ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

Σχολή Τεχνολογίας

Τμήμα Ψηφιακών Συστημάτων

Μελέτη Επιθέσεων και Τεχνικές Κυβερνοασφάλειας σε Δίκτυα Επικοινωνιών

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Θεμιστοκλής Προμυριώτης (ΑΜ: 3119069)

Επιβλέπων: ***Απόστολος Ξενάκης, Επίκουρος Καθηγητής***

ΛΑΡΙΣΑ, Μάρτιος 2024

UNIVERSITY OF THESSALY

School of Technology

Digital Systems Department

A Study of Attacks and Cybersecurity Techniques in Communication Networks

BACHELOR THESIS

Themistoklis Promyriotis (RN: 3119069)

Supervisor: ***Apostolos Xenakis, Assistant Professor***

LARISSA, March 2024

Υπεύθυνη Δήλωση περί Ακαδημαϊκής Δεοντολογίας και Πνευματικών Δικαιωμάτων

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, δηλώνω ρητά ότι η παρούσα πτυχιακή εργασία, καθώς και τα ηλεκτρονικά αρχεία και πηγαίοι κώδικες που αναπτύχθηκαν ή τροποποιήθηκαν στα πλαίσια αυτής της εργασίας, αποτελεί αποκλειστικά προϊόν προσωπικής μου εργασίας, δεν προσβάλλει κάθε μορφής δικαιώματα διανοητικής ιδιοκτησίας, προσωπικότητας και προσωπικών δεδομένων τρίτων, δεν περιέχει έργα/εισφορές τρίτων για τα οποία απαιτείται άδεια των δημιουργών/δικαιούχων και δεν είναι προϊόν μερικής ή ολικής αντιγραφής, οι πηγές δε που χρησιμοποιήθηκαν περιορίζονται στις βιβλιογραφικές αναφορές και μόνον, και πληρούν τους κανόνες της επιστημονικής παράθεσης. Τα σημεία όπου έχω χρησιμοποιήσει ιδέες, κείμενο, αρχεία ή/και πηγές άλλων συγγραφέων, αναφέρονται ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή.

Αναλαμβάνω πλήρως, ατομικά και προσωπικά, όλες τις νομικές και διοικητικές συνέπειες που δύναται να προκύψουν στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δεν μου ανήκει διότι είναι προϊόν λογοκλοπής.

Ο/Η Δηλών/ούσα

(Υπογραφή)

Θεμιστοκλής Προμυριώτης

04/03/2024

Εγκρίνεται από την Επιτροπή Εξέτασης:

Επιβλέπων/πουσα	**Απόστολος Ξενάκης** Επίκουρος Καθηγητής, Τμήμα Ψηφιακών Συστημάτων
Μέλος	**Κωνσταντίνος Χαϊκάλης** Αναπληρωτής Καθηγητής, Τμήμα Ψηφιακών Συστημάτων
Μέλος	**Όμηρος Ιατρέλλης** Επίκουρος Καθηγητής, Τμήμα Ψηφιακών Συστημάτων

Ημερομηνία έγκρισης: 04-03-2024

Περίληψη

Η παρούσα πτυχιακή εργασία προσεγγίζει εκτενώς τον όρο "Διαδίκτυο των Πραγμάτων" (IoT) με στόχο την εμβάθυνση της κατανόησης του, εξετάζοντας διεξοδικά τη φύση ενος τέτοιου περιβάλλοντος από βασικές ωρολογίες, εφαρμογές στον κόσμο μας, προβλήματα και απειλές μέσω διαφόρων ειδών επιθέσεων μέχρι και ανάλυσης έξυπνων συσκευών και των χρήσεων τους.

Παράλληλα, παρουσιάζονται κάποια λογισμικά ανίχνευσης και ανάλυσης επιθέσεων, τα οποία αναδεικνύονται ως ζωτικά εργαλεία για τον αποτελεσματικό έλεγχο και την ενίσχυση της ασφάλειας συστημάτων IoT, αφού συνεισφέρουν στην ανίχνευση, ανάλυση και την πιθανή αντιμετώπιση πολλών πιθανών περιστατικών επιθέσεων.

Επίσης, η εργασία αναπτύσσει μελέτες πραγματικών περιστατικών επιθέσεων, προσφέροντας συγκεκριμένα παραδείγματα του πραγματικού κόσμου για την εμβάθυνση στον χαρακτήρα και τις πιθανές επιπτώσεις που μπορεί να επιφέρει. Μέσα από αυτήν την προσέγγιση, επισημαίνεται η σημασία της ανάπτυξης προηγμένων πρακτικών ασφαλείας, εστιάζοντας στη διασφάλιση της ακεραιότητας και της προστασίας των συστημάτων IoT από ενδεχόμενες απειλές και επιθέσεις.

Abstract

The present thesis extensively explores the term "Internet of Things" (IoT) with the aim of deepening our understanding, thoroughly examining the nature of such an environment, including fundamental concepts, real-world applications, challenges, and threats posed by various types of attacks.

Additionally, it introduces specific software for detecting and analyzing attacks, crucial tools for effective control and enhancement of the security of IoT systems, contributing to the detection, analysis, and potential mitigation of various attack incidents.

Furthermore, the thesis delves into case studies of real-world attack incidents, providing concrete examples to deepen our comprehension of the nature and potential consequences of such incidents. Through this comprehensive approach, the importance of developing advanced security practices is emphasized, focusing on ensuring the integrity and protection of IoT systems against potential threats and attacks.

Ευχαριστίες

Θέλω να εκφράσω ευχαριστίες μου προς τον καθηγητή μου και την οικογένεια μου για την ανεκτίμητη υποστήριξη τους κατά τη διάρκεια της εκπόνησης της πτυχιακής μου εργασίας. Ο καθηγητής μου, απέδειξε την επαγγελματική του δεξιοτεχνία και εμπειρία, καθοδηγώντας με σε κάθε μου βήμα προς την ολοκλήρωση του έργου μου. Η στήριξη και οι συμβουλές του με βοήθησαν να αναπτύξω τις ικανότητές μου και να κατανοήσω βαθύτερα το θέμα μου. Επίσης, θέλω να εκφράσω τη βαθιά μου ευγνωμοσύνη προς την οικογένειά μου για την συνεχή στήριξη, την ενθάρρυνση και την αγάπη τους.

Θεμιστοκλής Προμυριώτης

04/03/2024

Περιεχόμενα

1 Εισαγωγή

Το Διαδίκτυο των Πραγμάτων αποτελεί μια από τις πιο αναδυόμενες τεχνολογίες των τελευταίων ετών, καθώς έχει επαναπροσδιορίζει τον τρόπο με τον οποίο συνδέονται και αλληλεπιδρούν τα αντικείμενα γύρω μας. Με τη δυνατότητα σύνδεσης στο διαδίκτυο, τα πράγματα αποκτούν ικανότητες επικοινωνίας και ευφυΐα, επηρεάζοντας θεμελιωδώς τους τρόπους παραγωγής, διαχείρισης πόρων και αλληλεπίδρασης στην καθημερινή μας ζωή. Αυτή η καινοτομία σχεδιάζει ένα μέλλον όπου οι συσκευές αυτόματα ανταποκρίνονται στις ανάγκες μας, επηρεάζοντας θετικά την επίλυση προβλημάτων και τη βελτίωση της αποτελεσματικότητας σε διάφορους τομείς της ζωής μας.

Βασικό ορόσημο αποτελεί η χρονολογία 1982, με μια τροποποιημένη αυτόματη μηχανή πώλησης Coca-Cola στο Πανεπιστήμιο Carnegie Mellon να γίνεται η πρώτη συσκευή που συνδέθηκε στο ARPANET, ικανή να αναφέρει το απόθεμα της και εάν τα προσφάτως φορτωμένα αναψυκτικά ήταν κρύα ή όχι.

Το άρθρο του Mark Weiser του 1991 με θέμα ubiquitous computing, "Ο Υπολογιστής του 21ου αιώνα", καθώς και ακαδημαϊκές εκδηλώσεις όπως το UbiComp και το PerCom δημιούργησαν το σύγχρονο όραμα του IoT.

Το 1994, ο Reza Raji περιέγραψε τον συγκεκριμένο τομέα στο IEEE Spectrum ως τη μεταφορά μικρών πακέτων δεδομένων σε ένα μεγάλο σύνολο κόμβων, προκειμένου να ενσωματωθούν και να αυτοματοποιηθούν τα πάντα από οικιακές συσκευές έως ολόκληρα εργοστάσια. Μεταξύ του 1993 και του 1997, αρκετές εταιρείες πρότειναν λύσεις όπως η Microsoft at Work ή το NEST της Novell. Ο τομέας απέκτησε βλέψεις όταν ο Bill Joy φαντάστηκε την επικοινωνία μεταξύ συσκευών ως μέρος του πλαισίου των "Six Webs" του, που παρουσιάστηκε στο World Economic Forum στο Davos το 1999.

Ο όρος "Internet of Things" (Διαδίκτυο των Πραγμάτων) και η έννοια του εμφανίστηκαν για πρώτη φορά σε μια ομιλία του Peter T. Lewis, στο Congressional Black Caucus Foundation 15th Annual Legislative Weekend, που πραγματοποιήθηκε στην Ουάσιγκτον, D.C., και δημοσιεύτηκε τον Σεπτέμβριο του 1985. Σύμφωνα με τον Lewis, "Το Διαδίκτυο των Πραγμάτων, ή IoT, είναι η ενσωμάτωση ανθρώπων, διεργασιών και τεχνολογίας με συνδεδεμένες συσκευές και αισθητήρες για να

διευκολύνει την απομακρυσμένη παρακολούθηση, την κατάσταση, την αναστροφή και την αξιολόγηση των τάσεων αυτών των συσκευών".

Ο όρος "Internet of things" δημιουργήθηκε ανεξάρτητα από τον Kevin Ashton της Procter & Gamble, αργότερα του MIT Auto-ID Center, το 1999, αν και προτιμά τη φράση "Internet for things". Εκείνη την περίοδο, θεωρούσε τη ραδιοσυχνότητα αναγνώρισης (RFID) απαραίτητη για το Διαδίκτυο των Πραγμάτων, το οποίο θα επέτρεπε στους υπολογιστές να διαχειρίζονται όλα τα μεμονωμένα πράγματα. Το κύριο θέμα του Διαδικτύου των Πραγμάτων είναι να ενσωματώνονται κινητοί πομποδέκτες μικρής εμβέλειας σε διάφορες συσκευές και καθημερινές ανάγκες, προκειμένου να διευκολύνουν νέες μορφές επικοινωνίας μεταξύ ανθρώπων και πραγμάτων, καθώς και μεταξύ των πραγμάτων.

Το 2004, ο Cornelius "Pete" Peterson, CEO της NetSilicon, προέβλεψε ότι, "Η επόμενη εποχή της πληροφορικής θα κυριαρχείται από τις συσκευές IoT, και οι δικτυωμένες συσκευές θα αποκτήσουν τεράστια δημοφιλία και σημασία μέχρι το σημείο που θα υπερβούν κατά πολύ τον αριθμό των δικτυωμένων υπολογιστών και workstation." Ο Peterson πίστευε ότι οι ιατρικές συσκευές και οι βιομηχανικοί ελεγκτές θα γινόντουσαν κυρίαρχες εφαρμογές της τεχνολογίας.

Η Cisco Systems ορίζοντας το Διαδίκτυο των Πραγμάτων ως "απλώς τη στιγμή στο χρόνο όταν περισσότερα 'πράγματα ή αντικείμενα' συνδέονταν στο Διαδίκτυο από τους ανθρώπους", εκτίμησε ότι το IoT "γεννήθηκε" μεταξύ του 2008 και του 2009, με τον λόγο αντικειμένων/ανθρώπων να αυξάνεται από 0,08 το 2003 σε 1,84 το 2010.

2 Ο όρος «Διαδίκτυο Των Πραγματων»

Ο όρος της φράσης Διαδίκτυο των πραγμάτων ή Ίντερνετ των πραγμάτων (IoT - Internet of things) αναφέρεται σε ένα δίκτυο επικοινωνίας από μια πληθώρα συσκευών όπως οικιακών συσκευών ή συσκευών αυτοκινήτων καθώς και κάθε αντικειμένου που ενσωματώνει ηλεκτρονικά μέσα, λογισμικό, αισθητήρες και συνδεσιμότητα σε δίκτυο ώστε να επιτρέπεται η σύνδεση και η ανταλλαγή δεδομένων. Απλούστερα, η φιλοσοφία

του IoT είναι η σύνδεση όλων των ηλεκτρονικών συσκευών μεταξύ τους (τοπικό δίκτυο) ή με δυνατότητα σύνδεσης στο διαδίκτυο (παγκόσμιο ιστό).

Παρόλα αυτά, υπάρχουν ανησυχίες για τους κινδύνους που σχετίζονται με την ανάπτυξη των τεχνολογιών και προϊόντων του Διαδικτύου των Πραγμάτων, ιδίως στους τομείς της ιδιωτικότητας και της ασφάλειας. Ως αποτέλεσμα, έχουν γίνει βήματα από τη βιομηχανία και τους φορείς κυβέρνησης για την αντιμετώπιση αυτών των ανησυχιών, συμπεριλαμβανομένης της ανάπτυξης διεθνών και τοπικών προτύπων, κατευθυντηρίων γραμμών και κανονιστικών πλαισίων.

2.1 Εφαρμογές IoT

Τα δίκτυα επικοινωνιών IoT χρησιμοποιούνται σε ένα ευρύ φάσμα εφαρμογών που κατά βάση χωρίζεται σε καταναλωτικές, εμπορικές, βιομηχανικές και εφαρμογές υποδομών (infrastructure). Παρακάτω, αναλύονται συνοπτικά κάποια παραδείγματα ανά κατηγορία.

2.1.1 Καταναλωτές

Ένα μεγάλο ποσοστό του πληθυσμού γνωρίζει και συσχετίζει τον όρο «IoT» με την ευρύτερη έννοια του αυτοματισμού μιας κατοικίας ή αλλιώς την μετατροπή ενός απλού χώρου σε έξυπνο σπίτι (smart home) που μπορεί να περιλαμβάνει συσκευές φωτισμού, θέρμανσης, κλιματισμού, μέσων ενημέρωσης, συστημάτων ασφαλείας και καμερών.

Βασικό πεδίο εφαρμογής του έξυπνου σπιτιού αποτελεί η παροχή βοήθειας σε ηλικιωμένα άτομα και άτομα με αναπηρίες. Μια σημαντική λειτουργία είναι ο φωνητικός έλεγχος, ο οποίος μπορεί να βοηθήσει τους χρήστες με προβλήματα όρασης και κινητικότητας. Επιπλέον, μπορούν να εξοπλιστούν με αισθητήρες που παρακολουθούν επείγουσες ιατρικές καταστάσεις, όπως πτώσεις ή κρίσεις παρέχοντας μεγαλύτερη αυτονομία και καλύτερη ποιότητα ζωής.

2.1.2 Οργανισμοί

Με τον όρο «Enterprise IoT» αναφερόμαστε σε συσκευές που χρησιμοποιούνται από επιχειρήσεις και οργανισμούς. Οι εφαρμογές τους επεκτείνονται σε πολλούς τομείς, όπως η ιατρική και η υγειονομική περίθαλψη, που αναφέρεται στη συλλογή και ανάλυση δεδομένων για έρευνα και παρακολούθηση μέχρι και στα μέσα μεταφορών που

περιλαμβάνουν την επικοινωνία μεταξύ ανθρώπου και οχήματος, τον έξυπνο έλεγχο κυκλοφορίας εως και τα ηλεκτρονικά συστήματα είσπραξης διοδίων.

2.1.3 Βιομηχανίες

Οι βιομηχανικές συσκευές του Διαδικτύου των Πραγμάτων (IIoT) αποκτούν και αναλύουν δεδομένα από συνδεδεμένο εξοπλισμό, επιχειρησιακή τεχνολογία (Operational Technology), τοποθεσίες και άτομα. Σε συνδυασμό με συσκευές παρακολούθησης, το IIoT βοηθά στον έλεγχο και την παρακολούθηση βιομηχανικών συστημάτων. Επιπλέον, μπορεί να χρησιμοποιηθεί και για την αυτοματοποιημένη ενημέρωση των εγγραφών τοποθέτησης περιουσιακών στοιχείων σε βιομηχανικές μονάδες αποθήκευσης, καθώς τα περιουσιακά στοιχεία μπορεί να κυμαίνονται από μια μικρή βίδα έως έναν ολόκληρο ανταλλακτικό κινητήρα, και η λανθασμένη τοποθέτηση τέτοιων περιουσιακών στοιχείων μπορεί να προκαλέσει απώλεια αθρώπινου δυναμικού, χρόνο, και χρήματα.

2.1.4 Υποδομές

Η παρακολούθηση και ο έλεγχος λειτουργιών βιώσιμων αστικών και αγροτικών υποδομών, όπως γέφυρες, σιδηροδρομικές γραμμές και αιολικά πάρκα, αποτελεί σημαντική εφαρμογή του Διαδικτύου των Πραγμάτων (IoT). Η υποδομή του IoT μπορεί να χρησιμοποιηθεί για την παρακολούθηση οποιασδήποτε αλλαγής ή συμβάντος στις δομικές συνθήκες που μπορεί να θέσει σε κίνδυνο την ασφάλεια και αυξήσει τον κίνδυνο. Το IoT μπορεί να επιφέρει οικονομία σε κόστη, μείωση του χρόνου, βελτίωση της ποιότητας της εργασίας, ροή εργασίας χωρίς χρήση χαρτιού και αύξηση της παραγωγικότητας.

2.1.5 Στρατιωτικές Ενέργειες

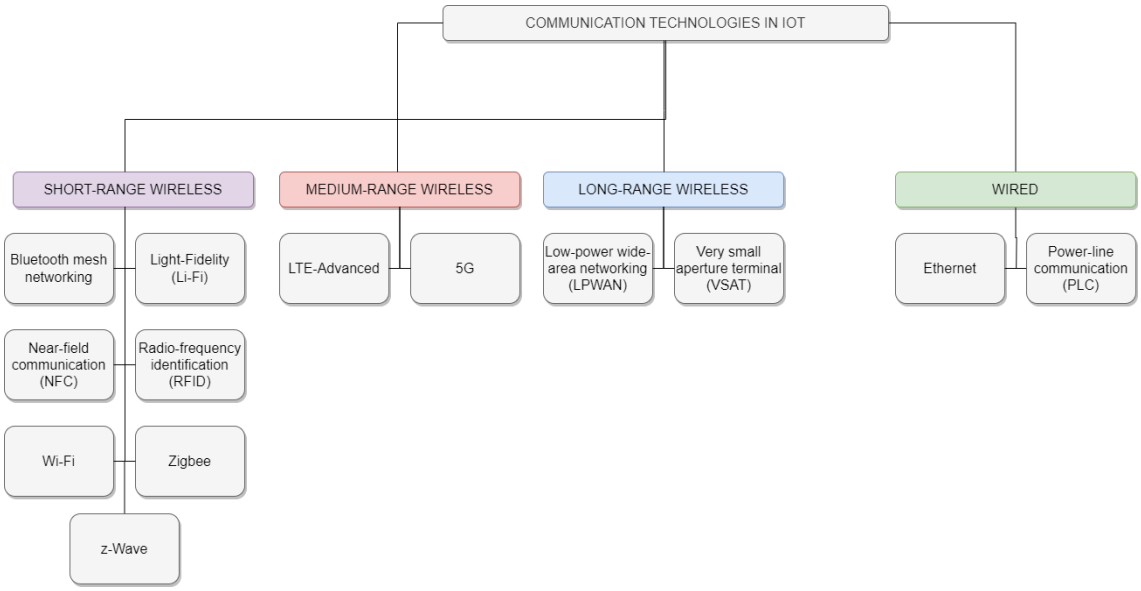
Το Διαδίκτυο των Στρατιωτικών Πραγμάτων (IoMT) αναφέρεται στη χρήση των τεχνολογιών του Διαδικτύου των Πραγμάτων στον στρατιωτικό τομέα για τους σκοπούς της αναγνώρισης, της παρακολούθησης και άλλων στρατιωτικών στόχων. Αυτό επηρεάζεται σημαντικά από τις μελλοντικές προοπτικές του πολέμου σε αστικό περιβάλλον και περιλαμβάνει τη χρήση αισθητήρων, πυρομαχικών, οχημάτων, ρομπότ, βιομετρικών δεδομένων που φορούν οι στρατιώτες και άλλων έξυπνων τεχνολογιών που είναι σημαντικές στο πεδίο της μάχης.

2.2 Είδη Δικτύων Επικοινωνιών IoT

Υπάρχουν ποικίλες τεχνολογίες που δίνουν την δυνατότητα στις συσκευές IoT να επικοινωνούν μεταξύ τους και να ανταλλάσσουν δεδομένα. Η χρήση κάποιας συγκεκριμένης τεχνολογίας εξαρτάται με τις απαιτήσεις των εφαρμογών τους, όπως η διάρκεια ζωής της μπαταρίας, η απόσταση κάλυψης, η ταχύτητα μετάδοσης δεδομένων και η εμβέλεια.

Τα δημοφιλέστερα είδη δικτύων επικοινωνιών IoT μπορούν να διακριθούν με βάση τις παρακάτω κατηγορίες:

2.2



Εικόνα 1 : Τα είδη δικτύων επικοινωνιών IoT ανά κατηγορία

2.2.1 Ασύρματα Δίκτυα Μικρής Εμβέλειας (Short-Range Wireless Networks)

Οι τεχνολογίες ασύρματης επικοινωνίας μικρού εύρους εχουν ποικίλες εφαρμογές στην καθημερινότητα μας όπως RFID, συστήματα πυρασφάλειας, συναγερμοί ασφαλείας, ραντάρ οχημάτων, ασύρματα μικρόφωνα και ακουστικά, σήματα κυκλοφορίας, ασύρματοι ελεγκτές πυλών γκαράζ, αναγνώστες barcode, ανιχνευτές κίνησης, και πολλά άλλα.

Παρακάτω, αναφέρονται συνοπτικά ορισμένα μικρού-εύρους δίκτυα επικοινωνιών μαζί με τις λειτουργίες τους.

- Zigbee : Τα Zigbee αποτελούν πρωτόκολλα επικοινωνίας για προσωπικά δίκτυα βασισμένα στο πρότυπο IEEE 802.15.4 και είναι μια ιδανική επιλογή καθώς παρέχουν χαμηλή κατανάλωση ενέργειας, χαμηλό ρυθμό μετάδοσης δεδομένων, χαμηλό κόστος και υψηλή ροή δεδομένων.

- Z-Wave : Το Z-Wave είναι ένα ασύρματο πρωτόκολλο επικοινωνίας κυρίως για εφαρμογές αυτοματισμού και ασφάλειας στο σπίτι.

- Αναγνώριση με ραδιοσυχνότητα (RFID) : Η συγκεκριμένη τεχνολογία χρησιμοποιεί ηλεκτρομαγνητικά πεδία για την ανάγνωση δεδομένων αποθηκευμένων σε ετικέτες που ενσωματώνονται σε άλλα αντικείμενα.

- Wi-Fi : Το Wi-Fi βασίζεται σε τεχνολογία για τοπικά δίκτυα μέσω του προτύπου IEEE 802.11, όπου οι συσκευές επικοινωνούν μέσω κοινού σημείου πρόσβασης ή απευθείας μεταξύ ατομικών συσκευών. Είναι μια από τις πιο γνωστές τεχνολογίες επικοινωνίας και χρησιμοποιείται σε μεγάλο ποσοστό από καθημερινούς χρήστες παγκοσμίως.

- Επικοινωνία Κοντινού Πεδίου (Near-field communication - NFC) : Τα πρωτόκολλα NFC είναι πρωτόκολλα επικοινωνίας που επιτρέπουν σε δύο ηλεκτρονικές συσκευές να επικοινωνούν σε απόσταση μέχρι 4 εκατοστά. Ένα παράδειγμα χρήσης NFC είναι σε κινητές συσκευές όπου μπορούμε να πραγματοποιήσουμε ανέπαφες πληρωμές ή ακόμη και να μεταφέρουμε δεδομένα.

- Light-Fidelity (Li-Fi) : Το Li-Fi αποτέλει ασύρματη τεχνολογία παρόμοια με το Wi-Fi η οποία χρησιμοποιεί το φως για την μετάδοση των δεδομένων μεταξύ συσκευών.

- Bluetooth Mesh Networking : Αναφέρεται σε μια προδιαγραφή που παρέχει μια εκδοχή δικτύου με σύνδεση για το Bluetooth low energy (BLE) με αυξημένο αριθμό κόμβων και τυποποιημένο επίπεδο εφαρμογής (μοντέλα).

2.2.2 Ασύρματα Δίκτυα Μεσαίας Εμβέλιας (Medium-Range Wireless Networks)

Οι τεχνολογίες ασύρματης επικοινωνίας μέσαιου εύρους αποτελούν τεχνολογίες που απευθύνονται κυρίως σε δίκτυα τηλεπικοινωνιών όπως 5G και LTE Advanced δίκτυα.

Παρακάτω, αναφέρονται συνοπτικά ορισμένα μεσαίου-εύρους δίκτυα επικοινωνιών μαζί με τις λειτουργίες τους.

- Δίκτυα 5G : Όπως και οι προκάτοχοί τους, τα δίκτυα 5G είναι κυψελωτά, με την περιοχή εξυπηρέτησης (service area) να διακρίνεται σε μικρά γεωγραφικά σημεία που ονομάζονται κύτταρα (cells). Όλες οι ασύρματες συσκευές 5G σε ένα κύτταρο συνδέονται στο Διαδίκτυο και το τηλεφωνικό δίκτυο μέσω ραδιοκυμάτων μέσω μιας βάσης και μιας κεραίας στο κύτταρο.

- LTE Advanced : Αποτελεί προδιαγραφή υψηλής ταχύτητας επικοινωνίας για κινητά δίκτυα προσφέροντας βελτιώσεις στο πρότυπο LTE με επέκταση κάλυψης, αυξημένη ροή δεδομένων και μειωμένη καθυστέρηση.

2.2.3 Ασύρματα Δίκτυα Μεγάλης Εμβέλιας (Long-Range Wireless Networks)

Οι τεχνολογίες ασύρματης επικοινωνίας μεγάλου εύρους έχουν ως βασικό γνώρισμα το μεγάλο εύρος τους, καθώς η γεωγραφική τους κάλυψη είναι πολύ μεγαλύτερη από τις προαναφερθέντες κατηγορίες ενώ παράλληλα διατηρούν χαμηλό ενεργειακό κόστος.

Παρακάτω, αναφέρονται συνοπτικά ορισμένα μεγάλου-εύρους δίκτυα επικοινωνιών μαζί με τις λειτουργίες τους.

- Low-power wide-area networking (LPWAN) : Τα LPWAN είναι ασύρματα δίκτυα σχεδιασμένα για επικοινωνία μεγάλης εμβέλειας σε χαμηλό ρυθμό μετάδοσης δεδομένων, με στόχο τη μείωση της κατανάλωσης ενέργειας και του κόστους για τη μετάδοση.

- Very Small Aperture Terminal (VSAT) : Το VSAT αναφέρεται σε τεχνολογία επικοινωνίας με δορυφόρο που χρησιμοποιεί μικρές κεραίες για τη μετάδοση δεδομένων σε στενή και ευρεία ζώνη.

2.2.4 Ενσύρματα Δίκτυα (Wired)

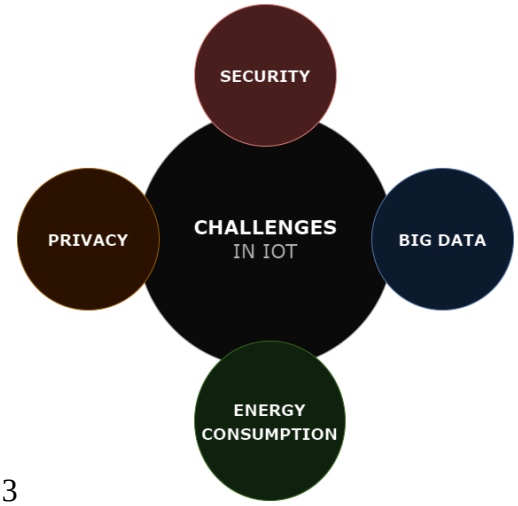
Στις τεχνολογίες ενσύρματης επικοινωνίας η σύνδεση μεταξύ των συσκευών επιτυγχάνεται μέσω φυσικών καλωδίων, εξασφαλίζοντας μια σταθερή και αξιόπιστη επικοινωνία. Αυτό το είδος δικτύου συχνά θεωρείται πιο ασφαλές και έχει ευρεία χρήση σε γραφεία, σπίτια και επιχειρηματικά περιβάλλοντα.

Παρακάτω, αναφέρονται συνοπτικά ορισμένα ενσύρματα δίκτυα επικοινωνιών μαζί με τις λειτουργίες τους.

- Ethernet : Το Ethernet αποτελεί ένα πρότυπο δικτύωσης γενικής χρήσης που χρησιμοποιεί συνδέσεις απλού ή διπλού ζεύγους καλωδίων και οπτικές ίνες σε συνδυασμό με κεντρικούς κόμβους ή διακόπτες. Σύνηθως χρησιμοποιείται σε οικίες και γράφεια ώστε να παρέχει ταχύτερη και αποδοτικότερη σύνδεση στο Διαδύκτιο σε συσκευές όπως υπολογιστές, λάπτοπ και διαφόρων άλλων συσκευών.

- Power-line communication (PLC) : Αποτελεί τεχνολογία επικοινωνίας που χρησιμοποιεί την ηλεκτρική καλωδίωση για τη μεταφορά τόσο ηλεκτρικής ενέργειας όσο και δεδομένων. Προδιαγραφές όπως το HomePlug ή το G.hn εκμεταλλεύονται το PLC για το δίκτυο συσκευών IoT.

2.3 Προβλήματα, κίνδυνοι και απειλές



2.3

Εικόνα 2 : 4 βασικές προκλήσεις σε δίκτυα IoT

Παρά τα οφέλη και την τεχνολογική εξέλιξη που επέφερε το Διαδίκτυο Των Πραγμάτων στον τρόπο που αλληλεπιδρούμε με το περιβάλλον και τις συσκευές μας, έχουμε έρθει αντιμέτωποι και με πολλές προκλήσεις όσο ανάφορα την ασφάλεια, την μεταφορά των δεδομένων μέχρι και την ενεργειακή κατανάλωση.

Στις παρακάτω παραγράφους, αναφέρονται κάποιες κατηγορίες πιθανών προβλημάτων που μπορεί να αναγνωριστούν σε περιβάλλοντα δίκτυων επικοινωνιών IoT.

2.3.1 Ασφάλεια (Security)

Το πρόβλημα της ασφάλειας αποτελεί έναν από τους κυριότερους παράγοντες προκλήσεων στον τομέα των δικτύων, με εμφανή επίδραση και στο πλαίσιο του Διαδικτύου των Πραγμάτων (IoT). Καθώς τα πακέτα δεδομένων περνούν μέσω διαφορετικών συνδέσμων και συσκευών προς τον τελικό προορισμό τους στο διαδίκτυο, απαιτούνται μέτρα για τη διατήρηση της εμπιστευτικότητας και της ακεραιότητας των δεδομένων. Παράλληλα, η χαμηλή κατανάλωση ισχύος στις περισσότερες συσκευές IoT αποτελεί εμπόδιο στην απευθείας εφαρμογή των υφισταμένων κρυπτογραφικών λύσεων.

Επιπλέον, κατά την ενσωμάτωση εφαρμογών στη δομή του δικτύου, δίνεται μεγαλύτερη έμφαση στη λειτουργικότητα και αμελείται η ασφαλεία κατά τον σχεδιασμό. Αυτό δημιουργεί κενά για πιθανές επιθέσεις και απόπειρες χακαρίσματος (hacking), απαιτώντας εξειδικευμένες ασφαλείς πρακτικές κατά την ανάπτυξη και υλοποίηση των λειτουργιών του δικτύου στο πλαίσιο του IoT.

2.3.2 Ιδιωτικότητα (Privacy)

Η ιδιωτικότητα στο Διαδίκτυο των Πραγμάτων (IoT) αποτελεί πρωτεύον πρόβλημα λόγω της εκτεταμένης και αλληλοσυνδεδεμένης φύσης των συσκευών IoT. Κεντρικό θέμα αποτελεί η προστασία των προσωπικών δεδομένων του ατόμου και το δικαίωμά του να ελέγχει τη συλλογή, χρήση και διαμοιρασμό αυτών των δεδομένων. Στο πλαίσιο του IoT, οι συσκευές συλλέγουν και μεταδίδουν συνεχώς ένα εκτεταμένο φάσμα δεδομένων, περιλαμβάνοντας τόσο τις καθημερινές μας ρουτίνες όσο και ευαίσθητες πληροφορίες υγείας ενός ατόμου. Η πρόκληση στο συγκεκριμένο ζήτημα είναι η δημιουργία ισχυρών μηχανισμών προστασίας της ιδιωτικότητας των χρηστών που θα αντιμετωπίζουν τον κίνδυνο, σε περίπτωση μη εξουσιοδοτημένης πρόσβασης και δυνητικής κατάχρησης αυτών των πληροφοριών.

2.3.3 Κατανάλωση Ενέργειας (Power Consumption)

Η ενέργεια είναι κρίσιμη για τις έξυπνες συσκευές IoT, καθώς πολλές λειτουργούν με μπαταρίες ή χρησιμοποιούν τεχνικές ενεργειακής συλλογής. Είναι σημαντικό να μην σπαταλάται ενέργεια με τη μετάδοση περιττών δεδομένων και πρωτοκόλλων. Ο σχεδιασμός μιας ενεργειακά αποδοτικής δικτυακής αρχιτεκτονικής και ενός έξυπνου μηχανισμού δρομολόγησης εξακολουθεί να είναι μεγάλη πρόκληση στα δίκτυα IoT.

2.3.4 Όγκος και Μεταφορά Δεδομένων (Big Data)

Ανά τα χρόνια, οι έξυπνες συσκευές εκμεταλλεύονται και διαχειρίζονται μαζικές ποσότητες δεδομένων (Big Data) που συλλέγονται από αυτές, αποτελώντας καίριο χαρακτηριστικό τους. Αυτό δημιουργεί την ανάγκη ανάπτυξης προηγμένων τεχνικών προκειμένου να διαμορφωθούν αυτά τα δεδομένα και να αποτελέσουν χρήσιμα.

Η αντιμετώπιση αυτών των προκλήσεων απαιτεί μια πολυτομεακή προσέγγιση που αφορά την ανάλυση των δεδομένων, τα πρωτόκολλα επικοινωνίας, τα μέτρα ασφαλείας, και την επεκτασιμότητα των υποδομών. Καθώς ο τομέας εξελίσσεται, η συνεχής έρευνα και καινοτομία είναι κρίσιμη για την αντιμετώπιση αυτών των προκλήσεων στο πλαίσιο του big data στο Διαδίκτυο των Πραγμάτων (IoT).

3 Είδη Επιθέσεων Σε Δίκτυα Επικοινωνιών

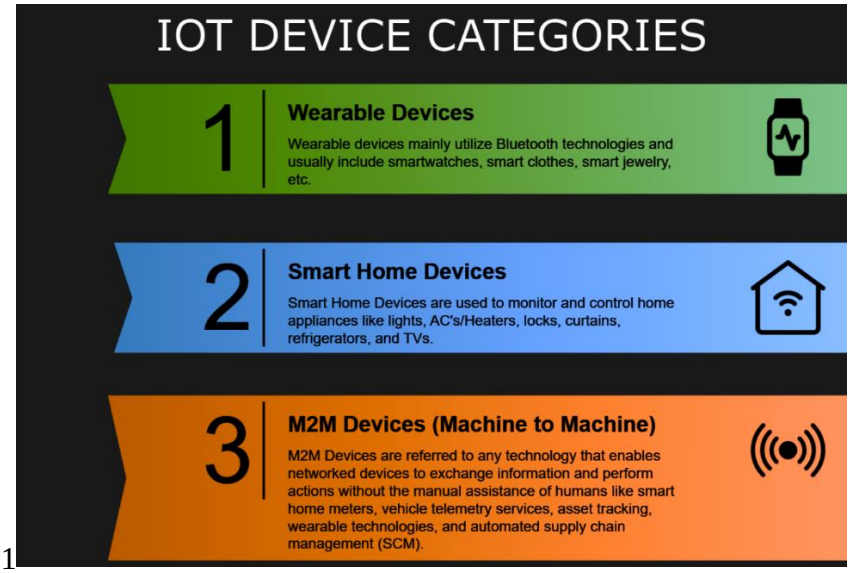
Σύμφωνα με τη ενημέρωση του Cyber Threat Report της SonicWall για το 2023, κατά τους πρώτους έξι μήνες του έτους, παρατηρήθηκε αύξηση κατά 37% στον παγκόσμιο όγκο κακόβουλου λογισμικού σε συσκευές του Internet of Things (IoT), καταλήγοντας σε συνολικό αριθμό 77,9 εκατομμυρίων επιθέσεων, σε σύγκριση με τις 57 εκατομμύρια επιθέσεις κατά τους πρώτους έξι μήνες του 2022. Γνωρίζοντας αυτήν την πληροφορία, μπορούμε να αναλογιστούμε ότι, παρόλο που το Διαδίκτυο Των Πραγμάτων αποτελεί μια τεχνολογία αιχμής, δεν παύει να κρύβει και αρκετούς κινδύνους.

Στο συγκεκριμένο κεφάλαιο, επεξηγούνται τα είδη των IoT συσκευών και περιγράφονται ορισμένες μέθοδοι επιθέσεων καθώς και τρόποι αντιμετώπισης και πρόληψης τους.

3.1 Συσκευές σε ένα IoT περιβάλλον

Προτού γίνει η εισαγωγή στα είδη επιθέσεων, πρέπει πρώτα να υπάρχει μια βασική κατανόηση των συσκευών σε ένα περιβάλλον IoT.

3.1



Εικόνα 3 : Κατηγορίες συσκευών IoT

Οι συσκευές του Διαδικτύου των Πραγμάτων (IoT) μπορούν να κατηγοριοποιηθούν στις ακόλουθες τρεις κατηγορίες, ανάλογα με τον τύπο τους και την χρησιμότητα τους :

3.1.1 Φορητές Συσκευές (Wearable Devices)

Οι φορητές συσκευές μπορούν να κατηγοριοποιηθούν βάσει τριών κυρίων λειτουργιών: ηλεκτρονική υγεία (e-health), επικοινωνία, και κινητή πληρωμή. Οι συσκευές ηλεκτρονικής υγείας επικεντρώνονται στον παρακολούθηση των κινήσεων ή ενεργειών των χρηστών, συνδέονται συνήθως με ένα smartphone μέσω τεχνολογίας Bluetooth, παρέχοντας στοιχεία που αφορούν την υγεία του χρήστη. Οι χρήσεις τους αφορούν κυρίως τον τομέα της ιατρικής, συμβάλλοντας στην παρακολούθηση της ψυχοσωματικής υγείας του ασθενούς. Εκτός του ρόλου τους στην επικοινωνία, παρέχουν δυνατότητες πληρωμής, εξαλείφοντας την ανάγκη κινητής συσκευής ή τραπεζικών καρτών. Παραδείγματα τέτοιων φορητών συσκευών περιλαμβάνουν έξυπνα ρολόγια, έξυπνα ρούχα, έξυπνα κοσμήματα, κ.α.

3.1.2 Συσκευές έξυπνου σπιτιού (Smart Home Devices)

Οι έξυπνες συσκευές στο σπίτι επιτρέπουν στους χρήστες να διαχειρίζονται τον χώρο τους από οποιοδήποτε μέρος μέσω μιας εφαρμογής ή φωνητικών εντολών. Αυτές οι συσκευές περιλαμβάνουν, μεταξύ άλλων, τα φώτα, τα κλιματιστικά/θερμαντήρες, τις κλειδαριές, τις κουρτίνες, τα ψυγεία και τις τηλεοράσεις. Για τον έλεγχο τους, αυτές οι συσκευές συνδέονται στο διαδίκτυο του σπιτιού, προσφέροντας πρόσβαση στον χρήστη, είτε εντός του χώρου του είτε εκτός μέσω απομακρυσμένης διαχείρισης.

3.1.3 Μηχανή προς Μηχανή (Machine to Machine – M2M Devices)

Οι συσκευές M2M (Machine-to-Machine) είναι ικανές να επικοινωνούν και να εκτελούν λειτουργίες χωρίς την ανάγκη ανθρώπινης παρέμβασης. Αυτές οι μηχανές μπορούν να λαμβάνουν και να εκτελούν εργασίες μέσω του Διαδικτύου, εξαλείφοντας την ανάγκη συνεχούς ανθρώπινης επιτήρησης. Σημαντικοί τομείς εφαρμογής περιλαμβάνουν την τηλεϊατρική, τη ρομποτική, τον έλεγχο της κυκλοφορίας, την αυτοκινητοβιομηχανία και τον έλεγχο στόλων.

Η αρχιτεκτονική των συσκευών M2M χωρίζεται σε 3 domains : M2M, δικτύου και εφαρμογής. Κάθε domain εξυπηρετεί συγκεκριμένες λειτουργίες στο πλαίσιο αυτού του συστήματος.

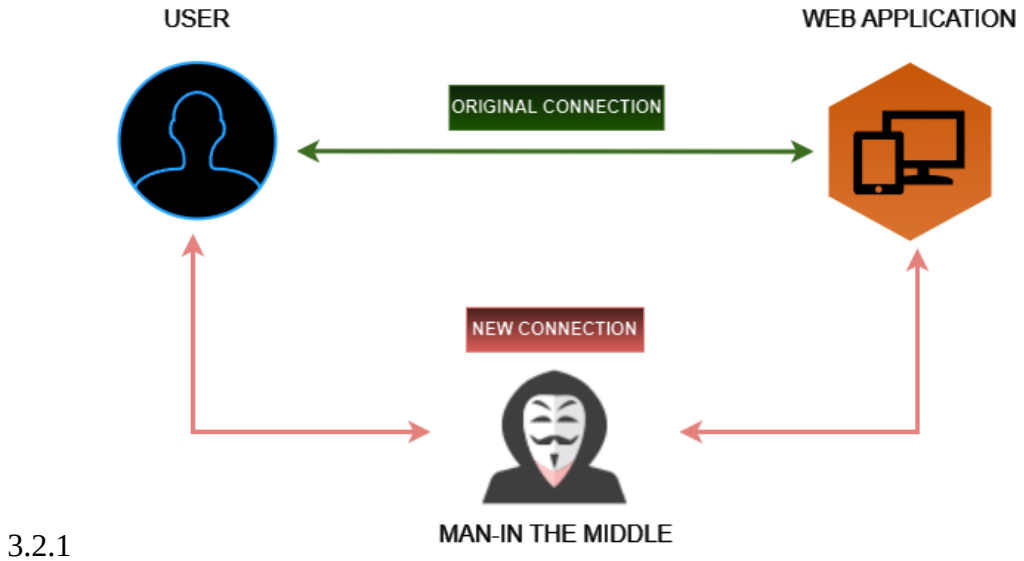
- M2M Domain (Machine to Machine) : Αυτό το domain περιλαμβάνει μια ποικιλία συσκευών που χρησιμοποιούνται κατά την δημιουργία επικοινωνιών M2M. Ανάμεσα σε αυτές τις συσκευές, ορισμένες είναι εξοπλισμένες με αισθητήρες για τον εντοπισμό αλλαγών, ενώ άλλες διαθέτουν δυνατότητες αποθήκευσης. Οι πληροφορίες που συλλέγονται προωθούνται σε απομακρυσμένους διακομιστές για περαιτέρω ανάλυση.
- Network Domain (Δίκτυο) : Το Network Domain περιλαμβάνει μια ποικιλία δικτυακών συσκευών που χρησιμοποιούνται για την πρόσβαση στο Διαδίκτυο και τη διευκόλυνση της επικοινωνίας. Οι συσκευές που αναπτύσσονται σε αυτό απαιτούν ελάχιστους χρόνους απόκρισης, καθώς τα domains M2M και εφαρμογής εξαρτώνται από την συνεχή τους επικοινωνία. Οι διάφορες τεχνολογίες πρόσβασης που χρησιμοποιούνται περιλαμβάνουν, μεταξύ άλλων το Ethernet, xDSL, WiMax, 3G και LTE.
- Application Domain (Εφαρμογή) : Το συγκεκριμένο domain περιλαμβάνει απομακρυσμένους διακομιστές στους οποίους γίνεται η μεταφορά και αποθήκευση των πληροφοριών. Οι πληροφορίες, στη συνέχεια, διατίθενται σε εξουσιοδοτημένους χρήστες μέσω μιας εφαρμογής. Οι εν λόγω εφαρμογές επιτρέπουν την απομακρυσμένη ανάλυση δεδομένων, τον απομακρυσμένο έλεγχο και την απομακρυσμένη ανίχνευση.

3.2 Συχνές περιπτώσεις επιθέσεων

Η αντίληψη της φύσης των επιθέσεων σε περιβάλλοντα IoT είναι κρίσιμη για την πλοήγηση στο σύνθετο και δυναμικό τοπίο της κυβερνοασφάλειας, όπου η συνεχής επαγρύπνηση και η σωστή επεξήγηση και κατανόηση των απειλών αποτελούν απαραίτητα για την προστασία από πιθανές παραβιάσεις.

Παρακάτω, αναφέρονται και αναλύονται ορισμένα δημοφιλή είδη επιθέσεων που μπορεί να παρατηρηθούν σε Δίκτυα Επικοινωνιών IoT.

3.2.1 Man in the middle attack



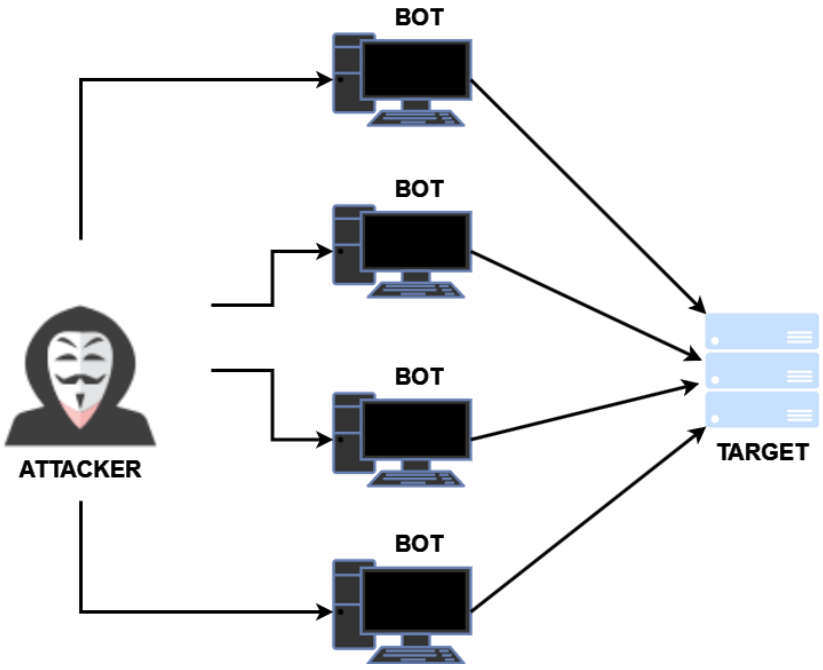
3.2.1

Εικόνα 4 : Διάγραμμα αναπαράστασης επίθεσης man-in-the-middle

Η επιτεύξη μιας επίθεσης "man-in-the-middle" προϋποθέτει την κρυφή τοποθέτηση του επιτιθέμενου μεταξύ του χρήστη και του Διαδικτύου. Κατά την απόκτηση πληροφορίας από το Διαδίκτυο, αυτή διαμορφώνεται μέσω πολλαπλών δρομολογητών προτού φτάσει στον προορισμό της. Με τον τρόπο αυτό, οι επιτιθέμενοι, διακριτικά τοποθετημένοι, διαβάζουν τις πληροφορίες που διακινούνται και περνούν από αυτούς, εφόσον αυτές δεν υπόκεινται σε διαδικασίες κρυπτογράφησης.

Ωστόσο, στην περίπτωση κρυπτογραφημένων δεδομένων και κατά την απόκτηση του κλειδιού που χρησιμοποιείται για την κρυπτογράφηση, είναι δυνατή η τροποποίηση των πληροφοριών. Μια παραλλαγή αυτής της επίθεσης περιλαμβάνει την αποθήκευση των πληροφοριών που ανακαλύφθηκαν για το θύμα, χωρίς να προβεί σε τροποποίηση των δεδομένων. Αυτού του είδους επιθέσεις χαρακτηρίζονται ως δύσκολες στον εντοπισμό τους, καθώς δεν υπάρχει διαθέσιμο μέσο για τον χρήστη προκειμένου να επαληθεύσει την ακεραιότητα των παρεχόμενων πληροφοριών.

3.2.2 Denial-of-Service (DoS) και Distributed-Denial-of-Service (DDoS)



3.2.2

Εικόνα 5 : Διάγραμμα αναπαράστασης επίθεσης DDoS

Η επίθεση που χαρακτηρίζεται ως Denial-of-Service (DoS) ή Distributed-Denial-of-Service (DDoS) χρησιμοποιείται με σκοπό τον προσωρινό ή μόνιμο αποκλεισμό ενός συστήματος ή ενός δικτύου, περιορίζοντας ή αποκλείοντας την πρόσβαση για κάθε χρήστη.

Η περίπτωση της επίθεσης DDoS πρόκειται για μια παραλλαγή της επίθεσης DoS, όπου πολλαπλές συσκευές χρησιμοποιούνται για την συντονισμένη εκτέλεση της επίθεσης. Αυτές οι επιθέσεις υλοποιούνται μέσω της υπερχείλισης του στόχου με εκτεταμένα αιτήματα πρόσβασης, με στόχο την πρόκληση αδυναμίας στις υποδομές του. Ειδικότερα, οι επιθέσεις DoS και DDoS εκμεταλλεύονται μια ευπαθή συνθήκη που εντοπίζεται στο Πρωτόκολλο Ελέγχου Μετάδοσης (TCP).

Οι επιθέσεις DDoS (Distributed Denial of Service) μπορούν να χωριστούν σε τρεις βασικές κατηγορίες βάσει των χαρακτηριστικών τους και των τεχνικών που χρησιμοποιούν.

- Application Layer Attacks : Οι επιθέσεις αυτές επικεντρώνονται στο να διεισδύσουν στο επίπεδο 7 του μοντέλου OSI, όπου δημιουργούνται οι

ιστοσελίδες ως απόκριση στο αίτημα που προέρχεται από τον τελικό χρήστη. Για τον πελάτη, η παραγωγή ενός αιτήματος δεν επιφέρει σημαντικό φορτίο, και είναι δυνατόν να παράγει εύκολα πολλαπλά αιτήματα προς τον διακομιστή. Αντίθετα, η ανταπόκριση σε ένα αίτημα επιφέρει σημαντικό φορτίο για τον διακομιστή, καθώς πρέπει να δημιουργήσει όλες τις σελίδες, να υπολογίσει οποιεσδήποτε ερωτήσεις και να φορτώσει τα αποτελέσματα από τη βάση δεδομένων σύμφωνα με το αίτημα. Παραδείγματα περιλαμβάνουν την επίθεση HTTP Flood και την επίθεση σε υπηρεσίες DNS.

- Protocol Attacks : Αυτές οι επιθέσεις επικεντρώνονται σε ευπάθειες στο επίπεδο 3 και επίπεδο 4 του μοντέλου OSI. Είναι χαρακτηριστικό τους να εξαντλούν πόρους όπως διακομιστές, τοίχοι προστασίας (firewalls) και εξισορροπιστές φορτίου (load balancers). Παραδείγματα περιλαμβάνουν την επίθεση SYN Flood και την επίθεση Ping of Death.

- Volumetric Attacks : Οι volumetric επιθέσεις επικεντρώνονται με στόχο να καταναλώσουν το εύρος ζώνης του δικτύου με σκοπό να περιορίσουν τη διαθεσιμότητά του στους χρήστες. Είναι εύκολο να παραχθούν, απλώς καθοδηγώντας μια μαζική ροή κυκλοφορίας προς τον στόχο/διακομιστή. Παραδείγματα περιλαμβάνουν την Ενίσχυση NTP, την Ενίσχυση DNS, την επίθεση UDP Flood και την επίθεση TCP Flood.

3.2.3 Password Cracking

Οι κωδικοί πρόσβασης αποτελούν κρίσιμα εργαλεία για τη διασφάλιση της προστασίας προσωπικών πληροφοριών. Επιθέσεις προς την ασφάλεια των κωδικών πρόσβασης πραγματοποιούνται με διάφορες μεθόδους, όπως η μαντεψιά, η επαναφορά και η καταγραφή. Η μαντεψιά αναφέρεται σε σενάριο όπου ο θύτης εισάγει συνήθως χρησιμοποιούμενους συνδυασμούς μέχρι να εντοπίσει τον σωστό κωδικό. Γνωστότερες τεχνικές password guessing αποτελούν τα dictionary attacks, credential stuffing, brute-force attacks και password spraying.

Στο παρακάτω κείμενο, αναφέρονται οι πιο γνωστές τεχνικές password cracking πιο αναλυτικά :

- Brute-Force Attacks : Στις επιθέσεις brute-force, εφαρμόζονται όλοι οι δυνατοί συνδυασμοί κωδικών πρόσβασης με σκοπό την αποκρυπτογράφηση του κωδικού. Αυτή η μέθοδος επιχειρεί συνήθως να ξεπεράσει την κρυπτογράφηση κωδικών πρόσβασης, όπου οι κωδικοί αποθηκεύονται ως κρυπτογραφημένο κείμενο. Σε παλαιότερα συστήματα Linux, χρησιμοποιούνταν σχήματα hashing MD5 για την αποθήκευση των κωδικών.

  Στο λειτουργικό σύστημα υπάρχει ένα αρχείο κωδικών πρόσβασης που περιλαμβάνει τους κωδικούς των χρηστών μαζί με τα ονόματα τους. Εάν αυτό το αρχείο κλαπεί, μπορεί να αποκτηθεί πρόσβαση στους κωδικούς. Ο πραγματικός κωδικός πρόσβασης δεν είναι παρών στο αρχείο, αλλά αντιπροσωπεύεται από ένα hash MD5. Αν και το κρυπτογραφημένο αυτό hash φαίνεται ασφαλές, είναι ευάλωτο σε επίθεση brute-force.

  Ο επιτιθέμενος μετατρέπει αρχικά όλους τους συνδυασμούς κωδικών πρόσβασης σε hashes MD5. Για να αποκρυπτογραφήσει τον κωδικό πρόσβασης, εξάγει αρχικά το hash του υποπτευόμενου κωδικού από το αρχείο κωδικών που βρίσκεται στο σύστημα. Στη συνέχεια, το hash αυτό συγκρίνεται με όλα τα hashes ένα προς ένα. Όταν βρεθεί κάποια αντιστοιχία, επιλέγεται ο αντίστοιχος κωδικός πρόσβασης.

- Dictionary Attacks : Η επίθεση με λεξικό είναι ταχύτητερη σε σύγκριση με τις επιθέσεις Brute-Force. Σε αντίθεση με την προσέγγιση της επίθεσης brute-force που εξετάζει όλους τους πιθανούς συνδυασμούς, η επίθεση με λεξικό επιχειρεί να εντοπίσει τον κωδικό πρόσβασης αντιστοιχίζοντάς τον με συχνά εμφανιζόμενες λέξεις ή λέξεις που χρησιμοποιούνται συχνά στη καθημερινότητα μας. Οι χρήστες τείνουν να χρησιμοποιούν κωδικούς που σχετίζονται με τα ονόματα κατοικιδιών, τόπων γεννήσεως, ονόματα διάσημων ηθοποιών κ.λπ.

  Κατά τη διεξαγωγή της επίθεσης, ο επιτιθέμενος δημιουργεί ένα "λεξικό" που περιλαμβάνει συνήθεις λέξεις που θα μπορούσαν να χρησιμοποιηθούν ως κωδικοί πρόσβασης, και στη συνέχεια εφαρμόζει αυτές τις λέξεις για την αποκρυπτογράφηση του κωδικού πρόσβασης.

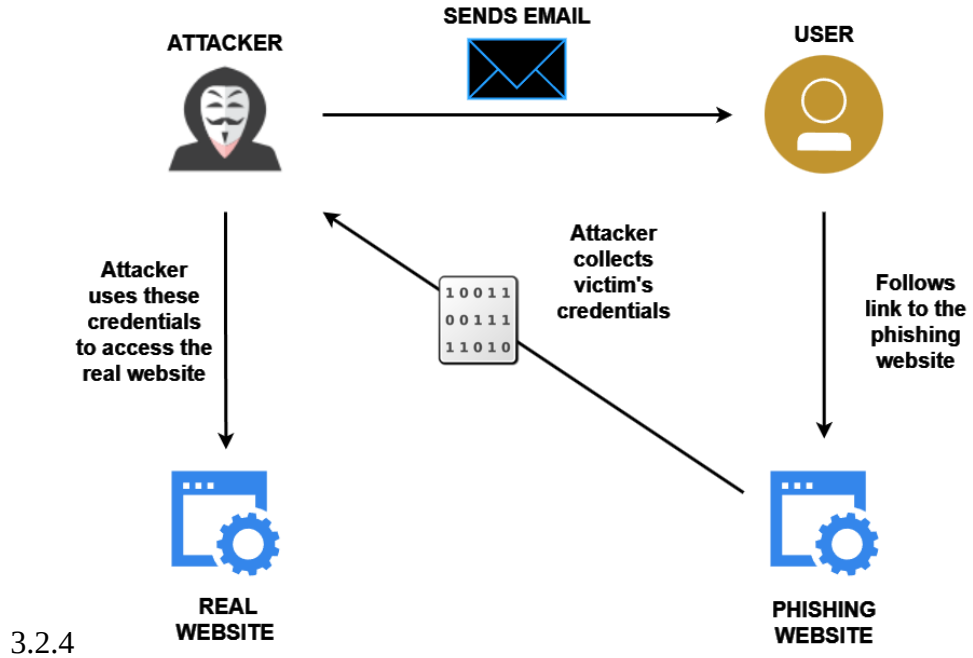
- Password Spraying : Οι επιτιθέμενοι μπορεί να χρησιμοποιούν μια ενιαία ή μια μικρή λίστα από κοινά χρησιμοποιούμενους κωδικούς πρόσβασης κατά την προσπάθειά τους να αποκτήσουν έγκυρα διαπιστευτήρια λογαριασμού. Η τεχνική του "password spraying" χρησιμοποιεί έναν κωδικό πρόσβασης (π.χ. 'Password01') ή μια μικρή λίστα από κοινά χρησιμοποιούμενους κωδικούς πρόσβασης που πιθανώς να συμμορφώνονται με τις πολιτικές πολυπλοκότητας του domain. Κατόπιν, πραγματοποιούνται προσπάθειες σύνδεσης με αυτόν τον κωδικό πρόσβασης έναντι πολλών διαφορετικών λογαριασμών σε ένα δίκτυο, προκειμένου να αποφευχθούν τα κλειδώματα λογαριασμών που θα συνέβαιναν κανονικά κατά τη διάρκεια μιας επίθεσης brute-force σε έναν μεγάλο αριθμό κωδικών πρόσβασης για έναν μοναδικό λογαριασμό.

- Credential Stuffing : Κατά καιρούς, παρατηρείται η δημοσίευση μεγάλου αριθμού ζευγών ονομάτων χρήστη και κωδικού πρόσβασης (username και passwords) στο διαδίκτυο, όταν ένας ιστότοπος ή μια υπηρεσία παραβιάζεται. Αυτή η πληροφορία μπορεί να αξιοποιηθεί από έναν επιτιθέμενο που επιχειρεί να παραβιάσει λογαριασμούς, εκμεταλλευόμενος την τάση των χρηστών να χρησιμοποιούν τους ίδιους κωδικούς πρόσβασης σε προσωπικούς και επαγγελματικούς λογαριασμούς. Η επαναχρησιμοποίηση κωδικών πρόσβασης αποτελεί πρόβλημα, καθώς η απόκτηση του κωδικού επιτρέπει την πρόσβαση σε πολλαπλούς λογαριασμούς.

  Τέλος, υπάρχει και η περίπτωση χρήσης κακόβουλου λογισμικού για τον παρακολούθηση των πλήκτρων που χρησιμοποιούνται κατά την καταχώρηση του κωδικού πρόσβασης (keylogger attack).

- Keylogger Attack : Τα keyloggers είναι λογισμικά προγράμματα που καταγράφουν τη δραστηριότητα του χρήστη καταγράφοντας κάθε πλήκτρο που πατά. Ο επιτιθέμενος εγκαθιστά το λογισμικό keylogger στο σύστημα του χρήστη, είτε ο ίδιος, είτε μέσω απάτης που παρακινεί τον χρήστη να το εγκαταστήσει. Το keylogger καταγράφει τα πλήκτρα που πατά ο χρήστης και στη συνέχεια στέλνει το αρχείο καταγραφής στη διεύθυνση email του επιτιθέμενου. Με αυτόν τον τρόπο, ο επιτιθέμενος αποκτά τον κωδικό, κερδίζοντας πρόσβαση στον επιθυμητό στόχο.

3.2.4 Phishing attack



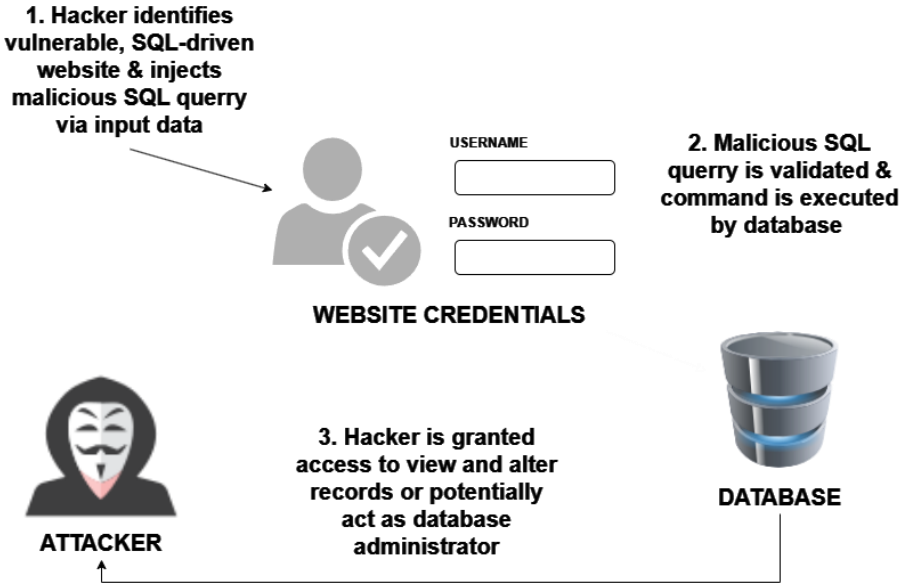
3.2.4

Εικόνα 6 : Διάγραμμα αναπαράστασης επίθεσης Phishing

Η διαδικασία του phishing χρησιμοποιείται με σκοπό να παραπλανήσει τους χρήστες, προκειμένου να καταχωρήσουν τα προσωπικά τους στοιχεία ή να λάβουν κακόβουλο λογισμικό με ικανότητα διάδοσης malware. Οι πιο διαδεδομένες μορφές επιθέσεων phishing περιλαμβάνουν ηλεκτρονικά μηνύματα που περιέχουν συνδέσμους προς πλαστές ιστοσελίδες και/ή κακόβουλα συνημμένα αρχεία. Για την υλοποίηση της επίθεσης, ο επιτιθέμενος δημιουργεί ένα παραπλανητικό ηλεκτρονικό μήνυμα με ρεαλιστική εμφάνιση και το αποστέλλει σε έναν επιλεγμένο χρήστη. Ένα παράδειγμα θα μπορούσε να είναι ένα ηλεκτρονικό μήνυμα με θέμα "Συγχαρητήρια, κερδίσατε μια κλήρωση" και στο περιεχόμενο του, ο χρήστης καλείται να καταχωρίσει προσωπικά του στοιχεία για να λάβει το υποτιθέμενο "δώρο".

Αντίθετα, ο χρήστης δεν είναι ενήμερος ότι οι σύνδεσμοι στο ηλεκτρονικό μήνυμα οδηγούν σε μια παραπλανητική ιστοσελίδα που συλλέγει τις πληροφορίες αυτές και τις χρησιμοποιεί με κακόβουλους σκοπούς. Μια παρόμοια μέθοδος ενσωματώνει κακόβουλο λογισμικό σε συνημμένα αρχεία ηλεκτρονικού ταχυδρομείου.

3.2.5 SQL injection



3.2.5

Εικόνα 7 : Διάγραμμα αναπαράστασης επίθεσης SQL Injection

Η χρήση SQL injection αποσκοπεί στην απόκτηση διαχειριστικής πρόσβασης σε βάσεις δεδομένων, εκμεταλλεύοντας τυχόν ευπάθειες στο δίκτυο του θύματος. Για την υλοποίηση μιας επίθεσης SQL injection, εισάγονται πλαστές εντολές SQL σε ιστοσελίδες, προκαλώντας την εκτέλεση τους, με σκοπό την ανάκτηση προσωπικών πληροφοριών. Σε περίπτωση που η βάση δεδομένων ή η ιστοσελίδα δεν είναι πλήρως ασφαλισμένη, αυτές οι πλαστές εντολές εκτελούνται χωρίς αντίρρηση, παρέχοντας πρόσβαση στις προσωπικές πληροφορίες που αναζητά.

3.3 Τρόποι αποφυγής και βελτίωσης της ασφάλειας

Γνωρίζοντας τους πολλαπλούς κινδύνους που ανέρχονται στα δίκτυα IoT, είναι σημαντικό να έχουμε προετοιμασμένες κάποιες μεθόδους βελτίωσης της ασφάλειας, ώστε να αποφευχθεί ή τουλάχιστον να μειωθεί η πιθανότητα κάποιας πιθανής μελλοντικής επίθεσης. Παρακάτω αναλύονται κάποια μέτρα που μπορούν να παρθούν ώστε να μπορούν επιχειρήσεις, δημόσιες υποδομές και προσωπικοί χώροι που φιλοξενούν έξυπνα συστήματα να ελέγχουν και να προστατεύουν τα δεδομένα που κυκλοφορούν στο δίκτυο τους.

3.3.1 Ενημερώσεις λογισμικού (Software/Firmware Updates)

Η ενημέρωση του λογισμικού αποτελεί καθοριστικό παράγοντα για την πρόληψη κυβερνοεπιθέσεων στο πλαίσιο του Internet of Things (IoT), καθώς παλαιότερες εκδόσεις συχνά εκτίθενται σε ευπάθειες και ασφαλειακά κενά που μπορούν να αξιοποιηθούν από κακόβουλους χρήστες. Σε επιστημονικό επίπεδο, η συνεχής αναβάθμιση του λογισμικού αποτελεί ένα κρίσιμο μέτρο ασφαλείας, καθώς οι κατασκευαστές αντιλαμβάνονται και αντιμετωπίζουν τις αδυναμίες και τις ευπάθειες που μπορούν να εμφανιστούν μέσω της διαρκούς έρευνας και ανάπτυξης. Η λήψη και εγκατάσταση των τακτικών ενημερώσεων αποτελεί ένα σημαντικό μέσο αντιμετώπισης ευπαθειών, προστατεύοντας τη συνολική ακεραιότητα και ασφάλεια ενός συστήματος IoT.

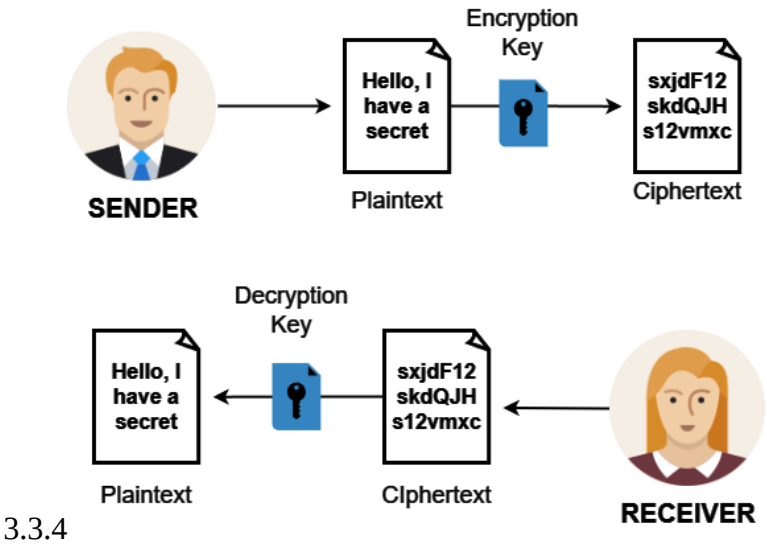
3.3.2 Δημιουργία αντιγράφου ασφαλείας (Data Backup)

Στην περίπτωση αδυναμίας πρόληψης ενός κινδύνου, ακόμη και μιας πιθανής υποκείμενης απώλειας, αλλοίωσης ή κλοπής των δεδομένων, η διασφάλιση της διαθεσιμότητας και ακεραιότητας των δεδομένων αποτελεί προτεραιότητα και απαιτεί την ύπαρξη συστημάτων αντιγράφων ασφαλείας. Η απώλεια δεδομένων, ειδικά σε ένα επιχειρηματικό περιβάλλον, μπορεί να επιφέρει σημαντικές επιπτώσεις, επομένως, η δημιουργία και συντήρηση αντιγράφων ασφαλείας αποτελεί κρίσιμο μέτρο για τη διασφάλιση της επιχειρησιακής συνέχειας και λειτουργίας καθώς και τη μείωση του κινδύνου αναπλήρωσης δεδομένων.

3.3.3 Διαχείριση κωδικών πρόσβασης

Στην σημερινή εποχή, ένα μεγάλο ποσοστό του πλυθησμού χρησιμοποιεί αδύναμους κωδικούς πρόσβασης. Κατά το έτος 2023, σύμφωνα με την πέμπτη ετήσια έρευνα του NordPass, ο κωδικός "123456" αναδείχθηκε ως ο πλέον διαδεδομένος κωδικός πρόσβασης των Αμερικανών πολιτών. Με βάση αυτόν τον γνώμονα, όπως αναφέρθηκε και στην προηγούμενη υποενότητα, υπάρχουν πολλές μέθοδοι επιθέσεων password cracking όπως τα Dictionary Attacks, που στοχεύουν στην εύρεση του κωδικού ενός χρήστη μέσω μιας καθημερινής λέξης, παραδείγματος χάρη την ημερομηνία γεννήσεως. Συνεπώς, η επιβολή αυστηρών πρακτικών για τη δημιουργία και διαχείριση ασφαλών κωδικών πρόσβασης αναδεικνύεται ως ουσιαστική πτυχή στην προστασία των συστημάτων IoT.

3.3.4 Encryption



3.3.4

Εικόνα 8 : Πως λειτουργεί η κρυπτογράφηση/αποκρυπτογράφηση

Η κρυπτογράφηση των δεδομένων σε συσκευές του Internet of Things (IoT) αντιπροσωπεύει μια καθοριστική πτυχή της ασφάλειας των πληροφοριών κατά την μεταφορά και την αποθήκευση τους. Η διαδικασία αυτή εμποδίζει αποτελεσματικά την ανεπιθύμητη πρόσβαση σε ευαίσθητα δεδομένα, καθιστώντας τα μη αποκρίσιμα σε επιθέσεις.

Οι αλγόριθμοι κρυπτογράφησης μπορούν να διαχωριστούν σε δύο βασικές κατηγορίες:

- Symmetric Cipher (Συμμετρική Κρυπτογράφηση) : Στη συμμετρική κρυπτογράφηση, χρησιμοποιείται το ίδιο κλειδί τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση. Ο αποστολέας και ο παραλήπτης πρέπει να μοιράζονται το μυστικό κλειδί εκ των προτέρων. Τα δεδομένα κρυπτογραφούνται με αυτό το κλειδί και μπορούν να αποκρυπτογραφηθούν μόνο με το ίδιο κλειδί. Η συμμετρική κρυπτογράφηση χρησιμοποιείται συχνά σε περιβάλλοντα όπου η διαχείριση και η ανταλλαγή πολλαπλών κλειδιών είναι ανέφικτη. Επίσης είναι ιδιαίτερα αποδοτική στην ασφάλεια μεγάλων όγκων δεδομένων.

- Asymmetric Cipher (Ασύμετρή Κρυπτογράφηση) : Στην ασύμμετρη κρυπτογράφηση, χρησιμοποιείται ένα ζεύγος κλειδιών, ένα δημόσιο κλειδί και

ένα ιδιωτικό κλειδί. Το δημόσιο κλειδί διανέμεται ανοιχτά, ενώ το ιδιωτικό κλειδί παραμένει εμπιστευτικό. Δεδομένα που έχουν κρυπτογραφηθεί με το δημόσιο κλειδί μπορούν να αποκρυπτογραφηθούν μόνο με το αντίστοιχο ιδιωτικό κλειδί και αντίστροφα.

Κάποιοι από τους πιο δημοφιλείς αλγορίθμους αποτελούν οι Advanced Encryption Standard (AES), Triple Data Encryption Standard (DES), Blowfish και Rivest-Shamir-Adleman (RSA). Με τη χρήση ισχυρών αλγορίθμων κρυπτογράφησης οι συσκευές IoT μπορούν να παρέχουν υψηλό επίπεδο ασφάλειας. Η κρυπτογράφηση διασφαλίζει την εμπιστευτικότητα των δεδομένων, ενώ παράλληλα διευκολύνει την ελεγχόμενη και ασφαλή ανταλλαγή πληροφοριών μεταξύ των συσκευών, συμβάλλοντας στη δημιουργία ενός ασφαλούς οικοσυστήματος IoT.

4 Λογισμικά Ανίχνευσης και Ανάλυσης Επιθέσεων

Στο κεφάλαιο αυτό, θα αναλυθούν κάποια προγράμματα ανίχνευσης και ανάλυσης επιθέσεων μαζί με κάποια παραδείγματα χρήσης για το κάθε ένα από αυτά, με screen-shots βήμα προς βήμα. Τα προγράμματα είναι δωρεάν και το κάθε ένα συμβάλλει σε διαφορετικές χρήσεις ανάλογα με την ανάγκη όπως για παράδειγμα την ανίχνευση της κίνησης ένος δικτύου, τη σάρωση κάποιων θυρών (ports) ή και το θέσιμο εξατομικευμένων κανόνων για ένα πιθανό scan.

4.1 Wireshark (Network Protocol Analyzer)

4.1

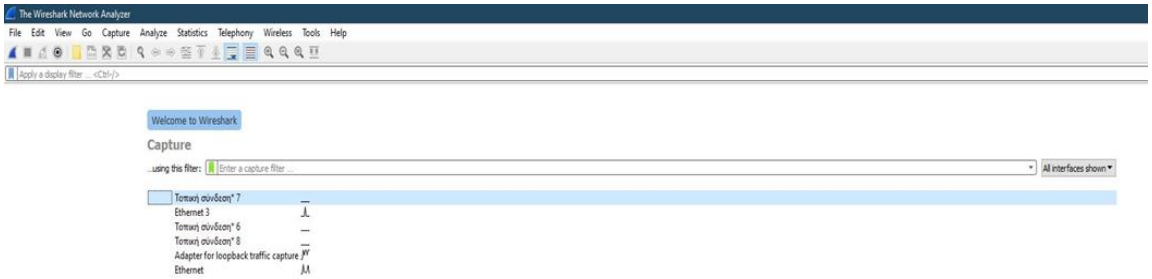
Εικόνα 9 : Το λογότυπο του προγράμματος Wireshark

Το Wireshark αποτελεί έναν αναλυτή πρωτοκόλλων δικτύου που επιτρέπει στους χρήστες να καταγράφουν και να αλληλεπιδρούν διαδραστικά με την κίνηση που εκτελείται σε ένα δικτυακό χώρο. Με μια πλούσια και ισχυρή συλλογή χαρακτηριστικών, αποτελεί το πιο δημοφιλές εργαλείο της κατηγορίας του. Λειτουργεί σε πολλές πλατφόρμες, συμπεριλαμβανομένων των Windows, macOS, Linux και UNIX. Επαγγελματίες δικτύου, ειδικοί ασφαλείας, προγραμματιστές και εκπαιδευτικοί σε όλο τον κόσμο χρησιμοποιούν ευρέως αυτό το πρόγραμμα. Λειτουργεί ως λογισμικό ανοιχτού κώδικα, προσφέροντας δωρεάν πρόσβαση, και δημοσιεύεται υπό την άδεια GNU General Public License έκδοση 2.

4.1.1 Πως λειτουργεί το Wireshark;

Αρχικά, μπορούμε να εγκαταστήσουμε την εφαρμογή δωρεάν από την επίσημη σελίδα του Wireshark. Αφού πραγματοποιήσουμε την εγκατάσταση, αντικρίζουμε την ακόλουθη οθόνη με όλα τα interfaces, δηλαδή όλες τις συνδέσεις που μπορούμε να παρακολουθήσουμε από τον υπολογιστή μας. Στην περίπτωση μας, θα επιλέξουμε την τοπική σύνδεση στην οποία είναι συνδεδεμένος ο υπολογιστής που πραγματοποιείται η ανίχνευση.

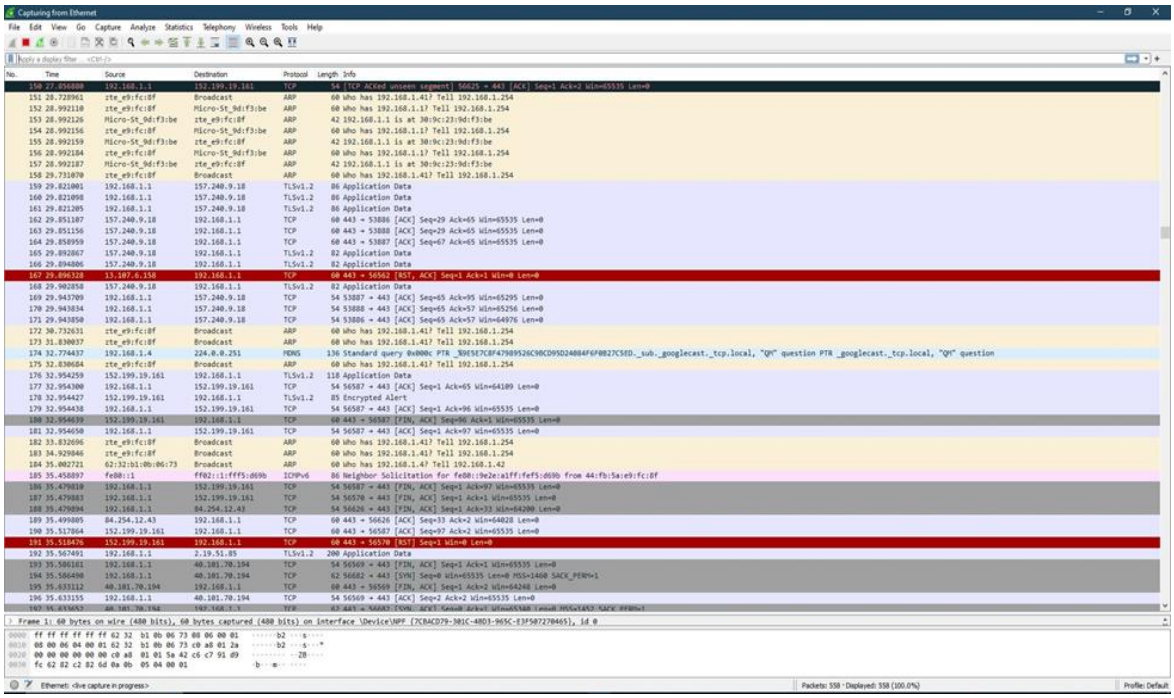
4.1



Εικόνα 10 : Λίστα με διαθέσιμες συνδέσεις

Έπειτα, αφού επιλέξουμε το interface που επιθυμούμε να παρακολουθήσουμε, κάνουμε κλικ το σύμβολο με το πτερύγιο ώστε να ξεκινήσει η αιχμαλώτιση (capture) της διαδικτυακής κίνησης της σύνδεσης.

4.1



Εικόνα 11 : Τα captures της σύνδεσης σε πραγματικό χρόνο

Με το που θέσουμε σε λειτουργία την διαδικασία αιχμαλώτισης, μπορούμε να δούμε σε πραγματικό χρόνο τα πακέτα που εντόπισε το Wireshark αναλυτικά. Προαιρετικά,

οποιαδήποτε στιγμή μπορούμε να τερματίσουμε την διαδικασία πατώντας το κόκκινο τετράγωνο που υποδηλώνει το Stop.

4.1.2 Ιδιότητες πακέτου

Όπως παρατηρούμε, ένα πακέτο αποτελείται από συγκεκριμένες ιδιότητες.

- Η αρίθμηση (no.) : Η σειρά αιχμαλώτισης των πακέτων.
- Η χρονική σήμανση (time) : Το χρονικό διάστημα από την αρχή της αιχμαλώτισης μέχρι την αιχμαλώτιση αυτού του πακέτου.
- Η πηγή (source) : Η IP διεύθυνση του συστήματος που απέστειλε το πακέτο.
- Ο προορισμός (destination) : Η IP διεύθυνση του συστήματος που έλαβε το πακέτο.
- Το πρωτόκολλο (protocol): Ο τύπος του κάθε πακέτου, όπως TCP, DNS, DHCPv6, ARP κ.λπ.
- Το μήκος (length) : Το μέγεθος του πακέτου σε bytes.
- Οι πληροφορίες (info) : Περισσότερες λεπτομέρειες για το περιεχόμενο του πακέτου.

4.1.3 Χρωματισμοί και ενδείξεις πακέτου

Εκτός από τις ιδιότητες ενός πακέτου μπορούμε να διακρίνουμε ότι φέρουν και κάποιους χρωματισμούς, ανάλογα με τον τύπο τους. Στην πρώτη εκκίνηση του προγράμματος, και χωρίς κάποια τροποποίηση, τα προεπιλεγμένα χρώματα (Color Coding) του Wireshark μαζί με το τι αντιπροσωπεύουν αναγράφονται στον παρακάτω πίνακα :

Πίνακας 1 : Προεπιλεγμένα χρώματα πακέτων του Wireshark.

Χρώματα	**Τύπος Πακέτου**
Ανοιχτό μωβ	TCP Πακέτο
Ανοιχτό μπλε	UDP Πακέτο

Μαύρο	Πακέτο με σφάλματα (Errors)
Ανοιχτό πράσινο	Κίνηση HTTP
Ανοιχτό κίτρινο	Κίνηση εστιασμένη σε Windows (Windows-specific), συμπεριλαμβανομένων του Server Message Blocks (SMB) και του Net-BIOS
Σκούρο κίτρινο	Δρομολόγηση (Routing)
Σκούρο γκρι	Κίνηση TCP SYN, FIN και ACK

4.1.4 Τα Capture και Display Filters

Η σημαντικότερη λειτουργία του Wireshark, η οποία αποτελεί και το πιο αξιοσημείωτο κομμάτι του προγράμματος, είναι τα φίλτρα. Τα φίλτρα όπως τα Capture και Display Filters εξυπηρετούν στο να προσαρμόσουμε τον έλεγχο των αιχμαλωτισμένων πακέτων όπως εμείς επιθυμούμε με σκοπό την καλύτερη και αποδοτικότερη επιδιόρθωση ενός πιθανού δικτυακού προβλήματος ή μιας αναγνώρισης επίθεσης δικτύου.

Τα Capture Filters δεν πρέπει να συγχέονται με τα Display Filters καθώς έχουν κάποιες αξιοσημείωτες διαφορές. Τα πρώτα επικεντρώνονται στον περιορισμό των πακέτων που καταγράφονται, προκειμένου να μειωθεί ο όγκος των δεδομένων και είναι πιο περιορισμένα στην χρήση τους. Αντίθετα, τα Display Filters εξυπηρετούν στην απόκρυψη ορισμένων πακέτων από την λίστα.

Τα Capture Filters ορίζονται πριν την έναρξη της αιχμαλώτισης και δεν επιτρέπεται η αλλαγή τους κατά τη διάρκεια της διαδικασίας. Αντίθετα, τα Display Filters δεν υφίστανται αυτόν τον περιορισμό και μπορούν να προσαρμοστούν κατά τη διάρκεια της ανάλυσης των δεδομένων.

Κάποια συχνά παραδείγματα εντολών των δύο φίλτρων είναι τα εξής :

Πίνακας 2 : Παραδείγματα εντολών φίλτρων.

Χρήση	**Σύνταξη (Syntax)**

Βάσει διεύθυνσης IP	ip.addr == 10.10.50.1
Βάσει διεύθυνσης προορισμού (Destination IP)	ip.dest == 10.10.50.1
Βάσει URL	http.host == “host name’
Βάσει εύρους διευθύνσεων IP	ip.addr >= 10.10.50.1 and ip.addr <= 10.10.50.1
Βάσει πόρτας (port)	tcp.port == 25
Βάσει υπο-δικτύου (subnet)	ip.addr == 10.10.50.1/24
Βάσει host	ip.host == hostname

4.1.5 Συμπεράσματα

Εν κατακλείδι, το Wireshark είναι ένα εξαιρετικό εργαλείο που χρησιμοποιείται από επαγγελματίες του κλάδου της πληροφορικής, είτε για να έχουν μια γενικότερη εικόνα της κίνησης του δικτύου τους, είτε ακόμη και για λόγους ασφαλείας καθώς αποτελεί μια καλή επιλογή βάσει των δυνατοτήτων που προσφέρει δεδομένου ότι διανέμεται δωρεάν.

4.2 Snort (Network Intrusion Prevention)

Εικόνα 12 : Το λογότυπο του προγράμματος Snort.

Το Snort είναι ένα open source σύστημα πρόληψης διείσδυσης (Intrusion Prevention System). Χρησιμοποιεί ένα σύνολο κανόνων που ανιχνεύουν κακόβουλες δραστηριότητες στο δίκτυο και εντοπίζει πακέτα που τα πληρούν, δημιουργώντας ειδοποιήσεις για τους χρήστες.

Μπορεί επίσης να εκτελείται σε λειτουργία inline για τον αποκλεισμό τέτοιων πακέτων. Οι τρεις βασικές χρήσεις του είναι: ως packet sniffer όπως το tcpdump, ως packet logger που είναι χρήσιμος για την αντιμετώπιση προβλημάτων στη δικτυακή κυκλοφορία, και ως ένα πλήρες σύστημα πρόληψης διείσδυσης στο δίκτυο. Το Snort

παρέχεται για προσωπική και επαγγελματική χρήση, με δυνατότητες ρύθμισης ανάλογα με τις ανάγκες του χρήστη.

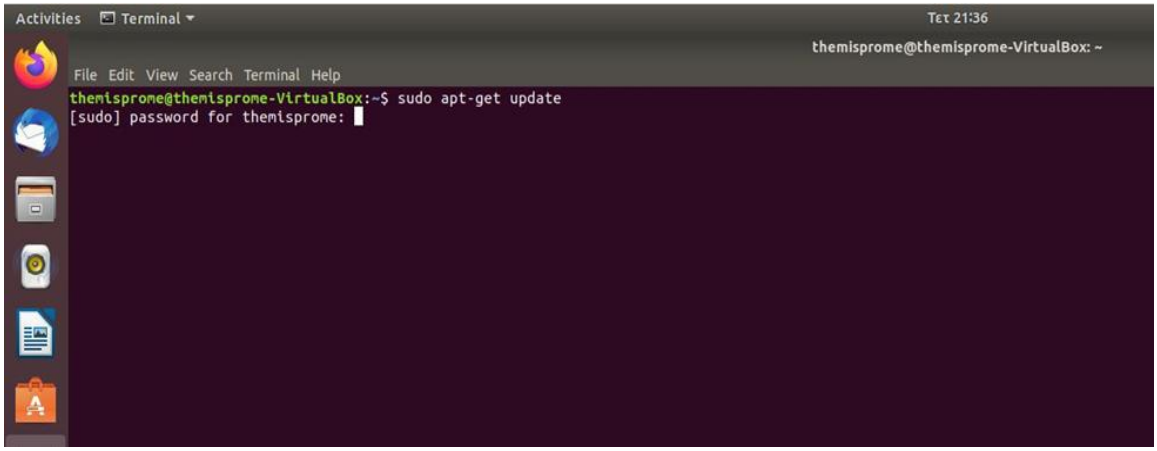
4.2.1 Πως λειτουργεί το Snort;

Ο βέλτιστος τρόπος για να χρησιμοποιήσουμε το Snort, είναι να το εγκαταστήσουμε σε λειτουργικό σύστημα Linux. Στην συγκεκριμένη περίπτωση χρησιμοποιήθηκαν τα Linux Ubuntu μέσω της εφαρμογής Virtual Box.

Σε αντίθεση με τις άλλες εφαρμογές που παρουσιάστηκαν, το Snort δεν διαθέτει κάποιο GUI (γραφικό περιβάλλον) οπότε θα χρησιμοποιήσουμε το Linux Terminal για να τρέξουμε τις εντολές του.

Για να εγκαταστήσουμε το Snort, πρέπει αρχικά να σιγουρευτούμε ότι το λειτουργικό μας σύστημα (repositories) είναι ενημερωμένο. Οπότε τρέχουμε την εντολή “sudo apt-get update”.

4.2

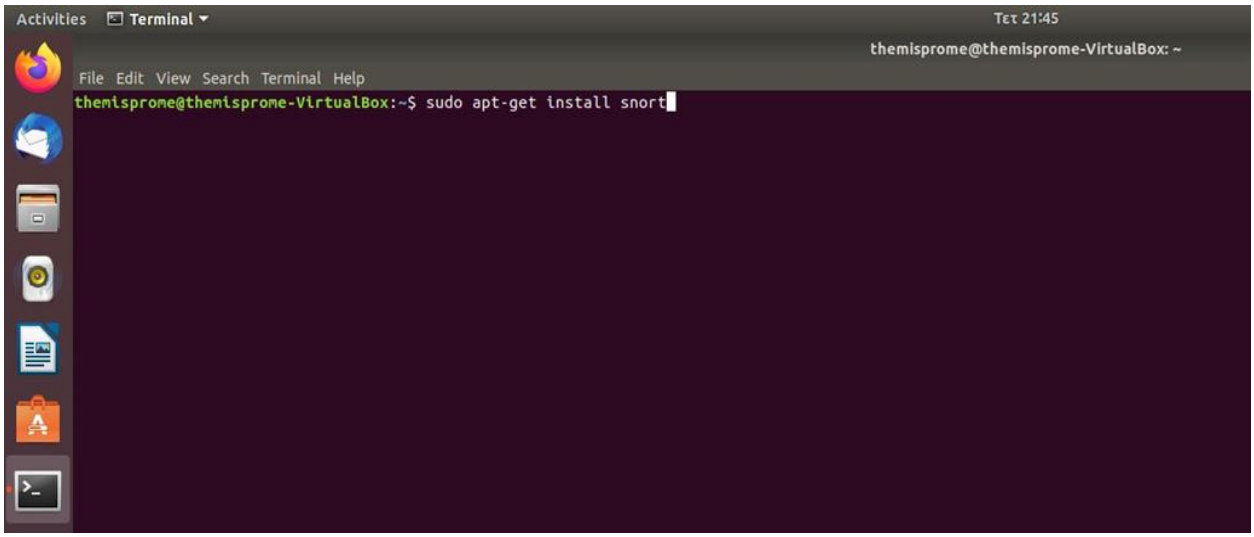


Εικόνα 13 : Ενημέρωση των repositories

Αφού πραγματοποιήσαμε την ενημέρωση, χρησιμοποιούμε την εντολή “sudo apt-get install snort’’ για να εγκαταστήσουμε το Snort. Με αυτό το τρόπο θα εγκαταστήσουμε τα απαραίτητα αρχεία που χρειάζομαστε για να αξιοποιήσουμε τις λειτουργίες του. Χρησιμοποιώντας το “sudo” δίνουμε τις απαραίτητες άδειες στον χρήστη του

συστήματος (administrator), ώστε να μπορεί να έχει πρόσβαση στις λειτουργίες του προγράμματος.

4.2



Εικόνα 14 : Εγκατάσταση του Snort

Στον πυρήνα του, το Snort αποτελεί ένα σύστημα ανίχνευσης και πρόληψης εισβολών (IDS, IPS), με την ικανότητα να ανιχνεύει ανεπιθύμητες παρεμβάσεις σε ένα δίκτυο και να λαμβάνει προληπτικά μέτρα. Αυτό επιτυγχάνεται με την συγγραφή και χρήση κανόνων (rules). Η σύνταξη ενός κανόνα γίνεται είτε από εμάς, είτε με την χρήση έτοιμων κανόνων.

Ένας κανόνας συνήθως αποτελείται από τα εξής :

Ενέργεια, πρωτόκολλο, ip διευθύνσεις, χειριστής κατεύθυνσης, αριθμοί πορτών

Η συγκεκριμένη γραμμή κώδικα ονομάζεται Rule Header και αποτελείται από κάποια βασικά μέρη που αναλύονται περισσότερο στις παρακάτω υποενότητες :

Πριν αναλύσουμε το τι που μπορούμε να επιλέξουμε ως action πρέπει να γνωρίζουμε ότι οι ενέργειες των κανόνων (Rule Actions) καθορίζουν το πως πρέπει το Snort να χειριστεί τα πακέτα που ταιριάζουν με τον κανόνα που εμείς θέσαμε στο πρόγραμμα.

Αυτό μπορεί, για παράδειγμα να είναι μια ειδοποίηση ή ακόμη και αποκλεισμός ενός πακέτου που πληρεί τα κριτήρια της εντολής.

4.2.2 Οι βασικές ενέργειες του Snort

Υπάρχουν πέντε βασικές ενέργειες:

- alert: δημιουργεί μια ειδοποίηση για το τρέχον πακέτο
- block: αποκλείει το τρέχον πακέτο και όλα τα επόμενα πακέτα σε αυτήν τη ροή
- drop: απορρίπτει το τρέχον πακέτο
- log: καταγράφει το τρέχον πακέτο σε αρχείο καταγραφής
- pass: επισημαίνει το τρέχον πακέτο ως περασμένο

Το πρωτόκολλο (Protocol) : Το πεδίο του πρωτοκόλλου δίνει κατευθύνσεις στο Snort για τον τύπο των πρωτοκόλλων που πρέπει να εξετάσει ένας συγκεκριμένος κανόνας που δίνεται, και αυτά που υποστηρίζονται επί του παρόντος περιλαμβάνουν τα πρωτόκολλα ip, icmp, tcp και udp. Κάθε κανόνας μπορεί να έχει μόνο ένα πρωτόκολλο ορισμένο, και το όνομα του πρωτοκόλλου τοποθετείται μετά τη δράση του κανόνα.

Τις IP διευθύνσεις : Οι διευθύνσεις IP σε ένα Rule Header δίνουν οδηγίες στο Snort για το ποιες πηγαίες και προορισμένες διευθύνσεις IP θα ισχύσουν για τον συγκεκριμένο κανόνα. Ένας κανόνας θα ταιριάξει μόνο αν οι πηγαίες και προορισμένες διευθύνσεις IP ενός συγκεκριμένου πακέτου ταιριάζουν με τις διευθύνσεις IP που έχουν οριστεί σε αυτόν τον κανόνα.

4.2.3 Δηλώσεις διεύθυνσης

Οι δηλώσεις μιας διεύθυνσης μπορούν να πραγματοποιηθούν με έναν από τους τέσσερις τρόπους:

- Ως αριθμητική διεύθυνση IP με προαιρετικό CIDR block (π.χ. 192.168.0.5, 192.168.1.0/24)
- Ως μεταβλητή που έχει καθοριστεί στη διαμόρφωση του Snort και καθορίζει μια διεύθυνση δικτύου ή ένα σύνολο διευθύνσεων δικτύου

(π.χ. $EXTERNAL_NET, $HOME_NET, κλπ.)

- Τη λέξη-κλειδί "any", που σημαίνει οποιαδήποτε διεύθυνση IP
- Μια λίστα διευθύνσεων IP, μεταβλητών διευθύνσεων IP και/ή

εύρους θυρών, περικλεισμένη σε αγκύλες και χωρισμένη με κόμματα (π.χ. [192.168.1.0/24,10.1.1.0/24])

4.2.4 Αριθμοί θηρών και δηλώσεις

Τους αριθμούς θυρών (port numbers) : Οι αριθμοί θυρών σε ένα Rule Header προσδιορίζουν στο Snort να εφαρμόσει ένα συγκεκριμένο κανόνα στην κίνηση που στέλνεται από ή προς τις καθορισμένες πηγαίες και προορισμένες θύρες.

Οι θύρες δηλώνονται με διάφορους τρόπους:

- Ως οποιεσδήποτε/any θύρες (σημαίνει ταιριάζει με την κίνηση

που αποστέλλεται από ή προς οποιαδήποτε θύρα)

- Ως στατική θύρα (π.χ. 80, 445, 21)
- Ως μεταβλητή θύρα που έχει οριστεί στη διαμόρφωση του Snort

και καθορίζει μια θύρα ή ένα σύνολο θυρών (π.χ. $HTTP_PORTS)

- Ως εύρος θυρών που υποδηλώνεται με τον τελεστή εύρους :

(π.χ. 1:1024, 500:)

- Ως λίστα στατικών θυρών, μεταβλητών θυρών και/ή ευρών

θυρών, περικλεισμένη σε αγκύλες και χωρισμένη με κόμματα (π.χ. [1:1024,4444,5555,$HTTP_PORTS])

4.2.5 Ο χειριστής κατεύθυνσης

Τον χειριστή κατεύθυνσης (direction operator) : Ο τελεστής κατεύθυνσης ο header υποδηλώνει την κατεύθυνση της κίνησης για την οποία θα ισχύει ο κανόνας.

Υπάρχουν δύο έγκυροι τελεστές κατεύθυνσης:

Ο τελεστής -> είναι ο πιο συνηθισμένος και υποδηλώνει ότι οι διευθύνσεις IP και οι αριθμοί θυρών στην αριστερή πλευρά αντιπροσωπεύουν την πηγή και οι διευθύνσεις IP και οι αριθμοί θυρών στη δεξιά πλευρά αντιπροσωπεύουν τον προορισμό.

Η λειτουργία <> είναι ο διπλής κατεύθυνσης τελεστής και λέει στο Snort να θεωρήσει τα δύο ζευγάρια διευθύνσεων IP και αριθμών θυρών είτε ως πηγή είτε ως προορισμό.

Ο τελεστής κατεύθυνσης τοποθετείται μετά τη δήλωση των θυρών στο header.

4.2.7 Πως γράφουμε μια εντολή

Για να γράψουμε μια εντολή πρέπει να βρούμε το αρχείο local.rules. Συνήθως βρίσκεται στο directory /etc/snort/rules/local.rules. Προτείνεται η χρήση του Vim (Επεξεργαστής κειμένου) για την συγγραφή και πρόσβαση του αρχείου.

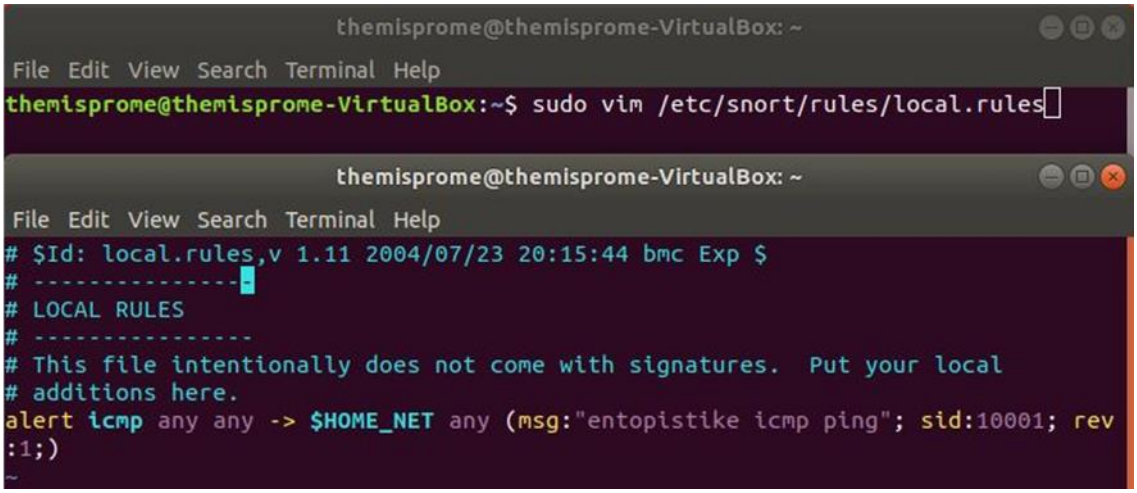
Στην προκειμένη περίπτωση, θα προσθέσουμε έναν κανόνα που θα στέλνει μέσω ping πακέτα icmp (Internet Control Message Protocol) σε μια συσκευή στο τοπικό μας δίκτυο και στην επιστροφή των μηνυμάτων (echo reply) θα προβάλλει ένα alert με το μήνυμα “entopistike icmp ping’’.

Ο κανόνας είναι ο εξής :

alert icmp any any -> $HOME_NET any (msg:” entopistike icmp ping”; sid:10001; rev:1;)

Αφού το κάνουμε αυτό, πατάμε esc και πληκτρολογούμε :w και enter για να γράψουμε τις αλλαγές στο αρχείο. Μπορούμε να αποκτήσουμε πρόσβαση στο local.rules χρησιμοποιώντας την εντολή sudo vim και τον κατάλογο (directory) που αναφέρθηκε παραπάνω. Εκεί μπορούμε να εντοπίσουμε το αρχείο κανόνων, όπου μπορούμε να προσθέσουμε τις δικές μας εξατομικευμένες εντολές.

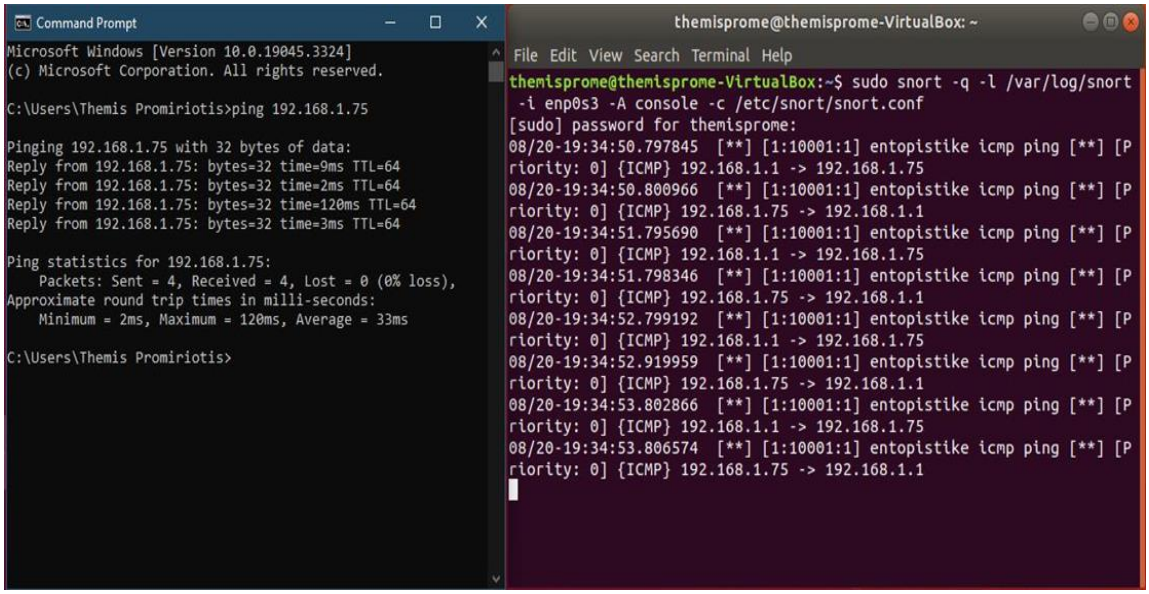
4.2



Εικόνα 15 : Το αρχείο local.rules στο οποίο προσθέσαμε τον κανόνα

Για να θέσουμε σε λειτουργία το Snort, θα τρέξουμε στο terminal μια συγκεκριμένη εντολή με κάποιες παραμέτρους. Η εντολή αυτή θα σκανάρει το τοπικό μας δίκτυο (-i enp0s3), θα αποθηκεύσει οτιδήποτε εντοπίσει σε ένα αρχείο log ώστε να μην χάσουμε τα ευρήματα μας (-l /var/log/snort), θα εμφανίσει τα αποτελέσματα στην κονσόλα (-A console -c) και όλα αυτά βάσει των ρυθμίσεων του Snort που υπάρχουν στο configuration αρχείο (-c /etc/snort/snort.conf).

4.2



Εικόνα 16 : Εντοπισμός ICMP πακέτων στο τοπικό δίκτυο βάσει του κανόνα που θέσαμε

Στην παραπάνω εικόνα χρησιμοποιήθηκε το command prompt των Windows για να κάνει ping μια συσκευή στο ίδιο δίκτυο, συγκεκριμένα μια IP διεύθυνση κινητής συσκευής. Το πρόγραμμα εντόπισε, βάσει εντολής, τα icmp πακέτα που στάλθηκαν και εμφάνισε στην κονσόλα το μήνυμα που θέσαμε. Πιο συγκεκριμένα, μπορούμε να δούμε την πηγαία διεύθυνση (την διεύθυνση του υπολογιστή) που έκανε το ping και την διεύθυνση προορισμού (την διεύθυνση του κινητού) του κάθε πακέτου.

4.2.8 Συμπεράσματα

Συνοψίζοντας, το Snort είναι ένα από τα καλύτερα εργαλεία ανίχνευσης και αποφυγής επιθέσεων καθώς παρέχει την δυνατότητα συγγραφής ποικίλων κανόνων που προσαρμόζονται από τον ίδιο τον χρήστη, ανάλογα την ανάγκη του, και παρέχει άμεση ενημέρωση σε κινήσεις του δικτύου ώστε να αποφευχθούν πιθανές εισβολές και απειλές εγκαίρως.

4.3 NMap (Port Scanning Tool)

4.3 

Εικόνα 17 : Το λογότυπο του προγράμματος NMap.

Το Nmap (Network Mapper) είναι ένα εργαλείο ανοιχτού κώδικα που προσφέρει δωρεάν λειτουργίες ανακάλυψης δικτύου και ελέγχου ασφαλείας. Αποτελεί ένα χρήσιμο εργαλείο για διαχειριστές συστημάτων και δικτύων και βοηθά στην ανακάλυψη δικτύων, τη διαχείριση προγραμμάτων αναβάθμισης υπηρεσιών και την παρακολούθηση της λειτουργίας των οικοδεσποτών και υπηρεσιών.

Το Nmap χρησιμοποιεί ακατέργαστα πακέτα IP με καινοτόμους τρόπους για να προσδιορίσει την διαθεσιμότητα των οικοδεσποτών στο δίκτυο, τις υπηρεσίες που προσφέρουν (όνομα και έκδοση εφαρμογής), τα λειτουργικά συστήματα που εκτελούν και τα χαρακτηριστικά τους, όπως τα φίλτρα πακέτων/τείχη firewall. Δημιουργήθηκε για

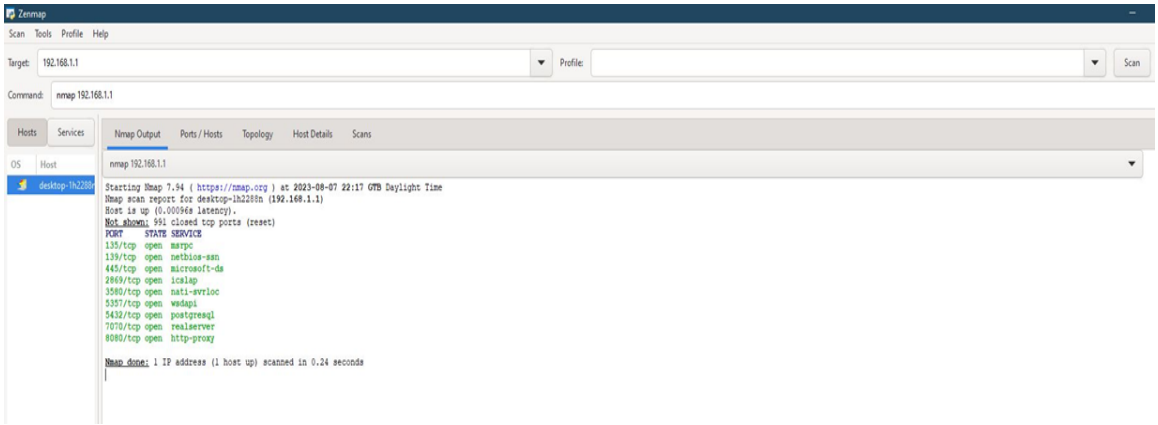
γρήγορη σάρωση μεγάλων δικτύων, αλλά λειτουργεί εξίσου καλά για μεμονωμένους οικοδεσπότες. Υποστηρίζει όλα τα κύρια λειτουργικά συστήματα υπολογιστών, παρέχοντας επίσημα δυαδικά πακέτα για Linux, Windows και Mac OS X.

4.3.1 Πως λειτουργεί το NMap;

Όπως και στο Wireshark, εγκαθιστούμε το εργαλείο από την επίσημη ιστοσελίδα. Στα Windows, το Nmap τρέχει μέσω του Zenmap GUI ώστε να έχουμε ένα πιο φιλικό γραφικό περιβάλλον. Προαιρετικά, εάν διαθέτουμε Kali Linux, μπορούμε να το ανοίξουμε κατευθείαν καθώς είναι προ-εγκατεστημένο στο λειτουργικό σύστημα.

Η εντολή για να εκτελέσουμε βασικά scans σε έναν target είναι η εντολή nmap target, οπού ως target, μπορεί να θεωρηθεί μια διεύθυνση ή ένα hostname. Με αυτόν τον τρόπο σκανάρουμε έναν και μόνο host, ενώ αν προσθέσουμε με κενά και άλλα targets, μπορούμε να σκανάρουμε πολλά παράλληλα. Ανοίγοντας το πρόγραμμα, μπορούμε να δοκιμάσουμε να κάνουμε scan στο δίκτυο μας χρησιμοποιώντας την εντολή, nmap.

4.3



Εικόνα 18 : Αποτελέσματα scan ενός στόχου

4.3.2 Είδη θυρών στο Nmap (Ports)

Αφού τρέξουμε το scan και ανακαλύψουμε τα ports του στόχου μας, υπάρχουν 3 κύριες περιπτώσεις που μπορεί να εντοπίσουμε στο terminal του προγράμματος. Ανοιχτές, κλειστές και φιλτραρισμένες θύρες.

Ανοιχτές θύρες (Open Ports) : Σε μια ανοιχτή θύρα, μια εφαρμογή είναι ενεργά έτοιμη να δεχτεί συνδέσεις TCP, πακέτα UDP ή συναλλαγές SCTP. Κατά την σάρωση θυρών, η ανακάλυψη αυτών των ανοιχτών θυρών αποτελεί συχνά το κύριο στόχο. Αναγνωρίζοντας την κρίσιμη σημασία, εκείνοι με ανησυχίες για την ασφάλεια γνωρίζουν ότι κάθε ανοιχτή θύρα δημιουργεί έναν πιθανό δρόμο επίθεσης. Επιτιθέμενοι και ειδικοί σε δοκιμές ασφαλείας αναζητούν τρόπους να εκμεταλλευτούν αυτές τις αδύναμες συνδέσεις, ενώ οι διαχειριστές προσπαθούν να αποτρέψουν τις επιθέσεις, κλείνοντας ή προστατεύοντας τις ανοιχτές θύρες με τείχη προστασίας, χωρίς να επηρεάζουν τη λειτουργία των νόμιμων χρηστών.

Κλειστές θύρες (Closed Ports) : Μια κλειστή θύρα είναι προσβάσιμη (λαμβάνει και ανταποκρίνεται σε πακέτα ερωτήματος Nmap), αλλά δεν υπάρχει εφαρμογή που ακούει σε αυτήν. Οι κλειστές θύρες μπορούν να βοηθήσουν στην επιβεβαίωση της ύπαρξης ενός ενεργού υπολογιστή σε μια συγκεκριμένη διεύθυνση IP (ανίχνευση της ύπαρξης του υπολογιστή ή σάρωση ping), καθώς και να αποτελέσουν μέρος της διαδικασίας ανίχνευσης του λειτουργικού συστήματος. Λόγω του ότι οι κλειστές θύρες είναι προσβάσιμες, είναι δυνατόν να εξεταστεί η πιθανότητα μελλοντικής σάρωσης, αν κάποιες από αυτές ανοίξουν. Σε περίπτωση ανοίγματος, οι διαχειριστές μπορεί να εξετάσουν τον αποκλεισμό τέτοιων θυρών με τη χρήση ενός τείχους προστασίας.

Φιλτραρισμένες θύρες (Filtered Ports): Ο Nmap δεν μπορεί να επαληθεύσει εάν η θύρα είναι ανοιχτή επειδή το φίλτρο πακέτων εμποδίζει τις ερωτήσεις του να φτάσουν στη θύρα. Αυτό το φιλτράρισμα μπορεί να αποτελείται από εξειδικευμένες συσκευές τείχους, κανόνες δρομολογητή ή λογισμικό τείχους που εκτελείται στον υπολογιστή. Αυτές οι περιπτώσεις είναι ενοχλητικές για τους εισβολείς, καθώς παρέχουν ελάχιστες πληροφορίες. Σε μερικές περιπτώσεις, μπορεί να ανταποκριθούν με μηνύματα σφάλματος ICMP, όπως το τύπος 3 και κωδικός 13 (αδυναμία προορισμού: η επικοινωνία είναι απαγορευμένη από διαχειριστή). Ωστόσο, είναι συνηθέστερο τα φίλτρα απλά να αγνοούν τις ερωτήσεις χωρίς να ανταποκρίνονται. Αυτό αναγκάζει το Nmap να επαναλάβει τις προσπάθειές του αρκετές φορές, με σκοπό να διαπιστώσει εάν η ερώτηση απορρίφθηκε λόγω κυκλοφοριακής συμφόρησης αντί για φιλτράρισμα. Αυτή η διαδικασία επιβραδύνει σημαντικά τη σάρωση των θυρών.

Σε συγκεκριμένες περιπτώσεις, μπορούμε να παρατηρήσουμε και θύρες που είναι unfiltered, open|filtered ή και closed|filtered. Αυτό σημαίνει ότι το πρόγραμμα δεν κατόρθωσε να προσδιορίσει την κατάσταση της θύρας, δηλαδή αν είναι ανοιχτή/κλειστή, ανοιχτή/φιλτραρισμένη ή κλειστή/φιλτραρισμένη.

4.3.3 Είδη σαρώσεων (Scanning)

Εκτός από βασικά scans το Nmap μπορεί, βάσει κάποιον ιδιοτήτων που προστίθονται μετά την εντολή, να σκανάρει πιο στοχευμένα. Η τρείς συχνότερες τεχνικές port scanning στο Nmap είναι οι εξής:

TCP Connect Scan (-sT) : Χρησιμοποιείται για την επιβεβαίωση και ολοκλήρωση της τρικατευθυντής χειραψίας (three-way handshake) ανάμεσα στον επιτιθέμενο και τον στοχευμένο υπολογιστή. Ένας τέτοιος τύπος σάρωσης μπορεί να ανιχνευθεί εύκολα, καθώς το service απαριθμεί τις πόρτες που ανταποκρίθηκαν, και αυτό μπορεί να ενεργοποιήσει τα συστήματα ανίχνευσης εισβολών.

TCP SYN Scan (-sS) : Σε αντίθεση με την κανονική σάρωση TCP, το Nmap χρησιμοποιεί το δικό του SYN πακέτο, που είναι το πρώτο πακέτο που αποστέλλεται για να προσπαθήσει να εγκαταστήσει μια σύνδεση TCP. Σημαντικό είναι να επισημάνουμε ότι η σύνδεση δεν ολοκληρώνεται ποτέ πραγματικά, αλλά οι απαντήσεις που λαμβάνονται από τον στοχευμένο υπολογιστή αναλύονται από το Nmap.

UDP Scan (-sU) : Αυτό το είδος σάρωσης χρησιμοποιείται για να εξετάσει την ύπαρξη προσβάσιμων UDP θυρών που περιμένουν εισερχόμενες συνδέσεις στον επιθυμητό υπολογιστή. Σε αντίθεση με το πρωτόκολλο TCP, το πρωτόκολλο UDP δεν παρέχει μηχανισμούς επιβεβαίωσης παραλαβής πακέτων, και αυτό οδηγεί σε περιπτώσεις "false positive" (λανθασμένα θετικά) στις αναγνώσεις. Αυτό το είδος σάρωσης είναι επίσης πιο αργό σε σχέση με τις σαρώσεις TCP, καθώς τα μηχανήματα τείνουν να καθυστερούν τις απαντήσεις τους σε τέτοιες κινήσεις, ως μέτρο προφύλαξης.

4.3.4 Συμπεράσματα

Εν τέλει, το Nmap αποτελεί ένα ισχυρό εργαλείο με πολλαπλές λειτουργίες που χρησιμοποιείται από διαχειριστές δικτύων, επαγγελματίες ασφάλειας και ηθικούς χάκερ για τον εντοπισμό ευπαθειών και σε έλεγχο των κινήσεων του δικτύου.

5 Μελέτες επιθέσεων (Real-World Incidents) και κινδύνων σε δίκτυα IoT

Η ερευνητική προσέγγιση σε πραγματικά περιστατικά, γνωστή και ως Case Studies, αποτελεί ένα ισχυρό εργαλείο που επιτρέπει την εμβάθυνση στην κατανόηση των προκλήσεων και των αντίστοιχων λύσεων που αντιμετωπίζουν οι οργανισμοί άπο επιθέσεις. Το τελευταίο κεφάλαιο επικεντρώνεται στην ανάλυση πραγματικών περιστατικών, παρέχοντας ενδελεχή εικόνα των προκλήσεων που αντιμετώπισαν οι επιχειρήσεις και οι οργανισμοί κατά τη διάρκεια των αναπάντεχων αυτών συμβάντων. Μέσω της ανάλυσης αυτών των περιστατικών θα μπορέσουμε να έχουμε μια καλύτερη κατανόηση των κινδύνων που μπορεί να υπάρχουν στην καθημερινότητα μας.

5.1 Mirai Botnet Attack (2016)

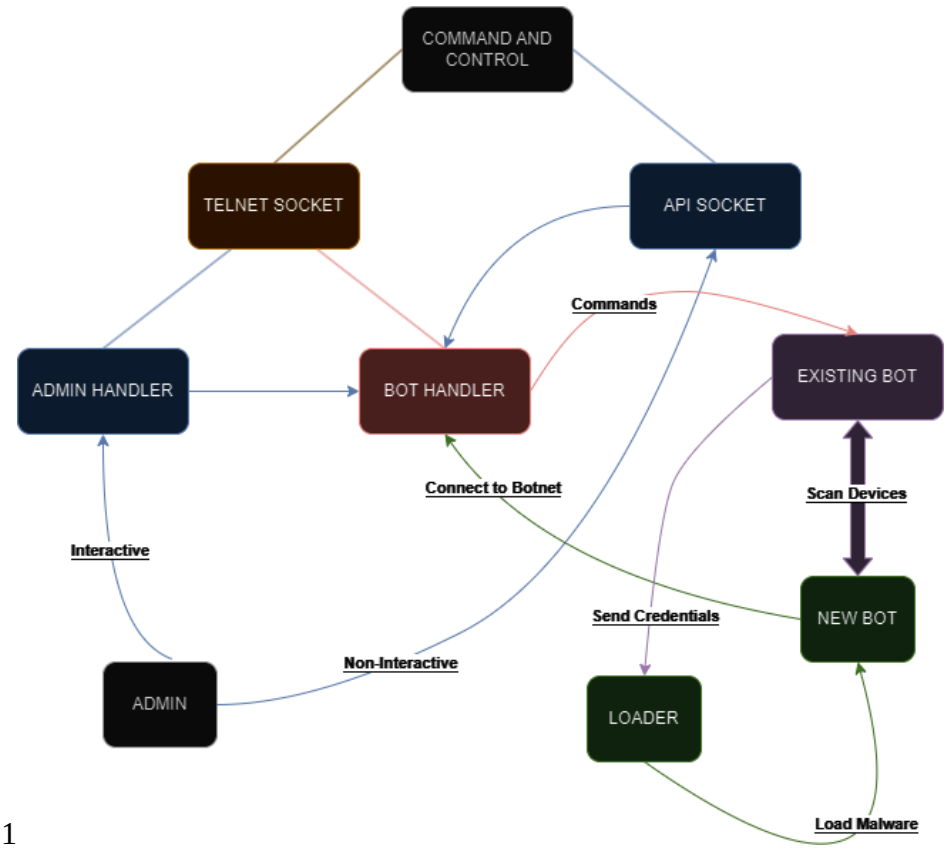
Στις 20 Σεπτεμβρίου 2016, η ιστοσελίδα του αξιόλογου δημοσιογράφου ασφάλειας, Brian Krebs, βγήκε εκτός λειτουργίας από μια από τις μεγαλύτερες επιθέσεις Distributed Denial Of Service (DDoS) που έχουν καταγραφεί. Αυτή η επίθεση προήλθε από το Mirai Botnet και σημάδεψε την έναρξη μιας ανησυχητικής εποχής στον κόσμο του Διαδικτύου.

Μόλις 10 μέρες μετά την πρώτη επίθεση, στις 30 Σεπτεμβρίου 2016, ένας χρήστης με το όνομα "Anna-Senpai" ανέβασε στο HackForums.net τον πηγαίο κώδικα και τις οδηγίες του Mirai Botnet. Αυτή η ενέργεια οδήγησε τον Brian Krebs στην έρευνα για την ταυτότητα του δημιουργού του Mirai, καταφέρνοντας να αποκαλύψει τον χρήστη "Anna-Senpai" και τουλάχιστον έναν συνεργό του.

Σχεδόν τρεις μήνες μετά, στις 21 Οκτωβρίου 2016, πραγματοποιήθηκε η μεγαλύτερη επίθεση DDoS της εποχής, με μέγεθος 1,2 Tbps, κατευθυνόμενη κατά της δημοφιλούς πάροχου Dynamic DNS, Dyn. Η επίθεση αυτή προκάλεσε την αναστολή λειτουργίας μεγάλου αριθμού ιστότοπων και υπηρεσιών που χρησιμοποιούσαν τη Dyn ως πάροχο DNS, προσελκύοντας μεγάλο ενδιαφέρον από τα μέσα ενημέρωσης.

5.1.1 Αρχιτεκτονική

Το Mirai Botnet είναι ειδικά σχεδιασμένο για την πραγματοποίηση επιθέσεων DDoS, που αναφέρθηκαν σε προηγούμενο κεφάλαιο. Αυτού του είδους οι επιθέσεις συνήθως χρησιμοποιούνται με σκοπό την υπερφόρτωση ιστοσελίδων και άλλων υπηρεσιών, καθιστώντας τις μη λειτουργικές. Η εξαιρετική αποτελεσματικότητα του Mirai στο να εκμεταλλεύεται νέες συσκευές εξηγεί τη διακριτική του διάδοση ανάμεσα σε άλλα bot-nets που κυκλοφορούσαν. Το πλήρες σχήμα της αρχιτεκτονικής του Mirai παρουσιάζεται στην Εικόνα 19, με το κάθε τμήμα του να αναλύεται παρακάτω.



5.1.1

Εικόνα 19 : Η αρχιτεκτονική του Mirai Botnet

Η διάταξη που παρουσιάζεται στην Εικόνα 19 προσδιορίζεται ως εξής:

Ο διακομιστής ελέγχου και εντολών (Command and Control Server) εκτελεί δύο socket listeners: έναν για συνδέσεις Telnet και έναν για ένα προγραμματιστικό API. Το socket του Telnet ακούει στη θύρα 23 και δρομολογεί οποιεσδήποτε έγκυρες συνδέσεις προς αυτόν στους αντίστοιχους χειριστές bot ή διαχειριστή (Bot or Admin Handler).

Το socket του API ακούει στη θύρα 101 και δρομολογεί οποιεσδήποτε έγκυρες επιθέσεις που αποστέλλονται σε αυτό στα συνδεδεμένα bots. Επιπλέον, κάθε συνδεδεμένο bot σαρώνει το Διαδίκτυο για νέες ευάλωτες συσκευές. Μόλις ανακαλυφθεί μία, τα credentials, η διεύθυνση IP και η θύρα που χρησιμοποιήθηκαν για πρόσβαση αποστέλλονται σε ένα διακομιστή φόρτωσης (loader server).

Αυτός ο loader εμφανίζει τις πληροφορίες στην κονσόλα για ενδεχόμενη αποθήκευση σε αρχείο και στη συνέχεια χρησιμοποιεί τα δεδομένα για την λήψη και εκτέλεση mal-ware στη συσκευή. Αυτή η διαδικασία επαναλαμβάνεται από κάθε μολυσμένη συσκευή, δημιουργώντας το εφέ snowball.

5.1.3 Τύποι επιθέσεων

Παρακάτω αναφέρονται κάποιες περιπτώσεις επιθέσεων που μπορούν να πραγματοποιηθούν μέσω του Mirai.

5.1.3.1 DNS Flood

Η επίθεση πλημμύρας του DNS Resolver, αποστέλλει προεπιλεγμένα στη θύρα 53 και δημιουργεί ένα αναδρομικό αίτημα DNS με τυχαία δεδομένα, προκειμένου να φορτώσει τον διακομιστή DNS και να τον αποκλείσει. Αυτό οδηγεί τον διακομιστή DNS στο να επαναμεταδώσει το αίτημα σε άλλο διακομιστή DNS, ο οποίος επιτίθεται στον στόχο, με αποτέλεσμα η επίθεση να μην προέρχεται ποτέ απευθείας από ένα bot.

5.1.3.2 SYN και ACK Flood

Η επίθεση SYN flood στοχεύει στη δημιουργία ανοιχτών συνδέσεων και στην πλημμύρα του διακομιστή με πακέτα SYN. Αναλυτικότερα, δημιουργεί έγκυρα πακέτα TCP με μόνο τη SYN flag ορισμένη από προεπιλογή, ενώ τυχαία ορίζει τα flags MSS, WS και TSV (Max Segment Size, Window Scale, and Timestamp Value). Η επίθεση ACK flood

είναι παρόμοια με την SYN flood, αλλά στέλνει μόνο το ACK flag και δεν ορίζει τα flags WS ή TSV.

5.1.3.3 TCP STOMP Flood

Η επίθεση TCP STOMP flood είναι παρόμοια με την επίθεση ACK flood, αλλά χρησιμοποιεί το πρωτόκολλο STOMP (Streaming Text Oriented Messaging Protocol), ένα text-based ανοιχτό πρωτόκολλο μηνυμάτων. Η επίθεση ανοίγει ένα TCP handshake και στη συνέχεια στέλνει τυχαία δεδομένα τα οποία είναι διαμορφωμένα να μοιάζουν με ένα αίτημα STOMP. Αυτό κατακλύζει το δίκτυο και μπορεί να απορροφήσει πόρους εάν ο στόχος έχει ρυθμιστεί να ερμηνεύει μηνύματα STOMP.

5.1.3.4 HTTP Flood

Η επίθεση HTTP flood σχεδιάστηκε ειδικά για να προκαλέσει φόρτο σε έναν διακομιστή ιστού (web server) με την αποστολή μεγάλου αριθμού αιτημάτων, τα οποία απαιτούν σημαντικό χρόνο επεξεργασίας. Επιπλέον, διατηρεί ανοικτές συνδέσεις για να καταλάβει τους διαθέσιμους χώρους σύνδεσης στο διακομιστή, εμποδίζοντας τη λήψη νέων συνδέσεων.

Κάθε μια από τις επιθέσεις που καλύφθηκαν σε αυτήν την υποενότητα είναι σε θέση να προκαλέσει μεγάλη ζημιά. Το Mirai δεν λειτουργεί χωρίς να υπάρχει κάποια ανταπόκριση από τον διακομιστή ελέγχου και εντολών. Μόλις ένας από τους χειριστές συνδεθεί στο διαχειριστή μέσω Telnet, είναι σε θέση να στείλει εντολές στα bots που θα εκτελέσουν την καθορισμένη επίθεση σε έναν στόχο.

Οι δυνατότητες DDoS που υπάρχουν στο Mirai δεν κάνουν κάτι που δεν έχει παρατηρηθεί σε παλαιότερα χρόνια, αλλά η ικανότητά του να εξαπλωθεί σε νέες συσκευές δεν είχε αντίπαλο μέχρι την αποκάλυψη του πηγαίου του κώδικα. Οι δυνατότητες προσβολής με τη μορφή Worm (σκουλικιού) του Mirai σε συνδυασμό με τις επιθέσεις που είναι διαθέσιμες το καθιστούν σημαντικό και επικίνδυνο.

5.1.4 Τρόποι άμυνας και αποφυγής

Στην υποενότητα αυτή, παρουσιάζονται κάποιοι τρόποι αντιμετώπισης που μπορούν να παρέχουν μια μορφή άμυνας ή και αποφυγής σε συσκευές που είναι ευάλωτες σε επιθέσεις.

5.1.4.1 Αλλαγή των Credentials

Η πιο συνηθισμένη προσέγγιση για την προστασία των συσκευών από το Mirai είναι η αλλαγή του ονόματος χρήστη και του κωδικού πρόσβασης που χρησιμοποιούνται για την πρόσβαση στη συσκευή μέσω SSH ή Telnet. Αυτό είναι εφικτό με διαφορετικούς τρόπους για κάθε συσκευή, αλλά συνήθως γίνεται μέσω του δικτυακού περιβάλλοντος (web interface) της συσκευής. Ωστόσο, πρέπει να σημειωθεί ότι ο κωδικός που μπορεί να αλλάξει με αυτόν τον τρόπο ενδέχεται να μην είναι ο ίδιος με αυτόν που χρησιμοποιείται για τη σύνδεση στη συσκευή μέσω SSH ή Telnet. Ως αποτέλεσμα, είναι σημαντικό να εφαρμοστεί περαιτέρω προστασία, εάν είναι εφικτό.

5.1.4.2 Κλείσιμο αχρησιμοποίητων θυρών

Οι θύρες 22 (SSH) και 23 (Telnet) χρησιμοποιούνται από το Mirai για να ελέγξει την έγκυρη είσοδο στις συσκευές. Συνήθως, αυτές οι θύρες δεν θα έπρεπε να είναι προσβάσιμες δημοσίως, εκτός αν γίνεται εκ των προτέρων από έναν προχωρημένο χρήστη που είναι ενήμερος για τους κινδύνους που υπάρχουν. Εάν είναι εφικτό, οι θύρες αυτές θα πρέπει να κλείσουν μέσω των ρυθμίσεων του δρομολογητή (router), προκειμένου να μπλοκάρονται οι προσπάθειες σύνδεσης προς εσωτερικές συσκευές.

5.1.4.3 Δημιουργία ενός Automated Protection Script

Ως εναλλακτική λύση, μπορεί να χρησιμοποιηθεί ένα script που είναι βελτιστοποιημένο για τον τελικό χρήστη (end-user optimized script) για τον έλεγχο και την ενίσχυση οποιασδήποτε συσκευής IoT σε ένα δίκτυο. Το script θα είναι σε θέση να σαρώσει το τρέχον δίκτυο του χρήστη για να ελέγξει αν υπάρχουν ευάλωτες συσκευές. Αν και υπάρχει ένα παρόμοιο εργαλείο σάρωσης, περιορίζεται από το γεγονός ότι ελέγχει μόνο τις θύρες 22 και 23, οι ίδιες δηλαδή που χρησιμοποιεί το Mirai για να μολύνει συσκευές.

Το σενάριο θα πρέπει να χρησιμοποιείται εντός ενός τοπικού δικτύου για να ελέγξει όλες τις συσκευές και να επιβεβαιώσει ότι είναι ασφαλείς. Όταν μια συσκευή

ανακαλύπτεται, θα πρέπει να γίνουν προσπάθειες σύνδεσης που είναι πανομοιότυπες με αυτές που πραγματοποιεί το Mirai και άλλα γνωστά samples κακόβουλου λογισμικού IoT. Αυτό θα επιβεβαιώσει με ασφάλεια ότι, αν η συσκευή ανακαλυφθεί από έναν επιτιθέμενο, θα είναι ασφαλής από επιθέσεις σύνδεσης (login attacks).

Εάν το script είναι σε θέση να αποκτήσει πρόσβαση στη συσκευή χρησιμοποιώντας συνδιασμούς του username και του κωδικού που χρησιμοποιήθηκαν κακόβουλα, θα πρέπει να χρησιμοποιήσει την πρόσβαση που έχει αποκτήσει για να αλλάξει αυτόματα τα credentials της συσκευής, να ελέγξει τη συσκευή και να αφαιρέσει οποιοδήποτε προ-υπάρχων κακόβουλο λογισμικό, και να ενημερώσει τον χρήστη, ειδικά αν έχουν αλλάξει τα credentials της συσκευής.

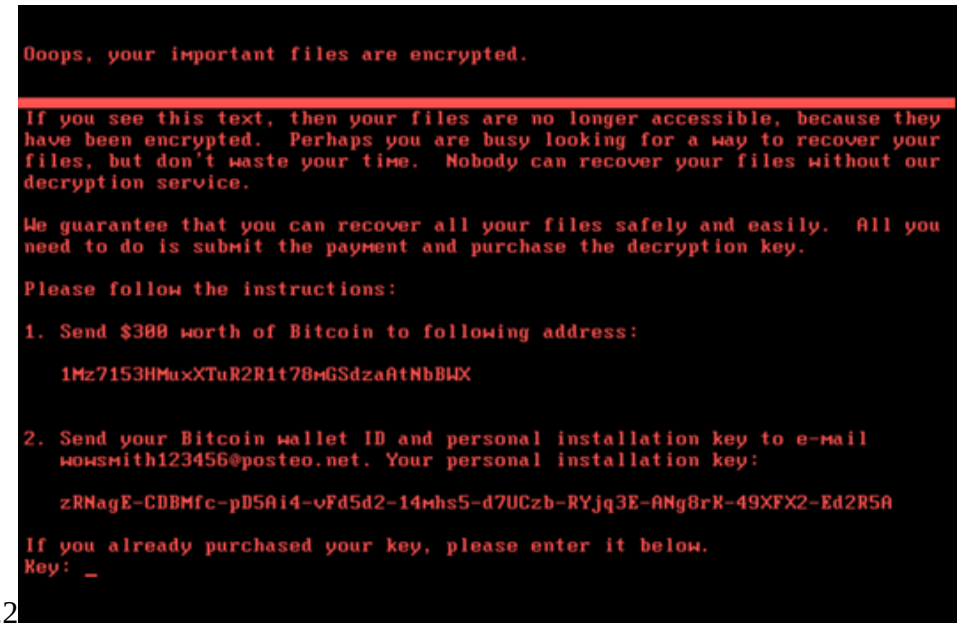
5.1.5 Συμπεράσματα

Το Mirai Botnet είναι δύσκολο από άποψη διαχείρισης λόγω της ευρείας διάδοσης του και της ταχύτητας του. Παρ' όλα αυτά, δεν είναι αδύνατο να ανιχνευθεί ή να σταματηθεί. Με τη χρήση των τεχνικών που προτάθηκαν, οι συσκευές μπορούν να προστατευθούν επαρκώς και οι προτεινόμενες λύσεις είναι εύκολο να εφαρμοστούν, καθώς μερικές από αυτές μπορούν να πραγματοποιηθούν από τους ιδιοκτήτες των συσκευών. Το Mirai πρέπει να θεωρηθεί ως μάθημα για την βιομηχανία των IoT συσκευών, καθώς προσφέρει σημαντικές ενδείξεις για βελτίωση της ασφάλειας στο μέλλον.

5.2 NotPetya Attack (2017)

Το NotPetya, κατά την εμφάνισή του το 2017, είχε αρχικά ταξινομηθεί ως ransomware. Αυτό το κακόβουλο πρόγραμμα εισβάλλει στον υπολογιστή εισάγοντας κακόβουλο κώδικα, με στόχο την απόκτηση πρόσβασης διαχειριστή (admin rights). Στη συνέχεια, διαδίδεται σε άλλους υπολογιστές στο δίκτυο, εκμεταλλευόμενο από την ευπάθεια του EternalBlue Server Message Block (SMB). Μετά την μόλυνση, οι σκληροί δίσκοι κρυπτογραφούνται, και κατά την εκκίνηση του υπολογιστή, εμφανίζεται συνήθως κάποιο μήνυμα απαίτησης λύτρων. Η ιδιαιτερότητα του NotPetya είναι ότι δεν παρέχει αρκετές πληροφορίες για την αποκρυπτογράφηση, καθιστώντας την ανάκτηση δεδομένων αδύνατη. Οι επιπτώσεις της επίθεσης εκτείνονται σε επιχειρήσεις διαφόρων τομέων, με περιορισμένες προοπτικές ανάκαμψης του συστήματος.

5.2



Εικόνα 20 : Παράδειγμα μηνύματος επίθεσης NotPetya

Το NotPetya υποκρίνεται το Petya Ransomware και επιτίθεται σε εταιρείες και μη κερδοσκοπικούς οργανισμούς, από λιμάνια αποστολής, σούπερ μάρκετ μέχρι και δικηγορικά γραφεία. Μόλις εισβάλει στο σύστημα μιας εταιρείας, προκαλεί μεγάλη καταστροφή, μεταφέροντας τον κακόβουλο κώδικα από υπολογιστή σε υπολογιστή και καταστρέφοντας τα συστήματα εγγράφων των μηχανών. Αν και ζητά περίπου 300 δολάρια σε Bitcoin για να αποκρυπτογραφήσει τα δεδομένα, οι μηχανισμοί που συγκεντρώνουν αυτό το ποσό από τις εταιρείες που αποτελούν θύματα καταρρέουν σε λίγα λεπτά.

Το κακόβουλο αυτό λογισμικό χρησιμοποιεί ένα προκαθορισμένο πακέτο εργαλείων για να διαπεράσει το δίκτυο μιας εταιρείας, μολύνοντας μηχανές καθώς προχωρά. Συγκεκριμένα, χρησιμοποιεί μια προσαρμοσμένη μορφή του ανοιχτού κώδικα Mimikatz για να αφαιρέσει τις διαπιστεύσεις του διαχειριστή δικτύου (network admin credentials) από τη μνήμη λειτουργίας του υπολογιστή. Έπειτα, χρησιμοποιεί αυτές τις πληροφορίες για να συνδεθεί και να εκτελέσει εργασίες σε διάφορες μηχανές, χρησιμοποιώντας τα PsExec και το Windows Management Instrumentation Command-line (WMIC) για να τις μολύνει. Μπορεί είτε να κάνει channel υποδικτύα για συσκευές είτε, αν τρέχει σε έναν ελεγκτή περιοχής (area controller), να χρησιμοποιήσει την υπηρεσία Dynamic Host Configuration Protocol (DHCP) για τον εντοπισμό γνωστών host.

Παρομοίως, χρησιμοποιεί και μια τροποποιημένη έκδοση των εργαλείων SMB EternalBlue και EternalRomance της Εθνικής Υπηρεσίας Ασφάλειας (NSA), που προηγουμένως είχαν κλαπεί και διαρρεύσει, για να μολύνει διάφορα συστήματα εισάγοντας κακόβουλο κώδικα σε αυτά. Αυτά τα κυβερνο-όπλα επιτίθενται σε ευπάθειες που είχαν διορθωθεί πρόσφατα από τη Microsoft, γεγονός που καθιστά την κλοπή των credentials πιο επιτυχημένη, τουλάχιστον σε θέσεις που έχουν υπερβεί τις ενημερώσεις των Windows. Με επιτακτικότητα, το NotPetya στοχεύει στο να αποκτήσει πρόσβαση διαχειριστή σε έναν υπολογιστή, και στη συνέχεια να χρησιμοποιήσει αυτή την ενέργεια για να αναλάβει τον έλεγχο σε διάφορους υπολογιστές στο δίκτυο, εκμεταλλεύοντας το γεγονός ότι πολλές οργανώσεις χρησιμοποιούν επίπεδα δίκτυα (leveled networks) στα οποία ένας διαχειριστής σε ένα άκρο μπορεί να ελέγχει πολλούς υπολογιστές ή να κατασκοπεύει (sniff) τα managerial credentials του δικτύου περιοχής μέσα στη μνήμη, μέχρι τη στιγμή που θα αποκτήσει πλήρης έλεγχο του δικτύου των Windows.

Με πρόσβαση διαχειριστή, το κακόβουλο λογισμικό μπορεί να προκαλέσει σοβαρές ζημιές όπως το να αλλοιώσει το Master Boot Record (MBR) του σκληρού δίσκου στον διπλανό υπολογιστή, επιτρέποντας την εκκίνηση αποκλειστικά του κακόβουλου λογισμικού κατά την επανεκκίνηση, και όχι των Windows. Αυτό επιτρέπει στο λογισμικό να εμφανίσει αιτήματα απόκτησης κλειδιού ξεκλειδώματος. Επιπλέον, μπορεί να παραβιάσει τους πίνακες και τα αρχεία του New Technology File System (NTFS) στο δίσκο, κρυπτογραφώντας τα δεδομένα των χρηστών με τον αλγόριθμο AES-128.

5.2.1 Προβλήματα και προκλήσεις

5.2.1.1 Σε εταιρίες υγειονομικής περίθαλψης

Στον τομέα της υγείας, οι υγειονομικές εγκαταστάσεις αποτελούν έναν κρίσιμο στόχο για πιθανούς εγκληματίες, με βάση αυτά που παρουσιάζονται στην έκθεση Verizon Data Breach Investigations New Report (DBIR). Αυτός ο τομέας βρίσκεται υπό μεγαλύτερο κίνδυνο σε σύγκριση με άλλους, με το 72% όλων των επιθέσεων κακόβουλου λογισμικού να επικεντρώνεται στον τομέα της υγείας. Ο λόγος τείνει να βασίζεται στο ότι οι πληροφορίες των ασθενών είναι ζωτικής σημασίας για τα νοσοκομεία και μπορεί να αποτελέσουν θέμα ζωής και θανάτου, οπότε οι εγκληματίες γνωρίζουν ότι μπορούν να πάρουν το αίτημα λύτρων που ζητήθηκε. Ένα εξαιρετικό παράδειγμα θα ήταν η

κατάσταση του Κέντρου Ιατρικής του Hollywood Presbyterian, το οποίο κατέβαλε περίπου 17.000 δολάρια σε κυβερνοεγκληματίες για το κλειδί αποκρυπτογράφησης προκειμένου να ασφαλίσει πίσω τα έγγραφά του.

5.2.1.2 Στην εκπαίδευση

Σύμφωνα με αναφορά της BitSight Insights, ο τομέας της εκπαίδευσης και γενικότερα οι εκπαιδευτικές δομές έχουν αποτελέσει βασικό στόχο για επιθέσεις ransomware. Ερευνητές ανέφεραν ότι ο τομέας της εκπαίδευσης είχε το υψηλότερο ποσοστό εμφάνισης ransomware, με τουλάχιστον ένα στους δέκα να έχει πληγεί. Πλεονέκτημα για κυβερνοεπιθέσεις αποτελεί είτε η αδυναμία τους να χειριστούν πολλούς συνδεδεμένους χρήστες καθημερινά, είτε λόγω της ευκολίας εκτέλεσης επιθέσεων spear phishing. Επιπλέον, οι εκπαιδευτικές οργανώσεις δεν διαθέτουν επαρκή εξειδικευμένο προσωπικό στον τομέα της διαχείρισης δικτύου, ειδικά για αυτού του είδους τις επιθέσεις, ενώ συχνά αντιμετωπίζουν και οικονομικά προβλήματα που εμποδίζουν κάποια μελλοντική επένδυση τους στην κυβερνοασφάλεια. Ένα πρόσφατο παράδειγμα είναι το University College London που είδε τους σκληρούς του δίσκους και το σύστημα διαχείρισης των φοιτητών του να πέφτουν θύματα κυβερνοεπίθεσης.

5.2.1.3 Σε διοικητικές υπηρεσίες

Μια άλλη βιομηχανία που αποτελεί ευάλωτο σημείο για επιθέσεις ransomware είναι οι διοικητικές υπηρεσίες και οι οργανισμοί δημόσιας διοίκησης που λειτουργούν και διατηρούν σημαντικές και εξαιρετικά ευαίσθητες προσωπικές πληροφορίες. Η συγκεκριμένη κατηγορία φαίνεται να είναι αρκετά ευάλωτη επειδή οι κυβερνοεγκληματίες γνωρίζουν ότι οι κυβερνητικές εγκαταστάσεις πρέπει να είναι λειτουργικές και αποδοτικές, καθιστώντας πιθανότερο το ενδεχόμενο να πληρώσουν το αντίτιμο για να ανακτήσουν τα δεδομένα τους. Ένα παράδειγμα αποτελεί η εκμετάλλευση της αδυναμίας κάποιων κρίσιμων εταιρειών, όπως ορισμένων κυβερνητικών τμημάτων στην Ουκρανία ή και ανθρώπων που δήλωσαν ότι δεν μπορούσαν να έχουν πρόσβαση στους υπολογιστές τους.

5.2.1.4 Σε νομικές εταιρίες

Οι νομικές εταιρείες είναι ένας ακόμη τομέας που αντιμετωπίζει σοβαρό κίνδυνο, καθώς είναι υπεύθυνες για τα δεδομένα πολλών πελατών τους, τα οποία είναι άκρως εμπιστευτικά και μυστικά και ενδέχεται να έχουν τα κατάλληλα κίνητρα για να πληρώσουν το απαιτούμενο λύτρο ώστε να τα ανακτήσουν. Ένα αληθινό παράδειγμα αποτελεί η νομική εταιρεία DLA Piper που αποτέλεσε θύμα του ransomware Petya, καθώς παρατήρησε τους υπολογιστές της μολυσμένους με το κακόβουλο λογισμικό.

5.2.2 Αύξηση της επίγνωσης του κινδύνου μέσω του Gamification

Παρότι το NotPetya είναι malware, είναι πολύ ανθεκτικό. Οι αναλυτές ασφαλείας ακόμα και σήμερα αναζητούν τρόπους για την απενεργοποίηση του NotPetya μετά την πρόσβαση στους υπολογιστές, αλλά μια οριστική λύση εξακολουθεί να μην έχει βρεθεί. Ωστόσο, υπάρχει ένα εμβόλιο (vaccine) που μπορεί να εξαπατήσει το κακόβουλο λογισμικό NotPetya και να του αποτρέψει την κρυπτογράφηση του σκληρού δίσκου του υπολογιστή, το οποίο προτάθηκε από τα LogRhythm Labs. Αυτό συμβαίνει επειδή, πριν το NotPetya ξεκινήσει την κρυπτογράφηση του σκληρού δίσκου, ελέγχει εάν η συσκευή έχει προηγουμένως μολυνθεί ή όχι, αναζητώντας το αρχείο 'perfc' ή 'perfc.dat'. Εάν το αρχείο υπάρχει, τότε σταματά τη διαδικασία κρυπτογράφησης.

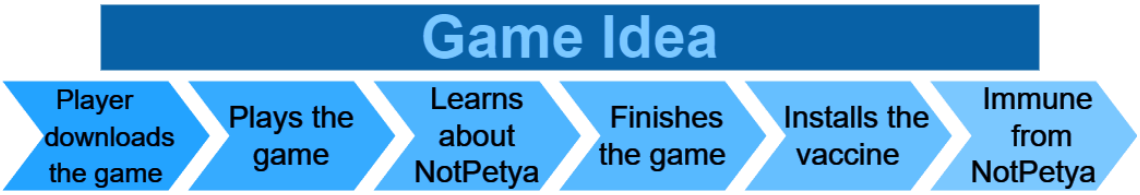
Τα βήματα για να δημιουργηθεί το vaccine αναφέρονται συνοπτικά παρακάτω :

- Ρύθμιση των Windows για εμφάνιση των επεκτάσεων αρχείων (file extensions)
- Μετάβαση στο directory C:\Windows
- Δημιουργία ενός νέου αρχείου
- Μετονομασία του νέου αρχείου σε 'perfc'
- Μετατροπή του 'perfc' σε read-only.

Επαναλαμβάνουμε τα βήματα 3, 4 και 5 και προσθέτουμε τις επεκτάσεις αρχείων '.dat' και '.dll' ως επέκταση του αρχείου ('perfc.dat' και 'perfc.dll').

Παρόλο που η διαδικασία μοιάζει απλή, μπορεί να φανεί δύσκολη σε κάποιον άπειρο χρήστη. Με αφορμή αυτή την διαδικάσια, μπορούμε να διαδώσουμε την επίγνωση αυτού του κινδύνου μέσω του gamification. Με αυτό τον τρόπο απλοί χρήστες θα έχουν την

δυνατότητα να εκπαιδευτούν και να μάθουν για το NotPetya malware μέσω ενός βιντεοπαιχνιδιού.



Εικόνα 21 Ιδέα εκπαιδευτικού παιχνιδιού σε βήματα

Το παιχνίδι μπορεί να έχει ως κυρίο στόχο την ευαισθητοποίηση του παίκτη δια μέσου μιας ιστορίας και διαφόρων παζλ, όπου ο παίκτης υποδύθεται έναν detective που διεξάγει μια έρευνα για ransomware (που θα μοιάζει με το NotPetya). Κατά την διάρκεια του παιχνιδιού μπορούν να χρησιμοποιηθούν πραγματικές πληροφορίες βασισμένες στο NotPetya ώστε να κατασκευαστεί μια εκπαιδευτική εμπειρία. Οι παίκτες θα κληθούν να χρησιμοποιήσουν κριτική σκέψη για να λύσουν τα παζλ που προσφέρονται και παράλληλα θα αποκτήσουν μια βαθύτερη κατανόηση των υπολογιστικών συστημάτων και των όρων που χρησιμοποιούνται.

Παρόλο που θεωρητικά μοιάζει με ένα εκπαιδευτικό παιχνίδι, θα δώσει μεγαλύτερη ώθηση ώστε οι χρήστες να λάβουν μέτρα για την προστασία του συστήματος τους. Αυτό μπορεί να πραγματοποιηθεί στον τερμάτισμο του παιχνιδιού, όπου θα πετάγεται ένα μήνυμα προεραιτικής εγκατάστασης του vaccine. Αν ο χρήστης δεχτεί τα αρχεία και τα βήματα που αναφέραμε στην αρχή της υποενότητας θα δημιουργούνται αυτόματα μέσω ενός .bat αρχείου.

5.2.3 Συμπεράσματα

Για να κατανοήσουμε τον πυρήνα του NotPetya, πραγματοποιήθηκε εκτεταμένη έρευνα ξεκινώντας από τον προκάτοχο του, τον Petya. Αυτό ήταν απαραίτητο για να κατανοήσουμε τις ομοιότητες και τις διαφορές μεταξύ τους, διότι είναι παρόμοια συμπεριφορικά, αλλά η υλοποίησή τους διαφέρει δραματικά. Με βάση αυτές τις διαφορές, οι αναλυτές ασφαλείας κατάφεραν να συμπεράνουν οριστικά ότι το NotPetya είναι malware. Όχι μόνο αυτό, αλλά και ότι δεν υπάρχει πραγματική λύση για την αποκρυπτογράφηση των σκληρών δίσκων που έχουν κρυπτογραφηθεί. Μέσω αυτού του

ευρήματος, ήταν γνωστό ότι η λύση έπρεπε να αντιμετωπιστεί από μια εντελώς διαφορετική οπτική γωνία.

6 Συμπεράσματα

Μέσα από την έρευνα μου για την παρούσα πτυχιακή, εμπλούτισα το θεωρητικό μου υπόβαθρο σχετικά με την κυβερνοασφάλεια σε συσκευές και δίκτυα IoT, εστιάζοντας στους ορισμούς και τις ωρολογίες που διαμορφώνουν αυτό το πεδίο και παρέχοντας ένα βαθύτερο επίπεδο κατανόησης σχετικά με τις επιθέσεις που απειλούν την κυβερνοασφάλεια, διαμορφώνοντας μια πιο ολοκληρωμένη εικόνα του τομέα.

Έπειτα, μέσω της παρουσίασης εξειδικευμένων προγραμμάτων ανίχνευσης και ανάλυσης επιθέσεων, προστέθηκαν στο γνωστικό μου πεδίο τα απαραίτητα εφόδια για τον αποτελεσματικό έλεγχο ενός δικτύου. Αυτή η επέκταση γνώσεων και δυνατοτήτων θα μου επιτρέψει να αντιλαμβάνομαι και να ανταποκρίνομαι σε πιθανές αδυναμίες και σημεία ευπάθειας, ενισχύοντας την ικανότητά μου να συμβάλλω στη διασφάλιση της ασφάλειας σύγχρονων δικτύων.

Τέλος, με την παρουσίαση πραγματικών παραδειγμάτων επιθέσεων, επισημάνθηκαν αδυναμίες στις συσκευές και τα πρωτόκολλα επικοινωνίας. Τα ευρήματα αυτά υπογραμμίζουν την ανάγκη για στρατηγικές κυβερνοασφάλειας που θα ενισχύσουν την προστασία των συστημάτων IoT. Σκοπός της έρευνας, είναι να προωθήσει την ανάπτυξη πιο ασφαλών και ευέλικτων λύσεων, προκειμένου να διασφαλιστεί η αξιοπιστία και η ασφάλεια στην εποχή της ολοένα αυξανόμενης χρήσης των συσκευών IoT.

Βιβλιογραφία

[1] Farhan, Laith, et al. “A Concise Review on Internet of Things (IoT) -Problems, Challenges and Opportunities.” IEEE Xplore, 1 July 2018, ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8471762.

[2] “Internet of Things.” Wikipedia, Wikimedia Foundation, 16 Mar. 2019, en.wikipedia.org/wiki/Internet_of_Things.

[3] “What Is a Wireless Network?-Wi-Fi Network.” Cisco, www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/wireless-network.html#~introduction.

[4] Wikipedia Contributors. “5G.” Wikipedia, Wikimedia Foundation, 8 June 2019, en.wikipedia.org/wiki/5G.

[5] “Short-Range Device.” Wikipedia, 3 Sept. 2021, en.wikipedia.org/wiki/Short-range_device.

[6] Anna Marton, Safepay Systems. “IoT Malware Attacks up by 37% in the First Half of 2023.” IoTAC, 3 Aug. 2023, iotac.eu/iot-malware-attacks-up-by-37-in-the-first-half-of-2023/. Accessed 6 Dec. 2023.

[7] Shah, Yash, and Shamik Sengupta. “A Survey on Classification of Cyber-Attacks on IoT and IIoT Devices.” 2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), 28 Oct. 2020, https://doi.org/10.1109/uemcon51285.2020.9298138.

[8] “Denial of Service DDoS Attack.” GeeksforGeeks, 13 July 2018, www.geeksforgeeks.org/denial-of-service-ddos-attack/.

[9] Raza, Mudassar, et al. “A Survey of Password Attacks and Comparative Analysis on Methods for Secure Authentication.” World Applied Sciences Journal, vol. 19, no. 4, 2012, pp. 439–444, https://doi.org/10.5829/idosi.wasj.2012.19.04.1837. Accessed 18 Dec. 2023.

[10] “Brute Force: Password Spraying, Sub-Technique T1110.003 - Enterprise | MITRE ATT&CK®.” Attack.mitre.org, attack.mitre.org/techniques/T1110/003/.

[11] “Brute Force: Credential Stuffing, Sub-Technique T1110.004 - Enterprise | MITRE ATT&CK®.” Attack.mitre.org, attack.mitre.org/techniques/T1110/004/.

[12] “123456” Is the Most Common Password in the US in 2023 | Mission Critical Magazine.”www.missioncriticalmagazine.com,www.missioncriticalmagazine.com/articles/94990-123456-is-the-most-common-password-in-the-us-in-2023.Accessed 20 Dec. 2023.

[13] Lyon, Gordon Fyodor. Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning. Nmap Project https://nmap.org/book/toc.html

[14] Wireshark Foundation. “Wireshark.” Wireshark.org, 2016, www.wireshark.org/.

[15] Nmap. “Nmap.” Nmap.org, 2017, nmap.org/.

[16] Snort. “Snort - Network Intrusion Detection & Prevention System.” Snort.org, 2019, www.snort.org/.

[17] Wireshark. “Wireshark User’s Guide.” Wireshark.org, 2019, www.wireshark.org/docs/wsug_html_chunked/.

[18] “Snort 3 Rule Writing Guide - Snort 3 Rule Writing Guide.” Docs.snort.org, docs.snort.org/.

[19] ORACLE. “Oracle vm VirtualBox.” Virtualbox.org, 2023, www.virtualbox.org

[20] Margolis, Joel, et al. “An In-Depth Analysis of the Mirai Botnet.” IEEE Xplore, 1 July 2017, ieeexplore.ieee.org/document/8392610.

[21] Sood, Karan. “NotPetya Ransomware Attack [Technical Analysis].” Crowdstrike.com, 7 June 2018, www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/.

[22] Lika, Reyner Aranta, et al. “NotPetya: Cyber Attack Prevention through Awareness via Gamification.” IEEE Xplore, 1 July 2018, ieeexplore.ieee.org/document/8538431.