσπόζουσα, σχετική μορφή για κακόβουλη-παράνομη ηλεκτρονική δραστηριότητα είναι το *κυβερνοέγκλημα ή η-έγκλημα*[485]. Η έννοια του κυβερνοεγκλήματος ή ηλεκτρονικού εγκλήματος είναι στενά συναφής με αυτής της πληροφοριακής εχθροπραξίας, που μελετά η παρούσα εργασία. Στην ουσία αποτελεί ένα *υπερσύνολο της εχθροπραξίας* με την προσθήκη και των πλαισίων της παιδικής πορνογραφίας, του πάσης φύσεως παρεμπορίου και της καταπάτησης των πνευματικών δικαιωμάτων (π.χ. μέσω πειρατείας). Το κυβερνοέγκλημα, λοιπόν, περιλαμβάνει τις ακόλουθες (υστερόβουλες) πράξεις, που αφορούν το πεδίο και τα μέσα πληροφορικής τεχνολογίας:[486]

1. Μη εξουσιοδοτημένη ή παράνομη πρόσβαση
2. Παράνομη παρακολούθηση/Υποκλοπή επικοινωνιών
3. Κακόβουλη παρεμβολή σε δεδομένα και λειτουργίες συστημάτων
4. Πρόκληση υλικών βλαβών (σε ΠΣ)
5. Πλαστογραφία/Πλαστοπροσωπία
6. Εξαπάτηση/Δυσφήμηση
7. Παιδική πορνογραφία
8. Καταπάτηση πνευματικών δικαιωμάτων
9. Παρεμπόριο
10. Τρομοκρατία

Στα πλαίσια επιθέσεων κακόβουλου λογισμικού, και οι 10 παραπάνω αιτιάσεις ηλεκτρονικού εγκλήματος είναι εφικτές, αν και μόνο οι περιπτώσεις 1-6 και 10 αφορούν την τρέχουσα έρευνα καθώς συνιστούν ξεκάθαρη, πληροφοριακή εχθροπραξία, όπως αυτή ορίστηκε και περιγράφηκε καθ' όλη τη διπλωματική εργασία.

Στόχος των κείμενων και μελλοντικών νόμων είναι η θεσμική υποστήριξη ανθρώπων, οργανισμών και κρατών στην πρόληψη και καταδίκη παρόμοιας σε βάρους τους παραβατικότητας με την παροχή των μέτρων και προϋποθέσεων για την επιβολή κατάλληλων αντιποίνων (αποζημίωση, πρόστιμο, κοινωνική εργασία, φυλάκιση), πολλές φορές

---

[485] Πηγή: Διαδίκτυο, ιστοχώρος της online εγκυκλοπαίδειας WikiPedia, http://en.wikipedia.org/wiki/Cybercrime.

[486] Πηγή: "CYBER CRIME", Pati Parthasarathi, 2003, διαθέσιμο από το δεσμό http://www.naavi.org/pati/pati_cybercrimes_dec03.htm.

παραδειγματικής/αποτρεπτικής φύσεως, στην προκαλούσα οντότητα, λαμβάνοντας πάντοτε υπόψιν καθοριστικούς παράγοντες εξέλιξης του εγκλήματος (προφίλ δραστών, μέγεθος αντίκτυπου) και διαφυλάσσοντας παράλληλα την επικυριαρχία βασικών δικαιωμάτων[487] και λοιπών, νομικών υποχρεώσεων και τη μη αντίβαση/αντίφαση αναμεταξύ τους.

4.7.2 Σύντομη εξιστόρηση της νομοθεσίας ενάντια στο η-έγκλημα

Η πρώτη, ουσιαστική πρωτοβουλία κόντρα στο έγκλημα διαμέσω και κατά υπολογιστικών συστημάτων ήταν μια μελέτη από την Επιτροπή κυβερνητικών διαδικασιών της Συγκλήτου των ΗΠΑ (U.S. Senate Committee on Government Operations), που διενεργήθηκε το Φεβρουάριο του 1977.[488] Αυτή η μελέτη εξέτασε διάφορα προβλήματα που συνδέθηκαν με τα προγράμματα υπολογιστών, και σύστησε ότι η νομοθεσία πρέπει να εξεταστεί που θα απαγόρευε την αναρμόδια χρήση των υπολογιστών. Ο πρόεδρος αυτής της επιτροπής ήταν ο γερουσιαστής Abe Ribicoff. Ο γερουσιαστής Ribicoff ήταν αυτό που στα τέλη του 1977 παρουσίασε και το περιβόητο νομοσχέδιο Ribicoff.

Σουηδία

Η σοσιαλιστική διακυβέρνηση της Σουηδίας πρώτευσε (1973) στο να θεσπίσει δράσεις προστασίας δεδομένων προκειμένου να ρυθμιστούν κανονιστικά η συλλογή, συντήρηση, χρήση και διάδοση προσωπικών δεδομένων (στο σουηδικό νόμο του 1973 για τα δεδομένα, η παράγραφός 21 προέβλεπε προστασία ενάντια στην αναρμόδια πρόσβαση σε όλες τις κατηγορίες δεδομένων).

Το Ribicoff Bill

Αυτό το σχέδιο νόμου ήταν η πρώτη πρόταση στις ΗΠΑ για ομοσπονδιακή νομοθεσία κατά του εγκλήματος μέσω και εναντίον υπολογιστών που συγκεκριμένα θα απαγόρευε την κακόβουλη χρήση των υπολογιστών. Το υπ. αριθμ. S. 1766 (95ο Κογκρέσο) νομοσχέδιο ονομάστηκε "Ομοσπονδιακή δράση προστασίας υπολογιστικών συστημάτων του 1977"[489], αλλά έμεινε ευρύτερο γνωστό με το όνομα του γερουσιαστή που το εμπνεύστηκε και υποστήριξε. Το νομοσχέδιο τελικά δεν υιοθετήθηκε, αλλά αυτή η εντυπωσιακά πρωτοποριακή πρόταση έγινε πρότυπο μοντέλο για νομοθεσία κυβερνοεγκλήματος στις

[487] Ανθρώπινων, αλλά και επιχειρησιακών/εταιρικών και ευρύτερων, κοινωνικών ομάδων, κρατών και διακρατικών ενώσεων.

[488] Κύρια, βιβλιογραφική αναφορά: [SCHJOLBERG_HUBBARD-HNLAC].

[489] Πηγή: "The Omnibus Antiterrorism Act", Samuel Francis, 1978, διαθέσιμο από το δεσμό http://www.heritage.org/Research/Crime/IB34.cfm.

Ηνωμένες Πολιτείες και προκάλεσε παράλληλη, ακόμη μεγαλύτερη, διεθνή συνειδητοποίηση και ευαισθητοποίηση επί του θέματος.

INTERPOL

Η INTERPOL ήταν ο πρώτος διεθνής οργανισμός που ασχολήθηκε ενεργά με το κυβερνοέγκλημα και την ποινική δικονομία. Στη διάρκεια μιας διάσκεψης της INTERPOL το 1981, ανακοινώθηκε μια έρευνα που πραγματοποιήθηκε στις χώρες-μέλη της INTERPOL για το έγκλημα μέσω και κατά υπολογιστών και την κείμενη, ποινική νομοθεσία τους και προσδιόρισε διάφορα προβλήματα στην εφαρμογή του υπάρχοντος θεσμικού πλαισίου επισημαίνοντας πληθώρα ελλείψεων.

ΟΟΣΑ

Ο ΟΟΣΑ διόρισε το 1983 στο Παρίσι μια ειδική επιτροπή για να συζητήσει το σχετικό με υπολογιστές έγκλημα και την ανάγκη για αλλαγές στους ποινικούς κώδικες.[490] Αυτή η επιτροπή προέβη σε μια πρόταση που θα μπορούσε να αποτελέσει τον κοινό παρονομαστή μεταξύ των διαφορετικών μεθόδων που θα υιοθετούνταν από τις χώρες-μέλη του.

Το Ευρωπαϊκό Συμβούλιο (CoE)

Το Ευρωπαϊκό Συμβούλιο διόρισε το 1985 μια άλλη επιτροπή εμπειρογνωμόνων, προκειμένου να συζητηθούν τα νομικά ζητήματα του σχετικού με υπολογιστές εγκλήματος. Μια περίληψη των οδηγιών προς τα εθνικά νομοθετικά σώματα με πρόταση για εμπλοκή ευθυνών για τις σκόπιμες πράξεις και μόνο, παρουσιάστηκε στη Σύσταση του 1989 (1989 E.C. Recommendation)[491].

Ο Οργανισμός Ηνωμένων Εθνών (Ο.Η.Ε.)

Τα Η.Ε. ενέκριναν ένα ψήφισμα σχετικά με τη νομοθεσία ηλεκτρονικού εγκλήματος στο 8ο συνέδριο των Η.Ε., που είχε κεντρικό θέμα την πρόληψη του εγκλήματος και τη μεταχείριση των παραβατών στην Αβάνα της Κούβα, το 1990 (8th Congress on the Prevention of Crime and the Treatment of Offenders in Havana, Cuba).[492] Το σχετικό εγχειρίδιο των Ηνωμένων

[490] Πηγή: "The Legal Framework - Unauthorized Access To Computer Systems: Penal Legislation In 44 Countries", Stein Schjolberg, 2003, διαθέσιμο από το δεσμό http://www.mosstingrett.no/info/legal.html.

[491] Κύρια, βιβλιογραφική αναφορά: [SCHJOLBERG_HUBBARD-HNLAC].

[492] Το υλικό του συνεδρίου έχει αναρτηθεί και δημοσιεύεται στον ιστοχώρο της Αμερικανικής Εγκληματολογικής Ένωσης (American Society of Criminology), http://www.asc41.com/8th%20UN%20Congress%20on%20the%20Prevention%20of%20Crime/8th_congress.htm.

Εθνών για την πρόληψη και τον έλεγχο του κυβερνοεγκλήματος δημοσιεύθηκε τελικά το 1994.

Οι διασκέψεις του Wurzburg

Ως τελευταίο μέρος αυτής της ιστορικής αναδρομής αναφέρουμε τις διασκέψεις του Wurzburg, που οργανώθηκαν από το πανεπιστήμιο του Wurzburg (Γερμανία) το 1992.[493] Αυτές οι διασκέψεις οδήγησαν σε 29 εθνικές εκθέσεις, και συστάσεις, για την ανάπτυξη των ιδιαίτερων, νομοθετικών πλαισίων του κυβερνοεγκλήματος.

Οι περισσότερες χώρες στην Ευρώπη ενέκριναν και τροποποίησαν νέους ποινικούς νόμους σύμφωνα με τις εκάστοτε συστάσεις στις δεκαετίες του '80 και ’90. Παρόμοια εξέλιξη εμφανίστηκε και στις ΗΠΑ, τον Καναδά και το Μεξικό· επίσης, στην Ασία, όπου η Ιαπωνία, η Σιγκαπούρη, η Νότιος Κορέα και η Μαλαισία υπήρξαν οι πρώτες, καινοτομικές χώρες. Στην Αυστραλία, τέλος, η Κοινοπολιτεία πρόσθεσε νόμους κατά του εγκλήματος μέσω και εναντίον υπολογιστών στη δράση κατά εγκλημάτων του 1989 (Australian Crimes Act, 1989).

4.7.3 Σύγχρονη διεθνής παρουσία και ισχύς

Σήμερα, διαπιστώνεται μια εκτεταμένη προσπάθεια να θεσμοθετηθούν, εκ νέου, διεθνείς και μοντέρνοι κανόνες και να γεφυρωθούν τα όποια, νομικά χάσματα μεταξύ των χωρών στο θέμα της κυβερνοασφάλειας και του η-εγκλήματος.

Παρακάτω, συνοψίζονται οι επίκαιρες δράσεις συγκεκριμένων φορέων, που πιστοποιούν την προλεγόμενη κλιμάκωση των συνομιλιών και θέρμανση της συνεργασίας μεταξύ των κρατών σε αυτά τα άκρως σημαντικά θέματα.

CoE 2001 Convention on Cybercrime

Η Συνθήκη του 2001 του Ευρωπαϊκού Συμβουλίου σχετικά με το κυβερνοέγκλημα είναι ένα ιστορικό σημείο αναφοράς στον αγώνα παροχής της απαραίτητης νομικής προστασίας και έχει συναντήσει την ευρύτατη αποδοχή της παγκόσμιας κοινότητας, σε κρατικό τουλάχιστον επίπεδο.[494]

---

[493] Κύρια, βιβλιογραφική αναφορά: [SCHJOLBERG_HUBBARD-HNLAC].

[494] Ολόκληρο το κείμενο της συνθήκης βρίσκεται στον ιστοχώρο του Συμβουλίου της Ευρώπης, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

Το Συμβούλιο της Ευρώπης καθιέρωσε μια επιτροπή εμπειρογνωμόνων για το έγκλημα στον κυβερνοχώρο το 1997. Η επιτροπή αυτή εκπόνησε μια πρωτότυπη πρόταση για μια Συνθήκη σχετικά με το ηλεκτρονικό έγκλημα και η συνθήκη αυτή υιοθετήθηκε και ανοίχτηκε για υπογραφές σε μια διάσκεψη στη Βουδαπέστη (Ουγγαρία), το 2001, στα πλαίσια του Ευρωπαϊκού Συμβουλίου. Η συνθήκη τέθηκε σε ισχύ την 1η Ιουλίου του 2004.

Με την επικύρωση ή την αποδοχή τμήματος της Cybercrime Convention του Συμβουλίου της Ευρώπης ή την εφαρμογή των αρχών της, τα κράτη συμφωνούν να εξασφαλίσουν ότι οι εσωτερικοί τους νόμοι (εντός του αμιγούς, ουσιαστικού ποινικού δικαίου) ποινικοποιούν τις παραβατικές συμπεριφορές, που περιγράφονται στη συνθήκη, και καθιερώνουν τα αναγκαία, διαδικαστικά εργαλεία, για να ερευνήσουν και να διώξουν ποινικώς τέτοια εγκλήματα. Αυτό συνιστά μια πρώτη εναρμόνιση των εθνικών, νομικών προσεγγίσεων στο κοινό, φλέγον θέμα του κυβερνοεγκλήματος.

Από τον Φεβρουάριο του 2007, ο συνολικός αριθμός υπογραφών χωρών που δεν ευόδωσαν ακόμη σε νομοθετικές μεταρρυθμίσεις είναι 22 (ανάμεσα τους και η Ελλάδα). Ο συνολικός αριθμός πρακτικών επικυρώσεων της συνθήκης από υπογράφουσες χώρες είναι 21.

Τα κράτη μέλη εντός εύλογου χρονικού διαστήματος πρέπει να ολοκληρώσουν την επικύρωση της συνθήκης ενώ και τα άλλα κράτη καλό θα ήταν να εξετάσουν τις δυνατότητές ή να αξιολογήσουν τη σκοπιμότητα των αρχών της. Με τη Συνθήκη του 2001 του Συμβουλίου της Ευρώπης, αλλά και τις παρόμοιες, ιδιαίτερες συστάσεις από τον Ο.Η.Ε. και τους οργανισμούς G8, OAS και APEC, μπορούμε να ευελπιστούμε στο στόχο ενός οικουμενικού, νομικού πλαισίου ενάντια στο ηλεκτρονικό έγκλημα.

Ηνωμένη Έθνη

Ένα ψήφισμα σχετικά με την καταπολέμηση της εγκληματικής χρήσης των πληροφοριακών τεχνολογιών εγκρίθηκε από τη γενική συνέλευση στις 4 Δεκεμβρίου του 2000 (A/res/55/63), συμπεριλαμβανομένων των εξής σημαντικών σημείων:[495]

"(α) τα κράτη πρέπει να εξασφαλίσουν ότι οι νόμοι και η πρακτική τους εξαφανίζουν τα όποια ασφαλή καταλύματα για όσους πραγματοποιούν ποινικά κολάσιμες χρήσεις της πληροφοριακής τεχνολογίας.

…… ……. …….

[495] Κύρια, βιβλιογραφική αναφορά: [UN55_63-2001].

(ε) Τα νομικά συστήματα πρέπει να προστατεύουν την εμπιστευτικότητα, την ακεραιότητα, και τη διαθεσιμότητα δεδομένων και υπολογιστικών συστημάτων από αναρμόδια εξασθένηση και να εξασφαλίσουν ότι η εγκληματική κατάχρηση τιμωρείται ποινικά."

Ευρωπαϊκή Ένωση (E.U.)

Στην Ευρωπαϊκή Ένωση, η Επιτροπή των Ευρωπαϊκών Κοινοτήτων (Κομισιόν) κατέθεσε στις 19 Απριλίου 2002 ενώπιον του Ευρωπαϊκού Συμβουλίου μια πρόταση για κοινοτικού πλαισίου απόφαση (Council Framework Decision), σχετικά με τις επιθέσεις ενάντια σε συστήματα πληροφοριών. Η πρόταση εγκρίθηκε από το Συμβούλιο στις 27 Φεβρουαρίου 2003 και περιλαμβάνει τα Άρθρο 2: Παράνομη πρόσβαση στα συστήματα πληροφοριών, Άρθρο 3: Παράνομη παρέμβαση σε συστήματα και Άρθρο 4: Παράνομη παρέμβαση σε δεδομένα:[496]

- Άρθρο 2-παράνομη πρόσβαση στα συστήματα πληροφοριών

  1. Κάθε κράτος μέλος θα λάβει τα απαραίτητα μέτρα για να εξασφαλίσει ότι η σκόπιμη και χωρίς δικαίωμα πρόσβαση στο σύνολο ή οποιοδήποτε μέρος ενός συστήματος πληροφοριών είναι τιμωρητέα ως ποινικό αδίκημα, τουλάχιστον για τις περιπτώσεις που δε θεωρούνται πταίσματα.

  2. Κάθε κράτος-μέλος μπορεί να αποφασίσει ότι η συμπεριφορά που αναφέρεται στην παράγραφο 1 ενοχοποιείται μόνο όπου η παρατυπία σημειώνεται με την παραβίαση κάποιου υπάρχοντος μέτρου ασφάλειας.

- Άρθρο 3-παράνομη παρέμβαση στα συστήματα.

  Κάθε κράτος-μέλος θα λάβει τα απαραίτητα μέτρα για να εξασφαλιστεί ότι σκόπιμη σοβαρή παρεμπόδιση ή διακοπή της λειτουργίας ενός συστήματος πληροφοριών με την εισαγωγή, διαβίβαση, καταστροφή, διαγραφή, επιδείνωση, αλλαγή, καταστολή ή μετατροπή σε απρόσιτων των δεδομένων υπολογιστών είναι κολάσιμη ως ποινικό αδίκημα όταν εκτελείται χωρίς δικαίωμα, τουλάχιστον για περιπτώσεις που δε θεωρούνται πταίσματα.

- Άρθρο 4-παράνομη παρέμβαση στα δεδομένα

  Κάθε κράτος-μέλος θα λάβει τα απαραίτητα μέτρα για να εξασφαλιστεί ότι σκόπιμη διαγραφή, καταστροφή, επιδείνωση, αλλαγή, καταστολή ή μετατροπή σε απρόσιτων των δεδομένων των υπολογιστών σε κάποιο σύστημα πληροφοριών είναι κολάσιμη

[496] Κύρια, βιβλιογραφική αναφορά: [SCHJOLBERG_HUBBARD-HNLAC].

ως ποινικό αδίκημα, όταν εκτελείται χωρίς δικαίωμα, τουλάχιστον για τις περιπτώσεις που δε θεωρούνται πταίσματα.

Ένωση Κοινοπολιτείας Κρατών (Commonwealth Association)

Σε μια προσπάθεια να εναρμονιστεί το σχετικό με τα η-εγκλήματα ποινικό δίκαιο στα 53 κράτη-μέλη της Κοινοπολιτείας, ένας πρότυπος νόμος εγκρίθηκε βάσει της εργασίας της Συνθήκης του 2001 του Συμβουλίου της Ευρώπης για το Κυβερνοέγκλημα.[497] Ο πρότυπος, τούτος νόμος χρησιμεύει ως ένα παράδειγμα των κοινών αρχών και πρακτικών που κάθε κράτος-μέλος μπορεί να χρησιμοποιήσει, ώστε να υιοθετήσει θεσμικό, ρυθμιστικό πλαίσιο συμβατό με άλλα κράτη της Κοινοπολιτείας.

Οργανισμός αμερικανικών κρατών (OAS)

Οι Υπουργοί δικαιοσύνης ή άλλοι Υπουργοί και οι γενικοί εισαγγελείς των μελών στην οργάνωση των αμερικανικών κρατών (REMJA, OAS) συνέστησαν στο Περού το 1999 την καθιέρωση μιας ομάδας κυβερνητικών εμπειρογνωμόνων στο κυβερνοέγκλημα[498]. Σε μια συνεδρίαση στο Τρινιντάντ και Τομπάγκο το 2002 οι συστάσεις υιοθετήθηκαν, δίνοντας στην ομάδα εμπειρογνωμόνων την ακόλουθη εξουσιοδότηση:

"Να εξετάσει την προετοιμασία των σχετικών, διαμερικανικών, νομικών οργάνων και την πρότυπη νομοθεσία με σκοπό την ενίσχυση της ημισφαιρικής συνεργασίας στην καταπολέμηση του η-εγκλήματος, λαμβάνοντας υπόψιν πρότυπα σχετικά με την ιδιωτικότητα, την προστασία των πληροφοριών, τις διαδικαστικές πτυχές και την πρόληψη εγκλήματος".

Η εκτίμηση των συμπερασμάτων της ομάδας συζητήθηκε σε μια συνεδρίαση στην Ουάσιγκτον, στις 23-24 Ιουνίου του 2003.

Η πέμπτη συνεδρίαση των Υπουργών και των γενικών εισαγγελέων των χωρών του OAS στην Ουάσιγκτον τον Απρίλιο του 2004, ενέκρινε ορισμένα συμπεράσματα και συστάσεις προς τη γενική συνέλευση του OAS, συμπεριλαμβανομένων των εξής:[499]

"Πως τα κράτη μέλη θα αξιολογήσουν τη σκοπιμότητα των αρχών της Συνθήκης του Συμβουλίου της Ευρώπης σχετικά με το Κυβερνοέγκλημα (2001) και θα εξετάσουν τη δυνατότητα συμμετοχής στη σύμβαση αυτή."

---

[497] Όπως στην προηγούμενη υποσημείωση.

[498] Οι σχετικές λεπτομέρειες για τις δράσεις της εν λόγω ομάδας μπορούν να βρεθούν με επισκόπηση του ιστοχώρου της OAS, http://www.oas.org/juridico/english/cyber.htm.

[499] Τα πρακτικά όλων των σχετικών συνεδριάσεων των Υπουργών και των γενικών εισαγγελέων των χωρών του OAS είναι διαθέσιμα από τον ιστοχώρο του OAS, στη διεύθυνση http://www.oas.org/juridico/english/cyber_meet.htm.

Η γενική συνέλευση του OAS στη συνεδρίαση της 7 Ιουνίου 2005 ζήτησε από το μόνιμο Συμβούλιο να συγκαλέσει νέα συνεδρίαση της ομάδας κυβερνητικών εμπειρογνωμόνων στο κυβερνοέγκλημα.

Το μόνιμο Συμβούλιο του OAS αποφάσισε στις 15 Δεκεμβρίου 2005 πως η ομάδα των κυβερνητικών εμπειρογνωμόνων στο κυβερνοέγκλημα πρέπει να συναντηθεί στις 27-28 Φεβρουαρίου 2006, με σκοπό την πραγμάτωση των εξουσιοδοτήσεων που αναφέρονται στα συμπεράσματα και τις συστάσεις της πέμπτης συνεδρίασης των Υπουργών της δικαιοσύνης στις 28-30 Απριλίου του 2004.

Η ομάδα των κυβερνητικών εμπειρογνωμόνων στο κυβερνοέγκλημα συναντήθηκε στις 27-28 Φεβρουαρίου του 2006 στην Ουάσιγκτον. Η ημερήσια διάταξη περιέλαβε εκτός των άλλων:[500] «Προκλήσεις στην πρόσβαση, σύνταξη και τροποποίηση νομοθεσίας σύμφωνης με τις αρχές, και τον ουσιαστικό και διαδικαστικό νόμο της Συνθήκης του Συμβουλίου της Ευρώπης σχετικά με το Κυβερνοέγκλημα (2001)».

Στην έκτη συνεδρίαση των Υπουργών της δικαιοσύνης τον Ιούνιο του 2006 έγινε η εξής δήλωση:

"...να ενισχύσει τη συνεργασία με το Συμβούλιο της Ευρώπης, έτσι ώστε τα κράτη-μέλη του OAS μπορούν να προχωρήσουν στη σκέψη εφαρμογής των αρχών της Συνθήκης του 2001 του Συμβουλίου της Ευρώπης σχετικά με το κυβερνοέγκλημα και να δεχτούν επιπλέον να μελετήσουν την έγκριση των νομικών και άλλων μέτρων που απαιτούνται για την εφαρμογή της. Ομοίως, συνεχίζονται οι προσπάθειες που ενισχύουν τους μηχανισμούς για την ανταλλαγή των πληροφοριών και τη συνεργασία με άλλες διεθνείς οργανώσεις και αντιπροσωπείες στον τομέα του κυβερνοεγκλήματος, όπως τα Ηνωμένα Έθνη, η Ευρωπαϊκή Ένωση, το φόρουμ οικονομικής συνεργασίας των ασιατικών χωρών του Ειρηνικού, ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ), η G-8, η Κοινοπολιτεία και η INTERPOL, ώστε τα κράτη-μέλη OAS να επωφελούνται από την πρόοδο που σημειώνεται σε αυτές τις ομάδες."

Η ομάδα χωρών G8

Τα κράτη-μέλη του G8 (Η.Π.Α., Καναδάς, Ηνωμένο Βασίλειο, Γαλλία, Ιταλία, Γερμανία, Ρωσία, Ιαπωνία) καθιέρωσαν το 1997 την υποομάδα εγκλήματος υψηλής τεχνολογίας (hi-tech crime subgroup).[501] Σε μια συνεδρίαση στην Ουάσιγκτον το 1997, οι χώρες του G8 υιοθέτησαν δέκα, θεμελιώδεις αρχές στον αγώνα ενάντια στο η-έγκλημα. Ο στόχος ήταν να

[500] Το υλικό όλων των συναντήσεων της ομάδας των ειδικών βρίσκεται αναρτημένο στον ιστοχώρο του OAS, http://www.oas.org/juridico/english/cyber_experts.htm.

[501] Κύρια, βιβλιογραφική αναφορά: [SCHJOLBERG_HUBBARD-HNLAC].

εξασφαλιστεί ότι κανένας κυβερνοεγκληματίας δε θα λαμβάνει νομικό καταφύγιο οπουδήποτε στον κόσμο.

Στη συνεδρίαση των Υπουργών δικαιοσύνης και εσωτερικών του G-8 στην Ουάσιγκτον, που έλαβε χώρα το Μάιο του 2004 εκδόθηκε ένα κοινό ανακοινωθέν ως εξής:[502]

"Συνεχίζουμε να ενισχύουμε τους εσωτερικούς νόμους. Για να δημιουργηθούν πραγματικές παγκόσμιες δυνατότητες καταπολέμησης των τρομοκρατικών και άλλων εγκληματικών χρήσεων του Διαδικτύου, όλες οι χώρες πρέπει να συνεχίσουν να βελτιώνουν τους νόμους, που ποινικοποιούν τις υστερόβουλες χρήσεις των δικτύων υπολογιστών και που επιτρέπουν ταχύτερη συνεργασία στις δικαστικές έρευνες σχετικά με το Διαδίκτυο. Με τη Συνθήκη του Συμβουλίου της Ευρώπης σχετικά με το Κυβερνοέγκλημα, που τίθεται σε ισχύ την 1η Ιουλίου του 2004, πρέπει να λάβουμε μέτρα για να ενθαρρύνουμε τη θέσπιση των νομικών προτύπων που περιέχει σε πιο ευρεία βάση".

Σε μια δήλωση από τη συνεδρίαση της G8 του 2005 δόθηκε, επίσης, έμφαση στο σημαντικό στόχο της γρήγορης και αποτελεσματικής ανταπόκρισης των οργάνων επιβολής του νόμου σε σοβαρές κυβερνοαπειλές και κρίσιμα γεγονότα.

Τέλος, στη συνεδρίαση της Μόσχας το 2006 οι Υπουργοί δικαιοσύνης και εσωτερικών των χωρών-μελών συζήτησαν τα ζητήματα εγκλημάτων του κυβερνοχώρου. Σε ένα απόσπασμα αναφέρεται:[503]

"Συζητήσαμε επίσης τα ζητήματα σχετικά με τη διανομή της συσσωρευμένης, διεθνούς εμπειρίας στην καταπολέμηση της τρομοκρατίας, καθώς επίσης και τη συγκριτική ανάλυση των σχετικών κομματιών της νομοθεσίας στο θέμα αυτό. Συζητήσαμε την ανάγκη για αποτελεσματικά αντίμετρα που θα αποτρέψουν τις πράξεις κυβερνοτρομοκρατίας στην σφαίρα των υψηλών τεχνολογιών. Για αυτό, είναι απαραίτητο να εφεύρουμε ένα σύνολο μέτρων για να αποτραπούν τέτοιες πιθανές εγκληματικές πράξεις, που περιλαμβάνουν τον τομέα των τηλεπικοινωνιών. Αυτό εμπλέκει και εργασία ενάντια στην πώληση των ιδιωτικών δεδομένων, την πλαστογράφηση πληροφοριών και την εφαρμογή ιών και άλλων επιβλαβών προγραμμάτων υπολογιστών. Θα καθοδηγήσουμε τους εμπειρογνώμονές μας για να παραγάγουμε ενοποιημένες προσεγγίσεις στην πάλη κατά της ηλεκτρονικής εγκληματικότητας και θα χρειαστούμε μια διεθνή νομική βάση για αυτήν την ιδιαίτερη εργασία· και θα εφαρμόσουμε όλα αυτά ώστε να αποτρέψουμε τους τρομοκράτες από τη

---

[502] Υπάρχει ειδικά αφιερωμένος ιστοχώρος για τη συγκεκριμένη συνεδρίαση, που είναι προσπελάσιμος διαμέσω της ηλεκτρονικής διεύθυνσης http://www.usdoj.gov/ag/events/g82004/index.html του Αμερικανικού Υπουργείου Δικαιοσύνης.

[503] Η συνέντευξη τύπου της διϋπουργικής συνεδρίασης είναι διαθέσιμη μέσω του επίσημου ιστοχώρου της G8, στη σελίδα http://www.g7.utoronto.ca/justice/justice2006.htm.

χρησιμοποίηση του υπολογιστή και των χώρων του Διαδικτύου για τη μίσθωση νέων τρομοκρατών και τη στρατολόγηση άλλων παράνομων δραστών."

Οργανισμός οικονομικής συνεργασίας ασιατικών χωρών του Ειρηνικού (APEC)

Οι Υπουργοί και οι ηγέτες του οργανισμού οικονομικής συνεργασίας των ασιατικών χωρών του Ειρηνικού (APEC) δεσμεύτηκαν σε μια συνεδρίαση του 2002 για:[504]

"Προσπάθεια για θέσπιση μέχρι τον Οκτώβριο του 2003 ενός περιεκτικού συνόλου εμπεριστατωμένων νόμων σχετικά με την κυβερνοασφάλεια και το κυβερνοέγκλημα, που να είναι σύμφωνοι με οδηγίες διεθνών νομικών οργάνων, συμπεριλαμβανομένου του ψηφίσματος της γενικής συνέλευσης των Ηνωμένων Εθνών 55/63 (2000) και της Συνθήκης του Ε.Σ. σχετικά με το Κυβερνοέγκλημα (2001)".

Το 2003 δημιουργήθηκε ειδικό πρόγραμμα για την ενίσχυση των υποδομών κατάστρωσης και επιβολής νομοθεσίας σχετικής με το κυβερνοέγκλημα (γνωστή ως πρωτοβουλία e-Security Task Group της ειδικής ομάδας εργασίας πληροφορικής και τηλεπικοινωνιών (TEL) του APEC).

Στη συνεδρίαση της ομάδας τηλεπικοινωνιών και πληροφορικής του APEC στις 7-9 Σεπτεμβρίου 2005, στη Σεούλ της Ν. Κορέας, ακούστηκαν τα εξής:[505]

"Οι οικονομίες θεσπίζουν και εφαρμόζουν αυτήν την περίοδο νόμους για την κυβερνοασφάλεια, σύμφωνους με το ψήφισμα της γενικής συνέλευσης των Ηνωμένων Εθνών 55/63 (2000) και της Συνθήκης του Ε.Σ. σχετικά με το Κυβερνοέγκλημα (2001). Το πρόγραμμα TEL ενίσχυσης υποδομών κατάστρωσης και επιβολής νομοθεσίας σχετικής με το κυβερνοέγκλημα θα υποστηρίξει τα αρχές και τα όργανα ώστε να εφαρμόσουν τους νέους νόμους".

Στην διϋπουργική συνεδρίαση του Νοέμβριο του 2005, οι Υπουργοί ανανέωσαν την υποχρέωσή τους δηλώνοντας:[506]

"Ενθαρρύνοντας όλες τις οικονομίες να μελετήσουν τη Συνθήκη σχετικά με το Κυβερνοέγκλημα (Ε.Σ., 2001) και να προσπαθήσουν να θεσπίσουν ένα περιεκτικό σύνολο εμπεριστατωμένων νόμων σχετικά με την κυβερνοασφάλεια και το κυβερνοέγκλημα, που να είναι σύμφωνοι με διεθνή νομικά όργανα, συμπεριλαμβανομένου του ψηφίσματος της γενικής συνέλευσης των Ηνωμένων Εθνών 55/63 (2000) και της Συνθήκης του Ε.Σ. σχετικά με το Κυβερνοέγκλημα (2001)…".

---

[504] Κύρια, βιβλιογραφική αναφορά: [APEC-2002].

[505] Κύρια, βιβλιογραφική αναφορά: [APEC-2005].

[506] Πηγή: Διαδίκτυο, ιστοχώρος της οργάνωσης APEC, http://www.apec.org/content/apec/ministerial_statements/sectoral_ministerial/telecommunications/2005.html.

Ένωση Χωρών Νοτιοανατολικής Ασίας (ASEAN)

Η Ένωση των Χωρών Νοτιοανατολικής Ασίας (ASEAN) έχει καθιερώσει μια υψηλού επιπέδου, διακρατική/διϋπουργική συνεδρίαση για το διεθνές έγκλημα (AMMTC). Σε μια τέτοια συνεδρίαση στην Μπανγκόκ της Ταϋλάνδης, στις 8 Ιανουαρίου 2004, αναγνωρίστηκε η σημασία της κυβερνοασφάλειας και επισημάνθηκε η ανάγκη για μια αποτελεσματική, νομική συνεργασία να ενισχυθεί η πάλη ενάντια στο διεθνές κυβερνοέγκλημα.

Επίσης, ένα σχέδιο δράσης για να εφαρμοστεί μια κοινή διακήρυξη σχετικά με στρατηγική συνεργασία ASEAN και Κίνας για την ειρήνη και η ευημερία, υπογράφηκε στις 8 Οκτωβρίου 2003, στο Μπαλί της Ινδονησίας. Η ASEAN και η Κίνα σύμφωνα με τη διακήρυξη αυτή θα ακολουθήσουν από κοινού τις πιο κάτω ενέργειες και μέτρα:[507]

"…2.5.7. Διατυπώστε συνεργατικές διαδικασίες δράσης έκτακτης ανάγκης με σκοπό τη διατήρηση και ενίσχυση της κυβερνοασφάλειας και την παρεμπόδιση και καταπολέμηση του κυβερνοεγκλήματος…".

Τέλος, σε μια δήλωση από το περιφερειακό φόρουμ της ASEAN (ARF) τον Ιούλιο του 2006 υπογραμμίστηκε ότι:[508]

"…Πιστεύοντας ότι μια αποτελεσματική πάλη ενάντια στις κυβερνοεπιθέσεις και την τρομοκρατική ή άλλη κακόβουλη χρήση του κυβερνοχώρου απαιτεί διαρκώς αυξανόμενες, γρήγορες και καλής λειτουργίας, νομικές και άλλες μορφές συνεργασίας:

1. Οι συμμετέχουσες στο ARF χώρες και οργανισμοί θα αποπειραθούν να θεσπίσουν, εάν ακόμη δεν το έχουν κάνει, και να εφαρμόσουν ειδικό θεσμικό πλαίσιο για την κυβερνοασφάλεια και τα κυβερνοεγκλήματα σύμφωνα με τους κείμενους εθνικούς νόμους και με αναφορά σε σχετικά, διεθνή όργανα και συστάσεις/οδηγίες για την πρόληψη, διάγνωση, μείωση και περιορισμό των παρακείμενων επιθέσεων, συμπεριλαμβανομένων των δέκα συστάσεων του ψηφίσματος 55/63 της Γενικής Συνέλευσης του Ο.Η.Ε., σχετικά με την καταπολέμηση της εγκληματικής χρήσης της πληροφορικής τεχνολογίας.

2. Οι συμμετέχουσες στο ARF χώρες και οργανισμοί αναγνωρίζουν τη σημασία ενός εθνικού πλαισίου για τη συνεργασία και συνεννόηση στην αντιμετώπιση εγκληματικής, ακόμη και τρομοκρατικής, κακόβουλης χρήσης του κυβερνοχώρου και ενθαρρύνουν τη διατύπωση ενός τέτοιου πλαισίου... ".

---

[507] Η εν λόγω διακήρυξη είναι αναρτημένη στο portal της ASEAN και διαθέσιμη από το δεσμό http://www.aseansec.org/16805.htm.

[508] Αναλυτικά η δήλωση του προεδρεύοντος του φόρουμ είναι μεταξύ άλλων διαθέσιμη από την ιστοσελίδα του portal του ΥΠΕΞ της Ιαπωνίας, http://www.mofa.go.jp/region/asia-paci/asean/conference/arf/state0607-3.html.

Αλλά ενδεικτικά υποδείγματα της ισχύουσας κατάστασης

Οι παρακάτω αποτελούν μερικές ακόμη ενδεικτικές περιπτώσεις και σημαίνοντα γεγονότα της αυξημένης, στις μέρες μας, δραστηριότητας στο χώρο της νομοθεσίας περί του η-εγκλήματος:

- Η εταιρεία McConnell International πραγματοποίησε και δημοσιοποίησε το Δεκέμβρη του 2000 μια παγκόσμια έρευνα με τίτλο "Cybercrime… and Punishment?".[509] Στην έρευνα αυτή αναλύει την κατάσταση στη νομοθεσία 52 χωρών, όσον αφορά την προστασία από το κυβερνοέγκλημα και τα πρώτα συμπεράσματα δεν ήταν ενθαρρυντικά. Ο θετικός αντίκτυπος που είχε η εν λόγω έρευνα στην περαιτέρω ευαισθητοποίηση, δραστηριοποίηση και πρόοδο υπήρξε σημαντικός.
- Μια Διεθνής Διάσκεψη με μεγάλη συμμετοχή και θέμα "Cybercrime: A Global Challenge, A Global Response"[510] διοργανώθηκε στη Μαδρίτη τον Δεκέμβριο του 2005, σε μια κοινή προσπάθεια από το Συμβούλιο της Ευρώπης, την Ισπανία και τον οργανισμό των αμερικανικών κρατών (OAS), τα αποτελέσματα της οποίας κρίθηκαν ιδιαίτερα ικανοποιητικά στο πεδίο συζήτησης και προώθησης διακρατικών νομικών πρωτοβουλιών στα πλαίσια του κυβερνοεγκλήματος. Μεταξύ των συμπερασμάτων της διαβάζουμε: «Αναγνωρίζουμε τη σημασία της μόνης διεθνούς συνθήκης σε αυτόν τον τομέα: η Συνθήκη σχετικά με το Κυβερνοέγκλημα που είναι ανοικτή σε όλα τα κράτη καθώς επίσης και τη σημαντικότητα ενδυνάμωσης του διεθνούς νομικού πλαισίου. Ενθαρρύνουμε έντονα τα κράτη να εξετάσουν τη δυνατότητα να γίνουν συμβαλλόμενα μέρη σε αυτήν την Συνθήκη προκειμένου να χρησιμοποιηθούν αποτελεσματικοί και συμβατοί νόμοι και εργαλεία που να παλεύουν με το κυβερνοέγκλημα, σε εσωτερικό επίπεδο και εξ ονόματος της διεθνούς συνεργασίας. Αναγνωρίζουμε την ανάγκη μεγαλύτερης συνεργασίας, προσφοράς τεχνικής βοήθεια και οργάνωσης παρόμοιων γεγονότων σε άλλες περιοχές του κόσμου.»
- Οι διεθνείς φορείς και διακρατικοί οργανισμοί για την παγκόσμια ανάπτυξη, συνεργασία και ειρήνη, όπως ο Ο.Η.Ε. και ο Ο.Ο.Σ.Α., παρακολουθούν στενά το θέμα της η-ασφάλειας και του κυβερνοεγκλήματος και κατά καιρούς διατηρούν μόνιμες, σχετικές ομάδες εργασίας, που εκδίδουν γενικές συστάσεις και οδηγίες και

[509] Η εταιρεία δημοσιεύει την έρευνα και στον ιστοχώρο της, μέσω της ιστοσελίδας http://www.mcconnellinternational.com/services/cybercrime.htm.

[510] Τα συμπεράσματα της εν λόγω συνάντησης είναι ιδιαίτερα ενδιαφέροντα και δημοσιεύονται εκτός των άλλων στο Διαδίκτυο, στον ιστοχώρο του Συμβουλίου της Ευρώπης (CoE), όπου και γίνονται διαθέσιμα στο ευρύ κοινό μέσω του δεσμού www.coe.int/t/e/legal_affairs/about_us/cooperation/CYB%20_2005_%20Conclusions%20E.pdf.

προωθούν ψηφίσματα.[511] Η δράση αυτών των οργανισμών έχει αναδειχθεί σε σημαντικό παράγοντα καθοδήγησης και συμμόρφωσης των χωρών σε συναφή, νομικά θέματα.

- Ειδικά παραρτήματα και ομάδες κρούσης[512] π.χ. στο FBI, την Interpol και το Πεντάγωνο των Η.Π. και διάφορα κατά τόπους σώματα (εκτελεστικά όργανα) δίωξης ηλεκτρονικού εγκλήματος συστήνονται (με αυξανόμενο ρυθμό) και εντέλλονται να διερευνούν υποθέσεις κακόβουλης παραβίασης της κυβερνοασφάλειας και να διεξαγάγουν -πολλές φορές μεγάλης κλίμακας- επιχειρήσεις για την προσαγωγή υπόπτων η-εγκληματικής δράσης.
- Μια πολύ ενδιαφέρουσα, εμπεριστατωμένη και αρκούντως πλήρης, στατιστική έρευνα για τη νομική κατάσταση, με παράθεση σχετικής νομοθεσίας από τις διάφορες χώρες στο ευαίσθητο θέμα του ηλεκτρονικού εγκλήματος, παρουσιάζεται στην πλούσια σε ενημερωτικό υλικό ιστοσελίδα http://www.cybercrimelaw.net/ και από εκεί μπορεί κανείς να αντλήσει χρήσιμα στοιχεία για τις ισχύουσες συνθήκες σε παγκόσμιο επίπεδο.

4.7.4 Αποτελεσματικότητα

Τον Αύγουστο του 2000 ένα σώμα κατηγόρων αναγκάστηκε να αποσύρει όλες τις κατηγορίες ενάντια στον Onel de Guzman, τον Φιλιππινέζο σπουδαστή του κολλεγίου AMA Computer University of Makati, που κατηγορήθηκε για την απελευθέρωση του ιού «I Love You».[513] Ο εν λόγω ιός επιτέθηκε στα συστήματα ηλεκτρονικού ταχυδρομείου σε όλο τον κόσμο προκαλώντας κατ' εκτίμηση $10 δισεκατομμύρια ζημίες. Ο λόγος για την απόσυρση των κατηγοριών ήταν η έλλειψη εφαρμόσιμης νομοθεσίας στο νομικό κώδικα των Φιλιππίνων. Ο Πρόεδρος Joseph Estrada υπέγραψε αμέσως έναν νόμο, που προγράφει τα περισσότερα σχετικά με υπολογιστή εγκλήματα, αλλά ο νόμος δεν μπορούσε να εφαρμοστεί αναδρομικά στο συντάκτη του διαβόητου "Love Bug". Δυστυχώς, αυτό δεν είναι ένα μεμονωμένο γεγονός. Σύμφωνα με την έκθεση “Cybercrime… and Punishment?”[514], που εκπονήθηκε από την εταιρεία συμβούλων διαχείρισης τεχνολογίας McConnell International το 2000, μόνο εννέα από τις 52 χώρες που διερευνήθηκαν βρέθηκαν να έχουν τροποποιήσει τους νόμους

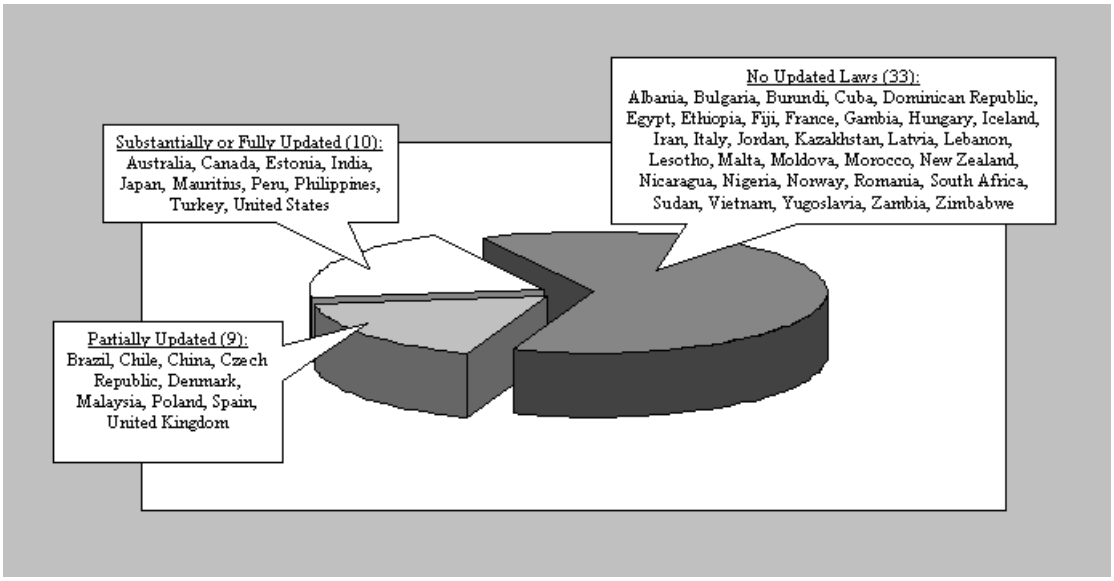
[511] Κύρια, βιβλιογραφική αναφορά: [CHIK-CCLMNGIS].

[512] Τις συναντά κανείς με εύηχα ονόματα όπως CyberSecurity Task-Forces και CyberSecurity Divisions.

[513] Πηγή: “Love Bug Suspect Off The Hook”, CBS News, 2000, διαθέσιμο από το δεσμό http://www.cbsnews.com/stories/2000/08/21/tech/main226472.shtml.

[514] Κύρια, βιβλιογραφική αναφορά: [MCCONNELL-CCP].

τους επαρκώς, ώστε να καλύπτουν πτυχές από τα κυβερνοεγκλήματα. *"Το μακρύ χέρι του νόμου δεν φθάνει ακόμα σε ολόκληρο το παγκοσμιοποιημένο Διαδίκτυο"*, δήλωνε χαρακτηριστικά ο Bruce McConnell, πρόεδρος της McConnell International προσθέτοντας πως *"οι οργανισμοί πρέπει για τώρα να στηριχθούν στα δικά τους αμυντικά μέτρα"*.



Σχήμα 32: Η έρευνα της McConnell International (έτος 2000), που αποκαλύπτει την ανυπαρξία ή ανεπάρκεια κατάλληλων θεσμικών πλαισίων για το η-έγκλημα σε πολλές χώρες του κόσμου

Αν και σε πολλές περιπτώσεις, 8 χρόνια μετά, μια πρώιμη, ισχυρή νομοθεσία ενάντια στους ιούς υπολογιστών και τα σκουλήκια υφίσταται πλέον σε μεγάλο αριθμό χωρών (http://www.mcconnellinternational.com/services/Updatedlaws.htm) και οι περισσότερες από τις ανεπτυγμένες τουλάχιστον χώρες εργάστηκαν στην κατεύθυνση κατάλληλης επεξεργασίας και αναθεώρησης των θεσμικών τους πλαισίων, ώστε να συμπεριλάβουν τα η-εγκλήματα και τις δράσεις των κακόβουλων απειλών, αλλά και ευρύτερης συνεργασίας και συνεννόησης μεταξύ τους στα θέματα αυτά (βλέπε αμέσως επόμενο σχήμα), υπάρχουν ακόμη περιπτώσεις που παρατηρείται απαράδεκτη ανευθυνότητα, νωθρότητα και κωλυσιεργία. Απαιτείται, λοιπόν, και γίνεται ακόμα πολλή έρευνα και προσπάθεια στην κατεύθυνση μιας ουσιαστικής, νομικής προστασίας και καταστολής του κυβερνοεγκλήματος και της όποιας πληροφοριακής εχθροπραξίας με τα πρώτα, νωπά αποτελέσματα -αν και όχι αποκαρδιωτικά- να μην είναι ακόμη ιδιαίτερα ικανοποιητικά.[515] Είμαστε ακόμη μοναχά στην αρχή και ο δρόμος που πρέπει να διανύσουν οι χώρες, προκειμένου να στήσουν ένα αποτελεσματικό, θεσμικό δίκτυο καταπολέμησης των ηλεκτρονικών εγκλημάτων και συρράξεων, διαφαίνεται

[515] Περισσότερα για το θέμα της αποτελεσματικότητας αναφέρονται στο κεφάλαιο 5, στο σχετικό εδάφιο 5.3.

μακρύς. Μέχρι τότε οι οργανισμοί θα πρέπει να συνεχίζουν να στηρίζονται σε πολύ μεγάλο βαθμό στην επάρκεια και επίδοση των δικών τους μηχανισμών και διαδικασιών ασφάλειας και προστασίας.

Country	Data Crimes			Network Crimes		Access Crimes		Related Crimes		
	Data Interception	Data Modification	Data Theft	Network Interference	Network Sabotage	Unauthorized Access	Virus Dissemination	Aiding and Abetting Cyber Crimes	Computer-Related Forgery	Computer-Related Fraud
Australia	X	X	X	X		X			X	X
Brazil		X			X	X		X		
Canada	X	X	X	X	X	X	X			X
Chile	X	X	X	X	X					
China		X		X			X			
Czech Republic		X	X		X	X				X
Denmark		X		X						X
Estonia		X	X	X	X	X	X	X		X
India		X	X	X	X	X	X	X		X
Japan	X	X	X	X	X	X		X	X	X
Malaysia		X				X		X		X
Mauritius	X	X		X	X	X	X	X	X	
Peru	X	X	X	X	X	X				X
Philippines	X	X	X	X	X	X	X	X	X	X
Poland		X	X	X				X		
Spain	X	X	X					X		X
Turkey		X	X	X	X		X	X	X	X
United Kingdom		X		X	X	X		X		
United States	X	X	X	X	X	X	X	X		X

Σχήμα 33: Η νομική κατάσταση σε διάφορες χώρες στον τομέα του κυβερνοεγκλήματος (απόσπασμα από την σχετική έρευνα της εταιρείας McConnell International το έτος 2000)

4.8 Οργάνωση και Διοίκηση στην Ασφάλεια/ Ανυπέρβλητοι Περιορισμοί

Η *μακρόχρονη απουσία ενός προστατευτικού, ισχυρού, νομικού πλέγματος*[516] για την κυβερνοασφάλεια, αλλά και η ανάγκη να καθορίσουν το δικό τους προσωπικό στίγμα στις διάφορες τοπικές και διεθνείς περιβαλλοντικές συγκυρίες, πίεσαν τους οργανισμούς να κινηθούν με σθένος στην κατεύθυνση της αυτοάμυνας και της αυτοπροστασίας με την κατάστρωση και υλοποίηση επιτηδευμένων διαδικασιών για την ασφάλεια των ΠΣ τους. Η

[516] Όπως διαπιστώσαμε στο αμέσως προηγούμενο εδάφιο 4.7.

επένδυση σε αυτά τα νομοτελειακής πλέον αναγκαιότητας εσωτερικά μέτρα προστασίας έχει πάψει εν πολλοίς να θεωρείται επιχειρησιακό ρίσκο, αλλά αντίθετα γίνεται σταδιακά αντιληπτή ευρύτερα ως ισχυρά περιοριστική δράση κατά του κινδύνου, που παράγεται για έναν οργανισμό από τη συνεχή του έκθεση στα αυξανόμενα πυρά των διαφόρων, πληροφοριακών επιθέσεων· το αναλαμβανόμενο κόστος για την προμήθεια/υλοποίηση κάποιων από αυτούς τους μηχανισμούς έχει αρχίσει να αποκτά δευτερεύουσα σημασία, αφού πια προέχουν αφενός η υποσχόμενη, μεγαλύτερη, δυνατή διασφάλιση/διαβεβαίωση της απρόσκοπτης, στρατηγικής λειτουργίας (και άρα η ανταπόδοση της επένδυσης) και αφετέρου η χρηστή και αποτελεσματικότερη αξιοποίηση/διοίκηση/διαχείριση των εν λόγω συστημάτων προστασίας (που μεγιστοποιεί τα οφέλη).

Οι μεταβλητές κινδύνου για την ασφάλεια των σύγχρονων οργανισμών και επιχειρήσεων, όπως είδαμε κατά μήκος της εργασίας αυτής, απαρτίζονται από τις απειλές και ευπάθειες, τις διαφορετικές τεχνικές επίθεσης, την αναμενόμενη συχνότητα των επιθέσεων, τις λειτουργίες και χρησιμοποιούμενες τεχνολογίες εντός του εκάστοτε οργανισμού και τη συνολική, αμυντική του στάση. Οι μεταβλητές αυτές, σε πλείστες περιπτώσεις, βρίσκονται σε διαρκή μεταβολή, προκειμένου ακόμη και για το ίδιο υπόδειγμα. Επομένως, η *διαχείριση του κινδύνου (risk management)* απαιτεί μια συνεχή, τεκμηριωμένη και επαρκώς οριοθετημένη, εσωτερική διαδικασία.

Η ασφάλεια των πληροφοριών (και συνεπώς και η προστασία από τη δράση κακόβουλων όπλων) στο επιχειρησιακό επίπεδο αφαίρεσης, σήμερα, είναι ιδανικά μια συντονισμένη διαδικασία με την οποία ένας οργανισμός μπορεί να προστατεύει και να διασφαλίζει συστήματα, μέσα αποθήκευσης και εγκαταστάσεις, που επεξεργάζονται και διατηρούν τις οικείες πληροφορίες ζωτικής, λειτουργικής σημασίας.

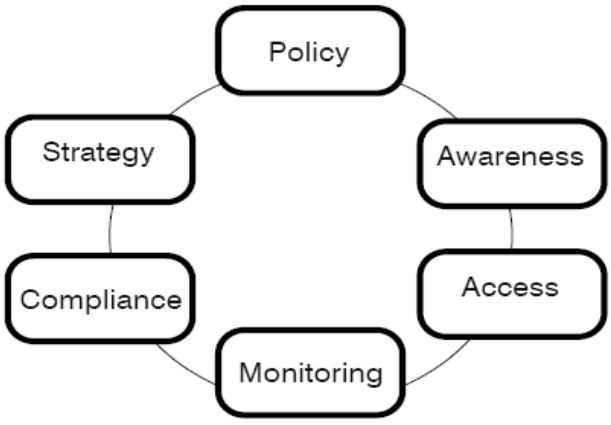
Οι διάφοροι οργανισμοί και οι φορείς παροχής πληροφοριακών/τηλεπικοινωνιακών υπηρεσιών πρέπει να διαθέτουν και να διατηρούν αποτελεσματικά προγράμματα ασφάλειας, επαρκή για τη λειτουργική πολυπλοκότητά τους. Αυτά τα προγράμματα ασφάλειας πρέπει να απολαμβάνουν την ισχυρή υποστήριξη από μέρους του διοικητικού συμβουλίου και της ανώτερης διαχείρισης, να προβλέπουν και να εφαρμόζουν την ενσωμάτωση και ενοποίηση των δραστηριοτήτων ασφάλειας και των ελέγχων σε όλες τις επιχειρησιακές διαδικασίες και να καθορίζουν σαφή υπευθυνότητα για την ανάληψη και απόδοση ευθυνών ασφάλειας.

Επίσης, έχουν πια αρχίσει να γίνονται περισσότερο ορατοί και αντιληπτοί κάποιοι, εγγενείς περιορισμοί των μηχανισμών και διαδικασιών ασφάλειας και οι οργανισμοί, οι επιχειρήσεις, οι κυβερνήσεις και τα άτομα καλούνται να δραστηριοποιηθούν ακόμη πιο πολύ, με κατάλληλες παρεμβάσεις, τροποποιήσεις, αναθεωρήσεις και εναλλακτικές στις στρατηγικές τους, για να ανταπεξέλθουν καλύτερα στις επίκαιρες και μελλοντικές προκλήσεις.

4.8.1 Διαδικασιοστρεφής και Επιχειρησιοκεντρική Προσέγγιση

Οι οργανισμοί, συχνά, ανακριβώς θεωρούν την ασφάλεια πληροφοριών ως την κατάσταση των όποιων ελέγχων σε μια δεδομένη, χρονική συγκυρία. Η ασφάλεια στην πραγματικότητα είναι μια διαρκής διαδικασία, στα πλαίσια της οποίας η δεδομένη κατάσταση των ελέγχων μιας επιχείρησης είναι μόνο ένας δείκτης της γενικής στάσης ασφάλειάς της. Άλλοι ενδεικτικοί δείκτες περιλαμβάνουν τη δυνατότητα ενός οργανισμού να αξιολογεί συνεχώς τη στάση του και να αντιδρά κατάλληλα, παρά τη μεγάλη ταχύτητα στις μεταβολές, στις απειλές, τις τεχνολογίες και τις εσωτερικές και περιβαλλοντικές, επιχειρησιακές συνθήκες.

Μια επιχείρηση καθιερώνει και διατηρεί μια αληθινά αποτελεσματική ασφάλεια πληροφοριών, όταν και μόνο όταν ολοκληρώνει συνεχώς διαδικασίες, ανθρώπους και τεχνολογία για να μετριάζει τον κίνδυνο, πάντα σε συμφωνία με μια, τρέχουσα αξιολόγηση του κινδύνου και τα όποια αποδεκτά όρια ανοχής αυτού.[517] Οι οργανισμοί επικεντρώνουν τις προσπάθειές τους στις *επιχειρησιακά κρίσιμες (mission-critical) πληροφορίες* τους[518] και τα αντίστοιχα ΠΣ και μεριμνούν για την προστασία τους με τη θέσπιση και υλοποίηση μιας διαρκούς, εξειδικευμένης διαδικασίας ασφάλειας που προσδιορίζει τους κινδύνους, διαμορφώνει μια στρατηγική για να τους διαχειριστεί, εφαρμόζει αυτή τη στρατηγική, εξετάζει την αποτελεσματικότητα και τα όποια προβλήματα στην εφαρμογή και παρακολουθεί συνεχώς το περιβάλλον για να ελέγξει τους κινδύνους.



Σχήμα 34: Διαδικασία διαχείρισης της ασφάλειας

Η *διαδικασία ασφάλειας*, λοιπόν, είναι εκείνη *"η εμπεριστατωμένη μέθοδος που χρησιμοποιούν και εφαρμόζουν με τη μεγαλύτερη δυνατή συνέχεια και συνέπεια οι οργανισμοί*

[517] Κύρια, βιβλιογραφική αναφορά: [FFIEC-IS].

[518] Κύρια, βιβλιογραφική αναφορά: [CARALLI-CSM].

στην προσπάθεια τους να επιτύχουν τους εκάστοτε στρατηγικούς στόχους για την ασφάλεια των ΠΣ τους" και περιλαμβάνει τα ακόλουθα διακριτά στάδια:[519]

1. **Αποτίμηση/Αξιολόγηση κινδύνου σχετικού με ασφάλεια πληροφοριών (Infosec Risk Assessment)**:

   Μια διαδικασία για να προσδιορίζονται και να αξιολογούνται κάθε φορά οι απειλές, ευπάθειες, επιθέσεις, πιθανότητες των περιστατικών και οι εκβάσεις-επιπτώσεις.

2. **Χάραξη στρατηγικής (Infosec Security Roadmap)**:

   Μιλάμε για εκείνο το διοικητικό, καλά τεκμηριωμένο σχέδιο μετριασμού ή αποφυγής ή μετατόπισης του κινδύνου, που ενσωματώνει κατάλληλα την τεχνολογία, τις πολιτικές, τις διαδικασίες και την σχετική κατάρτιση. Το πλάνο αυτό πρέπει να αναθεωρείται και να εγκρίνεται εκ νέου, σε τακτά χρονικά διαστήματα, από τα διάφορα, διοικητικά συμβούλια και τους στρατηγικά συμμέτοχους στον οργανισμό, προκειμένου να παραμένει επίκαιρο και αποτελεσματικό.

3. **Υλοποίηση μέτρων, ελέγχων και υπηρεσιών ασφάλειας (Security Controls Implementation)**:

   Στο στάδιο αυτό πραγματοποιείται η απόκτηση, παραμετροποίηση/διαρρύθμιση (tailoring) και λειτουργία προστατευτικής τεχνολογίας, η συγκεκριμένη ανάθεση καθηκόντων και ευθυνών στους διάφορους διευθύνοντες και στο προσωπικό και η εγκατάσταση και επέκταση των κατάλληλων ελέγχων, κανόνων και μέτρων ασφάλειας και, επίσης, εδώ λαμβάνεται και η δεδομένη, απαραίτητη φροντίδα, ώστε να εξασφαλίζεται η μεγαλύτερη δυνατή διαβεβαίωση ότι η διοίκηση και το προσωπικό καταλαβαίνουν τις ευθύνες τους και έχουν τη γνώση, τις δεξιότητες και τα απαραίτητα κίνητρα για να εκπληρώνουν τα καθήκοντά τους.

4. **Παρακολούθηση ασφαλούς λειτουργίας συστημάτων (Systemic Monitoring)**:

   Αφορά στη χρήση διαφόρων μεθοδολογιών για να κερδίσει κανείς τη διαβεβαίωση ότι οι κίνδυνοι αξιολογούνται κατάλληλα και μετριάζονται/αποφεύγονται. Αυτές οι μεθοδολογίες πρέπει να επιβεβαιώνουν πως τα όποια, ουσιώδη μέτρα ασφάλειας ακολουθεί ο οργανισμός εκτελούνται σωστά, είναι αποτελεσματικά και αποδίδουν όπως είναι επιθυμητό.

5. **Συνεχής Παρακολούθηση, Αναθεώρηση και Βελτιστοποίηση της διαδικασίας (Procedural Monitoring & Process Reengineering)**:

[519] Κύρια, βιβλιογραφική αναφορά: [FFIEC-IS].

Η διαδικασία συνεχούς συλλογής και ανάλυσης πληροφοριών σχετικά με τις νέες απειλές και ευπάθειες, τις πραγματικές επιθέσεις στον οργανισμό και τα άλλα περιστατικά ασφάλειας, σε συνδυασμό με περιοδικές, τακτές μετρήσεις και άλλες εκτιμήσεις αποτελεσματικότητας των υπαρχόντων διεργασιών, ελέγχων και μέτρων ασφάλειας. Αυτές οι πληροφορίες χρησιμοποιούνται για να ενημερώνουν και αναβαθμίζουν κάθε φορά την αξιολόγηση του κινδύνου, τη στρατηγική και τους ελέγχους και τις υπόλοιπες, σχετικές με την ασφάλεια, διεργασίες. Η διαρκής παρακολούθηση και αναθεώρηση και της εν λόγω διαδικασίας εγγυώνται τη συνέχεια και συνέπειά τόσο της ίδιας όσο και ολόκληρης της διαδικασίας διαχείρισης της ασφάλειας.

4.8.2 Στοχοθέτηση

Σε μια *επιχειρησιοκεντρική προσέγγιση (mission-centric, mission-focused approach)*, δεν μπορούμε να αμελήσουμε την ανάγκη ευθυγράμμισης οποιασδήποτε, επιχειρησιακής διαδικασίας, άρα και αυτής της διαχείρισης της ασφάλειας, με τους ευρύτερους, στρατηγικούς στόχους του οργανισμού.[520] Οι ιδιαίτεροι στόχοι για τους οργανισμούς στο ευαίσθητο θέμα της ασφάλειας δε θα μπορούσαν να είναι άλλοι, παρά η μεγαλύτερη δυνατή ικανοποίηση των διαφόρων υπηρεσιών ασφάλειας, που περιγράφονται από τα CIA, Parkerian και τα άλλα θεωρητικά μοντέλα (π.χ. ακεραιότητα, εμπιστευτικότητα, διαθεσιμότητα, υπευθυνότητα κτλ), ειδικά όσον αφορά τα επιχειρησιακά κρίσιμα συστήματα πληροφοριών, σε συνδυασμό με το μεγαλύτερο δυνατό βαθμό διαβεβαίωσης (assurance) στους στρατηγικούς παίχτες (υπάλληλοι, χρήστες, πελάτες, συνεργάτες κλπ) και τη διοίκηση πως τα συστήματα των πληροφοριών του οργανισμού παρέχουν την προοριζόμενη λειτουργία αποτρέποντας τις όποιες ανεπιθύμητες ενέργειες.

Οι 2 αυτοί στόχοι είναι πρόδηλα συνυφασμένοι, αλλά ταυτόχρονα και ξεκάθαρα διαφορετικοί στην όψη και τη βαθύτερή τους ουσία· ο πρώτος αφορά τη σχετική επιτυχία στην εκπλήρωση των επιθυμητών υπηρεσιών ασφάλειας, που εξασφαλίζουν ούτως ή άλλως σημαντική προστασία έναντι σε αναγνωρισμένους (και μη) κινδύνους, ενώ ο δεύτερος έχει να κάνει με την παροχή του κατάλληλου πλαισίου για αποτελεσματικότερη διαχείριση (εχέγγυα επιβεβαίωσης και διάρκειας της όποιας επιτυχίας) και ευρύτερη επικοινώνηση ενός σταθερά αποδεκτού και ικανοποιητικού επιπέδου ασφάλειας, για την καλλιέργεια κλίματος αυτοπεποίθησης, αλλά και εμπιστοσύνης για τον οργανισμό, με σκοπό τη διατήρηση ή αύξηση της αποκομιδής κέρδους ή άλλου στρατηγικού πλεονεκτήματος και την

[520] Κύρια, βιβλιογραφική αναφορά: [CARALLI-CSM].

αποφυγή/περιορισμό της όποιας απώλειας από την ανασφάλεια των στρατηγικών παιχτών και της διοίκησης και τις όποιες ζημιογόνες αντιλήψεις τους για μη αξιοπιστία του οργανισμού. Η ικανοποίηση των 2 αυτών, ξεχωριστών στόχων για την ασφάλεια αποτελεί εγγύηση καλής λειτουργίας του οργανισμού στην κατεύθυνση εξυπηρέτησης των ευρύτερων στρατηγικών του στόχων, αφού εξασφαλίζει τον έλεγχο και περιορισμό των ζημιών και επιπτώσεων και υποστηρίζει ευθέως την ανάπτυξη ενός γόνιμου και παραγωγικού κλίματος.

4.8.3 Οργανωτική Δομή, Υπευθυνότητα και Διακυβέρνηση

Η διακυβέρνηση απαιτείται στην οργάνωση και διοίκηση της ασφάλειας πληροφοριών για να εξασφαλίσει ότι οι υποχρεώσεις/διεργασίες ολοκληρώνονται κατάλληλα, ότι η υπευθυνότητα διατηρείται, και ότι ο κίνδυνος ελέγχεται και ρυθμίζεται για την όλη επιχείρηση. Μια αποτελεσματική διακυβέρνηση, στα πλαίσια της ασφάλειας, επιτυγχάνεται συνήθως μέσω *ευέλικτης, διοικητικής/οργανωτικής δομής, συνεπούς ανάθεσης των ευθυνών και διάκρισης ρόλων και εξουσιών, καθιέρωσης κατάλληλων πολιτικών, προτύπων και διαδικασιών, ουσιαστικής κατανομής πόρων, άρτιας εκπαίδευσης, διαρκούς παρακολούθησης και ελέγχου και δέσμευσης στην υπευθυνότητα*.[521]

Η ασφάλεια των πληροφοριών είναι ένας σημαντικός, επιχειρησιακός κίνδυνος και απαιτεί την *αφοσίωση και δέσμευση* του διοικητικού συμβουλίου και της ανώτερης διοίκησης κάθε οργανισμού. Επιπλέον, είναι *ευθύνη κάθε οντότητας που έχει αυξημένες δυνατότητες πρόσβασης στις κρίσιμες πληροφορίες* του οργανισμού. Η ασφάλεια πληροφοριών πρέπει να υποστηριχθεί κατά μήκος όλης της επιχείρησης, συμπεριλαμβανομένου του διοικητικού συμβουλίου, της ανώτερης διοίκησης, των λειτουργών της ασφάλειας πληροφοριών, των απλών εργαζομένων, αλλά και των πάσης φύσεως ελεγκτών, των φορέων παροχής υπηρεσιών στην επιχείρηση, των αναδόχων έργων για αυτήν και του λοιπού εξωτερικού της περιβάλλοντος. Κάθε ρόλος έχει και διαφορετικές ευθύνες όσον αφορά την ασφάλεια πληροφοριών και κάθε άτομο πρέπει να είναι υπεύθυνο για τις ενέργειές του. Η υπευθυνότητα απαιτεί σαφείς γραμμές υποβολής εκθέσεων στην ανώτερη διοίκηση και το Δ.Σ., αντίστροφα σαφή επικοινώνηση των στρατηγικών προσδοκιών από τη διοίκηση και, φυσικά, σώφρονα ανάθεση/μεταβίβαση εξουσιοδοτήσεων και *συνετή χρήση των αρμόδιων εξουσιών*, για να επιφέρει ικανοποιητική συμμόρφωση με τις ιδιαίτερες πολιτικές, τα πρότυπα, και τις διαδικασίες εντός του οργανισμού.

[521] Κύρια, βιβλιογραφική αναφορά: [JECUSC-SIA].

Ρόλοι, Ευθύνες και Αρμοδιότητες

Ένα, *βασισμένο στους επιχειρησιακούς ρόλους (role-based management)* των συστατικών μερών ενός οργανισμού και τη μεταξύ τους διάκριση ευθυνών και αρμοδιοτήτων, σύστημα διοίκησης της πληροφοριακής ασφάλειας και διαχείρισης του σχετικού κινδύνου είναι το πλέον εφαρμόσιμο πρότυπο για την υλοποίηση αποτελεσματικών διαδικασιών ασφάλειας και επιτυχημένου σχήματος αμυντικής στάσης και προστασίας, για τους σύγχρονους οργανισμούς.

Παρακάτω, αναφέρονται συνοπτικά οι *ρόλοι, ευθύνες και αρμοδιότητες* των διαφόρων, βασικών μερών μιας τυπικής, επιχειρησιακής δομής:

Ι. Διοικητικό Συμβούλιο

Το διοικητικό συμβούλιο, ή μια κατάλληλη επιτροπή εξ αυτού, είναι αρμόδιο για την *επιτήρηση της ανάπτυξης, της εφαρμογής και της συντήρησης του προγράμματος* ασφάλειας πληροφοριών του οργανισμού και για να καθιστά την ανώτερη διαχείριση υπεύθυνη για τις ενέργειές της. Μια σωστή εποπτεία απαιτεί από ένα Δ.Σ. να παρέχει την *απαραίτητη καθοδήγηση στην ανώτερη διοίκηση*, να εγκρίνει σχέδια, πολιτικές και προγράμματα ασφάλειας πληροφοριών και να επιθεωρεί εκθέσεις σχετικά με την αποτελεσματικότητα του προγράμματος ασφάλειας. Πρέπει ακόμη να *παρέχει στα κλιμάκια διοίκησης τις προσδοκίες και τις απαιτήσεις του και να καθιστά τα αρμόδια, διοικητικά στελέχη υπεύθυνα* για τα ακόλουθα:[522]

1. Κεντρική εποπτεία, διαχείριση και συντονισμό.

2. Ανάθεση ευθυνών και αρμοδιοτήτων.

3. Αξιολόγηση και μέτρηση κινδύνου.

4. Παρακολούθηση και δοκιμές του συστήματος ασφάλειας.

5. Υποβολή κατάλληλων εκθέσεων.

6. Αποδοχή εναπομείνουσας επικινδυνότητας (residual risk acceptance)

Τα Δ.Σ. καλό θα ήταν τουλάχιστον ετησίως να εγκρίνουν τις γραπτές πολιτικές ασφάλειας και τις γραπτές εκθέσεις σχετικά με την αποτελεσματικότητα του προγράμματος ασφάλειας πληροφοριών. Μια γραπτή έκθεση προς το Δ.Σ. πρέπει να περιγράφει τη γενική κατάσταση του προγράμματος ασφάλειας πληροφοριών. Στην ελάχιστη περίπτωση, η έκθεση αυτή

[522] Κύρια, βιβλιογραφική αναφορά: [FFIEC-IS].

πρέπει να απευθύνεται σε θέματα όπως τα αποτελέσματα της διαδικασίας αξιολόγησης κινδύνου, τις σχετικές αποφάσεις διαχείρισης και ελέγχου κινδύνου, τις τυχόν ρυθμίσεις φορέων παροχής υπηρεσιών, τα αποτελέσματα παρακολούθησης και δοκιμών του συστήματος ασφάλειας, τις όποιες παραβιάσεις ασφάλειας ή/και τις αποτυχίες συμμόρφωσης σε διοικητικές απαιτήσεις και τέλος πρέπει να παρέχει συστάσεις για αλλαγές/τροποποιήσεις στο όλον πρόγραμμα ασφάλειας. Μια τέτοια ετήσια έγκριση από μεριάς ενός Δ.Σ. πρέπει πάντοτε προηγουμένως να λαμβάνει υπόψιν μερικά, βασικά στοιχεία, όπως τα αποτελέσματα των αξιολογήσεων και των αναθεωρήσεων της διοίκησης, την όποια εσωτερική και εξωτερική δραστηριότητα σχετική με την ασφάλεια πληροφοριών, τις επιθεωρήσεις τρίτων μερών σε σχέση με το πρόγραμμα και τα μέτρα ασφάλειας (external auditing/testing), καθώς και άλλες εσωτερικά ή εξωτερικά προερχόμενες, ανάλογες μελέτες και αναφορές, με σκοπό να αξιολογηθεί με τον καλύτερο τρόπο η επάρκεια των τρεχόντων ελέγχων και μέτρων ασφάλειας πληροφοριών και να δοθούν τα κίνητρα και οι οδηγίες για κατάλληλη τροποποίηση ή αλλαγή στάσης και στρατηγικής.

ΙΙ. Ανώτερη Διοίκηση (Senior Management)

Η στάση της ανώτερης διοίκησης απέναντι στην ασφάλεια πληροφοριών έχει επιπτώσεις στη δέσμευση και τη συναίνεση ολόκληρου του οργανισμού. Παραδείγματος χάριν, η αποτυχία ενός Προέδρου ή Διευθυντή οργανισμού να συμμορφωθεί με τις όποιες πολιτικές ασφάλειας θα μπορούσε να υπονομεύσει τη δέσμευση ολόκληρης της επιχείρησης στην ασφάλεια των πληροφοριών.

Η ανώτερη διαχείριση πρέπει να τηρεί πρώτιστα η ίδια και κατόπιν να επιβάλλει, με *ευδιάκριτη και ξεκάθαρη επικοινώνηση/ανάθεση των διαφόρων ευθυνών*, τις ιδιαίτερες απαιτήσεις/δεσμεύσεις του προγράμματος ασφάλειας, ενώ πρέπει ακόμη να καθιστά τα κατάλληλα άτομα υπεύθυνα για τη συμμόρφωση με αυτές τις απαιτήσεις. *Μια κεντρική αρχή είναι συνήθως αρμόδια για την εφαρμογή και τον έλεγχο του προγράμματος ασφάλειας*[523]. Οι διοικητικές ευθύνες ασφάλειας, εντούτοις, μπορούν να διανεμηθούν στις διάφορες γραμμές της επιχείρησης ανάλογα πάντα με το μέγεθος του οργανισμού, τη λειτουργική του πολυπλοκότητα, την επιχειρησιακή κουλτούρα και τη φύση των διαδικασιών και άλλων παραγόντων. Ο *διαχωρισμός/διανομή των καθηκόντων (Separation/Distribution of Duties)* και η κατανομή των πόρων από μεριάς της διοίκησης είναι πολύ σημαντικό θέμα στη διαχείριση της ασφάλειας, που πρέπει να εξασφαλίζει έναν κατάλληλο καταμερισμό

[523] Ομάδα κρούσης ή ολόκληρη, οργανωσιακή μονάδα με αντικείμενο το συντονισμό και τη διοίκηση της ασφάλειας του οργανισμού.

εργασίας, ευθυνών και αρμοδιοτήτων, μεταξύ των μεμονωμένων ατόμων ή των ομάδων εργασίας[524].

Η ανώτερη διαχείριση έχει, επίσης, την ευθύνη να εξασφαλίζει την ολοκλήρωση των ελέγχων και μέτρων ασφάλειας σε όλη την επιχείρηση. Για να υποστηρίξει την επιθυμητή ενσωμάτωση-ολοκλήρωση, η ανώτερη διοίκηση πρέπει να: [525]

- Διασφαλίζει ότι η διαδικασία ασφάλειας κυβερνάται από οργανωτικές πολιτικές και πρακτικές που εφαρμόζονται με συνέπεια.
- Απαιτεί δεδομένα και πληροφορίες με παρόμοια χαρακτηριστικά κρισιμότητας και ευαισθησίας προστατεύονται με συνέπεια ανεξάρτητα από το που συγκεκριμένα αποθηκεύονται/φυλάσσονται.
- Επιβάλλει τη συμμόρφωση (compliance) με το πρόγραμμα ασφάλειας με έναν ελεγχόμενο, ισορροπημένο και συνεπή τρόπο σε ολόκληρη την επιχείρηση.
- Συντονίζει/Εναρμονίζει την ασφάλεια πληροφοριών με τη φυσική ασφάλεια.
- Εξασφαλίζει πως ένα αποτελεσματικό πρόγραμμα κατάρτισης και συνειδητοποίησης (security education and awareness) της ασφάλειας πληροφοριών υλοποιείται και δρα κατά μήκος ολόκληρης της επιχείρησης.

Μεταξύ και των παραπάνω θεμάτων η ανώτερη διοίκηση πρέπει γενικότερα να είναι υπεύθυνα απασχολημένη με:[526]

- Σαφή υποστήριξη όλων των πτυχών του προγράμματος ασφάλειας πληροφοριών
- Εκτέλεση του προγράμματος ασφάλειας πληροφοριών όπως εγκρίνεται από το διοικητικό συμβούλιο
- Καθιέρωση/Θέσπιση των κατάλληλων πολιτικών, διαδικασιών και ελέγχων
- Συμμετοχή στην αξιολόγηση της επίδρασης και του επιχειρησιακού αντίκτυπου των ζητημάτων ασφάλειας στον οργανισμό και τις στρατηγικές του γραμμές και διαδικασίες
- Επισήμανση και σκιαγράφηση των γραμμών ευθύνης και υπευθυνότητας για τις αποφάσεις διαχείρισης κινδύνου στην ασφάλεια πληροφοριών

[524] Κύρια, βιβλιογραφική αναφορά: [LEHTINEN-CSB].

[525] Κύρια, βιβλιογραφική αναφορά: [FFIEC-IS].

[526] Όπως στην προηγούμενη υποσημείωση.

- Καθορισμό των προϋποθέσεων, των εννοιών, των μετρήσιμων οντοτήτων και των κριτηρίων μέτρησης/αξιολόγησης του κινδύνου
- Καθιέρωση των αποδεκτών επιπέδων του κινδύνου για την ασφάλεια πληροφοριών
- Επιδίωξη και επιτήρηση δραστηριοτήτων μετριασμού/περιορισμού κινδύνου (risk mitigation).

Οι ανώτερες βαθμίδες της διοίκησης, τέλος, πρέπει να λαμβάνουν τις αποφάσεις τους, σχετικά με την αποδοχή κινδύνου και την αποτελεσματικότητα/επίδοση των δραστηριοτήτων μετριασμού του κινδύνου, βασιζόμενες και στην καθοδήγηση (guidance) και τις συστάσεις από το διοικητικό συμβούλιο. Οι αποφάσεις αυτές πρέπει να ενσωματώνονται στις πολιτικές, τα πρότυπα και τις διαδικασίες του οργανισμού.

III. Εξειδικευμένο προσωπικό ασφάλειας

Η ανώτερη διαχείριση πρέπει να υποδείξει ένα ή περισσότερα άτομα ως ανώτερους υπαλλήλους ασφάλειας πληροφοριών. Οι ανώτεροι υπάλληλοι ασφάλειας πρέπει να είναι *αρμόδιοι και υπεύθυνοι για την οργάνωση του προγράμματος ασφάλειας και τη διαχείριση/καθοδήγηση του υπόλοιπου, κατάλληλα καταρτισμένου, προσωπικού ασφάλειας πληροφοριών*, καθώς και πρωταρχικά για την *καλή λειτουργία των συστημάτων*. Οι ανώτεροι υπάλληλοι στην ασφάλεια πληροφοριών πρέπει να αναφέρονται άμεσα στο Δ.Σ. ή την ανώτερη διοίκηση, ενημερώνοντας για τις σχετικές εξελίξεις, και, ζητώντας/λαμβάνοντας οδηγίες, να προχωρούν σε λήψεις αποφάσεων και άλλες διαχειριστικές ενέργειες (έχουν δηλαδή και διοικητικό ρόλο). Πρέπει ακόμα να απολαμβάνουν *ικανοποιητική ανεξαρτησία και εξουσία* προκειμένου να εκτελούν τα συγκεκριμένα, εξαιρετικά κρίσιμα καθήκοντά τους. Χαρακτηριστικά μιλώντας, οι ανώτεροι υπάλληλοι ασφάλειας πρέπει να είναι και να φέρονται σα διαχειριστές κινδύνου (διοικητικά όργανα) και όχι απλά ως ένας ακόμη παραγωγικός πόρος που διορίζεται/τοποθετείται στο τμήμα τεχνολογίας πληροφοριών (IT) ενός οργανισμού. Οι ανώτεροι υπάλληλοι ασφάλειας, τέλος, είναι θεμιτό να έχουν την απαραίτητη, *άρτια συγκρότηση και επαρκή εξουσιοδότηση*, ώστε με δική τους διαταγή για λήψη κατάλληλων ενεργειών έκτακτης ανάγκης να προστατεύουν το δείνα οργανισμό και τους πελάτες του από μια επικείμενη απώλεια πληροφοριών ή αξίας ή στρατηγικού πλεονεκτήματος.

Γενικότερα, όλοι οι εργαζόμενοι στο χώρο της ασφάλειας πληροφοριών πρέπει να διαθέτουν *συνεπή και επαρκή γνώση, υπόβαθρο και τεχνολογική κατάρτιση*[527], που να τους επιτρέπουν να

[527] Κύρια, βιβλιογραφική αναφορά: [ERBSCHLOE-TWS].

εκτελούν τους ορισμένους στόχους τους με επιτυχία και να διακρίνονται για τη διάθεσή τους. Επιθυμητό είναι δε να διακρίνονται για το ήθος, την υπευθυνότητα και την αφοσίωσή τους στην εξυπηρέτηση των ιδιαίτερων στόχων ασφάλειας του οργανισμού. Ό ρόλος τους είναι εξαιρετικά βαρύνουσας σημασίας, καθώς *αποτελούν κυριολεκτικά τις γραμμές άμυνας και προστασίας του οργανισμού ενάντια στις πληροφοριακές εχθροπραξίες και τα ηλεκτρονικής φύσεως εγκλήματα*, όπως επίσης και τους υπερασπιστές της γενικότερα καλής και αναμενόμενης λειτουργίας των δικτυακών υπηρεσιών και των συστημάτων πληροφοριών.[528] Τα συμβουλευτικά/εκπαιδευτικά τους καθήκοντα δεν πρέπει επίσης να παραγνωρίζονται, καθώς *θεωρούνται υπεύθυνοι για την παροχή υποστήριξης και καθοδήγησης σε τελικούς χρήστες και γενικά σε όλο το υπόλοιπο επιχειρησιακό περιβάλλον* που ενεργεί διαμέσω των πληροφοριακών υποδομών του οργανισμού, με σκοπό την αποτελεσματικότερη και ασφαλέστερη χρήση των συστημάτων. Σαν τελική παρατήρηση, αναμένει κανείς πως η τήρηση, διαφύλαξη και επικοινώνηση των διαδικασιών ασφάλειας πρέπει να αποτελεί αναπόσπαστο κομμάτι -πρωτίστως και ευδιακρίτως από όλα τα υπόλοιπα μέλη ενός οργανισμού- στην εργασία των ανθρώπων αυτών.

IV. Υπόλοιποι εργαζόμενοι

Οι υπάλληλοι πρέπει να γνωρίζουν, να καταλαβαίνουν, και να είναι υπεύθυνοι για την περάτωση των αρμοδιοτήτων τους σε θέματα ασφάλειας. Οι οργανισμοί πρέπει να καθορίσουν με ξεκάθαρο τρόπο αυτές τις αρμοδιότητες στην πολιτική ασφάλειάς τους. Οι περιγραφές εργασίας ή οι συμβάσεις πρέπει να διευκρινίζουν οποιεσδήποτε, πρόσθετες ευθύνες και υποχρεώσεις στα πλαίσια της ασφάλειας πέρα από τις όποιες, γενικές πολιτικές. Οι επιχειρήσεις μπορούν να επιτύχουν την *αποτελεσματική συνειδητοποίηση/κατανόηση*, τη *συμπαράσταση/συναίνεση και την συμμετοχή/συμμόρφωση* στις όποιες, εξειδικευμένες πολιτικές και διαδικασίες από πλευράς των υπαλλήλων τους, μέσω παροχής κατάλληλης *εκπαίδευσης και κατάρτισης στα θέματα της ασφάλειας και των (κυβερνο)επικοινωνιών*[529], με την *ευρύτερη τεκμηρίωση των απαιτούμενων συμπεριφορών* και με την *ενθάρρυνση πιστοποιήσεων συμμόρφωσης, (αυτό)αξιολογήσεων, ελέγχων* και ευρύτερης (διακριτικής και με γνώμονα την ασφάλεια) *παρακολούθησης και υποστήριξης* της εργασιακής δραστηριότητας.[530]

---

[528] Κάτι τέτοιο φυσικά συνοδεύεται και από μια απαίτηση για εποικοδομητική παροχή κινήτρων -όχι απαραίτητα μόνο μέσω οικονομικής φύσεως ρυθμίσεων και ικανοποιητικών απολαβών, αλλά ευρύτερων πλαισίων επιβράβευσης και ψόγου- στις ομάδες αυτών των ανθρώπων, προκειμένου να πραγματοποιούν αποτελεσματικότερα και πιο ωφέλιμα το ουσιαστικά πολύτιμο, κρίσιμο και επίπονο, έργο τους.

[529] Κύρια, βιβλιογραφική αναφορά: [ERBSCHLOE-TWS].

[530] Κύρια, βιβλιογραφική αναφορά: [FFIEC-IS].

Οι εργαζόμενοι αποτελούν την «ψυχή» και την κινητήριο δύναμη κάθε οργανισμού, συνεπώς αποτελούν ουσιαστικούς στυλοβάτες της ασφάλειάς του και έτσι πρέπει να αντιμετωπίζονται στα πλαίσια των προγραμμάτων και διαδικασιών προστασίας.

V. Εξωτερικά, στρατηγικά μέρη και λοιπό περιβάλλον

Μια σωστή διαχείριση πρέπει επίσης να *εξετάζει και να ελέγχει τους ρόλους και τις ευθύνες των εξωτερικών, συμβαλλόμενων μερών*.[531] Οι ευθύνες ασφάλειας των φορέων παροχής υπηρεσιών τεχνολογίας (TSPs), των αναδόχων έργων, των πελατών, αλλά και όλων των υπολοίπων, περιβαλλοντικών οντοτήτων που έχουν κάποιου είδους πρόσβαση στα συστήματα και τα δεδομένα ενός οργανισμού (π.χ. ελεγκτές, διαδικτυακοί επισκέπτες), πρέπει με σαφή και ευδιάκριτο τρόπο να επισημανθούν, σκιαγραφηθούν και τεκμηριωθούν στις διάφορες συμβάσεις ή σε άλλους όρους χρήσης της πληροφοριακής υποδομής του οργανισμού, με ξεκάθαρες αναφορές όπου χρειάζεται και στην κείμενη θεσμική νομοθεσία για την ασφάλεια (εγχώρια ή/και διεθνή). *Ικανοποιητικοί όροι και ρήτρες* πρέπει να περιληφθούν στις εκάστοτε συμβάσεις και άλλες συμφωνίες που ενέχουν νομικής ισχύος, για να επιτραπεί στη διοίκηση να επιβάλλει τις όποιες, συμβατικές απαιτήσεις ή να επωφεληθεί από κάποιας μορφής αντίμετρου, αλλά πρώτα-πρώτα για να εξασφαλίσει μεγάλο βαθμό εκφοβισμού (deterrence) των επίδοξων παραβατών. Στοχευμένοι και χρηστικά σχεδιασμένοι *μηχανισμοί συλλογής και υποβολής πληροφοριών* (π.χ. συστήματα CRM, KMS και άλλα ηλεκτρονικού εμπορίου και η-επιχειρηματικότητας, σε συνδυασμό με εκτεταμένους μηχανισμούς καταγραφής ουσιωδών δραστηριοτήτων) στα ανώτερα κλιμάκια διοίκησης, *όσον αφορά την καλή σχέση και την τήρηση των συμφωνιών και των όρων με τα εξωτερικά, στρατηγικά μέρη ενός οργανισμού και το περιβάλλον του ιδικού του ΠΣ*, είναι απαραίτητο να υφίστανται, προκειμένου να λαμβάνονται κάθε φορά οι πλέον επωφελείς αποφάσεις στις εκάστοτε δράσεις και προκλήσεις του εξωτερικού περιβάλλοντος.

4.8.4 Κανονιστικοί πόροι και πρότυπα καθοδήγησης

Οι οργανισμοί που αναπτύσσουν ή αναθεωρούν τους ελέγχους, τις πολιτικές και τις διαδικασίες της ασφάλειας πληροφοριών τους έχουν σήμερα ποικίλες πηγές, στις οποίες και μπορούν να βασιστούν για να αντλήσουν υλικό και οδηγίες.[532]

---

[531] Όπως στην προηγούμενη υποσημείωση.

[532] Η τεκμηριωμένη καθοδήγηση και τα διεθνώς αποδεκτά πρότυπα σε θέματα ασφάλειας αποτελούσαν πάντοτε ζητούμενο, τόσο για τις νεοσύστατες επιχειρήσεις, όσο και για τους έμπειρους και κραταιούς οργανισμούς. Σήμερα, είναι ευτυχές πως πληθαίνουν οι συναφείς, συντονιστικοί πόροι, ενώ παρατηρείται και κλιμάκωση της σχετικής τους δράσης.

Καταρχάς, τα νομικά όργανα και οι άλλοι, θεσμικοί ρυθμιστές εντός χωρών αλλά και παγκοσμίως έχουν, όπως είδαμε και σε προηγούμενο εδάφιο, κατά καιρούς εκδώσει πολυάριθμα έγγραφα (συστάσεις, νομοσχέδια) σχετικά με την ασφάλεια Επίσης, οι διάφοροι οργανισμοί έχουν δυνατότητα πρόσβασης στους *χρήσιμους πόρους* εξειδικευμένων εταιρειών της βιομηχανίας της ασφάλειας (συμπεριλαμβανομένων των εξωτερικών ελεγκτών, των συμβουλευτικών και ασφαλιστικών εταιρειών και των οργανώσεων επαγγελματιών στο χώρο της ασφάλειας πληροφοριών) *για την καθοδήγηση τους*. Επιπλέον, πολλοί εθνικοί και διεθνείς φορείς τυποποίησης εργάζονται για να καθορίσουν πρότυπα ασφάλειας πληροφοριών και βέλτιστες πρακτικές για ασφαλείς, ηλεκτρονικές συναλλαγές. Δεν υπάρχει βέβαια προς το παρόν κάποιο επίσημα αποδεκτό, οικουμενικό βιομηχανικό πρότυπο ασφάλειας, εντούτοις αυτές οι μέχρι τώρα προσπάθειες παρέχουν πολύτιμες συγκριτικές μετρήσεις επιδόσεων (benchmarks) διαφορετικών πολιτικών και διαδικασιών, στις οποίες μπορούν να βασιστούν οι οργανισμοί για την ανάπτυξη των δικών τους πρακτικών και στάσεων ασφάλειας ωσότου οι εργασίες τυποποίησης φθάσουν σε κάποιο προφανές αποτέλεσμα. Μερικές από τις πιο γνωστές ομάδες τυποποίησης με σχετικές δράσεις είναι και ακόλουθες οργανώσεις:[533]

- Το εθνικό ίδρυμα προτύπων και τεχνολογίας (NIST, www.nist.gov) με μια πληθώρα συστάσεων και τεχνικών ερευνών και ανακοινώσεων[534].
- Ο διεθνής οργανισμός τυποποίησης (ISO, www.iso.org) με συγκεκριμένα πρότυπα όπως:
    - Ο κώδικας συμπεριφοράς (code of practice) για τη διαχείριση ασφάλειας πληροφοριών (ISO/IEC 17799) και
    - Πληροφορική Τεχνολογία-Τεχνικές για την ασφάλεια-Κριτήρια αξιολόγησης για την ασφάλεια στην τεχνολογία πληροφοριών (ISO/IEC 15408).
- Η ένωση έρευνας και ελέγχου πληροφοριακών συστημάτων (ISACA), με τη συναφή δράση «Στόχοι ελέγχου για την τεχνολογία πληροφοριών» (COBIT, www.isaca.org/cobit.htm).

4.8.5 Εγγενείς Αδυναμίες

Η αποτελεσματικότητα της όλης διαχείρισης της διαδικασίας και των ιδιαίτερων προγραμμάτων ασφάλειας των οργανισμών παρουσιάζει *σημαντικές δυσκολίες*, που αφορούν

[533] Κύρια, βιβλιογραφική αναφορά: [FFIEC-IS].

[534] Όπως η αναφερόμενη στη βιβλιογραφία πηγή: [NIST-ICS].

τόσο τις ανθρώπινες αδυναμίες και τα λάθη/παραπτώματα, όσο και τις τεχνικές ατέλειες, που μπορούν να έχουν διαδικαστικό αντίκτυπο, και εξαρτάται εν τέλει από πολλούς παράγοντες, σαν και αυτούς που ακολουθούν:[535]

- Σχεδιαστικές αδυναμίες και δυσκαμψίες των ΠΣ και των συστημάτων προστασίας τους.
- Ατέλειες Εγκατάστασης και Υλοποίησης των ΠΣ και των συστημάτων προστασίας τους.
- Λάθη στην Παραμετροποίηση των ΠΣ και των συστημάτων προστασίας τους.
- Λειτουργικές αστοχίες, παραλείψεις και παραπτώματα.
- Ανεπάρκεια/Ανεδαφικότητα των μέτρων, των πολιτικών και των ελέγχων ασφάλειας.
- Απουσία ισχυρής βούλησης και δέσμευσης από πλευράς οργάνωσης και διοίκησης και λοιπών φορέων της λήψης αποφάσεων (weak commitment of decision-makers).
- Αδυναμία/Απροθυμία συνολικής συμμόρφωσης στις πολιτικές και τις απαιτήσεις των προγραμμάτων και συστημάτων ασφάλειας.
- Μη ξεκάθαρες ευθύνες και αρμοδιότητες.

Η συνειδητοποίηση των παραπάνω προβλημάτων, σε συνδυασμό με την επίγνωση της διαρκούς ρευστότητας του επιχειρησιακού και του λοιπού, εσωτερικού πλαισίου και εξωτερικού περιβάλλοντος των σύγχρονων οργανισμών, επιβάλλει και επιτάσσει τη συνεχή ανανέωση των εκάστοτε υλοποιημένων στρατηγικών, διαδικασιών και μέτρων προστασίας και τη συντονισμένη, ελεγκτική δράση για την ικανοποιητική εφαρμογή, λειτουργία και απόδοσή τους κατά μήκος του δικτύου συμφερόντων του κάθε οργανισμού, ώστε να εξασφαλίζεται κάθε φορά η καταλληλότητα της επιλεγμένης στρατηγικής, η μέγιστη συμμόρφωση με αυτά που επιβάλλει και επαγωγικά η βέλτιστη αντιμετώπιση των εκάστοτε, σχετικών με την ασφάλεια, περιβαλλοντικών προκλήσεων.

Οι οργανισμοί σήμερα «πλέουν σε μια θάλασσα ρίσκου»[536]. Ο πραγματικός, παρεχόμενος βαθμός ασφάλειας κάθε συστήματος και μηχανισμού προστασίας επιβεβαιώνεται στην πράξη από την αντοχή και προσαρμογή του ΠΣ στις περιβαλλοντικές προκλήσεις (αλλαγές, απειλές)

[535] Κύρια, βιβλιογραφική αναφορά: [FFIEC-IS].

[536] Στην αγγλική, κυρίως, βιβλιογραφία απαντάται πολύ συχνά η έκφραση αυτή ως "sea of risk".

και στην ουσία το ζητούμενο για τον οποιοδήποτε οργανισμό είναι ο μετριασμός του αναμενόμενου κινδύνου σε αποδεκτά για τη στρατηγική του επίπεδα Δεν υπάρχει τελειότητα στην ασφάλεια, τόσο λόγω του ταχύτατα και διαρκώς μεταβαλλόμενου περιβάλλοντος και των τεχνολογικών εξελίξεων, όσο και λόγω των ξεκάθαρων και πιθανών, ενδογενών αδυναμιών, που αναφέρθηκαν παραπάνω. Η κρισιμότητα και ευαισθησία των πληροφοριών και των συστημάτων είναι εκείνη που θα καθορίσει τελικά την απαιτούμενη ασφάλεια και οι οργανισμοί θα κληθούν, αν μη τι άλλο, να ανταπεξέλθουν στις αναγκαιότητες αυτές, κρινόμενοι αναπόφευκτα από την επιτυχία τους στην αποστολή αυτή. Η *έγκαιρη αναγνώριση* των ευπαθών (ανθρώπινων, τεχνικών και διαδικαστικών) σημείων, η *αξιολόγηση του αντίκτυπου* από τις παραβιάσεις/υποβαθμίσεις στην ασφάλεια και ο *κατάλληλος περιορισμός του κινδύνου* (με τη βοήθεια και εφαρμογή διαδικασιών και μηχανισμών πρόληψης, διάγνωσης και ανταπόκρισης) είναι οι πρωταρχικοί, διοικητικοί στόχοι για το κάθε πρόγραμμα και σύστημα διαχείρισης και παροχής ασφάλειας, ενώ μια *διαρκής αναβάθμιση/βελτιστοποίηση διαδικασιών, πολιτικών, μέτρων και μηχανισμών ασφάλειας* πρέπει να είναι εξίσου πρώτο μέλημα, καθώς αποτελεί εχέγγυο προστασίας και ανθεκτικότητας σε βάθος χρόνου.

5 Μελλοντικές κατευθύνσεις έρευνας

Σκοπός του παρόντος τμήματος της διπλωματικής εργασίας είναι η ανάδειξη των πλέον πρόσφατων διαταραχών στην πάντα τρικυμισμένη «θάλασσα» της πληροφοριακής ασφάλειας. Τεχνολογίες αιχμής, ερευνητικά και πρότυπα συστήματα που ευαγγελίζονται εξελίξεις που διατρέχουν όλο το φάσμα ενδεχομένων· από την πλήρη ανοσοποίηση των καίριων δομημάτων, για την πλευρά των υπερασπιστών, έως την ολική κατάρρευση των υποδομών ασφάλειας, προκειμένου για την πλευρά των ραδιούργων. Στα ίδια πλαίσια και τα ολοένα κλιμακούμενα τεκταινόμενα, στις κατά τόπους νομικές καλένδες και τα θεσμοθετήματα των χωρών, με το κέντρο βάρους να στρέφεται στοn εκσυγχρονισμό και την εξύφανση διεθνών και σφαιρικότερων εγγυήσεων, παρά τις συνολικές, διαφαινόμενες ανισότητες, καθώς και τις υπόλοιπες, ειδικότερες αδυναμίες.

Το σίγουρο είναι πάντως πως κάποιες -αν όχι όλες- από τις παρακάτω περιγραφόμενες κυματώσεις θα αποτελούν σύντομα τη νέα πραγματικότητα, φέρνοντας ανακατατάξεις στο ήδη θολό πεδίο της πληροφοριακής αναμέτρησης και της αντίστασης στις πληροφοριακές απειλές και συρράξεις και θα συνεχίζουν να μας απασχολούν για πολύ καιρό ακόμα καθορίζοντας τον ορίζοντα δράσεων και γεγονότων, την κατανομή των δυνάμεων και τις μελλοντικές αλλαγές. Αυτός είναι και ο κύριος λόγος που κρίθηκαν ως άξιες μιας ξεχωριστής μνείας. Στην ουσία, εδώ, υπογραμμίζονται και απομονώνονται οι νεωτερισμοί και νεολογισμοί εκείνοι που πιστεύεται πως θα αποδειχθούν στην πράξη ιδιαίτερου ενδιαφέροντος και συνεισφοράς στη διαμόρφωση καινούριων δεδομένων και που σίγουρα χρήζουν μελλοντικά μιας εξονυχιστικότερης μελέτης.

5.1 Τεχνολογία ιομορφικού ή μη, αυτοαναπαραγόμενου λογισμικού

Ξεκινάμε τη διαδρομή στο μέλλον με αφετηρία ορισμένες, πρόσφατες, τεχνολογικές εξελίξεις που αναδεικνύουν προοπτικές εξυπηρέτησης των ευρύτερων, κυριαρχικών σκοπών του οπλολογισμικού και των επιτιθέμενων, προεξοφλώντας έτσι νέες παθογένειες για τα ΠΣ.

5.1.1 Δυναμική της στεγανογραφίας και των συγκαλυμμένων καναλιών

Τελευταίως ακούγονται και γράφονται πολλά για τις δυνατότητες υποβάθμισης της ασφάλειας πληροφοριών που πηγάζουν από τη χρήση των στεγανογραφικών τεχνασμάτων καθώς και των ευρύτερων απειλών των λεγόμενων συγκαλυμμένων καναλιών (covert channels). Οι μηχανεύσεις αυτές δεν είναι τίποτε άλλο παρά πολύ συγκεκριμένα μέσα για μια *καλά κρυμμένη, όσο περισσότερο μη ανιχνεύσιμη γίνεται, υποβάθμιση της ασφάλειας* ενός συστήματος-στόχου.

- **Στεγανογραφία**

  Η στεγανογραφία είναι έννοια συγγενής της κρυπτογραφίας, που την ακολουθεί στην ιστορική της πορεία ανά τους αιώνες.[537] Ενώ η κρυπτογράφηση βασίζεται στη δημιουργία κωδικοποιημένων εκδοχών των πληροφοριών/μηνυμάτων και κατάλληλης διανομής των «κλειδιών» αποκρυπτογράφησής τους στα συμβαλλόμενα μέρη, η στεγανογράφηση αρέσκεται στο να *φέρει πιο τεχνηέντως τα όποια μυστικά*. Κρυμμένο μήνυμα στη στεγανογραφία δε σημαίνει απαραίτητα και κρυπτογραφημένο, αλλά προϋποθέτει ένα σαφή τρόπο απόκρυψης του από την αδιάκριτη επιθεώρηση και αντίστοιχα μιαν επίσης ομαλή μέθοδο ανακατασκευής του κρυφού νοήματος, γνωστές ιδανικά μόνο στους σκόπιμα προορισμένους/προετοιμασμένους και συνεννοημένους να δεχθούν τις πληροφορίες αυτές.

  Από μια τεχνική σκοπιά, ένα στεγανοποιημένο μήνυμα θα εμφανίζεται συνήθως στα «ανυποψίαστα μάτια» ως κάτι άλλο πιο προφανές και φαινομενικά αβλαβές, το οποίο και αποκαλείται *μέσο κάλυψης (cover medium, stego medium)* των μυστικών δεδομένων.[538] Όσο μεγαλύτερη είναι δυνατότητα του μέσου κάλυψης να μεταφέρει στεγανά μηνύματα

[537] Πηγή: Διαδίκτυο, ιστοχώρος της online εγκυκλοπαίδειας WikiPedia, http://en.wikipedia.org/wiki/Steganography.

[538] Πηγή: "Steganography: Hiding Data Within Data", Gary Kessler, 2001, διαθέσιμο από το δεσμό http://www.garykessler.net/library/steganography.html.

χωρίς να προκαλεί αισθητές και αντιληπτές αλλοιώσεις στην εκ πρώτης όψεως αθώα εικόνα του, τόσο καλύτερο και αξιόπιστο θεωρείται. Το μέτρο αυτής της δυνατότητας ονομάζεται *στεγο-χωρητικότητα (steganographic capacity)*[539] *του μέσου* και αφορά ακριβώς την αποθήκευση και μεταφορά πρόσθετης, συγκαλυμμένης πληροφορίας, χωρίς εμφανή σημάδια καταπόνησης/παραποίησης, που θα μπορούσαν να εκθέσουν/προδώσουν την παρουσία των μυστικών. Η λογική που υποβόσκει στην επιστήμη της στεγανογραφίας[540] περιγράφεται σε γενικές γραμμές από την *προσπάθεια* αυτή *εμφωλιασμού των απόκρυφων πληροφοριών εντός περισσειών ή μη σημαντικών και εύκολα εντοπίσιμων τμημάτων* των εν γένει επαρκούς χωρητικότητας και εγνωσμένης βασικής χρησιμότητας και αποδοχής μέσων κάλυψης, ώστε αυτά να συμβάλλουν αποτελεσματικότερα στο καλύτερο δυνατό καμουφλάρισμα της κρυμμένης πληροφορίας και στη μεγαλύτερη παραπλάνηση των αδιάκριτων/ανυποψίαστων βλεμμάτων. Για την επίτευξη ακόμη περισσότερης αδιαφάνειας και σύγχυσης, τα μυστικά δεδομένα συνήθως κωδικοποιούνται (με χρήση κρυπτογραφικών συναρτήσεων) και διασπείρονται με κάποιον εξεζητημένο αλγόριθμο στην πληροφοριακή «άβυσσο» του μέσου κάλυψης. Μόνο ο εντεταλμένος χρήστης ή διεργασία θα πρέπει να γνωρίζει τους τρόπους[541]:

--ανίχνευσης και εντοπισμού των δομικών λίθων του κρυφού μηνύματος,

--ανασύνθεσης της όλης κωδικοποιημένης πληροφορίας και

--αποκωδικοποίησης του κρυφού νοήματός της.

Τα πάσης φύσεως υδατογραφήματα, τα «αόρατα» στίγματα-σφραγίδες στην ψηφιακή εκτύπωση, εν γένει τα μηνύματα που γράφονται ή αναγνωρίζονται με μέσα φθορισμού, η τυχαία παρεμβολή χαρακτήρων εντός μεγαλύτερου, κατά τα φαινόμενα συνηθισμένου ή/και αδιάφορου κειμένου, όλα αποτελούν γνωστές μορφές στεγανογραφίας[542], στις οποίες η δυσεύρετη σημειολογία ενδέχεται να αποκρύπτει με επιτυχία μια πολύ μεγαλύτερη σημασιολογία. Στην ψηφιακή τεχνολογία όμως των σύγχρονων, δικτυοκεντρικών ΠΣ, η εκτεταμένη παρουσία των *πολυμεσικών αρχείων* με το μεγάλο συνήθως μέγεθος, τη βολική ύπαρξη αρκετών περιττών ή αχρησιμοποίητων εσωτερικών πληροφοριακών περιοχών και την εξαιρετική ανοχή σε τροποποιήσεις και

[539] Κύρια, βιβλιογραφική αναφορά: [CHANDRAMOULI_MEMON-SCAP].

[540] Πηγή: "Steganography Revealed", Kristy Westphal, 2003, διαθέσιμο από το δεσμό http://www.securityfocus.com/infocus/1684.

[541] Κύρια, βιβλιογραφική αναφορά [DANG_KOTA-ISSS].

[542] Κύρια, βιβλιογραφική αναφορά: [BAKSHI-S].

μετασχηματισμούς της ενδότερης δομής τους, όσον αφορά τη διατήρηση της γενικής, συνολικής τους εικόνας, σε συνδυασμό με την ευρύτατη διάδοση και συχνή κυκλοφορία τους τα κάνει να φαντάζουν ως τα ιδανικά μέσα κάλυψης και μεταφοράς στεγο-δεδομένων.[543] Τα πασίγνωστα και ντε φάκτο πανταχού παρόντα πρότυπα όπως αρχεία μουσικής MP3 ή εικόνας JPEG, ακόμα και βίντεο τύπου AVI κτλ, έχει δειχθεί επανηλειμένα πως μπορούν να χρησιμεύσουν αξιοποιώντας τη μεγάλη στεγο-χωρητικότητά τους, για τη διακίνηση κρυμμένων πληροφοριών και μηνυμάτων, με κατάλληλη μεταβολή/αντικατάσταση ορισμένων περιεχομένων τους από το κυοφορούμενο μήνυμα, με τρόπο που δεν αλλοιώνει τα γενικά χαρακτηριστικά τους (ήχος, εικόνα, αντίληψη κίνησης, ταχύτητα, μέγεθος) ή εν πάσει περιπτώσει τα επηρεάζει ελάχιστα και με τρόπο όχι εύκολα αντιληπτό από την απλή επαφή/χρήση ή την ανάλυση με μη εξειδικευμένα εργαλεία (διάσπαρτα και δύσκολα ανιχνεύσιμα bits και bytes εν μέσω πολυμεσικού, πληροφοριακού χάους, από τα οποία για να ανασυνθέσει κανείς το όλο κρυμμένο νόημα χωρίς γνώση του εκάστοτε αλγορίθμου μοιάζει απλά δυσκατόρθωτο έργο).[544]

Μια ακόμη ικανοποιητική δυνατότητα διαβλέπει κάποιος σήμερα και στο εξίσου χαοτικό σημειολογικό-σημασιολογικό περιεχόμενο των διαδικτυακών ιστοχώρων και των διαφόρων εμπλουτισμένων σελίδων τους.[545] Λογισμικό και άτομα μπορούν να τοποθετούν και να ακολουθούν στεγανογραφικά ίχνη κατάλληλα ενσωματωμένα (embedded) στην πληροφοριακή ύλη κατά μήκος του αχανούς WWW νέφους, προκειμένου να μεταφέρουν τα κρυφά τους μηνύματα. Ο *εντοπισμός και η ανάλυση* τοιουτοτρόπως δομημένων και κατανεμημένων δεδομένων *δεν μπορεί να πραγματοποιηθεί με συμβατικά μέσα*[546], καθώς η ύπαρξη του κρυμμένου μηνύματος γίνεται άμεσα αντιληπτή μόνο από όσους γνωρίζουν ήδη την ύπαρξή του και η εκφορά του αντίστοιχα μόνο από εκείνους που κατέχουν τον τρόπο ανασυναρμολόγησής/αποκωδικοποίησής του.

Αν τώρα σκεφτεί κανείς πως εφόσον οι παραπάνω τεχνικές μπορούσαν να εφαρμοστούν πιο οργανωμένα στα πλαίσια επιθέσεων με κακόβουλο λογισμικό, θα παρείχαν ένα εξαιρετικό εφόδιο για μια *μη ευκόλως ανιχνεύσιμη αποθήκευση και επικοινώνηση*

---

[543] Πηγή: "A detailed look at Steganographic Techniques and their use in an Open-Systems Environment", Bret Dunbar, SANS Institute 2002, διαθέσιμο από το δεσμό http://www.sans.org/reading_room/whitepapers/covert/677.php.

[544] Κύρια, βιβλιογραφική αναφορά: [PROVOS_HONEYMAN-HSAIS].

[545] Πηγή: "On Hiding a Message in a Web Page", Bill Grundman, 2003, διαθέσιμο από το δεσμό http://home.comcast.net/~t129wojce647/games/stego/index.html.

[546] Λόγου χάρη σε δοθέν, ύποπτο στεγομήνυμα μια απλή ή πιο σύνθετη αποκρυπτογράφηση δεν αρκεί, χρειάζεται και λειτουργική ανασύνθεση της κυοφορούμενης πληροφορίας, πράγμα αρκετά πιο πολύπλοκο, στα πλαίσια αλγοριθμικής λογικής δοκιμών.

χρήσιμων πληροφοριών στο χώρο ενεργειών μεταξύ δράστη και οπλολογισμικού, αντιλαμβάνεται ότι οι εφαρμογές και εκδηλώσεις που θα προκύψουν (ή ενδεχομένως συμβαίνουν τώρα ή έχουν ήδη συμβεί)[547] ενισχύουν ακόμη περισσότερο την ανθεκτικότητα, ανωνυμία και αξιοπιστία των εκτυλισσόμενων επιθέσεων, τροφοδοτώντας έτσι με νέες ορέξεις και κίνητρα τους συγγραφείς επιζήμιων προγραμμάτων και τους δράστες πληροφοριακών επιθέσεων με όπλα λογισμικού.

- **Συγκαλυμμένα κανάλια επικοινωνίας**

Ένα *συγκαλυμμένο κανάλι (covert channel)* περιγράφεται ως: *"οποιοδήποτε κανάλι επικοινωνίας που μπορεί να γίνει αντικείμενο εκμετάλλευσης από μια διαδικασία για να μεταφερθούν πληροφορίες με τρόπο που να παραβιάζεται η πολιτική ασφάλειας των κείμενων ΠΣ."*[548] Ουσιαστικά, είναι ένα *παρασιτικό κανάλι επικοινωνιών που «κλέβει» εύρος ζώνης από κάποιο άλλο εξουσιοδοτημένο και προνομιούχο κανάλι προκειμένου να διαβιβαστούν πληροφορίες χωρίς την έγκριση ή τη γνώση του σχεδιαστή, ιδιοκτήτη ή χειριστή του νόμιμου καναλιού*, μια μέθοδος επικοινωνίας που δεν είναι μέρος ενός πραγματικού σχεδίου δικτύωσης υπολογιστικών συγκροτημάτων, αλλά εκμεταλλευόμενο τις αδυναμίες/«τρύπες» της πραγματικής κίνησης μπορεί να χρησιμοποιηθεί για να μεταφέρει με απόκρυφο τρόπο πληροφορίες σε χρήστες ή διεργασίες συστημάτων, που υπό κανονικές συνθήκες δεν θα επιτρεπόταν να έχουν πρόσβαση στις πληροφορίες αυτές.[549]

Τα συγκαλυμμένα κανάλια χειρίζονται χαρακτηριστικά έξυπνα ορισμένες ιδιότητες του μέσου επικοινωνιών, με έναν απροσδόκητο, μη συμβατικό ή απλά απρόβλεπτο τρόπο, προκειμένου να διαβιβαστούν πληροφορίες μέσω του διαύλου, χωρίς ανίχνευση από οποιαδήποτε οντότητα, εκτός από εκείνες που ενεργοποιούν και καθορίζουν το συγκαλυμμένο κανάλι.[550] Όλα *τα απόκρυφα κανάλια μειώνουν βέβαια ως ένα βαθμό την απόδοση των νόμιμων διαύλων και αυτό μπορεί να χρησιμοποιηθεί ως ένας έμμεσος τρόπος εντοπισμού τους*· εντούτοις στις προσεκτικά οργανωμένες περιπτώσεις το εύρος ζώνης που απορροφάται είναι συνήθως επίτηδες μικρό και «κρυμμένο» καλά εντός της επιτρεπόμενης και φαινομενικά υπεράνω υποψίας κίνησης μετατρέποντας τα κανάλια αυτά σε εξαιρετικά δύσκολους εχθρούς.

---

[547] Κύρια, βιβλιογραφική αναφορά: [COCHRAN-SCW].

[548] Πηγή: "A Discussion of Covert Channels and Steganography", Mark Owens, SANS Institute 2002, διαθέσιμο από το δεσμό http://www.sans.org/reading_room/whitepapers/covert/678.php.

[549] Πηγή: Διαδίκτυο, ιστοχώρος της online εγκυκλοπαίδειας WikiPedia, http://en.wikipedia.org/wiki/Covert_channel.

[550] Κύρια, βιβλιογραφική αναφορά: [ROGERS-KKUCCC].

Με μια πρώτη ματιά, τα συγκαλυμμένα κανάλια δεν είναι τίποτε παραπάνω από μια *προέκταση των αρχών και πρακτικών της στεγανογραφίας* στο χώρο της δικτυακής μηνυματοδοσίας μεταξύ συνεργαζόμενων κόμβων. Στην τετριμμένη περίπτωση, μάλιστα, μια απλή αποστολή/λήψη μέσω τυποποιημένου δικτύου στεγανο-ποιημένων, πολυμεσικών δεδομένων -όπως περιγράφηκαν στο αμέσως προηγούμενο σκέλος- μεταξύ κακόβουλα προδιατεθειμένων οντοτήτων, κάλλιστα, συνιστά ένα υποτυπώδες, απόκρυφο κανάλι. Στην πράξη, όμως, όταν μιλά κανείς για κατεξοχήν συγκαλυμμένα κανάλια επικοινωνίας, τα διαχωρίζει από τις απλές, στεγανογραφικές τεχνικές, που αφορούν τροποποίηση σε επίπεδο εφαρμογής· *η υπονόμευση προχωρά πλέον στο βάθος των επιπέδων μεταφοράς και δικτύου της OSI αρχιτεκτονικής* και ειδικότερα σε άμεση αναφορά στο παρόν των δικτυοκεντρικών συστημάτων εκμεταλλεύεται υπαρκτές *αδυναμίες* (ή από μια άλλη οπτική διευκολύνσεις) στα πρωτόκολλα TCP/UDP της *TCP/IP στοίβας*.

Μια διερευνητική ματιά στα ενδότερα των επικεφαλίδων των TCP και UDP πρωτοκόλλων, καθώς και της αντίστοιχης του μεταφερόμενου IP «φορτίου» φανερώνει μια πληθώρα προαιρετικών ή αχρησιμοποίητων περιοχών, που μπορούν να εξυπηρετήσουν με πολύ αποτελεσματικό τρόπο σκοπούς αποθήκευσης και μετάδοσης μυστικών δεδομένων, παρέχοντας έντεχνες και δύσκολα ανιχνεύσιμες κρυψώνες.[551] Αν σκεφτεί κανείς μάλιστα πως η έλευση του IPv6 εισάγει στην IP κεφαλίδα μια περίσσεια από 12 bytes (με παράλληλη αύξηση των αχρησιμοποίητων ή προαιρετικών πεδίων), σε σχέση με το τρέχον IPv4, μπορεί να εικάσει πως οι πιθανές θέσεις για το «καταχώνιασμα» στεγανών πληροφοριών μοιάζουν να αυξάνονται επικίνδυνα. Αλλά και σε εγνωσμένα, χρησιμοποιούμενα πεδία των κεφαλίδων αυτών το πρόβλημα που υφίσταται δεν είναι μικρότερο. Ενδεικτικά αναφέρουμε τις δυνατότητες που προκύπτουν από πολύ «διάσημα» τμήματα όπως:[552]

- **Το πεδίο προσδιορισμού πακέτων IP (IP identification field manipulation)**

  Ο αριθμός στο πεδίο αυτό επιλέγεται έτσι, ώστε να αντιστοιχίζεται κατόπιν μετατροπής σε επιθυμητό χαρακτήρα π.χ. ASCII ή άλλης απλής κωδικοποίησης, επιτρέποντας τη διάφανη επικοινώνηση δεδομένων μεταξύ συνεννοημένων οντοτήτων.

---

[551] Κύρια, βιβλιογραφική αναφορά: [DICKMAN-OS].

[552] Πηγή: "Covert Channels in the TCP/IP Protocol Suite", Greg Rowland, 1997, διαθέσιμο από το δεσμό http://www.firstmonday.org/issues/issue2_5/rowland/.

Επειδή το πεδίο αυτό ευρίσκεται εντός της IP επικεφαλίδας, είναι σχετικά ευάλωτο σε φιλτράρισμα και απώλεια πληροφορίας λόγω επανεγγραφής από τα διάφορα αντιπυρικά συστήματα.

- **Το πεδίο αρχικού αριθμού ακολουθίας TCP (TCP ISN forging)**[553]

  Με την ίδια λογική, ο 32-bit-ος αυτός αριθμός (μέγεθος ικανό για αποθήκευση αρκετών δεδομένων σε λίγα μόλις πακέτα) αποκωδικοποιείται στο δέκτη της μυστικής επικοινωνίας σε χρήσιμη πληροφορία, με βάση κάποιο -συμφωνημένο μεταξύ των συναλλασσόμενων μερών- πρότυπο κωδικοποίησης.

  Το γεγονός πως το πεδίο αυτό εδρεύει στην TCP κεφαλίδα -αποτελώντας μάλιστα το πρώτο και αναντικατάστατο κομμάτι κάθε TCP χειραψίας- σημαίνει πως η συνδιαλλαγή είναι εγγενώς προστατευμένη από τις «ανεπιθύμητες» παρεμβάσεις ενός αντιπυρικού τείχους.

- **Τα πεδία διευθύνσεων και θυρών πηγής&προορισμού καθώς και το flag TCP SYN (TCP ASN bouncing)**

  Η παραποίηση των πεδίων διευθύνσεως και θύρας πηγής σε συνδυασμό με την κατάλληλη κωδικοποίηση του TCP ISN (initial sequence number), όπως αυτή αναλύθηκε αμέσως πριν, αποτελούν τα μέσα για την εξαπόλυση πακέτων προς «κρυμμένες» οντότητες, με την ταυτόχρονη προσποίηση πως αυτά κατευθύνονται σε αξιόπιστο και ασφαλή προορισμό. Ο επιλεγμένος, αξιόπιστος εξυπηρετητής της κίνησης που λαμβάνει τα δεδομένα αποστέλλει την όποια απάντηση στην τροποποιημένη εκδοχή της πηγής, που στην ουσία είναι το τρίτο, κρυφό μέρος της επικοινωνίας, και όχι στην πραγματική προέλευση τους. Μαζί με την απάντηση στέλνεται στον τρίτο πόλο και ο αρχικός αριθμός ακολουθίας TCP (ως μέρος της επαλήθευσης στη φάση της TCP χειραψίας) επαυξημένος κατά ένα, που περιέχει και τα κωδικοποιημένα, μυστικά δεδομένα.[554] Μάλιστα λαμβάνεται ειδική μέριμνα, ώστε ο συνδυασμός των πεδίων της επικεφαλίδας να υπερπηδά ακόμη και τυχόν υποτυπώδη SPI φίλτρα πακέτων που καραδοκούν στο χώρο δράσης του τρίτου μέρους, που δεν έχει πραγματικά εκκινήσει την επικοινωνία, αλλά γίνεται

---

[553] Κύρια, βιβλιογραφική αναφορά: [MURDOCH_LEWIS-ECCTI].

[554] Στην TCP χειραψία ισχύει: $newisn = isn + 1$, σε κάθε πακέτο της χειραψίας και για κάθε συναλλασσόμενο μέρος/άκρο της επικοινωνίας.

φαινομενικά απροσδόκητος δέκτης αυτής.[555] Πάντως, μια πιο σοφά σχεδιασμένη επάνω σε πίνακες κατάστασης, αποτρεπτική μέθοδος, σε συνδυασμό με κάποιου είδους ενσωματωμένους, επιπέδου εφαρμογής ελέγχους φέρει σε γενικές γραμμές τους σπόρους απόρριψης των συγκαλυμμένων πακέτων, μαζί παράλληλα με την όποια έγερση υποψιών και σύσταση (προσωρινής ή μόνιμης) επιφυλακής, για παρόμοιες προσπάθειες επικοινωνίας, από τους μηχανισμούς ασφάλειας των συστημάτων.

Είναι ευτυχές το γεγονός πως αυτού του είδους η μέθοδος επίθεσης περιορίζεται, συνήθως, σε κρυφούς διαλόγους εντός τοπικών δικτύων, καθώς το λογισμικό των κεντρικών, αντιπυρικών μηχανισμών[556] είναι συνήθως προγραμματισμένο να απορρίπτει τιμές στα πεδία διεύθυνσης πηγής, που δεν ανήκουν στο εσωτερικό δίκτυο. Παρόλ' αυτά, συμβαίνει ένας τέτοιος έλεγχος να μην είναι πάντοτε ενεργοποιημένος εξ αρχής και να χρειάζεται η ανθρώπινη επέμβαση για τη σωστή διαμόρφωση του δικτυακού μηχανισμού άμυνας. Έτσι, η όποια παράλειψή του μπορεί να οδηγήσει σε δυσάρεστες, συγκαλυμμένες καταστάσεις.

Τα συστήματα ανάλυσης και αποδοχής/απόρριψης δικτυακών πακέτων και μηνυμάτων, που αποτελούν το μέτρο της επιβολής ασφάλειας στις επικοινωνίες, βασίζονται και επιμένουν στην πλειοψηφία τους σε μια *σημειολογική ανίχνευση (αριθμητικού τύπου έλεγχος εγκυρότητας)* ορισμένων βασικών πεδίων των παραπάνω κεφαλίδων, χωρίς να προβαίνουν σε λεπτομερή εξέταση όλων των περιοχών τους, πόσο μάλλον των προαιρετικών και συνήθως αχρησιμοποίητων. Ακόμα και στην περίπτωση περιοχών που αποτελούν γνωστά σημεία ανάλυσης, τα συστήματα προστασίας, αν και παρακολουθούν τις τιμές των εν λόγω πεδίων, εμφανίζονται μάλλον εγγενώς αδύναμα μπροστά σε μια νόμιμη τιμή των περιεχομένων που μπορεί να επιδέχεται *κάποιας μορφής σημασιολογικού τύπου «μετάφρασης» μεταξύ των 2 μερών ενός άξονα συγκάλυψης*. Τέλος, τυχόν ανθρώπινες αβλεψίες στην κατάλληλη παραμετροποίηση των συστημάτων αυτών αποδεικνύονται ιδιαίτερα επωφελείς για την ευκολότερη εγκαθίδρυση και διατήρηση κρυφών συνομιλιών. Αυτά εν ολίγοις αποδίδουν το όλο νόημα των τεχνικών «στεγανογραφικής» τροποποίησης/παραποίησης στα επίπεδα δικτύου και μεταφοράς, που ουσιαστικά εκθέτουν τους μηχανισμούς ασφάλειας χτυπώντας τους στην «αχίλλειο πτέρνα» των μέχρι πρόσφατα θεσφάτων επιλογής, ρύθμισης και χειρισμού των

[555] Δυστυχώς, όπως βλέπουμε στην πράξη, μια απλή SPI προσέγγιση είναι τρωτή και δεν επαρκεί σε περιβάλλοντα υψηλού κινδύνου.

[556] Όπως αυτά που μελετήθηκαν κατά μήκος του εδαφίου 4.1.

ελεγχόμενων πεδίων/τιμών απόφασης. Μόνο τα εξαιρετικά σχεδιασμένα και ιδανικά σταθμισμένα, αποτρεπτικά μέσα, που πραγματοποιούν σύνθετους ελέγχους και στο επίπεδο εφαρμογής (deep packet inspection, DPI), μπορούν να υπομείνουν τη *διαπεραστική ικανότητα* των συγκαλυμμένων πακέτων, απαγορεύοντας την απευθείας συνδιάλεξη μεταξύ λογικά διαχωρισμένων περιοχών των δικτύων.[557] Τέτοια αμυντικά συστήματα βέβαια δεν αποτελούν σήμερα τον κανόνα.

Εφαρμογές των συγκαλυμμένων καναλιών, λοιπόν, υπάρχουν άφθονες αρχής γενομένης από την απλή παράκαμψη των φίλτρων πακέτων, ανιχνευτών παρείσφρυσης και άλλων αναλυτών/ελεγκτών δικτυακής κίνησης (sniffers, proxies), προχωρώντας στην ενθυλάκωση κρυπτογραφημένης ή μη «παράνομης» πληροφορίας εντός νόμιμων πακέτων για σύναψη μυστικής επικοινωνίας και φθάνοντας στην αποκορύφωση με την απόκρυψη του πραγματικού προορισμού των μεταδιδόμενων απόκρυφων δεδομένων, χάρη στην παραχάραξη πακέτων με παραλήπτες τοποθεσίες εκ των προτέρων διαπιστωμένες ως αβλαβείς και αξιόπιστες (bouncing). Ως εκ τούτου, συντονισμένες προσπάθειες συγγραφής κακόβουλου, αυτοαναπαραγόμενου λογισμικού, που θα μπορεί να εκμεταλλεύεται με τον πλέον αποδοτικό τρόπο αυτές τις ευνοϊκές συνθήκες, κάνοντας καλά ενορχηστρωμένη χρήση των καναλιών συγκάλυψης, αναμένεται να κλιμακωθούν στο άμεσο μέλλον.[558]

Αναλογίζεται, λοιπόν, κανείς το μέγεθος της αναπτυσσόμενης δυναμικής για τους σκοπούς της πληροφοριακής εχθροπραξίας και τους νέους ορίζοντες που διανοίγονται, ειδικότερα για το κακόβουλο λογισμικό, συνολικά από τις τεχνολογίες στεγανογραφίας και συγκαλυμμένης επικοινωνίας και άμεσα προκύπτει το λογικό συμπέρασμα πως ό,τι βλέπουμε δεν είναι παρά μόνο η αρχή όσον αφορά τις δράσεις βασισμένου σε αυτές τις ευκαιρίες επιβλαβούς λογισμικού. Ήδη τα γνωστά rootkits παρέχουν, όπως θα δούμε παρακάτω, ένα πολύ αξιόλογο και ισχυρό πλαίσιο για την υλοποίηση και περαιτέρω αξιοποίηση αυτών των μεθόδων από ιούς και σκουλήκια. Πάντως, η μέχρι στιγμής εικόνα έχει θορυβήσει αρκετά πολλούς υποστηρικτές της ασφάλειας των πληροφοριών, που προτρέπουν με διάφορες αξιοπρόσεχτες συνεισφορές (που θα παρουσιαστούν πιο λεπτομερώς στα μετέπειτα εδάφια) για γοργά βήματα αντιμετώπισης του κινδύνου που φαίνεται να έχει ανακύψει.

---

[557] Πηγή: "Firewall Evolution - Deep Packet Inspection", Ido Dubrawsky, 2003, διαθέσιμο από το δεσμό http://www.securityfocus.com/infocus/1716.

[558] Κύρια, βιβλιογραφική αναφορά: [RUTKOWSKA-FSMTVOS], [RUTKOWSKA-RSbDM].

5.1.2 Ευκαιρίες από την υπονόμευση των Λ/Σ

Στις μέρες μας, οι εργασίες παραβίασης κι υποβάθμισης της ασφάλειας των συστημάτων έχουν γίνει περισσότερο συστηματικές, με την έλευση και εκτεταμένη χρήση της τεχνολογίας της εκ βαθέων υπονόμευσης των Λ/Σ. Οι επίβουλες αυτές προσπάθειες έχουν βρει τον κυριότερο εκφραστή τους, στο πρόσωπο των λεγόμενων τεχνικών του λογισμικού φαντασμάτων, που είναι περισσότερο γνωστό με το όνομα rootkit. Ο τελευταίος όρος ξεκίνησε να χρησιμοποιείται πριν από μια περίπου δεκαετία, για να περιγράψει το σύνολο των προγραμμάτων και του κώδικα, που επιτρέπουν μια παραμένουσα ή απλά συμπαγή, μη ανιχνεύσιμη (κρυφή) παρουσία σε κάποιο υπολογιστικό σύστημα.[559] Το σημείο-κλειδί είναι η συνθήκη μη ανιχνευσιμότητας στην παράβαση.

Στις πρώτες τους ενσαρκώσεις, τα φαντάσματα έδρευαν *στο επίπεδο του χρήστη (user-mode, user-level)* εκτελώντας τον κώδικά τους με μέγιστα δικαιώματα αυτά του πιο προνομιούχου λογαριασμού χρήσης.[560] Αυτό όμως περιόριζε σημαντικά την επιτυχία της εγκατάστασής τους, καθώς ενείχε τον ρεαλιστικό κίνδυνο αποκάλυψης της παρουσίας τους λόγω των αυξημένων δυνατοτήτων διάγνωσης ανωμαλιών και καταγραφής δραστηριοτήτων στο επίπεδο αυτό. Στις σύγχρονές τους εκδοχές, «πακετάρονται» πλέον ως επί το πλείστον σαν προγράμματα οδήγησης συσκευών υλικού (device drivers) ή εικονικών μηχανών (virtual machine (device) drivers) και με αυτόν τον τρόπο καταφέρνουν να παρεισφρύσουν *στα ενδότερα στρώματα του πυρήνα των Λ/Σ (kernel-mode, kernel-level)*, αποκτώντας παράλληλα τα υπερπρονόμια επεξεργασίας και διαχείρισης που συνοδεύουν τις εκείθεν ορμώμενες διεργασίες. Το αποτέλεσμα της εισχώρησης, που πρακτικά είναι δύσκολα εντοπίσιμο από τους εξωτερικούς παρατηρητές, συνίσταται στο πιο συχνό υπόδειγμα σε ελαφρές, καλοσχεδιασμένες τροποποιήσεις του «πυρηνικού, γενετικού υλικού».

Στο επίπεδο του πυρήνα, τα rootkits *ενεργούν ως μέρος του Λ/Σ* και έτσι έχουν τη δυνατότητα να παρεμβαίνουν πλέον και να επηρεάζουν κατά βούληση όλες τις βασικές, λειτουργικές διαδικασίες, όπως είναι η διαχείριση των διεργασιών, η πρόσβαση στο αρχεία δεδομένων, ο έλεγχος και η εκτέλεση των εγγενών αμυντικών μηχανισμών, η πρόσβαση στο δίκτυο και η διαχείριση της μνήμης, που συντονίζονται από το κεντρικό αυτό σημείο, και μάλιστα με τρόπο -εκ κατασκευής του Λ/Σ- μη ευδιάκριτο, μη κατανοήσιμο και δυσκόλως αναγνωρίσιμο από τους τελικούς χρήστες των συστημάτων και τις διεργασίες επιπέδου χρήστη.[561] Δεν είναι καθόλου τυχαίο λοιπόν το γεγονός πως η πλειοψηφία των χρηστών σπάνια συναινεί σε

---

[559] Κύρια, βιβλιογραφική αναφορά: [BUTLER_HOGLUND-ROOTKITS].

[560] Ο λογαριασμός αυτός στα τύπου UNIX Λ/Σ φέρει το χαρακτηριστικό όνομα root (=ρίζα), από όπου και προέκυψε και ο όρος root-kit, δηλαδή εργαλειοθήκη για την απόκτηση και διατήρηση πρόσβασης, με μέγιστα δικαιώματα, σε υπό εξέταση σύστημα.

[561] Κύρια, βιβλιογραφική αναφορά: [BUTLER_HOGLUND-VICE].

ενδεχόμενη παρουσία τους αντιμετωπίζοντας τα ούτε λίγο ούτε πολύ σαν μη εγκεκριμένα παράσιτα, ακόμα και όταν επιτελούν επωφελές έργο. Οι ερευνητές της ασφάλειας πληροφοριών είναι εξίσου επιφυλακτικοί μπροστά στη χρήση rootkit μεθόδων για την ενίσχυση της προστασίας των συστημάτων, παρά τις αδιαμφισβήτητα επαυξημένες ικανότητες που αυτές φέρονται να προσδίδουν στα τεχνάσματα της πληροφοριακής άμυνας.[562] Η πιθανότητα ύπαρξης τεχνικών αδυναμιών και σφαλμάτων υλοποίησης ενός καλοπροαίρετου φαντάσματος ή/και ενός συνακόλουθου κενού ασφάλειας, που αυτό άθελά του εισάγει, δύνανται να καταστήσουν ένα σύστημα «υπογείως» ευάλωτο και εγείρουν μοιραία επαρκείς συγκυρίες συγγραφής ενός κακόβουλου προγράμματος, που θα μπορεί να εκμεταλλεύεται τις ευπάθειες αυτές, για να χαλιναγωγήσει ιδανικά προς όφελός του τις αστείρευτες δυνάμεις της υπονόμευσης.

Για να συνειδητοποιήσουμε καλύτερα το μέτρο των συνιστάμενων, απεριόριστων επιλογών συνοψίζουμε ξανά παρακάτω ορισμένες από τις βασικές δυνατότητες της rootkit τεχνολογίας, που πηγάζουν από τη *δράση στην καρδιά ενός Λ/Σ και την κατάλληλη τροποποίηση των πιο κεντρικών και βασικών συστατικών του*[563]:

1. Απόκρυψη διεργασιών στην κύρια μνήμη.
2. Απόκρυψη αρχείων στο σύστημα αρχειοθέτησης.
3. Κεντρικός συντονισμός και παρακολούθηση λειτουργικών δραστηριοτήτων (μνήμη, επεξεργαστής, κάρτα δικτύου).
4. Έλεγχος εγγενών μηχανισμών ασφάλειας (αυθεντικοποίηση-έλεγχος πρόσβασης-καταγραφή).
5. Προνομιακή πρόσβαση σε κατώτερου επιπέδου, κρίσιμες πληροφορίες και ρουτίνες.

Από τα παραπάνω, με εύκολο τρόπο, συμπεραίνει κανείς τις μεγάλες ευκαιρίες και τα πολλαπλά κέρδη που προκύπτουν από μια κακόβουλη χρήση των rootkit προνομίων από τα προγράμματα ιών και σκουληκιών.

Το λογισμικό φαντασμάτων μπορεί και γίνεται αισθητό, επίσης, χάρη στην *εξαιρετική του ιδιότητα να συμπορεύεται με τις εξελίξεις και να αναπροσαρμόζει ταχύτατα τις μεθόδους του*, ενστερνιζόμενο τις όποιες καινούριες ιδέες και πρακτικές από το χώρο των Λ/Σ και της

---

[562] Πηγή: "Anti-spyware Battles Rootkits with Rootkit Tactics", Paul Roberts, 2005, διαθέσιμο από το δεσμό http://www.eweek.com/c/a/Security/Antispyware-Battles-Rootkits-with-Rootkit-Tactics/.

[563] Κύρια, βιβλιογραφική αναφορά: [BUTLER_HOGLUND-ROOTKITS].

ψηφιακής επικοινωνίας. Τρεις αξιοσημείωτες τεχνοτροπίες, που προέρχονται από συναφείς τομείς, φανερώνουν τα πολυάριθμα σενάρια αξιοποίησης μιας rootkit υπονόμευσης και αναφέρονται ενδεικτικά ακολούθως:

- **Υπονόμευση μέσω εικονικοποίησης**[564]

  Στην ερευνητική εργασία[565] των Peter Chen και Samuel King του Michigan University και ομάδας ειδικών από τη Microsoft Research απομονώνεται μια ιδιαίτερη κλάση rootkit (VMBR[566]), που αναβαθμίζει τις επεκτατικές δυνατότητες της υπονόμευσης μεταφέροντας το επίκεντρό της σε ακόμη χαμηλότερο του πυρήνα και σημαντικότερο του από πλευράς λειτουργιών επίπεδο. Το πρόγραμμα SubVirt που υλοποιήθηκε στα πλαίσια της δημοσίευσης είναι λογισμικό πλήρους εικονικοποίησης (VMM), που δημιουργεί ένα ανεξάρτητο υπόστρωμα στο οποίο και επικάθεται πλέον το Λ/Σ το οποίο παρήγγειλε την εκτέλεσή του (καθώς και κάθε άλλο εγκατεστημένο στο ίδιο μηχάνημα λειτουργικό) με μη αντιληπτό για εκείνο τρόπο και το οποίο είναι ικανό να φιλοξενήσει, σε χώρο μακριά από τα αδιάκριτα μάτια και με ελάχιστα περιθώρια ανίχνευσης, πάσης φύσεως κακόβουλες δραστηριότητες. Η δύναμη του SubVirt έγκειται στις παρεχόμενες δυνατότητες εξωτερικού ελέγχου και παρέμβασης στα Λ/Σ από το κατώτερο κέλυφος που παράγει η εικονική μηχανή, έτσι ώστε η όποια επιβλαβής λειτουργία να περνάει σχεδόν απαρατήρητη από διεργασίες και χρήστες εντός του υπερκείμενου Λ/Σ (ακόμα και ευρισκόμενες στο επίπεδο του πυρήνα).

  Σε μια αντίστοιχη προσπάθεια, η αναλυτής ασφάλειας Joanna Rutkowska παρουσιάζει τη δική της εκδοχή κακόβουλης εικονικοποίησης, το περίφημο rootkit με την κωδική ονομασία Red Pill.[567] Το συγκεκριμένο πρόγραμμα εκμεταλλεύεται την ύπαρξη της λεπτής υπερεποπτικής επίστρωσης (thin hypervisors) στα νέα Λ/Σ της Microsoft Windows Vista και Longhorn Server, όπου και εγκαθίσταται. Από εκεί απολαμβάνει καρπούς μέγιστης απόκρυψης και καθολικών προνομίων επί των ανώτερων Λ/Σ και των καθηκόντων τους.

---

[564] Βλέπε σε αντιδιαστολή και προς σύγκριση και το αντίστοιχο εδάφιο 5.2.1, περί δυναμικής της εικονικοποίησης στην ασφάλεια πληροφοριών.

[565] Κύρια, βιβλιογραφική αναφορά: [CHEN_KING-SubVirt].

[566] Virtual-Machine Based Rootkit, που αποδίδεται ως rootkit βασισμένο σε εικονική μηχανή ή λογισμικό εικονικοποίησης.

[567] Κύρια, βιβλιογραφική αναφορά: [RUTKOWSKA-VOSC].

- **Υπονόμευση σε επίπεδο BIOS[568] και περιφερειακών συσκευών[569]**

Η υπονόμευση βέβαια μπορεί να προχωρήσει και ακόμη βαθύτερα φθάνοντας καμιά φορά και τα έγκατα της μονάδας BIOS ή των περιφερειακών υλισμικών (κάρτα ήχου-κάρτα γραφικών-μόντεμ κτλ), όταν δεν υλοποιείται κάποιο εξειδικευμένο μέτρο προστασίας της εκεί ευρισκόμενης ηλεκτρονικά προγραμματίσιμης, τύπου ROM, μνήμης επέκτασης.[570] Άπαξ και ένα φάντασμα τοποθετηθεί σε αυτά τα επίπεδα, που αρχικοποιούνται πολύ πριν από την επίδοση της σκυτάλης ελέγχου στο λειτουργικό, τα πράγματα είναι άσχημα· το Λ/Σ δεν είναι πια σε θέση να αναγνωρίζει με άνεση την παρουσία και δράση του εν λόγω προγράμματος, το οποίο μπορεί πλέον να δρα χωρίς προφανείς οχλήσεις από τους βασικούς, εγγενείς και πρόσθετους μηχανισμούς ασφάλειας[571].

Η υπό συζήτηση περίπτωση υπονόμευσης καθώς και η αντίστοιχη μέσω εικονικοποίησης αποτελούν χαρακτηριστικά παραδείγματα αυτού που η Rutkowska αποκαλεί γλαφυρά *κακόβουλο πρόγραμμα τύπου III (type III malware)*[572], λογισμικού δηλαδή που έχει τη δυνατότητα να εκτελείται σε κάποιο υπολογιστικό σύστημα με εξαιρετικά ανεπαίσθητο τρόπο, χειραγωγώντας το και πραγματοποιώντας γενικά επιζήμιες από πλευράς ασφάλειας πληροφοριών διεργασίες, χωρίς όμως να αφήνει πίσω σε αυτό κανένα πρόδηλο ίχνος, που θα μπορούσε ίσως να χρησιμεύσει για τον εντοπισμό του.

- **Ακόμη πιο συγκαλυμμένες επικοινωνίες[573]**

Τα φαντάσματα συνεργάζονται περίφημα με γνωστές από το πεδίο των συγκαλυμμένων καναλιών ιδιότητες, για να παράγουν έναν πολύ χρήσιμο από άποψη ανωνυμίας, αλλά συνάμα θανάσιμο συνδυασμό, λόγω των κινδύνων που εγκυμονεί για παράνομη και κακόβουλη δράση. Η rootkit πρόσβαση σε θεμελιώδεις, εξειδικευμένες συναρτήσεις ελέγχου του Λ/Σ σχετικά με το χειρισμό των δικτυακών επικοινωνιών παρέχει ένα εύφορο έδαφος για την αμεσότερη, ευκολότερη και πιο προστατευμένη εγκατάσταση, διατήρηση και εποπτεία των απόκρυφων καναλιών.[574]

---

[568] Πηγή: "Researchers: Rootkits headed for BIOS", Robert Lemos, 2006, διαθέσιμο από το δεσμό http://www.securityfocus.com/news/11372.

[569] Κύρια, βιβλιογραφική αναφορά: [HEASMAN-IDAPCIR], [HEASMAN-IDABR].

[570] Πηγή: Διαδίκτυο, ιστολόγιο AntiRootkit Blog του, βαρύνουσας σημαντικότητας για κάθετι σχετικό με την τεχνολογία των rootkits, ιστοχώρου antirootkit.com, http://www.antirootkit.com/blog/category/bios-rootkits/.

[571] Όπως προσεγγίστηκαν και διασαφηνίστηκαν οι εν λόγω μηχανισμοί στο κεφάλαιο 4 και τα ανάλογα εδάφια.

[572] Κύρια, βιβλιογραφική αναφορά: [RUTKOWSKA-ISMT].

[573] Στη λογική που διέπει το σχετικό εδάφιο 5.1.1.

[574] Κύρια, βιβλιογραφική αναφορά: [RUTKOWSKA-CHAMELEON].

Από πλευράς εισαγωγής και παραμονής σε ένα σύστημα, τα προγράμματα των φαντασμάτων *επιβουλεύονται ένα σύνολο από μη επαρκώς τεκμηριωμένες, χαμηλού επιπέδου ρουτίνες, σε συνδυασμό με εγνωσμένες τεχνικές ατέλειες των Λ/Σ, για να εγκαταστήσουν και να εγγράψουν τους εαυτούς τους ως παρασκηνιακές διεργασίες υψηλής προτεραιότητας και μέγιστων εξουσιοδοτήσεων*.[575] Οι διεργασίες αυτές μπορούν να δρουν με μη άμεσα αντιληπτό από τους χρήστες και ανιχνεύσιμο από μη εξειδικευμένα προγράμματα τρόπο, καθώς φαίνεται πως απουσιάζουν από τη συνηθισμένη επισκόπηση του συστήματος, ενώ οι ίδιες καταφέρνουν να φορτώνονται -περιστασιακά ή με πιο μόνιμο τρόπο- στη μνήμη και να εκτελούνται ανενόχλητες μέχρι να αφαιρεθούν τρόπον τινά από την κύρια μνήμη (random memory-residents) ή/και τις συσκευές αποθήκευσης (constant, non-volatile residents).[576]

Τα rootkits από μόνα τους *δε διαθέτουν ξεκάθαρα επιβλαβή χαρακτήρα*, πέρα ίσως από τη *μη προβλεπόμενη και μη συνηθισμένη τροποποίηση*, που εισάγουν σε στοιχεία του λογισμικού οδήγησης και λειτουργίας των επεξεργαστικών κόμβων, και την *αναπόφευκτη αδιαφάνεια στη δράση τους*, αλλά οφείλουν πρώτα-πρώτα την κακή τους φήμη και την όποια προκατάληψη στον *«επιθετικό» τρόπο τοποθέτησης* και τις *πιθανές, εφιαλτικές συνέπειες από τη λειτουργία τους, στα άδυτα των συστημάτων*. Μπορούν, όμως, να αποτελέσουν πρώτης τάξεως δύναμη πυρός για τις κακόβουλες προθέσεις των αυτοαναπαραγόμενων όπλων και των πληροφοριακών μαχητών, που εκμεταλλευόμενοι τις άμεσες και έμμεσες επιπτώσεις rootkit παρουσίας και δράσης καταφέρνουν μια σε βάθος υπονόμευση και χειραγώγηση των υπολογιστικών συστημάτων. Οι υστερόβουλες χρήσεις του λογισμικού φαντασμάτων από τους φορείς πληροφοριακής εχθροπραξίας εστιάζονται κυρίως στους τομείς της με δόλο απομακρυσμένης διαχείρισης και καθοδήγησης ΠΣ και της παράνομης παρακολούθησης ή υποκλοπής δεδομένων και επικοινωνιών, που ως γνωστόν κάλλιστα είναι ικανές να επιφέρουν και πρόσθετες ή σε δεύτερο χρόνο επιθέσεις, στη λογική της χιονοστιβάδας.[577]

Όσον αφορά την μέχρι στιγμής αντιμετώπιση των φαντασμάτων και των προβλημάτων υπονόμευσης που αυτά κομίζουν (anti-rootkit technology), η επιστήμη και η αγορά συγκλίνουν σε «εντός των τειχών» λύσεις (βλέπε και επόμενο εδάφιο 5.2.5 για θωράκιση κόμβων), όπως τα συστήματα hIPS ή άλλα εξεζητημένα εργαλεία ανάλυσης[578] (ως ξεχωριστά

---

[575] Πηγή: "Windows rootkits of 2005, part one", James Butler and Sherri Sparks, 2005, διαθέσιμο από το δεσμό http://www.securityfocus.com/infocus/1850.

[576] Πηγή: "Windows rootkits of 2005, part two", James Butler and Sherri Sparks, 2005, διαθέσιμο από το δεσμό http://www.securityfocus.com/infocus/1851.

[577] Κύρια, βιβλιογραφική αναφορά: [BUTLER_HOGLUND-ROOTKITS].

[578] Πηγή: "Windows rootkits of 2005, part three", James Butler and Sherri Sparks, 2005, διαθέσιμο από το δεσμό http://www.securityfocus.com/infocus/1854.

προγράμματα ή ως μέρη σουΐτας αντι-κακόβουλων εφαρμογών) που εφαρμόζουν τεχνικές παρόμοιες στη σύλληψη ή ίδιες με τα rootkits, αλλά με πιο διάφανο στο χρήστη τρόπο και χωρίς ιδανικά να προκαλούν μόνιμες τροποποιήσεις ή αλλοιώσεις στα συστήματα, πέραν της διάρκειας εκτέλεσής τους. Μια ακόμη, ευρέως διαδεδομένη μέθοδος ανίχνευσης μιας υπονόμευσης του Λ/Σ είναι η *παθητική και σε άεργη φάση (offline) σύγκριση των περιεχομένων* του υπό εξέταση συστήματος με ένα «καθαρό» αντίστοιχό του,[579] τουλάχιστον σε επίπεδο δεδομένων πυρήνα· το μέγεθος και η βαρύτητα των όποιων διαφοροποιήσεων υπονοούν την παρουσία σκόπιμων αλλαγών και σηματοδοτούν το εύρος της υπονόμευσης. Τέλος, πολλές βάσιμες προσδοκίες πρόληψης φαίνεται πως αναπτύσσονται τελευταία και στον τομέα της επιβεβαίωσης των Λ/Σ, το ιδιαίτερο σχήμα της οποίας αναλύεται σε επόμενη ενότητα του τρέχοντος κεφαλαίου.

Πάντως, σε γενικές γραμμές, *η στοχευμένη, προστατευτική δράση εναντίον των απειλών τύπου rootkits βρίσκεται εν πολλοίς ακόμη στα σπάργανα ή σε νηπιακή ηλικία*, επιτρέποντας την αποτελεσματική εξαπόλυση και σχετική επιτυχία μεθοδικά στημένων και ενορχηστρωμένων, βασισμένων σε φαντάσματα, πληροφοριακών επιθέσεων.[580] Σαν κατακλείδα του τρέχοντος σκεπτικού αξίζει να αναφέρουμε πως σε πλείστες περιπτώσεις ακόμη και αν ανιχνευθεί επιτυχώς μια υπονόμευση και εντοπιστούν τα διάφορα, συστατικά της μέρη, η πλήρης απομάκρυνση τους έρχεται με τίμημα τη μεγάλη πιθανότητα για σοβαρές βλάβες ή άλλες, ανεπιθύμητες παρενέργειες στο υπάρχον ΠΣ[581]· τα rootkits φημίζονται για το ότι αναπτύσσουν μια *πολύ συμβιωτικού χαρακτήρα σχέση* με το σύστημα που τα «φιλοξενεί». Είναι ευτυχές που τα *φαντάσματα υφίστανται τουλάχιστον τους περιορισμούς και τις εξαρτήσεις που επιβάλλουν οι διαφορετικές αρχιτεκτονικές υλικού και οικογένειες Λ/Σ*[582] - ακουμπώντας ακροθιγώς και το για πολλοστή φορά ανακύπτον ζήτημα της πλουραλιστικής αναγκαιότητας και σπουδαιότητας-, αλλιώς θα μιλούσαμε τώρα για έναν ακατανίκητο «δήμιο και δυνάστη» των ΠΣ.

Το μήνυμα είναι σαφές: Παρατηρείται, πλέον, ξεκάθαρα, μια *ακατανίκητη έλξη των κυβερνοκακοποιών προς τις επιτηδευμένες τεχνικές υπονόμευσης*, που μεταφράζεται σε μια πρόδηλη αύξηση στους ρυθμούς παραγωγής και εξάπλωσης των προγραμμάτων που

---

[579] Πηγή: Διαδίκτυο, ιστοχώρος της online εγκυκλοπαίδειας WikiPedia, http://en.wikipedia.org/wiki/Rootkit.

[580] Πηγή: "Rootkits in the mist", Pedro Bustamante, 2007, διαθέσιμο από το δεσμό http://research.pandasecurity.com/archive/Rootkits-in-the-mist.aspx.

[581] Η σε βάθος προσβολή ενός συστήματος, με τρόπο πολλές φορές ανεξιχνίαστο-απρόβλεπτο, συχνά δεν επιτρέπει την αφαίρεση ενός rootkit, χωρίς την παράλληλη και μη αναστρέψιμη καταστροφή/αλλοίωση καίριων δομικών αρθρωμάτων του Λ/Σ. Μονόδρομο τότε για το σύστημα αποτελεί η επανεγκατάστασή του ή η επαναφορά μιας αμόλυντης εκδοχής, εφόσον κάτι τέτοιο υποστηρίζεται.

[582] Κύρια, βιβλιογραφική αναφορά: [BUTLER_HOGLUND-ROOTKITS].

εκμεταλλεύονται τις ελέω rootkit δυνατότητες και ευκαιρίες.[583] Διενεργείται, λοιπόν, σήμερα από την πλευρά των οργάνων και λειτουργών της ασφάλειας πληροφοριών με εσπευσμένο και ραγδαίο τέμπο *επισταμένη αναζήτηση εκείνων των προστατευτικών μηχανισμών, που θα απαντούν με υψηλές επιδόσεις στις προκλήσεις που έχει εισάγει η εφικτή διαμέσω rootkit υπόσκαψη των λειτουργικών θεμελίων, υποβάθμιση της αξιοπιστίας και διατάραξη της ομαλότητας των ΠΣ*.

5.1.3 «Παράθυρα» εκμετάλλευσης της μνήμης τυχαίας προσπέλασης

Σε μια πρόσφατη δημοσίευσή της,[584] η ερευνήτρια Joanna Rutkowska, φώτισε τα κακώς κείμενα στη διαχείριση της μνήμης από τα σύγχρονα υπολογιστικά συστήματα, φανερώνοντας την σχετική ισχύ ήδη γνωστών, αλλά και εντελώς νέων, δυνατών απειλών που εκπορεύονται από την ύπαρξη της εν λόγω αδυναμίας.

Ως γνωστόν, η μνήμη τυχαίας προσπέλασης (RAM) και γενικότερα κάθε μη παραμένουσα (persistent) όπως στα μέσα αποθήκευσης, αλλά μεταβαλλόμενη (volatile) μνήμη όπως είναι η φυσική μνήμη ενός υπολογιστή, αποτελεί ένα πρώτης τάξεως πεδίο εμφωλιασμού και εκδήλωσης πάσης φύσεως κακόβουλου λογισμικού.[585] Η *ανάγκη για μια ασφαλή και έγκυρη ανάκτηση (aquisition) περιεχομένων της μνήμης* αυτού του τύπου είναι ουσιώδους σημασίας, τόσο για την ανίχνευση μιας εισβολής/παραβίασης, όσο και για την ευρύτερη ανάλυση μιας εντοπισμένης κακοτοπιάς/δυσλειτουργίας κακόβουλης ή μη προέλευσης. Η διαρκής παρουσία και δράση μη μόνιμων/παραμενουσών απειλών -που δεν μπορούν να διαγνωστούν με ενδοσκόπηση στα μέσα αποθήκευσης, γιατί πολύ απλά δεν εδρεύουν εκεί- κάνει την ανάγκη αυτή περισσότερο επιτακτική. Στην προσπάθεια αυτή για ανάγνωση από τις συσκευές μη μόνιμης μνήμης αρωγοί στέκονται τόσο το λογισμικό, όσο και ορισμένο εξεζητημένο υλικό:

- <u>Λύσεις με χρήση λογισμικού</u>:

  Το Λ/Σ και πρόσθετα, κατάλληλα προγράμματα (ακόμα και στο επίπεδο ενός hypervisor[586]) παρέχουν τις απαραίτητες μεθόδους για μια όχι και τόσο αξιόπιστη απόκτηση των περιεχομένων μιας volatile μνήμης. Κακόβουλο λογισμικό που «τρέχει» με τα ίδια δικαιώματα όπως το λογισμικό εμφάνισης της μνήμης μπορεί με εύκολο τρόπο

[583] Κύρια, βιβλιογραφική αναφορά: [OVERTON-RRIP].

[584] Κύρια, βιβλιογραφική αναφορά: [RUTKOWSKA-BTCDHBRA].

[585] Το Κεφάλαιο 3 «βρίθει» από περιγραφές τέτοιων μεθόδων προσβολής (στη μορφή κυρίως TSR επιθέσεων).

[586] Περισσότερα για τους υπερεπόπτες στο αντίστοιχο εδάφιο 5.2.1.

να επηρεάσει (δυσχεραίνοντας ή/και τροποποιώντας) τη διαδικασία ανάγνωσης. Επίσης, στην περίπτωση αυτή η παρατήρηση της μνήμης προϋποθέτει και απαιτεί απευθείας επεξεργαστική αλληλεπίδραση με την έννοια ότι το λογισμικό (Λ/Σ και εξειδικευμένα εργαλεία λογισμικού) εμφάνισης και ανάλυσής της αναγκαστικά εκτελείται εντός της μονάδας επεξεργασίας και διαμέσω της μνήμης-στόχου ή εγγράφοντας κάποια έστω και ελάχιστα δεδομένα σε αυτήν. Μια τέτοιου είδους διαταραχή του υπό εξέταση συστήματος μνήμης μπορεί πολλές φορές και ειδικά υπό την παρουσία κακόβουλων προγραμμάτων να εκθέσει συνολικά σε αστάθεια ή άλλους κινδύνους το περιβάλλον επεξεργασίας «τινάζοντας στον αέρα» το όλο εγχείρημα και σίγουρα δεν αποτελεί την πιο ενδεδειγμένη προσέγγιση. Τέλος, η παρεχόμενη ανάγνωση (non-DMA) σπάνια ξεπερνά στην πράξη τα όρια της εικονικής μνήμης, για της οποίας το περιεχόμενο εύκολα μπορεί κανείς να παραπλανηθεί από πρόθυμους και καλά προετοιμασμένους, επιβλαβείς μηχανισμούς.[587]

- Λύσεις με τη βοήθεια υλικού:

Εξειδικευμένο υλικό με τη μορφή εσωτερικών π.χ. PCI ή εξωτερικών π.χ. Firewire, PCMCIA συσκευών κάνοντας χρήση των διευκολύνσεων της DMA τεχνολογίας, που εξαλείφει την αναγκαιότητα χρήσης της μονάδας επεξεργασίας, καθώς και των πρόσθετων προγραμματιστικών εφαρμογών, αποτυπώνει μια πιο αξιόπιστη εικόνα της μη μόνιμης μνήμης, όπως αυτή ιδανικά «φαίνεται» και στο σύστημα επεξεργασίας.[588] Η προσφερόμενη πληρότητα της απεικόνισης είναι αξιοθαύμαστη περιλαμβάνοντας το σύνολο της φυσικής μνήμης με μοναδική υπαρκτή παραφωνία/εξαίρεση τις αδυναμίες εμφάνισης στις σελίδες που βρίσκονται εντός του swap[589] χώρου και εκτός φυσικής, μη μόνιμης μνήμης (paged-out memory).

Το υλικό «μιλά» απευθείας με τον ελεγκτή της μη μόνιμης μνήμης και έτσι δεν επεμβαίνει με «επιθετικό» τρόπο στην υπόλοιπη ροή εργασίας του συνολικού συστήματος. Στην ιδεατή περίπτωση, το μόνο μειονέκτημα μοιάζει να είναι η μικρή πιθανότητα καθυστέρησης ή δυσλειτουργίας (όπως ξαφνικά κολλήματα και προβλήματα race conditions) του όλου υπολογιστικού συστήματος κατά τις φάσεις ανάγνωσης της

[587] Implementation Specific Attacks (ISA), δηλαδή επιθέσεις ταιριαστές με την εκάστοτε υλοποίηση του λογισμικού-θύματος, αρκεί το δείνα κακόβουλο πρόγραμμα να διαθέτει προνόμια χρήσης/πρόσβασης/εκτέλεσης ίδια ή μεγαλύτερα με αυτά του θύματος.

[588] Κύρια, βιβλιογραφική αναφορά: [MARTIN-FWMDWXPCFA].

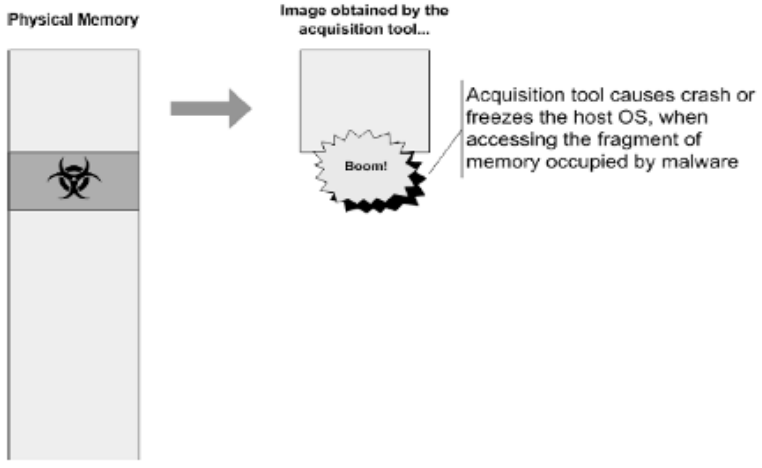
[589] Το αλλιώς γνωστό ως pagefile (=χώρος σελιδοποιημένης μνήμης στο δίσκο).

μνήμης-στόχου από την ειδική συσκευή, όταν δεν προβλέπονται από το υλισμικό ανάγνωσης οι σχετικές, προγραμματιστικές προφυλάξεις.[590]

Δυστυχώς για τους εγγυητές της ασφάλειας των ΠΣ τα πράγματα δεν είναι τελικά και τόσο ιδανικά, όσο υπόσχονται οι H/W λύσεις. Όπως εύστοχα και εύγλωττα παρουσιάζει η Joanna, *τα μέχρι τώρα στεγανά των μεθόδων ανάκτησης μνήμης μέσω συστημάτων υλικού απειλούνται με ξεκάθαρο τρόπο από το λιγότερο 3 αναγνωρισμένους τύπους*[591] *προσεχτικά σχεδιασμένων επιθέσεων με κακόβουλες εφαρμογές*, που οφείλονται σε ασθένειες του τρέχοντος σχεδιασμού σε υλικό και λογισμικό των υπολογιστικών συστημάτων και των συσκευών απεικόνισης και που τυγχάνει να υποστηρίζονται αριστουργηματικά από τις προαναφερόμενες μεθόδους της τεχνολογίας λογισμικού φαντασμάτων:

1. **Επίθεση τύπου άρνησης εξυπηρέτησης (DoS attack)**

   Σε αυτή την κατάσταση ο επιτιθέμενος μπορεί να έχει παραμετροποιήσει το πρόγραμμά του με τέτοιο τρόπο, ώστε να *παρακολουθεί τις λειτουργίες ανάγνωσης στη μνήμη και όταν ανιχνεύει απόπειρες DMA «διαβάσματός» της εξ επί τούτου να παγώνει το όλο σύστημα ή να το οδηγεί σε αστοχία*. Ένας ανυποψίαστος και απρόσεχτος ερευνητής μπορεί να οδηγήσει τελικά κρίσιμα συστήματα σε διακοπή ή βλάβη επισύροντας για τον ίδιο μέχρι και επικίνδυνες νομικές κυρώσεις ακόμα και αν είχε τις πιο αδιαμφισβήτητα καλές προθέσεις.



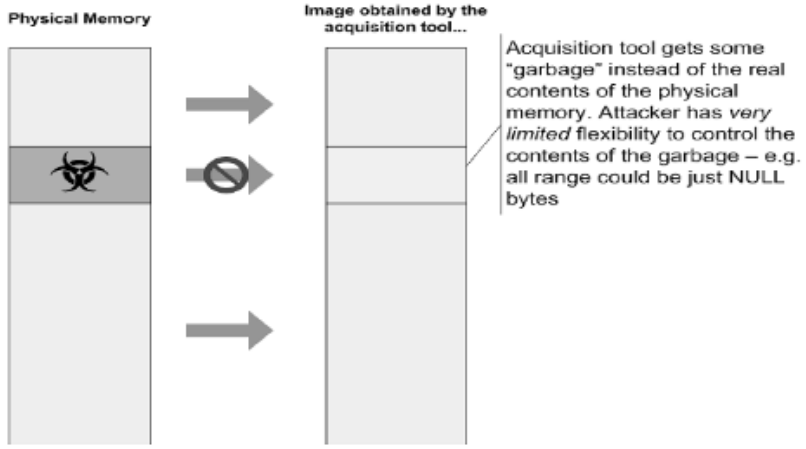
Σχήμα 35: Επίθεση τύπου DoS, κατά την ανάγνωση φυσικής μνήμης

[590] Αφορά κυρίως κατεξοχήν, πολυνηματικά, επεξεργαστικά περιβάλλοντα.

[591] Κύρια, βιβλιογραφική αναφορά: [RUTKOWSKA-BTCDHBRA].

2. Επίθεση συγκάλυψης (covering attack)

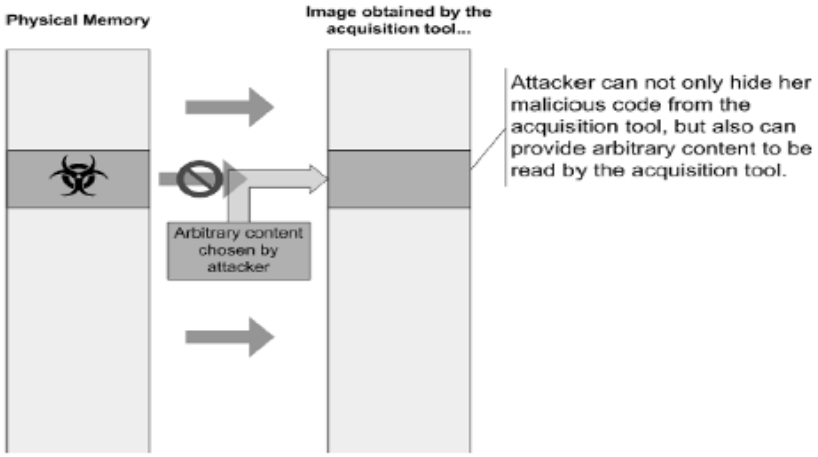
Το πρόγραμμα του επιτιθέμενου σε αυτή την περίπτωση παγιδεύει με αντίστοιχο τρόπο τις εξειδικευμένες κλήσεις των συστημάτων ανάλυσης *επιστρέφοντας* σε αυτές *άχρηστα δεδομένα αντί των πραγματικών που η επεξεργαστική μονάδα «βλέπει»*, όταν αναγκαστεί αργά ή γρήγορα να τα εκτελέσει. *Η ευελιξία του επιτιθέμενου στις επιστρεφόμενες τιμές εμφανίζεται κάπως περιορισμένη* (συνήθως οι τιμές είναι απλά μηδενικά ή στην καλύτερη περίπτωση για τον κακόβουλο δράστη τυχαίες), πράγμα που μπορεί να «προδώσει» την υπονόμευση, αλλά σε καμιά περίπτωση δεν επιτρέπεται μια βαθύτερη και επισταμένη ανάλυση και εξακρίβωση των εκάστοτε ιδιαίτερων χαρακτηριστικών της μόλυνσης.



Σχήμα 36: Επίθεση συγκάλυψης, κατά την ανάγνωση φυσικής μνήμης

3. Επίθεση ολικής αντικατάστασης (full replacing attack)

Στις επιθέσεις αυτής της κατηγορίας οι δυνατότητες του επιτιθέμενου -που ελαφρώς διαφάνηκαν στις επιθέσεις συγκάλυψης- για τροποποίηση των διαβαζόμενων τιμών από τα συστήματα απεικόνισης της μνήμης επεκτείνονται με παρόμοια λογική αλλά με πιο στοχευμένο και κατάλληλο σχεδιασμό, ώστε εν τέλει να ενδυναμώνονται σε σχεδόν απεριόριστο βαθμό. Ουσιαστικά, *το κακόβουλο πρόγραμμα και ο χρήστης του μπορούν πλέον να επηρεάζουν κατά βούληση τα περιεχόμενα των επιστρεφόμενων δεδομένων*, απομακρύνοντας ιδιοφυώς τις υποψίες μόλυνσης και παρέχοντας ενδεχομένως παραπλανητικά στοιχεία, με ό,τι αρνητικό αυτό συνεπάγεται για τυχόν λανθασμένα συμπεράσματα ενός ερευνητή που θα αξιολογήσει τα στοιχεία αυτά. Οι νομικές ευθύνες κάνουν και πάλι αισθητή την παρουσία τους σε περίπτωση εσφαλμένης εκτίμησης του κινδύνου από πλευράς των επαγγελματιών υπέρμαχων της ασφάλειας.



Σχήμα 37: Επίθεση ολικής αντικατάστασης κατά την ανάγνωση φυσικής μνήμης

Αξίζει να σημειωθεί και να τονιστεί πως η παρατηρούμενη σήμερα έξαρση των επιβλαβών προγραμμάτων που εκμεταλλεύονται τα «οφέλη» της υπονόμευσης των Λ/Σ που συζητήθηκαν προηγούμενα, παράγει ένα ιδιαίτερα πρόσφορο έδαφος για την εκδήλωση των περιγραφόμενων από την Rutkowska επιθέσεων. Εν πολλοίς, μια σε βάθος υπονόμευση ενός Λ/Σ με rootkit τεχνικές αποτελεί έναν αξιόλογο, αν όχι και τον πιο βασικό, προωθητήριο μοχλό, για την εκτέλεση των απαραίτητων στις επιθέσεις αυτές προαναφερόμενων ενεργειών διαρκούς, δυναμικής, ει δυνατόν όσο γίνεται πιο κρυφής, παρακολούθησης της μη μόνιμης μνήμης και αντίστοιχης επίμονης και «υπόγειας»/απαρατήρητης σύλληψης και εξαπάτησης των κλήσεων εμφάνισής/ανάλυσής της. Επίσης, η μέχρι στιγμής εμπορική απουσία συσκευών μνήμης με IOMMU[592] δυνατότητες διευκολύνει το έργο μιας πιο άμεσης αλλοίωσης των περιεχομένων της κύριας μνήμης (με την χρησιμοποίηση τυχόν διαθέσιμων ανέσεων και παροχών τύπου DMA προσβάσεων, αυτή τη φορά όμως από την πλευρά των κακόβουλων προγραμμάτων[593]) και συμβάλλει ενεργά στην όξυνση του διαπιστωμένου προβλήματος.

Το μόνο παρήγορο στοιχείο και στις 3 παραπάνω περιπτώσεις εγγενούς ευπάθειας στα συστήματα απεικόνισης της μνήμης είναι ότι οι όποιες προκύπτουσες παραβιάσεις θα απαιτήσουν περίπλοκο προγραμματισμό και έναν αν μη τι άλλο υψηλό δείκτη τεχνογνωσίας.

Η εργασία της Rutkowska καταλήγει με την ανησυχητική και αξιοσημείωτη παρατήρηση πως *η ανάγνωση της μεταβαλλόμενης μνήμης από τα υπολογιστικά μας συστήματα εξακολουθεί μέχρι και σήμερα να παραμένει σε μεγάλο βαθμό αναξιόπιστη και ευάλωτη σε μη*

[592] Όπως είδαμε σχετικά στο εδάφιο 4.3.3.

[593] Σε μια τέτοια κατάσταση ένα HW εργαλείο ανάλυσης και απευθείας ανάγνωσης της μνήμης θα μπορούσε να χρησιμοποιηθεί εις βάρος του συστήματος, αλλά και των αναλυτών αυτού, αν χειραγωγηθεί κατάλληλα από το κακόβουλο όπλο, παράγοντας επιπλέον και πιο άμεσες δυνατότητες -χάρη στις διευκολύνσεις του DMA τρόπου πρόσβασης- παράτυπης αλλαγής των περιεχομένων της κύριας (ή/και άλλης non-volatile) μνήμης.

ευκαταφρόνητων επιπτώσεων επιθέσεις, ακόμα και όταν κανείς καταφεύγει σε συστηματική χρήση ακριβών τεχνολογιών υλικού· η ερευνήτρια ολοκληρώνει τη διαπίστωσή της προτρέποντας για μια ριζική αναθεώρηση του σχεδιασμού (σε λογισμικό και υλικό) των υπολογιστικών συστημάτων, ώστε αυτά με κάποιο τρόπο να μετατραπούν σε περισσότερο επιβεβαιώσιμα[594] και συνεπώς πιο αξιόπιστα και ασφαλή. Η απευθείας ανάγνωση της μνήμης για τον εντοπισμό υπονομεύσεων από κακόβουλα όπλα δεν πρέπει πάντως πια, τουλάχιστον επί του παρόντος, να θεωρείται «αλεξίσφαιρη» λύση, πράγμα που εκ των πραγμάτων συνιστά ύπαρξη πληθώρας ευκαιριών για τους συγγραφείς και χρήστες τέτοιων όπλων και πρόβλημα προς άμεση δράση παράκαμψης και υπερκερασμού, αν όχι επίλυσης, για τους «εργάτες» της ασφάλειας πληροφοριών.

5.2 Αντι-ιομορφική τεχνολογία – Ασφάλεια πληροφοριών

Στον αντίποδα του προηγούμενου τμήματος του παρόντος κεφαλαίου θα εξετάσουμε τις αντίστοιχες, καινοτομικές προσεγγίσεις στα πλαίσια της υπεράσπισης των ΠΣ, που γενικά παρέχουν υποσχέσεις για μεγαλύτερη και πιο συγκροτημένη διασφάλιση των κρίσιμων δεδομένων και επικοινωνιών, πιθανώς αντισταθμίζοντας σε πολλές περιπτώσεις και τα όσα επικίνδυνα προοικονομούν οι νέες ευκαιρίες κακόβουλης εκμετάλλευσης και υπονόμευσης που καταμαρτυρήθηκαν προηγουμένως.

5.2.1 Δυναμική της εικονικοποίησης

Η εικονικοποίηση, ως *"γενικευμένη τεχνική για την απόκρυψη των φυσικών χαρακτηριστικών των πόρων ενός ΠΣ από τον τρόπο με τον οποίο άλλα συστήματα, εφαρμογές ή τελικοί χρήστες αλληλεπιδρούν με αυτούς τους πόρους"*, έχει βρει εκτός των άλλων πολλές εφαρμογές στην υπηρεσία της προστασίας των υπολογιστικών συστημάτων από κακόβουλο λογισμικό.[595]

Τρεις κυρίως προσεγγίσεις για την ασφάλεια των ΠΣ, που βασίζονται στον μηχανισμό της εικονικοποίησης, εμφανίζουν την κατάλληλη δυναμική, ώστε να περιμένει κανείς πως στο εγγύς μέλλον θα συνεχίσουν να απασχολούν με συνεχή ρυθμό ή θα αποκτήσουν ιδιαίτερα

[594] Η έννοια και η τεχνοτροπία της επιβεβαίωσης των συστημάτων γίνεται αντικείμενο μελέτης σε ξεχωριστό εδάφιο (5.2.2).

[595] Για παράδειγμα, πλήθος των -εξαιρετικής ικανότητας στη «σύλληψη» σκουληκιών- δικτυακών παγίδων τύπου honeypots υλοποιούνται με τη βοήθεια λογισμικού και εξειδικευμένων συστημάτων εικονικοποίησης εξαιτίας των προτιμητέων, σε σχέση με ένα πραγματικό σύστημα, ιδιοτήτων, που προκύπτουν από την περιορισμένη, μη άμεση αλληλεπίδραση ενός εικονικοποιημένου πλαισίου λειτουργίας με τους φυσικούς πόρους.

σημαίνουσα βαρύτητα, πυροδοτώντας και επηρεάζοντας τις όποιες εξελίξεις στη μάχη για την αντιμετώπιση ιών και σκουληκιών:

1. Εξομοίωση (Emulation)

Τα ιδιαίτερα χαρακτηριστικά της εξομοίωσης ως εγνωσμένης μεθόδου προστασίας από τους κινδύνους του κακόβουλου λογισμικού επισημάνθηκαν στο αμέσως προηγούμενο κεφάλαιο, όπου περιγράφηκε η *θετική δράση τους στον εντοπισμό επιβλαβούς κώδικα (και ιδιαίτερα των πολυμορφικού τύπου μεταλλάξεων του)*.

Τα συστήματα εξομοίωσης εισάγουν ένα καλά ελεγχόμενο και αποτελεσματικό πλαίσιο διάγνωσης μιας πληροφοριακής απειλής τύπου ιού ή σκουληκιού, που αναμένεται να βρίσκει διαρκώς αυξανόμενη εφαρμογή:

- Ως αυτόνομο, αυτοματοποιημένο μέσο θωράκισης ή μέρος ευρύτερου αυτόματου μηχανισμού άμυνας των ΠΣ, με τον τρόπο που περιγράφηκε στο Κεφάλαιο 4.
- Ως κατεξοχήν τρόπος για λιγότερο επικίνδυνες εργασίες ανίχνευσης νέων υποστάσεων και μορφών κακόβουλου κώδικα από μέρους αναλυτών και ερευνητών στο χώρο της ασφάλειας δεδομένων και συστημάτων.

2. Εγκιβωτισμός (Sandboxing)

Ο *εγκιβωτισμός* είναι *"ένας μηχανισμός ασφάλειας για ακίνδυνη εκτέλεση προγραμμάτων σε απομονωμένο, επεξεργαστικό περιβάλλον"*.[596] Χρησιμοποιείται συχνά κατά την εκτέλεση μη δοκιμασμένου κώδικα ή προγραμμάτων από μη έμπιστες, τρίτες οντότητες, προμηθευτές και χρήστες.

Κάθε τυπικό sandbox παρέχει ένα *στενά-ελεγχόμενο σύνολο πόρων* (όπως scratch space σε δίσκο και μνήμη) *και δικαιωμάτων* για τα φιλοξενούμενα προγράμματα, ώστε αυτά να «τρέξουν» μέσα σε αυτό το πλαίσιο. Η πρόσβαση στο δίκτυο, η δυνατότητα επιθεώρησης του συστήματος φιλοξενίας ή/και η ανάγνωση από τις συσκευές εισόδου συνήθως απαγορεύονται ρητώς ή περιορίζονται σε μεγάλο βαθμό.[597]

Μερικά παραδείγματα γνωστών sandboxes είναι:

---

[596] Πηγή: Διαδίκτυο, ιστοχώρος του «γκουρού» της Πληροφορικής Amit Singh, http://www.kernelthread.com/publications/security/sandboxing.html.

[597] Πηγή: Διαδίκτυο, ιστοχώρος της online εγκυκλοπαίδειας WikiPedia, http://en.wikipedia.org/wiki/Sandbox_(computer_security).

* Τα Applets είναι ανεξάρτητα προγράμματα που τρέχουν σε μια εικονική μηχανή ή έναν scripting γλωσσικό διερμηνευτή (όπως η JavaVM), που πραγματοποιεί τον εγκιβωτισμό. Αυτή η ρύθμιση είναι δημοφιλής στους περιηγητές Ιστού, οι οποίοι χρησιμοποιούν αυτόν τον μηχανισμό για να εκτελέσουν ακίνδυνα τα applets, που ενσωματώνονται σε διάφορες μη έμπιστες ιστοσελίδες. Τα applets της Java ειδικότερα καταλαμβάνουν (στο ελάχιστο) κάποιο ορθογώνιο τμήμα του συνολικού χώρου της οθόνης, με το οποίο μπορεί να αλληλεπιδρούν με το χρήστη και κάποιο μόνιμο χώρο αποθήκευσης (με τη σύμφωνη άδεια του χρήστη).

* Το σύστημα Jails είναι ένα ειδικό είδος ορίου στους πόρους, που επιβάλλεται στα προγράμματα (και τους χρήστες) και «ξεπήδησε» από το λειτουργικό σύστημα FreeBSD.

* Οι εικονικές μηχανές (virtual machines) μιμούνται έναν πλήρη οικοδεσπότη υπολογιστή, στον οποίο μπορεί να τρέξει ένα ολόκληρο λειτουργικό σύστημα. Το Λ/Σ που φιλοξενείται δεν «τρέχει» ενδογενώς στον οικοδεσπότη και μπορεί να έχει επιπτώσεις στο σύστημα φιλοξενίας, μόνο μέσω του εκάστοτε μεσάζοντα εικονικοποιητή (virtualizer) και την επίδραση αυτού επάνω στους κοινούς πόρους, όπως π.χ. τους τοπικούς σκληρούς δίσκους.

* Λύσεις application streaming εγκιβωτίζουν εφαρμογές στα μηχανήματα πελάτη.

* Τα συστήματα ικανότητας (capability systems) μπορούν να θεωρηθούν ως sandboxing μηχανισμός, στον οποίο τα προγράμματα έχουν τη δυνατότητα να κάνουν συγκεκριμένα πράγματα με βάση τις ιδιαίτερες «ικανότητες» τους.

* Οι XAML εφαρμογές των φυλλομετρητών (browsers) είναι προγράμματα που μπορούν να τρέξουν μέσα από προγράμματα περιήγησης, όπως ο Microsoft Internet Explorer ή ο Mozilla FireFox, και περιορίζονται σε ελάχιστη ή καμία πρόσβαση σε κατεξοχήν συστημικά στοιχεία.

Οι εγγενείς περιορισμοί που εισάγει ο εγκιβωτισμός στα φιλοξενούμενα προγράμματα είναι:[598]

- Αφενός, αποτρέπεται σε πολύ μεγάλο βαθμό η δυνατότητα εκτέλεσης κακόβουλου, ιομορφικού κώδικα ή κώδικα σκουληκιού.
- Διαφορετικά, στην περίπτωση επιτυχημένης εκτέλεσης τυχόντος κακόβουλου λογισμικού διατηρούν στο ελάχιστο τις αρνητικές επιδράσεις μιας τέτοιας επιβλαβούς δραστηριότητας μέσω των ιδανικά απαράβατων ορίων-φραγμάτων, που θέτουν εκ των προτέρων στους συστημικούς πόρους.

[598] Κύρια, βιβλιογραφική αναφορά: [TANENBAUM-MOS9].

3. Υπερεποπτεία (Hypervisory)

Ένας *υπερεπόπτης ή hypervisor* (επίσης: εικονικό όργανο ελέγχου μηχανών ή Virtual Machine Monitor, VMM) είναι *"μια πλατφόρμα εικονικοποίησης, που επιτρέπει σε πολλαπλά λειτουργικά συστήματα να τρέχουν συγχρόνως σε κάποιον οικοδεσπότη υπολογιστή".*[599]

Οι υπερεπόπτες αυτήν την περίοδο είναι ταξινομημένοι σε δύο κυρίως τύπους:

*** Ένας τύπου I (ή ενδογενής) hypervisor** είναι λογισμικό που τρέχει άμεσα σε δεδομένη πλατφόρμα υλικού (ως πρόγραμμα ελέγχου λειτουργικών συστημάτων). Ένα φιλοξενούμενο λειτουργικό σύστημα μπορεί έτσι να τρέχει στο δεύτερο επίπεδο επάνω από το υλικό. Ο κλασικότερος τύπου 1 υπερεπόπτης ήταν ο CP/CMS, που αναπτύχθηκε από την IBM στη δεκαετία του '60, πρόγονος του τρέχοντος z/VM της ίδιας εταιρείας. Τα πιο πρόσφατα παραδείγματα είναι το σύστημα Xen, ο ESX Server της VMware, τα L4 microkernels, το TRANGO, ο LPAR hypervisor της IBM (PR/SM), η λύση της Microsoft Hype-V (beta έκδοση, κωδική ονομασία Viridian) και το Logical Domains Hypervisor της Sun Microsystems (2005). Μια παραλλαγή του τύπου I συμβαίνει όταν ενσωματώνεται το hypervisor στο firmware υλισμικό μιας πλατφόρμας, όπως γίνεται στην περίπτωση του hypervisor Virtage της Hitachi. Το σύστημα KVM, τέλος, που μετατρέπει έναν πλήρη πυρήνα Linux σε hypervisor, είναι επίσης τύπος I.

*** Ένας hypervisor τύπου II (ή φιλοξενούμενος)** είναι λογισμικό που τρέχει μέσα σε ένα υπάρχον περιβάλλον Λ/Σ. Ένα φιλοξενούμενο, λειτουργικό σύστημα μπορεί έτσι να τρέχει στο τρίτο επίπεδο επάνω από το υλικό. Τα παραδείγματα περιλαμβάνουν προϊόντα της VMWare (Server, Workstation, Fusion), Microsoft (Virtual PC, Virtual Server), την ανοιχτού κώδικα λύση QEMU, το VirtualBox της InnoTek, καθώς επίσης και τις προτάσεις της SWsoft (Parallels Workstation, Parallels Desktop).

Οι τύπου II υπερεπόπτες αποτελούν εγνωσμένες λύσεις εικονικοποίησης, που προτιμώνται από οργανισμούς, διαχειριστές συστημάτων και χρήστες για την υποστήριξη πληθώρας δραστηριοτήτων και μπορούν μεταξύ άλλων να χρησιμοποιηθούν και ως λύσεις εξομοίωσης ή εγκιβωτισμού, όπως περιγράφηκαν ευθύς προηγουμένως, για την ενίσχυση της ασφάλειας των συστημάτων. Αντιθέτως, οι τύπου I hypervisors έχουν αρχίσει τώρα τελευταία να προσελκύουν το μεγαλύτερο ενδιαφέρον των ερευνητών

[599] Πηγή: Διαδίκτυο, ιστοχώρος της online εγκυκλοπαίδειας WikiPedia, http://en.wikipedia.org/wiki/Hypervisor.

ασφάλειας ΠΣ, μιας και παρέχουν ένα επιπλέον στρώμα ελέγχου και προστασίας από κακόβουλες ενέργειες και προγράμματα. Ιδιαίτερη προσοχή πρέπει να δοθεί στον σχεδιασμό για την κατάλληλη λειτουργία των hypervisory μηχανισμών, ώστε αυτοί *να μην υπόκεινται σε εύκολη υπονόμευση από κακόβουλες εφαρμογές ή να μην εξυπηρετούν κανένα σκοπό της διάδοσης επιβλαβούς λογισμικού*, αλλά αντίθετα να αποκλείουν την πρόσβαση σε ευαίσθητες επεξεργαστικές δυνατότητες στα μη έμπιστα ή μη εξουσιοδοτημένα προγράμματα ή/και εναλλακτικά να συνδράμουν πιο ενεργητικά στην αντιμετώπισή τους, με τρόπο διάφανο ή αδιαφανή στον τελικό χρήστη. Παραδείγματος χάριν, πέρα από την ύπαρξη παθητικών πολιτικών για την πρόσβαση στο κατώτερο επίπεδο σε επίπεδο υπερεπόπτη, μπορεί κανείς να αναμένει την παρουσία και δράση και κάποιου ενεργητικού μηχανισμού διάγνωσης, αναγνώρισης και αποτροπής κακόβουλων ενεργειών (λ.χ. επιβλαβείς εντολές CPU), εν είδη λογισμικού προστασίας που θα «τρέχει» σε αυτό το επίπεδο, ελέγχοντας έτσι κάθε υπερκείμενο Λ/Σ με τρόπο μη αντιληπτό και αδιάφανο σε οποιαδήποτε εφαρμογή αυτού.[600] Όπως είδαμε, όμως, χαρακτηριστικά στο εδάφιο της δυναμικής της υπονόμευσης των Λ/Σ, η δυνατότητα για σε βάθος μόλυνση ενός Λ/Σ και του ευρύτερου υλισμικού μιας πλατφόρμας και η διαρκώς αυξανόμενη διάδοση της χρήσης των rootkit τεχνικών ενέχουν τον κίνδυνο εμφάνισης κακόβουλων απειλών, που θα μπορούν να εκμεταλλεύονται προς όφελός τους το πρόσθετο hypervisory στρώμα, για να αποκτήσουν ακόμα μεγαλύτερη απόκρυψη από τους χρήστες και τα συστήματα ασφάλειας.[601] Επίσης, η προσωρινή, μη διαθεσιμότητα στο εμπόριο συσκευών αξιόπιστης διαχείρισης της κύριας μνήμης από περιφερειακές συσκευές (βλέπε IOMMU[602]) μπορεί να λειτουργήσει εις αρκούντως σημαντικό βάρος των πρώιμων συστημάτων υπερεποπτείας, που βασίζονται θεμελιωδώς στην παροχή των απαραίτητων χαμηλού επιπέδου λειτουργιών προσπέλασης της κύριας μνήμης και του συστήματος επεξεργασίας στα ανώτερα, υποστηριζόμενα, εικονικά ή παρέχοντα φιλοξενία Λ/Σ και τους οδηγούς συσκευών τους.

Πρόσφατες CPUs από την Intel και την AMD προσφέρουν x86 εντολές εικονικοποίησης, ώστε κάποιος μηχανισμός υπερεποπτείας να ελέγχει την πρόσβαση σε επίπεδο Ring 0[603]. Αν και αμοιβαίως ασύμβατοι, τόσο οι "Vanderpool" (ή VT) της Intel όσο και οι "Pacifica" (ή AMD-V) της AMD δημιουργούν ένα νέο επίπεδο πρόσβασης "Ring -1", ώστε κάθε φιλοξενούμενο Λ/Σ να μπορεί να εκτελεί Ring 0 λειτουργίες ενδογενώς, χωρίς

---

[600] Κύρια, βιβλιογραφική αναφορά: [GARFINKEL_ROSENBLUM-VMIBAID].

[601] Κύρια, βιβλιογραφική αναφορά: [DAVIES-HM].

[602] Το θέμα θίχτηκε στο εδάφιο 4.3.3 του 4ου μέρους της εργασίας.

[603] Τα rings είναι τα διαφορετικά επίπεδα δικλείδων ασφάλειας και επεξεργαστικών προνομίων, που επιτρέπουν οι κατασκευαστές των διαφόρων CPUs.

να επηρεάζει άλλα φιλοξενούμενα ή το παρέχον φιλοξενία Λ/Σ.[604] Αυτό είναι ενδεικτικό πως και *η βιομηχανία του υλικού των προσωπικών Η/Υ κινείται γοργά στην κατεύθυνση, που υποδεικνύουν οι προσδοκίες από τους μηχανισμούς hypervisor*. Το ίδιο όμως κάνει και η κοινότητα των συγγραφέων κακόβουλου λογισμικού, όπως τονίζουν εμφατικά οι περιπτώσεις των SubVirt και Blue Pill, που συζητήθηκαν προηγούμενα.

Σίγουρα, στο μέλλον, οι hypervisory τεχνολογίες θα μας απασχολήσουν πολύ περισσότερο, καθώς αναμένεται να τύχουν ακόμη μεγαλύτερης αποδοχής και εφαρμογής στον τομέα της ασφάλειας και προστασίας υπολογιστικών συστημάτων, με ό,τι αντιδράσεις αυτό συνεπάγεται και από τους θιασώτες του κακόβουλου λογισμικού.

5.2.2 Προοπτική των επιβεβαιώσιμων Λ/Σ (verifiable OS)

Η διαδικασία επιβεβαιώσεων στα Λ/Σ φαντάζει ως η *νέα, μεγάλη πρόκληση για την αντιμετώπιση κατά κύριο λόγο των προβλημάτων υπονόμευσής* τους, που κομίζουν τα προγράμματα «φαντασμάτων». Η δυνατότητα εντοπισμού κακόβουλου κώδικα μέσω απλής ανάγνωσης της μη μόνιμης μνήμης, όπως είδαμε, δεν επαρκεί, καθώς έχει συναντήσει εδώ και κάποιο καιρό κριτική που δεν μπορεί να παραγνωριστεί.[605] Από την άλλη, οι διάφορες εφαρμογές διάγνωσης (σαρωτές, παρεμποδιστές, εξομοιωτές) έχουν διαπιστωθεί επανειλημμένα ως ευάλωτες σε επιβλαβές λογισμικό που τρέχει με τα ίδια δικαιώματα (ISA επιθέσεις σε διεργασίες του ιδίου επιπέδου εξουσιοδότησης) εντός του Λ/Σ.[606] Μια καινούρια και πρότυπη μεθοδολογία και δράση φαίνεται πως χρειάζεται, το δίχως άλλο, για να συμπληρώσει/συνδράμει στις υπάρχουσες εναλλακτικές.

Στα πλαίσια αυτά, μια ξεχωριστή πρόταση αναπτύχθηκε, το τελευταίο διάστημα, συνδυάζοντας σε μεγάλο ποσοστό και με χρήσιμο τρόπο ήδη γνωστές τεχνικές. Η επιβεβαίωση των Λ/Σ[607] γεννήθηκε πάνω στις παρακάτω, βασικές αρχές λειτουργίας:

1. Το υποκείμενο σύστημα επεξεργασίας (CPU) υποστηρίζει εκτενώς κατάλληλους μηχανισμούς και σημάνσεις μη εκτελέσιμου κώδικα, που συζητήθηκαν και στο Κεφάλαιο 4[608], σε επίπεδο σελίδας μνήμης.

---

[604] Πηγή: Διαδίκτυο, ιστοχώρος της online εγκυκλοπαίδειας WikiPedia, http://en.wikipedia.org/wiki/Ring_(computer_security).

[605] Στο εδάφιο 5.1.3 προσεγγίσαμε το ευαίσθητο αυτό θέμα.

[606] Μια ματιά στα Κεφάλαια 3, 4 αρκεί για να πείσει και τον πιο δύσπιστο.

[607] Κύρια, βιβλιογραφική αναφορά: [TUCH_KLEIN_HEISER-OSVN].

[608] Στο εδάφιο 4.3 περί αρχιτεκτονικής έμπιστου υλικού και πλατφόρμες ασφαλούς επεξεργασίας.

2. Το Λ/Σ συντηρεί έναν αισθητό και επαρκή διαχωρισμό των τμημάτων κώδικα και δεδομένων, σε επίπεδο σελίδας μνήμης.
3. Η επιβεβαίωση κώδικα πραγματοποιείται ιδανικά με ρητά διατυπωμένη, μαθηματική ακρίβεια (μέσω συγκεκριμένης φόρμουλας ή τύπου υπολογισμού) και λαμβάνει χώρα, σε επίπεδο σελίδας μνήμης και με τη βοήθεια υλικού και λογισμικού. Ειδικές συσκευές -στα πρότυπα του TPM- μπορούν να ελέγχουν την εγκυρότητα της κάθε εκτελούμενης διεργασίας (ή τμήματος αυτής) με βάση προτυπωμένες πληροφορίες ιδιοκτησίας[609], ενώ και οι ψηφιακές υπογραφές στο λογισμικό αναδεικνύονται σε μια πολύ βολική λύση -ακόμα και για μια καθαρά S/W προσέγγιση, στη λογική του PatchGuard της Microsoft- για τους σκοπούς αυτούς.
4. Δύο εναλλακτικές:
    a. Το Λ/Σ πρέπει να φροντίζει για μια αξιόπιστη ανάγνωση μνήμης μέσω ενός προγράμματος-μηχανισμού που θα φωλιάζει στα άδυτα του συστήματος ή εξόν αυτού (με δυνατότητες τουλάχιστον επιπέδου πυρήνα), δίνοντας πολύ μικρή πιθανότητα υπονόμευσης στα κακόβουλα παράσιτα. Τα στρώματα hypervisor παρουσιάζονται ως ιδανικοί υποψήφιοι για την υλοποίηση τέτοιων μηχανισμών, αρκεί να είναι αρκετά λεπτά και θωρακισμένα, ώστε να αποτρέπουν μια τύπου ISA παρείσφρυση και καθυπόταξη.[610]
    b. Η μνήμη «διαβάζεται» με τη βοήθεια ειδικής, εξωτερικής συσκευής (π.χ. FireWire ή PCI DMA), ενώ η σελιδοποίησή της στο δίσκο δεν επιτρέπεται και απενεργοποιείται.[611]

Για κάθε σελίδα στη μνήμη, η επιβεβαίωση πραγματοποιείται σε 2 στάδια:

-πρώτα από όλα ελέγχεται, αν η σελίδα έχει χαρακτηριστεί εκτελέσιμη ή όχι, και

-κατόπιν λαμβάνει χώρα ο έλεγχος εγκυρότητας του περιεχόμενου σε αυτήν κώδικα (το «ψηφιακό αποτύπωμά» του επιβεβαιώνεται ως αξιόπιστο και αποδεκτό, με κύριο γνώμονα την προέλευσή του και τη φερεγγυότητα αυτής[612]) με τη βοήθεια εξεζητημένων προγραμματιστικών βιβλιοθηκών ή/και επιτηδευμένων συσκευών υλικού.

---

[609] Το TPM τσιπ και οι ενδιαφέρουσες απόρροιες από τη χρήση του μας απασχόλησαν στο εδάφιο 4.3.2.

[610] Οι ISA επιθέσεις συζητήθηκαν σε προηγούμενη υποσημείωση.

[611] Προκειμένου να αποφευχθούν απλοϊκές, παραμένουσες μολύνσεις και να εξισορροπηθεί η προαναφερόμενη αδυναμία των συσκευών υλικού να «διαβάσουν» από τη swap memory.

[612] Έμπιστες, Τρίτες Οντότητες (TrustedThirdParty) καλούνται να εγγυηθούν για την αξιοπιστία του εκδότη του ζεύγους κώδικα-«αποτυπώματος».

Σε περίπτωση που σε κάποια εκτελέσιμη σελίδα ο έλεγχος εγκυρότητας αποτύχει ή δεν αποδώσει τα επιθυμητά επίπεδα εμπιστοσύνης, το υλικό&λογισμικό επιβεβαίωσης αποφαίνονται αρνητικά ως προς την εκτέλεση του υπό κρίση κώδικα (αποτροπή εκτέλεσης) και προειδοποιούν τους ιδιοκτήτες/χρήστες για ενδεχόμενη κακόβουλη δραστηριότητα (συναγερμός).

Όλα τα σύγχρονα, λειτουργικά συστήματα της εποχής μας *έχουν αρχίσει να αφομοιώνουν τρόπον τινά τις τάσεις που κατέδειξε η λογική της επιβεβαίωσης*, εγκολπώνοντας, άλλα σε περισσότερο, άλλα σε λιγότερο βαθμό, τα παραπάνω χαρακτηριστικά σχεδιασμού.[613] Το σύστημα NetBSD, προς το παρόν, μοιάζει να είναι πιο κοντά στο θεωρητικό αρχέτυπο προστασίας μέσω επιβεβαίωσης του Λ/Σ. Όπως και να 'χει πάντως, στο μέλλον, μάλλον θα συνεχίσουμε να απασχολούμαστε με αυτήν την πρωτότυπη και πολλά υποσχόμενη μέθοδο, με το βλέμμα της έρευνας και της παραγωγής να βρίσκεται τώρα στραμμένο στην άμεση *περαιτέρω βελτιστοποίηση και ενσωμάτωση των νεογνών μοντέλων και συστημάτων* επιβεβαίωσης.

5.2.3 Νέες τάσεις στην ταυτοποίηση των προνομιούχων οντοτήτων

Τα τελευταία -όχι πολλά- χρόνια έχουν αναπτυχθεί τα θεωρητικά πλαίσια και έχουν διατεθεί στην αγορά νέα, *καινοτομικά προϊόντα, στο χώρο της αυθεντικοποίησης και του γενικότερου σχήματος αυθεντικοποίηση-έλεγχος πρόσβασης-καταγραφή (ΑΑΑ)*, που φιλοδοξούν να συμπληρώσουν ή να υποκαταστήσουν με αρμονικό τρόπο τις ήδη υπάρχουσες μεθοδεύσεις. Ανάμεσα στα καινούρια αυτά μοντέλα ξεχωρίζουν με διαφορά οι 5 παρακάτω περιπτώσεις:

1. Συστήματα RFID[614]

Τα συστήματα αυτά αποτελούν το επιστέγασμα των προσπαθειών στο χώρο μιας *διάφανης, κυρίαρχης (pervasive & ubiquitous) και ολοκληρωμένης διαδικασίας μιας αξιόπιστης και ισχυρής αυθεντικοποίησης φυσικών προσώπων και αντικειμένων*, που γίνεται με ασύρματο τρόπο χάρη στις υψηλές ταχύτητες εκπομπής και λήψης δεδομένων στις ραδιοσυχνότητες. Οι ασύρματοι πομποδέκτες μπορούν να φέρουν ειδικά ψηφιακά πιστοποιητικά εντός πολύ μεγάλης κλίμακας ολοκλήρωσης τυπωμένων κυκλωμάτων (VLSI circuits), τα οποία και

[613] Κύρια, βιβλιογραφική αναφορά: [RUTKOWSKA-FSMTVOS].

[614] Κύρια, βιβλιογραφική αναφορά: [THORNTON-RFIDS].

ανιχνεύονται/επιβεβαιώνονται κατόπιν «μυστικής χειραψίας»[615] από συστήματα ανάγνωσης (RFreaders), που λειτουργούν στην ίδια συχνότητα.

Ήδη, συναντάμε γύρω μας *πολλαπλές εφαρμογές*[616] *του συγκεκριμένου τεχνουργήματος*· άνθρωποι και συσκευές που δε διαθέτουν τα κατάλληλα αναγνωριστικά θα αποκλείονται από τη μη εξουσιοδοτημένη είσοδό τους *σε ευαίσθητους, ελεγχόμενους χώρους*[617] ή την *πραγματοποίηση ιδιαίτερα κρίσιμων, πληροφοριακών ενεργειών*[618], ενώ τα διάφορα εμπορεύματα είναι πλέον εύκολο να παρακολουθούνται[619] σε όλες τις φάσεις από την παραγωγή μέχρι την κατανάλωση. Οι RFID τεχνοτροπίες έχουν στις μέρες μας εγείρει μια *θύελλα αντιδράσεων και καχυποψίας*[620] λόγω ορισμένων κακόβουλα «εκμεταλλεύσιμων» τεχνικών αδυναμιών τους, αλλά και των εκπεφρασμένων φόβων και εγκυμονούντων κινδύνων παραβίασης της ιδιωτικότητας, από την προαναγγελθείσα κλιμάκωση της χρήσης τους.

2. Συμπεριφορική Αυθεντικοποίηση

Με την έννοια αυτή αποδίδεται κάθε συγκεκριμενοποιημένη διαδικασία *επιβεβαίωσης της ταυτότητας μιας οντότητας, με βάση εγνωσμένα και αποδεκτά, συμπεριφορικά χαρακτηριστικά και μοτίβα δράσης της εκάστοτε συναλλαγής*.[621] Η υλοποίηση αυτού του είδους της αυθεντικοποίησης δεν μπορεί να αποκτήσει ιδιαίτερο βαθμό αυτονομίας, μιας και ο ρόλος της προβλέπεται περισσότερο ως *επικουρικός για τα πιο ουσιώδη συστήματα ΑΑΑ*. Η ύπαρξη πρόσθετων συμπεριφορικών ελέγχων περαιτέρω επιβεβαίωσης μιας φερόμενης ως αυθεντικής ταυτότητας μπορεί να αποτελέσει *ένα ακόμη προστατευτικό στάδιο «κοσκινίσματος» των συναλλαγών*, στις οποίες εμφανίζονται ασυνήθιστες ή μη αναμενόμενες ενέργειες, που ενδέχεται να υποδεικνύουν κακόβουλες δραστηριότητες.

---

[615] Ανταλλαγή και επιβεβαίωση κρυπτογραφημένων συνθηματικών.

[616] Πηγή: " 25 RFID Case Studies Contents", 2007, Sam Polniak, διαθέσιμο από το δεσμό http://www.bin95.com/case_studies/RFID_Technology_Applications.htm.

[617] Όπως σε αεροδρόμια, χώρους στάθμευσης οχημάτων, νοσοκομεία, computer rooms κτλ.

[618] Όπως ανάγνωση ή τροποποίηση «ευαίσθητων» δεδομένων.

[619] Πηγή: "RFID Applications in Inventory Control", The Decision Maker's Direct, 2001, διαθέσιμο από το δεσμό http://www.decisioncraft.com/dmdirect/rfidapplications.htm.

[620] Πηγή: Διαδίκτυο, ιστοχώρος της online εγκυκλοπαίδειας WikiPedia, http://en.wikipedia.org/wiki/RFID#Problems_and_Concerns.

[621] Κύρια, βιβλιογραφική αναφορά: [FFIEC-IS].

3.Ταυτοποίηση υλικού

Η αυθεντικοποίηση συσκευών βρίσκει εφαρμογή είτε γενικά ως συμπλήρωμα στην αυθεντικοποίηση χρηστών και διεργασιών είτε όταν ειδικότερα απαιτείται (πρόσθετη) *ισχυρή διαβεβαίωση ότι η δείνα συσκευή εξουσιοδοτείται για να βρίσκεται και να πραγματοποιεί επικοινωνίες στο δίκτυο*.[622] Οι συσκευές επικυρώνονται μέσω απλών, κατάλληλα δομημένων, κρυπτογραφημένων μυστικών, όπως π.χ. προεγκατεστημένα στο υλικό κλειδιά (σαν το TPM endorsement key[623]) ή χάρη σε πιο περίπλοκες υποδομές δημοσίου κλειδιού (PKI), Kerberos και Sesame. Η αυθεντικοποίηση μπορεί να λαμβάνει χώρα συνήθως σε επίπεδα ανώτερα του στρώματος δικτύου του OSI (συμπεριλαμβανομένου και αυτού), με σημαντική εξαίρεση τις βασισμένες στο επίπεδο ζεύξης δεδομένων τεχνικές, που βασίζονται σε τυποποιημένα, μοναδικά χαρακτηριστικά των μέσων δικτύωσης (όπως οι διευθύνσεις MAC των καρτών δικτύου).

4. Συστήματα αμοιβαίας αυθεντικοποίησης/εμπιστοσύνης[624]

Η αμοιβαία αυθεντικοποίηση συμβαίνει, όταν *«συστήνονται» όλοι οι συμμετέχοντες σε μια επικοινωνία στα υπόλοιπα, συμβαλλόμενα μέρη*.[625] Ένα παράδειγμα μιας τέτοιας επικύρωσης είναι ο προσδιορισμός ενός τραπεζικού χρήστη Διαδικτύου στο πιστωτικό ίδρυμα, με την επίδειξη ενός κοινού τους μυστικού (στην κατοχή της τράπεζας, εν γνώσει του χρήστη) από το τραπεζικό σύστημα στο χρήστη, σε συνδυασμό με την πρότερη, σύγχρονη ή συνακόλουθη παρουσίαση ενός δεύτερου κοινού τους μυστικού (στην κατοχή του χρήστη, με τις «ευλογίες» της τράπεζας) από το χρήστη στο σύστημα. Το βασικό πλεονέκτημα της αμοιβαίας επικύρωσης είναι η *διαβεβαίωση ότι οι επικοινωνίες που πραγματοποιούνται είναι μεταξύ υπεύθυνα αλληλεμπιστευόμενων, συναλλασσόμενων οντοτήτων*. Οι υποδομές Kerberos και Sesame παρέχουν μια ισχυρή βάση για την εγκαθίδρυση αμοιβαία αυθεντικοποιημένων επικοινωνιών και συναλλαγών.

5. Ισορροπημένες μορφές SSO

Τα οφέλη από τις *μεθόδους ενιαίας (Single-Sign-On) αυθεντικοποίησης (ελέγχου πρόσβασης και καταγραφής)* είναι λίγο έως πολύ γνωστά· ταχύτητα, ευελιξία, εξοικονόμηση, αποδοχή, χρηστικότητα. Εφόσον, όμως, υποθετικά τα συστήματα SSO επιτρέπουν *ενιαία, ταυτόχρονη σύνοδο με πολλαπλές περιπτώσεις ευαίσθητων δεδομένων ή κρίσιμων συστημάτων*, το όλο

---

[622] Όπως στην προηγούμενη υποσημείωση.

[623] Βλέπε και σχετικό εδάφιο 4.3.2.

[624] Κύρια, βιβλιογραφική αναφορά: [KALYANI-AVA].

[625] Πηγή: Διαδίκτυο, ιστοχώρος της online εγκυκλοπαίδειας WikiPedia, http://en.wikipedia.org/wiki/Mutual_authentication.

προστατευτικό σχήμα *οφείλει να παρέχει ορισμένες, επιπρόσθετες δικλείδες ασφάλειας*. Η εξισορρόπηση των ωφελειών του SSO μοντέλου επιτελείται στη βάση της *επαρκούς ενδυνάμωσης των υπολοίπων υπηρεσιών ασφάλειας* του υφιστάμενου ΠΣ και της υπό συνθήκες *επαναληπτικής ζήτησης-διακρίβωσης των διαπιστευτηρίων* των πρότερα αναγνωρισμένων και υπό τρέχουσα εξυπηρέτηση οντοτήτων[626] (ιδιαίτερα στις περιπτώσεις χαρακτηριστικά σημαντικών ενεργειών από μέρους τους αλλά ακόμα και σε τυχαίες περιστάσεις, από απλή διάθεση για πρόληψη).

Τα 5 παραπάνω, τεχνολογικά κύματα είναι οι *καινούριες, επαναστατικές τάσεις στην εξακρίβωση των πληροφοριακών προνομίων* και μπορούν σίγουρα να αποτελέσουν χρήσιμα εργαλεία στον ευρύτερο αγώνα για περιορισμό των εχθρικών πράξεων των κακόβουλων προγραμμάτων, με την προϋπόθεση πως θα τεθούν υπό διεξοδικότερη περίσκεψη, εξορθολογισμό και βελτίωση των χαρακτηριστικών τους. Στην ιδανική εκδοχή, η ασφάλεια πληροφοριών χρειάζεται επειγόντως καινούρια πυρομαχικά και πολεμοφόδια να «μπαλώνουν υπάρχουσες τρύπες» (ακάλυπτα κενά ασφάλειας) και όχι βιαστικώς τοποθετημένα πρόσθετα να δημιουργούν και άλλες, ανεξερεύνητες ακόμα ευκαιρίες εκμετάλλευσης.

5.2.4 Κρυπτογραφία Παντού - Στεγανογραφικές δυνατότητες - Στεγανάλυση

Η τέχνη της κρυπτογραφίας έχει πια αρχίσει να δημιουργεί άρρηκτους δεσμούς με τις τρέχουσες προσεγγίσεις στην ασφάλεια και την προστασία δεδομένων τόσο σε ερευνητικό στάδιο όσο και στις παραγωγικές λύσεις. Ο ρόλος της *ξεπερνά πλέον τα στενά πλαίσια της εμπιστευτικότητας* και προοδευτικά παρουσιάζεται επιπλέον και ως εξέχουσας σημασίας δομικό κομμάτι για τη *διατήρηση της ισχύος της πλειοψηφίας των υπηρεσιών ασφάλειας*[627], τόσο του CIA όσο και του ευρύτερου Parkerian μοντέλου, με τα οποία γνωριστήκαμε στο Κεφάλαιο 2.

Στο εδάφιο αυτό αναδεικνύουμε, επίσης, το αυξημένο, ξεχωριστό ενδιαφέρον που εμφανίζει σταδιακά η εφαρμογή ορισμένων, στεγανογραφικών μεθόδων στην ασφάλεια πληροφοριών, αναπτύσσοντας την υπάρχουσα λογική στην περιρρέουσα ατμόσφαιρα και επισημαίνοντας τα πιθανά, πολλαπλά οφέλη από τη νόμιμη χρήση τους[628]. Χρησιμοποιώντας κανείς τη γενικότερη φιλοσοφία που διακατέχει τα στεγανογραφικά πρότυπα και τις αρχές που διέπουν

---

[626] Όπως στην προηγούμενη υποσημείωση.

[627] Πηγή: "Cryptography, Security and the Future", Bruce Schneier, 1997, διαθέσιμο από το δεσμό http://www.schneier.com/essay-005.html.

[628] Κύρια, βιβλιογραφική αναφορά: [JUDGE-SPPF].

τα συγκαλυμμένα κανάλια μπορεί να τα «εξημερώσει» προς την κατεύθυνση μιας αφενός υπερθετικού βαθμού ασφαλούς αποθήκευσης και αφετέρου σχεδόν απαρατήρητης από κακόβουλα «πλοκάμια» επικοινώνησης πληροφοριών:

1. **Στεγανά συστήματα αρχείων**

   Με τη βοήθεια -συγκριτικά αδιάφορων για κακόβουλους σκοπούς- μέσων κάλυψης με μεγάλη στεγο-χωρητικότητα (ικανό πλεόνασμα «άχρηστων» δεδομένων) όπως είναι τα αρχεία πολυμέσων, την εκτενή χρήση κρυπτογραφίας στα υπό κάλυψη δεδομένα και έναν επαρκή βαθμό τυχαιότητας στη διαρρύθμιση/διασπορά στα αποθηκευτικά μέσα επιτυγχάνεται η κατασκευή ενός στεγανογραφικού στρώματος/κελύφους για την αρχειοθέτηση κρίσιμων πληροφοριών. Ένα συμβατό Λ/Σ θα πρέπει να έχει προβλεφθεί να παρέχει σε χρήστες και καλόντα προγράμματα κατάλληλες ρουτίνες (API) για την -ανά πάσα ώρα και στιγμή- επιθυμητή και αυθεντικώς εξουσιοδοτημένη πρόσβαση (ανάγνωση/εγγραφή/εκτέλεση) στις εν λόγω πληροφορίες[629]. Μια πρωτότυπη υλοποίηση ενός τέτοιου συστήματος αρχείων είναι το StegFS[630] των Ross Anderson, Roger Needham και Adi Shamir.

2. **Αποστολή και λήψη στεγο-μηνυμάτων**

   Κρίσιμες πληροφορίες κρύβονται μέσα σε καθόλα νόμιμη και φυσιολογική κυκλοφορία διαφόρων πακέτων, αλλά και στα περιεχόμενα μεγαλύτερων ομάδων δικτυακών δεδομένων, παράγοντας έναν πολύ δύσκολα μετρήσιμο και εντοπίσιμο στεγο-θόρυβο στις επικοινωνίες.[631] Τα μηνύματα κάλυψης επιλέγονται με τέτοιο σκεπτικό, ώστε να παρουσιάζουν/προκαλούν το μικρότερο δυνατό ενδιαφέρον στον επίδοξο επιτιθέμενο και το προσαρμοσμένο στους στόχους του οπλολογισμικό του. Η οντότητα που είναι επιθυμητό να λάβει το στεγο-μήνυμα πρέπει να είναι σε θέση να γνωρίζει/περιμένει εκ των προτέρων ή να επιβεβαιώνει την ύπαρξη κάποιας, χρήσιμης πληροφορίας που την αφορά εντός της εισερχόμενης κίνησης, πέρα από το να έχει στην κατοχή της κατάλληλες εξουσιοδοτήσεις και να διαθέτει τα απαραίτητα μέσα για την εμφάνιση/ανακατασκευή των περιεχομένων του κρυφού μηνύματος.

Το μεγάλο πλεονέκτημα από τη χρήση της στεγανογραφίας και των απόκρυφων καναλιών είναι πάντοτε οι εξαιρετικές ιδιότητες του εμπλεκόμενου στεγανογραφήματος, σε

---

[629] Κύρια, βιβλιογραφική αναφορά: [KUHN-SFSL].

[630] Κύρια, βιβλιογραφική αναφορά: [ANDERSON_NEEDHAM_SHAMIR-SFS].

[631] Κύρια, βιβλιογραφική αναφορά: [EDMEAD-SAIH].

αντιπαραβολή με ένα κρυπτογράφημα, να προορίζεται για όχι απλά, αλλά σημασιολογικά προνομιούχες και εξουσιοδοτημένες οντότητες επεξεργασίας, να μην προσελκύει εκ των προτέρων τα «αδιάκριτα μάτια» και να μην κινεί υποψίες για κρίσιμο-χρήσιμο περιεχόμενο. Για τους λόγους τούτους μπορεί να φανεί και ιδιαίτερα ευεργετική η προληπτική δράση των μηχανισμών αυτών στον αγώνα για τον περιορισμό της κυριαρχίας και της εξάπλωσης των αυτοαναπαραγόμενων, κακόβουλων προγραμμάτων.

Στον τομέα της διάγνωσης των κακοπροαίρετων, συγκαλυμμένων καναλιών και στεγανογραφημάτων, τέλος, παρατηρείται το τελευταίο διάστημα μια σημαντική αναμόχλευση του ερευνητικού ενδιαφέροντος. Ο όψιμος κίνδυνος από την κακόβουλη εκμετάλλευση των παρεχόμενων δυνατοτήτων (όπως είδαμε σε προηγούμενο εδάφιο του τρέχοντος κεφαλαίου) έχει κινητοποιήσει τους ανθρώπους της ασφάλειας, που εργάζονται με σκοπό τον περιορισμό του.

Με τη συνδρομή της στατιστικής και της φασματικής ανάλυσης[632] και των λεξικογραφικών ή ωμής δύναμης δοκιμών[633] είμαστε πλέον σε θέση με ικανοποιητική επιτυχία να αναγνωρίζουμε τις πιθανές ευκαιρίες-εκδηλώσεις στεγανογραφικής απόκρυψης, τουλάχιστον στο επίπεδο της επεξεργασμένης, ψηφιακής εικόνας. Όσον αφορά τις λοιπές, στεγανογραφικά ενδιαφέρουσες, κατηγορίες των πολυμέσων, όμως, η πρόοδος της επιθυμητής στεγανάλυσης[634] δεν είναι τόσο αξιοσημείωτη κυρίως λόγω της γενικότερα μεγαλύτερης στεγο-χωρητικότητας και όγκου ανάλυσης των μέσων αυτών, αλλά και εξαιτίας των αξιόλογων, σημασιολογικότερων δυνατοτήτων τους. Μόνος σύμμαχος σε αυτές τις περιπτώσεις είναι ο απλός (π.χ. με τη βοήθεια MD5 συναρτήσεων σύνοψης) ή πιο σύνθετος έλεγχος ακεραιότητας,[635] που απαιτεί όμως άμεση/έμμεση αναφορά σε θεωρούμενο ως «μη πειραγμένο» πρωτότυπο, για να ανιχνεύσει την όποια στεγανογραφική τροποποίησή του και με αυτή την έννοια δεν μπορεί να αποτελέσει μια καθολική, ικανοποιητική λύση. Αν δε προχωρήσει κανείς στη διερεύνηση των εξελίξεων στην αντιμετώπιση των συγκαλυμμένων επικοινωνιών τα πράγματα μοιάζουν χειρότερα· μόνο ειδικά διαμορφωμένα ανιχνευτικά ή αντιπυρικά μέσα στο επίπεδο εφαρμογής και τυχόν εξειδικευμένοι έλεγχοι κατάστασης εμφανίζουν κάποιες αξιόλογες, αποτρεπτικές ικανότητες[636], με τα απόκρυφα πακέτα στις περισσότερες περιπτώσεις να μπορούν προς το παρόν να ταξιδεύουν με ανεμπόδιστο και ανεπαίσθητο τρόπο διατρέχοντας τις διάφορες, πληροφοριακές εγκαταστάσεις, ιδιαίτερα όταν

---

[632] Κύρια, βιβλιογραφική αναφορά: [DICKMAN-OS].

[633] Κύρια, βιβλιογραφική αναφορά: [PROVOS_HONEYMAN-HSAIS].

[634] Η τέχνη της «αποστεγανογράφησης» ενός στεγανογραφήματος, έννοια σημασιολογικά σε ομόρροπη κατεύθυνση με εκείνην της κρυπτανάλυσης.

[635] Κύρια, βιβλιογραφική αναφορά: [DICKMAN-OS].

[636] Κύρια, βιβλιογραφική αναφορά: [SIEFFERT-SIDS].

τα συστήματα δεν διακατέχονται από τάσεις και πολιτικές πρόληψης, όπως αυτή των μειωμένων/ελαχίστων δικαιωμάτων χρήσης[637]. Συνεπώς, έχοντας υπόψιν την αναμενόμενη δυναμική και τον αντίκτυπο από διάφορες, κακόβουλες υλοποιήσεις, γίνεται άμεσα αντιληπτό πως υπάρχει σαφής και δεδηλωμένη ανάγκη για πιο δραστήρια, επιστημονική μελέτη, δοκιμή και εφεύρεση νέων προσεγγίσεων στην ανάλυση και προστασία από τις απειλές αυτές, με στόχο την καθιέρωση πιο αποδεκτών και ενιαίων λύσεων ασφάλειας.

5.2.5 Πολιτική της «Θωράκισης του κάθε κόμβου»

Αναμφίβολα, η κεντρικού τύπου προστασία που παρέχουν τα διάφορα, δικτυακά συστήματα ασφάλειας είναι απαραίτητη για την άμυνα ενάντια στις εχθροπραξίες, που εκδηλώνονται μέσω ιών και σκουληκιών. Σήμερα, όμως, παρατηρείται μια *μεγαλύτερη αναθέρμανση του ενδιαφέροντος για τις εντός κόμβων λύσεις*, καθώς δεν είναι λίγες οι μελέτες που καταλήγουν και οι καταστάσεις που καταδεικνύουν την αναγκαιότητα ισχυρών πλεγμάτων θωράκισης και καταστολής, σε επίπεδο κάθε συμμετέχοντα σε δοθέν ΠΣ κόμβο[638]. Αυτό *δε σημαίνει πως οι δικτυακού τύπου λύσεις παραμελούνται, πόσο μάλλον παραγκωνίζονται, αλλά πως δεν επαρκούν από μόνες τους*, καθώς πλέον υφίστανται αντικειμενικές συνθήκες που αναβαθμίζουν τη σπουδαιότητα του ρόλου των ενδοκομβικών, προστατευτικών μηχανισμών στην ασφάλεια των πληροφοριακών συγκροτημάτων.

Παράγοντες, όπως η διαφαινόμενη έξαρση των λογισμικών υπονόμευσης των Λ/Σ και η δυνατότητα κλιμακωτών επιθέσεων με στόχο την επικράτεια ενός ΠΣ, με ορμητήριο ακόμα και ένα μόνο παραβιασμένο μέλος του, έχουν συντελέσει σε μια στροφή προς μια πιο *αποκεντρωμένη και κατανεμημένη θεώρηση της ασφάλειας*.[639] Τα δικτυακού επιπέδου, περιμετρικά συστήματα φαίνεται πως δεν καταφέρνουν να ελέγξουν αποτελεσματικά ένα σημαντικό μερίδιο πιθανών υποβαθμίσεων, με κυριότερο επίκεντρο τα εντός κάποιου κόμβου τεκταινόμενα, που μπορούν να αποκτήσουν άμεσες διακλαδώσεις σε γειτονικούς σταθμούς, καρκινοβατώντας έτσι σταδιακά σε ολόκληρη τη δικτυακή υποδομή. Ο συνολικός βαθμός ασφάλειας κάθε ΠΣ κρίνεται άλλωστε πάντοτε στο επίπεδο του πιο ασθενούς σημείου του[640], για αυτό και ο περιορισμός των αδύναμων κρίκων/δικτυακών κόμβων και η ενδυνάμωση

---

[637] Κύρια, βιβλιογραφική αναφορά: [ROGERS-KKUCCC].

[638] Κύρια, βιβλιογραφική αναφορά: [KALYANI-AVA].

[639] Πηγή: "The Perimeter Problem", Simson Garfinkel, 2005, διαθέσιμο από το δεσμό http://www.csoonline.com/read/110105/machine.html.

[640] Πηγή: "Weakest Link Security", Bruce Schneier, 2005, διαθέσιμο από το δεσμό http://www.schneier.com/blog/archives/2005/12/weakest_link_se.html.

τους με ισχυρά, προστατευτικά/αντιστασιακά μέτρα εμφανίζονται ως τόσο σημαντικές διαδικασίες για την όλη «αρτιότητα» του οικοδομήματος.

Τεχνολογίες, όπως τα συστήματα hIDS/hIPS, τα κατεξοχήν λογισμικού τύπου «προσωπικά» αντιπυρικά τείχη, τα εμφατικά, αξιόπιστα συστήματα επεξεργασίας και περιφερειακά των υπολογιστικών συστημάτων και φυσικά πάσης φύσεως σαρωτές, εξομοιωτές, παρεμποδιστές, ελεγκτές ακεραιότητας και λοιπά εξειδικευμένα εργαλεία ανάλυσης και προστασίας, που εδρεύουν εντός της σφαίρας ενός κόμβου, σε συνδυασμό με την ενίσχυση των δεδομένων, εγγενών μηχανισμών και δικλείδων του Λ/Σ αυτού -πράγματα που συζητήθηκαν διεξοδικά στο Κεφάλαιο 4 κυρίως-, προβάλλουν ολοένα και περισσότερο ως το ποθητό σήμερα, αποτρεπτικό και κατασταλτικό για τη δράση των αυτοαναπαραγόμενων όπλων, δίχτυ ασφάλειας.[641] Αυτές οι λύσεις εμφανίζουν *ιδιαίτερα αυξημένη δυναμική επιτυχίας* στην αναγνώριση και αντιμετώπιση εκείνων των απειλών, που εφορμούν από «εντός των τειχών» ενός υπονομευμένου κόμβου και δε γίνονται με τόσο άμεσο τρόπο αντιληπτές από τους δικτυακά ευρισκόμενους ομολόγους της άμυνας.

Στην περίπτωση ενός απλού και μικρού σε μέγεθος δικτύου πληροφοριών η εφαρμογή, η παραμετροποίηση και ο έλεγχος των προηγούμενων μηχανισμών από τους χρήστες/χειριστές του είναι σχετικά εύκολα πραγματοποιήσιμες και το κέρδος από τον εξοπλισμό των κόμβων του με τις όποιες εν λόγω τεχνολογίες θα φανεί άμεσα. Τα παραπάνω συστήματα, όμως, στα πλαίσια ενός πολυπληθούς δικτυώματος και ενός περιβάλλοντος χρήσης με συγκεκριμένες αρμοδιότητες και ευθύνες εποπτείας του από ειδικευμένο προσωπικό, είναι σίγουρα *επίπονο, πολυδάπανο και πολύπλοκο να τα εγκαταστήσει, παραμετροποιήσει και να τα διαχειριστεί κάποιος σωστά και αποδοτικά*, σε σχέση με τις πιο κεντρικές, δικτυακές λύσεις. Η πιο ενδιαφέρουσα, υπάρχουσα προοπτική, που παρουσιάζεται ως η πλέον πιθανή, μελλοντική και *βέλτιστα συμβιβαστική οδός, είναι η ενσωμάτωση προτερημάτων της κεντρικοποιημένης διαχείρισης στα ενδοκομβικά συστήματα* με τη μορφή π.χ. αυτοδύναμων, ανεξάρτητων μα αλληλοσυνεργαζόμενων πρακτόρων λογισμικού, που (θα μπορούν να) συντονίζονται και ελέγχονται συνολικά από κάποια, κεντρικά σημεία του πολυδύναμου, υπολογιστικού δικτύου.

Όπως και να ’χει, οι σύγχρονες απειλές έχουν φανερώσει την αναγκαιότητα και αποτελεσματικότητα μέτρων και μηχανισμών ασφάλειας στο επίπεδο του κάθε κόμβου, που θα δύνανται να ψηλαφούν την οποιαδήποτε σπιθαμή τους για την παραμικρή υπόνοια υπονόμευσης και πληροφοριακής επιθετικότητας, ενισχύοντας έτσι τη συνολική φερεγγυότητα και ανθεκτικότητα του υπερκείμενου ΠΣ. Η στάση της επιστημονικής κοινότητας και των υπευθύνων ασφάλειας πληροφοριών, που συνεχώς προτρέπουν και

---

[641] Πηγή: “The Science of Host Based Security”, Ray Zadjmool, 2004, διαθέσιμο από το δεσμό http://www.windowsecurity.com/articles/Science_Host_Based_Security.html.

προτάσσουν τη *μεγαλύτερη προώθηση της εφαρμογής ενδοκομβικών συστημάτων*[642], συνηγορεί υπέρ αυτής της διαπίστωσης.

5.3 Νομική Διάσταση

Τα συμπεράσματα από τη μέχρι τώρα προσπάθεια/πρόοδο θέσπισης και επιβολής νόμων για την προστασία από το η-έγκλημα και συνεπώς και την πληροφοριακή εχθροπραξία με κακόβουλα όπλα δεν είναι ούτε ιδιαίτερα ενθαρρυντικά ούτε κολακευτικά[643] και απαιτείται μια ριζική, συλλογική ανατροπή/αναδιάρθρωση της μέχρι στιγμής επικρατούσας κατάστασης[644]:

1. *Η εμπιστοσύνη στους μη εξεζητημένους νόμους του αστικού κώδικα είναι μια μη υποσχόμενη προσέγγιση που πρέπει να εγκαταλειφθεί/αποθαρρυνθεί*. Παρά την πρόοδο που σημειώνεται σε πολλές χώρες, οι περισσότερες χώρες στηρίζονται ακόμα στο γενικόλογο, αστικό δίκαιο για να διώξουν τα κυβερνοεγκλήματα. Η ισχυρή πλειοψηφία των χωρών, επίσης, στηρίζεται σε αρχαΐζοντα καταστατικά, που προηγούνται χρονικά της γέννησης του κυβερνοχώρου και δεν έχουν παρά ελάχιστα δοκιμαστεί από τα δικαστήρια. Απαιτείται άμεση επανεξέταση και αναθεώρηση των αντίστοιχων, ανεπαρκών και μη αποδοτικών, νομοθετικών πρακτικών και αναδιάρθρωσή τους σε πιο ουσιαστική και επίκαιρη, ποινική βάση.

2. Υφίσταται *σημαντική ανάγκη κατάλληλης εκπαίδευσης* συνηγόρων, στα θέματα που άπτονται του ευρύτερου πεδίου της κυβερνοασφάλειας, ώστε να είναι δυνατή η μεγαλύτερη εξειδίκευσή τους και άρα η αποτελεσματικότερη υπεράσπιση των συμφερόντων τυχόντων εμπλεκόμενων σε υποθέσεις κυβερνοεγκλημάτων. Εκπαίδευση εννοείται πως χρειάζεται και σε κάθε ενδιαφερόμενο (από τον απλό πολίτη μέχρι τον εργαζόμενο στο χώρο του κυβερνοχώρου) κατόπιν της θεσμοθέτησης νέων μέτρων και κωδίκων, προκειμένου να κατανοήσει και να συμμορφωθεί καλύτερα στις καινούριες απαιτήσεις/επιταγές, διαφυλάσσοντας παράλληλα τα όποια δικαιώματά του. Κατάλληλη κατάρτιση και εξειδίκευση, τέλος, απαιτείται ξεχωριστά και από τα εκτελεστικά όργανα και σώματα επιβολής του νόμου, στα θέματα του κυβερνοχώρου και της ασφάλειάς του, κάτι που προς το παρόν υφίσταται σε πενιχρό, γενικά, βαθμό[645].

---

[642] Πηγή: Διαδίκτυο, ιστοχώρος της Gartner Research, http://www.gartner.com/DisplayDocument?doc_cd=119940.

[643] Κύρια, βιβλιογραφική αναφορά: [MCCONNELL-CCP], [CHIK-CCLMNGIS].

[644] Κύρια, βιβλιογραφική αναφορά: [BRENNER_GOODMAN-CNHNPPL].

[645] Κύρια, βιβλιογραφική αναφορά: [SHINDER-SC].

3. *Οι αδύνατες, ποινικές ρήτρες περιορίζουν την αποτροπή του πολέμου*. Στα περισσότερο ενημερωμένα, εγκληματικά καταστατικά περιέχεται πλέον κάποια έστω στοιχειώδης και βάσιμη πρόβλεψη για κυρώσεις τουλάχιστον για τα εγκλήματα, που μπορούν να έχουν μεγάλης κλίμακας οικονομικά και κοινωνικά αποτελέσματα.

4. *Η προετοιμασία των οργανισμών για την αυτοάμυνα παραμένει η πρώτη γραμμή υπεράσπισης*. Η γενική αδυναμία των θεσμών αυξάνει τη σημασία των προσπαθειών του ιδιωτικού και ευρύτερου επιχειρηματικού τομέα να αναπτυχθούν και να υιοθετηθούν ισχυρές και αποδοτικές τεχνικές λύσεις και διοικητικές πρακτικές, για την ασφάλεια πληροφοριών και συστημάτων διασύνδεσης και διεπικοινωνίας.

5. *Η διεθνής προοπτική των σχετικών νόμων προς το παρόν δημιουργεί λίγη βεβαιότητα* ως προς την εφικτότητα και πιθανή επιτυχία της, παρά τα θαρραλέα[646] και σίγουρα θεμιτά, πρώτα βήματα. Λίγη συναίνεση υπάρχει μεταξύ των χωρών σχετικά με το ποιες ακριβώς προληπτικές-αποτρεπτικές συνταγές ενάντια στα η-εγκλήματα πρέπει να ακολουθήσουν σε κοινή βάση τη νομική οδό.

6. Μια πρότυπη προσέγγιση απαιτείται. Οι περισσότερες χώρες, ιδιαίτερα όσες εδρεύουν στον αναπτυσσόμενο κόσμο, επιδιώκουν ένα *πρότυπο μοντέλο συμπεριφοράς που να συνεισφέρει καλές, εφαρμόσιμες πρακτικές*. Τέτοιες χώρες, ενώ -σε επίπεδο διακυβέρνησης τουλάχιστον- συνήθως αναγνωρίζουν σε μεγάλο βαθμό τη σημασία της πάταξης των σχετικών με υπολογιστές κακόβουλων πράξεων, προκειμένου να προωθηθεί ένα ασφαλές περιβάλλον για το ηλεκτρονικό εμπόριο, τις συναλλαγές και τις υπηρεσίες, λίγες διαθέτουν τους απαραίτητους νομικούς, οικονομικούς και τεχνικούς πόρους ή/και την απαιτούμενη βούληση, ώστε να εξετάσουν τις περιπλοκές της προσαρμογής των εγκληματικών καταστατικών τους στις ιδιομορφίες και τα ιδιαίτερα γνωρίσματα του κυβερνοχώρου. Μια *συντονισμένη συνεργασία και σύμπραξη φορέων του δημοσίου και του ιδιωτικού τομέα*[647], για την ανάπτυξη/παραγωγή (προ)τυποποιημένων προσεγγίσεων στις χώρες αυτές, μπορεί να βοηθήσει στην *εξάλειψη του πιθανού κινδύνου δημιουργίας «ασφαλών λιμένων»*[648] για το κυβερνοέγκλημα και τους θιασώτες αυτού.

Αυτό σε καμία περίπτωση δε σημαίνει πως δεν γίνεται «δουλειά»· υπάρχει, όπως είδαμε, συντονισμένη, παγκόσμια προσπάθεια θεσμοθέτησης και επιβολής νόμων κατά των υστερόβουλων δράσεων στον κυβερνοχώρο (προεξάρχουσας και της Συνθήκης του 2001 του

---

[646] Όπως παρουσιάστηκαν στο εδάφιο 4.7 του αμέσως προηγούμενου κεφαλαίου.

[647] Κύρια, βιβλιογραφική αναφορά: [COCHRAN-PSNI].

[648] Πηγή, "Cybercrime Havens: Challenges and Solutions", Susan Brenner and Joseph Schwerha, 2007, διαθέσιμο από το δεσμό http://www.abanet.org/buslaw/blt/2007-11-12/schwerha.shtml.

Ευρωπαϊκού Συμβουλίου για το Κυβερνοέγκλημα αλλά και των σχετικών ψηφισμάτων του Ο.Η.Ε.). Απλά, οι θεωρητικές δεσμεύσεις των χωρών και οι διακρατικές συμβάσεις εμφανίζουν συχνά ποικίλα προβλήματα επιτυχημένης υλοποίησης και αποτελεσματικής μετατροπής σε ποινικό κώδικα, με αποτέλεσμα να εκκρεμούν ή να αποτυγχάνουν/απορρίπτονται επιχειρήσεις και δικαστικές πράξεις κατά των η-κακοποιών, ενώ δε λείπουν και οι περιπτώσεις χωρών που αδυνατούν ή είναι απρόθυμες να συνεισφέρουν στην καταπολέμηση του κυβερνοεγκλήματος, αποτελώντας έτσι καταφύγιο για τους εγκληματίες του είδους. Και ας μην ξεχνάμε πως όσο οι νόμοι δεν αλλάζουν και δεν ενδυναμώνονται η λογική του δεδικασμένου στα απαρχαιωμένα συστήματα θα διασφαλίζει την εύκολη ατιμωρησία των δραστών.

Τα βασικότερα αίτια των προβλημάτων, που συναντώνται ακόμη και σήμερα στο χώρο της νομικής προσέγγισης της κυβερνοασφάλειας, είναι κατά κύριο λόγο θέματα οργάνωσης και διοίκησης και λιγότερο πια ευαισθητοποίησης/συνειδητοποίησης σε κρατικό επίπεδο:

- Οι γραφειοκρατικές καθυστερήσεις και τα λοιπά προσκόμματα των κατά τόπους νομοσχεδίων και ψηφισμάτων.
- Τα διακρατικά, νομικά χάσματα και οι συναφείς διαφοροποιήσεις/αντιθέσεις.
- Τα «παραθυράκια», οι προχειρότητες και οι παραλείψεις του σχετικού, αστικού/ποινικού δικαίου.
- Η απροθυμία ή η έλλειψη ισχυρής κρατικής βούλησης στις νομοθετικές (μεταρ)ρυθμίσεις.
- Η απουσία συντονιστικών οργάνων, η ανεπάρκεια των διαδικασιών και των δομών και η έλλειψη κατάλληλων, στρατηγικών πλαισίων αναφοράς κυρίως για τις αναπτυσσόμενες χώρες.
- Η έλλειψη κονδυλίων για τη χρηματοδότηση σχετικής έρευνας στις αναπτυσσόμενες ή υπανάπτυκτες χώρες.
- Οι εκτελεστικές και δικαστικές αδυναμίες των οργάνων και λειτουργών επιβολής του νόμου και ιδίως σε θέματα εγκλημάτων σχετικών με τις όψιμες, ψηφιακές τεχνολογίες[649].

Αναμένεται, λοιπόν, στο μέλλον, καθώς είναι ιδιαίτερα επιθυμητή και αναγκαία, μια ακόμη μεγαλύτερη προσπάθεια από πλευράς νομολογίας και πρότασης νομοσχεδίων και από τη σκοπιά μιας καλύτερα σχεδιασμένης και πιο ολοκληρωμένης και συνάμα καθολικής

[649] Κύρια, βιβλιογραφική αναφορά: [SHINDER-SC].

εφαρμογής των θεωρητικών εξαγγελιών και των διεθνών και τοπικών ψηφισμάτων και οι προσδοκίες παραμένουν υψηλές. Αυτό το κλίμα φανερώνουν άλλωστε και πρόσφατες συνεδριάσεις του Ο.Η.Ε.[650]

Το κυβερνοέγκλημα και ειδικά ο κυβερνοπόλεμος μέσω κακόβουλων προγραμμάτων είναι ένα ευρύ πρόβλημα που αψηφά και διαπερνά όλα τα σύνορα και τα όρια, και ως εκ τούτου πρέπει ομοίως να δρουν τα εργαλεία επιβολής του νόμου. Υπάρχει *έντονη ανάγκη για ακόμη διεξοδικότερη, διακρατική και δια-οργανωσιακή συνεργασία και συμφωνία-εναρμόνιση στην ιδιαίτερη νομοθεσία και θεσμική αντιμετώπιση*[651], που πρέπει να διέπει τα δικτυοκεντρικά ΠΣ και κύρια το Διαδίκτυο, σε ευαίσθητα θέματα όπως το κυβερνοέγκλημα και το κακόβουλο λογισμικό, ώστε να αποτρέπονται και να τιμωρούνται παραδειγματικά τέτοιες δράσεις, ανάλογα με το ειδικό βάρος τους (προθέσεις, στόχοι) και τα αποτελέσματά τους, σε υπερεθνικό επίπεδο και χωρίς απαράδεκτες εξαιρέσεις. Η *οικονομική ενίσχυση των χωρών με ασθενέστερες υποδομές και κανονιστικά πλαίσια* και η παροχή πρόσθετων κινήτρων ίσως θα πρέπει να θεωρηθεί πλέον μια πρακτική στρατηγικής σημασίας για την εξέλιξη των πραγμάτων. Ομοίως και η *επιβολή κυρώσεων ή ρητρών*, στην περίπτωση ανεπιτυχούς ή αδόκιμης εφαρμογής των κοινά συμφωνημένων πρακτικών. Τα διεθνή δικαστήρια (π.χ. Χάγη), οι διάφοροι παγκόσμιοι οργανισμοί (ITU, US-CERT, ENISA, IETF, ICANN) που παρατηρούν, συντονίζουν ή συντηρούν τον κόσμο του Διαδικτύου και των δικτυοκεντρικών ΠΣ και τα εκτελεστικά όργανα του νόμου και της τάξης (Interpol, Σ.Δ.Η.Ε.) μπορούν και πρέπει να συνεισφέρουν ακόμη περισσότερο με κατάλληλο τρόπο στην προσπάθεια αυτή (θιγόμενων) κυβερνήσεων και επιχειρήσεων να «στριμώξουν» περαιτέρω τους κακόβουλους δράστες, τηρώντας πάντα το δέοντα σεβασμό στα πανανθρώπινα δικαιώματα (ελευθερία, επικοινωνία, ιδιωτικό απόρρητο κτλ) και τους υπόλοιπους, κείμενους νόμους.

[650] Πηγή: "Law Comes To Cyberspace", Stein Schjolberg, 2005, διαθέσιμο από το δεσμό http://www.cybercrimelaw.net/documents/UN_Bangkok_05.htm.

[651] Κύρια, βιβλιογραφική αναφορά: [SCHJOLBERG_HUBBARD-HNLAC].

6 *Σκέψεις-Αναλύσεις-Προτάσεις*

Στο κομμάτι αυτό της εργασίας, αφού παρατίθενται χρήσιμα και ενδιαφέροντα στοιχεία για τα πρωταρχικά αίτια, τους εμπνευστές και δράστες και τελικά τα αποτελέσματα των πληροφοριακών μαχών με χρήση οπλολογισμικού, προχωρούμε σε μια παρακαταθήκη απόψεων για μια ρεαλιστική και συλλογικής φύσης αντιμετώπιση του κινδύνου -όπως αυτός αναλύθηκε στην πορεία της διπλωματικής αυτής- από τις διαχρονικές και σήμερα καλά κρατούσες πληροφοριακές πράξεις εχθρότητας που τυγχάνουν της συνδρομής του αυτοαναπαραγόμενου προγράμματος-υπερόπλου.

6.1 Κίνητρα για τη συγγραφή και χρήση κακόβουλων όπλων

Η διερεύνηση των ενδότερων μηχανισμών που ωθούν άτομα στη συγγραφή και τη χρήση ιών και σκουληκιών παρουσιάζει εξαιρετικό ενδιαφέρον από κάθε άποψη και δεν είναι σε καμία περίπτωση απλή υπόθεση. Τα κίνητρα αντικατοπτρίζονται στο είδος και την πολυπλοκότητα του παραγόμενου, κακόβουλου προγράμματος και είναι αυτά που επίσης καθορίζουν σε μεγάλο βαθμό τη φύση και τη δεινότητα μιας πληροφοριακής εχθροπραξίας[652], με όπλο το εκάστοτε εν λόγω λογισμικό. Ακόμα, η ανεύρεση των αιτίων που οδηγούν ορισμένες ομάδες ανθρώπων στην κατασκευή και χρήση κακόβουλων όπλων μπορεί να μας βοηθήσει να

[652] Το στοιχεία υπέρ αυτού του επιχειρήματος είναι διάχυτα στα Κεφάλαια 2 και 3.

κατανοήσουμε καλύτερα το προφίλ των ανθρώπων αυτών και να αποκτήσουμε μια καλύτερη εικόνα για την ευρύτητα της κοινωνικής διείσδυσης των συγκεκριμένων ομάδων.[653]

Γενικότερα, διακρίνει κανείς *τρία επίπεδα νοήμονος σχεδιασμού ή/και συνειδητής χρήσης* κακόβουλων όπλων λογισμικού[654]:

6.1.1 Συναισθηματική Σφαίρα

Στην κατηγορία αυτή ανήκουν τα κίνητρα που αφορούν *ανθρώπινες παρορμήσεις ή συναισθηματικής φύσης επιθυμίες*[655], όπως για παράδειγμα:

- Καταξίωση/Δόξα/Αναγνωρισιμότητα/Ματαιοδοξία.
- Διασκέδαση-Παιχνίδι/Πειραματισμός.
- Εκδίκηση.
- Απέχθεια/Μίσος/Παράνοια.

Οι πολύ προσωπικές αυτές, συναισθηματικές επιλογές ή έξεις αποτελούν τυπικά μοτίβα της βαθύτερης ιδιοσυγκρασίας κακόβουλων προγραμματιστών ή δραστών και κάποιες από αυτές είναι συχνά ευδιάκριτες σε μεγάλο πλήθος παραδειγμάτων σχεδιασμού οπλολογισμικού και επίθεσης με χρήση αυτού.

6.1.2 Οικονομική Σφαίρα

Η σφαίρα αυτή αφορά *ιδιοτελείς -κατεξοχήν οικονομικού χαρακτήρα- ανάγκες ή επιθυμίες του συγγραφέα ή του δράστη* και έχει κυρίως 2 εκφραστές[656]:

- Άμεσο, οικονομικό κέρδος ή αντάλλαγμα από συναλλαγή (πώληση οπλολογισμικού, οικονομικού τύπου εξαπάτηση-εκβιασμός θυμάτων).

---

[653] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM].

[654] Κύρια, βιβλιογραφική αναφορά: [CARNAHAN_ROBERTS_SHAY_YEARY-MBCV], [WEAVER_PAXSON-TCW].

[655] Πηγή: "The Viral Mind: Understanding the Motives of Malicious Coders", D.D.Shelby, 2002, διαθέσιμο από το δεσμό http://www.securityfocus.com/infocus/1583.

[656] Πηγή: "Some human dimensions of computer virus creation and infection", Andy Bisset, Geraldine Shipton, 2000, διαθέσιμο από το δεσμό http://vx.netlux.org/lib/mab00.html.

- Έλεγχος/Σαμποτάζ αντίπαλης, ανταγωνιστικής οντότητας υπό τη μορφή απόσπασης, δέσμευσης, υποκλοπής, παραχάραξης ή καταστροφής κρίσιμων για εκείνη πληροφοριών.

Ο αθέμιτος ανταγωνισμός και οι διάφορες, οικονομικές απάτες είναι μια εγνωσμένη, διεθνής πραγματικότητα. Το ίδιο ρεαλιστικό είναι και το σενάριο παροχής (συνήθως καλο)πληρωμένων υπηρεσιών παραγωγής (και διάθεσης) κακόβουλων προϊόντων από προγραμματιστές σε επίδοξους χρήστες-δράστες πληροφοριακής εχθροπραξίας. Στο κλίμα που αυτές οι καταστάσεις διαμορφώνουν, η *κατασκευή ή χρήση του κακόβουλου, αυτοαναπαραγόμενου λογισμικού αναδεικνύεται είτε σε ιδανικό πλουτοπαραγωγικό μέσο είτε σε αποτελεσματικό δίαυλο επίτευξης κάποιου ευρύτερου, στρατηγικού πλεονεκτήματος*.

Στις οικονομικού τύπου αιτίες πρέπει, ίσως, να αναζητηθεί και αποδοθεί η μεγαλύτερη πηγή των κακόβουλων προϊόντων και επιθέσεων, σήμερα.

6.1.3 Πολιτική-Ιδεολογική Σφαίρα

Η περίπτωση αυτή είναι η πιο εξεζητημένη από τις υπό διερεύνηση και αυτή που δύναται να παρουσιάσει τον πλέον επικίνδυνο αντίκτυπο, όπως αυτός θα αναλυθεί σε επόμενο εδάφιο. Άνθρωποι με συγκεκριμένες ιδεολογίες ή ιδεοληψίες καταφεύγουν στην παραγωγή κακόβουλων όπλων με σκοπό τη χρήση τους για τη διακήρυξη του πολιτικού/ιδεολογικού τους μανιφέστου ή οράματος.[657] Σε αυτήν τη σφαίρα κινήτρων εμπίπτουν οι (αιτιολογίες για όλες τις) εχθροπραξίες που λαμβάνουν τη μορφή συνειδητής, πολιτικής πράξης όπως π.χ. η ενεργητική διακήρυξη-υπεράσπιση ανθρωπίνων δικαιωμάτων ή ελευθεριών, η (κυβερνο)τρομοκρατία, ο στρατιωτικός, πληροφοριακός πόλεμος και η στοχευμένη επίθεση ή επιθετικός ακτιβισμός σε βάρος κυβερνητικών, στρατιωτικών, πολυεθνικών ή διεθνών οργανώσεων.[658]

Η *ιδεολογική προσέγγιση* στη συγγραφή και χρήση των επιβλαβών, αυτοαναπαραγόμενων προγραμμάτων μπορεί είτε να χρησιμοποιηθεί ως «άλλοθι» ή επισκίαση (συχνό κατά καιρούς φαινόμενο με τις διάφορες ιδεολογίες) βαθύτερων συναισθηματικών ή οικονομικών κινήτρων είτε ακόμα να εκφράσει μια πιο «σκληροπυρηνική» και αποφασιστική εχθροπραξία, που δε

---

[657] Πηγή: Διαδίκτυο, ιστοχώρος για το κυβερνοέγκλημα από το ThinkQuest της Oracle, http://library.thinkquest.org/04oct/00460/crimeMotives.html.

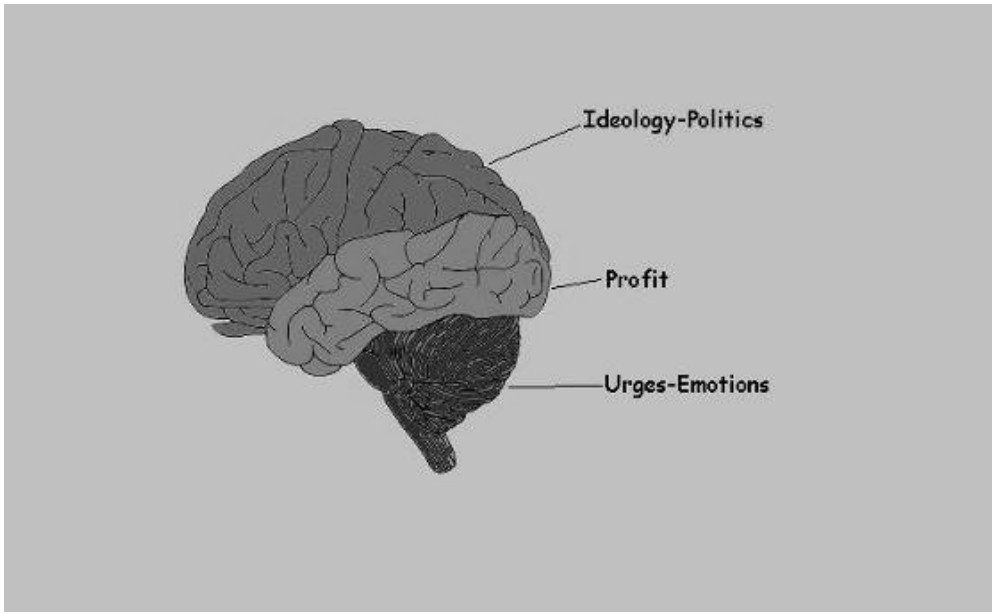
[658] Πηγή: Διαδίκτυο, ιστοχώρος της εταιρείας αντιϊομορφικών προϊόντων Sophos, http://www.sophos.com/pressoffice/news/articles/2005/02/va_deadcode.html.

φέρει απαραίτητα έντονες τέτοιες εξαρτήσεις, αλλά βασίζεται στην επιθυμία για καθαρά «πολιτικής» υφής εγχειρήματα και τοποθετήσεις.

Η δυνατότητα δημιουργίας κακόβουλων απειλών λογισμικού ικανών *να περάσουν κάποιου είδους «πολιτικό μήνυμα» ή να επιφέρουν μια «νέα πολιτική πραγματικότητα»* μέσω των διασυνδεδεμένων, δικτυοκεντρικών ΠΣ έχει «ανησυχήσει» και δραστηριοποιήσει εδώ και καιρό πολλούς, πιθανούς -καλοπροαίρετα ή κακοπροαίρετα- ενδιαφερόμενους[659] και η συνεχιζόμενη, παγκόσμια, τεχνολογική ανάπτυξη, συνεργασία και διαλειτουργικότητα αναμένεται να αυξήσει περαιτέρω τις πιθανότητες εκδήλωσης κρουσμάτων με ανάλογα κίνητρα.

Τα πραγματικά αίτια, στα οποία οφείλεται η συγγραφή ή η χρήση κάποιου ιού ή σκουληκιού από μέρους μιας οντότητας, συμβαίνει πολλές φορές να είναι ένας συνδυασμός ορισμένων από τα παραπάνω κίνητρα, ανεξαρτήτως του ειδικότερου διαχωρισμού αυτών στις 3 σφαίρες.

Τα παραπάνω περιγραφόμενα, «εγκεφαλικά επίπεδα» του κακόβουλου συγγραφέα ή δράστη εχθροπραξίας με οπλολογισμικό αποτυπώνονται γλαφυρά στο ακόλουθο σχήμα:



Σχήμα 38: Το «μυαλό» ενός κακόβουλου συγγραφέα ή δράστη

[659] Πηγή: "Political hacking: Crime or activism?", Kevin Komiega, 2000, διαθέσιμο από το δεσμό http://searchsecurity.techtarget.com/news/article/0,,sid14_gci506135,00.html.

6.2 Προφίλ συγγραφέων και χρηστών

Η διάκριση μεταξύ κάποιου που απλά κατασκευάζει ένα κακόβουλο πρόγραμμα και κάποιου ατόμου που το χρησιμοποιεί ως μέσο πληροφοριακής επίθεσης είναι προφανής· ο δεύτερος είναι ο φυσικός αυτουργός μιας εχθροπραξίας, ενώ ο πρώτος π.χ., όπως είδαμε στο αμέσως προηγούμενο εδάφιο, μπορεί απλά να κάνει το κέφι του ή/και να εκπληρώνει μια παραγγελία με οικονομικό αντάλλαγμα, χωρίς να ενδιαφέρεται για το πότε, πού, από ποιους και πώς θα χρησιμοποιηθεί το πρόγραμμά του. Οι δύο αυτές οντότητες μπορούν βεβαίως και να ταυτίζονται και μάλιστα κάτι τέτοιο παρατηρείται συχνά· και πάλι όμως δεν είναι απαραίτητο ο κατασκευαστής ενός δεδομένου ιού ή σκουληκιού να είναι και ο αποκλειστικός ή μοναδικός χρήστης του, όπως θα διαπιστώσουμε παρακάτω.

Η σκιαγράφηση των χαρακτηριστικών των δραστών και των ηθικών αυτουργών ή άλλων συνεργών τους είναι μια *εξαιρετικά σημαντική πτυχή της αποτελεσματικής επιβολής του νόμου*, είτε στον πραγματικό είτε στον ηλεκτρονικό κόσμο. Πολλοί ερευνητές και ψυχολόγοι έχουν αφιερώσει τις ζωές τους σε εργασίες και πειράματα που μελετούν και καταχωρούν την εγκληματική συμπεριφορά και το όποιο συναφές υπόβαθρο. Όσον αφορά το κυβερνοέγκλημα και ειδικότερα τον κλάδο του της συγγραφής και χρήσης κακόβουλου λογισμικού, η μακρόχρονη, ερευνητική προσπάθεια και η εμπειρική, βιωματική διαδικασία έχουν καταδείξει μέχρι τώρα τους ακόλουθους τύπους-κατηγορίες κακοποιών[660]:

I. Επαγγελματίες ανώτερης κοινωνικής βαθμίδας και επιστημονικής κατάρτισης (White-collar criminals)[661]

Η ομάδα αυτή υφίσταται ως *τρανή απόδειξη της κοινωνικής διάστασης του κυβερνοεγκλήματος*. Σε αντίθεση με τα λοιπά κοινά εγκλήματα, το η-έγκλημα και ειδικά η συγγραφή και χρήση κακόβουλων προγραμμάτων δεν ανήκει στις αξιόποινες πράξεις που με μεγαλύτερη πιθανότητα θα διέπρατταν καταπιεσμένες και αδικημένες κοινωνικές ομάδες ή άτομα των κατώτερων στρωμάτων ή/και με χαμηλό δείκτη πνευματικής ωριμότητας. Τέτοιου είδους πράξεις είναι εκτελέσιμες και επιτεύξιμες συνήθως από *άτομα με επαρκή ευφυΐα που κατέχουν σημαντικές, παραγωγικές θέσεις και διαβιούν στα μεσαία και ανώτερα, κοινωνικά επίπεδα*.

Το είδος αυτού του κυβερνοεγκληματία αποτελεί επίσης μια *διαρκή υπενθύμιση της ύπαρξης μιας εκ των έσω απειλής*, για την ασφάλεια των πληροφοριών και των

---

[660] Κύρια, βιβλιογραφική αναφορά: [SHINDER-SC].

[661] Πηγή: "The rise of the white collar hacker", John Leyden, 2004, διαθέσιμο από το δεσμό http://www.theregister.co.uk/2004/03/31/the_rise_of_the_white/.

συστημάτων οργανισμών και επιχειρήσεων από τα διαφορετικά κίνητρα (εκδίκηση, φιλαργυρία, δωροδοκία, εκβιασμός κτλ) των εργαζομένων και του προσωπικού τους (και ειδικά του περισσότερο τεχνολογικά εξοικειωμένου).

II. Κλινικές περιπτώσεις[662]

Για τις χρήζουσες ιατρικής γνωμάτευσης και φροντίδας περιπτώσεις κυβερνοκακοποιών και ιδιαιτέρως συγγραφέων και χρηστών κακόβουλων προγραμμάτων δεν μπορούν να ειπωθούν και πολλά παραπάνω από ό,τι στις αντίστοιχες περιπτώσεις του κοινού, ποινικού δικαίου. Και εδώ η αντιμετώπιση από τα δικαστήρια θεωρείται χαλαρή, σε σύγκριση με τους σώας τας φρένας και εν πλήρει συνειδήσει «συναδέλφους» τους. Η όποια *τεχνολογική ιδιοφυΐα* στις καταστάσεις αυτές συμβαίνει, πολλές φορές, να συνοδεύεται από ή να συμπληρώνει μια *αποκλίνουσα συμπεριφορά* (απομονωτισμός, αλλοτρίωση, επιθετικότητα, παραφιλία κτλ) ή μια *παρανοϊκή διάθεση* (εκδικητικότητα, μανίες, σχιζοφρένεια κτλ).

III. Καλλιτέχνες της απάτης (Con Artists, Spammers)[663]

Η *στροφή στην εκμετάλλευση των οικονομικών ευκαιριών που προκύπτουν μέσα από τη συγγραφή και χρήση κακόβουλων όπλων λογισμικού* έχει διαμορφώσει μια εκλεπτυσμένη μορφή η-εγκληματία, που ειδικεύεται στην *εξαπάτηση ή ύπουλη υπονόμευση χρηστών και συστημάτων* με τη βοήθεια επιβλαβούς λογισμικού και τις περισσότερες φορές με σκοπό την εξασφάλιση χρηματικού κέρδους. Το έγκλημα που συντελείται διαπράττεται από *τεχνολογικά καταρτισμένους επιτηδευματίες*, που βρίσκουν στη διάδοση και διάχυση των σύγχρονων μέσων ηλεκτρονικής επικοινωνίας (όπως π.χ. η ηλεκτρονική αλληλογραφία), συνεργασίας και ψυχαγωγίας το ιδανικό κανάλι για την εφαρμογή μεγαλεπήβολων σχεδίων -οικονομικής κυρίως- απάτης, σε ευρεία κλίμακα.

IV. Κυβερνοστρατιώτες-Χάκερς[664]

Η ιδιαίτερη αυτή και μαζική ομάδα ανθρώπων με τον χαρακτηρισμό χάκερ περιλαμβάνει στις τάξεις της ανθρώπους τόσο κείμενους στο μέρος της υπεράσπισης

---

[662] Πηγή: Διαδίκτυο, ιστοχώρος για το κυβερνοέγκλημα από το ThinkQuest της Oracle, http://library.thinkquest.org/04oct/00460/psychiatric.html.

[663] Πηγή: "Con artists on the Net", Timeri Murari, 2002, διαθέσιμο από το δεσμό http://www.thehindubusinessline.com/2002/08/17/stories/2002081700120800.htm.

[664] Πηγή: Διαδίκτυο, ιστοχώρος της online εγκυκλοπαίδειας WikiPedia, http://en.wikipedia.org/wiki/Hacker.

της ασφάλειας (white hats), όσο και στον αντίποδα αυτής (black hats). Δε λείπουν βέβαια και οι περιπτώσεις επαμφοτερίζοντων μελών (grey hats), που προσεταιρίζονται κατά το δοκούν την μια ή την άλλη αντιμαχόμενη πλευρά, σε διαφορετικές συγκυρίες. Μερικά χαρακτηριστικά των κακόβουλων συγγραφών και χρηστών, που ανήκουν στο γκρουπ των χάκερς, είναι *η οξύνοια, η επάρκεια γνώσης του αντικειμένου και μια γενικότερα δογματική και ελιτίστικη άποψη, συμπεριφορά και δράση, με εμμονή στο «λακωνίζειν»*.

Οι κακόβουλοι χάκερς προβάλλουν ως εκείνοι οι *εξειδικευμένοι επαΐοντες* της πληροφορικής και ειδικότερα των θεμάτων που άπτονται του πεδίου της ασφάλειας πληροφοριών, που μπορούν συνήθως για πολύ συγκεκριμένους και σκόπιμους λόγους και κατόπιν επήρειας υπό ισχυρό δέλεαρ (αντάλλαγμα υποκειμενικής σημαντικότητας) να στρατολογηθούν ή να ταχθούν αυτοδικαίως π.χ. για πολιτικούς λόγους (hacktivists) στη μάχη εναντίον των προστατευτικών μηχανισμών των ΠΣ.

Οι χάκερς -όπως και οι κράκερς- *δουλεύουν συνήθως συνεργατικά σε συνασπισμούς* και αγέλες όμοιων συμφερόντων, χωρίς όμως να είναι λίγα τα περιστατικά μοναχικών ή ανεξάρτητων πρακτόρων.

V. «Ρομπέν των Δασών»-«Πειρατές»-Κράκερς[665]

Αυτός ο όρος αναφέρεται γενικά σε ανθρώπους, που παραβιάζουν πνευματικά δικαιώματα, προς όφελος όσων «αρνούνται» να πληρώσουν για κατοχυρωμένη ιδιοκτησία, όπως συμβαίνει συχνά για το λογισμικό και τη μουσική. Επίσης, πολλές φορές προβάλλουν ως *εφάμιλλοι των κακόβουλων χάκερς*, λόγω της εκδηλωμένης τάσης τους να εισβάλλουν παρανόμως σε μη οικεία συστήματα πληροφοριών, για την εξυπηρέτηση των ιδιαίτερων συμφερόντων τους. Η συνδρομή του κακόβουλου λογισμικού στην προώθηση των στόχων των κοινοτήτων κράκερς μπορεί να είναι πραγματικά ουσιώδης.

Οι κράκερς ομοιάζουν με τους χάκερς, όσον αφορά την οργάνωση και τη φιλοσοφία των ατόμων, αλλά και την εκλεκτή στελέχωση των ομάδων τους, διαφέρουν όμως στο σημείο ότι είναι *άμεσα συνδεδεμένοι/στιγματισμένοι με παράνομες δραστηριότητες*, σε αντίθεση με τους κοντινούς -κατά τα άλλα- συγγενείς τους.

---

[665] Πηγή: "Software crackers crave a challenge", Dani Cooper, 2008, διαθέσιμο από το δεσμό http://www.abc.net.au/science/articles/2008/02/21/2166871.htm.

VI. Μικρής ηλικίας και ικανότητας παραβάτες (Newbies, Script kiddies)[666]

Στην κατηγορία αυτή ανήκουν νεαροί -πολύ συχνά ανήλικοι (έφηβοι)- άνθρωποι των οποίων *η μικρή ενασχόληση και η περιέργεια στα θέματα πληροφορικής συνεπικουρούμενες από μια έμφυτη διάθεση για περιπέτεια (τεχνολογική έξαψη)* οδήγησε στην υιοθέτηση παραβατικής συμπεριφοράς. Λόγω της *μικρής συνήθως ηλικίας* τους, πολλές φορές, διαφεύγουν μιας παραδειγματικής τιμωρίας.

Το κυρίαρχο γνώρισμα των ατόμων αυτών είναι η *προσφυγή στη χρήση ή ελαφριά τροποποίηση, ήδη υπαρχόντων και από άλλους κατασκευασθέντων, επιβλαβών προγραμμάτων λόγω μικρής, προσωπικής δεξιοτεχνίας, τεχνογνωσίας και εμπειρίας*. Αποτέλεσμα αυτής της πραγματικότητας είναι να εκτυλίσσεται σχεδόν πάντοτε μια πλημμελώς συντονισμένη και προγραμματισμένη, απροσδιόριστης κατεύθυνσης ή/και αδόκιμου σκοπού, χρήση των κακόβουλων τεχνολογιών που μπορεί να προξενήσει απρόσμενα αποτελέσματα και να έχει αδιευκρίνιστης βαρύτητας συνέπειες.

Η μελέτη και αξιολόγηση των διαφορετικών προφίλ, αλλά και των κινήτρων των συγγραφέων κακόβουλων όπλων, όπως επίσης αντίστοιχα και των δραστών πληροφοριακών επιθέσεων με αυτά, μπορεί και πρέπει να αποτελέσει μιας πρώτης τάξεως αμυντική τακτική, τόσο στα πρότυπα όσων συνιστούσε και ο Sun Tzu όσο και με τη λογική της διαχείρισης κινδύνου. Η εν δυνάμει προκύπτουσα, προληπτική συνέργεια και τα υπόλοιπα, χρήσιμα συμπεράσματα που μπορούν να εξαχθούν από μια ανάλογη δραστηριότητα είναι σημαντικά θεμέλια για τη στήριξη, κατεύθυνση και στοχοθέτηση των συστημάτων προστασίας, αλλά και των λοιπών μηχανισμών ασφάλειας πληροφοριών, που θα θελήσει να υλοποιήσει ο δείνα οργανισμός και η εκάστοτε επιχείρηση, στο πλαίσιο λειτουργίας και δράσης της.

6.3 Συνέπειες-Αντίκτυπος πληροφοριακού πολέμου μέσω αυτοαναπαραγόμενου οπλολογισμικού

Ο αντίκτυπος από τα κακόβουλα όπλα λογισμικού διατρέχει *όλες τις διαστάσεις της ανθρώπινης δραστηριότητας* και οι πιθανές συνέπειες από τα διάφορα περιστατικά πληροφοριακού πολέμου, βασισμένου στα όπλα αυτά, μπορούν να συνταράσσουν συθέμελα

[666] Πηγή: "Script kiddies: The Net's cybergangs", Robert Lemos, 2000, διαθέσιμο από το δεσμό http://news.zdnet.com/2100-9595_22-502632.html?legacy=zdnn.

όλες τις δομές, στις οποίες το είδος μας και ιδίως ο σύγχρονος, τεχνολογικός του πολιτισμός στηρίζεται.

6.3.1 Πολιτικός[667]

Στον πολιτικό αντίκτυπο εντάσσονται δράσεις όπως η (κυβερνο)τρομοκρατία και ο στρατιωτικός, πληροφοριακός πόλεμος. Ακόμα, οι όποιες επιθέσεις σε κυβερνητικούς, στρατιωτικούς, πολυεθνικούς και διεθνείς οργανισμούς για λόγους ιδεολογικού ή πολιτικού προβληματισμού και οι πολύπλευρες επιπτώσεις που αυτές ενδεχομένως έχουν, αποτελούν εκφάνσεις του πώς μπορούν να επηρεάσουν οι πληροφοριακές εχθροπραξίες με χρήση κακόβουλων όπλων τον πολιτικό πυλώνα της ανθρώπινης κοινωνίας. Χαρακτηριστικό γνώρισμα όλων των παρόμοιου είδους απειλών είναι πως η έκθεση σε αυτές συνοδεύεται αρκετές φορές και από την *ύπαρξη ή πρόκληση, ευρύτερου δημοσίου κινδύνου*.

Οι συνέπειες από τέτοια φαινόμενα (μπορεί να) είναι *απρόβλεπτες* και εν δυνάμει (να) *πλήττουν μεγάλα τμήματα του κοινωνικών συνόλων*.

6.3.2 Οικονομικός

Στον οικονομικό στίβο εμφανίζονται *στη μεγαλύτερη πλειοψηφία τους και με τον πλέον ευδιάκριτο τρόπο οι «καρποί» του πληροφοριακού πολέμου με οπλολογισμικό*.[668]

Μεγάλου μήκους απάτες (όπως π.χ. mass dialers, phishing, spamming), εκβιασμοί (για παράδειγμα οι cryptoviral extortion attacks) και υποκλοπές (λ.χ. keylogging, data stealing, monitoring) γίνονται εφικτά ενδεχόμενα χάρη στο κακόβουλο, αυτοαναπαραγόμενο λογισμικό με *δυσμενείς, οικονομικές συνέπειες για τα μεμονωμένα θύματα. Η απώλεια χρόνου και χρήματος* τόσο από την ίδια την προσβολή, όσο και για τη διαδικασία θεραπείας και αποκατάστασης, είναι αρκετά σημαντική και επιβαρυντική οδηγώντας πολλά άτομα δικαίως στην αγανάκτηση ή/και την απόγνωση.

Από την άλλη μεριά, για τις επιχειρήσεις και τους οργανισμούς μια υποβάθμιση του επιπέδου ασφάλειας πληροφοριών μπορεί να σημάνει (άμεση) απώλεια εισοδήματος ή ακόμα χειρότερα, σε περίπτωση ας πούμε που συμβεί διαρροή κρίσιμων πληροφοριών, του ίδιου του στρατηγικού, επιχειρησιακού πλεονεκτήματος, που κατέχουν κόντρα στους όποιους ανταγωνιστές. Για το λόγο αυτό, συνήθως, προβαίνουν στην υλοποίηση κάποιου συστήματος

---

[667] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM].

[668] Πηγή: Διαδίκτυο, ιστοχώρος της εταιρείας λύσεων ασφάλειας Global Secure Systems, http://www.gss.co.uk/news/article/4029/go.

προστασίας για τα ευαίσθητα και μη δεδομένα του οποίου το κόστος μελέτης, αγοράς και εγκατάστασης, μαζί με τα πάγια έξοδα λειτουργίας και συντήρησης, συχνά αθροίζεται σε κάποιο αξιοσέβαστο ποσό. Ο επιχειρησιακός κίνδυνος από τις επιθέσεις είναι όπως εύκολα διαπιστώνει κανείς μεγάλος και η ανάγκη προστασίας από τα κακόβουλα όπλα συνεπάγεται πολλές φορές την αναγκαιότητα για ανάλογες δαπάνες (έμμεση οικονομική επιβάρυνση). Στα έξοδα αυτά περιλαμβάνονται και οι αμοιβές για την απασχόληση και το χρόνο εξειδικευμένου προσωπικού που ως μέρος του συστήματος ασφάλειας μεριμνά για την παρακολούθηση και εφαρμογή των διαδικασιών προστασίας (πρόληψη, διάγνωση, θεραπεία). Συνυπολογίζοντας τα συνολικά έξοδα αρχικής τοποθέτησης και λειτουργίας ενός συστήματος ασφάλειας, την πολύπλευρη, άμεση και παράπλευρη, οικονομική απώλεια ή ζημία σε επιχειρησιακούς πόρους ή στρατηγικούς στόχους από την οιαδήποτε, καταστροφική δράση μιας ιομορφικής κακόβουλης απειλής ή ενός σκουληκιού και το ολικό κόστος αποκατάστασης μιας πληροφοριακής δομής από μια προσβολή/μόλυνση στη φυσιολογική της λειτουργία συμπεραίνει κανείς πως *ο οικονομικός αντίκτυπος των επιθέσεων με κακόβουλα κυβερνοόπλα φανερώνεται με ένα συχνά δυσβάσταχτο φορτίο για τους οργανισμούς*.

Τέλος, σαν μια θετική οικονομική συνέπεια της ευρύτατης χρήσης των αυτοαναπαραγόμενων, κακόβουλων προγραμμάτων στη διενέργεια πληροφοριακής εχθροπραξίας μπορούμε να λογίσουμε την *τόνωση της αγοράς εργασίας* (εξειδικευμένο τεχνικό προσωπικό ασφάλειας, ανάγκες στελέχωσης για τους κατασκευαστές προγραμμάτων προστασίας, πρωτοκόλλων και εφαρμογών/υπηρεσιών, Λ/Σ και υλικού) *και της βιομηχανίας* (επενδύσεις, διαρκής ανάπτυξη, άνθιση κλάδου) *στο χώρο της Ασφάλειας ΠΣ*.[669]

6.3.3 Τεχνολογικός[670]

Ο τεχνολογικός τομέας της ανθρώπινης δραστηριότητας επηρεάζεται καθημερινά από την ύπαρξη κακόβουλων προγραμμάτων και τη συνακόλουθη εκτέλεση πληροφοριακών επιθέσεων και μάλιστα με ιδιαίτερα εμφανή τρόπο.

Ο τεχνολογικός αντίκτυπος μπορεί να είναι *είτε άμεσος είτε έμμεσος*· άμεσος λόγω της επιβάρυνσης, υπονόμευσης ή καταστροφής των τεχνολογικών υποδομών που μια πληροφοριακή εχθροπραξία δύναται να προκαλέσει και έμμεσος λόγω της βαθμιαία αυξανόμενης ανάγκης για περαιτέρω τεχνολογική ανάπτυξη και εξοπλισμό εξαιτίας του αέναου ανταγωνισμού μεταξύ των διαφόρων απειλών και συστημάτων προστασίας.

---

[669] Πηγή: "The Impact of Computer Viruses on Society", Jimming Lin, Chia-Hao Chang, 1989, διαθέσιμο από το δεσμό http://vx.netlux.org/lib/ajl00.html.

[670] Όπως στην προηγούμενη υποσημείωση.

Οι άμεσες συνέπειες αποτελούν το φυσικό επόμενο μιας οιασδήποτε πληροφοριακής εχθροπραξίας μέσω οπλολογισμικού, αφού η κακόβουλη δραστηριότητα σχεδόν πάντα συνιστά ή επισύρει πληθώρα τεχνικών προκλήσεων και προβλημάτων για τους χειριστές και τους χρήστες αυτών.

Ο έμμεσος αντίκτυπος επιφέρει πίεση τόσο στους -νόμιμους ή κακόβουλους- κατασκευαστές και προμηθευτές της πληροφορικής τεχνολογίας (υλικό, λογισμικό, υπηρεσίες κτλ), όσο και στους χρήστες ή αγοραστές αυτής, ώστε να υπάρχει διαρκής εξέλιξη, βελτίωση και αναβάθμιση των παρεχόμενων και χρησιμοποιούμενων συστημάτων και προϊόντων. Τα διάφορα τεχνολογικά επιτεύγματα, των οποίων μάρτυρες γινόμαστε κατά καιρούς, τόσο από την πλευρά των κακόβουλων προγραμμάτων και των μεθόδων τους, όσο και από εκείνη των συστημάτων ασφάλειας των ΠΣ, είναι επακόλουθα της περί ούσας ο λόγος πίεσης.

6.3.4 Κοινωνικός-Πολιτισμικός

Η ευρύτερη συγγραφή και δράση κακόβουλων όπλων έχει επηρεάσει διαφανώς και αδιαφανώς τον σύγχρονο κοινωνικό ιστό διαμορφώνοντας παράλληλα *νέους κανόνες και θεσμούς συμπεριφοράς και συνύπαρξης* και *καινούριες τάσεις κουλτούρας, συνηθειών, πνευματικότητας και ηθικότητας*, στα πλαίσια του ήδη κραταιού, τεχνολογικού πολιτισμού.

Το ελλιπές, όπως διαπιστώσαμε πρωτύτερα στην εργασία, μα συνεχώς διαμορφούμενο, νομικό πλαίσιο, που έρχεται για να παρέχει ασπίδα προστασίας στα ΠΣ του κόσμου από τα κακόβουλα όπλα, τους κατασκευαστές τους και τους δράστες επιθέσεων με αυτά, είναι άμεση απόρροια του κλίματος που επικρατεί από την ευρύτατη χρήση τους.

Από καθαρά κοινωνιολογική σκοπιά, η παρουσία και έντονη διάδοση της χρήσης των κακόβουλων πληροφοριακών όπλων έχει επηρεάσει τη δομή της κοινωνίας. Οι επιπτώσεις από την κακόβουλη δραστηριότητα σιγά-σιγά ξεκίνησαν να αποτυπώνονται στις συνήθειες, το πνευματικό γίγνεσθαι και την ηθική των συστατικών μερών όλων των σύγχρονων κοινωνιών, άλλοτε με πολύ ξεκάθαρο τρόπο και άλλοτε με όχι και τόσο διαφανή μηχανισμό. Νέες, δυναμικές κοινωνικές ομάδες μεγάλης διείσδυσης και ευρείας διαστρωμάτωσης αναδύονται και παίζουν ρόλο πρωταγωνιστή στις πληροφοριακές μάχες. Από τη μια όχθη στέκονται οι δυνάμεις των AV(er)s (εταιρείες ασφάλειας, διαχειριστές ΠΣ, μεγάλοι κατασκευαστές υλικού και λογισμικού), δηλαδή των υπέρμαχων της ασφάλειας Η/Υ και δικτυοκεντρικών ΠΣ, ενώ στην αντίπερα όχθη αντιπαρατάσσονται οι λεγεώνες των VXers (hackers, crackers, script-kiddies κτλ), που σκοπό έχουν να την υποβαθμίσουν και να πραγματοποιήσουν πληροφοριακές εχθροπραξίες.[671] Επίσης, πολλές είναι εκείνες οι τρίτες

[671] Πηγή: "Notes from the virus Underground...", Kim Neely, 1999, διαθέσιμο από το δεσμό http://vx.netlux.org/lib/p0021.html.

οντότητες που με τον ένα ή τον άλλο τρόπο παρεμβαίνουν στη διαμάχη είτε συμμαχώντας με ένα εκ των δύο στρατευμάτων είτε εκμεταλλευόμενες πότε τη δράση της μιας και πότε της άλλης, κατά το δοκούν ή το εκάστοτε συμφέρον τους. Η μάχη είναι σφοδρή και αδιάκοπη και η πόλωση μεγάλη· βέβαια, δε λείπουν και εντός των κόλπων των ομοϊδεατών και συνεργαζόμενων ομάδων οι αψιμαχίες και η διχόνοια, προϊόντα ως επί το πλείστον εσωτερικών συγκρούσεων για την ανάδειξη των πρωτοπόρων και των «στρατηγών» και προσδοκίας-εμμονής για τις όποιες «δάφνες» ή «λάφυρα» συνοδεύουν αυτούς τους τίτλους, χωρίς αυτό να μειώνει δραστικά τη συσπείρωση των μελών, γύρω από την ευρύτερη ομάδα και τους στόχους αυτής. Η κοινωνική αυτή διάσταση του κακόβουλου οπλολογισμικού και των εκδηλώσεων πληροφοριακών επιθέσεων με χρήση του γίνεται ιδιαίτερα εμφανής και χαρακτηριστικά διάχυτη κυρίως μέσω των διαφόρων ηλεκτρονικών χώρων, υπηρεσιών και δικτύων ανθρώπινης επικοινωνίας και συνεργασίας (communication and collaboration sites, services and networks). Στην υπόλοιπη κοινωνική δράση τους, κατά τα άλλα, τα μέλη των 2 διαφορετικών ομάδων και οι θιασώτες τους διαβιούν και (συμπερι)φέρονται, κατά πάσα πιθανότητα, όπως λοιπά φυσιολογικά άτομα και όχι ως έντονες παρεκκλίσεις από τα συνηθισμένα μοτίβα.

Από πλευράς πολιτισμού, σε τελική ανάλυση, η συνεξελικτική πρόοδος κακόβουλων προγραμμάτων και συστημάτων ασφάλειας είχε ως αποτέλεσμα να προικιστεί επιπλέον ο ήδη τεχνολογικά προσανατολισμένος (θαρρεί κανείς ορισμένες φορές και βεβαρημένος) χαρακτήρας του με νέες, πρόσθετες ορολογίες (γλώσσα, σημειολογία, σημασιολογία) και δράσεις (δημιουργήματα, εκφράσεις).[672]

6.4 Πεδία δράσης παγκόσμιας κοινότητας

Έχοντας πια μια καλή εικόνα τόσο της πραγματικότητας και των μεθόδων των κακόβουλων όπλων και της πληροφοριακής εχθροπραξίας που είναι δυνατή μέσω αυτών, όσο και του αντίκτυπου που στην εποχή μας φαίνεται να έχουν φέρει και μπορούν επιπλέον να προκαλέσουν, συνειδητοποιεί κανείς πως *η ώρα έχει προ πολλού έλθει για την κατάστρωση και ενθάρρυνση νέων, γενναίων και ευρύτερων κοινωνικών, πολιτισμικών, τεχνολογικών, οικονομικών και πολιτικών πρωτοβουλιών και δράσεων*, στην κατεύθυνση της αντιμετώπισης αυτής της σύγχρονης και επικίνδυνης απειλής και του περιορισμού των αρνητικών επιδράσεων και συνεπειών της.

---

[672] Επιβεβαίωση της παραπάνω διατύπωσης η ύπαρξη online εγκυκλοπαιδειών των σύγχρονων αυτών νεολογισμών, όπως π.χ. στον άκρως ενδιαφέροντα ιστοχώρο της NetLingo http://www.netlingo.com/inframes.cfm.

Ορισμένες υψηλής προτεραιότητας προσεγγίσεις στο πλαίσιο της ενστέρνισης και περαιτέρω επιφοίτησης επάνω στις αλήθειες της ανωτέρω διαπίστωσης περιλαμβάνουν:

I. Πληροφορική Παιδεία - Εκπαίδευση χρηστών

Ως πρώτο βήμα πρόληψης απέναντι σε οποιαδήποτε από τις δυσάρεστες καταστάσεις, στις οποίες μπορεί να οδηγήσουν η τεταμένη, πληροφοριακή σύγκρουση και η χρήση κακόβουλων όπλων, πρέπει να θεωρείται η *κατάλληλη, πολυσχιδής και εμπεριστατωμένη ενημέρωση-εκπαίδευση των χρηστών* των δικτυοκεντρικών ΠΣ, όσον αφορά τον ορθολογικό και ασφαλή χειρισμό της σύγχρονης, ψηφιακής τεχνολογίας, αλλά και τους ποικίλους, παρελκόμενους κινδύνους που καραδοκούν.[673]

Παράλληλα, ειδική μέριμνα πρέπει να λαμβάνεται, ώστε να αποτρέπεται μέσω *ισχυρής νουθεσίας, εκμάθησης αρετών και αντιστάσεων και έντονης, καθοδήγησης και συμβουλευτικής/παραινετικής δράσης* η διολίσθηση, των νεαρών κυρίως, μελών της κοινωνίας της Γνώσης στα μονοπάτια του κυβερνοεγκλήματος. Ο συνετός δρόμος πρέπει να χαραχτεί από νωρίς, στα πρώτα κιόλας βήματα μύησης των ατόμων στον κόσμο της Πληροφορικής.

II. Χρηματοδότηση-ενίσχυση αντιϊομορφικής έρευνας, μαζί με την έρευνα για ασφαλείς επικοινωνίες και κρατικού τύπου επιδότηση/επιχορήγηση των επιχειρήσεων για την επιτυχή υλοποίηση υποδομών ασφάλειας[674]

Η παροχή κινήτρων και χορηγιών, καθώς και η επιβράβευση των καρποφόρων, ακαδημαϊκών και επιχειρηματικών προσπαθειών, στα πεδία της ασφάλειας πληροφοριών και συστημάτων, πέρα από την ανάδειξη και επιβίωσή τους, αποτελούν αναμφίβολα μακροπρόθεσμους εγγυητές εντατικοποίησης και μεγαλύτερης αποτελεσματικότητάς τους.

Σε ένα παρόμοιας λογικής πλαίσιο, σκόπιμη κρίνεται και η θέσπιση και ενεργοποίηση δράσεων άμεσης κρατικού τύπου ενθάρρυνσης και οικονομικής ενίσχυσης επιχειρήσεων και οργανισμών, κυρίως του δημοσίου (λόγω της ενδεχόμενης μεγαλύτερης κρισιμότητας) αλλά φυσικά και του ιδιωτικού τομέα, για τη μελέτη εφαρμογής και τη σταδιακή ενσωμάτωση ολοκληρωμένων συστημάτων και

---

[673] Πηγή: "Transforming victims into cyber-border guards: education as a defence strategy", Jeannette Jarvis, VB2007 Microsoft, διαθέσιμο από το δεσμό http://www.virusbtn.com/pdf/conference_slides/2007/JeannetteJarvis_slideVB2007.pdf.

[674] Ενδεικτικά αναφέρουμε τις ερευνητικές ζώνες της ασφάλειας (Security) και της τεχνολογίας πληροφορικής και επικοινωνιών (ICT) στο 7ο Ερευνητικό Πρόγραμμα-Πλαίσιο της Ευρωπαϊκής Ένωσης, που κινούνται στη σωστή κατεύθυνση και αποτελούν αντιπροσωπευτικές, αξιόλογες, σχετικές δράσεις/πολιτικές. Περισσότερο στον ιστοχώρο της CORDIS http://cordis.europa.eu/en/home.html.

μηχανισμών προστασίας και ασφάλειας πληροφοριών. Κάτι τέτοιο σίγουρα θα διευκολύνει, τους απρόθυμους ή ανίκανους να ανταπεξέλθουν στο οικονομικό ή άλλο οροβόρο βάρος μιας μακρόπνοης επένδυσης στην ασφάλεια, να εκκινήσουν εκείνες τις δραστηριότητες, που θα βελτιστοποιήσουν εν τέλει μακροπρόθεσμα, στο σύνολο τους, τις υπάρχουσες υποδομές ασφάλειας μιας χώρας, αυξάνοντας έτσι το γενικό δείκτη της πάντοτε επιθυμητής ποιότητας των υπηρεσιών της, αλλά και την αντίστοιχη στάθμη της απαραίτητης, παρεχόμενης προς όλους τους πολίτες, γενικής διαβεβαίωσης ως προς την κοινωνική προστασία και συνοχή, που βλάπτονται ουσιαστικά και ορισμένες φορές σε μεγάλο βαθμό από τις δυνητικές συνέπειες των εκάστοτε, πληροφοριακών συρράξεων.

III. Ποια θεωρείται τελικά ομόφωνα «κρίσιμη πληροφορία», τι αποδεχόμαστε καθολικά ως «ευαίσθητα δεδομένα» και ποιες είναι αποδεκτές, ειδικές περιπτώσεις;[675] Θεμελίωση των σχετικών όρων, ανάλυση και κατηγοριοποίηση δεδομένων, στοιχειοθέτηση/σταχυολόγηση των πιθανών, επίβουλων πηγών, κατάρτιση διαδικασιών αξιολόγησης του κινδύνου, καθορισμός των επιπέδων μυστικότητας και δράση για την εξασφάλισή συνθηκών μέγιστης προστασίας, με έμφαση στη νομοθετική υποστήριξη και επιβολή τους, σε καθεμιά από τις παρακάτω περιοχές ενδιαφέροντος:

- **a.** Προσωπική σφαίρα.
- **b.** Οικονομική-επιχειρηματική σφαίρα.
- **c.** Επιστημονική σφαίρα.
- **d.** Κρατική/Κυβερνητική σφαίρα.

Στόχος είναι **να αποσαφηνιστεί η ιδιαίτερη υφή των όσων τελικά, πραγματικά διακυβεύονται** και να προωθηθούν έτσι, ολικά πιο προσηλωμένες και αποδοτικές, πολιτικές ασφάλειας.

IV. Περιφρούρηση δικτύωσης, ηλεκτρονικής επικοινωνίας, συνεργασίας και διαμοίρασης "αγαθών"

Το χαρακτηριστικό αυτό προνόμιο προβάλλει ανέκαθεν ως *πανανθρώπινο αίτημα-δικαίωμα, αλλά και ως ξεχωριστή ανάγκη του καθενός μας*[676]. Εκτός αυτού, πάνω στο προνόμιο τούτο ακριβώς, βασίζεται χρόνια τώρα κάθε έννοια ανεπτυγμένης, πολιτισμένης κοινωνίας και εύρωστης, ανθηρής οικονομίας· το ίδιο ισχύει και για τα ψηφιακά έκδοχά τους.

---

[675] Πηγή: "Practices for Protecting Information Resources Assets", Department of Information Resources, State of Texas, Austin, 2003, διαθέσιμο από το δεσμό http://burrowowl.dir.state.tx.us/IRAPC/practices/word/02.doc.

[676] «Ο άνθρωπος είναι από τη φύση του κοινωνικό ον», «Πολιτικά Βιβλίο Γ», Αριστοτέλης, μεταξύ 340-330 π.Χ.

V. Διάλογος κυβερνήσεων και οργανώσεων πολιτών για την ορθολογική χρήση των τηλεπι-κοινωνιών με ξεκάθαρους στόχους:

a. Επαναδιακήρυξη - πολιτική συμφωνία στο "απόρρητο" και το "ελεύθερο" των πληροφορικών επικοινωνιών, με γνώμονα τα ανθρώπινα δικαιώματα ως ολότητα, ατομικά και κοινωνικά.[677]

Ο κρατικός μηχανισμός θα πρέπει να διαφυλάττει την νομοτέλεια των συστημάτων από τις κυβερνοαπειλές, επεμβαίνοντας μόνο με σαφή, προδεδηλωμένο και προσυμφωνημένο, διερευνητικό/κατασταλτικό τρόπο στην ελεύθερη, πληροφοριακή συναλλαγή και διακίνηση και πάντοτε με σεβασμό στα θεμελιώδη, ανθρώπινα δικαιώματα και νομικά κεκτημένα. Από την άλλη, όμως, ο κάθε σύγχρονος πολίτης οφείλει να μην συγχέει την αδιαφιλονίκητη, ψηφιακή ελευθερία και ιδιωτικότητά του με ασύδοτη, ανεξέλεγκτη αναρχία και να αναγνωρίζει την εκχωρημένη εξουσία αιρετών, αρμόδιων, διακυβερνητικών οργάνων και πολιτειακών ομάδων να παρεμβαίνουν ρυθμιστικά, συντονιστικά και κατευναστικά, με αφετηρία και προορισμό το κοινό καλό του κοινωνικού συνόλου.

b. Αποφυγή «Οργουελιανών» σεναρίων-κοινωνιών[678] ή ψυχροπολεμικών τελμάτων, εξαιτίας της διάχυτης αναστάτωσης και του αισθήματος τρομολαγνείας-τρομοκρατίας, που μπορεί εύκολα να διαδώσουν οι τρέχουσες και «προφητευόμενες», παγκόσμιες εκφάνσεις του πληροφοριακού πολέμου.

VI. Ευρύτερη, στρατηγική συνεργασία και συνεννόηση όλων των συμμέτοχων στην ασφάλεια πληροφοριών[679], κατασκευαστών υλικού και λογισμικού, εξειδικευμένων εργατών και ειδικών ασφάλειας (ή/και καλοπροαίρετων χάκερ), κυβερνήσεων, οργανισμών διασφάλισης ανθρωπίνων δικαιωμάτων, σε όλα τα παραπάνω άκρως σημαντικά θέματα με το βλέμμα στραμμένο στην αντιμετώπιση των μελλοντικών όπλων πληροφοριακής καταστροφής και των πιθανών επιπλοκών που θα δημιουργήσουν, επιλέγοντας ως στάση:

a. Ανοιχτά "χαρτιά", πρακτικές ή και κώδικας, όταν είναι εφικτό.

b. Επικοινώνηση-τεκμηρίωση γνώσης και μεθόδων στο βαθμό του επιτρεπτού από το ανταγωνιστικό πλεονέκτημα.

VII. Συνοπτικά προβάλλονται, λοιπόν, ως οι **πλέον φλέγουσες επιταγές των καιρών** οι ακόλουθες:

---

[677] Πηγή: "Balancing Privacy and Security", Wall Street Journal, 2006, διαθέσιμο από το δεσμό http://online.wsj.com/public/article/SB114770347659052946-r55Jg7SFeKsLXThBxp6GoNZrhGQ_20060614.html.

[678] "Animal Farm", George Orwell, 1945.

[679] Κύρια, βιβλιογραφική αναφορά: [OZEREN-GRCCMICVA].

a. Ολομέτωπη *σύγκρουση με τα οργανωμένα δίκτυα (πληροφορικής) τρομοκρατίας (cyberterrorism)* που δρουν στον κυβερνοχώρο και απειλούν με τις πράξεις ή εκπεφρασμένες επιθυμίες τους την παγκόσμια σταθερότητα και τη διεθνή ασφάλεια, υπονομεύοντας τις καλές σχέσεις των χωρών και εξωθώντας τες στα όρια των συγκινησιακών αντοχών τους.

b. Έμμετρος *περιορισμός της υπερβολικής, κρατικής παρακολούθησης*, εφόσον αυτή υφίσταται και εκδηλώνεται με τρόπο ανεξέλεγκτο και αδικαιολόγητο από τα όποια συμβάντα ή με τρόπο που συνιστά απροκάλυπτη παραβίαση της ιδιωτικότητας του ατόμου.

c. *Αντιμετώπιση/Καταπολέμηση* της έντονης και τόσο νοσογόνας, *βιομηχανικής κατασκοπείας*, με στόχο τη διασφάλιση της επιχειρηματικότητας και των επαγγελματικών μυστικών και την υπεράσπιση των κατοχυρωμένων, πνευματικών κόπων μιας ερευνητικής δραστηριότητας.[680]

d. *Προστασία των καταναλωτών* από τις διάφορες, δικτυοκεντρικές, *οικονομικού τύπου απάτες* των επιτήδειων.

e. Διασφάλιση της *ακεραιότητας και εμπιστευτικότητας των ουσιωδών, κυβερνητικών απορρήτων* και προφύλαξη των πολιτών από τους κινδύνους έκθεσης σε «ευαίσθητες», απόκρυφες ή παράνομες πληροφορίες.

Η παγκόσμια κοινότητα πρέπει να εργαστεί συλλογικά και με αποφασιστικότητα για τη μεγαλύτερη δυνατή ικανοποίησή τους.

VIII. Νομικό πλαίσιο – Ηθοπλαστική

Τέλος, δεν πρέπει να αμελήσει ποτέ κανείς την ξεκάθαρη ανάγκη για κατάστρωση *αντικειμενικών, θεσμικών δικλείδων ασφάλειας* σε διεθνές, αλλά και ενδοκρατικό επίπεδο.[681] Η ανεπάρκεια ή/και αναποτελεσματικότητα των υπαρκτών μέτρων και κανόνων έχει οδηγήσει στη δυσοίωνη κατάσταση της επί του παρόντος έξαρσης των πληροφοριακών συρράξεων και εγκλημάτων. Η παρουσία πιο σφιχτών, αυστηρών και ολοκληρωμένων θεσπισμάτων είναι σίγουρο πως θα περιορίσει κάπως την κακόβουλη δραστηριότητα και θα ενισχύσει εμφανώς το αίσθημα της ασφάλειας.

---

[680] Πηγή: "Economic and Industrial Espionage: a Threat to Corporate America", Wanja Eric Naef, Infocon 2003, διαθέσιμο από το δεσμό http://www.iwar.org.uk/infocon/economic-espionage.htm.

[681] Πηγή: "Cybercrime laws aren't working, says minister", Tom Espiner, 2005, διαθέσιμο από το δεσμό http://news.zdnet.co.uk/security/0,1000000189,39234106,00.htm.

Ως παράλληλη δράση, επίσης, αποκτά ενδιαφέρον και ξεχωριστή σημασία, σήμερα, η κατάλληλη διάπλαση της κοινωνικής ηθικής[682], μέσω της διασποράς ενός κοινού συναισθήματος, ενός *ιδεώδους πληροφοριακής ορθοπραξίας* (ορθόδοξης ή ορθολογιστικής χρήσης) και μιας συνεπίγνωσης της διαφοράς και των συνεπειών της επιλογής μεταξύ καλοπροαίρετου-επωφελούς και επιβλαβούς τρόπου χρήσης της τεχνολογίας, που μπορεί και πρέπει να καλλιεργηθεί εκτενώς, προκειμένου να εμποδίσει την ραγδαία, κοινωνική διείσδυση του κακόβουλου, πληροφοριακού πολεμιστή, να προκαλέσει μια, σε βάθος χρόνου, μερική απομυθοποίηση του προτύπου του και να επιτρέψει στο σύγχρονο, ψηφιακό πολιτισμό να ευελπιστεί σε πιο ειρηνικές και πλέον ασφαλείς ημέρες παραγωγής, φύλαξης και ανταλλαγής-διάδοσης της γνώσης.

Σχήμα 39: Η ασφάλεια των ΠΣ είναι τελικά «υπόθεση όλων μας»

[682] Στα πρότυπα της εξαιρετικής πρωτοβουλίας CyberEthics του ιστοχώρου Cybercrime.gov, http://www.usdoj.gov/criminal/cybercrime/cyberethics.htm.

7 *Επίλογος*

Κλείνοντας το παρόν έργο προβαίνουμε σε μια σύντομη ανασκόπηση των πεπραγμένων και καταλήγουμε σε μια αποτίμηση των εξαγόμενων συμπερασμάτων. Δε θα μπορούσε, τέλος, παρά να είναι παράλειψη η μη απόδοση των προσωπικών μου ευχαριστιών σε όλα εκείνα τα άτομα, που συνέβαλλαν με το δικό τους τρόπο στην πετυχημένη ολοκλήρωση και αποπεράτωση αυτής της εργασίας.

7.1 Σύνοψη έρευνας

Η διπλωματική αυτή κινήθηκε επιμελώς μεταξύ δύο αντίρροπων και πολλαπλώς τεμνόμενων αξόνων, που αφορούν το εξαιρετικά ευαίσθητο θέμα της πληροφοριακής εχθροπραξίας, η οποία προκαλεί ποικίλους κλυδωνισμούς στην ισορροπία και την τάξη του ευμετάβλητου «χάρτη» της παγκόσμιας, ανθρώπινης συναλλαγής και επικοινωνίας:

- Αφενός μεν, αποσκοπεί στην *ανάδειξη του μείζονος και πολυσήμαντου ρόλου που έχει αποκτήσει το κακόβουλο, αυτοαναπαραγόμενο λογισμικό στη διάδοση, ένταση και έκβαση των σύγχρονων πληροφοριακών συρράξεων και διαμαχών*. Για το λόγο αυτό περιγράφεται ένα μίγμα παραδοσιακών, αλλά και πιο πρόσφατων και ανανεωτικών, χαρακτηριστικών ιδιοτήτων και μεθόδων των προγραμμάτων αυτών, που τα έχει καταστήσει ιδανικά όπλα του πληροφοριακού πολέμου και τόσο πετυχημένες απειλές. Στη βάση αυτού του συνόλου μάλιστα και με κεντρικό γνώμονα την μεγαλύτερη επιτυχία στην εκπλήρωση των εκάστοτε σκοπών της επιτιθέμενης οντότητας, ταξινομήθηκαν τα ποικίλα είδη από αυτό το οπλοστάσιο λογισμικού σε μια πρότυπη απόπειρα κατηγοριοποίησης σε ευκρινώς ορισμένους, διαφορετικούς

(σε πολυπλοκότητα, εμβέλεια και στοχοθέτηση) τύπους όπλων, με παράλληλη απομόνωση των ιδιαιτέρως ξεχωριστών γνωρισμάτων και αποτύπωση της αποτελεσματικότητας του κάθε διακριτού τύπου.[683]

- Αφετέρου δε, *παρουσιάζει και αποτιμά την υπερασπιστική δυναμική του αντίπαλου δέους στη μορφή επίκαιρων, αλλά και πλέον νεωτεριστικών μέτρων, μηχανισμών και συστημάτων ασφάλειας και προστασίας των ΠΣ*, που επιδιώκουν την αναχαίτιση των εχθρικών πυρών και επιχειρήσεων κατά της πληροφοριακής -ατομικής ή ομαδικής- περιουσίας/ιδιοκτησίας. Μεταξύ άλλων προσεγγίζονται θέματα υλικοτεχνικής, λογισμικής, διαδικαστικής-διαχειριστικής και νομικής υφής που άπτονται αυτής της γενικότερης αμυντικής δραστηριότητας, στη φιλοσοφία του τρίπτυχου πρόληψη-διάγνωση-θεραπεία.[684]

Η διττή αυτή ανάπτυξη καταλήγει αρμονικά στην επισήμανση και ψηλάφηση του υπαρκτού ουσιαστικού κινδύνου, των παραφυάδων του και των εν δυνάμει φορέων αυτού και τελικά φιλοδοξεί να φέρει την ψηφιακή κοινωνία των «δικτυωμένων» πολιτών (netizens) προ των ευθυνών της επιθυμώντας τη μαζικότερη επίγνωση και ευαισθητοποίηση και εφιστώντας μέγιστη επαγρύπνηση και εντονότερη, πιο συλλογική προσπάθεια αντίστασης-θωράκισης στα σημεία των καιρών.[685]

Συνολικά, εξάγονται αρκετά χρήσιμα συμπεράσματα, που παρατίθενται και σχολιάζονται στο αμέσως παρακάτω εδάφιο.

7.2 Συμπεράσματα

Ανάμεσα στα περισσότερο *ασφαλή και γόνιμα πορίσματα* της προκείμενης εργασίας προβάλλουν άμεσα ως πλέον εξέχοντα και αξιοσημείωτα τα ακόλουθα:

I. Η σύγχρονη κοινωνία της γνώσης και της πολύ χρήσιμης, μα υπερβολικής συχνά, εναπόθεσης ζωτικής σημασίας λειτουργιών στην ψηφιακή τεχνολογία και τα ΠΣ μαστίζεται από *σοβαρά και ολοένα κλιμακούμενα, θερμά επεισόδια στα πλαίσια του πληροφοριακού ανταγωνισμού*. Η διαρκής αυτή διαπάλη εγκυμονεί *επικίνδυνες*

[683] Τα θέματα αυτά παρουσιάστηκαν στα Κεφάλαια 3 και 5 της εργασίας.

[684] Τα εν λόγω σημεία υπήρξαν αντικείμενο των Κεφαλαίων 4 και 5.

[685] Παρομοίως, πρόκειται για το υλικό του Κεφαλαίου 6.

περιπτύξεις, με ευρύτατο αντίκτυπο[686] σε όλους σχεδόν τους τομείς της ανθρώπινης δραστηριότητας.

II. Το *αυτοαναπαραγόμενο, κακόβουλο λογισμικό* αποτελεί ένα πρώτης τάξεως *πολυεργαλείο/οπλικό σύστημα*, στα χέρια επίδοξων και επιτήδειων πληροφοριακών μονομάχων, με *πληθώρα δυνατοτήτων και επωφελών (sic) ιδιοτήτων*[687], για την αποτελεσματικότερη εξυπηρέτηση των ξεχωριστών στόχων μιας επίθεσης.

III. *Το εκάστοτε μέτρο της ασφάλειας πληροφοριών είναι μια περίπλοκη συνάρτηση* των παραγόντων εκείνων, που διαμορφώνουν το συμπαγές, δομικό σχήμα Υλικό-Λογισμικό-Διαδικασίες-Δεδομένα-Άνθρωπος[688], που καθορίζει και διέπει την οργάνωση και λειτουργία του κάθε ΠΣ. Οποιοσδήποτε, αδύναμος κρίκος στην παραπάνω αλυσίδα αποτελεί ευπάθεια του συνολικού συστήματος και είναι σχεδόν βέβαιο πως επιφέρει μικρή ή μεγάλη πιθανότητα εκδήλωσης επιθέσεων. Η κρισιμότητα των δεδομένων και ο ιδιαίτερος χαρακτήρας των ευπαθειών (πλήθος, ποιότητα) και των περιβαλλοντικών συνθηκών καθορίζουν με δυναμικό τρόπο τις διαφαινόμενες απειλές, τις εφαρμοζόμενες, κατάλληλες πρακτικές, αλλά και το ρίσκο-κόστος που πρέπει να είναι διατεθειμένοι να αναλάβουν οι ενδιαφερόμενοι οργανισμοί και οντότητες, είτε ως πορθητές είτε ως προστάτες.

IV. Οι διάφορες επιθετικές και αμυντικές τεχνολογίες και τεχνοτροπίες[689] βρίσκονται εδώ και χρόνια σε μια *διαδικασία αδιάκοπης συνεξέλιξης και αλληλοτροφοδότησης*. Όπως στους περισσότερους τεχνολογικά πλαισιωμένους χώρους δράσης που φέρουν αντίθετα κινούμενες, αλληλοσυγκρουόμενες απόψεις και δυνάμεις, έτσι και στο ζήτημα της ασφάλειας πληροφοριών και συστημάτων, σχεδόν κάθε, σχετικό επίτευγμα της ανθρώπινης διανόησης και «καλλιτεχνίας» μπορεί να γίνει εν δυνάμει όπλο στα χέρια και των 2 αντιπαλόμενων ρευμάτων και των υποστηρικτών/μαχητών τους, χωρίς κάποια ουσιώδη διάκριση, και να χρησιμοποιηθεί είτε καλοπροαίρετα είτε με κακόβουλη διάθεση[690]. Οι εξελίξεις

---

[686] Βλέπε χαρακτηριστικά το εδάφιο 6.3.

[687] Το κεφάλαιο 3 είναι καθ' ολοκληρία αφιερωμένο στην παρουσίαση και το σχολιασμό τους.

[688] Η τεκμηρίωση αυτή έχει πραγματοποιηθεί ήδη από το Κεφάλαιο 2, στο σχετικό με τα ΠΣ εδάφιο και τους εκεί ορισμούς.

[689] Σαν και αυτές που αναλύθηκαν στα Κεφάλαια 3 και 4.

[690] Το στοιχείο της ουδετερότητας των τεχνολογικών εφευρέσεων και μεθόδων το εντοπίζουμε σε πολλές εκφάνσεις συστημάτων που προκρίνονται άλλοτε ως λύσεις προστασίας και άλλοτε ως μηχανισμοί επίθεσης, ενώ στην ουσία αποτελούν ταυτόσημες ή παραπλήσιας λογικής προσεγγίσεις ή διαφορετικές όψεις του ίδιου πάντοτε, όμως, νομίσματος. Για παράδειγμα αναφέρουμε τις στεγανογραφικές τεχνοτροπίες, την καλοπροαίρετη ή κακόβουλη εισαγωγή κώδικα στους πυρήνες των Λ/Σ, τη διττή φύση/υπόσχεση της εικονικοποίησης, μα ως τρανότερη όλων διακρίνουμε ακόμη την κρυπτογραφία, που προβάλλει ως το «υλικό» προστασίας-επίδοσης και στους 2 διαφορετικούς ρόλους και σκοπούς των πληροφοριακών πολεμιστών (άμυνα&επίθεση).

στον ένα τομέα επηρεάζουν ουσιαστικά την ισορροπία δυνάμεων και πυροδοτούν έτσι, αναπόφευκτα, αντιδραστικές, αντίστοιχες αποκρίσεις εκ μέρους του άλλου[691]. Η αέναη πρόοδος και η καινοτομική έξαρση του τεχνικού μας πολιτισμού συντείνει σε ένα συνεχώς μεταβαλλόμενο πεδίο μάχης και εγγυάται προς το παρόν τη διαιώνιση αυτής της σχέσης μεταξύ των 2 αντιμαχόμενων στρατών[692], που δ*εν έχει κατατείνει ποτέ έως τώρα σε ξεκάθαρο, μόνιμο νικητή, παρά μόνο σε εφήμερες επιτυχίες ή κάποια, αξιόλογα ορόσημα εκατέρωθεν*. Παρόλα αυτά, νέες και πρωτοποριακές θεωρήσεις και κατασκευές και στους 2 χώρους, με συχνά αδιαφιλονίκητη όπως είδαμε δυναμική[693], υπόσχονται να γείρουν την πλάστιγγα περισσότερο προς τη μια ή την άλλη πλευρά. Το παρελθόν, όμως, και οι *ισχυρές εξαρτήσεις από τις, επαμφοτερίζοντος -όπως συχνά αποδεικνύεται- χαρακτήρα, τεχνολογικές εξάψεις*, μάλλον, επιβάλλουν *δίκαια κάποιον σκεπτικισμό επ' αυτών των ενδεχομένων και κάποιες επιφυλάξεις* για τα όσα σπουδαία προοικονομούνται από διάφορες «Κασσάνδρες» ή υπεραισιόδοξους, ένθεν κακείθεν. Στο ίδιο αυτό επίκαιρο συμπέρασμα αυτό καταλήγουν πολλοί, σύγχρονοι ερευνητές[694].

V. Ο συνδυασμός των 2 παραπάνω οδηγεί στην υιοθέτηση της άποψης πως *στην ασφάλεια πληροφοριών τα πράγματα είναι ρευστά και δεν πρέπει επ' ουδενί να θεωρούνται εξασφαλισμένα επ' αόριστον τα όποια, πρόσκαιρα κεκτημένα και εχέγγυα, από πλευράς προστασίας των ΠΣ*. Οι ξαφνικές αλλαγές και η ποικιλία των συνισταμένων δυνάμεων γεννούν πιθανές ανατροπές και αποτρέπουν την ομαλή εδραίωση μιας καθεστηκυΐας ασφάλειας και ενός υψηλού δείκτη διαβεβαίωσης. Μόνο μέσω μιας *προτυποποιημένης, διαδικασιοστρεφούς προσέγγισης*[695], που να προβλέπει αδιάλειπτη εκτέλεση και τακτική αναθεώρηση ευέλικτων και εξελίξιμων κανόνων, μηχανισμών και διεργασιών προστασίας, μπορεί κανείς να ευελπιστεί σε ελαχιστοποίηση των ευπαθειών και άρα των απειλών και μεγαλύτερη αντοχή σε επιθέσεις, προσδοκώντας έτσι υψηλή απόδοση στις όποιες, αναγκαίες υπηρεσίες ασφάλειας και μικρότερο, συνολικό, επιχειρησιακό κίνδυνο. Η *επένδυση σε μια καλά σχεδιασμένη και τεκμηριωμένη, ευπροσάρμοστη και κλιμακώσιμη διαδικασία ασφάλειας* των πληροφοριών όσον αφορά τους πόρους (χρόνος, κεφάλαια και

---

[691] Για παράδειγμα αναφέρουμε τα εξής εξελικτικά πολύπολα: Α)πολυμορφισμός->εξομοίωση->αντιεξομοίωση, Β)επίπεδο-χρήστη->σάρωση->επίπεδο πυρήνα->εικονικοποίηση->υπονόμευση hypervizors->επιβεβαίωση, Γ)πρώιμος αντιϊομορφισμός->ρετροϊομορφισμός->θωράκιση και έλεγχοι ακεραιότητας των προγραμμάτων προστασίας κ.ό.κ. Τέτοια πολύπολα παράλληλης, αλυσιδωτής αντίδρασης μεταξύ των 2 αντίθετων χώρων σκέψης και δραστηριότητας, αν ψάξει κανείς, θα βρει άφθονα.

[692] Κύρια, βιβλιογραφική αναφορά: [BAILEY-DADA].

[693] Οι περιπτώσεις του πέμπτου κεφαλαίου.

[694] Κύρια, βιβλιογραφική αναφορά: [AYCOCK-CVM], [RUTKOWSKA-RSbDM].

[695] Όπως αυτή συζητήθηκε στο εδάφιο 4.8.

ανθρώπινο δυναμικό) μπορεί να μοιάζει μεγάλο βάρος και να εισάγει πρόσθετο ρίσκο, όμως, η σχετική ανταπόδοση, λαμβάνοντας υπόψη την αβεβαιότητα και τις διαρκείς προκλήσεις του μόνιμα μεταβλητού περιβάλλοντος και τον όποιο, πιθανό, αρνητικό αντίκτυπο από μια ενδεχόμενη, επιτυχημένη επίθεση-υποβάθμιση, διαφαίνεται εξίσου μη ευκαταφρόνητη.

VI. Παρατηρείται, δυστυχώς, *σημαντική έλλειψη ισχυρού, νομικού πλαισίου καθώς και ελεγκτικών μηχανισμών*, σχετικά με την κυβερνοασφάλεια, με το συντονισμό των θεσμικά αποτρεπτικών ενεργειών, σε παγκόσμιο επίπεδο, να φαντάζει εξαιρετικά δύσκολη υπόθεση.[696] Το γεγονός αυτό σε συνδυασμό με τη μεγάλη, γεωγραφική διείσδυση, διάχυση και αλληλεπίδραση του Διαδικτύου και των δικτυοκεντρικών ΠΣ, καθώς και με την κρισιμότητα πολλών εκ των περιεχόμενων και διακινούμενων πληροφοριών αποτελούν καταλύτες για την έξαρση του η-εγκλήματος, ιδιαίτερα σε χώρες με «χαλαρές», νομικές δικλείδες, μετατρέποντας τες έτσι σε «επί γης παράδεισο» για τους συγγραφείς κακόβουλων προγραμμάτων, τους δράστες πληροφοριακών επιθέσεων και τους υπόλοιπους κυβερνοκακοποιούς. Τα φαινόμενα συνηγορούν υπέρ της ανάγκης για γρήγορη αλλαγή αυτής της δυσάρεστης κατάστασης και οι απανταχού υπεύθυνοι οφείλουν να το αντιληφθούν και να κινηθούν πιο γοργά, ώστε λίαν συντόμως τα ανάλογα, διαχειριστικά νομοθετήματα να γίνουν από καθοδόν θεωρία πράξη.

VII. Οι άνθρωποι και οι ομάδες, που καταφεύγουν στη συγγραφή ή/και χρήση κακόβουλων όπλων λογισμικού, δεν είναι ξένοι, αλλά ισότιμα μέλη, ενεργοί «παίκτες» και εταίροι, της παγκόσμιας, ψηφιακής κοινοπολιτείας. «Ζουν παντού ανάμεσά μας και όχι στο υπερπέραν» και θα μπορούσαν κάλλιστα να ταιριάζουν σαν ιδιοσυγκρασία και προφίλ[697] σε εμάς τους ιδίους ή σε κάποιον κατά τα άλλα γνωστό, συνεργάτη, φίλο ή συγγενή μας. Τα κίνητρα και οι επιδιώξεις τους από την πληροφοριακή εχθροπραξία έχουν καθαρά ανθρώπινη πηγή και εξήγηση και τις περισσότερες φορές εμφανίζουν μια κάποια, λογική συνέπεια (παιχνίδι-πειραματισμός-έρευνα, οικονομικό κέρδος, πολιτική δήλωση), παρά το κατακριτέο τα πράξης. Η *παροχή αντικινήτρων* για την αποφυγή επιζήμιων, τέτοιων παρεκκλίσεων, αλλά και την απομάκρυνση από σχετικές, νοσογόνες συμπεριφορές, είναι υπόθεση και ευθύνη όλων στα πλαίσια μιας «υγιούς», πληροφοριακής εκπαίδευσης. Η *κατάλληλη ρύθμιση προϋποθέσεων, ορίων ανοχής και ποινών σωφρονισμού* στα πλαίσια της θεσμοθέτησης κανονιστικών κωδίκων και μέτρων

[696] Όπως επισημάνθηκε στο εδάφιο 5.3.

[697] Με βάση τα εδάφια 6.1 και 6.2.

είναι απαραίτητη για τη *συγκρότηση μιας ευνομούμενης και εύρυθμης, αποτρεπτικής, κοινωνικής «ομπρέλας προστασίας»*.

VIII. Εν είδει Υστερόγραφου: Τα αυτοαναπαραγόμενα όπλα «είναι εδώ για να μείνουν», δυνατότερα, εξελιξιμότερα και προσαρμοστικότερα από ποτέ, με εμφανή διάθεση να πρωταγωνιστήσουν σε νέας γενιάς και ευρείας κλίμακας πληροφοριακές συρράξεις και να εξυπηρετήσουν πάσης φύσεως και αντίκτυπου, κακόβουλα εγχειρήματα. Από την άλλη, οι απανταχού φρουροί της ασφάλειας δεν «κάθονται με σταυρωμένα τα χέρια», αλλά διαρκώς προσπαθούν να εφευρίσκουν και να «εξοπλίζονται» με νέα, τεχνικής, διαδικαστικής και νομικής φύσεως, ευφυέστερα και αποδοτικότερα συστήματα προστασίας, για να αντέξουν τη σφοδρότητα των τρεχουσών και επικείμενων μαχών. Κανείς, λοιπόν, δεν μπορεί να «διαβάσει» και να προβλέψει το μέλλον με απόλυτη βεβαιότητα…

Τελικά, η διαπίστωση της τρέχουσας πραγματικότητας αναγκάζει σε παραδοχή της κρισιμότητας του ζητήματος της πληροφοριακής εχθροπραξίας μέσω κακόβουλων, αυτοαναπαραγόμενων προγραμμάτων. Το οπλολογισμικό δεν είναι μια μονοσήμαντη απειλή για την ασφάλεια και τη σταθερότητα στους χώρους της συλλογής, επεξεργασίας και ανταλλαγής πληροφοριών, αλλά μπορεί να τις εκθέσει ποικιλοτρόπως. Ακόμη, ως γνήσιο γέννημα της τεχνολογίας δεν παύει ποτέ να αναπτύσσεται, ενώ μέχρι τώρα διακρίνεται για τη μεγάλη ικανότητά του να συμπορεύεται με τα εκάστοτε, νέα επιτεύγματα της ανθρώπινης, ευρυδιάστατης πολυμηχανίας και τις επιταγές/ευκαιρίες, που αυτά κομίζουν. Η αντιμετώπιση, λοιπόν, του όλου προβλήματος δεν έγκειται αποκλειστικά σε μια στείρα εφαρμογή κανόνων και μέτρων προστασίας, αλλά στη διαρκή βελτίωση και αναπροσαρμογή αυτών στις εκάστοτε νέες συνθήκες και προκλήσεις του ταχέως εξελισσόμενου περιβάλλοντος.

"Πάντες ἄνθρωποι τοῦ εἰδέναι ὀρέγονται φύσει"[698], ανέκαθεν, πόσο μάλλον στην εποχή της Πληροφορίας, όμως, ο δαρβινικού τύπου, σκληρός και ανελέητος ανταγωνισμός, που κορυφώνεται, σήμερα, στην ύπατη μορφή του ως πληροφοριακή εχθροπραξία (με πολύ χρήσιμη τη συμμετοχή και αποδεδειγμένη τη δραστική, «θετική» συνέργεια/συναυτουργία των επιβλαβών όπλων λογισμικού) έφτασε η ώρα να τεθεί υπό κάποιον, μερικό έστω, έλεγχο και αυτό είναι η πρόκληση και το ξεχωριστό στοίχημα των καιρών μας. Πλέον, περισσότερο από ποτέ, επιβάλλεται συνδυασμένη, συλλογική, ενωτική, συντονισμένη δράση μεταξύ όλων των εμπλεκόμενων και επηρεαζόμενων οντοτήτων στο χώρο της υπεράσπισης της ασφάλειας των δικτυοκεντρικών ΠΣ και των ευαίσθητων-κρίσιμων δεδομένων αυτών, προκειμένου να

[698] «*Όλοι οι άνθρωποι από τη φύση τους επιθυμούν την γνώση*», Αριστοτέλης, «Μεταφυσικά - Βιβλίο Α», μεταξύ 340-330 π.Χ.

εντοπιστούν και υλοποιηθούν ρεαλιστικές πολιτικές[699] καταστολής της επιθετικής δραστηριότητας και περιορισμού των κινδύνων που ελλοχεύουν από τις μαινόμενες αψιμαχίες.

7.3 Ευχαριστίες

Στο σημείο αυτό και με την ευκαιρία της ολοκλήρωσης της εργασίας θα ήθελα να χαιρετήσω με όλη μου την καρδιά τη μητέρα μου **Κα Γιαννίκη Χρυσούλα**, καθώς και τη σύντροφό μου **Δίδα Διακοπούλου Κυριακή**, τις οποίες ευγνωμονώ για την αμέριστη υπομονή και έμπρακτη συμπαράστασή τους, όλο το διάστημα της επίπονης -για όλους μας- αυτής περιόδου.

Ακόμη, θα ήθελα να ευχαριστήσω ιδιαιτέρως θερμά τον Καθηγητή του Πανεπιστημίου Πειραιώς **Κο Κάτσικα Σωκράτη**, διακεκριμένου ειδήμονα/επιστήμονα στο χώρο της Ασφάλειας Πληροφοριακών Συστημάτων και Δικτύων Η/Υ, για την αγαστή μας συνεργασία και για το γεγονός πως ως επιβλέποντας της παρούσας διπλωματικής συνέβαλλε τα μέγιστα στην επιτυχή αποπεράτωσή της, με καταλλήλως στοχευμένη, πολύπλευρη και πολύτιμη συμβουλευτική, υποστηρικτική και εποικοδομητική δράση, καθ' όλη τη διάρκεια του έργου.

Τέλος, δε θα μπορούσα να παραλείψω να σταθώ στη θετική συνεισφορά του εργασιακού μου περιβάλλοντος και των συνεργατών μου στην **εταιρεία ΜΟΔ αε**, που με το διακριτικό πάντα τρόπο τους και με συναδελφικό πνεύμα προσέθεσαν αρκετά «λιθαράκια» στην από μέρους μου δύσκολη προσπάθεια οικοδόμησης, εξομαλύνοντας ποικιλοτρόπως πολλαπλά κωλύματα και επιτρέποντάς μου να αξιοποιώ στο έπακρο το διαθέσιμο χρόνο μου για να ανταποκριθώ και στη φοιτητική μου ιδιότητα και τις απορρέουσες από αυτήν απαιτήσεις.

[699] Ενδεικτικά σαν κι αυτές στο επιμύθιο του έκτου κεφαλαίου (εδάφιο 6.4).

8 *Κύρια Βιβλιογραφία*

Η προτεινόμενη και η κατά μήκος της εργασίας αναφερόμενη βιβλιογραφία, που επισημαίνεται με τη βοήθεια πυκνών, αριθμημένων, υποσημειώσεων, οργανώνεται και χωρίζεται σε υλικό επεξήγησης/τεκμηρίωσης αποτελούμενο, πρώτον, από διαδικτυακές παραπομπές σε άρθρα επιστημονικών περιοδικών ή δημοσιεύματα ενημερωτικών δικτύων, έγκυρα λήμματα αναγνωρισμένης ποιότητας εγκυκλοπαιδειών, όπως η WikiPedia ή η VirusList, και αναφορές εταιρειών συναφών με την Πληροφορική και τα Συστήματα Ασφάλειας Πληροφοριών, όλα άμεσα διαθέσιμα από παρεχόμενους υπερσυνδέσμους, και δεύτερον, κατά κύριο λόγο, από την ακόλουθη συλλογή ελληνικών ή ξενόγλωσσων βιβλίων και άλλων, διακεκριμένων, επιστημονικών εργασιών, των οποίων η επαναλαμβανόμενη συμβολή στην εκπόνηση της παρούσας διατριβής υπήρξε καθοριστικής σημασίας και εξαιρετικής αξίας:

8.1 Εγχώρια/Ελληνική

[GRITZALIS-ISSHSE]	"Ασφάλεια Πληροφοριακών Συστημάτων σε περιβάλλοντα υψηλής ευπάθειας", Γκρίτζαλης Δημήτρης, Διδακτορική Διατριβή, Πανεπιστήμιο Αιγαίου, Μάιος 1994.
[GRITZALIS-SICTFA]	"Ασφάλεια στις τεχνολογίες πληροφοριών και επικοινωνιών: Εννοιολογική θεμελίωση", Γκρίτζαλης Δημήτρης, Εκδόσεις Νέων Τεχνολογιών, 1996.

[JILIAD-MS]	"Κακόβουλο Λογισμικό", Ηλιάδης Ιωάννης, Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων Πανεπιστήμιο Αιγαίου, Πανεπιστήμιο Αιγαίου, Ιούλιος 2004.
[KATSIKAS-ICSS]	"Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων (Εννοιολογική θεμελίωση)", Κάτσικας Σωκράτης, Σημειώσεις Ασφάλειας, Τμήμα Μηχανικών Πληροφοριακών & Επικοινωνιακών Συστημάτων Πανεπιστήμιο Αιγαίου.
[KIKIRAS-IW]	"Εισαγωγή στον πληροφοριακό πόλεμο (Information Warfare)", Κίκιρας Παναγιώτης, Τμήμα Ηλεκτρολόγων Μηχανικών & Μηχανικών Η/Υ, Ε.Μ.Π.
[KIOUNTOUZIS-MISS]	"Μοντέλα Ασφάλειας Πληροφοριακών Συστημάτων", Κιουντούζης Ε, Ασφάλεια Πληροφοριών, Τεχνικά, Νομικά και Κοινωνικά θέματα, Εκδόσεις ΕΠΥ, Αθήνα, 1995.
[KOKOLAKIS-ISMIS]	"Ανάπτυξη και Διαχείριση Ασφάλειας Πληροφοριακών Συστημάτων", Κοκολάκης Σ, Διδακτορική Διατριβή, Οικονομικό Πανεπιστήμιο Αθήνας, Ιούνιος 2000.
[LEKKAS-ICSTTP]	"Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων με χρήση υπηρεσιών Έμπιστης Τρίτης Οντότητας Λειτουργικά, Αρχιτεκτονικά και Οργανωτικά ζητήματα", Λέκκας Δημήτρης, Διδακτορική Διατριβή, Τμήμα Μηχανικών Πληροφοριακών & Επικοινωνιακών Συστημάτων, Πανεπιστήμιο Αιγαίου, Ιανουάριος 2002.

8.2 Διεθνής

[ALBERTS-IA]	"The Information Age: An Anthology on Its Impact and Consequences", David S. Alberts and Daniel S. Papp, CCRP Publication Series, 1997.
[ALBERTS-IAT]	"Information Age Transformation: Getting To A 21st Century Military", David S. Alberts, CCRP Publication Series.

[ALBERTS-UIAW]	"Understanding Information Age Warfare", David S. Alberts, CCRP Publication Series.
[APEC-2002]	"Apec Leaders' Statement On Fighting Terrorism And Promoting Growth", Los Cabos, Mexico, 26 October 2002.
[APEC-2005]	"Report of the Telecommunications and Information Working Group (TELWG) to SOM III", APEC Secretariat, APEC Telecommunications and Information Working Group 32nd Meeting, Seoul, Korea, 5-9 September 2005.
[ASHLEY-PISOSAAT]	"Practical Intranet Security: Overview of the State of the Art and Available Technologies", Paul Ashley and Mark Vandenwauver, Kluwer Academic Publishers, 1999.
[AYCOCK-CVM]	"Computer Viruses and Malware", John Aycock, University of Calgary, AB, Canada, © 2006 Springer Science+Business Media, LLC.
[BAILEY-DADA]	"Defense Against The Dark Arts: Using Computer Security To Teach Core Computer Science Concepts", Mark W. Bailey, Associate Professor, Hamilton College,Visiting Professor, University of Virginia at Microsoft Research Faculty Summit.
[BAKSHI-S]	"Steganography", Nishesh Bakshi, Syracuse University, May 6, 2007.
[BALEPIN-SCDC]	"Superworms and Cryptovirology: a Deadly Combination", Ivan Balepin, Department of Computer Science, University of California, Davis.
[BARKHAM-IWILUF]	"Information Warfare And International Law On The Use Of Force", Jason Barkham, Law Clerk, Honorable Naomi Reice Buchwald, U.S. District Court for the Southern District of New York; J.D., Harvard Law School, 2001; B.A., Yale University, 1998.
[BERG_GOEL-STNBA]	"Security Threats: Network Based Attacks", Lecture 2, George Berg/Sanjay Goel, School Of Business, University at Albany.

[BILAR-IM]	"Intro to Malware", Daniel Bilar, Wellesley College, CS342, Handout 11 Friday, Oct. 6th 2006.
[BRENNER_GOODMAN-CNHNPPL]	"Cybercrime: The Need to Harmonize National Penal and Procedural Laws", Susan W. Brenner and Marc D. Goodman, International Society for the Reform of Criminal Law, 16th Annual Conference,Technology and Its Effects on Criminal Responsibility, Security and Criminal Justice, December 6-10, 2002.
[BUTLER_HOGLUND-ROOTKITS]	"Rootkits: Subverting the Windows Kernel", James Butler and Greg Hoglund, © 2006 Pearson Education, Inc., Addison-Wesley.
[BUTLER_HOGLUND-VICE]	"VICE: Catch The Hookers", James Butler and Greg Hoglund, HBGary Software Security Success.
[CARNAHAN_ROBERTS_SHAY_YEARY-MBCV]	"The motivation behind computer viruses", Patrick Carnahan, Dusty Roberts, Zack Shay, Jeff Yeary, Georgia Institute of Technology.
[CHANDRAMOULI_MEMON-SCAP]	"Steganography Capacity: A Steganalysis Perspective", aR. Chandramoulia and bN.D. Memonb, a Department of E.C.E., Stevens Institute of Technology, b Department of Computer Science, Polytechnic University.
[CHEN_KING-SubVirt]	"SubVirt: Implementing malware with virtual machines", Samuel T. King and Peter M. Chen, University of Michigan, Yi-Min Wang, Chad Verbowski, Helen J. Wang and Jacob R. Lorch, Microsoft Research.

[CHIK-CCLMNGIS]	"Challenges to Criminal Law Making in the New Global Information Society: A Critical Comparative Study of the Adequacies of Computer-Related Criminal Legislation in the United States, the United Kingdom and Singapore", Warren Chik, Assistant Professor of Law, Singapore Management University, Executive Director, Society of International Law, Singapore, LLM in International Business Law, University College London, 2004, LLM in International & Comparative Law, Tulane University, 2001, LLB, National University of Singapore, 1996, Solicitor, England & Wales, Attorney & Counsellor at Law, New York, Advocate & Solicitor, Singapore.
[CHRISTODORESCU-STIMD]	"Software Transformations to Improve Malware Detection", Mihai Christodorescu, Somesh Jha, University of Wisconsin, Madison, Johannes Kinder, Stefan Katzenbeisser, and Helmut Veith, Technische Universitaet Muenchen.
[COCHRAN-PSNI]	"Partnership for Secure National Infrastructures", Jerry Cochran, Principal Security Strategist, Trustworthy Computing Group, Microsoft Corporation.
[COCHRAN-SCW]	"Steganographic Computer Warfare", Jordon T. Cochran, Captain, USAF, Department Of The Air Force, Air University, Air Force Institute Of Technology, Wright-Patterson Air Force Base, Ohio.
[COHEN-CV]	"Computer Viruses", Frederic Cohen, Ph.D. Thesis, University of Southern California, ASP Press, 1986.
[COHEN-SCCV]	"A Short Course on Computer Viruses", Frederic Cohen, Wiley Professional Computing, 2nd Edition April 1994.
[COLE_RUIZ-SEHEIW]	"Social Engineering: The human element of Information Warfare", Ray Cole, Mike Ruiz, Ryan Wakeham, Ryan Wilson, CS 4235A, Fall 2003.

[DANG_KOTA-ISSS]	"Case Study: An Implementation of a Secure Steganographic System", Xuan-Hien Dang and Krishna C. S. Kota, Department of Computer Science, University of Akron, Akron OH, USA.
[DAVIES-HM]	"Hypervisor Malware", Fionnbharr Davies, The University Of New South Wales, School Of Computer Science And Engineering, May 2007.
[DEWAN-M]	"Malware", Prashant Dewan, Applied Cryptography, 21st April, 2004.
[DICKMAN-OS]	"An Overview Of Steganography", Shawn D. Dickman, Infosec Techreport, James Madison University, Department of Computer Science, July 2007.
[EDMEAD-SAIH]	"Steganography – The Art of Information Hiding", Mark Edmead, CISSP, SSCP, TICSA, Information Security Consultant, MTE Software, 2002.
[ELSEVIER-CFS]	"Computer Fraud And Security", Elsevier, April 2005 Magazine Issue.
[ERBSCHLOE-TWS]	"Trojans, Worms, And Spyware: A Computer Security Professional's Guide to Malicious Code", Michael Erbschloe, © 2005, Elsevier Inc.
[FERNANDEZ_BUREAU-OM]	"Optimising Malware", José M. Fernandez and PierreMarc Bureau, École Polytechnique de Montréal, 2500 chemin de Polytechnique, Montréal, Québec, Canada.
[FFIEC-IS]	"Information Security", FFIEC, IT Examination Handbook, July 2006.
[FILIOL-BRADLEY]	"Strong Cryptography Armoured Computer Viruses Forbidding Code Analysis: The Bradley Virus", Major Eric Filiol, Army Signals Academy – Virology and Cryptology Laboratory, May 2005.
[FILIOL-CATHCCV]	"Applied Cryptanalysis of Cryptosystems and Computer Attacks Through Hidden Ciphertexts Computer Viruses", Eric Filiol, INRIA, January 2002.

[GARFINKEL_ROSENBLUM-VMIBAID]	"A Virtual Machine Introspection Based Architecture for Intrusion Detection", Tal Garfinkel Mendel Rosenblum, Computer Science Department, Stanford University.
[GRAFF_VANWYK-SCPP]	"Secure Coding: Principles and Practices", Mark Graff and Kenneth Van Wyk, O'Reilly, July 2003.
[GRASSER-SSCSTTDESABOA]	"Simulation of a Secure CPU with SecureTag Technique to Defend Embedded Systems Against Buffer Overflow Attacks", Michael Georg Grasser, Johannes Priebsch, Georg Hofer, Thomas Hodanek, Graz University of Technology, Institute for Technical Informatics.
[GRIMES-MMCVPW]	"Malicious Mobile Code: Virus Protection for Windows", Roger Grimes, O' Reilly, August 2001.
[HEASMAN-IDABR]	"Implementing And Detecting An ACPI BIOS Rootkit", John Heasman, NGS Consulting.
[HEASMAN-IDAPCIR]	"Implementing and Detecting a PCI Rootkit", John Heasman, NGSSoftware Insight Security Research (NISR), 15th November 2006.
[HEIDARI-MCD]	"Malicious codes in depth: Taxonomy of malicious Code", Mohammad Heidari, November 13, 2004.
[HEISER-UTM]	"Understanding today's malware", Jay G. Heiser, Principal Analyst, TruSecure Ltd, Surrey.
[HOLGERSSON-WSS]	"Web Service Security – Vulnerabilities and Threats in the Context of WS-Security", Jesper Holgersson And Eva Söderström, University of Skoevde, Sweden, SIIT 2005, ITU, Geneva, September 2005.
[IBM-ACGIS]	"Anatomy of a Commercial-Grade Immune System", Steve R. White, Morton Swimmer, Edward J. Pring, William C. Arnold, David M. Chess, John F. Morar, IBM Thomas J. Watson Research Center, NY.
[ISG-CCTC]	"Combating Crimeware with Trusted Computing", Shane Balfe, Eimear Gallery, Chris J. Mitchell and Kenneth G. Paterson, Information Security Group, University of London, July 9, 2007.

[JECUSC-SIA]	"Security In The Information Age: New Challenges, New Strategies", Joint Economic Committee, United States Congress, May 2002.
[JOHANSSON-CVTEALF]	"Computer Viruses: The Technology and Evolution of an Artificial Life Form", Karsten Johansson, 1994.
[JUDGE-SPPF]	"Steganography: Past, Present, Future", J.C. Judge, Lawrence Livermore National Laboratory, U.S. Department of Energy, December 1, 2001.
[KALYANI-AVA]	"Analysis of Virus Algorithms", 1Jyoti Kalyani, 2Karanjit Singh Kahlon, 3Harpal Singh and. 4Anu Kalyani, 1CBM Department, GNDU Amritsar, Punjab, India, 2Department of Computer Science and Engineering, GNDU, Amritsar, Punjab, India, 3Department of Computer Science, LIM, Jalandhar, Punjab, India, 4Department of Computer Science, Punjab Technical University, Jalandhar, Punjab, India, Journal of Computer Science 2 (10): 785-788, 2006, © 2006 Science Publications.
[KOEHLER-TCTP]	"Trusted Computing: From Theory to Practice in the Real World", Dipl. Math. Alexander W. Koehler, Utimaco Safeware AG, Germany.
[KROSS-JDCCW]	"Joint Doctrine for Command and Control Warfare (C2W)", Walter Kross, Lieutenant General, USAF, Director, Joint Staff, 7 February 1996.
[KRUKOV-CVDRPM]	"Computer Viruses: Detection, Removal & Protection Methods", Andrew Krukov, AVP Team.
[KUHN-SFSL]	"StegFS: A Steganographic File System for Linux", Andrew D. McDonald and Markus G. Kuhn, University of Cambridge, Computer Laboratory, New Museums Site, United Kingdom, © Springer-Verlag Berlin Heidelberg 2000.
[LEHTINEN-CSB]	"Computer Security Basics", 2nd Edition, Rick Lehtinen, O'Reilly, June 2006.

[LIE-IUOSTH]	"Implementing an Untrusted Operating System on Trusted Hardware", David Lie, Dept. of Comp. and Elec. Eng., University of Toronto, Chandramohan A. Thekkath, Microsoft Research, Mark Horowitz, Computer Systems Lab., Stanford University
[LUDWIG-CVALE]	"Computer Viruses, Artificial Life and Evolution", Mark Ludwig, American Eagle Publications, 1993.
[LUDWIG-GBBCV]	"The Giant Black Book Of Computer Viruses", Mark Ludwig, American Eagle Publications, 1995
[LUDWIG-LBBCV]	"The Little Black Book Of Computer Viruses", Mark Ludwig, American Eagle Publications, 1996
[MARTIN-FWMDWXPCFA]	"FireWire Memory Dump of a Windows XP Computer: A Forensic Approach", Antonio Martin, Copyright © 2007.
[MCCLOSKEY-CV]	"Cryptography And Viruses", Simone McCloskey, Math 187: Introduction to Cryptography, Spring 2005
[MCCONNELL-CCP]	"Cyber Crime . . . And Punishment? Archaic Laws Threaten Global Information", Mcconnell International, December 2000
[MCGRAW-SST]	"Software Security Testing", Gary McGraw, Cigital and Bruce Potter, Booz Allen Hamilton, IEEE SECURITY & PRIVACY, 2004.
[MURDOCH_LEWIS-ECCTI]	"Embedding Covert Channels into TCP/IP", Steven J. Murdoch and Stephen Lewis, University of Cambridge, Computer Laboratory, 15 JJ Thomson Avenue, Cambridge CB3 0FD, United Kingdom.
[NEILSON-STIW]	"Sun Tzu And Information Warfare", Robert E. Neilson, Information Resources Management College, National Defense University Press, Washington, DC, 1997.
[NILSSON-TPMHbS]	"Trusted Platform Modules and Hardware-based Security", Andreas Nilsson, Master's Student at Nada, KTH Pointsec Mobile Technologies.

[NISER-FCW]	"Future Cyber Weapons", Zahri Yunos and Ahmad Nasir Mohd Zin, National ICT Security and Emergency Response Centre (NISER), (This article was published in The Star InTech on 13 November 2003).
[NIST-ICS]	"An Introduction To Computer Security: The NIST Handbook", NIST, Special Publication 800-12.
[NORMAN-NBCV]	"Norman Book on Computer Viruses", Norman ASA, Last revised February 2003.
[O'CONNOR_TOBLER-CIHV]	"CIH Virus", Kevin O'Connor and John Tobler.
[OVERTON-RRIP]	"Rootkits: Risks, Issues and Prevention", Martin Overton, IBM Global Services, UK.
[OZEREN-GRCCMICVA]	"Global Response To Cyberterrorism And Cybercrime: A Matrix For International CooperationAnd Vulnerability Assessment", Suleyman Ozeren, B.A., M.S., Dissertation Prepared For The Degree Of Doctor Of Philosophy, University Of North Texas, August 2005.
[PEARCE-VP]	"Viral polymorphism", Stephen Pearce, SANS Institute, October 2003
[PROVOS_HONEYMAN-HSAIS]	"Hide and Seek: An Introduction to Steganography", Niels Provos And Peter Honeyman, University of Michigan, 2003 IEEE Security & Privacy
[RABAIOTTI-CIS]	"Counter Intrusion Software, Malware Detection using Structural and Behavioural Features and Machine Learning", Joseph Rabaiotti, School of Computer Science, Cardi University, August 4, 2007.
[RAYNAL-MCAC]	"Malicious Crypto: (Ab)use Cryptology", Frederic Raynal, EADS Corporate Research Center & MISC Magazine, EuSecWest 2006.
[ROGERS-KKUCCC]	"The Keys To The Kingdom: Understanding Covert Channels Of Communication", Russ Rogers, CEO Security Horizon, Inc. & Co-Founder of securitytribe.com, BlackHat Japan 2004.

[RUTKOWSKA-BTCDHBRA]	"Beyond the CPU: Defeating Hardware-Based RAM Aquisition (part1: AMD case)", Joanna Rutkowska, COSEINC Advanced Malware Labs, Black Hat DC 2007.
[RUTKOWSKA-CHAMELEON]	"Concepts for the Stealth Windows Rootkit (The Chameleon Project)", Joanna Rutkowska, 2003.
[RUTKOWSKA-FSMTVOS]	"Fighting Stealth Malware – Towards Verifiable OSes", Joanna Rutkowska, COSEINC Advanced Malware Labs, 23rd Chaos Communication Congress Berlin, Germany, December 28th, 2006.
[RUTKOWSKA-ISMT]	"Introducing Stealth Malware Taxonomy", Version 1.01, Joanna Rutkowska, COSEINC Advanced Malware Labs, November 2006.
[RUTKOWSKA-RSbDM]	"Rootkit vs. Stealth-by-Design Malware", Joanna Rutkowska, invisiblethings.org, Black Hat Amsterdam 2006.
[RUTKOWSKA-VOSC]	"Virtualization – the other side of the coin", Joanna Rutkowska, Invisible Things Lab, invisiblethings.org.
[SCHJOLBERG_HUBBARD-HNLAC]	"Harmonizing National Legal Approaches On Cybercrime", Judge Stein Schjølberg & Amanda M. Hubbard, ITU 2005.
[SCHWARTAU-CESIW]	"INFORMATION WARFARE: Chaos on the Electronic Superhighway", Winn Schwartau, All rights Reserved, Thunder's Mouth, Press, 1996.
[SHINDER-SC]	"Scene of the Cybercrime Assisting Law Enforcement In Tracking Down and Prosecuting Cybercriminals", Debra Shinder, Las Vegas BlackHat 2002.
[SIEFFERT-SIDS]	"Stego Intrusion Detection System", Michael Sieffert1, Rodney Forbes1, Charles Green1, Leonard Popyack1, Thomas Blake2, 1Assured Information Security, Inc. PO Box 1182, Rome NY 13442, USA, 2Air Force Research Laboratory, 525 Brooks Road, Rome NY 13442, USA.
[SMU-RCVW]	"Research in Computer Viruses and Worms", Tom Chen, SMU, London, 10 June 2004.

[SPAFFORD-CVAL]	"Computer Viruses As Artificial Life", Eugene H. Spafford, Department of Computer Sciences, Purdue University West Lafayette.
[STALLINGS-CNS]	"Cryptography and Network Security", William Stallings, Prentice Hall, 4/e 2005.
[STAMP_WONG-HME]	"Hunting For Metamorphic Engines", Mark Stamp and Wing Wong, August 5, 2006.
[SYMANTEC-EIWLSS]	"The Economics of Information Warfare - Poking Layered Security with a Stick", Mark Wells and Woody Thrower, Symantec.
[SYMANTEC-STRIKER]	"Understanding and Managing Polymorphic Viruses", The Symantec Enterprise Papers Volume XXX, Carey Nachenberg, Symantec.
[SYMANTEC-UVB32BOE]	"Understanding Virus Behavior in 32-bit Operating Environments", Symantec AntiVirus Research Center, Symantec.
[SYMANTEC-WMMR]	"When Malware Meets Rootkits", Elia Florio, Symantec Security Response, Dublin, Symantec.
[SZOR-ACVRD]	"The Art Of Computer Virus Research And Defense", Peter Szor, Addison-Wesley Professional, February 03, 2005.
[TAKASHI-ISVSPSVTBBA]	"Introduction of Security Profile for staff verification by token based biometric authentication", Shirakata Takashi, R&D Headquarters, NTT DATA Corporation, 66th ICCC 2005 in Tokyo, 29 September 2005.
[TANENBAUM-MOS9]	"Modern operating systems", Andrew Tanenbaum, Prentice Hall, ISBN 0-13-031358-0, 2001.
[THORNTON-RFIDS]	"RFID Security: Protect The Supply Chain", Frank Thornton, Brad Haines, Anand M. Das, Hersh Bhargava, Anita Campbell, John Kleinschmidt, Syngress Publishing.
[TUCH_KLEIN_HEISER-OSVN]	"OS Verification — Now!", Harvey Tuch, Gerwin Klein and Gernot Heiser, National ICT Australia, University of New South Wales.

[UN55_63-2001]	"United Nations A/RES/55/63: Combating the criminal misuse of information technologies", U.N. General Assembly, 22 January 2001.
[VASLIN_PEGATOQUET-TCNCES]	"Trusted computing - A new challenge for embedded systems", Romain Vaslin, Guy Gogniat, Jean-Philippe Diguet, LESTER UBS/CNRS FRE 2734, Alain Pegatoquet, WTBU – CSSD, Texas Instruments, ©2006 IEEE.
[WALENSTEIN-DSMM]	"The Design Space of Metamorphic Malware", Andrew Walenstein†, Rachit Mathur‡, Mohamed R. Chouchane†, and Arun Lakhotia†, †University of Louisiana at Lafayette, Lafayette, LA, U.S.A., ‡McAfee Avert Labs, Beaverton, OR, U.S.A.
[WEAVER_PAXSON-TCW]	"A Taxonomy of Computer Worms", Nicholas Weaver, UC Berkeley, Vern Paxson, ICSI, Stuart Staniford, Silicon Defense and Robert Cunningham, MIT Lincoln Laboratory, WORM'03, October 27, 2003, Washington, DC, USA.
[WEBSTER_MALCOLM-DMCVAS]	"Detection of metamorphic computer viruses using algebraic specification", Matt Webster and Grant Malcolm, 31 August 2006, © Springer-Verlag France 2006.
[WU_LIDAR-QM]	"Quantum Malware", Lian-Ao Wu(1) and Daniel A. Lidar(1,2), (1)Chemical Physics Theory Group, Department of Chemistry and Center for Quantum Information and Quantum Control, University of Toronto, (2)Departments of Chemistry, Electrical Engineering-Systems and Physics, University of Southern California, Los Angeles, 27 Jan 2006.
[XUEMIN-ISMSoC]	"Information Security of Multimedia System-on-Chip", Sherman (Xuemin) Chen, Ph. D., Broadcom®.
[XUKAI-SC]	"Security and Cryptography Notes", Xukai Zou, CSCI 436, Principles of Computer Networks (Spring 2006), Department of Computer and Information Science, School of Science, Purdue University at IUPUI, 723 W. Michigan St., SL280, Indianapolis, IN 46202.

[YOUNG_YUNG-CEBSTC]	“Cryptovirology: Extortion-Based Security Threats And Counterneasures”, Adam Young, Dept. of Computer Science, Columbia University, Moti Yung, IBM T.J. Watson Research Center, New York.
[ZANERO-FFEIIT]	“Flaws and frauds in the evaluation of IDS/IPS technologies”, Stefano Zanero, DEI - Politecnico di Milano.

Λίστα Σχημάτων