ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ
ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ
ΑΣΦΑΛΕΙΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΤΙΤΛΟΣ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

" Αξιολόγηση ασφάλειας air-gapped δικτύου

(Security Assessment of an air-gapped network) „

ΤΟΥ: ΜΕΤΑΝΙΑ ΓΕΩΡΓΙΟΥ - ΧΡΗΣΤΟΥ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: ΞΕΝΑΚΗΣ ΧΡΗΣΤΟΣ

ΠΕΙΡΑΙΑΣ ΜΑΪΟΣ 2023

ΠΕΡΙΛΗΨΗ

Στη σύγχρονη εποχή του ψηφιακού μετασχηματισμού, η προστασία των ευαίσθητων δεδομένων γίνεται όλο και πιο ζωτικής σημασίας. Οι απειλές και οι επιθέσεις στον κυβερνοχώρο έχουν γίνει πιο εξελιγμένες και ακόμη και τα πιο ασφαλή δίκτυα είναι ευάλωτα σε παραβιάσεις. Ως αποτέλεσμα, οι οργανισμοί που διαχειρίζονται μεγάλο όγκο προσωπικών δεδομένων πελατών και εργαζομένων, οικονομικές πληροφορίες αλλά και εμπορικά μυστικά, στρέφονται σε απομονωμένα δίκτυα ως μέσο προστασίας των πιο ευαίσθητων περιουσιακών τους στοιχείων. Τέτοιου είδους δίκτυα παρέχουν ένα επιπλέον επίπεδο ασφάλειας, απομονώνοντας κρίσιμα συστήματα από το Διαδίκτυο και άλλα δίκτυα. Αυτή η απομόνωση καθιστά δύσκολο για τους εισβολείς να αποκτήσουν πρόσβαση σε αυτά και να κλέψουν ευαίσθητα δεδομένα. Ωστόσο, τα air-gapped δίκτυα δεν είναι άτρωτα και εξακολουθούν να είναι ευάλωτα σε διάφορους κινδύνους, συμπεριλαμβανομένων των εσωτερικών απειλών, της φυσικής πρόσβασης και των κακόβουλων λογισμικών που εισάγονται μέσω αφαιρούμενων μονάδων. Αυτή η εργασία λοιπόν, στοχεύει στην διερεύνηση των πλεονεκτημάτων και μειονεκτημάτων τέτοιων απομονωμένων δικτύων, στα συνήθη τρωτά σημεία και τις μεθόδους διείσδυσης, καθώς και στις διαφορετικές μεθόδους ανίχνευσης. Επιπλέον, γίνεται αναφορά στην γεφύρωση μεταξύ air-gapped δικτύων και δικτύων συνδεδεμένα στο Διαδίκτυο για κοινή χρήση πληροφοριών και ανταλλαγή δεδομένων, διατηρώντας παράλληλα την ασφάλεια τους. Κατανοώντας τους πιθανούς κινδύνους και τις μεθόδους προστασίας, οι οργανισμοί εν τέλη μπορούν να αξιολογήσουν την καταλληλότητα των απομονωμένων δικτύων με βάση τις ανάγκες ασφαλείας τους.

ABSTRACT

In the modern era of digital transformation, the protection of sensitive data has become increasingly vital. Cyber threats and attacks have become more sophisticated, and even the most secure networks are vulnerable to breaches. As a result, organizations, that are handling a large amount of personal data of customers and employees, financial information and also trade secrets, are turning to air-gapped networks as a means of protecting their most sensitive assets. Air-gapped networks provide an extra layer of security by isolating critical systems from the internet and other networks. This isolation makes it difficult for attackers to gain access to these networks and steal sensitive data. However, air-gapped networks are not foolproof, and there are still vulnerable to various risks, including insider threats, physical access, and malware introduced through removable media. This paper aims to explore the advantages and disadvantages of air-gapped networks, the common vulnerabilities and methods of penetration, and the different methods of detection. Moreover, in the paper will also discuss how to bridge air-gapped networks to other networks and to the Network for information sharing and data transferring, while maintaining security. By understanding the potential risks and methods of protection, organizations can evaluate the suitability of air-gapped networks for their security needs.

ΣΕΛΙΔΑ ΕΥΧΑΡΙΣΤΗΡΙΩΝ

Θεωρώ υποχρέωσή μου να ευχαριστήσω τον επιβλέποντα καθηγητή Ξενάκη Χρήστο για την πολύτιμη καθοδήγησή του. Επιπλέον, θέλω να ευχαριστήσω θερμά τον Ταγματάρχη Βάσιο Γεώργιο, του τμήματος Κυβερνοάμυνας του Κέντρου Πληροφορικής Υποστήριξης του Ελληνικού Στρατού (ΚΕΠΥΕΣ), για την βοήθεια που μου πρόσφερε στην εύρεση στοιχείων. Επιπρόσθετα, οφείλω να αφιερώσω την διπλωματική μου εργασία στους γονείς μου που μου συμπαραστάθηκαν στα χρόνια της φοίτησής μου στο Πανεπιστήμιο Πειραιώς.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΠΙΝΑΚΑΣ ΕΙΚΟΝΩΝ

ΛΙΣΤΑ ΠΙΝΑΚΩΝ

ΚΕΦΑΛΑΙΟ 1ο : ΕΙΣΑΓΩΓΗ

1.1 Πρόλογος

Η αγαπημένη συνήθεια των επιτιθέμενων και των hackers, δεν είναι άλλη από το να κάθονται στην άνεση της καρέκλας του γραφείου τους, και να πραγματοποιούν απομακρυσμένες επιθέσεις σε ευάλωτα δίκτυα ανά τον κόσμο. Υπάρχουν όμως, ορισμένα κρίσιμα ηλεκτρονικά συστήματα, τα οποία δεν εκτίθενται στο δημόσιο Διαδίκτυο, παρά βρίσκονται με ασφάλεια απομονωμένα από τον υπόλοιπο κόσμο, λόγω έλλειψης σύνδεσης σε αυτό. Τοιουτοτρόπως, η διατήρηση ενός τέτοιου συστήματος αυξάνει τη στάση ασφαλείας του, χωρίς να λείπουν από την εξίσωση τα τρωτά σημεία που μπορεί να δημιουργηθούν, όταν οι χειριστές του πρέπει να απορροφήσουν δεδομένα ή να τα μεταφέρουν εκτός του δικτύου. Κατά συνέπεια, ένα “air-gapped” δίκτυο, όπως ονομάζεται, σε ορισμένες καταστάσεις έχει αποδειχθεί ευάλωτο σε επιθέσεις, κρίσιμες και μη.

1.2 Σκοπός και στόχοι της εργασίας

Σκοπός της εργασίας είναι η αξιολόγηση ασφαλείας των air-gapped δικτύων στον κυβερνοχώρο, ώστε να γίνει κατανοητό τι χρειάζεται και πόσο εύκολη είναι η διατήρηση ενός τέτοιου δικτύου, ποιοι είναι οι κίνδυνοι που καραδοκούν και πόσο σημαντική είναι η σωστή και ασφαλής λειτουργία τους στην σημερινή εποχή.

Οι στόχοι της εργασίας είναι:

1. ο προσδιορισμός της έννοιας “air-gapped network”,
2. τα πλεονεκτήματα και μειονεκτήματα της διατήρησης μιας τέτοιας υποδομής,
3. η ανάλυση και κατανόηση πιθανών κινδύνων ασφαλείας και τρωτών σημείων που προκύπτουν σε air-gapped δίκτυα και μπορούν να εκμεταλλευτούν επιτιθέμενοι,
4. η εξέταση μεθόδων και τεχνικών προσβολής φυσικά και λογικά απομονωμένων δικτύων,
5. η παρουσίαση αντιμέτρων και μεθόδων πρόληψης και εντοπισμού για καλύτερη προστασία, και
6. η εύρεση τρόπων γεφύρωσης air-gapped δικτύων με άλλα δημόσια-ιδιωτικά δίκτυα και το Διαδίκτυο.

1.3 Ορισμός

Το Air-gapping είναι ένα μέτρο ασφαλείας που περιλαμβάνει τη φυσική απομόνωση ενός υπολογιστή ή δικτύου και την αποτροπή του από την πραγματοποίηση συνδέσεων με συσκευές άλλων δικτύων ή με το Διαδίκτυο. Τα air-gaps βοηθούν στην προστασία κρίσιμων συστημάτων ή δεδομένων από πιθανές επιθέσεις όπως malware ή ransomware. Σε αντίθεση με άλλα backup ή recovery, τα air-gapped δίκτυα είναι εντελώς διαχωρισμένα από άλλες συσκευές και αόρατα από απομακρυσμένες απειλές και από σαρώσεις για εύρεση ευάλωτων μηχανημάτων. Επί τούτου, υπάρχει συνήθως καθορισμένος χώρος μεταξύ του απομονωμένου συστήματος και των καλωδίων άλλου τεχνικού εξοπλισμού, για την αποφυγή ηλεκτρομαγνητικών ή ηλεκτρονικών εκμεταλλεύσεων. Ορισμένα εξαιρετικά ευαίσθητα συστήματα διαθέτουν ακόμη ένα φυσικό περίβλημα που ονομάζεται Faraday Cage[1], για να εμποδίζει τη διαφυγή της ηλεκτρομαγνητικής ακτινοβολίας.

Για την μεταφορά δεδομένων από μια air-gapped συσκευή, πρέπει να χρησιμοποιηθεί μια αφαιρούμενη συσκευή αποθήκευσης, όπως ένα USB, και να συνδεθεί φυσικά στο άλλο σύστημα. Επίσης, υπάρχει η δυνατότητα τοποθέτησης air-gapped συσκευών με κρίσιμα δεδομένα στο ίδιο rack με άλλα συστήματα, στις περιπτώσεις όπου πρόκειται για διαχείριση διαφορετικών επιπέδων πληροφορίας, με προσοχή ωστόσο στην τοποθεσία του rack και στα άτομα που έχουν φυσική πρόσβαση εκεί.

[1] Περίβλημα ή δωμάτιο που αποτελείται από πλέγμα αγώγιμων υλικών και χρησιμοποιείται για να μπλοκάρει τα ηλεκτρομαγνητικά πεδία.

ΚΕΦΑΛΑΙΟ 2ο : AIR-GAPPED NETWORK

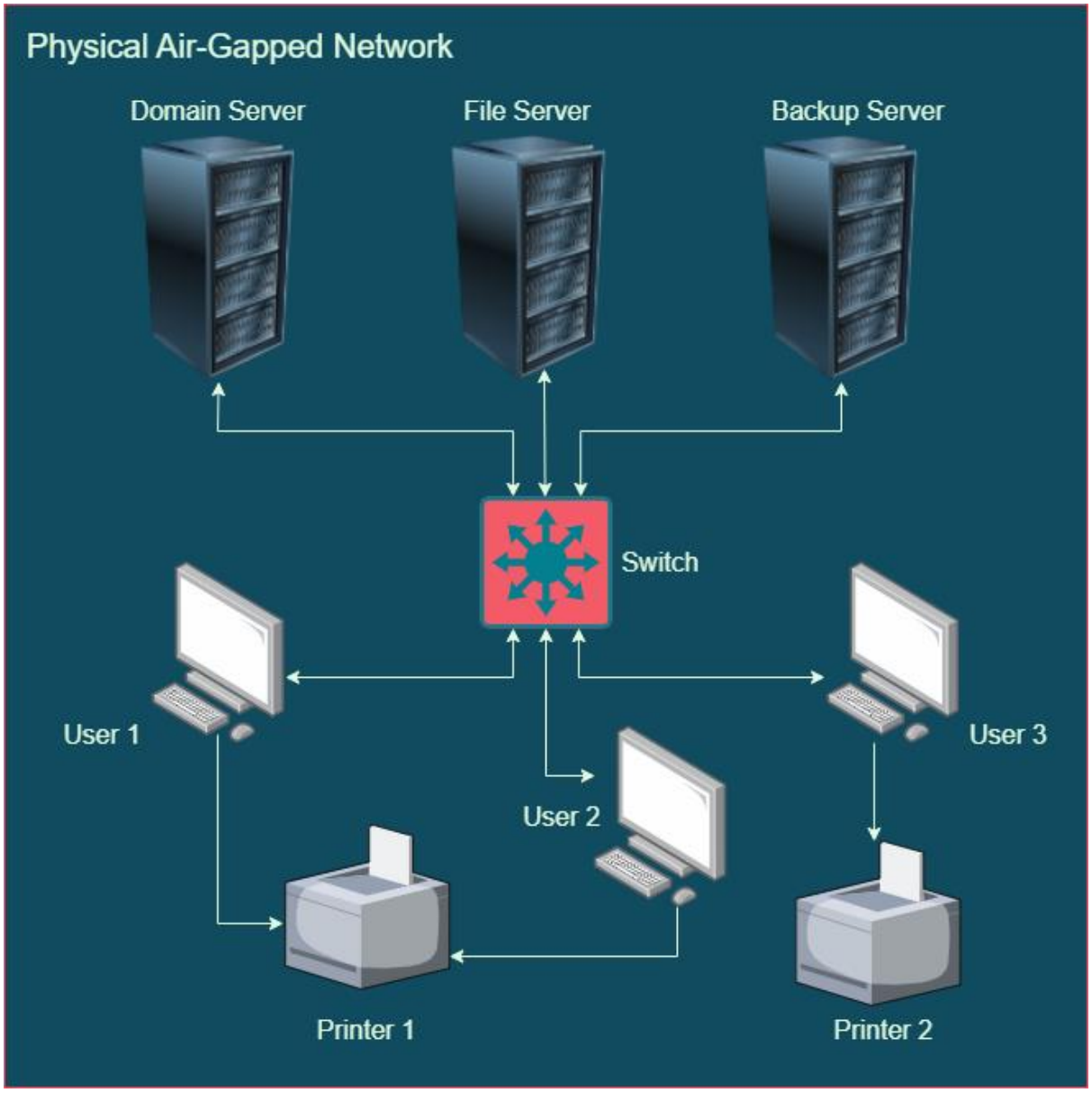
2.1 Η χρήση ενός air-gapped network

Τα air-gapped δίκτυα, όπως αναφέρθηκε στο προηγούμενο κεφάλαιο, χρησιμοποιούνται για την προστασία κρίσιμων συστημάτων από κακόβουλους χρήστες. Πολλές κρίσιμες υποδομές όπως οι Αμυντικές Υπηρεσίες του Στρατού, υπηρεσίες Έκτακτης Ανάγκης, Χρηματοπιστωτικές υπηρεσίες, Βιομηχανίες ενέργειας, Κυβερνητικές εγκαταστάσεις Υγείας, εκλογικά συστήματα καθώς και SCADA συστήματα λειτουργίας πυρηνικών αντιδραστήρων, χρησιμοποιούν air-gapped δίκτυα για να προστατεύσουν τα περιουσιακά τους στοιχεία, ευαίσθητα δεδομένα, σημαντικά αρχεία, μυστικές συνομιλίες, κρίσιμα μηχανήματα κ.α. Παρόλο που τέτοια δίκτυα είναι αποσυνδεδεμένα από άλλα συστήματα και το Διαδίκτυο, και επομένως δύσκολα ένας εισβολέας αποκτά πρόσβαση σε αυτά, έχουν πληγεί στο παρελθόν ουκ ολίγες φορές με κακόβουλο λογισμικό. Ως εκ τούτου air-gapped δίκτυα χρησιμοποιούνται και για δημιουργία αντιγράφων ασφαλείας και ανάκτησης. Εάν ένας οργανισμός χτυπηθεί από μια επίθεση ransomware, ο air-gapped backup server μπορεί να χρησιμοποιηθεί για ανάκτηση, αποφεύγοντας παράλληλα και την πληρωμή των λύτρων.

2.1 Τύποι air-gaps

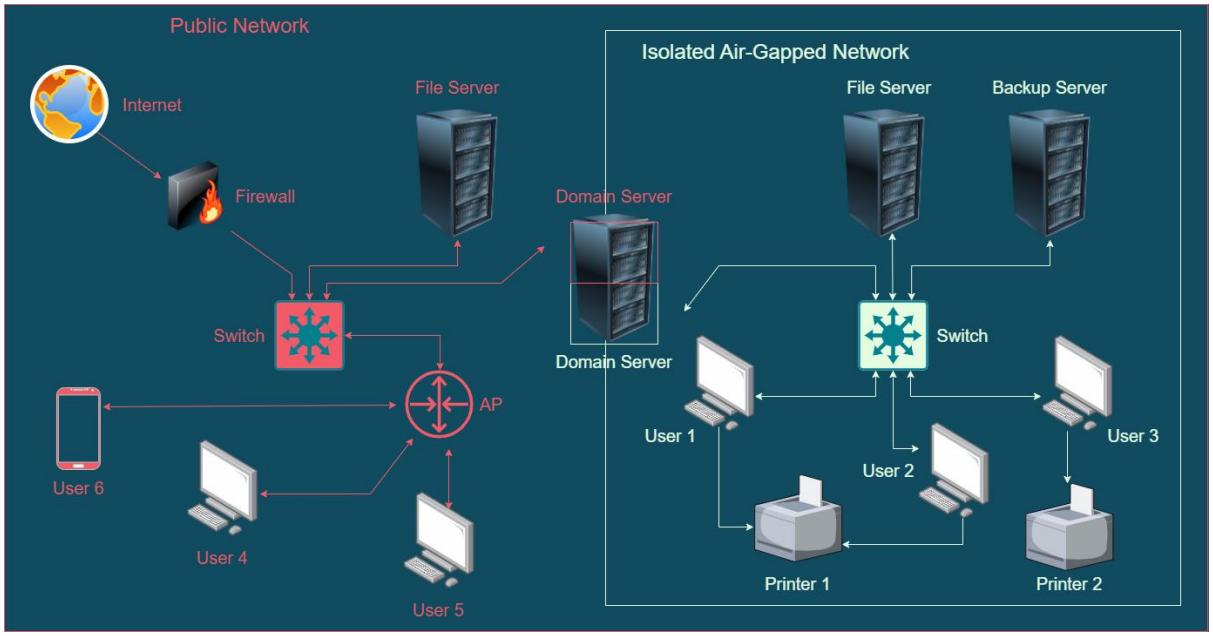
Υπάρχουν τριών ειδών air-gapped networks:

1. Τα **Total Physical Air-Gapped Networks** στα οποία το hardware ή το software είναι φυσικά απομονωμένο στο δικό του περιβάλλον. Στον συγκεκριμένο τύπο, διαχωρίζεται πλήρως ένα σύστημα από άλλα συνδεδεμένα στο δίκτυο συστήματα και έχει επίσης, περιορισμένη φυσική πρόσβαση.



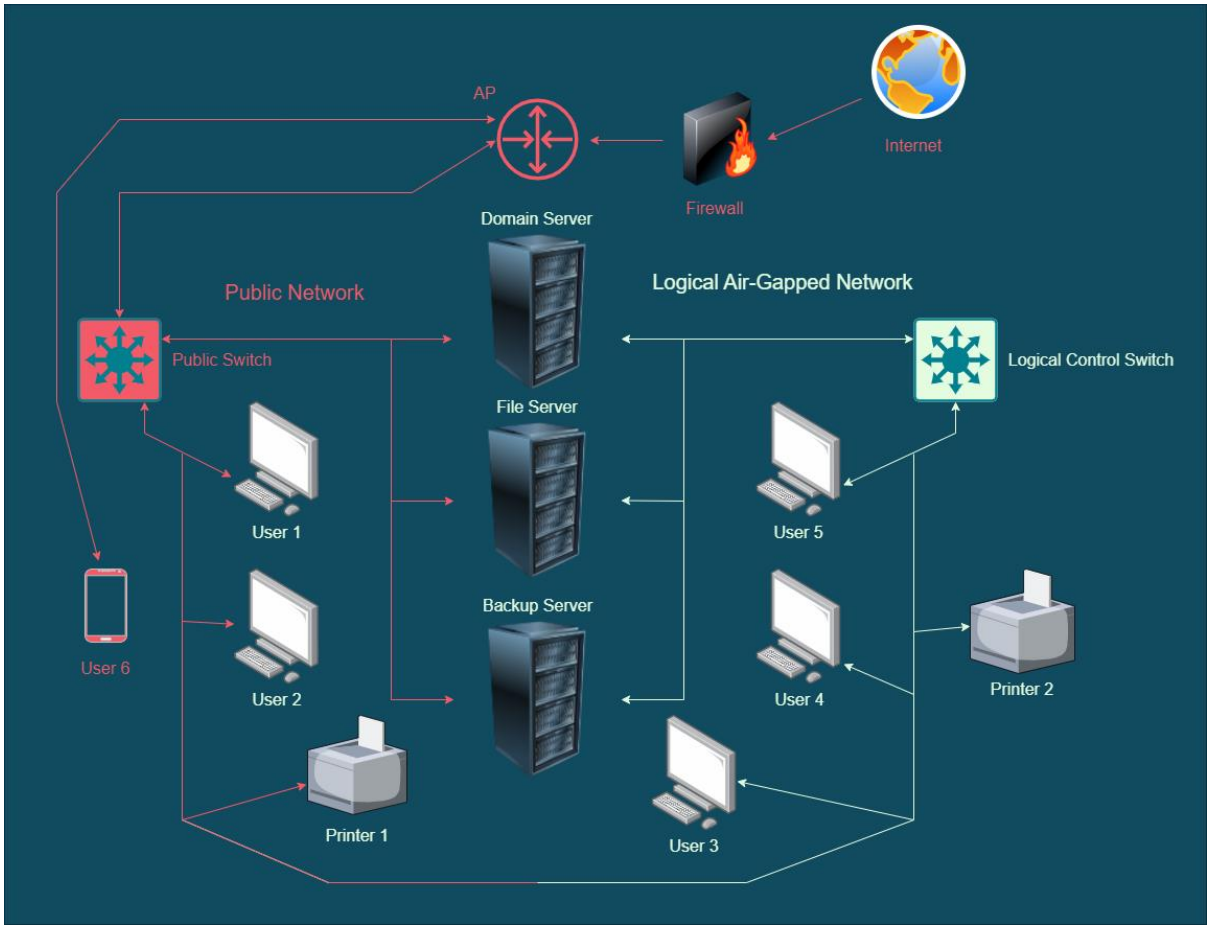
Εικόνα 1 Physical Air-Gapped Network

2. Τα **Isolated Air-Gapped Networks** είναι απομονωμένα air-gapped συστήματα που διαχωρίζονται από άλλα συστήματα στο ίδιο περιβάλλον, ίσως ακόμη και στο ίδιο rack, αλλά δεν είναι συνδεδεμένα στο ίδιο δίκτυο.



Εικόνα 2 Isolated Air-Gapped Network

3. Τα **Logical Air-Gapped Networks** διαχωρίζουν τα συστήματα μέσα στο ίδιο δίκτυο λογικά και όχι φυσικά. Σαν μέθοδοι λογικού διαχωρισμού χρησιμοποιούνται η κρυπτογράφηση, ο έλεγχος πρόσβασης βάσει ρόλων κ.α.



Εικόνα 3 Logical Air-Gapped Network

Αξιοσημείωτο είναι το γεγονός ότι σε αρκετούς οργανισμούς χρησιμοποιείται πάνω από ένας τύπος air-gapped δικτύων μιας και εκτός από κρίσιμες υποδομές, υπάρχουν δεδομένα και συστήματα που πρέπει να παραμένουν συνδεδεμένα στο Διαδίκτυο.

2.4 Πλεονεκτήματα & Μειονεκτήματα

Το βασικό πλεονέκτημα ενός air-gapped δικτύου είναι η ισχυρή στάση κυβερνοασφάλειας που δημιουργεί, προστατεύοντας ευαίσθητα δεδομένα και μηχανήματα, και επιτρέποντας μόνο σε άτομα που έχουν φυσική πρόσβαση να το χρησιμοποιούν. Αυτό σημαίνει ότι προτού ένας εισβολέας μπορέσει να εγκαταστήσει κακόβουλο λογισμικό ή ransomware, είτε να κλέψει δεδομένα από ένα απομονωμένο σύστημα, πιθανότατα θα χρειαστεί να ξεπεράσει πολλά στρώματα πυλών, τειχών και άλλων φυσικών αμυνών. Σημαίνει επίσης ότι οι εξουσιοδοτημένοι χρήστες εκτός του air-gapped δικτύου θα πρέπει να περνούν

από τα ίδια μέτρα ασφαλείας κάθε φορά που χρειάζεται να έχουν πρόσβαση ή να μοιράζονται δεδομένα, που παράγονται εντός του ασφαλούς δικτύου.

Ακόμη προστατεύει τα ψηφιακά περιουσιακά στοιχεία ενός οργανισμού από καταστροφές, περιορίζει τις δυνατότητες ενός malware να εξαπλωθεί και βελτιώνει τις πιθανότητες ανάκαμψης δεδομένων από τυχόν επιτυχείς επιθέσεις.

Ωστόσο, το κόστος και η αδιάκοπη φυσική παρουσία και παρακολούθηση που απαιτείται για πρόσβαση σε επιχειρησιακά δεδομένα, οδηγούν οργανισμούς και επιχειρήσεις στην εγκατάλειψη της ιδέας του air-gapping των συστημάτων τους. Με το cloud να μετατρέπεται ολοένα και περισσότερο σε θεμελιώδες στοιχείο για τη λειτουργία ζωτικής σημασίας υποδομών, η διατήρηση ενός air-gapped δικτύου γίνεται δυσκολότερη.

Ακόμη, ένα air-gapped δίκτυο, το οποίο δεν είναι συνδεδεμένο στο Διαδίκτυο, χάνει και την δυνατότητα της αυτόματης ενημέρωσης του λογισμικού που χρησιμοποιεί, καθώς και των applications που είναι εγκατεστημένα. Επομένως, οι διαχειριστές τέτοιων συστημάτων πρέπει να κατεβάζουν και να εγκαθιστούν με μη αυτόματο τρόπο νέες ενημερώσεις και patches. Αυτό απαιτεί συχνότερη χειροκίνητη εισαγωγή πληροφοριών, άρα και περισσότερη προσοχή από πλευράς των διαχειριστών, τόσο στην ακεραιότητα των ενημερώσεων που εγκαθιστούν όσο και στη διατήρηση ενός ενημερωμένου air-gapped δικτύου καθολικά, μιας και η παράβλεψη ενός μεμονωμένου συστήματος το καθιστά ξεπερασμένο και κατά συνέπεια απροστάτευτο από αναδυόμενες απειλές.

Τέλος τέτοια δίκτυα θα πρέπει να έχουν περιορισμένη πρόσβαση, να τοποθετούνται σε συγκεκριμένες τοποθεσίες προστατευμένες από τυχόν φυσικές καταστροφές και να φυλάσσονται διαρκώς. Ακόμα και τότε τα air-gaps εξακολουθούν να είναι επιρρεπή σε επιθέσεις. Μια πολύ γνωστή περίπτωση όπου ένα air-gapped δίκτυο δεν ήταν αρκετό για την προστασία των συστημάτων είναι το Stuxnet worm, που επιτέθηκε σε όλα τα απομονωμένα βιομηχανικά συστήματα ελέγχου. Θεωρείται ότι εισήχθη από ένα thumb drive υπαλλήλου της επιχείρησης.

Όπως θα διαπιστώσουμε και στο επόμενο κεφάλαιο, η εισαγωγή πληροφορίας με εσφαλμένο τρόπο σε ένα απομονωμένο δίκτυο, μπορεί να μολύνει με κακόβουλο λογισμικό μία συσκευή και εν συνεχεία ολόκληρο το δίκτυο, θέτοντας σε κίνδυνο όλα τα κρίσιμα και μη δεδομένα του.

ΚΕΦΑΛΑΙΟ 3ο : ΕΥΠΑΘΕΙΕΣ & ΤΡΩΤΑ ΣΗΜΕΙΑ

Οι οργανισμοί καταβάλουν τα μέγιστα για να προστατεύσουν τα εσωτερικά τους δίκτυα από Διαδικτυακές επιθέσεις διατηρώντας τα απομονωμένα χωρίς καμία φυσική ή λογική σύνδεση με το Διαδίκτυο. Ωστόσο, η air-gap απομόνωση δεν παρέχει απόλυτη προστασία. Επίδοξοι hacker τα τελευταία δεκαπέντε χρόνια έχουν δείξει ότι μπορούν να προσπελάσουν οποιοδήποτε διαχωριστικό επίπεδο και να μολύνουν με malware air-gapped δίκτυα ανά τον κόσμο χρησιμοποιώντας insider threat και attack vectors. Πρόκειται για τεχνικές που αποτελούν το εναρκτήριο μέσο με το οποίο ένας εισβολέας ή hacker μπορεί να αποκτήσει πρόσβαση σε έναν υπολογιστή ή network server εκμεταλλευόμενος τα τρωτά σημεία του δικτύου όπως εκείνος επιθυμεί.

3.1 Insider Threat

Ένας insider threat ή threat actor, μιας και πρόκειται για φυσικό πρόσωπο, είναι ένα security risk που προέρχεται από το εσωτερικό του οργανισμού-στόχου. Συνήθως αφορά έναν νυν ή πρώην υπάλληλο, είτε business associate που έχει πρόσβαση σε ευαίσθητες πληροφορίες ή privileged accounts (π.χ. administrator) εντός του απομονωμένου δικτύου και κάνει κατάχρηση αυτής της πρόσβασης. Η συγκεκριμένη απειλή αποτελεί τη σημαντικότερη ευπάθεια ενός air-gapped network μιας και τα παραδοσιακά μέτρα ασφαλείας τείνουν να επικεντρώνονται σε εξωτερικές απειλές και δεν είναι πάντα ικανά να εντοπίσουν μια απειλή που προέρχεται από το εσωτερικό του οργανισμού. Τύποι insider threats αποτελούν:

- **Malicious insider** – γνωστός και ως Turncloak[2], είναι κάποιος που σκόπιμα κάνει κατάχρηση νόμιμων διαπιστευτηρίων, συνήθως για να κλέψει πληροφορίες για οικονομικά ή προσωπικά κίνητρα. Για παράδειγμα, ένα άτομο που κρατά μνησικακία σε έναν πρώην εργοδότη ή ένας καιροσκόπος υπάλληλος που πουλά μυστικές πληροφορίες σε έναν ανταγωνιστή. Οι Turncloaks έχουν ένα πλεονέκτημα έναντι άλλων εισβολέων, επειδή είναι εξοικειωμένοι με τις πολιτικές και τις διαδικασίες ασφαλείας ενός οργανισμού, καθώς και με τα τρωτά σημεία του.
- **Nation State Actor** – με ‘license to hack’, πρόκειται για ειδική κατηγορία malicious insider, ο οποίος εργάζεται ως μυστικός πράκτορας για μία κυβέρνηση και μέσω του

[2] Όρος που χρησιμοποιείται για ένα ύπουλο, άπιστο άτομο που έχει προδώσει εκείνους που πίστευαν σε αυτόν, εκείνους που τον θεωρούσαν άξιο εμπιστοσύνης.

οργανισμού-στόχου μεταφέρει πολύτιμα δεδομένα και πληροφορίες που μπορούν να δημιουργήσουν περιστατικά διεθνής σημασίας. Μπορεί να αποτελούν κρυφά μέλη του «κυβερνο-στρατού» μιας χώρας ή πληρωμένοι hackers για εταιρείες που ευθυγραμμίζονται με τους στόχους μιας κυβέρνησης. Τέτοιου είδους άτομα γνωρίζουν πολύ καλά που εμπλέκονται καθώς και ότι το χάος που εξαπλώνουν στο εξωτερικό υποστηρίζεται σιωπηρά από το κράτος τους. Να σημειωθεί ότι στον πόλεμο μεταξύ Ρωσίας – Ουκρανίας, η Microsoft σε επίσημο έγγραφο «ξεσκέπασε» τουλάχιστον έξη Ρώσους nation state actors υπεύθυνους για cyber-attacks εναντίον Ουκρανικών υποδομών[3].

- **A mole** – ένας απατεώνας που είναι ξένος στον οργανισμό, αλλά καταφέρνει να αποκτήσει πρόσβαση στο air-gapped δίκτυο. Για να πετύχει κάτι τέτοιο παρουσιάζεται ως υπάλληλος ή συνεργάτης.
- **Careless insider** – ένα αθώο πιόνι που εκθέτει εν αγνοία του το σύστημα σε εξωτερικές απειλές. Αυτός είναι ο πιο συνηθισμένος τύπος insider threat, που υποπίπτει σε κοινά λάθη, όπως το να αφήνει μια συσκευή εκτεθειμένη ή να πέφτει θύμα ηλεκτρονικής απάτης κάνοντας κλικ σε έναν μη ασφαλή σύνδεσμο και μολύνοντας το σύστημα με κακόβουλο λογισμικό.

3.2 Supply-chain Attack

Μια supply-chain attack, ή αλλιώς third-party attack, συμβαίνει όταν ένας κακόβουλος χρήστης διεισδύει σε ένα υπολογιστικό σύστημα ή δίκτυο μέσω ενός εξωτερικού συνεργάτη ή παρόχου, που έχει πρόσβαση στα συστήματα και τα δεδομένα αυτών. Λόγω του ότι προμηθευτές και πάροχοι υπηρεσιών αγγίζουν όλο και περισσότερα ευαίσθητα δεδομένα τα τελευταία χρόνια, οι κίνδυνοι που συνδέονται με μία supply-chain attack είναι υψηλότεροι από ποτέ, μιας και οι επιτιθέμενοι πλέον έχουν περισσότερους πόρους και εργαλεία στη φαρέτρα τους.

Πρόκειται για συνηθισμένη ευπάθεια σε air-gapped δίκτυα ανά τον κόσμο και χρήζει μεγάλης προσοχής η επιλογή και εμπιστοσύνη των παρόχων software, όπως ένα ERP application system (π.χ. SAP), καθώς και των cloud services που χρησιμοποιεί ένας οργανισμός ή μία εταιρεία. Επομένως οι ενημερώσεις λογισμικού εφαρμογών που επιτρέπουν την διαχείριση και τον διαμοιρασμό πόρων ανά των υπαλλήλων μέσα στο air-gapped δίκτυο

[3] https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

του οργανισμού θα πρέπει να γίνεται προσεκτικά, διότι ένα, εν αγνοία, trojan update της εταιρείας παρόχου που θα εγκατασταθεί, καθιστά ευάλωτο ολόκληρο τον οργανισμό.

Χαρακτηριστικό παράδειγμα αποτελεί η πρόσφατη επίθεση στη SolarWinds το 2020. Μια ομάδα hackers που πιστεύεται ότι συνδέεται με τη ρωσική κυβέρνηση απέκτησε πρόσβαση σε συστήματα υπολογιστών που ανήκουν σε πολλά κυβερνητικά τμήματα των ΗΠΑ, συμπεριλαμβανομένου του Υπουργείου Οικονομικών και Εμπορίου, σε μια μακρά εκστρατεία που λέγεται ότι ξεκίνησε τον Μάρτιο του 2020. Οι hackers παραβίασαν την υποδομή της SolarWinds, μιας εταιρείας που πουλάει πλατφόρμα παρακολούθησης δικτύου και εφαρμογών με το όνομα Orion (ένα μέρος της ιδανικεύεται μάλιστα στην ανίχνευση insider threats) , και στη συνέχεια χρησιμοποίησαν αυτή την πρόσβαση για να παράγουν και να διανέμουν trojanized software updates[4] στους χρήστες. Σύμφωνα με σελίδα στον ιστότοπό της, που καταργήθηκε μετά το ξέσπασμα των ειδήσεων, η εταιρεία δήλωσε ότι ανάμεσα στους πελάτες της περιλαμβάνονται 425 εταιρείες από το Fortune 500[5] των ΗΠΑ, οι δέκα κορυφαίες εταιρείες τηλεπικοινωνιών των ΗΠΑ, οι πέντε κορυφαίες λογιστικές εταιρείες των ΗΠΑ, όλα τα υποκαταστήματα του αμερικανικού στρατού, Το Πεντάγωνο, το State Department, καθώς και εκατοντάδες πανεπιστήμια και κολέγια σε όλο τον κόσμο. Η συγκεκριμένη επίθεση επέτρεψε επίσης σε hackers να αποκτήσουν πρόσβαση στο δίκτυο της αμερικανικής εταιρείας κυβερνοασφάλειας FireEye.

3.3 Social Engineering Attack Techniques

Καθώς οι τεχνολογικές άμυνες γίνονται πιο ισχυρές, οι cyber-criminals χρησιμοποιούν όλο και περισσότερο social engineering τεχνικές για να εκμεταλλευτούν τον πιο αδύναμο κρίκο στην αλυσίδα ασφαλείας: τους ανθρώπους. Με μια ποικιλία μέσων, τόσο στο διαδίκτυο όσο και εκτός σύνδεσης, προσπαθούν να εξαπατήσουν ανυποψίαστους χρήστες (π.χ. υπαλλήλους), ώστε να θέσουν σε κίνδυνο την ασφάλειά τους, να μεταφέρουν χρήματα ή να δώσουν ευαίσθητες πληροφορίες (π.χ. κωδικούς πρόσβασης). Σε ένα μεγάλο ποσοστό η επιτυχία αυτής της απειλής οφείλεται στο ανθρώπινο λάθος ,μιας και πρόκειται για κάποιου είδους ψυχολογικής χειραγώγησης, που την καθιστά συνήθη ευπάθεια ενός isolated ή logical air-gapped δικτύου.

[4] Ενημερώσεις λογισμικού με αδύναμα-τρωτά σημεία.
[5] Είναι μια ετήσια λίστα που συντάσσεται και δημοσιεύεται από το περιοδικό Fortune και κατατάσσει τις 500 από τις μεγαλύτερες εταιρείες των Ηνωμένων Πολιτειών με βάση τα συνολικά έσοδα για τα αντίστοιχα οικονομικά έτη.

Υπάρχουν αρκετοί διαφορετικοί τύποι social engineering threats, ωστόσο θα γίνει αναφορά στον βασικότερο και πιο επικίνδυνο, που μπορεί να προκαλέσει σημαντική ζημιά σε εταιρείες και οργανισμούς που γίνονται στόχοι, κυρίως για τα ευαίσθητα δεδομένα που διαθέτουν. Το phishing λοιπόν, ή ηλεκτρονικό «ψάρεμα» είναι ο πιο συνηθισμένος τύπος διαδικτυακής απάτης που περιλαμβάνει την εξαπάτηση ατόμων, προς όφελος ενός φαινομενικά έμπιστου επιτιθέμενου. Μπορεί να γίνει κυρίως μέσω:

- **email,** όπου θα εμπεριέχεται link πίσω από το οποίο θα κρύβεται κακόβουλη ιστοσελίδα ή malware λογισμικό.
- **μέσων κοινωνικής δικτύωσης**, με μήνυμα όπου το περιεχόμενό του θα επιδιώκει να μπερδέψει το θύμα, ώστε να ενεργήσει προς όφελος του αποστολέα.
- **κακόβουλων ιστοσελίδων** όπου παρουσιάζονται σχεδόν ίδιες με γνωστές που χρησιμοποιεί το θύμα, έχοντας μικροδιαφορές στο όνομα ή στην εμφάνιση που περνούν απαρατήρητες.

Στο κομμάτι του εταιρικού δικτύου ή μιας γενικότερης αλυσίδας επικοινωνίας μεταξύ υπαλλήλων και καταστημάτων, ένας συχνός τρόπος επικοινωνίας είναι τα email που ανταλλάσσονται μεταξύ clients ή εξωτερικών συνεργατών με υπαλλήλους ενός εσωτερικού δικτύου, ακόμα και μεταξύ των ίδιων των υπαλλήλων. Με τον τρόπο αυτό μία phishing email επίθεση, που θα παρουσιάσουμε στη συνέχεια, μπορεί να ξεγελάσει τον υπάλληλο και να μολύνει τον εταιρικό υπολογιστή του με malware. Είναι τρεις τύποι phishing email attack:

- **Clone phishing**, όπου ένα email, που φαίνεται να προέρχεται από έναν αξιόπιστο αποστολέα, προέρχεται από malicious actor. Το μήνυμα θα περιέχει συχνά έναν σύνδεσμο προς έναν κλωνοποιημένο ιστότοπο, παρόμοιο με τον αρχικό και θα ζητάει από τον χρήστη να εισαγάγει τα credentials της σύνδεσής του, τα οποία θα κλέψει ο εισβολέας.
- **CEO fraud**, ένας τύπος απάτης κατά την οποία ο απατεώνας παρουσιάζεται ως Διευθύνων Σύμβουλος ή άλλο υψηλόβαθμο στέλεχος για να ξεγελάσει τους υπαλλήλους, ώστε να του παράσχουν εμπιστευτικές πληροφορίες. Θα επιδιώξει να επικοινωνήσει με τα θύματα μέσω BEC (business email compromise), τηλεφώνου ή μέσων κοινωνικής δικτύωσης και θα χρησιμοποιήσει τη θέση και την επιρροή που έχει σε αυτά, ώστε να πειστούν για την ταυτότητά του.

  Το BEC είναι ένας τύπος κυβερνοεπίθεσης όπου οι εισβολείς χρησιμοποιούν email για να εξαπατήσουν τους υπαλλήλους να τους μεταφέρουν ευαίσθητες πληροφορίες της εταιρείας. Οι επιθέσεις BEC πραγματοποιούνται συχνά με πλαστογράφηση της

διεύθυνσης ηλεκτρονικού ταχυδρομείου ενός ανώτερου στελέχους ή άλλου αξιόπιστου ατόμου σε έναν οργανισμό για να κερδίσουν την εμπιστοσύνη του θύματος[6].

3.4 Advanced Persistent Threat

Απόρροια των προηγούμενων attack vectors (stealthy threat actor) είναι η επονομαζόμενη Advanced Persistent Threat (APT), μία επίθεση κατά την οποία ο εισβολέας δημιουργεί και διατηρεί μια παράνομη, μακροχρόνια παρουσία σε ένα δίκτυο, ένα foothold, προκειμένου να εξάγει πληροφορίες και εξαιρετικά ευαίσθητα δεδομένα. Λόγω της μεγάλης προσπάθειας που απαιτείται και της δυσκολίας που έχει για να επιτύχει μία τέτοια επίθεση, οι στόχοι που επιλέγονται είναι είτε εταιρείες κολοσσοί, είτε κυβερνητικά – στρατιωτικά δίκτυα.

Η APT είναι μια μέθοδος επίθεσης που πρέπει να λαμβάνεται υπόψιν από τους cybersecurity engineer κάθε επιχείρησης. Ακόμη και οι μικρομεσαίες επιχειρήσεις, ειδικά εκείνες που αποτελούν supply-chain μιας μεγάλης εταιρείας, δεν πρέπει να αγνοήσουν αυτό το είδος επίθεσης μιας και οι εισβολείς τις χρησιμοποιούν ως σκαλοπάτι για να επιτεθούν στον τελικό τους στόχο. Μία APT επίθεση περνά από πέντε στάδια μέχρι να πετύχει διαρκή σύνδεση στο εκάστοτε σύστημα:

1. **Gain Access** – οι εγκληματίες του κυβερνοχώρου συνήθως αποκτούν είσοδο μέσω ενός μολυσμένου αρχείου (*threat actor*), phishing emails (*social engineering*) ή μιας ευπάθειας σε εφαρμογή (*supply-chain*) για την εισαγωγή malware σε ένα air-gapped δίκτυο-στόχο.
2. **Establish a Foothold** – με την εισαγωγή του malware αρχείου τους επιτρέπεται η δυνατότητα δημιουργίας backdoors και tunnels απ’ όπου μπορούν να κυκλοφορούν στα συστήματα απαρατήρητοι. Συνήθως το malware χρησιμοποιεί τεχνικές rewriting code για να βοηθήσει τους hackers να καλύψουν τα ίχνη τους.
3. **Deepen Access** – κατά την είσοδό τους στο σύστημα, οι εισβολείς, χρησιμοποιούν password cracking τεχνικές για να αποκτήσουν πρόσβαση σε administrator rights, ώστε να μπορούν να ελέγχουν μεγαλύτερο μέρος του συστήματος και να έχουν ακόμη μεγαλύτερα επίπεδα πρόσβασης.
4. **Move Laterally** – με administrator rights οι hackers μπορούν να μετακινούνται κατά βούληση και να επιχειρούν να αποκτήσουν πρόσβαση και σε άλλους servers, routers και air-gapped systems του δικτύου.

[6] https://www.enisa.europa.eu/topics/incident-response/glossary/what-is-social-engineering

5. **Look, Learn and Remain** – μέσα από το σύστημα, οι εισβολείς αποκτούν πλήρη κατανόηση του τρόπου λειτουργίας του και των τρωτών σημείων του, επιτρέποντάς τους να συλλέγουν τις πληροφορίες που θέλουν. Οι hacker μπορούν να επιχειρήσουν να διατηρήσουν αυτή τη διαδικασία μόνιμα (ενδεχομένως επ' αόριστο) ή να αποσυρθούν μόλις επιτύχουν έναν συγκεκριμένο στόχο. Συχνά αφήνουν μια backdoor ανοιχτή για να έχουν ξανά πρόσβαση στο σύστημα στο μέλλον.

ΚΕΦΑΛΑΙΟ 4ο : MALWARE & ΤΡΟΠΟΙ ΠΡΟΣΒΟΛΗΣ

Στο προηγούμενο κεφάλαιο αναπτύχθηκαν οι πιθανοί τρόποι διείσδυσης και μόλυνσης ενός air-gapped υπολογιστή, server και δικτύου γενικότερα μέσα σε μια εταιρεία η έναν οργανισμό. Κοινός παρονομαστής όλων αυτών των τεχνικών και επιθέσεων είναι η εμφύτευση malware στο σύστημα, είτε η επιχείρηση διαθέτει physical, isolated ή logical air-gapped network. Σε αυτό το κεφάλαιο θα μελετηθούν και θα παρουσιασθούν τα διάφορα κακόβουλα λογισμικά που κατά καιρούς έχουν παραβιάσει air-gapped δίκτυα, το πώς έχουν φτάσει στην άντληση ευαίσθητης πληροφορίας και δεδομένων, και με ποιες τεχνικές αυτά τα δεδομένα έχουν περάσει στον τελικό κακόβουλο χρήστη.

4.1 Ιστορικά επιβεβαιωμένα malicious frameworks

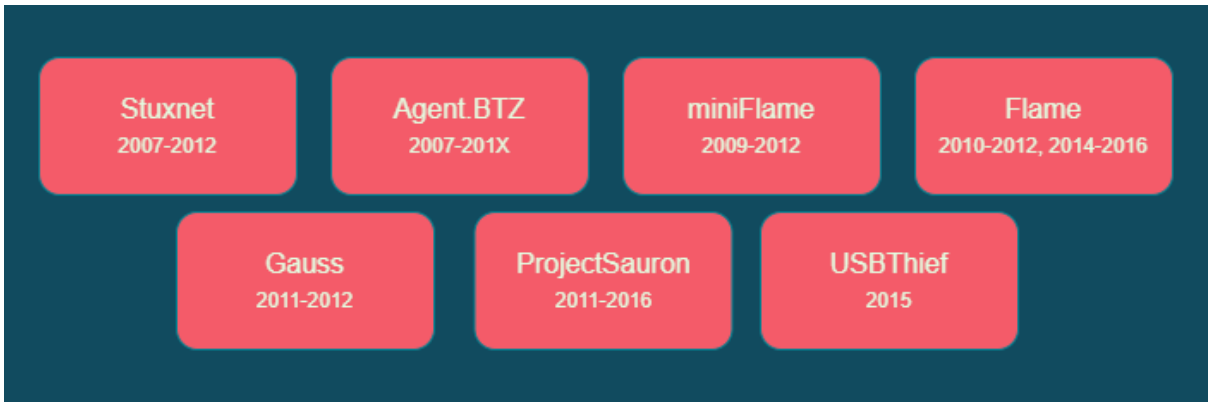
Σύμφωνα με στοιχεία που παρουσίασε το 2021 η εταιρεία ESET[7], ο συνολικός αριθμός των γνωστών malicious frameworks που παραβίασαν air-gapped δίκτυα ανά τον κόσμο έφτασε στα δεκαεφτά (17), από τις αρχές του 2005 μέχρι σήμερα. Θέλοντας να βελτιωθεί η ασφάλεια air-gapped δικτύων, αλλά και οι ικανότητες των μηχανικών ασφαλείας στο να ανιχνεύουν και να καταπολεμούν μελλοντικές επιθέσεις, είναι φρόνιμο να γίνει επανεξέταση αυτών των frameworks και κατηγοριοποίησή τους σε ομάδες.

Σημαντικός παράγοντας, όπως προαναφέρθηκε, αποτέλεσαν και αποτελούν οι threat actors που ευθύνονται για τα επόμενα κακόβουλα frameworks σχεδιασμένα με την APT τεχνική (μακροχρόνια παρουσία στο δίκτυο). Μαζί με ορισμένα frameworks ονοματίζονται και οι γνωστοί threat actors που βρίσκονται από πίσω:

[7] Γνωστή εταιρεία λογισμικού που ειδικεύεται στην κυβερνοασφάλεια με παροχή software σε πάνω από 200 χώρες.

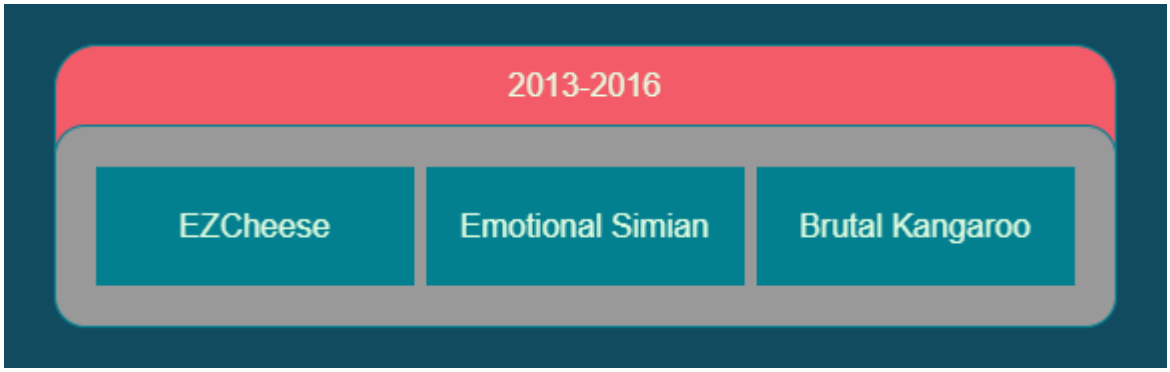
Εικόνα 4 Malicious frameworks & well-known threat actors

Παρουσιάζεται άλλη μία κατηγορία frameworks για τα οποία η απόδοση σε κάποιο φυσικό πρόσωπο ή οργάνωση ήταν αμφιλεγόμενη και έτσι δεν γνωρίζουμε τους υπαίτιους.



Εικόνα 5 Malicious frameworks χωρίς απόδοση σε threat actors

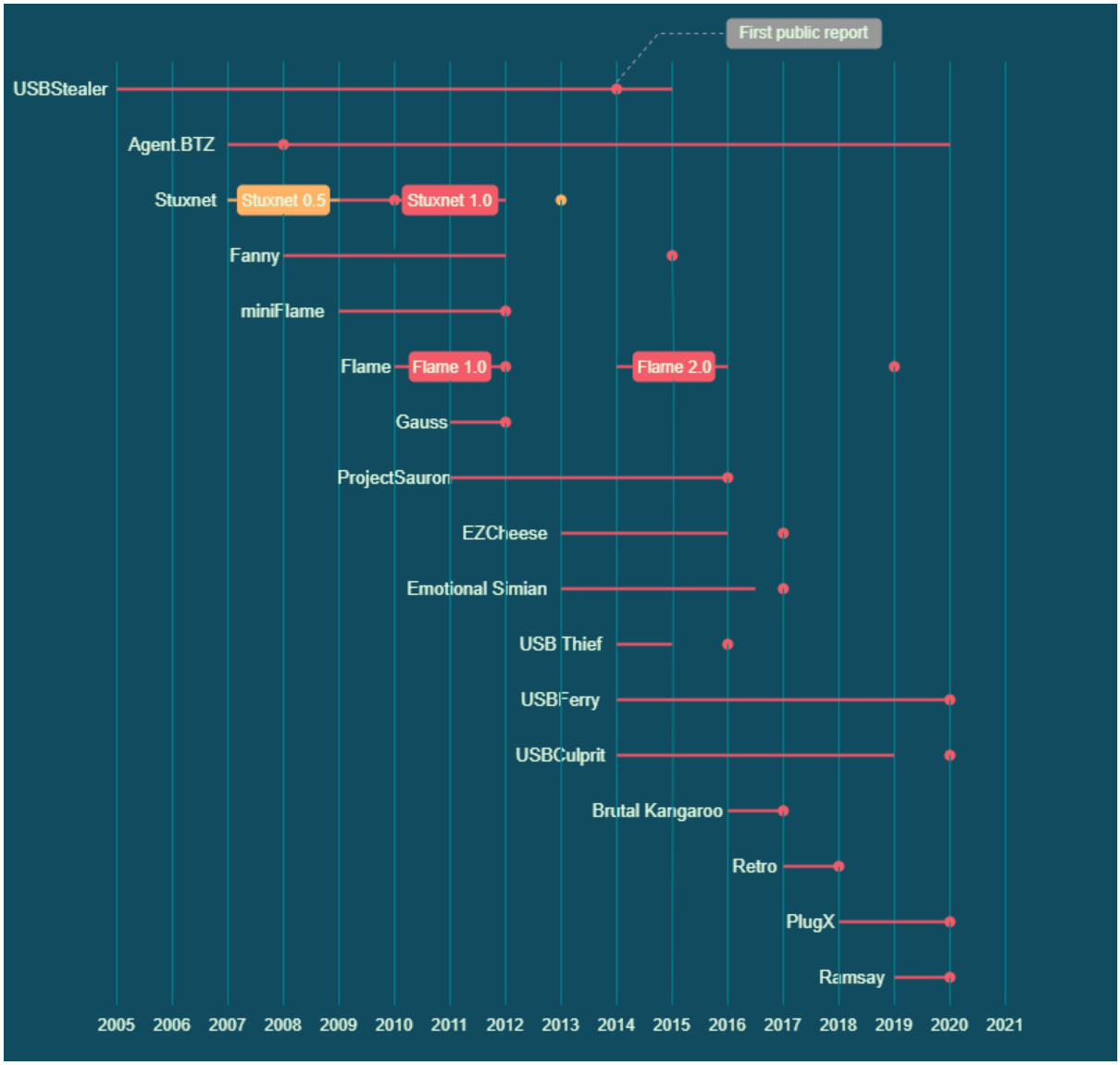
Τέλος παρουσιάζεται μία τριλογία frameworks ,τα οποία ήρθαν στο φως μέσω του WikiLeaks[8] και των αποδεικτικών εγγράφων Vault 7[9], και περιγράφεται ότι ήταν σε λειτουργία σε ένα χρονικό εύρος από το 2013 έως το 2016:



Εικόνα 6 Malicious frameworks documented in the Vault 7 leak

Παρά την ποικιλία των threat actors πίσω από τα frameworks, όλοι είχαν σαν κοινό σκοπό την κατασκοπεία. Ακόμη και το Stuxnet, γνωστότερο για τις δυνατότητες δολιοφθοράς του, συνέλεξε πληροφορίες για το λογισμικό Simatic Step 7 της Siemens. Λόγω της φύσης του στόχου του και των δυνατοτήτων του να λειτουργεί και να διαδίδεται, το Stuxnet αναφέρεται συχνά ως το πρώτο κακόβουλο λογισμικό που έχει σχεδιαστεί για να επιτίθεται σε air-gapped συστήματα. Ωστόσο, έρευνα που δημοσιεύτηκε χρόνια μετά την ανακάλυψη του Stuxnet προσδιόρισε με εύλογη σιγουριά ότι ένα δείγμα του Sednit's USBStealer χρονολογείται από το 2005[10]. Το σχήμα 7 δείχνει ιστορικά την περίοδο δραστηριότητας κάθε framework, μαζί με την χρονιά του αντίστοιχου πρώτου δημόσιου report. Αυτό είναι επίσης μια ένδειξη του πόσο δύσκολο είναι να εντοπιστεί ο κάθε τύπος framework.

[8] Διεθνής μη κερδοσκοπικός οργανισμός που δημοσιεύει εμπιστευτικές πληροφορίες και απόρρητα δεδομένα που προέρχονται από ανώνυμες πηγές.
[9] Μία σειρά αρχείων που δημοσιεύτηκαν από το WikiLeaks τον Μάρτιο του 2017 και περιγράφουν λεπτομερώς τις δραστηριότητες και δυνατότητες της CIA στην εκτέλεση ηλεκτρονικής επιτήρησης και κυβερνοπολέμου.
[10] J. Calvet, “Sednit Espionage Group Attacking Air Gapped Networks”. Available: https://www.welivesecurity.com/2014/11/11/sednit-espionage-group-attacking-air-gapped-networks/



Εικόνα 7 Περίοδος δραστηριότητας όλων των γνωστών frameworks

Το χρονοδιάγραμμα υπογραμμίζει ένα σημαντικό σημείο, ότι η πλειοψηφία των frameworks ήταν ενεργά για πολλά χρόνια πριν γίνουν αντιληπτά, αναλυθούν και αναφερθούν δημόσια.

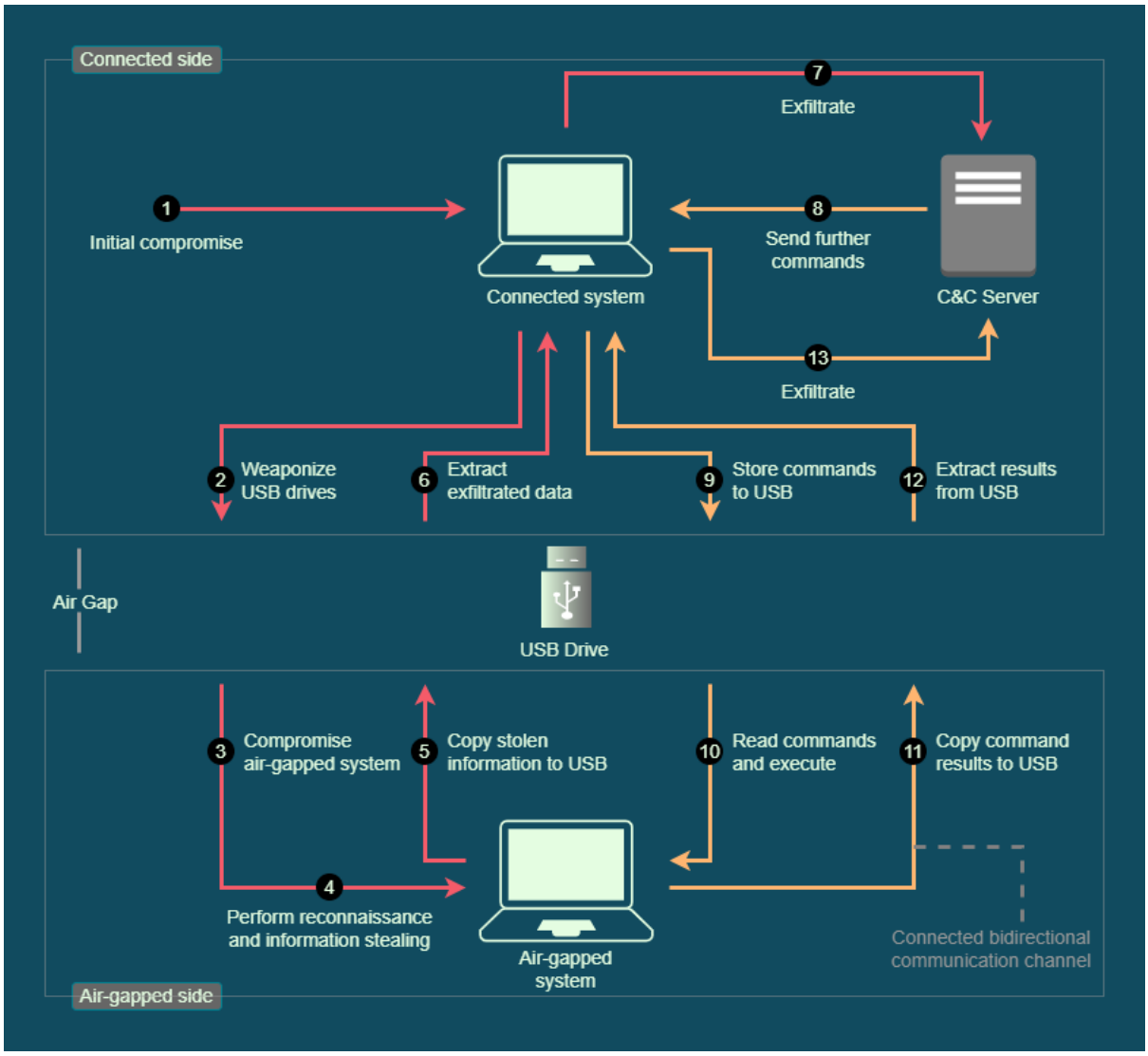
4.2 Ανάλυση malware & frameworks

Η επίθεση και παραβίαση συστημάτων σε air-gapped δίκτυα απαιτεί από τους εισβολείς την ανάπτυξη ικανοτήτων που επιτρέπουν στα εργαλεία τους να επικοινωνούν μέσω ασυνήθιστων καναλιών. Άξιο αναφοράς είναι ότι οι επιθέσεις δεν γίνονται όλες με τον ίδιο τρόπο και, στην πραγματικότητα, δεν υπάρχει ακριβής ορισμός του “air-gapped malware” από τεχνικής οπτικής. Ωστόσο σε μία προσπάθεια να οριστεί ένα air-gapped network malware ή ένα σύνολο malware στοιχείων που δρουν μαζί (framework), είναι η υλοποίηση ενός εκτός

σύνδεσης, κρυφού μηχανισμού επικοινωνίας μεταξύ ενός air-gapped συστήματος και του επιτιθέμενου, που μπορεί να είναι είτε αμφίδρομος (εντολή & απόκριση), ή μονής κατεύθυνσης (εξαγωγή δεδομένων). Για να μελετηθούν τα frameworks σωστά έγινε διαχωρισμός τους σε δύο γενικές κατηγορίες: σε σύνδεση και εκτός σύνδεσης.

4.2.1 Connected Frameworks

Τα περισσότερα frameworks είναι κατασκευασμένα ώστε να παρέχουν πλήρως απομακρυσμένη σύνδεση end-to-end μεταξύ του εισβολέα και των παραβιασμένων air-gapped συστημάτων. Αυτά αποκαλούνται «connected frameworks» και το γενικό σχήμα λειτουργίας τους δίνεται στην εικόνα 8.



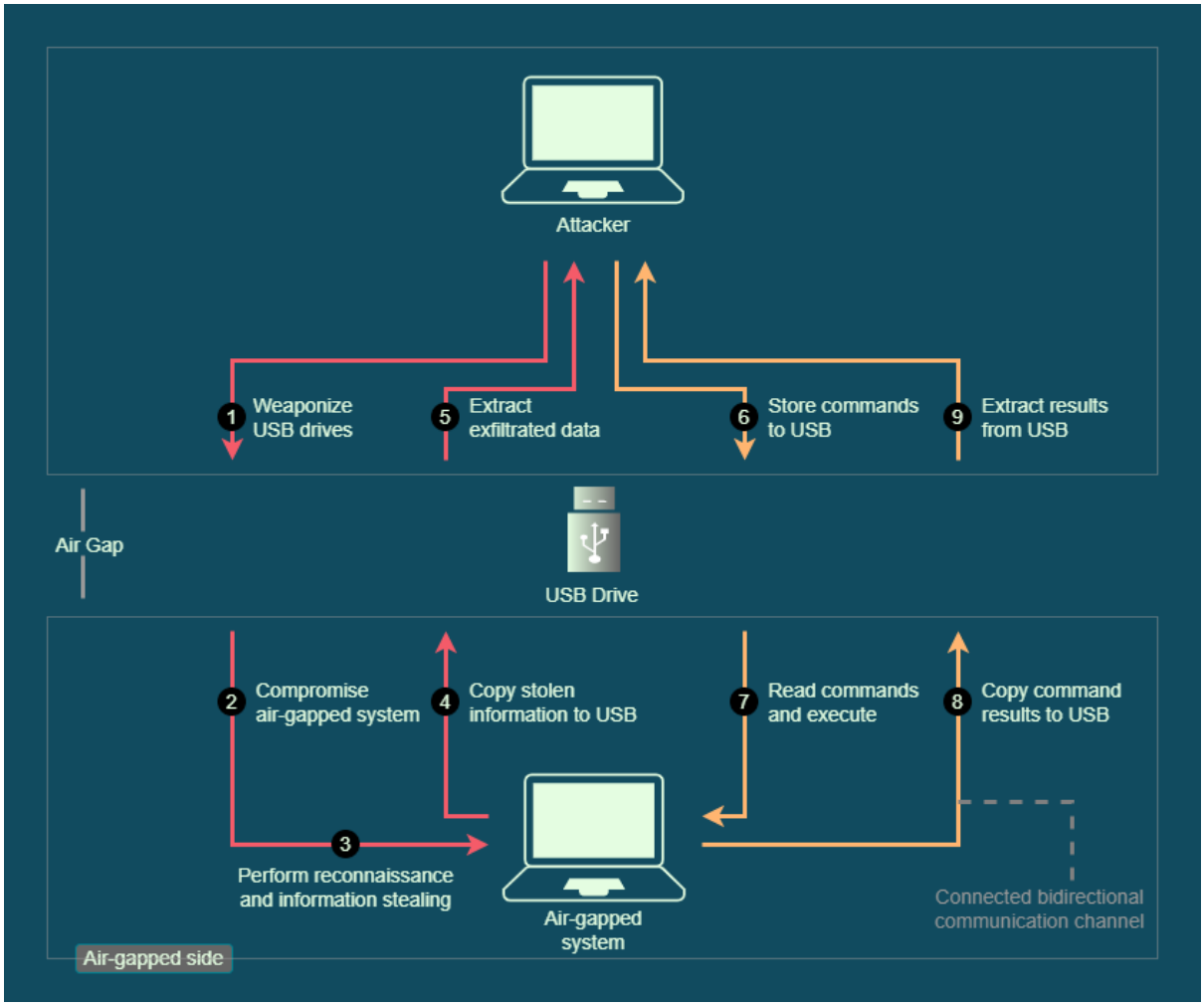
Εικόνα 8 Σύνολο συσκευών και ενεργειών ενός connected framework σχεδιασμένο για επιθέσεις σε air-gapped δίκτυα

Σε αυτό το σενάριο, η επίθεση ξεκινά στοχεύοντας ένα σύστημα συνδεδεμένο στο Διαδίκτυο που χρησιμοποιείται παράλληλα με ένα air-gapped δίκτυο (1). Μόλις παραβιαστεί αυτό το σύστημα, χρησιμοποιείται για την εισαγωγή σε USB drives malicious λογισμικό και ειδικό μηχανισμό ώστε να μπορέσει να παραβιάσει τον επόμενο στόχο: το air-gapped σύστημα (2). Αυτό επιτυγχάνεται τις περισσότερες φορές μιας και USB μονάδες χρησιμοποιούνται για τη μεταφορά πληροφοριών μεταξύ των δύο πλευρών, από ανυποψίαστο υπάλληλο-θύμα (3). Το malware που λειτουργεί στο air-gapped σύστημα συνοδεύεται συνήθως από αναγνώριση και κλοπή πληροφορίας (4), των οποίων η έξοδος αποθηκεύεται ξανά σε μονάδα USB (5). Όταν η μονάδα USB φτάσει ξανά το παραβιασμένο συνδεδεμένο σύστημα, τα περιεχόμενά του εξάγονται (6) και τα δεδομένα μεταφέρονται στον εισβολέα μέσω Διαδικτύου (7).

Ορισμένα frameworks προχωρούν ένα βήμα παραπέρα και υποστηρίζουν ένα πρωτόκολλο αμφίδρομης επικοινωνίας. Μέσω ενός παραβιασμένου συστήματος της συνδεδεμένης πλευράς, ο εισβολέας μπορεί να στέλνει εντολές στο malware που είναι τοποθετημένο στο air-gapped δίκτυο· αυτό γίνεται μέσω ενός κρυφού καναλιού επικοινωνίας που τοποθετείται συχνά σε μονάδα USB (8 /9 /10 /11 /12 /13). Αυτά είναι και τα πιο ισχυρά frameworks, που παρέχουν στους επιτιθέμενους τη δυνατότητα εκτέλεσης αυθαίρετου κώδικα μέσα σε air-gapped δίκτυα.

4.2.2 Offline Frameworks

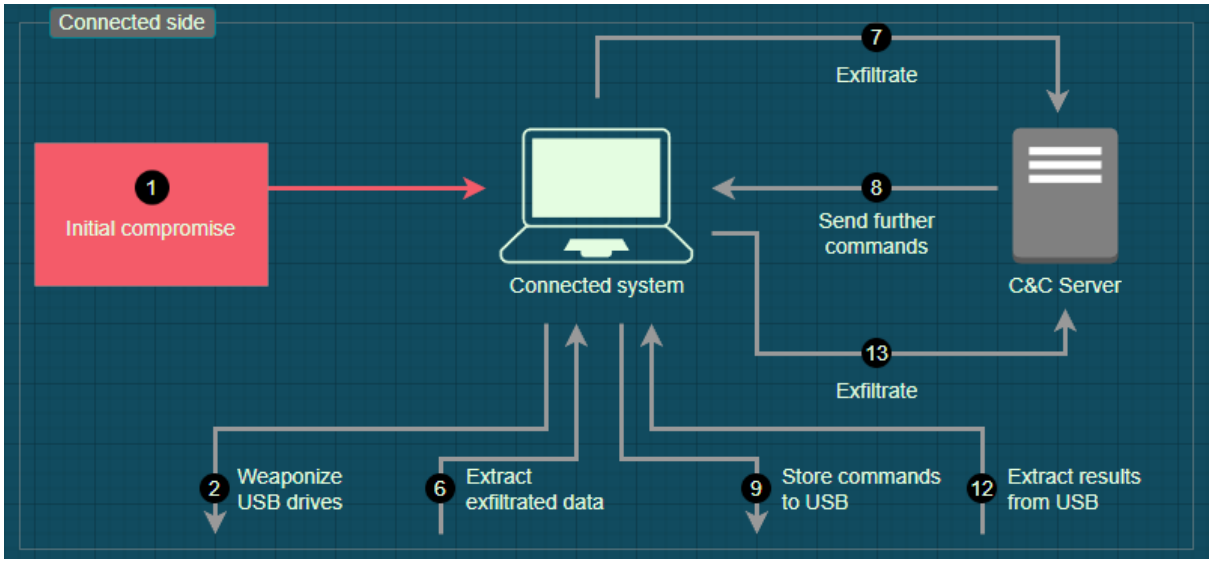
Στις άλλες, πιο σπάνιες περιπτώσεις όπως του Ramsay και USBThief, το σενάριο επίθεσης δεν περιλαμβάνει καθόλου συστήματα συνδεδεμένα με το Διαδίκτυο. Αυτά ονομάζονται «offline frameworks» και για να έχουν επιτυχία είναι απαραίτητη η παρουσία ατόμου (threat actor) εντός του air-gapped δικτύου ώστε να προετοιμάσει την αρχική κακόβουλη μονάδα USB (2), να εκτελέσει το malware στο σύστημα (3), να εξαγάγει τα δεδομένα που έχουν συλλεχθεί από τη μονάδα δίσκου (6) και να αποστείλει πρόσθετες εντολές στην air-gapped πλευρά (9). Η Εικόνα 9 δείχνει πόσο απλοποιείται το λειτουργικό σχήμα, τουλάχιστον από την οπτική του malware:



Εικόνα 9 Σύνολο συσκευών και ενεργειών ενός offline framework σχεδιασμένο για επιθέσεις σε air-gapped δίκτυα

4.3 Μέσα εκτέλεσης συνδεδεμένης πλευράς

Για connected frameworks, το πρώτο βήμα για την επιτυχή παραβίαση air-gapped δικτύου είναι ένα foothold στο σύστημα που διαθέτει σύνδεση στο Διαδίκτυο, όπως στην εικόνα 10. Όταν πρόκειται για APT επιθέσεις δεν είναι πάντα δυνατό να γνωρίζει κάποιος πώς συνέβη, αν και από τις περιπτώσεις που αναφέρθηκαν, οι μέθοδοι που παρατηρούνται είναι αρκετά γνώριμοι: email με malicious συνημμένα αρχεία, links, και USB worms. Όλες αυτές συνοψίζονται στον Πίνακα 1.



Εικόνα 10 Παραβίαση της online πλευράς του συστήματος (μέρος Εικόνας 8)

Frameworks	Compromise method	Details
USBStealer	Email	Υποψία spearphishing[11] με κακόβουλα συνημμένα αρχεία.
Agent.BTZ	USB worm	Μόλυνε με spyware USB μονάδες και εξαπλωνόταν χρησιμοποιώντας autorun για να αντιγράφει τον εαυτό του.
Stuxnet	Άγνωστη	Δεν είναι σαφές εάν η παραβίαση ξεκίνησε μέσω ενός συνδεδεμένου συστήματος ή εκτελέστηκε από ανθρώπινο χέρι με φυσική πρόσβαση.
Fanny	Άγνωστη	Πιθανώς να λήφθηκε και να εγκαταστάθηκε από άλλο component.
miniFlame	Άγνωστη	Πιθανώς να λήφθηκε και να εγκαταστάθηκε από το Gauss ή το Flame.
Flame	Άγνωστη	Υποψιάζεται ότι χρησιμοποιήθηκε σαν exploit για αρχική παραβίαση και καταγραφή οπτικοακουστικού υλικού υπολογιστών σημαντικών ανυποψίαστων θυμάτων.

[11] Στοχευμένο email σε συγκεκριμένο άτομο, οργανισμό ή επιχείρηση με σκοπό την εγκατάσταση malware στον υπολογιστή του.

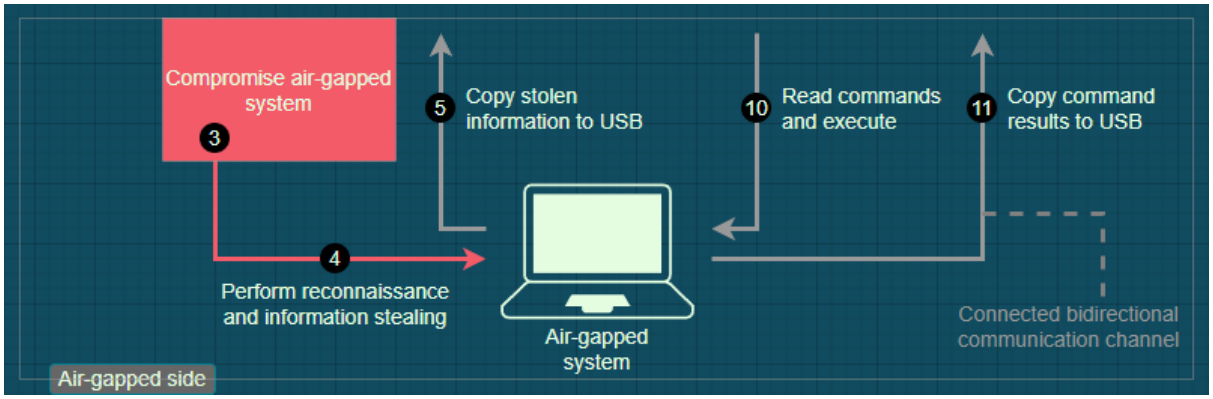
Gauss	Άγνωστη	Δεν έχει βρεθεί καμία λειτουργία αυτό-αντιγραφής επομένως είναι άγνωστη η λειτουργία διάδοσής του.
USBFerry	Email	Πρόγραμμα εγκατάστασης malware σε συνημμένο αρχείο.
USBCulprit	Email	Spearphishing με malicious έγγραφο RoyalRoad για εκμετάλλευση των days one (CVE-2012-0158, CVE-2017-11882, CVE-2018-0802), και στη συνέχεια το USBCulprit απορρίπτεται επιλεκτικά από τον εισβολέα.
Retro	Email	Spearphishing με έγγραφα που εκμεταλλεύονταν το CVE-2017-11882 glitch της Microsoft.
PlugX	Email	Spearphishing με ZIP αρχείο που περιείχε malicious LNK αρχείο.

Πίνακας 1 Τεχνικές που χρησιμοποιήθηκαν για παραβίαση της συνδεδεμένης πλευράς του δικτύου

Τα υπόλοιπα frameworks (ProjectSauron, EZCheese, Emotional, Simian, USBCulprit, USBThief, Brutal Kangaroo, Ramsay) δεν συμπεριλαμβάνονται καθώς ανήκουν στα offline.

4.4 Μέσα εκτέλεσης air-gapped πλευράς

Όλα τα frameworks που κατάφεραν να εγκαταστήσουν malware μέσα σε συστήματα air-gapped δικτύων έχουν ένα κοινό χαρακτηριστικό: χρησιμοποίησαν weaponized USB μονάδες. Η κύρια διαφορά μεταξύ connected και offline frameworks είναι ο τρόπος που γίνεται αυτό. Τα πρώτα, συνήθως αναπτύσσουν ένα component στο online σύστημα που θα παρακολουθεί το εισαγωγή νέων USB μονάδων και αυτόματα τοποθετεί το malicious component που χρειάζεται για την παραβίαση. Τα offline frameworks, από την άλλη πλευρά, βασίζονται στο ότι ο εισβολέας weaponizing σκόπιμα τη δική του USB μονάδα. Το ενδιαφέρον εδώ είναι οι διαφορετικές τεχνικές που έχουν χρησιμοποιηθεί με τον καιρό από αυτά τα frameworks, ώστε να καταφέρουν να εκτελέσουν το περιεχόμενό τους. Μπορούν να τοποθετηθούν σε τρεις μεγάλες κατηγορίες.



Εικόνα 11 Παραβίαση της offline πλευράς του συστήματος (μέρος Εικόνας 8)

4.4.1 Αυτόματη εκτέλεση

Η εκτέλεση κακόβουλου κώδικα απλώς με την σύνδεση malicious USB μονάδας σε υπολογιστή είναι η πιο αποτελεσματική τεχνική παραβίασης ενός air-gapped δικτύου.

Εκμετάλλευση τρωτών σημείων των LNK αρχείων

Τα malicious LNK αρχεία χρησιμοποιούνται συνήθως για την ενεργοποίηση και εκμετάλλευση μιας ευπάθειας παλιών components των Windows, όπως το Windows Shell, που επιτρέπουν στο malware την απομακρυσμένη εκτέλεση κώδικα (RCE) με μόνη ενέργεια την προβολή του αρχείου LNK στο Windows Explorer. Με την πιο διάσημη ευπάθεια να είναι χωρίς αμφιβολία το CVE-2010-2568, γνωστό και ως «Stuxnet LNK exploit», ανακαλύφθηκε αργότερα ότι το Fanny είχε χρησιμοποιήσει πολύ πριν αυτό το exploit και μάλιστα μετά την κυκλοφορία patch της Microsoft το 2010, τα Flame, Gauss και miniFlame frameworks συνέχισαν ακόμα να την χρησιμοποιούν. Οι διαρροές του Vault7 αποκάλυψαν επίσης ότι η σουίτα εργαλείων Brutal Kangaroo χρησιμοποιούσε δύο exploits που σχετίζονται με LNK file: το CVE-2015-0096 και ένα δεύτερο άγνωστο.

Τα τρωτά σημεία που σχετίζονται με LNK file είναι ένας εξαιρετικά ισχυρός τρόπος διάδοσης malware επειδή επιτρέπουν την εκτέλεση κώδικα χωρίς αλληλεπίδραση με τον χρήστη κατά την εισαγωγή USB μονάδας σε ευάλωτα συστήματα. Ο Πίνακας 2 δείχνει ότι ενώ μόνο δύο τέτοια τρωτά σημεία έχουν γίνει αντικείμενο εκμετάλλευσης επιβεβαιωμένων επιθέσεων, δεν έχουν κάτι το ασυνήθιστο· σχεδόν δώδεκα έχουν ανακαλυφθεί και διορθωθεί από τη Microsoft τα τελευταία δέκα χρόνια, τέσσερα μόλις το 2020.

Release date	CVE	Vulnerability name	Confirmed exploitation
02-08-2010	CVE-2010-2568	Shortcut Icon Loading Vulnerability (remote code execution)	Fanny, Stuxnet, Flame, Gauss, miniFlame
10-03-2015	CVE-2015-0096	DLL Planting Remote Code Execution Vulnerability	Brutal Kangaroo (υποψία)
13-06-2017	CVE-2017-8464	LNK Remote Code Execution Vulnerability	Blacksquid, Lucifer, etc.
14-08-2018	CVE-2018-8345	LNK Remote Code Execution Vulnerability	
14-08-2018	CVE-2018-8346	LNK Remote Code Execution Vulnerability	
13-08-2019	CVE-2019-1188	LNK Remote Code Execution Vulnerability	
10-09-2019	CVE-2019-1280	LNK Remote Code Execution Vulnerability	
11-02-2020	CVE-2020-0729	LNK Remote Code Execution Vulnerability	
10-03-2020	CVE-2020-0684	LNK Remote Code Execution Vulnerability	
09-06-2020	CVE-2020-1299	LNK Remote Code Execution Vulnerability	
14-07-2020	CVE-2020-1421	LNK Remote Code Execution Vulnerability	

Πίνακας 2 Ιστορικό RCE ευπαθειών σχετικά με LNK αρχεία

4.4.2 Μη-αυτόματη εκτέλεση (ενεργοποίηση εν αγνοία)

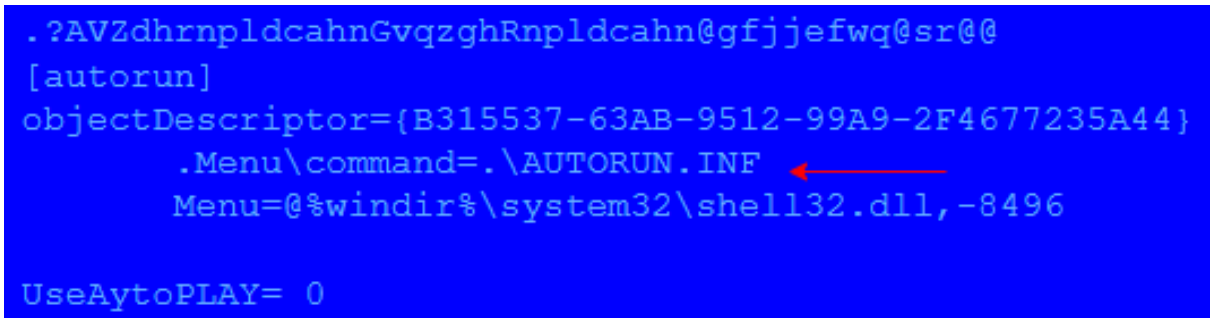
Σε αυτά τα σενάρια, η εκτέλεση του κακόβουλου κώδικα εξαρτάται από την εξαπάτηση ενός ανυποψίαστου νόμιμου χρήστη ώστε να την πραγματοποιήσει.

Χρήση της AutoRun/AutoPlay δυνατότητας των Windows

Πρόκειται για ένα παλιό, αλλά αρκετά πετυχημένο, μέσο εκτέλεσης που επέτρεψε σε πολλά είδη malware να εξαπλωθούν μέσω USB και network μονάδων. Ενώ το AutoRun υπάρχει από τα Windows 95, οι όροι AutoRun και AutoPlay χρησιμοποιούνταν εναλλακτικά μέχρι τα Windows XP όταν και διαφοροποιήθηκαν:

- Το AutoRun εισήχθη στα Windows 95 με σκοπό να διευκολύνει την ενεργοποίηση της αυτόματης εκτέλεσης προγραμμάτων εγκατάστασης σε CD ακολουθώντας τις οδηγίες ενός αρχείου με όνομα autorun.inf. Αυτός ο μηχανισμός χρησιμοποιούνταν επίσης όταν ο χρήστης έκανε διπλό κλικ στη συντόμευση της μονάδας στην My Computer καρτέλα. Αργότερα ενεργοποιήθηκε και επεκτάθηκε στα Windows XP για την υποστήριξη άλλων τύπων αφαιρούμενων μέσων όπως USB και network μονάδων.
- Αν και μια πρωτόγονη μορφή AutoPlay υπήρχε στα Windows 95 και 98, ανανεώθηκε παρουσιάζοντας στον χρήστη ένα αναδυόμενο παράθυρο με μενού επιλογών για εύκολη πρόσβαση και αυτόματη εκκίνηση αρχείων κατά την εισαγωγή μιας συσκευής.

Αυτά είναι και τα χαρακτηριστικά που καταχράστηκαν τα frameworks όπως το USBStealer και το Agent.BTZ, καθώς και μία παλαιότερη έκδοση του Stuxnet που υλοποίησε ένα Flame component το οποίο εξόπλιζε τις μονάδες USB με malicious autorun.inf αρχείο που περιείχε τόσο το εκτελέσιμο Stuxnet όσο και AutoRun οδηγίες. Έτσι απενεργοποιούσε το AutoPlay για να αναγκάσει τον χρήστη να μεταβεί στο My Computer ή να χρησιμοποιήσει την εισαγωγή στην Εξερεύνηση των Windows. Εκεί, με το shell32.dll περνούσε μια πρόσθετη εντολή "Open" στο context menu και εάν το πιθανό θύμα έκανε κλικ σε αυτό ή διπλό κλικ στη συντόμευση της μονάδας δίσκου εκτελούταν το Stuxnet.



Εικόνα 12 Μέρος του Stuxnet autorun.inf αρχείου

```
[autorun]
open=
shell\open= Explore
shell\open\command= "System Volume Information\USBGuard.exe" install
shell\open\Default= 1
```

Εικόνα 13 Μέρος του USBStealer autorun.inf αρχείου χωρίς την απενεργοποίηση του AutoPlay

Το 2009 η Microsoft κυκλοφόρησε μια ενημέρωση που απενεργοποιούσε την λειτουργία AutoRun για μέσα εκτός από CD και DVD. Στα Windows 7/8/8.1/10/11 το AutoRun δεν υποστηρίζει την πλειονότητα των οδηγιών που επιτρέπουν την εκτέλεση malicious κώδικα μέσω αρχείων autorun.inf, με αποτέλεσμα να μην υπάρχουν πλέον προσαρμοσμένες επιλογές στο AutoPlay παράθυρο. Δεδομένων αυτών των περιορισμών, ορισμένα frameworks όπως τα Stuxnet, Flame, Gauss και miniFlame μεταπήδησαν στη χρήση zero και one day εκμεταλλεύσεων.

"Εμφύτευση" malicious αρχείων

Εκτός από το AutoRun/AutoPlay, ένας εισβολέας μπορεί να εγκαταστήσει ένα κακόβουλο εκτελέσιμο αρχείο ή αρχείο LNK στη μονάδα USB με τρόπο τέτοιον ώστε να δελεάσει τον χρήστη να το εκτελέσει.

Το Ramsay, για παράδειγμα, χρησιμοποίησε έναν trojanized installer για το 7zip, ενώ το USBThief χρησιμοποίησε DLL hijacking[12] στις νόμιμες εφαρμογές Firefox, Notepad++ και TrueCrypt. Το PlugX λειτουργούσε λίγο διαφορετικά καθώς απαιτούσε ενέργειες από τον χρήστη. Αποθήκευε ένα αντίγραφο του εαυτού του σε μονάδες USB στον φάκελο "RECYCLE.BIN", απέκρυπτε όλους τους υπάρχοντες φακέλους στο root της μονάδας και, στη συνέχεια, δημιουργούσε ένα LNK αρχείο για κάθε κρυφό φάκελο. Αυτή η τακτική διατηρούσε τον δίσκο καθαρό και έτσι ο κακόβουλος κώδικας εκτελούταν μόλις ένας ανυποψίαστος χρήστης προσπαθούσε να εισέλθει σε έναν από τους φακέλους.

Τέλος, οι εισβολείς μπορούν επίσης να τοποθετήσουν κακόβουλα έγγραφα του Office σε μονάδες USB. Το Ramsay χρησιμοποιούσε ειδικά διαμορφωμένα κακόβουλα έγγραφα RTF που εκμεταλλεύονταν δύο γνωστές αδυναμίες ώστε να εγκατασταθούν. Το Retro χρησιμοποίησε μια ελαφρώς διαφορετική προσέγγιση, σαρώνοντας μονάδες USB αναζητώντας υπάρχοντα έγγραφα του Word και στη συνέχεια μετατρέποντάς τα σε μορφή RTF με ένα exploit που ενεργοποιούσε ένα script αντιγραφής του αναγνωρισμένου component

[12] Είναι μέθοδος εισαγωγής κακόβουλου κώδικα σε μία εφαρμογή εκμεταλλευόμενη τον τρόπο με τον οποίον ορισμένες Windows εφαρμογές αναζητούν και φορτώνουν τις Dynamic Link Libraries (DLL).

στο local drive και εκτέλεσής του. Αυτή η τεχνική είναι λιγότερο πιθανό να εγείρει υποψίες μιας και αναμένεται η παρουσία εγγράφων σε μονάδες USB.

4.4.3 Μη-αυτόματη εκτέλεση (σκόπιμη ενεργοποίηση)

Αυτή η περίπτωση είναι παρόμοια με την προηγούμενη τεχνική. Ωστόσο, σε αυτή οι επιτιθέμενοι δεν θέλουν και δεν περιμένουν για το λάθος ενός ανυποψίαστου χρήστη αλλά βασίζονται σε έναν human actor για την ενεργοποίηση της εκτέλεσης του malware.

Στην περίπτωση του USBCulprit, το κακόβουλο λογισμικό δεν ήταν προσβάσιμο ή ορατό στους χρήστες και δεν υπήρχε μηχανισμός ενεργοποίησης, αποτρέποντας έτσι την τυχαία εκτέλεση. Σε άλλες περιπτώσεις, όπως του USBThief, το κακόβουλο λογισμικό αναπτυσσόταν με τρόπο που υποστήριζε την κρυφή εκτέλεση από threat actors· οι εισβολείς τοποθετούσαν σε μονάδες USB, εκδόσεις γνωστού λογισμικού και χρησιμοποιούσαν τεχνικές DLL hijacking ή DLL side-loading για την έμμεση εκτέλεση του malware στο σύστημα-στόχο.

	Αυτόματη εκτέλεση		**Μη-αυτόματη εκτέλεση (ενεργοποίηση εν αγνοία)**				**Μη-αυτόματη εκτέλεση (σκόπιμη ενεργοποίηση)**
	Malicious LNK	Malicious autorun.inf με ενεργοποίηση αυτόματης εκτέλεσης (AutoRun)	Trojanized/hijacked PE	Malicious Office documents	Malicious LNK	Malicious autorun.inf χειραγωγώντας το AutoPlay	
Connected frameworks							
USBStealer						X	
Agent.BTZ						X	
Stuxnet	X					X	
Fanny	X						
miniFlame	X						
Flame	X					X	
Gauss	X						
USBFerry						X	
USBCulprit							X

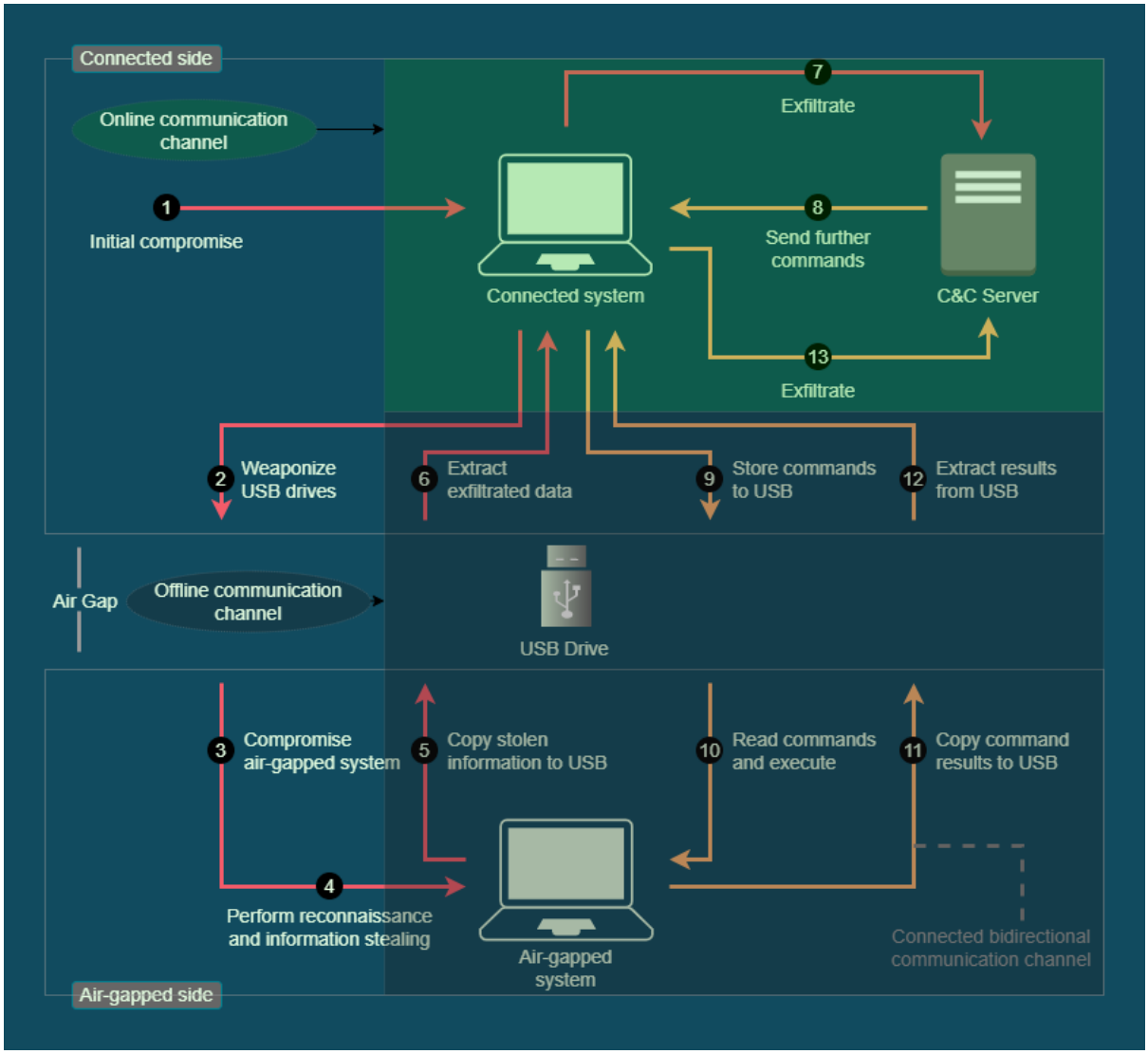
Retro				X			
PlugX					X		
Offline frameworks							
ProjectSauron							X *Hypothesis*
EZCheese	X						X
Emotional Simian	X						
USBThief			X				X
Brutal Kangaroo	X	X					X
Ramsay			X	X			X

Πίνακας 3 Τεχνικές παραβίασης πρώτης συσκευής air-gapped δικτύου

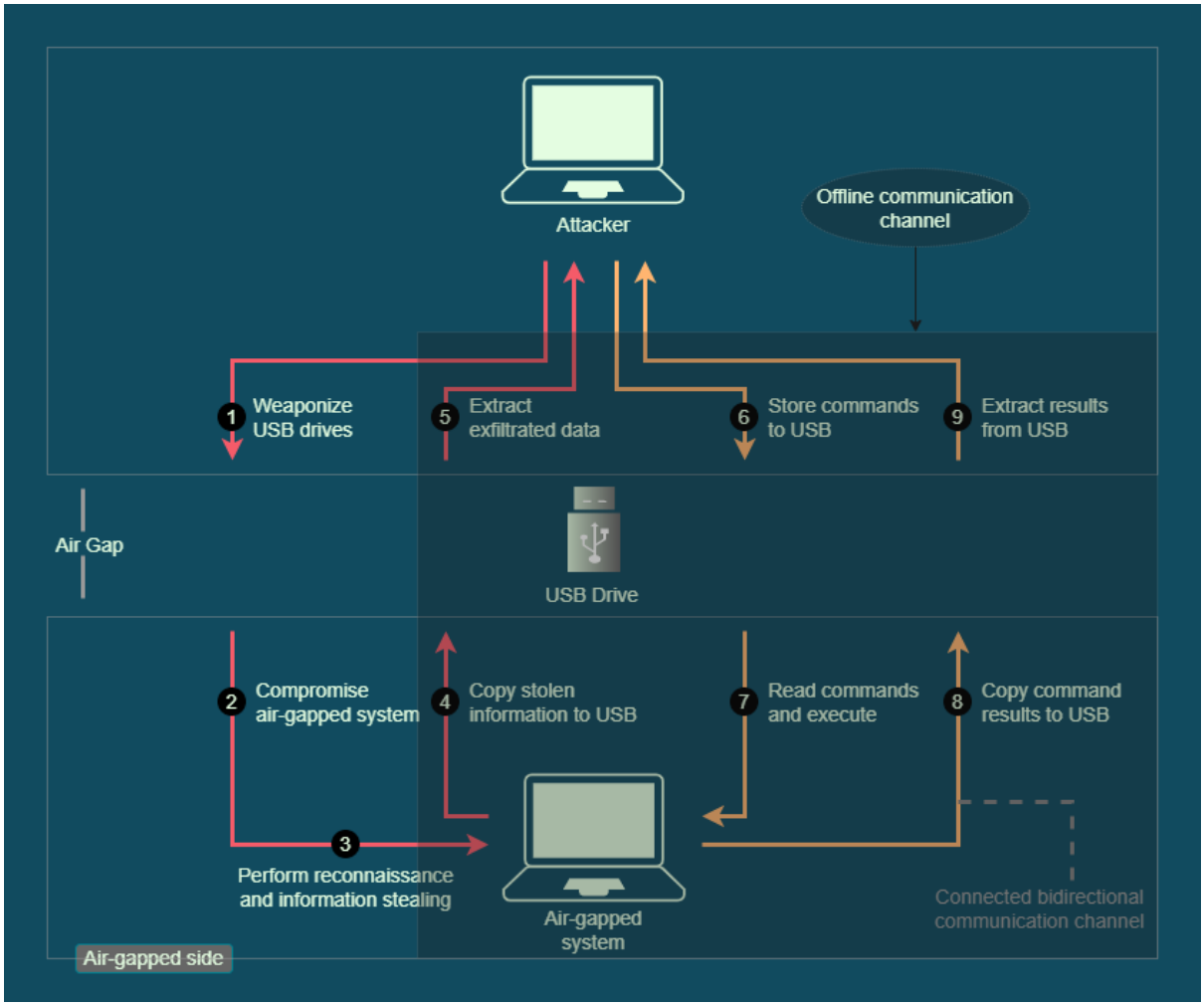
4.5 Κανάλια επικοινωνίας και διαρροής δεδομένων

Τα connected frameworks απαιτούν ένα online, παραδοσιακό C&C[13] κανάλι επικοινωνίας που συνδέει τον εισβολέα με τον παραβιασμένο κεντρικό υπολογιστή από τη συνδεδεμένη πλευρά και ένα εκτός σύνδεσης που συνδέει τον παραβιασμένο κεντρικό υπολογιστή με το air-gapped δίκτυο, όπως φαίνεται στην Εικόνα 14. Τα offline frameworks από την άλλη πλευρά, όπως στην Εικόνα 15, απαιτούν μόνο το τελευταίο.

[13] Από τις λέξεις command & control οι cybercriminals χρησιμοποιούν τέτοια κανάλια για να στέλνουν εντολές σε παραβιασμένα με malware συστήματα.



Εικόνα 14 Online και offline κανάλι επικοινωνίας στα connected frameworks



Εικόνα 15 Offline communication κανάλι επικοινωνίας στα offline frameworks

Online κανάλια

Ένα online κανάλι επικοινωνίας δεν διαφοροποιείται ως προς τα χαρακτηριστικά του όταν πρόκειται να χρησιμοποιηθεί για μεταφορά δεδομένων ενός air-gapped δικτύου και σε γενικές γραμμές το επίπεδο πολυπλοκότητας του είναι σχετικά ίδιο με το συνολικό επίπεδο των άλλων τμημάτων των ίδιων των frameworks.

Offline κανάλια

Η παρουσία ενός καναλιού επικοινωνίας εκτός σύνδεσης είναι το βασικό μέρος και ένας από τους στόχους ενός malware. Είναι ο τρόπος με τον οποίο ένα κακόβουλο λογισμικό θα παρακάμψει το στρώμα άμυνας του air-gap για να μεταφέρει πληροφορίες εντός και κυρίως εκτός από το δίκτυο-στόχο. Cybersecurity ερευνητές του Ben-Gurion Πανεπιστημίου του Negev έχουν παρουσιάσει μία ποικιλία τεχνικών που με φυσικά μέσα επιτρέπουν την μεταφορά πληροφοριών από air-gapped δίκτυα. Τα air-gapped **hidden channels**, όπως τα αποκαλούν, μπορούν να κατηγοριοποιηθούν ως ηλεκτρομαγνητικά, ακουστικά, θερμικά και

οπτικά και σχεδόν πάντα εφαρμόζονται πρωτόκολλα μονής κατεύθυνσης, δηλαδή οι πληροφορίες ρέουν από το παραβιασμένο air-gapped σύστημα στον εισβολέα και όχι το αντίστροφο:

- **Electromagnetic:** Πίσω το 1998, ο Kuhn και ο Anderson εισήγαγαν την επίθεση «Soft Tempest» που συμπεριλάμβανε κρυφή μετάδοση δεδομένων με χρήση ηλεκτρομαγνητικών εκπομπών από καλώδιο video[14]. Το AirHopper, που παρουσιάστηκε το 2014, είναι ένας τύπος κακόβουλου λογισμικού που στοχεύει στη διαρροή δεδομένων από air-gapped computers σε κοντινό κινητό τηλέφωνο δημιουργώντας σήματα FM radio signals από την κάρτα video[15]. Κακόβουλο λογισμικό GSMem, που παρουσιάστηκε το 2015, επιτρέπει τη διαρροή δεδομένων σε κυψελοειδείς συχνότητες μέσω ηλεκτρομαγνητικής εκπομπής, που παράγεται από το RAM bus του υπολογιστή[16]. Πιο πρόσφατα, ερευνητές παρουσίασαν το USBee που εκμεταλλεύεται τις ηλεκτρομαγνητικές παρεμβολές που δημιουργούνται από το USB[17]. Τέλος οι Matyunin, Szefer, Biedermann και Katzenbeisser κατάφεραν να χρησιμοποιήσουν τους αισθητήρες μαγνητικού πεδίου των κινητών συσκευών ως κρυφό κανάλι[18].
- **Sonic/Ultrasonic:** Οι μέθοδοι σχεδόν υπερήχων για air-gapped hidden channels συζητούνται σε μια σειρά ακαδημαϊκών έργων. Οι Hanspach και Goetz παρουσιάζουν μια μέθοδο για σχεδόν υπερηχητική κρυφή δικτύωση χρησιμοποιώντας ηχεία και μικρόφωνα σε φορητούς υπολογιστές[19]. Η έννοια της επικοινωνίας μέσω μη ακούσιων ήχων έχει εξεταστεί διεξοδικά από τους Lee, Kim και Yoon και έχει επίσης επεκταθεί για διαφορετικά σενάρια που χρησιμοποιούν φορητούς υπολογιστές και κινητά τηλέφωνα[20] [21]. Οι Guri, Solewicz, Daidakulov και Elovici εισήγαγαν τον Fansmitter και Disfiltration, νέες μέθοδοι που επιτρέπουν την εξαγωγή ακουστικών δεδομένων από υπολογιστές χωρίς

[14] M. G. Kuhn and R. J. Anderson, "Soft Tempest: Hidden data transmission using electromagnetic emanations", pp. 124-142, 1998.
[15] G. Mordechai, G. Kedma, A. Kachlon and Y. Elovici, "AirHopper: Bridging the air-gap between isolated networks and mobile phones using radio frequencies", pp. 58-67, 2014.
[16] M. Guri, A. Kachlon, O. Hasson, G. Kedma, Y. Mirsky and Y. Elovici, "GSMem: Data Exfiltration from Air-Gapped Computers over GSM Frequencies", 2015.
[17] https://github.com/funtenna
[18] N. Matyunin, J. Szefer, S. Biedermann and S. Katzenbeisser, "Covert channels using mobile device's magnetic field sensors", 2016.
[19] M. a. G. M. Hanspach, "On Covert Acoustical Mesh Networks in Air", 2014.
[20] V. T. M. t. C. A.-G. S. f. P. N. Attack, "Eunchong Lee; Hyunsoo Kim; Ji Won Yoon", pp. 187-199, 2015.
[21] S. J. O'Malley and K.-K. R. Choo, "Bridging the Air Gap: Inaudible Data Exfiltration by Insiders" in Americas Conference on Information Systems, 2014.

ηχεία ή υλικό ήχου[22] [23]. Οι προτεινόμενες μέθοδοι χρησιμοποίησαν ανεμιστήρες υπολογιστών και σκληρούς δίσκους για να παράγουν ακουστικά σήματα.

- **Thermal:** Το BitWhisper είναι ένα μοναδικό κρυφό κανάλι με διάκενο αέρα, που επιτρέπει αμφίδρομη κάλυψη επικοινωνία μεταξύ παρακείμενων υπολογιστών με διάκενο αέρα, χρησιμοποιώντας τις εκπομπές θερμότητας των υπολογιστών και τους ενσωματωμένους θερμικούς αισθητήρες των μητρικών καρτών των υπολογιστών[24].
- **Optical:** Στον οπτικό τομέα, οι Loughry and Umphress[25] και οι Sepetnitsky και Guri[26] συζητούν το κίνδυνοι σκόπιμης διαρροής πληροφοριών μέσω οπτικών σημάτων που αποστέλλονται από το πληκτρολόγιο και LED οθόνης. Εφάρμοσαν κακόβουλο λογισμικό που ελέγχουν τα LED τροφοδοσίας του πληκτρολογίου και της οθόνης μεταφορά δεδομένων σε απομακρυσμένη κάμερα. Το κύριο μειονέκτημα αυτών των μεθόδων είναι ότι είναι λιγότερες κρυφό: δεδομένου ότι τα LED του πληκτρολογίου και της οθόνης δεν αναβοσβήνουν συνήθως, οι χρήστες μπορούν εύκολα να το εντοπίσουν είδος επικοινωνίας. Οι Shamir et al έδειξαν πώς να δημιουργήσετε ένα κρυφό κανάλι με a κακόβουλο λογισμικό πάνω από το διάκενο αέρα χρησιμοποιώντας ένα λέιζερ που αναβοσβήνει και τυπικό εκτυπωτή all-in-one[27]. Ωστόσο, Αυτή η μέθοδος επίσης δεν είναι κρυφή και η επιτυχία της βασίζεται στην απουσία χρήστη. Πιο πρόσφατα, ο Lopes και ο Aranha[28] παρουσίασαν μια νέα προσέγγιση για τη διήθηση δεδομένων κενού αέρα χρησιμοποιώντας ένα κακόβουλο συσκευή αποθήκευσης που μεταδίδει δεδομένα μέσω υπέρυθρων LED που αναβοσβήνουν. Με αυτόν τον τρόπο επιθετικός μπορεί να διαρρεύσει ευαίσθητα δεδομένα που είναι αποθηκευμένα στη συσκευή, όπως διαπιστευτήρια και κρυπτογραφικά κλειδιά, στο α ταχύτητα 15 bit/s. Ο υπολογιστής δεν χρειάζεται να έχει μολυνθεί από κακόβουλο λογισμικό, αλλά αυτή η προσέγγιση το κάνει απαιτούν από τον εισβολέα να βρει έναν τρόπο να εισαγάγει το παραβιασμένο υλικό που έχει εμφυτευτεί με

[22] M. Guri, Y. Solewicz, A. Daidakulov and Y. Elovici, "Fansmitter: Acoustic Data Exfiltration from (Speakerless) Air-Gapped Computers", 2016.
[23] M. Guri, Y. Solewicz, A. Daidakulov and Y. Elovici, "DiskFiltration: Data Exfiltration from Speakerless Air-Gapped Computers via Covert Hard Drive Noise", 2016.
[24] M. Guri, G. Kedma, A. Kachlon and Y. Elovici, "AirHopper: Bridging the Air-Gap between Isolated Networks and Mobile Phones using Radio Frequencies", 2014.
[25] J. Loughry and A. D. Umphress, "Information leakage from optical emanations", pp. 262-289, 2002.
[26] V. Sepetnitsky, M. Guri and Y. Elovici:, "Exfiltration of Information from Air-Gapped Machines Using Monitor's LED Indicator", 2014.
[27] S. G. SC Magazine UK, "Light-based printer attack overcomes air-gapped computer security", 2014. Available: http://www.scmagazineuk.com/lightbased-printer-attack-overcomes-air-gapped-computer-security/article/377837/
[28] A. C. Lopes and D. F. Aranha, "Platform-agnostic low-intrusion optical data exfiltration", 2016.

υπέρυθρες LED στον οργανισμό. Ο Brasspup[29] έδειξε πώς να κρύβονται μυστικές εικόνες σε τροποποιημένη οθόνη LCD. Η μέθοδός του απαιτούσε την αφαίρεση του φίλτρου πόλωσης της οθόνης LCD γεγονός που το καθιστά λιγότερο πρακτικό για επιθέσεις στον πραγματικό κόσμο. Το VisiSploit[30] είναι ένα άλλο οπτικό μυστικό κανάλι στο οποίο διαρρέουν δεδομένα από την οθόνη LCD σε μια απομακρυσμένη κάμερα μέσω ενός λεγόμενου «αόρατη εικόνα». Με αυτήν τη μέθοδο, μια απομακρυσμένη κάμερα **μπορεί να ανακατασκευάσει έναν αόρατο κωδικό QR προβάλλεται στην οθόνη του** υπολογιστή.

Μέθοδοι	Παραδείγματα	Μέγιστο Bandwidth	Απόσταση
Ηλεκτρομαγνητική	AirHopper GSMem USBee	480 bit/s 1 to 1000 bit/s 4000 bit/s	≤ 5-10 μέτρων
Ακουστική	Fan noise (Fansmitter) Hard disk noise (DiskFiltration)	900 bit/h 10000 bit/h	≤ 15 μέτρων
Θερμική	BitWhisper	1-8 bit/h	Πεδίο όρασης
Οπτική	Keyboard LEDs Screen LEDs Implanted infrared LEDs HDD LEDs	150 bit/s 20 bit/s 15 bit/s 4000 bit/s	Πεδίο όρασης

Πίνακας 4 Σύνοψη των διαφορετικών hidden channels σε air-gapped networks

Όλα τα malicious frameworks που είναι γνωστά μέχρι σήμερα, χρησιμοποιούσαν μονάδες USB ως φυσικό μέσο μετάδοσης πληροφορίας. Θέλοντας να δούμε τι πρωτόκολλα χρησιμοποίησαν κατασκευάζουμε τον Πίνακα 5.

[29] S. Griffith, "How to make a computer screen INVISIBLE", 2013. Available: http://www.dailymail.co.uk/sciencetech/article-2480089/How-makescreen-INVISIBLE-Scientist-shows-make-monitor-blank-using-3D-glasses.html

[30] M. Guri, O. Hasson, G. Kedma and Y. Elovici, "VisiSploit: An Optical Covert-Channel", 2016.

	Exfiltration only (unidirectional)	Command and response (bidirectional)
Connected framework		
USBStealer		X
Agent.BTZ	X	
Stuxnet		X
Fanny		X
miniFlame	X	
Flame		X
Gauss	X	
USBFerry	X	
USBCulprit		X
Retro	X	
PlugX	X	
Offline framework		
ProjectSauron	X	
EZCheese	X	
Emotional Simian		X
USB thief	X	
Brutal Kangaroo		X
Ramsay		X

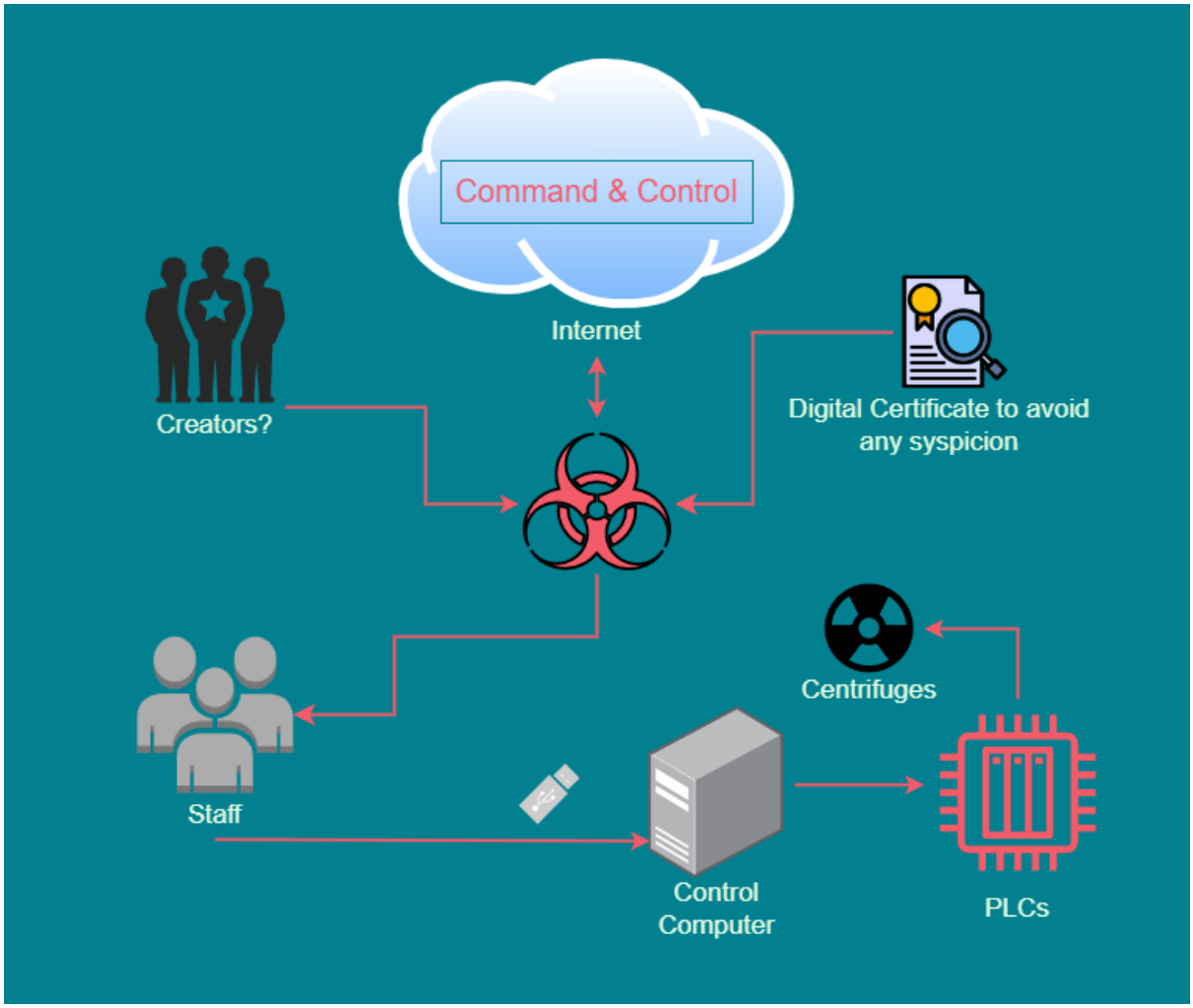
Πίνακας 5 Τύποι offline πρωτοκόλλων επικοινωνίας

ΚΕΦΑΛΑΙΟ 5ο : ΜΟΝΤΕΛΑ ΕΠΙΘΕΣΕΩΝ

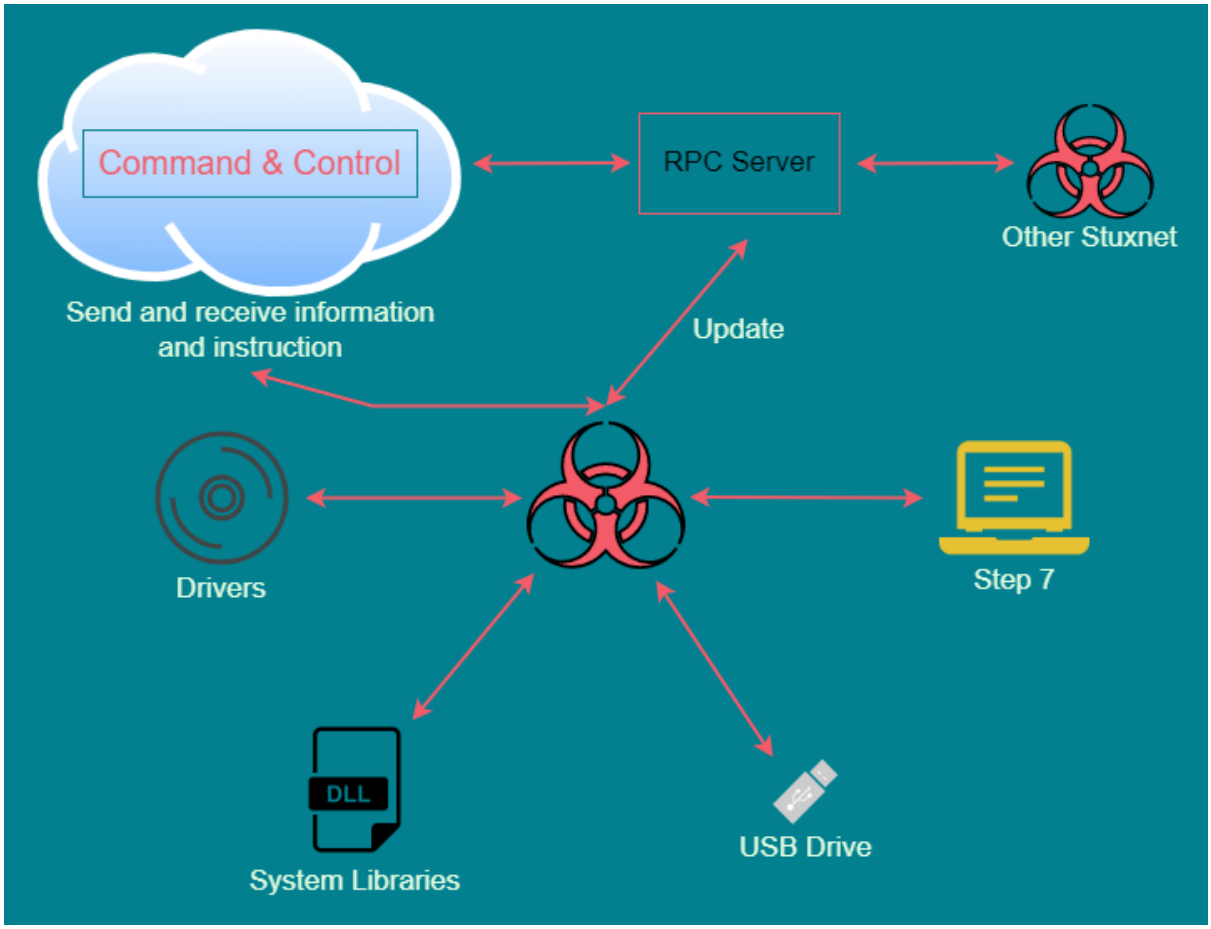
Σε μία προσπάθεια καλύτερης κατανόησης των malicious frameworks, υπό το πρίσμα μιας ολοκληρωμένης επίθεσης, παρουσιάζονται στη συνέχεια ορισμένα μοντέλα επιθέσεων, πραγματικά και πειραματικά. Έτσι θα μπορέσουμε να δούμε και να καταλάβουμε τους τρόπους με τους οποίους ενώνονται οι τεχνικές παραβίασης ενός air-gapped δικτύου, αλλά και το πως ένα malware δημιουργεί τις κατάλληλες συνθήκες για την συλλογή και αποστολή των δεδομένων πίσω στον εισβολέα.

5.1 Stuxnet

Ο ιός Stuxnet ή Stuxnet worm αποτελεί τον πιο γνωστό και έναν αρκετά πολύπλοκο ιό που κατασκευάστηκε αρχικά για συστήματα βιομηχανικού ελέγχου με μέγεθος 500 kbyte. Ανήκει στην κατηγορία των APTs και ήταν σε αναμονή δεκαεφτά ολόκληρους μήνες και καθυστερούσε έξυπνα τις διαδικασίες αντί να καταστρέψει εντελώς τους φυγοκεντρωτές. Δεν γνωρίζουμε με σιγουριά πως εισήλθε στα SCADA air-gapped συστήματα του Ιρανικού πυρηνικού εργοστασίου της πόλης Natanz, αν και μάλλον μέσω μολυσμένης μονάδας ή μονάδων USB. Χρησιμοποίησε τέσσερις zero-day vulnerabilities για να επιτεθεί και να κρυφτεί από τα antivirus προγράμματα. Οι διαφορετικές εκδόσεις ,βέβαια, χρησιμοποίησαν διαφορετικά exploits, με την πιο πρόσφατη να χρησιμοποιεί μία ευπάθεια Windows LNK (Windows Shell Link), ενώ οι παλαιότερες την ευπάθεια του αρχείου autorun.inf.



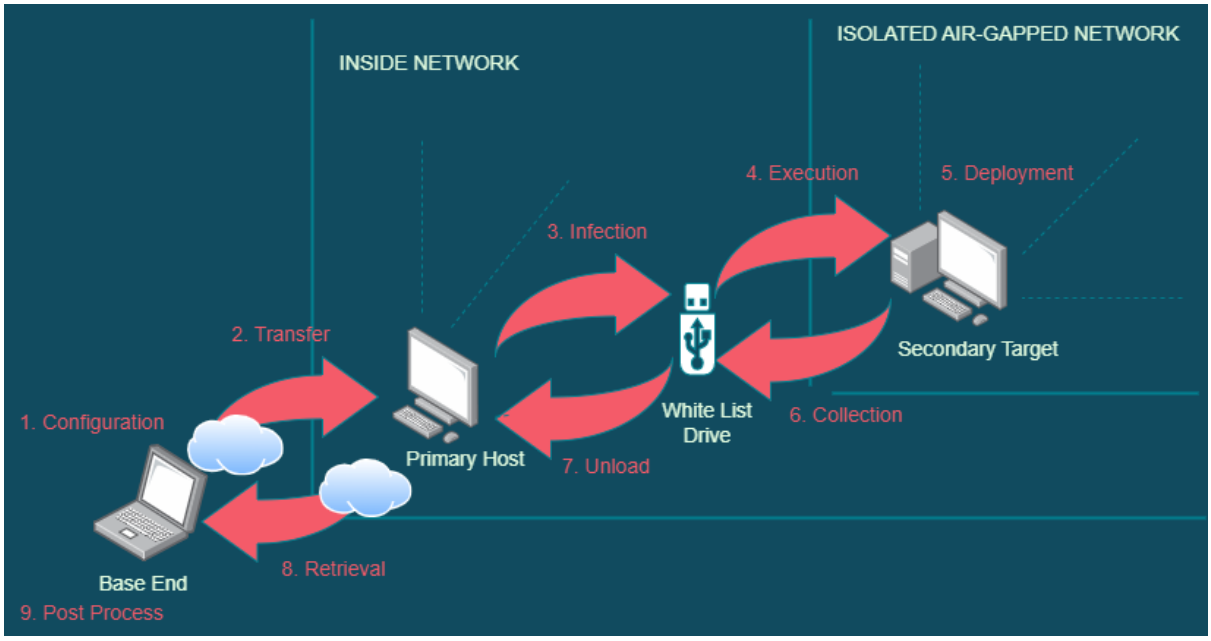
Εικόνα 16 Overview of Stuxnet



Εικόνα 17 Stuxnet components

5.2 Brutal Kangaroo

Με την ονομασία Brutal Kangaroo, η σουίτα εργαλείων φέρεται να σχεδιάστηκε από την CIA το έτος 2012 για να διεισδύσει σε ένα κλειστό δίκτυο ή έναν air-gapped υπολογιστή μέσα σε έναν οργανισμό ή επιχείρηση χωρίς να απαιτείται άμεση πρόσβαση.



Εικόνα 18 BrutalKangaroo Attack path

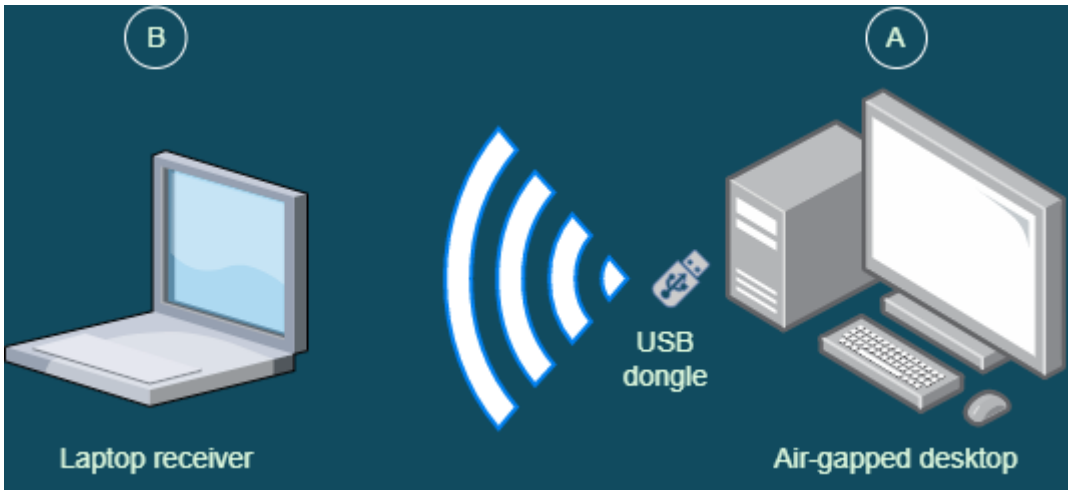
Όπως στις περισσότερες τεχνικές διείσδυσης κακόβουλου λογισμικού σε air-gapped δίκτυο, το hacking αυτό εργαλείο πρώτα μόλυνε έναν υπολογιστή συνδεδεμένο στο Διαδίκτυο εντός του οργανισμού-στόχου και στη συνέχεια εγκαθιστούσε το κακόβουλο λογισμικό Brutal Kangaroo σε αυτόν. Ακόμα και αν η προσέγγιση ενός συνδεδεμένου στο Διαδίκτυο υπολογιστή ήταν δύσκολη, μπορούσε να γίνει μόλυνση σε έναν ή περισσότερους υπολογιστές υπαλλήλων του οργανισμού. Μόλις ο υπάλληλος εισήγαγε μία μονάδα USB στον υπολογιστή του, το Shattered Assurance, ένα εργαλείο διακομιστή, όπλιζε τη μονάδα USB με ένα ξεχωριστό κακόβουλο λογισμικό, που ονομάζεται Drifting Deadline (γνωστό επίσης και ως “Emotional Simian”).

Η μονάδα USB στη συνέχεια, μόλυνε τον υπολογιστή εκμεταλλευόμενη την ευπάθεια Windows LNK κα τη φόρτωση και εκτέλεση προγραμμάτων DLLs. Μόλις το USB χρησιμοποιούταν για μεταφορά δεδομένων σε air-gapped υπολογιστή ή δίκτυο, το malware εξαπλωνόταν και σε αυτά τα συστήματα.

Τελικά, το κακόβουλο λογισμικό άρχιζε κρυφά να συλλέγει δεδομένα από compromised air-gapped computers.

5.3 USBee

Πρόκειται για ένα κακόβουλο λογισμικό που μπορεί να χρησιμοποιήσει μία μη τροποποιημένη συσκευή USB συνδεδεμένη σε υπολογιστή ως πομπό ραδιοσυχνοτήτων (RF). Το USBee μπορεί να διαρρεύσει δεδομένα από έναν air-gapped υπολογιστή σε έναν δέκτη μέσω σημάτων RF, σε μικρή εμβέλεια ωστόσο, χωρίς να απαιτείται τροποποιημένο dongle USB. Αυτό επιτυγχάνεται μέσω διαμόρφωσης οποιονδήποτε δυαδικών δεδομένων πάνω από τα ηλεκτρομαγνητικά κύματα και μετάδοσής τους σε κοντινό δέκτη. Η εικόνα που ακολουθεί παρουσιάζει ένα τέτοιο σενάριο επίθεσης.



Εικόνα 19 Illustration of USBee

Σε αυτό το σενάριο, το κακόβουλο λογισμικό, εγκατεστημένο σε παραβιασμένο υπολογιστή, χρησιμοποιεί μια μονάδα USB που είναι ήδη συνδεδεμένη στο υπολογιστή (Εικόνα 21, A) και δημιουργεί μία μετάδοση ραδιοσυχνοτήτων μικρής εμβέλειας, διαμορφωμένη με δεδομένα (π.χ. passwords ή encryption keys). Η μετάδοση μπορεί να ληφθεί από έναν κοντινό δέκτη (Εικόνα 21, B) ,όπου αποκωδικοποιείται και αποστέλλεται σε έναν εισβολέα[31].

Πρόκειται λοιπόν, για μία μέθοδο όπου η υποκλοπή δεδομένων γίνεται μέσω software, μιας και χρησιμοποιούνται για τον σκοπό αυτό ηλεκτρομαγνητικές εκπομπές ενός USB dongle, και όχι κάποια εκπομπή ραδιοσυχνοτήτων hardware.

[31] M. Guri, M. Monitz, Y. Elovici, "USBee: Air-Gap Covert-Channel via Electromagnetic Emission from USB", 2016.

5.4 LED-it-GO

Πρόκειται για μία μέθοδο που επιτρέπει σε κακόβουλο λογισμικό να διαρρέει δεδομένα από air-gapped υπολογιστές χρησιμοποιώντας το LED του HDD σκληρού δίσκου που υπάρχει σήμερα σε σχεδόν όλους τους επιτραπέζιους υπολογιστές. Ένα malware μπορεί να χειριστεί το LED του σκληρού δίσκου και να ελέγξει την περίοδο και την ταχύτητα που αυτό αναβοσβήνει, χρησιμοποιώντας ορισμένες HDD I/O λειτουργίες, όπως 'read' και 'write'. Τα αυθαίρετα δεδομένα που υποκλέπτονται μπορούν να διαμορφώνεται και να μεταδίδονται μέσω των οπτικών σημάτων. Σε σύγκριση με άλλες υπάρχουσες οπτικές μεθόδους, η μέθοδός αυτή είναι μοναδική με πέντε τρόπους:

- **Covertness** (Κρυφιότητα): Η συγκεκριμένη μέθοδος θεωρείται δύσκολα ανιχνεύσιμη, επειδή η δραστηριότητα των LED του HDD δίσκου είναι συχνά ενεργή και οι χειρισμοί του χρονισμού και της ταχύτητας που αναβοσβήνουν δεν ωθούν τον χρήστη σε όποια υποψία και παρατήρηση.
- **Speed** (Ταχύτητα): Οι μετρήσεις που πραγματοποιήθηκαν δείχνουν ότι το LED του HDD μπορεί να ελεγχθεί και να προσαρμοστεί σε μία σχετικά γρήγορη ταχύτητα, πάνω από 4000Hz. Ως εκ τούτου, επιτρέπεται η μετάδοση μηνυμάτων με μεγαλύτερη ταχύτητα από ό,τι κατάφεραν να επιτύχουν οι υπόλοιπες μέθοδοι LED. Αυτός ο ρυθμός επιτρέπει και την εξαγωγή ενός κλειδιού κρυπτογράφησης 4096 bit σε λίγα λεπτά, ακόμα και σε δευτερόλεπτα, ανάλογα με τον δέκτη.
- **Visibility** (Ορατότητα): Όταν το LED του σκληρού δίσκου αναβοσβήνει για σύντομο χρονικό διάστημα, οι άνθρωποι δεν είναι σε θέση συνήθως να αντιληφθούν τη δραστηριότητά του[32]. Επιπλέον, σε υψηλές ταχύτητες, άνω των 400Hz, το LED τρεμοπαίζει σε τέτοιο βαθμό που είναι αόρατο στο ανθρώπινο μάτι, κάνοντας το κανάλι περισσότερο απαρατήρητο.
- **Availability** (Διαθεσιμότητα): Η συγκεκριμένη μέθοδος δεν απαιτεί ειδικό hardware. Λειτουργεί με οποιοδήποτε υπολογιστή που διαθέτει HDD με LED λυχνία.
- **Privilege level** (Προνομιακό επίπεδο): Η ενεργοποίηση του LED του σκληρού δίσκου μπορεί να πραγματοποιηθεί από ένα συνηθισμένο user-level κώδικα και δεν απαιτείται ειδικό component στον kernel του λειτουργικού συστήματος.

[32] "Flicker fusion threshold" Available: https://en.wikipedia.org/wiki/Flicker_fusion_threshold

Αυτό το μοντέλο επίθεσης αποτελείται από δύο φάσεις: πρώτον, μόλυνση του υπολογιστή-στόχου με malware και δεύτερον, λήψη και αποκωδικοποίηση των σημάτων που διέρρευσαν μέσω του HDD LED.

Η μόλυνση μπορεί να επιτευχθεί μέσω supply chain attacks, ή χρησιμοποιώντας social engineering techniques είτε εκκίνηση hardware με προ-εγκατεστημένο malware για την απόκτηση πρόσβαση στο εκάστοτε μηχάνημα[33] [34] [35]. Το malware συλλέγει, στη συνέχεια, ευαίσθητες πληροφορίες από τον υπολογιστή του χρήστη (π.χ. τρόπος πληκτρολόγησης, κωδικοί πρόσβασης, κλειδιά κρυπτογράφησης και έγγραφα) και τελικά αρχίζει μετάδοση των δυαδικών δεδομένων μέσω του LED του HDD που αναβοσβήνει, χρησιμοποιώντας ένα επιλεγμένο σχήμα κωδικοποίησης.

Για την λήψη και αποκωδικοποίηση η επίθεση απαιτεί επίσης ψηφιακή κάμερα ή οπτικό αισθητήρα που έχει οπτική επαφή με τον υπολογιστή - θύμα. Αυτό μπορεί να δουλέψει είτε με ένα άτομο που κουβαλά μια κρυφή κάμερα και στέκεται σε σημείο χωρίς εμπόδια και παρεμβολές μεταξύ κάμερας και παραβιασμένου υπολογιστή, είτε με ένα τύπο απομακρυσμένης κάμερας ή οπτικού αισθητήρα στραμμένο στον παραβιασμένο υπολογιστή[36]. Υπάρχουν διάφοροι τύποι εξοπλισμού που μπορούν να παίξουν το ρόλο του δέκτη σε αυτό το μοντέλο επίθεσης.

- **Local hidden camera** (Τοπική κρυφή κάμερα): Μια κρυφή κάμερα που έχει μια οπτική γωνία στον υπολογιστή μετάδοσης.
- **High resolution remote camera** (Απομακρυσμένη κάμερα υψηλής ανάλυσης): Μια κάμερα υψηλής ανάλυσης (ή άλλος τύπος οπτικού αισθητήρα) που βρίσκεται έξω από το κτίριο, αλλά τοποθετημένο έτσι ώστε να έχει οπτική επαφή με τον υπολογιστή εκπομπής.
- **Drone camera:** Μια κάμερα εγκατεστημένη σε ένα ευέλικτο drone που πετάει σε μια τοποθεσία η οποία έχει οπτική επαφή με τον υπολογιστή εκπομπής, π.χ. κοντά στο παράθυρο.

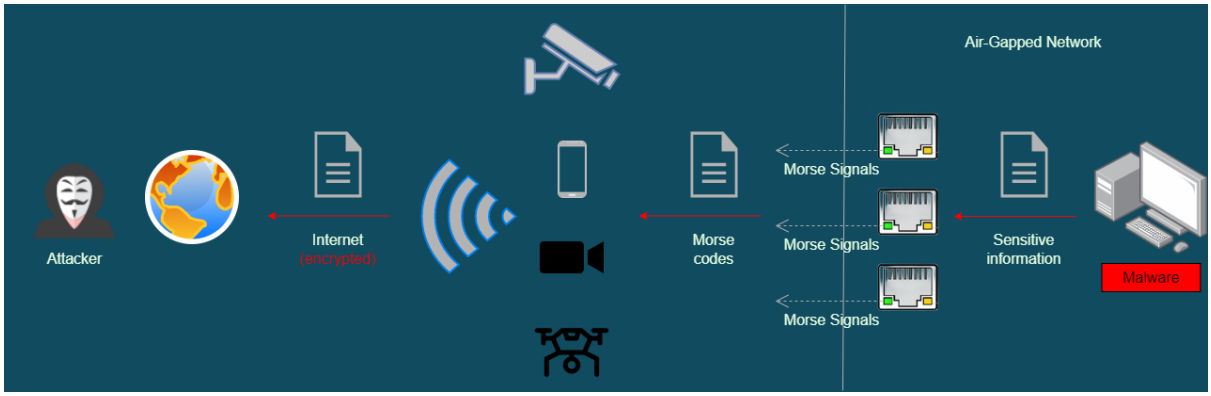
[33] A. Gostev, "Agent.btz: a Source of Inspiration?", 2014. Available: http://securelist.com/blog/virus-watch/58551/agent-btz-a-source-ofinspiration/
[34]] GReAT team, "A Fanny Equation: "I am your father, Stuxnet"", 2015. Available: https://securelist.com/blog/research/68787/a-fanny-equation-i-am-your-fatherstuxnet/
[35] D. Goodin, "Meet “badBIOS”, the mysterious Mac and PC malware that jumps airgaps,", 2013. Available: http://arstechnica.com/security/2013/10/meet-badbios-the-mysterious-mac-and-pcmalware-that-jumps-airgaps/
[36] A. Costin, "Security of CCTV and Video Surveillance Systems: Threats, Vulnerabilities, Attacks, and Mitigations", 2016.

- **Camera carried by malicious insider** (Κάμερα που μεταφέρεται από κακόβουλο άτομο): Ένα άτομο που βρίσκεται σε κοντινή απόσταση από τον υπολογιστή, φέρει smartphone ή φορητή βιντεοκάμερα και μπορεί να τοποθετηθεί έτσι ώστε να έχει οπτική επαφή με αυτόν.
- **Compromised security camera** (Παραβιασμένη κάμερα ασφαλείας): Μια κάμερα ασφαλείας τοποθετημένη σε μια τοποθεσία όπου έχει οπτική επαφή με τον υπολογιστή εκπομπής. Μια ολοκληρωμένη ανάλυση των απειλών, των τρωτών σημείων και των επιθέσεων σε βιντεο - παρακολούθηση, σύστημα τηλεόρασης κλειστού κυκλώματος και IP συστήματα κάμερας διεξήχθη από τον A. Costin[37].
- **Optical sensors** (Οπτικοί αισθητήρες): Ένας οπτικός αισθητήρας ικανός να ανιχνεύει το φως που εκπέμπεται από το LED του σκληρού δίσκου. Τέτοιοι αισθητήρες χρησιμοποιούνται εκτενώς σε VLC (επικοινωνία ορατού φωτός) και LED to LED επικοινωνία[38]. Σημειωτέων, οι οπτικοί αισθητήρες μπορούν να δειγματοληπτούν σήματα LED σε υψηλούς ρυθμούς, επιτρέποντας τη λήψη δεδομένων σε μεγαλύτερο εύρος ζώνης από μια τυπική βιντεοκάμερα.

5.5 EtherLED

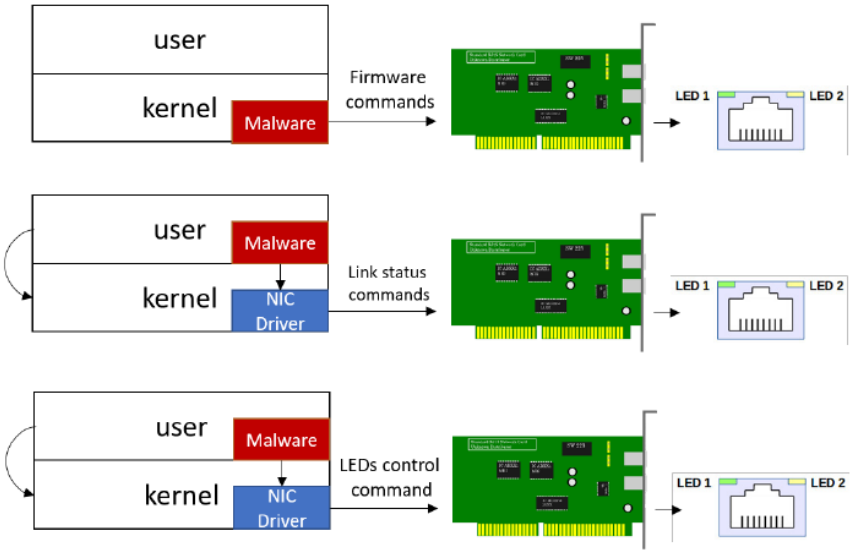
Ακόμη μία τεχνική έρχεται να προστεθεί στον οπτικό τομέα διαρροής δεδομένων από air-gapped networked συσκευές όπως κεντρικοί και φορητοί υπολογιστές, εκτυπωτές και σαρωτές, NAS χώροι αποθήκευσης, τηλεοράσεις και οθόνες LCD, ενσωματωμένοι controllers και servers. Ονομάζεται EtherLED και δραστηριοποιείται στις δικτυωμένες συσκευές με ενσωματωμένο network interface controller (NIC), που περιλαμβάνουν LED λαμπτήρες ενδείξεων. Ουσιαστικά ένα εγκατεστημένο malware ελέγχει τις LED λυχνίες αναβοσβήνοντας και εναλλάσσοντας χρώματα για να μεταφέρει πληροφορία και δεδομένα. Οι πληροφορίες μπορούν να κωδικοποιηθούν με απλό τρόπο όπως ο κώδικας Morse και να ληφθούν με κάποιο οπτικό μέσο (π.χ. τοπική κάμερα, κάμερα ασφαλείας, τηλεφώνου κ.α.). Το EtherLED αποτελεί APT μοντέλο επίθεσης και περιέχει στοιχεία πομπού και δέκτη.

[37] A. Costin, "Security of CCTV and Video Surveillance Systems: Threats, Vulnerabilities, Attacks, and Mitigations", 2016.
[38] S. Schmid, G. Corbellini, S. Mangold and T. R. Gross, "An LED-to-LED Visible Light Communication System with Software-Based Synchronization". Available: http://www.bu.edu/smartlighting/files/2012/10/Schmid_.pdf



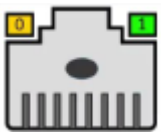
Εικόνα 20 ATP model συλλέγει ευαίσθητα δεδομένα, αυτά κωδικοποιούνται μέσω NIC LED λυχνιών, συλλέγονται από οπτικό μέσο και κρυπτογραφημένα στέλνονται στον επιτιθέμενο

Στο αρχικό στάδιο της επίθεσης, ο επιτιθέμενος εκτελεί κακόβουλο κώδικα εντός του συστήματος-στόχου για να πάρει τον έλεγχο των NIC LED. Ο στόχος μπορεί να είναι ένας air-gapped υπολογιστής ή άλλες συσκευές εντός του air-gapped δικτύου, όπως ενσωματωμένα συστήματα, εκτυπωτές, κάμερες και οποιαδήποτε συσκευή συνδεδεμένη ενσύρματα. Η μόλυνση μιας τέτοιας συσκευής μπορεί να επιτευχθεί μέσω supply chain επιθέσεων, social engineering techniques ή τη χρήση hardware με εγκατεστημένο software ή firmware.



Εικόνα 21 Μέθοδοι ελέγχου NIC LED

Σε δεύτερη φάση, ο κακόβουλος κώδικας συλλέγει δεδομένα από το παραβιασμένο δίκτυο. Τα δεδομένα μπορεί να είναι κάποιο κείμενο (π.χ. ονόματα χρηστών, κωδικοί πρόσβασης, keylogging) ή δυαδική (π.χ. κλειδιά κρυπτογράφησης, βιομετρικές πληροφορίες). Μετά τη συλλογή των πληροφοριών, το malware ξεκινά τη φάση της διήθησης. Χρησιμοποιεί δηλαδή, τη LED λυχνία κατάστασης της κάρτας



δικτύου για την κωδικοποίηση των κειμένων ή δυαδικών πληροφοριών σε διαμορφώσεις οπτικών δεδομένων και κώδικα Morse.

Ο εισβολέας, σε τρίτη φάση, λαμβάνει τα οπτικά σήματα μέσω καμερών σε οπτική επαφή με τις NIC LED λυχνίες της εκάστοτε συσκευής. Όπως προαναφέρθηκε, μπορούν να χρησιμοποιηθούν αρκετοί τύποι καμερών. Ένας άλλος πιθανός δέκτης είναι ένα drone με κάμερα υψηλής ανάλυσης. Τέλος οι επιτιθέμενοι μπορούν να χρησιμοποιήσουν άτομο που φέρει συσκευή εγγραφής (π.χ. smartphone) και μπορεί να τοποθετηθεί ώστε να έχει οπτική επαφή με τη συσκευή εκπομπής. Το μόνο που έχει να κάνει ο κακόβουλος χρήστης στη συνέχεια είναι να αποκωδικοποιήσει τα σήματα και να ανακτήσει τις κωδικοποιημένες πληροφορίες.

5.6 xLED

Θέλοντας να κλείσουμε το κεφάλαιο των LED λυχνιών και της υποκλοπής δεδομένων μέσω οπτικών συσκευών, παρουσιάζεται η τεχνική με όνομα xLED. Αυτή χρησιμοποιεί τα LED που υπάρχουν πάνω στα switches και routers που απαρτίζουν ένα air-gapped network. Παρόλο που είναι γνωστό ότι ο εξοπλισμός δικτύου εκπέμπει οπτικά σήματα που συσχετίζονται με τις πληροφορίες που επεξεργάζεται η συσκευή[39], μπορεί να πραγματοποιηθεί και εδώ σκόπιμος έλεγχος των LED για διαμόρφωση και μεταφορά κρίσιμων δεδομένων. Όπως και στις προηγούμενες περιπτώσεις έτσι και εδώ η εισαγωγή malware παίζει καταλυτικό ρόλο, είτε εγκατεστημένο στο firmware του switch ή router του δικτύου, είτε εγκατεστημένο σε υπολογιστή εντός του air-gapped δικτύου μέσω του οποίου θα ελέγχονται και οι λυχνίες.

Το συγκεκριμένο μοντέλο επίθεσης δρα σε ένα τυπικό κανάλι και αποτελείται από έναν πομπό και έναν δέκτη. Ο transmitter δεν είναι άλλος παρά ένα network switch ή router στον οποίο τα δεδομένα εξάγονται μέσω των LED του, ενώ ο receiver είναι μία απομακρυσμένη κάμερα ή οπτικός αισθητήρας που καταγράφει τα σήματα αυτών των LED.

Πομπός

Πρώτο βήμα από τον επιτιθέμενο είναι η εκτέλεση κακόβουλου κώδικα εντός του router-στόχου για να ενεργοποιήσει τον έλεγχο των LED. Αυτό μπορεί να το επιτύχει με δύο τρόπους, είτε τροποποιώντας το firmware του router, είτε εκτελώντας κακόβουλο script αρχείο σε ένα μη-τροποποιημένο router.

[39] J. Loughry and A. D. Umphress, "Information leakage from optical emanations", pp. 262-289, 2002.

- **Firmware modification:** Η τροποποίηση του firmware του router, που θα περιέχει πρόσθετο κώδικα για τον έλεγχο των LED και την κωδικοποίηση δεδομένων πάνω σε αυτό, μπορεί να επιτευχθεί με τεχνικές που έχουμε ήδη προαναφέρει, supply chain attack, social engineering ή προ εγκατεστημένο malware στο hardware του router[40] [41] [42].
- **Remote code execution:** Στη περίπτωση αυτήν, ο router-στόχος δεν χρειάζεται να έχει μολυνθεί από κακόβουλο firmware. Αντίθετα, ελέγχεται εξ αποστάσεως, από έναν υπολογιστή που έχει παραβιαστεί εντός του air-gapped δικτύου, μέσω τυπικών remote management καναλιών όπως το SSH και το telnet ή με την εκμετάλλευση ορισμένων ευπαθειών στο δρομολογητή. Στη συνέχεια, ο κώδικας μετάδοσης μεταφορτώνεται στο δρομολογητή με τη μορφή ενός shellcode ή ενός shell script.

Δέκτης

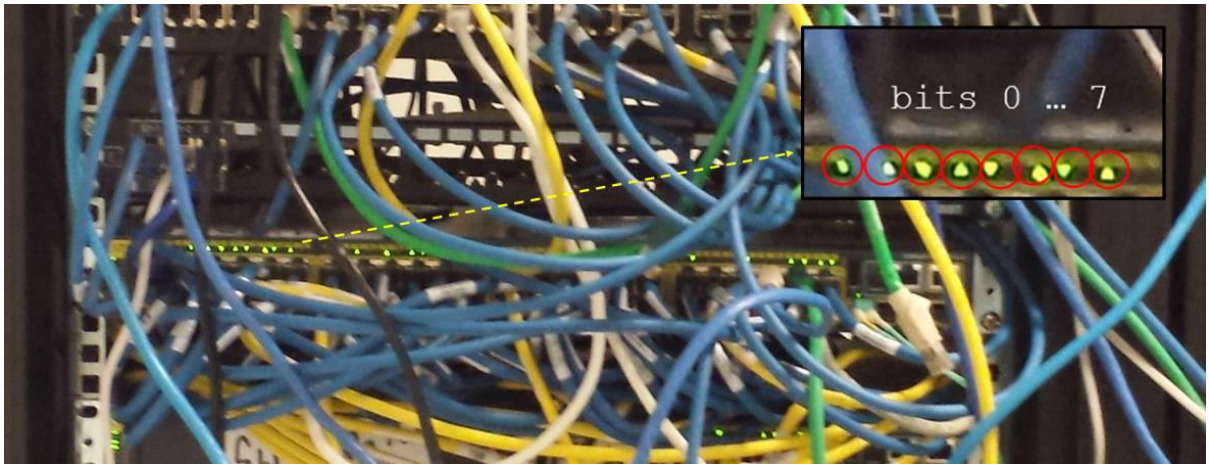
Ο δέκτης είναι μια ψηφιακή κάμερα ή ένας οπτικός αισθητήρας που έχει οπτική επαφή με τον πίνακα LED του router. Υπάρχουν διάφοροι τύποι εξοπλισμού που μπορούν να παίξουν το ρόλο του δέκτη στη συγκεκριμένη επίθεση όπως:

1. μια κρυφή κάμερα που έχει οπτική επαφή με τον transmitting router.
2. μια κάμερα υψηλής ανάλυσης που βρίσκεται έξω από το κτίριο αλλά τοποθετημένη έτσι ώστε να έχει οπτική επαφή με αυτόν.
3. παρακολούθηση βίντεο, τηλεόρασης κλειστού κυκλώματος ή κάμερα IP τοποθετημένη σε θέση όπου έχει οπτική επαφή με τον transmitting υπολογιστή[43].
4. ένας κακόβουλος χρήστης, γνωστός και ως evil maid (κακιά υπηρέτρια)[44], που φέρει ένα smartphone ή φορητή κρυφή βιντεοκάμερα[45] που μπορεί να τοποθετηθεί έτσι ώστε να έχει οπτική επαφή με το router.
5. ένας οπτικός αισθητήρας ικανός να ανιχνεύει το φως που εκπέμπεται από τα LED του router. Τέτοιοι αισθητήρες χρησιμοποιούνται εκτενώς στην επικοινωνία VLC

[40] A. Gostev, "Agent.btz: a Source of Inspiration?". Available: http://securelist.com/blog/virus-watch/58551/agent-btz-a-source-of-inspiration/
[41] Kaspersky Labs' Global Research & Analysis Team, "A Fanny Equation: "I am your father, Stuxnet"". Available: https://securelist.com/blog/research/68787/a-fanny-equation-i-am-your-father-stuxnet/
[42] D. Goodin, "Meet “badBIOS”, the mysterious Mac and PC malware that jumps airgaps". Available: http://arstechnica.com/security/2013/10/meet-badbios-the-mysterious-mac-and-pc-malware-that-jumps-airgaps/
[43] A. Costin, "Security of CCTV and Video Surveillance Systems: Threats, Vulnerabilities, Attacks, and Mitigations", 2016.
[44] TechTarget, "evil maid attack". Available: http://searchsecurity.techtarget.com/definition/evil-maid-attack
[45] TripWire, Irfhan Khimji, "The Malicious Insider". Available: http://www.tripwire.com/state-of-security/security-awareness/the-malicious-insider/

(επικοινωνία ορατού φωτός) και στην επικοινωνία LED to LED[46]. Συγκεκριμένα, οι οπτικοί αισθητήρες μπορούν να δειγματοληπτούν σήματα LED με υψηλούς ρυθμούς, επιτρέποντας τη λήψη δεδομένων σε μεγαλύτερο εύρος ζώνης από μια τυπική βιντεοκάμερα.

Ένα παράδειγμα του air-gapped καναλιού παρέχεται στην εικόνα 24 στην οποία τα δεδομένα κωδικοποιούνται σε δυαδική μορφή και μεταδίδονται κρυφά μέσω ενός συνόλου LED σημάτων. Μια κρυφή βιντεοκάμερα μαγνητοσκοπεί τη δραστηριότητα στο δωμάτιο, συμπεριλαμβανομένων των LED του router και του LAN switch. Ο εισβολέας μπορεί στη συνέχεια να αποκωδικοποιήσει τα σήματα και να ανακατασκευάσει τα διαμορφωμένα δεδομένα.



Εικόνα 22 Group LED σημάτων κωδικοποιούν σε δυαδική μορφή δεδομένα και τα μεταδίδουν κρυφά

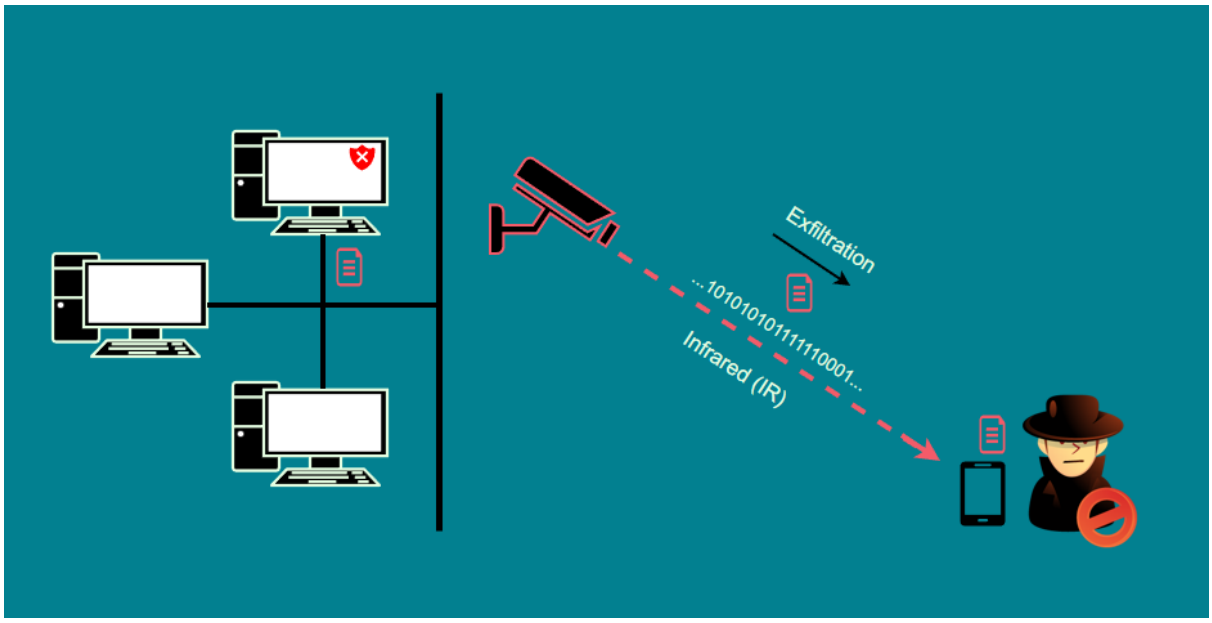
5.7 aIR-Jumper

Υπάρχει τρόπος ένας επιτιθέμενος να χρησιμοποιήσει κάμερες παρακολούθησης που είναι εξοπλισμένες με LED υπέρυθρου φωτός (Infrared Light) ώστε να δημιουργήσει αμφίδρομο κανάλι επικοινωνίας μεταξύ αυτού και ενός air-gapped δικτύου. Το IR (υπέρυθρο φως), δίνει την δυνατότητα αναπαραγωγής δύο σεναρίων για έναν κακόβουλο χρήστη ή και τον συνδυασμό τους: exfiltration και infiltration. Το isolated air-gapped δίκτυο ενός οργανισμού παραβιάζεται με κακόβουλο λογισμικό από τους διάφορους attack vectors που αναφέρθηκαν, έχοντας έτσι μία τυπική APT. Στη συνέχεια το malware σαρώνει τις IP για τον

[46] S. Schmid, G. Corbellini, S. Mangold and T. R. Gross, "An LED-to-LED Visible Light Communication System with Software-Based Synchronization". Available: http://www.bu.edu/smartlighting/files/2012/10/Schmid_.pdf

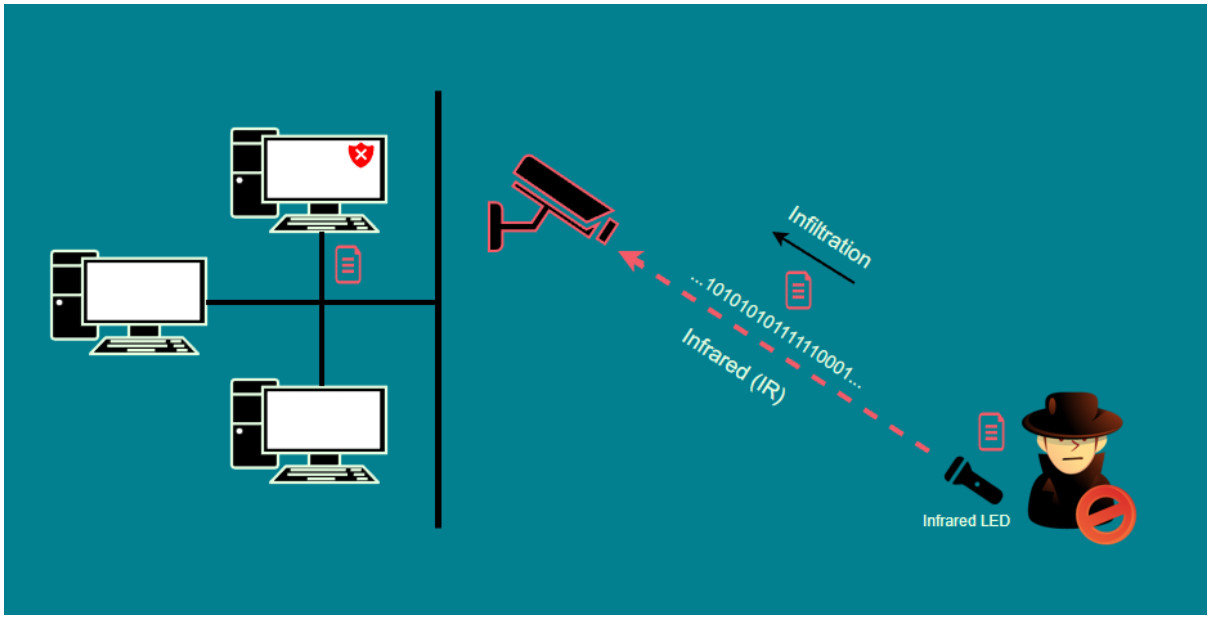
εντοπισμό των καμερών ασφαλείας και παρακολούθησης, εξετάζοντας ανοιχτές θύρες, HTTP αποκρίσεις ή MAC διευθύνσεις. Μόλις γίνει και η χαρτογράφηση των καμερών το malware πρέπει να είναι σε θέση να συνδεθεί με αυτές ώστε να μπορέσει να τις τροποποιήσει και να πάρει τον έλεγχο των IR LEDs.

- **Διαρροή δεδομένων (Exfiltration):** Για το σενάριο αυτό, όπως φαίνεται και στην εικόνα 23, το malware συλλέγει τα ευαίσθητα δεδομένα που θέλει να διαρρεύσουν. Εν συνεχεία κωδικοποιεί και μεταδίδει τα δεδομένα αυτά μέσω των σημάτων IR που εκπέμπονται από τα νυχτερινής όρασης IR LEDs. Η διαρροή μπορεί να πραγματοποιηθεί σε προκαθορισμένους χρόνους ή μέσω κάποιας ενεργοποίησης από την πλευρά του επιτιθέμενου. Ο τελευταίος που βρίσκεται συνήθως εκτός του οργανισμού μπορεί να λάβει τα υπέρυθρα σήματα χρησιμοποιώντας μια τυπική βιντεοκάμερα και στοχεύοντας την κάμερα παρακολούθησης που εκπέμπει. Το τελικό βίντεο υποβάλλεται σε επεξεργασία προκειμένου να αποκωδικοποιηθούν τα δεδομένα που λήφθηκαν.



Εικόνα 23 Προσομοίωση exfiltration καναλιού

- **Διείσδυση δεδομένων (Infiltration):** Για το σενάριο αυτό, όπως φαίνεται και στην εικόνα 24, ένας εισβολέας που βρίσκεται συνήθως εκτός του οργανισμού-στόχου δημιουργεί αόρατα σήματα υπέρυθρων με χρήση IR LED. Τα σήματα υπέρυθρων είναι διαμορφωμένα με C&C μηνύματα ώστε να παραδοθούν στο κακόβουλο λογισμικό. Το βίντεο που καταγράφτηκε από την κάμερα λαμβάνεται από το malware το οποίο στη συνέχεια επεξεργάζεται και αποκωδικοποιεί τα δεδομένα.



Εικόνα 24 Προσομοίωση infiltration καναλιού

5.8 MAGNETO

Το συγκεκριμένο μοντέλο επίθεσης με όνομα MAGNETO λόγω των μαγνητικών εκπομπών που χρησιμοποιεί περιλαμβάνει όχι μόνο την μόλυνση ενός air-gapped υπολογιστή, αλλά και του smartphone του υπαλλήλου που τον χρησιμοποιεί, με την ιδέα ότι συχνά οι τελευταίοι τοποθετούν τις κινητές συσκευές τους για αρκετή ώρα στο γραφείο και δει κοντά στον υπολογιστή. Σε πρώτο βήμα, κακόβουλο λογισμικό που έχει περάσει μέσω αφαιρούμενης συσκευής, προφανώς, διαδίδεται στο δίκτυο στοχεύοντας συγκεκριμένους υπολογιστές. Στο δεύτερο βήμα, το κινητό τηλέφωνο στοχευμένου υπαλλήλου μολύνεται, πιθανώς μέσω συνημμένων email, παραβιασμένων websites ή λήψεων κακόβουλων εφαρμογών, και εγκαθίσταται το application που θα παίξει το ρόλο του δέκτη.

Μόλις ολοκληρωθούν οι δύο αυτές φάσεις περνάμε στην φάση της εξαγωγής. Το malware που απαρατήρητα συλλέγει πληροφορίες και δεδομένα, τα διαρρέει μέσω της μαγνητικής εκπομπής που παράγεται από την CPU. Ταυτόχρονα η malicious εφαρμογή στο smartphone σαρώνει το μαγνητικό πεδίο για το σήμα που υποδηλώνει μια εισερχόμενη μετάδοση δεδομένων. Όταν τα σήματα λαμβάνονται και αποκωδικοποιούνται, τα δεδομένα μπορούν να προωθηθούν από το κινητό στον υπολογιστή του επιτιθέμενου κρυπτογραφημένα μέσω Wi-Fi.

Θέλοντας λίγο να αναλυθεί το μοντέλο στο πρακτικό κομμάτι του, η CPU είναι ένας από τους μεγαλύτερους καταναλωτές ενέργειας στη motherboard. Δεδομένου ότι οι σύγχρονες

CPU είναι ενεργειακά αποδοτικές, το στιγμιαίο workload της CPU επηρεάζει άμεσα τις δυναμικές αλλαγές στην κατανάλωση ενέργειας[47]. Ρυθμίζοντας το κατάλληλα είναι δυνατό να ελεγχθεί η κατανάλωση ενέργειας και, ως εκ τούτου, να ελέγχεται το μαγνητικό πεδίο που δημιουργείται, για παράδειγμα η υπερφόρτωση της CPU με υπολογισμούς θα καταναλώσει περισσότερο ρεύμα άρα θα δημιουργηθεί και ισχυρότερο μαγνητικό πεδίο. Τελικά ξεκινώντας και σταματώντας σκόπιμα το workload της CPU, μπορεί να δημιουργηθεί ένα μαγνητικό πεδίο σε απαιτούμενη συχνότητα και μάλιστα να διαμορφώνονται δυαδικά δεδομένα λόγω αυτών των up-and-downs.

Bit-Framing

Ο τρόπος μετάδοσης των δεδομένων γίνεται με μικρά frames των 40 bits που περιέχεται το preamble, το payload και ένα CRC όπως στον πίνακα.

Preamble (4 bits)	Payload (32 bits)	CRC (4 bits)

Πίνακας 6 Bit-Framing

- **Preamble:** Μεταδίδεται στην αρχή του κάθε πακέτου και αποτελείται από μια ακολουθία τεσσάρων εναλλασσόμενων συμβόλων ('1010') που βοηθά τον δέκτη να προσδιορίσει τις ιδιότητες του καναλιού, όπως τη συχνότητα και το πλάτος του φέροντος κύματος. Είναι απαραίτητο καθώς οι ιδιότητες αλλάζουν ανάλογα με την απόσταση του smartphone από το πομπό. Επιπλέον, το preamble χρησιμοποιείται από το δέκτη για την ανίχνευση της μετάδοσης του κάθε πακέτου.
- **Payload:** Αποτελείται από 32 bit ακατέργαστων δυαδικών δεδομένων.
- **CRC:** Χρησιμοποιούνται 4 bit κώδικα ελέγχου σφάλματος στο τέλος του frame ούτως ώστε να υπολογίζει ο δέκτης το CRC για το payload που έλαβε και να το συγκρίνει για τυχόν σφάλμα.

5.9 PowerHammer

Τελευταίος αλλά εξίσου σημαντικός τύπος malware είναι το PowerHammer, που μπορεί να εξάγει δεδομένα από air-gapped υπολογιστές μέσω των καλωδίων του ρεύματος. Το κακόβουλο αυτό λογισμικό διαμορφώνει, κωδικοποιεί και μεταδίδει δεδομένα μέσω των

[47] J. von Kistowski, H. Block, J. Beckett, C. Spradling, K.-D. Lange, and S. Kounev, “Variations in cpu power consumption”, pp. 147–158, 2016.

διακυμάνσεων του εναλλασσόμενου ρεύματος στα καλώδια, γνωστό και ως conducted emission. Μπορεί και εφαρμόζεται σε δύο versions: power-hammering σε επίπεδο γραμμής και power-hammering σε επίπεδο φάσης. Το μόνο που έχει να κάνει ο εισβολέας είναι να μετρήσει την αγώγιμη εκπομπή για να αποκωδικοποιήσει τα δεδομένα που έχουν εξαχθεί.

Η επίθεση αποτελείται από τέσσερα βήματα: (1) μόλυνση του συστήματος, (2) εμφύτευση δέκτη, (3) συλλογή δεδομένων, (4) εξαγωγή δεδομένων.

- **System Infection:** Η μόλυνση του δικτύου και εν συνεχεία των συστημάτων από το malware θα προέλθει με έναν από τους τρόπους των APTs αλλά και των Social Engineering επιθέσεων που έχουμε προαναφέρει.
- **Receiver Implantation:** Θα πρέπει να γίνει τοποθέτηση ενός ανιχνευτή είτε στο καλώδιο ρεύματος που τροφοδοτεί τον υπολογιστή-θύμα είτε στον κεντρικό πίνακα ηλεκτροδότησης. Ο ανιχνευτής αυτός μετρά το ρεύμα της γραμμής, επεξεργάζεται τα διαμορφωμένα σήματα, αποκωδικοποιεί τα δεδομένα και τα αποστέλλει στον επιτιθέμενο (π.χ. μέσω Wi-Fi transceiver).
- **Data Gathering:** Έχοντας μία επαφή στο σύστημα, το malware ξεκινά την ανάκτηση δεδομένων όπως αρχείων, κρυπτογραφικών κλειδιών, tokens και passwords. Με το πέρας της συλλογής διοχετεύονται μέσω υπολογιστή ή server.
- **Exfiltration:** Όπως και στο attack model MAGNETO, όταν έρθει η στιγμή της εξαγωγής και μετάδοσης των δεδομένων μέσω ηλεκτρομαγνητικών σημάτων στα καλώδια του ρεύματος, θα γίνει με αλλαγές στο workload στους πυρήνες της CPU. Τα σήματα που παράγονται με αυτόν τον τρόπο πλέον μπορούν να ληφθούν από τον ανιχνευτή στην γραμμή του ρεύματος και να παραδοθούν στον εισβολέα (π.χ. μέσω Wi-Fi).

Αν και τέτοιου είδους επιθετικά σενάρια φαίνονται και είναι αρκετά περίπλοκα, κανένα από αυτά δεν είναι εκτός των δυνατοτήτων των παρακινούμενων και ικανών attackers μιας και οι ανταμοιβές τους θα είναι πολύτιμες και ασφαλείς πληροφορίες που συχνά είναι εκτός του βελτηνεκούς πρόσβασης μέσω άλλων τύπων κρυφών καναλιών.

ΚΕΦΑΛΑΙΟ 6ο : ΑΝΤΙΜΕΤΡΑ & ΜΕΘΟΔΟΙ ΕΝΤΟΠΙΣΜΟΥ

Η προστασία air-gapped συστημάτων και δικτύων περιλαμβάνει μια πολυεπίπεδη προσέγγιση για την ασφάλεια, που ξεκινά από τη φυσική εγκατάσταση του συστήματος έως τους ανθρώπους που αλληλεπιδρούν με αυτό σε τακτική βάση. Ακολουθούν ορισμένες στρατηγικές που μπορούν να εφαρμόσουν οι οργανισμοί για να διασφαλίσουν ότι τα air-gapped δίκτυα που διαθέτουν, καθώς και τα δεδομένα που περιέχονται μέσα σε αυτά, δεν μπορούν να παραβιαστούν εύκολα, ούτε να υποκλαπούν πληροφορίες.

6.1 Physical Protection

Το πρώτο και πιο κρίσιμο μέτρο για τη διασφάλιση ενός air-gapped δικτύου είναι η φυσική ασφάλεια. Θα πρέπει να στεγάζεται σε ασφαλή τοποθεσία, με αυστηρούς ελέγχους πρόσβασης και επιτήρηση, ώστε να αποτρέπεται η μη εξουσιοδοτημένη πρόσβαση.

- **Access Control:** Τα μέτρα ελέγχου πρόσβασης μπορούν να χρησιμοποιηθούν για τον περιορισμό της φυσικής πρόσβασης στο air-gapped δίκτυο. Αυτό μπορεί να περιλαμβάνει φυσικά εμπόδια, όπως κλειδωμένες πόρτες ή πύλες, καθώς και ηλεκτρονικά συστήματα ελέγχου πρόσβασης, όπως κάρτες-κλειδιά ή βιομετρικούς σαρωτές. Ακόμη θα πρέπει να γίνεται έλεγχος και απαγόρευση οποιουδήποτε ηλεκτρονικού εξοπλισμού συμπεριλαμβανομένων και RF συσκευών που θέλουν να εισέλθουν στις περιοχές στέγασης συσκευών του air-gapped δικτύου. Αυτό γίνεται για την αντιμετώπιση διαφόρων τύπων ακουστικών, ηλεκτρομαγνητικών και οπτικών απειλών.
- **Video Surveillance:** Τα συστήματα παρακολούθησης βίντεο μπορούν να χρησιμοποιηθούν για την παρακολούθηση της φυσικής πρόσβασης στο δίκτυο με διάκενο αέρα. Οι βιντεοκάμερες μπορούν να τοποθετηθούν σε στρατηγικές τοποθεσίες σε όλο το δίκτυο για να παρακολουθούν τα σημεία εισόδου και εξόδου, καθώς και άλλες περιοχές ενδιαφέροντος. Ως αποτέλεσμα μπορούν να παρέχουν πολύτιμα στοιχεία σε περίπτωση παραβίασης της ασφάλειας. Ωστόσο όλα τα είδη καμερών απαγορεύονται σε ασφαλή δωμάτια καθώς η ίδια η κάμερα παρακολούθησης μπορεί να παραβιαστεί από κακόβουλο λογισμικό[48] [49] και να γίνει το μέσω μετάδοσης δεδομένων, εάν στο οπτικό της πεδίο υπάρχουν ethernet καλώδια με LED ενδείξεις ή HDD δίσκοι.

[48] ZDNET, "Surveillance cameras sold on Amazon infected with malware" 2016. Available: http://www.zdnet.com/article/amazon-surveillance-camerasinfected-with-malware/
[49] A. Costin, "Security of CCTV and Video Surveillance Systems: Threats, Vulnerabilities,

- **Protection from Optical Emanation:** Για την αντιμετώπιση των επιθέσεων LED αλλά και όσων βασίζονται σε οπτικά μέσα η κάλυψη όλων των LED λυχνιών σε σκληρούς δίσκους, monitor οθόνες, ethernet καλώδια, αλλά και pc towers με μαύρη ταινία είναι μία λύση[50]. Όσον αφορά τις περιπτώσεις οπτικής εκπομπής, μπορεί να εγκατασταθεί μια ειδική μεμβράνη παραθύρου που αποτρέπει την οπτική υποκλοπή[51].
- **Environmental Controls:** Μπορούν να χρησιμοποιηθούν περιβαλλοντικοί έλεγχοι για να διασφαλιστεί ότι το δίκτυο με διάκενο αέρα στεγάζεται σε ένα ασφαλές και ελεγχόμενο περιβάλλον. Αυτό μπορεί να περιλαμβάνει μέτρα όπως έλεγχος θερμοκρασίας και υγρασίας, συστήματα πυρόσβεσης και συστήματα ανίχνευσης νερού. Οι περιβαλλοντικοί έλεγχοι μπορούν να βοηθήσουν στην αποφυγή ζημιών στο δίκτυο και μπορούν να συμβάλουν στη διασφάλιση της λειτουργίας του σε περίπτωση φυσικής καταστροφής.
- **Physical Locks & Tamper Detection:** Οι φυσικές κλειδαριές και οι μηχανισμοί ανίχνευσης παραβίασης μπορούν να χρησιμοποιηθούν για την αποτροπή μη εξουσιοδοτημένης πρόσβασης στο δίκτυο με διάκενο αέρα. Αυτό μπορεί να περιλαμβάνει κλείδωμα ντουλαπιών, κλείδωμα ραφιών διακομιστή ή σφραγίδες σε κρίσιμα εξαρτήματα με προφανή παραβίαση. Οι φυσικές κλειδαριές και οι μηχανισμοί ανίχνευσης παραβίασης μπορούν να βοηθήσουν στην αποτροπή μη εξουσιοδοτημένης πρόσβασης και μπορούν να παρέχουν στοιχεία για τυχόν απόπειρες παραβιάσεων.
- **Secure Disposal:** Μπορούν να χρησιμοποιηθούν μέτρα ασφαλούς απόρριψης για να διασφαλιστεί ότι τα ευαίσθητα δεδομένα διατίθενται σωστά όταν δεν χρειάζονται πλέον. Αυτό μπορεί να περιλαμβάνει μέτρα όπως ο τεμαχισμός, η αποτέφρωση ή ο καθαρισμός των σκληρών δίσκων. Τα μέτρα ασφαλούς απόρριψης μπορούν να βοηθήσουν στην αποτροπή παραβιάσεων δεδομένων και μπορούν να βοηθήσουν να διασφαλιστεί ότι τα ευαίσθητα δεδομένα δεν θα πέσουν σε λάθος χέρια.

6.2 Firewall

Σημαντικό κομμάτι του air-gapped δικτύου αποτελεί το τείχος προστασίας που παρακολουθεί και ελέγχει την εισερχόμενη και εξερχόμενη κυκλοφορία με βάση

Attacks, and Mitigations", 2016.

[50] J. Loughry and A. D. Umphress, "Information leakage from optical emanations" pp. 262-289, 2002.

[51] https://www.signalsdefense.com/products

προκαθορισμένους κανόνες ασφαλείας. Τρόποι με τους οποίους μπορεί να χρησιμοποιηθεί ένα firewall είναι:

- **Perimeter Firewall:** Ένα περιμετρικό τείχος προστασίας τοποθετείται στην άκρη του δικτύου, μεταξύ αυτού και του Διαδικτύου ή άλλων εξωτερικών δικτύων. Βοηθάει στην αποτροπή μη εξουσιοδοτημένης πρόσβασης στο δίκτυο, αποκλείοντας την κυκλοφορία από πηγές που δεν συμμορφώνονται με τις πολιτικές ασφαλείας του.
- **Internal Firewall:** Ένα εσωτερικό τείχος προστασίας τοποθετείται εντός του δικτύου, μεταξύ διαφορετικών τμημάτων ή ζωνών του και βοηθάει στην πρόληψη της πλευρικής κίνησης, εμποδίζοντας την κυκλοφορία από το ένα στο άλλο σε περίπτωση παραβίασης.
- **Application Firewall:** Το τείχος προστασίας εφαρμογών έχει σχεδιαστεί για την προστασία συγκεκριμένων εφαρμογών ή υπηρεσιών από επιθέσεις, αποκλείοντας την κυκλοφορία που δεν συμμορφώνεται με τις πολιτικές ασφαλείας της εφαρμογής.
- **Deep Packet Inspection:** Ένα DPI εξετάζει τα περιεχόμενα των πακέτων για να προσδιορίσει εάν περιέχουν malicious περιεχόμενο ή άλλους κινδύνους ασφαλείας. Μπορεί να χρησιμοποιηθεί για τον αποκλεισμό κίνησης που περιέχει ιούς, malware ή άλλους τύπους κακόβουλου περιεχομένου.

Είναι σημαντικό να ελέγχονται και να ενημερώνονται τακτικά οι κανόνες ενός firewall για να διασφαλίζεται ότι παραμένουν αποτελεσματικοί με την πάροδο του χρόνου.

6.3 Network Monitoring

Ακόμα ένα απαραίτητο στοιχείο σε ένα air-gapped δίκτυο είναι η παρακολούθηση του για τον εντοπισμό πιθανών παραβιάσεων και τυχόν ανωμαλιών στην κυκλοφορία του. Ακολουθούν τρόποι με τους οποίους το network monitoring συμβάλλει στην ενίσχυση της ασφάλειας:

- **Security Information & Event Management (SIEM):** Αποτελεί το πρωταρχικό εργαλείο συγκέντρωσης και ανάλυσης δεδομένων καταγραφής διαφόρων πηγών, όπως συσκευών δικτύου, servers και εφαρμογές. Αυτό βοηθάει στον εντοπισμό μοτίβων που μπορεί να υποδηλώνουν επίθεση ή παραβίαση.
- **Intrusion Detection Systems (IDS):** Ένα σύστημα ανίχνευσης εισβολής μπορεί να εγκατασταθεί σε διάφορα σημεία του δικτύου, όπως στην περίμετρό του ή σε μεμονωμένες

συσκευές. Χρησιμοποιείται για την παρακολούθηση της κυκλοφορίας, την ανίχνευση ύποπτης δραστηριότητας και σκοπός του είναι να προειδοποιεί.

- **Intrusion Prevention System (IPS):** Ένα σύστημα πρόληψης εισβολής χρησιμοποιείται σε συνδυασμό με ένα IDS και δουλειά του είναι να λαμβάνει ενεργά μέτρα για να αποτρέπει την επιτυχία των επιθέσεων. Παρακολουθεί και αναλύει την κυκλοφορία του δικτύου σε πραγματικό χρόνο ώστε να μπλοκάρει άμεσα μια εσωτερική απειλή που επιχειρεί να συνδέσει για παράδειγμα μια μη εξουσιοδοτημένη συσκευή στο δίκτυο ή χρησιμοποιεί μια μονάδα USB για εξαγωγή ευαίσθητων δεδομένων.
- **Traffic Analysis:** Η ανάλυση της κίνησης του δικτύου συμβάλλει και αυτή στον εντοπισμό ασυνήθιστων μοτίβων από μη εξουσιοδοτημένες πηγές, που προσπαθούν να εισάγουν ή να εξάγουν δεδομένα.
- **Vulnerability Scanning:** Τακτικές σαρώσεις για ευπάθειες στο δίκτυο βοηθούν στον εντοπισμό πιθανών αδυναμιών που θα μπορούσαν να εκμεταλλευτούν οι εισβολείς. Έπειτα είναι δουλεία της ομάδας να λάβει προληπτικά μέτρα για την αντιμετώπιση αυτών των αδυναμιών και την μείωση του κινδύνου παραβίασης.
- **User Activity Monitoring:** Αρκετά σημαντική η παρακολούθηση της δραστηριότητας των χρηστών απ' όπου μπορούν να εντοπιστούν ασυνήθιστες συμπεριφορές που θα υποδηλώνουν την παρουσία ενός insider threat. Επιπλέον ενέργειες θα χρειαστούν και εδώ για το μπλοκάρισμα του χρήστη και την αποτροπή κλοπής δεδομένων.

6.4 Anti-Malware Protection

Anti-malware λογισμικό είναι απαραίτητο να χρησιμοποιείται σε ένα air-gapped network ώστε να υπάρχει έλεγχος κατά την εισαγωγή αφαιρούμενων μέσων. Πρακτικά σαρώνει οποιαδήποτε μονάδα εισέρχεται στο δίκτυο και αποτρέπει την εισαγωγή ή εκτέλεση malicious κώδικα σε αυτό. Διάφοροι τρόποι ενίσχυσης της ασφάλειας μέσω anti-malware protection είναι:

- **Endpoint Protection:** Πρόκειται για το λογισμικό προστασίας endpoint που έχει σχεδιαστεί για να προστατεύει μεμονωμένες συσκευές όπως φορητούς υπολογιστές, επιτραπέζιους υπολογιστές και διακομιστές από malware. Με δυνατότητες εντοπισμού και αφαίρεσης malware ή αποτροπής λήψης το λογισμικό θωρακίζει το air-gapped δίκτυο από το να παραβιαστεί.

- **Network-based Anti-Malware:** Μία anti-malware προστασία που σε δικτυακό επίπεδο είναι σχεδιασμένη να εντοπίζει και να αφαιρεί τυχόν κακόβουλο λογισμικό, το οποίο μεταδίδεται μέσω του δικτύου. Τέτοιο λογισμικό συνήθως εισάγεται μέσω αφαιρούμενων μονάδων.
- **Malware Analysis:** Σημαντική διαδικασία αποτελεί η ανάλυση malware σε ελεγχόμενο περιβάλλον. Όσο περισσότερο κατανοητή γίνεται η συμπεριφορά ενός malware τόσο βελτιώνεται και η ανάπτυξη στρατηγικών για εντοπισμό και αφαίρεσή του.
- **Regular Updates:** Με καινούρια CVE να παρουσιάζονται τακτικά, οι μηχανικοί ασφαλείας οφείλουν να κρατούν ενημερωμένο όλο το anti-malware λογισμικό προστασίας, ώστε να διασφαλίζεται η αποτελεσματικότητά του και έναντι των πρόσφατων κακόβουλων απειλών.
- **Software and Applications Updates:** Από τις πιο σημαντικές διαδικασίες η ενημέρωση των συστημάτων, των εφαρμογών και του λογισμικού που χρησιμοποιούν οι air-gapped υπολογιστές και διακομιστές, πρέπει να γίνεται σε τακτική βάση, με αρχεία από έμπιστες ιστοσελίδες και οργανισμούς χωρίς ωστόσο να παραλείπονται οι διαδικασίες ελέγχου για malware σε αυτά.

6.5 Access Controls

Τα στοιχεία ελέγχου πρόσβασης πρέπει να χρησιμοποιούνται για τον περιορισμό της πρόσβασης μόνο σε εξουσιοδοτημένο προσωπικό και συσκευές στο air-gapped δίκτυο. Αυτό επιτυγχάνεται με την χρήση strong passwords, multi-factor authentication και role-based access control. Ποιο αναλυτικά πρέπει να υλοποιούνται τα εξής:

- **User Authentication:** Πρόκειται για διαδικασία επαλήθευσης της ταυτότητας ενός χρήστη που επιχειρεί να αποκτήσει πρόσβαση στο δίκτυο, είτε μέσω απλού username-password, two factor authentication μέχρι χρήση βιομετρικών.
- **Device Authentication:** Πρόκειται για διαδικασία επαλήθευσης της ταυτότητας μιας συσκευής που επιχειρεί να αποκτήσει πρόσβαση στο δίκτυο, συνήθως με τη χρήση ψηφιακών πιστοποιητικών ή άλλων μορφών αναγνώρισης συσκευών.
- **Role-Based Access Control (RBAC):** Είναι μία μέθοδος ελέγχου πρόσβασης που εκχωρεί δικαιώματα με βάση τους ρόλους μεμονωμένων χρηστών. Για παράδειγμα, οι χρήστες με administrative privileges έχουν πρόσβαση σε πόρους που δεν έχουν οι κανονικοί χρήστες.

Επομένως το RBAC διασφαλίζει ότι οι χρήστες έχουν πρόσβαση μόνο στους πόρους που χρειάζονται για την εκτέλεση των εργασιακών τους καθηκόντων.

- **Disable USB ports:** Η απενεργοποίηση ή και αφαίρεση των USB θυρών από τους περισσότερους υπολογιστές του air-gapped δικτύου αποτελεί μεγάλο και σημαντικό κομμάτι της θωράκισής του. Προφανώς ορισμένες θύρες θα πρέπει να συνεχίζουν να υπάρχουν ώστε να μεταφέρονται τα δεδομένα και να γίνονται τα απαραίτητα updates, αλλά οφείλουν να είναι σε συγκεκριμένους υπολογιστές, να χρησιμοποιούνται μόνο από εξουσιοδοτημένο προσωπικό και η όποια κίνηση σε αυτές να καταγράφεται με ακρίβεια.
- **Restrict file execution on removable drives:** Μία τεχνική παραβίασης των air-gapped συστημάτων αποτελεί και η απευθείας εκτέλεση ενός εκτελέσιμου αρχείου που είναι κάπου αποθηκευμένο στην αφαιρούμενη μονάδα. Αυτό αποτρέπεται ρυθμίζοντας τις σχετικές *Removable Storage Access* πολιτικές σε όλα τα συστήματα του δικτύου.
- **Network Segmentation:** Η διαίρεση του δικτύου σε μικρότερα υποδίκτυα, με το καθένα να έχει το δικό του σύνολο από access controls, βοηθάει στον περιορισμό του αντικτύπου μιας πιθανής παραβίασης. Κρίσιμα συστήματα διαχωρίζονται και απομονώνονται από λιγότερο σημαντικά και σε περίπτωση παραβίασης του δικτύου αποτρέπεται η πλευρική μετακίνηση των εισβολέων.
- **Access Logs:** Σημαντικό κομμάτι του δικτύου αποτελούν τα αρχεία καταγραφής πρόσβασης. Διατηρώντας λεπτομερή αρχεία με το ποιος και πότε απέκτησε ή προσπάθησε να αποκτήσει πρόσβαση κάπου εντός του δικτύου, βοηθούν τον υπεύθυνο διαχειριστή που τα παρακολουθεί, να εντοπίζει τυχόν προσπάθειες μη εξουσιοδοτημένης πρόσβασης. Τέλος μπορούν να χρησιμοποιηθούν και για forensic analysis σε περιστατικό παραβίασης δεδομένων.

Εφαρμόζοντας τα παραπάνω αντίμετρα είναι πρακτικά αδύνατον η δραστηριότητα ενός εισβολέα στο air-gapped δίκτυο να μην αφήσει ίχνη και να περάσει απαρατήρητη.

6.6 Security Awareness Training

Είναι σημαντικό να υπάρχει ένα πρόγραμμα εκπαίδευσης για τους εργαζομένους σχετικά με τη σημασία της ασφάλειας και τους κινδύνους που συνδέονται με τη χρήση αφαιρούμενων μέσων και άλλων εξωτερικών συσκευών σε ένα air-gapped δίκτυο. Κάτι τέτοιο μπορεί να λειτουργήσει σαν αποτρεπτικός παράγοντας στην δημιουργία παραβιάσεων που προκαλούνται από ανθρώπινο λάθος. Πιο συγκεκριμένα:

- **Social Engineering Awareness:** Εφόσον οι social engineering επιθέσεις αποτελούν κοινή μέθοδο για την απόκτηση πρόσβασης σε ένα δίκτυο, η εκπαίδευση των υπαλλήλων στην αναγνώριση και αποφυγή τέτοιων ψυχολογικών χειραγωγήσεων θα λειτουργήσει ως ασπίδα.
- **Password Security:** Οι κωδικοί πρόσβασης συχνά αποτελούν την πρώτη γραμμή άμυνας ενάντια στους επιτιθέμενους. Χρειάζεται επομένως μια σωστή εκπαίδευση των υπαλλήλων σχετικά με την σημασία που έχει ο κωδικός, την μοναδικότητα με την οποία θα πρέπει να εφαρμόζεται, την τυχαιότητα που θα έχει με το άτομο που τον κατέχει, την πολυπλοκότητα αλλά και το που θα βρίσκεται αποθηκευμένος.
- **Device Security:** Θα πρέπει να επισημανθεί επίσης, πως οι εργαζόμενοι απαγορεύεται να χρησιμοποιήσουν και να συνδέσουν τις προσωπικές τους συσκευές για πρόσβαση στο air-gapped δίκτυο, μιας και μπορεί να περιέχουν ιούς και άλλα malicious frameworks που θα περάσουν σε αυτό.

Παρέχοντας σεμινάρια και συνεδρίες εκπαίδευσης διατηρούνται οι υπάλληλοι ενημερωμένοι σχετικά με τις πιο πρόσφατες απειλές και διαμορφώνεται μία κουλτούρα ασφάλειας εντός του οργανισμού.

6.7 Use of Secure Hardware

Το hardware ενός air-gapped δικτύου πρέπει να επιλέγεται και να σχεδιάζεται σωστά ώστε να πληροί αυστηρά πρότυπα ασφαλείας και να προστατεύει τον οργανισμό από πιθανές επιθέσεις. Τέτοια παραδείγματα αποτελούν:

- **Trusted Platform Module:** Το TPM είναι ένα hardware στοιχείο ενσωματωμένο στη motherboard ενός υπολογιστή. Χρησιμοποιεί κρυπτογράφηση αποθηκεύοντας βασικές και κρίσιμες πληροφορίες ώστε να γίνεται έλεγχος ταυτότητας. Πρακτικά, αποθηκεύονται credentials χρήστη, κωδικοί πρόσβασης, δακτυλικά αποτυπώματα, πιστοποιητικά και κρυπτογραφικά κλειδιά, ούτως ώστε κατά την ενεργοποίηση ενός Η/Υ το TPM αυθεντικοποιεί την συσκευή, ξεκλειδώνει την κρυπτογραφημένη μονάδα δίσκου και τον εκκινεί κανονικά. Σε περίπτωση παραποίησης του κλειδιού προφανώς δεν γίνεται εκκίνηση του υπολογιστή.
- **Encrypted USB Drives:** Η κρυπτογράφηση των αφαιρούμενων αποθηκευτικών μέσων, με BitLocker ή άλλο λογισμικό, είναι απαραίτητη για την μεταφορά ευαίσθητων

δεδομένων από και προς το air-gapped δίκτυο. Στην περίπτωση που ένας υπολογιστής εκτός δικτύου είναι μολυσμένος με malware, αυτό θα περάσει και στο USB drive κατά την είσοδό του. Εάν, ωστόσο, το USB χρησιμοποιεί κρυπτογράφηση τότε τα δεδομένα που περιέχει θα παραμείνουν ασφαλή και ακέραια.

- **Self-Erasing USB Drives:** Πρόκειται για μονάδες USB σχεδιασμένες να διαγράφουν το περιεχόμενό τους αυτόματα μετά από ορισμένο χρονικό διάστημα αδράνειας. Ωστόσο format της USB μονάδας θα πρέπει να γίνεται κάθε φορά που χρησιμοποιείται, πριν και μετά το πέρας της όποιας μεταφοράς, ώστε να αποφεύγονται τυχόν κακόβουλα αρχεία βρίσκονται εντός της μονάδας.
- **Secure Processors:** Επεξεργαστές σχεδιασμένοι να είναι ανθεκτικοί σε side-channel επιθέσεις. Μια τέτοια επίθεση εκμεταλλεύεται τις αδυναμίες στις φυσικές ιδιότητες του επεξεργαστή για την εξαγωγή ευαίσθητων πληροφοριών.
- **Powerline Signal Filtering:** Τα φίλτρα στις γραμμές του ρεύματος περιορίζουν την διαρροή της αγωγιμότητας και του θορύβου ακτινοβολίας[52] [53] [54] [55]. Τέτοια φίλτρα, γνωστά και ως φίλτρα EMI, έχουν σχεδιαστεί για λόγους ασφαλείας, καθώς ο θόρυβος που δημιουργείται από μια συσκευή στο δίκτυο τροφοδοσίας μπορεί να επηρεάσει άλλες συσκευές, προκαλώντας δυσλειτουργία τους. Με την τοποθέτησή τους στον κύριο ηλεκτρικό πίνακα του καναλιού του air-gapped δικτύου περιορίζεται το σήμα που παράγεται σε αυτό και έτσι μπορούν να αποφευχθούν line level power-hammering επιθέσεις. Χρειάζεται να εγκατασταθούν φίλτρα και σε κάθε πρίζα μεταξύ αυτής και του τροφοδοτικού του H/Y ή και ενσωματωμένα εντός του τροφοδοτικού[56].
- **Secure Printers:** Εκτυπωτές οι οποίοι διαθέτουν λειτουργίες όπως ασφαλής εκκίνηση, κρυπτογράφηση και εκκαθάριση σκληρού δίσκου που βοηθούν στην προστασία από μη εξουσιοδοτημένη πρόσβαση σε έντυπα έγγραφα.

[52] D. Liu and J. Jiang, “High frequency characteristic analysis of EMI filter in switch mode power supply (smps)”, pp. 2039–2043, 2002.
[53] S. Ye, W. Eberle, and Y.-F. Liu, “A novel EMI filter design method for switching power supplies”, pp. 1668–1678, 2004.
[54] F.-Y. Shih, D. Y. Chen, Y.-P. Wu, and Y.-T. Chen, “A procedure for designing EMI filters for ac line applications”, pp. 170–181, 1996.
[55] F. Lin and D. Y. Chen, “Reduction of power supply EMI emission by switching frequency modulation”, pp. 132–137, 1994.
[56] P. counterWolmarans, J. Van Wyk, and C. Campbell, “Technology for integrated rf-emi transmission line filters for integrated power electronic modules”, pp. 1774–1780, 2002.

ΚΕΦΑΛΑΙΟ 7ο : ΤΡΟΠΟΙ ΓΕΦΥΡΩΣΗΣ ΣΕ ΣΥΝΔΕΔΕΜΕΝΟ ΔΙΚΤΥΟ

Αναπόσπαστο κομμάτι ενός air-gapped δικτύου αποτελεί η σύνδεση που έχει με άλλα δίκτυα συνδεδεμένα στο Διαδίκτυο. Τα περισσότερα απομονωμένα δίκτυα συχνά πρέπει να ανταλλάσσουν δεδομένα με άλλα δίκτυα, αλλά και να ενημερώνουν τα συστήματα και τις εφαρμογές τους. Για να γίνουν τα απαραίτητα updates χρειάζονται αρχεία που είναι παρμένα από το Διαδίκτυο και μπορεί ωστόσο να κρύβουν ιούς. Θα παρουσιασθούν τρόποι και τεχνικές για το πως μπορεί να επιτευχθεί ασφαλής γεφύρωση δικτύων air-gapped και μη, διασφαλίζοντας της προστασία και ακεραιότητα των δεδομένων.

7.1 Sneakernet

Με τον όρο sneakernet περιγράφεται η μεταφορά δεδομένων με φυσικό τρόπο, όπως η αντιγραφή αρχείων σε δισκέτα, CD, εξωτερικό δίσκο ή USB μονάδα από έναν υπολογιστή σε έναν άλλον. Πρόκειται για κοινή μέθοδο που χρησιμοποιείται για εισαγωγή και εξαγωγή data σε air-gapped συστήματα και ασφαλή περιβάλλοντα.

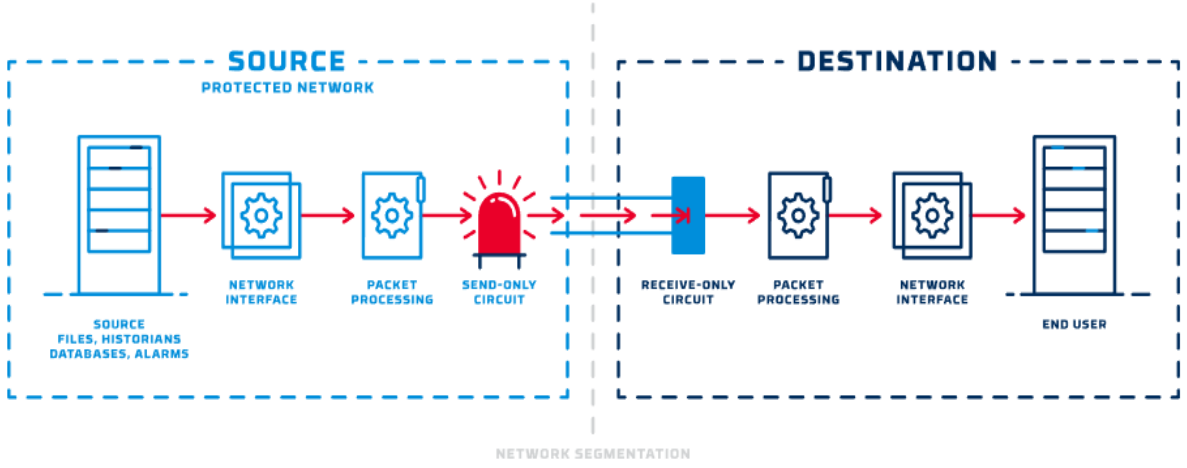
Για να διατηρείται η ασφάλεια, τα αφαιρούμενα μέσα πρέπει να σαρώνονται για κακόβουλο λογισμικό πριν από τη χρήση και να χρησιμοποιούνται με αυστηρά πρωτόκολλα. Οι αφαιρούμενες μονάδες πρέπει να χρησιμοποιούνται μόνο για τη μεταφορά δεδομένων προς και από το δίκτυο και δεν πρέπει να έρχονται σε επαφή με άλλα συστήματα. Τέλος μετά από κάθε διαδικασία θα πρέπει να σβήνεται το περιεχόμενό τους και να πραγματοποιείται format.

Το Sneakernet απαιτεί προσεκτικό σχεδιασμό και αυστηρά πρωτόκολλα ασφαλείας για να διασφαλιστεί ότι τα δεδομένα παραμένουν ασφαλή και ότι δεν εισάγεται κακόβουλο λογισμικό στο air-gapped δίκτυο. Συχνά είναι χρονοβόρα και επιρρεπής σε ανθρώπινο λάθος μέθοδος, και επομένως θα πρέπει να χρησιμοποιείται ως έσχατη λύση όταν δεν είναι δυνατές άλλες ασφαλείς μέθοδοι μεταφοράς δεδομένων.

7.2 One-way Transfer Protocol

Αυτή η μέθοδος επιτρέπει τη μεταφορά δεδομένων από το air-gapped δίκτυο σε ένα συνδεδεμένο δίκτυο, αλλά όχι το αντίστροφο. Αυτό μπορεί να επιτευχθεί χρησιμοποιώντας hardware devices, όπως data diodes.

Οι data diodes είναι εξειδικευμένες συσκευές hardware που επιτρέπουν μονόδρομη μεταφορά δεδομένων μεταξύ δικτύων. Φυσικά η ροή δεδομένων προς την αντίθετη κατεύθυνση αποτρέπεται, μαζί και οποιεσδήποτε τυχόν πιθανές επιθέσεις από το συνδεδεμένο δίκτυο. Χρησιμοποιούνται συνήθως σε περιβάλλοντα υψηλής ασφάλειας, όπως στρατιωτικοί, κυβερνητικοί και χρηματοπιστωτικοί οργανισμοί για προστασία από απειλές στον κυβερνοχώρο, όπως παραβιάσεις δεδομένων, κακόβουλο λογισμικό και απόπειρες εισβολής. Ορισμένες δίοδοι χρησιμοποιούν οπτικές ίνες ή άλλα φυσικά μέσα για τη δημιουργία ενός μονόδρομου καναλιού επικοινωνίας, ενώ άλλες χρησιμοποιούν software για να δημιουργήσουν μια virtual μονόδρομη σύνδεση. Οι δίοδοι δεδομένων, ωστόσο, είναι ακριβείς και απαιτούν τεχνογνωσία για την εφαρμογή και τη συντήρηση τους.



Εικόνα 25 Data Diode's one-way transfering

7.3 Virtualization

Αυτή η μέθοδος περιλαμβάνει την εκτέλεση μιας virtual machine σε έναν φυσικά απομονωμένο υπολογιστή που είναι συνδεδεμένος τόσο στο air-gapped δίκτυο όσο και στο συνδεδεμένο δίκτυο. Τα δεδομένα μπορούν να μεταφερθούν προς και από την virtual machine, η οποία είναι απομονωμένη και προστατεύεται από αυστηρά πρωτόκολλα ασφαλείας. Αυτό επιτρέπει μεγαλύτερη ευελιξία από τη One-way Transfer Protocol μέθοδο, καθώς τα δεδομένα μπορούν να μεταφερθούν και προς τις δύο κατευθύνσεις.

Ωστόσο, η virtualization απαιτεί τεχνογνωσία στη ρύθμιση και τη συντήρηση των virtual machines, καθώς και στη διασφάλιση ότι η μηχανή είναι σωστά ασφαλισμένη και απομονωμένη και από τα δύο δίκτυα. Οποιαδήποτε δεδομένα μεταφέρονται από ή προς πρέπει να σαρώνονται και να επαληθεύονται διεξοδικά για κακόβουλο λογισμικό πριν και μετά τη μεταφορά.

ΚΕΦΑΛΑΙΟ 8ο : ΕΠΙΛΟΓΟΣ

Στην εργασία αυτή έγινε αξιολόγηση των δυνατοτήτων και της ασφάλειας που προσφέρει ένα air-gapped δίκτυο. Περιγράφησαν οι διαφορετικές παραλλαγές του, που υπάρχουν ανά οργανισμούς, σύμφωνα πάντα με τις ανάγκες και δυναμικές του καθένα εξ αυτών. Έγινε αναφορά των θετικών στοιχείων από τα οποία επωφελείται μια εταιρεία που διατηρεί ένα τέτοιο δίκτυο, επισημάνθηκαν ωστόσο και τα αρνητικά στοιχεία, τα οποία πρέπει να προσέξει, ώστε τα δεδομένα της να μην κινδυνεύουν να διαρρεύσουν. Για τον λόγο αυτό αναλύθηκαν περεταίρω οι ευπάθειες και τα τρωτά σημεία από τα οποία πάσχουν, ορισμένες φορές, αυτά τα δίκτυα και έγινε αντιληπτή η καθοριστική σημασία που παίζει το ανθρώπινο λάθος στις μέρες μας. Υπάλληλοι και στελέχη πρέπει να ενημερώνονται καθημερινά για τους νέους τρόπους συναισθηματικής χειραγώγησης ή πονηριάς που "σκαρφίζονται" οι hacker ώστε να υποκλέψουν κωδικούς και στοιχεία από αυτούς και εν συνεχεία να διεισδύσουν σε λογαριασμούς της εταιρείας και στα απομονωμένα δίκτυα. Εντρυφώντας σε εκείνα τα λογισμικά που κάνουν και την περισσότερη ζημιά, τα λεγόμενα malware, πραγματοποιήθηκε μια επισκόπηση από το παρελθόν έως το σήμερα στο πως κατάφεραν να διεισδύσουν τελικά στα air-gapped δίκτυα. Έτσι, μαθαίνοντας από τα λάθη, οι εταιρείες του σήμερα οφείλουν να θωρακίσουν όσον το δυνατόν καλύτερα τα συστήματα τους και να λάβουν τα κατάλληλα αντίμετρα ώστε να είναι σε θέση να προλάβουν και να σταματήσουν έγκαιρα καταστάσεις και απειλές που παλαιότερα θα είχαν καταστροφικά αποτελέσματα, τόσο για τις ίδιες όσο και για όσες άλλες εταιρείες που εξαρτώνται από αυτές και ανήκουν στην εφοδιαστική αλυσίδα τους. Τέλος, οι γρήγορες εξελίξεις και η όλο και αυξανόμενη χρήση του cloud και των εφαρμογών του απαιτεί από τα απομονωμένα αυτά δίκτυα να διαθέτουν, ακόμα και σε real time, τα δεδομένα τους για ανταλλαγή πληροφοριών. Παρουσιάζονται λοιπόν, τρόποι επικοινωνίας και ανταλλαγής δεδομένων από και προς τα air-gapped δίκτυα με άλλα δίκτυα συνδεδεμένα στο Internet, ούτως ώστε να πραγματοποιείται και ενημέρωση των συστημάτων και εφαρμογών τους, κάτι που είναι απαραίτητο για την ομαλή λειτουργία των ίδιων.

ΠΑΡΑΡΤΗΜΑ

6.1 Αντιστοιχίσεις όρων

Αγγλικά	*Ελληνικά*
Account	Λογαριασμός
Actor	Ηθοποιός
Administrator	Διαχειριστής
Air-gapped Network	Δίκτυο απομονωμένο από το Διαδίκτυο
Antivirus	Προστασία από ιούς
Applications	Εφαρμογές
APT (Advanced Persistence Threat)	Προηγμένη Επίμονη Απειλή
Attack vector	Μέθοδος επίθεσης
Backup	Αντίγραφο Ασφαλείας
BEC (Business Email Compromise)	Παραβίαση Εταιρικής Αλληλογραφίας
CEO (Chief Executive Officer)	Διευθύνων Σύμβουλος
Client	Πελάτης
Clone	Κλώνος
Cloud	Νέφος
Commercial networks	Εμπορικά δίκτυα
Component	Στοιχείο – Κομμάτι
Compromise	Παραβίαση
Connected	Συνδεδεμένος
CPU (Central Processing Unit)	Κεντρική Μονάδα Επεξεργασίας
Cyber-criminals	Εγκληματίες του Κυβερνοχώρου
Data Bus	Δίαυλος Δεδομένων
Deeper	Βαθύτερη
Drives	Δίσκοι
EMI (Electromagnetic Interference)	Ηλεκτρομαγνητικές Παρεμβολές
Encryption keys	Κλειδιά κρυπτογράφησης
Engineer	Μηχανικός
ERP (Enterprise Resource Planning)	Σχεδιασμός Επιχειρηματικών Πόρων

Establish	Εγκαθιδρύω
Exploit	Εκμετάλλευση
Firmware	Είδος λογισμικού γραμμένο σε γλώσσα μηχανής
FM (Frequency Modulation)	Διαμόρφωση συχνότητας
Foothold	Παραθυράκι
Framework	Πλαίσιο / Δομή
Fraud	Απατεώνας
FTP (File Transfer Protocol)	Πρωτόκολλο Μεταφοράς Αρχείων
Gain	Κέρδος
GPU (Graphics Processing Unit)	Κάρτα Γραφικών
GSM (Global System for Mobile communications)	Ευρωπαϊκό Ψηφιακό Σύστημα Κινητής Τηλεφωνίας
Hacker	Χάκερ - Άτομο που αποκτά παράνομη πρόσβαση σε υπολογιστικό σύστημα
Hardware	Όλα τα υλικά μέρη που απαρτίζουν έναν υπολογιστή
HDD (Hard Disk Drive)	Σκληρός Δίσκος
Hidden	Κρυμμένος
IDS (Intrusion Detection System)	Σύστημα Ανίχνευσης Εισβολής
Insider	Γνώστης - Έμπιστος
Installer	Εγκαταστάτης
IPS (Intrusion Prevention System)	Σύστημα Αποτροπής Εισβολής
Isolated	Απομονωμένος
Kernel	Πυρήνας
Keylogging	Καταγραφή πληκτρολόγησης
Laptop	Φορητός υπολογιστής
LED (Light Emitting Diode)	Λαμπτήρας Φωτισμού (Δίοδος Εκπομπής Φωτός)

License	Άδεια
Links	Σύνδεσμοι
Logical	Λογικός
Malware	Είδος κακόβουλου λογισμικού
Modification	Τροποποίηση
Move Laterally	Πλευρική Μετακίνηση
Network	Δίκτυο
NIC (Network Interface Controller)	Ελεγκτής Διεπαφής Δικτύου
Offline	Εκτός σύνδεσης
One-way Transfer Protocol	Πρωτόκολλο μονόδρομης μεταφοράς
Passwords	Κωδικοί πρόσβασης
Patches	Ενημερώσεις Κώδικα
Primary persistence mechanism	Πρωταρχικός μηχανισμός επιμονής
Privileged	Προνομιούχος
Rack	Ράφι
RAM (Random Access Memory)	Μνήμη τυχαίας προσπέλασης
Ransomware	Είδος κακόβουλου λογισμικού
RCE (Remote Code Execution)	Απομακρυσμένη Εκτέλεση Κώδικα
Recovery	Ανάκτηση
Remote management	Απομακρυσμένη διαχείριση
Removable storage media	Αφαιρούμενα μέσα αποθήκευσης
Router	Δρομολογητής δικτύου
SAP (Systems Applications and Products)	Συστήματα Εφαρμογών και Προϊόντων

SCADA (Supervisory Control And Data Acquisition)	Εποπτικός Έλεγχος Και Απόκτηση Δεδομένων
Script file	Αρχείο κειμένου που περιέχει μία ακολουθία εντολών
Segmentation	Κατάτμηση
Server	Διακομιστής
Services	Υπηρεσίες
Shell	Φλοιός
Side-loading	Πλευρική φόρτωση
SIEM (Security Information and Event Management)	Ασφάλεια Πληροφοριών και Διαχείριση Συμβάντων
Social Engineering	Κοινωνική Μηχανική
Software	Λογισμικό
SSH (Secure Socket Shell)	Κέλυφος Ασφαλών Υποδοχών
Stealthy	Κρυφός
Supply-chain attack	Επίθεση στην αλυσίδα εφοδιασμού
Third-party attack	Επίθεση τρίτου μέρους
Threat	Απειλή
Thumb Drive	Άλλη ονομασία για το USB
Transmitter	Πομπός
Trojan	Κακόβουλο αρχείο που παρουσιάζεται ως νόμιμος κώδικας ή λογισμικό
USB (Universal Serial Bus) flash	Αποσπώμενη μονάδα αποθηκευτικού χώρου
Virtual machine	Εικονικό μηχάνημα
Vulnerabilities	Αδυναμίες – Τρωτά σημεία
Weaponizing	Οπλοφορία

Worms	Σκουλήκια
Zero-day	Ημέρα μηδέν

Πίνακας 7 Αντιστοιχίσεις όρων