ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

«Εργαλεία και διαδικασίες διαχείρισης κυβερνοεπιθέσεων. Συγκριτική αξιολόγηση εμπορικών και ανοιχτού κώδικα λύσεων»

Του φοιτητή
Πουνερίδη Σωκράτη
Αρ. Μητρώου: it154615

Επιβλέπων
Ονοματεπώνυμο Ηλιούδης
Χρήστος

Βαθμίδα Καθηγητής

Ημερομηνία 09/09/2024

Εργαλεία και διαδικασίες διαχείρισης κυβερνοεπιθέσεων: Συγκριτική αξιολόγηση εμπορικών και ανοιχτού κώδικα λύσεων
21335
Ονοματεπώνυμο φοιτητή/τών Σωκράτης Πουνερίδης
Ονοματεπώνυμο εισηγητή Χρήστος Ηλιούδης
Ημερομηνία ανάληψης Δ.Ε. 15/11/2023
Ημερομηνία περάτωσης Δ.Ε. 09/09/2024

Βεβαιώνω ότι είμαι ο συγγραφέας αυτής της εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, έχω καταγράψει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών, εικόνων και κειμένου, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επιπλέον, βεβαιώνω ότι αυτή η εργασία προετοιμάστηκε από εμένα προσωπικά, ειδικά ως πτυχιακή εργασία, στο Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του ΔΙ.ΠΑ.Ε.

Η έγκριση της πτυχιακής εργασίας από το Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του Διεθνούς Πανεπιστημίου της Ελλάδος, δεν υποδηλώνει απαραιτήτως και αποδοχή των απόψεων του συγγραφέα, εκ μέρους του Τμήματος.

Πρόλογος

Η πτυχιακή αυτή, προσφέρει κατανόηση των διάφορων κυβερνοεπιθέσεων σε βάθος. Επίσης, εξετάζονται οι τρόποι αντιμετώπισης αυτών, αλλά και οι μέθοδοι που χρησιμοποιούνται για την επίτευξή τους. Ακόμη, παρέχει μια αντικειμενική ανάλυση των διαθέσιμων εργαλείων και μεθόδων για την αντιμετώπιση των κυβερνοεπιθέσεων. Μέσω της παρουσίασής της, η εργασία παρέχει πολύτιμες πληροφορίες σχετικά με τον τρόπου που μπορούν να εφαρμοστούν οι λύσεις αυτές σε πραγματικές καταστάσεις. Τέλος, δίνει την ευκαιρία στον ερευνητή να αναπτύξει τις ικανότητές του στον τομέα των cyber-attacks και της κυβερνοασφάλειας, κάτι το οποίο είναι σημαντικό, αφού η τελευταία γίνεται όλο και πιο σημαντική στην σύγχρονη εποχή της ψηφιακής τεχνολογίας. Μέσω της εργασίας αυτής, ο φοιτητής θα αποκτήσει βαθύτερη γνώση των προκλήσεων και τον λύσεων που προσφέρονται στον τομέα αυτό, ενισχύοντας έτσι την επαγγελματική του ανάπτυξη.

Περίληψη

Η παρούσα πτυχιακή εργασία, επικεντρώνεται στη διερεύνηση των κυβερνοεπιθέσεων, εστιάζοντας σε ορισμένες από τις πλέον διαδεδομένες όπως το κακόβουλο λογισμικό (Malware), το Phishing, την SQL Injection, τις επιθέσεις Man-in-the-middle, τις Zero-day exploits επιθέσεις, το DNS Tunneling και τις επιθέσεις άρνησης εξυπηρέτησης (Denial of Service attacks). Στην εργασία περιγράφονται οι μέθοδοι που χρησιμοποιούνται για την πραγματοποίηση των επιθέσεων αυτών με λεπτομέρειες και ανάλυση των χαρακτηριστικών και των ιδιαιτεροτήτων τους.

Επίσης, εξετάζονται οι στρατηγικές αντιμετώπισης των παραπάνω απειλών και παρέχονται συγκριτικές αναλύσεις και διαθέσιμα εμπορικά εργαλεία αλλά και λύσεις ανοικτού κώδικα. Στόχος, είναι να διερευνηθούν οι διαφορές και οι

ομοιότητες μεταξύ αυτών των εργαλείων και να αξιολογηθεί η αποτλεσματικότητά τους.

Ακόμη, παρουσιάζονται βέλτιστες πρακτικές αντιμετώπισης των κυβερνοεπιθέσεων υπογραμμίζοντας τα πλεονεκτήματα και τα μειονεκτήματα κάθε τρόπου αντιμετώπισης. Παράλληλα, αναγράφεται η επίδραση των συγκεκριμένων τεχνολογιών στον επιχειρηματικό κόσμο αλλά και η σημασία τους στην προστασία των ψηφιακών περιουσιακών στοιχείων των οργανισμών. Επιπροσθέτως, γίνεται σύγκριση του κόστους αλλά και της ευκολίας της χρήσης και της δυνατότητας της προσαρμογής των παραπάνω πρακτικών σε διαφορετικά περιβάλλοντα.

Στο τελευταίο κεφάλαιο της εργασίας, παρουσιάζονται παραδείγματα επιθέσεων που αφορούν κάθε επίθεση που αναλύθηκε στην πτυχιακή εργασία. Αναλύονται οι τρόποι των επιθέσεων, το λογισμικό που χρησιμοποιήθηκε για τις επιθέσεις, αλλά δίνονται και τα αποτελέσματα των επιθέσεων αυτών. Τέλος, ο αναγνώστης μπορεί να διαβάσει τις επιπτώσεις που είχαν οι επιθέσεις των παραδειγμάτων στον πραγματικό κόσμο και στους χρήστες.

«Cyber Attack Management Tools and Processes:
Benchmarking Commercial and Open Source Solutions»

«Sokratis Pouneridis»

Abstract

This thesis focuses on the investigation of cyberattacks, focusing on some of the most widespread such as Malware, Phishing, SQL Injection, Man-in-the-middle attacks, Zero-day exploit attacks, DNS Tunneling and Denial of Service attacks. The paper describes the methods used to carry out these attacks with details and analysis of their characteristics and peculiarities.

Also, this paper examines the strategies for dealing with the above cyber threads and provide strategic and comparative analyzes, as well as the commercial tools and open-source solutions that are available. The aim is to explore the differences and similarities between these tools and to evaluate their effectiveness.

Furthermore, presents the best practices for dealing with cyberattacks, highlighting the advantages and disadvantages of each approach. At the same time, the effect of specific technologies on the business world is indicated, as well as their importance in protecting the digital assets of organizations. In addition, the paper compares the costs and the ease of use and the possibility of adapting the above practices to different environments.

In the last chapter of the thesis, there are presented examples of each cyberattack. Also, in the paper are analyzed the methods of the attacks, the software used for them and the results of each attack given. Finally, the reader can read the effects that the example attacks had on the real world and the users.

Ευχαριστίες

Θα ήθελα να εκφράσω τις ευχαριστίες μου στον κ. Χρήστο Ηλιούδη, καθηγητή του τμήματος Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του ΔΙΠΑΕ για την καθοδήγηση και την βοήθειά του στην αποπεράτωση αυτής της πτυχιακής εργασίας. Η ανάθεση αυτής, με βοήθησε τόσο στην επαγγελματική όσο και στην προσωπική μου ζωή, προσφέροντάς απαραίτητες για την συνέχεια της επαγγελματικής μου καριέρας γνώσεις. Επίσης, θα ήθελα να ευχαριστήσω από τα βάθη της καρδιάς μου, τους γονείς μου για την ανεκτίμητη υποστήριξή τους τόσο στην ολοκλήρωση των σπουδών μου, όσο και για την στήριξή τους σε όλη τη διάρκεια της επαγγελματικής μου καριέρας. Τέλος, θα ήθελα να ευχαριστήσω την κοπέλα μου Κριστιάνα για την, οχι απαραίτητα τεχνική αλλα γενική υποστήριξη της στην ζωη μου.

Περιεχόμενα

Κεφάλαιο 1ο Εισαγωγή

Η παρούσα πτυχιακή εργασία με τίτλο «Εργαλεία και διαδικασίες διαχείρισης κυβερνοεπιθέσεων: Συγκριτική αξιολόγηση εμπορικών και ανοιχτού κώδικα λύσεων» αναλύει τις διάφορες μορφές κυβερνοεπιθέσεων, όπως Malware, Phishing, Man-in-the-middle, Denial of service, SQL injection, Zero-day exploit και DNS Tunneling, καθώς και τις μεθόδους με τις οποίες επιτυγχάνονται. Η εργασία αναλύει επίσης τους διάφορους τρόπους αντιμετώπισης των επιθέσεων αυτών, χρησιμοποιώντας τόσο εμπορικά όσο και ανοικτού κώδικα εργαλεία.

Το κύριο αντικείμενο της πτυχιακής εργασίας, είναι να διερευνήσει τις διάφορες μορφές των κυβερνοεπιθέσεων που αντιμετωπίζουν οι οργανισμοί σήμερα, καθώς και τους τρόπους αντιμετώπισής τους. Μελετώντας προηγμένες τεχνικές, η εργασία αυτή βοηθάει τον αναγνώστη να κατανοήσει την σημαντικότητα των κυβερνοεπιθέσεων και τη σημασία των ψηφιακών περιουσιακών στοιχείων.

Η εργασία, προσφέρει ένα ολοκληρωμένο πλαίσιο κατανόησης των παραπάνω επιθέσεων και των τρόπων αντιμετώπισής τους. Μέσα από την ανάλυση των cyber-attacks και των αντίστοιχων τεχνολογιών ασφαλείας, οι αναγνώστες θα μπορούν να αποκτήσουν πλήρη εικόνα του τομέα αυτού και να εμπλουτίσουν τις γνώσεις τους σχετικά με την κυβερνο-ασφάλεια. Ακόμη, η σύγκριση μεταξύ εμπορικών λύσεων και λύσεων ανοικτού κώδικα παρέχει μια κατευθυντήρια αρχή για την επιλογή των κατάλληλων εργαλείων και μεθόδων ασφάλειας για κάθε επιχειρηματική περίπτωση.

Τέλος, η εργασία αυτή δείχνει πως μπορούν να εφαρμοστούν οι γνώσεις και οι τεχνικές αντιμετώπισης των κυβερνοεπιθέσεων σε πραγματικές επαγγελματικές καταστάσεις. Με αυτόν τον τρόπο, η πτυχιακή αυτή συμβάλει στην προσωπική και επαγγελματική ανάπτυξη των αναγνωστών, παρέχοντάς τους τα απαραίτητα εφόδια για να αντιμετωπίσουν αποτελεσματικά τις κυβερνοεπιθέσεις στο μέλλον.

1.1 Στόχοι της εργασίας

Στόχος της πτυχιακής εργασία είναι η ανάλυση των διαφόρων ειδών των κυβερνοεπιθέσεων. Η πτυχιακή αποσκοπεί στην κατανόηση των μεθόδων με τις οποίες επιτυγχάνονται οι επιθέσεις που θα αναλυθούν, προσφέροντας παράλληλα βαθιά γνώση και επίγνωση των απειλών που αντιμετωπίζουν οι οργανισμοί στον ψηφιακό κόσμο.

Επιπλέον, μέσω της ανάλυσης των τρόπων αντιμετώπισης των κυβερνοεπιθέσεων, είτε αυτές είναι εμπορικές είτε βασίζονται σε λύσεις με ανοιχτό κώδικα, η εργασία παρέχει μια ολοκληρωμένη εικόνα των

διαθέσιμων επιλογών και μεθόδων για την προστασία των δικτυακών συστημάτων. Μέσα σε αυτό το πλαίσιο, οι στόχοι είναι να αναδειχθούν οι καλύτερες πρακτικές και να διευκολυνθεί η διαδικασία λήψης αποφάσεων για την επιλογή των κατάλληλων εργαλείων και στρατηγικών αντιμετώπισης.

Επιπλέον, η πτυχιακή αυτή εργασία δίνει έμφαση στον τρόπο με τον οποίο επιτυγχάνονται οι κυβερνοεπιθέσεις και πώς μπορούν να αντιμετωπιστούν αποτελεσματικά. Μέσω πρακτικών παραδειγμάτων και αναλύσεων, η εργασία αυτή επιδιώκει να εκπαιδεύσει τους αναγνώστες σε θέματα κυβερνοασφάλειας και να τους παρέχει τα εφόδια για την αντιμετώπιση των κινδύνων από κυβερνοεπιθέσεις.

Τέλος, με την εμβάθυνση στον τομέα της κυβερνοασφάλειας, η εργασία προσφέρει στους ερευνητές και τους επαγγελματίες στον χώρο της πληροφορικής μια ευκαιρία να επεκτείνουν τις γνώσεις τους και να αναπτύξουν τις δεξιότητές τους σε έναν αναπτυσσόμενο και σημαντικό τομέα της τεχνολογίας. Συνολικά, η εργασία αυτή προσφέρει μια ευκαιρία για εκπαιδευτική και επαγγελματική ανάπτυξη στον σημαντικό τομέα της κυβερνοασφάλειας

1.2 Επιτεύγματα

Η παρούσα πτυχιακή εργασία προσφέρει μια εκτενή ανάλυση διάφορων κυβερνοεπιθέσεων. Μέσω της ανάλυσης που γίνεται, γίνονται κατανοητοί οι διάφοροι τρόποι με τους οποίους κάθε κυβερνοεπίθεση εκτελείται αλλά και αντιμετωπίζεται. Η πτυχιακή εργασία επίσης, συγκρίνει τις λύσεις ανοικτού κώδικα και λύσεις που υπάρχουν στο εμπόριο και μπορεί να γίνει κατανοητή η σημαντικότητα της επιλογές κατάλληλης λύσης για φυσικό πρόσωπο ή εταιρία. Γίνεται κατανοητό από την επιστημονική κοινότητα πως οι zero-cost λύσεις αφορούν φυσικά πρόσωπα και πως οι μεγάλες εταιρίες πρέπει να εμπιστευτούν λύσεις που θα βρουν στο εμπόριο. Το παρόν έγγραφο καθιστά σαφές πως οι αρμόδιοι χρήστες θα πρέπει να είναι άμεσα ενημερωμένοι στα νέα λογισμικά αντιμετώπισης κακόβουλων λογισμικών αλλά και στους νέους ιούς που κυκλοφορούν. Γίνεται σημαντική ανάλυση ανάμεσα σε λύσεις ανοικτού κώδικα και σε εμπορικές συγκρίνοντας τα θετικά και τα αρνητικά που παρέχει κάθε λύση. Επίσης, γίνεται εκτενής αναφορά σε διάφορους τρόπους επιθέσεων.

Αναγράφεται η λειτουργία τους αλλά και πιθανοί τρόποι αντιμετώπισής τους με σκοπό την ενημέρωση της επιστημονικής κοινότητας. Η εργασία αυτή μπορεί να βοηθήσει τον αναγνώστη που θέλει να ασχοληθεί με τον τομέα του cybersecurity, τόσο σε προσωπικό όσο και σε επαγγελματικό επίπεδο, αναλύοντάς του τύπους επιθέσεων, δωρεάν ή επί πληρωμή τρόπους αντιμετώπισής τους και τη σημαντικότητα της άμυνα στο περιβάλλον του διαδικτύου.

1.3 Διάρθρωση εργασίας

Ξεκινώντας η παρούσα μελέτη το κεφάλαιο 1 αποτελεί το εισαγωγικό κεφάλαιο της όπου θα βοηθήσει τον αναγνώστη να κατανοήσει το τι θα ακολουθήσει στο σύνολο της. Ακολούθως στο δεύτερο κεφάλαιο γίνεται η κατηγοριοποίηση και η παρουσίαση κάθε μίας ξεχωριστά των κυβερνοεπιθέσεων. Στο κεφάλαιο 3 συγκρίνονται οι κυβερνοεπιθέσεις σχετικά με τον τρόπο επίθεσης τους ενώ στο τέταρτο κεφάλαιο περιγράφονται οι αδυναμίες τους. Στο κεφάλαιο 5 παρουσιάζονται οι τρόποι αντιμετώπισης από κάθε κυβερνοεπίθεση ξεχωριστά και τέλος στο 6^{ο} της μελέτης παραθέτονται παραδείγματα από τις κυβερνοεπιθέσεις.Στο κεφάλαιο 7, συγκρίνονται λύσεις ανοικτού κώδικα και εμπορικές, για κάθε τύπο επίθεσης που αναλύθηκε παραπάνω. Τέλος στο κεφάλαιο 8 αναγράφονται συμπεράσματα και μελλοντικές επεκτάσεις σχετικά με τις κυβερνοεπιθέσεις και τους τρόπους αντιμετώπισής τους, αλλά και τις δωρεάν ή επί πληρωμή λύσεις τους.

Κεφάλαιο 2ο Κατηγοριοποίηση των Cyber-attacks

2.1 Επιθέσεις Malware

2.1.1 Εισαγωγή

Το malware (κακόβουλο λογισμικό), αποτελεί μια μορφή επίθεσης που σχεδιάζεται για να προκαλέσει διαταραχή ή ζημιά σε υπολογιστές, διακομιστές ή και δίκτυα υπολογιστών. Το κακόβουλο αυτό λογισμικό, μπορεί να επιτίθεται με πολλούς τρόπους συμπεριλαμβανομένης της διάδοσης μέσω κακόβουλων ιστότοπων, κακόβουλων email, η μπορούν να εκμεταλλευτούν ευπάθειες στο λογισμικό και το λειτουργικό σύστημα ενός υπολογιστή. Αφότου εισβάλει, το malware μπορεί να προκαλέσει διάφορες επιβλαβείς ενέργειες, όπως μη πρόσβαση σε πληροφορίες, κλοπή προσωπικών δεδομένων, ακόμη και εγκατάσταση κρυφής πύλης σε έναν υπολογιστή ή δίκτυο για μελλοντική πρόσβαση εισβολέα.

Η αντιμετώπιση του malware απαιτεί λήψη κατάλληλων μέτρων ασφάλειας, όπως η χρήση λογισμικού, η εφαρμογή antivirus και η εκπαίδευση των χρηστών για την αναγνώριση και αποφυγή κακόβουλων αρχείων και email. Τα περισσότερα κακόβουλα λογισμικά αναπτύσσονται από cyber criminals που στοχεύουν να κερδίσουν προσωπικά ή οικονομικά οφέλη, μετατρέποντας την αντιμετώπισή τους σε προτεραιότητα για την κυβέρνηση, τους επιχειρηματίες και τους ιδιώτες. Ο αριθμός των παραλλαγών των κακόβουλων λογισμικών αυξάνεται συνεχώς, δημιουργώντας μια σοβαρή απειλή για την ασφάλεια του διαδικτύου και των χρηστών του. Η πρόληψη και η αντιμετώπιση αυτών των λογισμικών, απαιτούν συνεχείς προσπάθειες από την πλευρά των χρηστών και των ειδικών στον τομέα των cyber-attacks. [16]

2.1.2 Ιστορία επιθέσεων malware

Ο Τζον φον Νόιμαν, είχε διατυπώσει την ιδές ότι ένα πρόγραμμα μπορεί να αναπαραχθεί, προσδίδοντας έτσι αληθοφάνεια στη θεωρία. Ο

Φρεντ Κόεν, με περισσότερα πειράματα επιβεβαίωσε την διατύπωση του φον Νόιμαν εξερευνώντας τις ιδιότητες του κακόβουλου λογισμικού όπως self-replication και το detection μέσω κρυπτογραφίας.

Οι ιοί των υπολογιστών, αρχικά εξαπλώνονται μέσω εκτελέσιμων προγραμμάτων ή μέσω cd και δισκετών σε υπολογιστές. Με την είσοδό τους στα προγράμματα αυτά, προκαλούσαν οι ιοί εκτελούνταν με κάθε εκτέλεση των προγραμμάτων. Αυτή η μέθοδος εξάπλωσης έγινε πιο δημοφιλής με την εμφάνιση του IBM PC και του MS-DOS. Τα πρώτα πειράματα στον χώρο των ιών, στράφηκαν στους προσωπικούς υπολογιστές Apple II και Macintosh, ενώ αργότερα επηρέασαν ευρύτερα τα συστήματα της Microsoft. Με την εισαγωγή των macros (μικρά κομμάτια κώδικα που χρησιμοποιούνται για την αυτοματοποίηση καθηκόντων και ενεργειών) σε εφαρμογές όπως το Word, έγινε δυνατή η δημιουργία ύπουλων ιών που μολύνουν έγγραφα, εκμεταλλευόμενοι την εκτέλεση macros ως μορφή εκτελέσιμου κώδικα.

Η διάδοση των ιών και των σκουληκιών (worms) στο διαδίκτυο, αλλάζει τον τρόπο επιθέσεων. Σκουλήκια όπως το Internet Worm του 1998 δεν απαιτούσαν εισαγωγή σε άλλα προγράμματα αλλά εκμεταλλευόταν κενά ασφαλείας σε προγράμματα δικτύου για να εξαπλωθούν. Η εξάπλωση του κακόβουλου λογισμικού μέσω email έχει επίσης γίνει συνήθης, με αναφορές που δείχνουν ότι το 92% των κακόβουλων λογισμικών, παραδίδεται μέσω email.

Τα σύγχρονα κακόβουλα λογισμικά προγράμματα, χρησιμοποιούνται για διαφορετικούς σκοπούς, συμπεριλαμβανομένης και της κλοπής προσωπικών δεδομένων ή οικονομικών πληροφοριών. Με την αύξηση της ψηφιακής σύνδεσης, οποιαδήποτε συσκευή συνδεθεί σε θύρα USB μπορεί να μολυνθεί με κακόβουλο λογισμικό, ανεξαρτήτων της λειτουργίας της. Αυτό επιτυγχάνεται είτε μέσω εκμετάλλευσης των ευπαθειών του λογισμικού, είτε μέσω προσθήκης κακόβουλου λογισμικού κώδικα κατά την κατασκευή της συσκευής. Μέσω ερευνητών, έχει παρατηρηθεί τριπλάσια αύξηση του κακόβουλου λογισμικού που διανέμεται μέσω USB κατά το

πρώτο εξάμηνο του 2023. (33)

2.2 Phishing

2.2.1 Εισαγωγή

Το ηλεκτρονικό ψάρεμα “Phishing” είναι μια δράση που αποσκοπεί στην εξαπάτηση των χρηστών του διαδικτύου, με τον 'θύτη' να προσποιείται ότι είναι μια αξιόπιστη οντότητα. Αυτό συμβαίνει επειδή οι χρήστες είναι ευάλωτοι λόγω της έλλειψης αποτελεσματικής προστασίας από ηλεκτρονικά εργαλεία και της έλλειψης ενημέρωσης. Σκοπός του είναι η παράνομη απόκτηση προσωπικών δεδομένων, όπως ευαίσθητες πληροφορίες και κωδικοί πρόσβασης.

Η ονομασία "ηλεκτρονικό ψάρεμα" αντανακλά την ουσία του φαινομένου, καθώς απορρέει από την αγγλική λέξη "fishing" (ψάρεμα). Στη διαδικασία αυτή, ο 'ψαράς' (ο θύτης) παριστάνει μια αξιόπιστη οντότητα με σκοπό να προσελκύσει τα θύματά του, η οποία είναι παρόμοια με τον τρόπο που ένα ψάρι τραβάει την προσοχή του δολώματος. Μια άλλη εξήγηση για τον όρο πηγάζει από τον κωδικό HTML "<><" που χρησιμοποιούνταν σε chat rooms και μοιάζει με ένα ψάρι, είναι δηλαδή δύσκολο να ανιχνευθεί. Η αλλαγή του "f" σε "ph" στον όρο "phishing" μπορεί να είναι τυχαία ή να έχει σχέση με τον παλαιότερο όρο "phreaking" ή "phone freaking", που αναφέρεται στην ανεξουσιοδότητη χρήση τηλεφωνικών δικτύων.

Το phishing, όπως αναφέρθηκε προηγουμένως, ξεκίνησε πριν αρκετό καιρό, όταν οι hackers επιτέθηκαν στα τηλεφωνικά δίκτυα μέσω της πρακτικής που ονομάζεται phone phreaking. Αυτό συνίστατο στο να επεμβαίνουν στις γραμμές και να αποκτούν πληροφορίες από προσωπικές συνομιλίες. Στο διαδίκτυο, η πρακτική αυτή εμφανίστηκε το 1995 μέσω του ηλεκτρονικού ταχυδρομείου και αργότερα μέσω των άμεσων μηνυμάτων. Ένας χάκερ αποστέλλει ένα ηλεκτρονικό ταχυδρομείο ή μήνυμα στο

"θύμα", παριστάνοντας ένα αξιόπιστο άτομο που συνήθως ανήκει σε μια εταιρία ή υπηρεσία και ζητά προσωπικές πληροφορίες.

Ένα βασικό εργαλείο αυτής της επίθεσης είναι οι παραπλανητικοί σύνδεσμοι, οι οποίοι οδηγούν τον χρήστη σε διαφορετική ιστοσελίδα από αυτή που αναφέρεται. Αυτό είναι κάτι κρίσιμο, αλλά εύκολο να υλοποιηθεί, καθώς μπορεί να γίνει με απλή αλλαγή στον κώδικα HTML. Οι ψεύτικες ιστοσελίδες είναι μια άλλη μορφή phishing, καθώς μέσω παραπλανητικών συνδέσμων προκαλούν τους χρήστες να μπουν σε σελίδες που φαίνονται πανομοιότυπες με αυθεντικές ιστοσελίδες, αλλά ανήκουν στον server του hacker.

Το phishing μπορεί να γίνει ακόμα πιο επικίνδυνο με τη χρήση πιο προηγμένων μεθόδων που είναι δυσκολότερες στην ανίχνευση. Μία από αυτές είναι το IDN spoofing, όπου οι παραπλανητικοί σύνδεσμοι μπορούν να οδηγήσουν σε διαφορετικές ιστοσελίδες λόγω απάτης στη χρήση διεθνών ονομάτων τομέων. Επίσης, οι hackers μπορούν να αποφεύγουν τα αντι-phishing προγράμματα ή να καλύπτουν τα ίχνη τους με χρήση φίλτρων όπως εικόνες ή Flash Player. Άλλες τεχνικές περιλαμβάνουν τη χρήση αναδυόμενων παραθύρων ή τη δημιουργία ψεύτικων δικτύων σε δημόσιους χώρους όπως αεροδρόμια, ξενοδοχεία και καφετέριες. [24] [57]

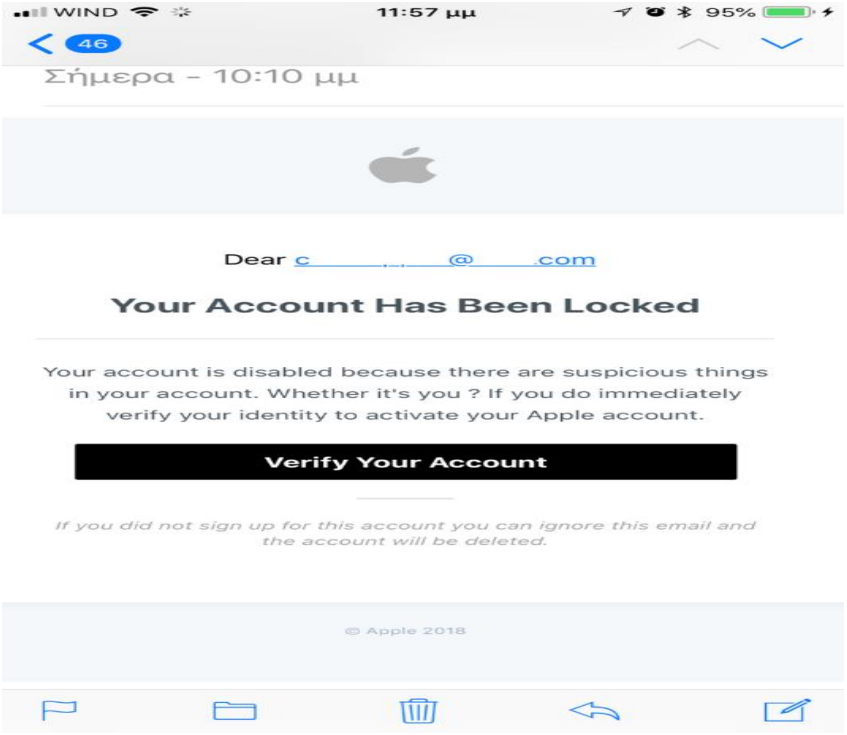

Figure 1: Phishing attack example (Wikipedia.org)

2.2.2 Ιστορία επιθέσεων Phishing

Η τεχνική του Phishing ξεκίνησε να επικρατεί από το 1987, όμως έγινε ευρέως γνωστή το 1995 μέσω επιθέσεων στην AOL. Οι επιτιθέμενοι, γνωρίζοντας την εμπιστοσύνη των χρηστών προς την εταιρία, παρίσταναν τους εργαζομένους της AOL και ζητούσαν προσωπικές πληροφορίες. Με τον καιρό, η επιθετική αυτή τεχνική εξελίχθηκε, και με την είσοδο εργαλείων όπως το AOHell, έγινε πιο εύκολη και αποτελεσματική.

Οι μεγάλες εταιρίες, όπως η Google, βρέθηκαν στόχος αναβαθμισμένων μορφών Phishing, και χώρες όπως η Κίνα κατηγορήθηκαν για επιθέσεις στη βάση δεδομένων τους. Αυτές οι επιθέσεις στόχευαν σε επιλεγμένα πρόσωπα ή οργανισμούς, με στόχο την κλοπή ευαίσθητων πληροφοριών. Σήμερα, το Phishing παραμένει μία από τις κυρίαρχες κινδύνους στον κυβερνοχώρο, με επιθέσεις να αυξάνονται κάθε χρόνο. Τόσο μικρές όσο και μεγάλες επιχειρήσεις αντιμετωπίζουν αυξημένο κίνδυνο, με

τις διαρροές δεδομένων να αποτελούν τον κύριο αντίκτυπο των επιθέσεων Phishing. Πολλές εταιρίες προτιμούν να μη δημοσιοποιούν επιθέσεις που δέχονται, προκειμένου να αποφύγουν την αναφορά στη δημοσιότητα. Οι έρευνες σχετικά με το Phishing δείχνουν μία σταθερή αύξηση των επιθέσεων και την δύναμη που έχει αυτή η τεχνική στον κυβερνοχώρο. Οι εταιρίες και οι οργανισμοί καλούνται να ενισχύσουν τις προστατευτικές τους μετρήσεις προκειμένου να αντιμετωπίσουν αυτήν την αυξανόμενη απειλή. [57]

2.3 Man-in-the-middle attack

2.3.1 Εισαγωγή

Η επίθεση "Man-in-the-middle" αποτελεί μια διαδεδομένη παραβίαση της ασφάλειας, όπου ένας επιτιθέμενος εισάγεται ανάμεσα σε δύο επικοινωνούντες που είναι αρχικά αξιόπιστοι συνομιλητές. Με αυτόν τον τρόπο, ο κακόβουλος ελέγχει και παρεμβαίνει στη ροή της επικοινωνίας, έχοντας τη δυνατότητα να παρακολουθεί, να αλλοιώνει ή ακόμα και να κλέβει πληροφορίες που ανταλλάσσονται μεταξύ των πρωταρχικών συνομιλητών. Τέτοιες επιθέσεις είναι ιδιαίτερα ανησυχητικές όταν εφαρμόζονται στο πρωτόκολλο Diffie-Hellman, ειδικά όταν η ανταλλαγή κλειδιών γίνεται χωρίς να υπάρχει επαλήθευση ταυτότητας. [23]

Figure 2: Man-in-the-middle attack (Wikipedia.org)

2.3.2 Ιστορία επιθέσεων Man-in-the-middle

Ο Γουλιέλμος Μαρκόνι (1874-1937) είναι ένας νομπελίστας του οποίου η κληρονομιά των εφευρέσεών του περιλαμβάνει την πρώιμη εργασία στη μετάδοση του ραδιοφώνου, τους ασύρματους τηλέγραφους και τον νόμο του Μαρκόνι. Μπορούμε να τον χαρακτηρίσουμε ως έναν πρωτοπόρο καινοτόμο σε ό,τι αφορά τα ασύρματα δίκτυα.

Οι κόμβοι σε ένα ασύρματο δίκτυο - τότε και τώρα - περιλαμβάνουν τον πομπό και τον δέκτη (ή και τους δύο). Τα μηνύματα που μεταφέρονται από τον πομπό στον δέκτη συνήθως προορίζονται μόνο για τον δέκτη και κανέναν άλλο.

Τι συμβαίνει, όμως, όταν ένας πομπός σε ένα ασύρματο δίκτυο, στέλνει ένα μήνυμα και ο δέκτης το λαμβάνει; Μπορεί ο δέκτης να εμπιστευτεί ότι προέρχεται από τον πομπό που περίμενε; Ίσως. Στην περίπτωση του Μαρκόνι και της εταιρείας του, ένας ειδικός σύμβουλος της εταιρείας έγινε "θύμα" της πιθανότατα πρώτης επίθεσης Man-in-the-Middle στην ιστορία. Σύμφωνα με τον μύθο, ο καθηγητής Φλέμινγκ (ένας κορυφαίος σύμβουλος του Μαρκόνι) έδειχνε την καινοτόμο ικανότητα να μεταδίδει ασύρματα ένα μήνυμα από ένα σημείο σε ένα άλλο. Και ο πομπός και ο δέκτης ήταν προετοιμασμένοι και έτοιμοι για την επίδειξη.

Ωστόσο, και ο "άνθρωπος στη μέση", ο κ. Μάσκελιν, ήταν έτοιμος. Ο κ. Μάσκελιν διέταξε τον δικό του δέκτη, παρακάμπτοντας το αυθεντικό μήνυμα που αποστέλλονταν από μια τοποθεσία στην Κορνουάλη προς έναν προορισμό (δέκτη) στο Βασιλικό Ινστιτούτο. Στη συνέχεια, ο κ. Μάσκελιν, χρησιμοποιώντας τον δικό του δέκτη, μετέδωσε ένα νέο/αναθεωρημένο μήνυμα (πιθανότατα ένα ειρωνικό, αν και δεν υπάρχει ακριβής καταγραφή των περιεχομένων του μηνύματος).

Ο καθηγητής Φλέμινγκ δεν ήταν και τόσο ενθουσιασμένος για το γεγονός ότι μια δημοφιλής επίδειξη τεχνολογίας ασύρματης επικοινωνίας κατέληξε σε ένα ανεπιθύμητο μήνυμα από ένα "άνθρωπο στη μέση". Αυτός

ο πρώτος γνωστός πειραματισμός της ασφάλειας σε ένα ασύρματο περιβάλλον προειδοποίησε για τις πιθανές ευπάθειες των νέων ασύρματων τεχνολογιών.

Αυτό το περιστατικό παρακίνησε επίσης σημαντικές συζητήσεις για το πώς να αντιμετωπίσουν οι επικοινωνίες ασύρματης τεχνολογίας πιθανές απειλές ασφαλείας. Η αντίδραση της επίθεσης "άνθρωπος στη μέση" αποτέλεσε μια αρχική αλλά σημαντική προσπάθεια για τη βελτίωση της ασφάλειας των ασύρματων δικτύων, ενώ επίσης αναδείχθηκε η ανάγκη για αυθεντικοποίηση της επικοινωνίας προκειμένου να αντιμετωπιστούν τέτοιου είδους επιθέσεις στο μέλλον. Αυτό το παράδειγμα αποτελεί έναν ισχυρό υπενθύμιση για το πόσο σημαντικό είναι να εξετάζουμε τις ασφάλειας σε όλες τις πτυχές της τεχνολογίας, ακόμα και σε πρωτοποριακές καινοτομίες όπως την ασύρματη επικοινωνία. Καθώς η τεχνολογία συνεχίζει να εξελίσσεται, η ασφάλεια πρέπει να παραμένει στο επίκεντρο των προσπαθειών μας, προκειμένου να προστατεύσουμε τις επικοινωνίες και τα δεδομένα μας από πιθανές απειλές και επιθέσεις. [32]

2.4 Denial-of-service attack

2.4.1 Εισαγωγή

Οι επιθέσεις άρνησης εξυπηρέτησης (Denial-of-service attack, DoS attack) αναφέρονται στις επιθέσεις που έχουν ως στόχο να απενεργοποιήσουν έναν υπολογιστή ή ένα δίκτυο, καθιστώντας το μη προσβάσιμο για τους αρχικούς χρήστες του. Οι επιθέσεις αυτές επιτυγχάνονται με το να υπερχειλίζουν τον στόχο με κίνηση δεδομένων ή να του στέλνουν πληροφορίες που προκαλούν κολλήματα. Σε κάθε περίπτωση, η επίθεση DoS στερεί από τους νόμιμους χρήστες (δηλαδή υπαλλήλους, μέλη ή κατόχους λογαριασμών) υπηρεσίες ή τους πόρους.

Τα θύματα των επιθέσεων DoS συχνά είναι οι ιστοσελίδες υψηλού προφίλ, όπως τράπεζες, εταιρίες εμπορίου και μέσα ενημέρωσης, ή

κυβερνητικές και εμπορικές οργανώσεις. Αν και οι επιθέσεις DoS συνήθως δεν οδηγούν στην κλοπή ή απώλεια σημαντικών πληροφοριών ή πόρων, μπορούν να κοστίσουν στο θύμα πολύ χρόνο και χρήματα για να τις αντιμετωπίσει. [18]

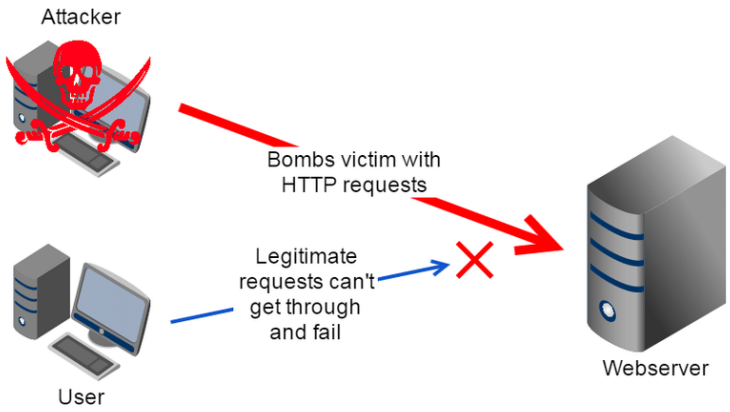

Figure 3: Simulation of DDoS attack (youtube.com)

2.4.2 Ιστορία επιθέσεων Denial-of-service

Τον Σεπτέμβριο του 1996, η Panix, η τρίτη παλαιότερη πάροχος υπηρεσιών Internet στον κόσμο, έγινε στόχος μιας πιθανώς πρώτης επίθεσης DoS. Η επίθεση SYN flood, που δέχθηκε την ημέρα αυτή, οδήγησε στην διακοπή των υπηρεσιών της για αρκετές ημέρες, ενώ οι προμηθευτές της, κυρίως η Cisco, εργάστηκαν για να βρουν μια κατάλληλη αμυντική λύση.

Ένα άλλο παράδειγμα επίθεσης DoS έγινε το 1997 από τον Khan C. Smith κατά τη διάρκεια ενός γεγονότος DEF CON, με αποτέλεσμα να διακοπεί η πρόσβαση στο Internet για πάνω από μια ώρα, στο Las Vegas Strip. Η δημοσίευση κώδικα κατά τη διάρκεια της επίθεσης, οδήγησε στην ηλεκτρονική επίθεση της Sprint, της EarthLink, της E-Trade και άλλων μεγάλων εταιρειών το ακόλουθο έτος.

Το μεγαλύτερο DDoS attack ως τώρα σημειώθηκε το Σεπτέμβριο του

2017, όταν η Google Cloud δέχθηκε μια επίθεση με όγκο 2,54 Tb/s. Τον Φεβρουάριο του 2020, η Amazon Web Services βρέθηκε αντιμέτωπη με μια επίθεση με όγκο 2,3 Tb/s. Τον Φεβρουάριο του 2023, η Cloudflare αντιμετώπισε μια επίθεση με 71 εκατομμύρια requests ανά δευτερόλεπτο, που ισχυρίζεται ότι ήταν η μεγαλύτερη επίθεση HTTP DDoS μέχρι εκείνη τη στιγμή.

Στις 10 Ιουλίου 2023, μια ομάδα hacker επιτέθηκε στην ιστοσελίδα fanfiction Archive of Our Own (AO3). Τον Αύγουστο του 2023, η ομάδα hacktivists *NoName057* στόχευσε σε αρκετά ιταλικά χρηματοπιστωτικά ιδρύματα, μέσω επιθέσεων DoS. Τον Οκτώβριο του 2023, η εκμετάλλευση μιας νέας ευπάθειας στο πρωτόκολλο HTTP/2 οδήγησε στην καταγραφή της μεγαλύτερης επίθεσης HTTP DDoS, με requests που έφθαναν τα 398 εκατομμύρια ανά δευτερόλεπτο, όπως παρατηρήθηκε από τη Google.

2.5 SQL Injection

2.5.1 Εισαγωγή

Η ενσωμάτωση SQL (SQL injection - SQLi) αποτελεί μια σοβαρή ευπάθεια ασφάλειας στον κόσμο του ιστού. Συμβαίνει όταν κακόβουλοι χρήστες εκμεταλλεύονται τη δομή των requests που μια εφαρμογή καταχωρεί στη βάση δεδομένων της. Αυτό επιτρέπει σε αυτούς τους επιτιθέμενους να αποκτήσουν πρόσβαση σε πληροφορίες που δεν θα έπρεπε να έχουν, όπως δεδομένα άλλων χρηστών ή ευαίσθητες πληροφορίες που ανήκουν στην εφαρμογή. Μπορεί να οδηγήσει σε παραβιάσεις της ασφάλειας, όπου οι επιτιθέμενοι μπορούν να τροποποιήσουν ή να διαγράψουν δεδομένα, μεταβάλλοντας έτσι τη συμπεριφορά ή το περιεχόμενο της εφαρμογής.

Ως εκ τούτου, η SQL injection δεν επηρεάζει μόνο την ασφάλεια της εφαρμογής, αλλά μπορεί επίσης να θέσει σε κίνδυνο ολόκληρο τον διακομιστή ή την υποδομή στην οποία βασίζεται η εφαρμογή. Αν οι επιτιθέμενοι καταφέρουν να προχωρήσουν, μπορεί ακόμα να προκαλέσουν

προβλήματα στη διαθεσιμότητα της υπηρεσίας, καθώς επίσης μπορούν να προκαλέσουν την αποτυχία του διακομιστή. Επομένως, είναι ζωτικής σημασίας για τους διαχειριστές συστημάτων και τους προγραμματιστές να λάβουν μέτρα προστασίας για να αποτρέψουν αυτού του είδους τις επιθέσεις.

Η επιτυχής επίθεση SQL injection μπορεί να έχει ως αποτέλεσμα την μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητα δεδομένα, όπως:

- Κωδικοί πρόσβασης.
- Στοιχεία πιστωτικών καρτών.
- Προσωπικές πληροφορίες χρηστών.

Οι επιθέσεις SQL injection έχουν χρησιμοποιηθεί σε πολλές διαρροές δεδομένων (data leaks) υψηλού προφίλ κατά τα χρόνια. Αυτές οι διαρροές έχουν προκαλέσει φθορά στη φήμη και πρόστιμα. Σε ορισμένες περιπτώσεις, ένας επιτιθέμενος μπορεί να αποκτήσει μια μόνιμη πίσω πόρτα στα συστήματα μιας οργάνωσης, οδηγώντας σε μακροχρόνιο συμβιβασμό που μπορεί να παραμείνει απαρατήρητος για μεγάλο χρονικό διάστημα. Στόχοι τέτοιων επιθέσεων είναι εταιρίες όπως η Yahoo, Zappos, Equifax, TalkTalk, LinkedIn και η Sony Pictures. Όλες οι παραπάνω επωνυμίες έχουν γίνει hacked από cybercriminals που χρησιμοποίησαν SQL injections. [17]

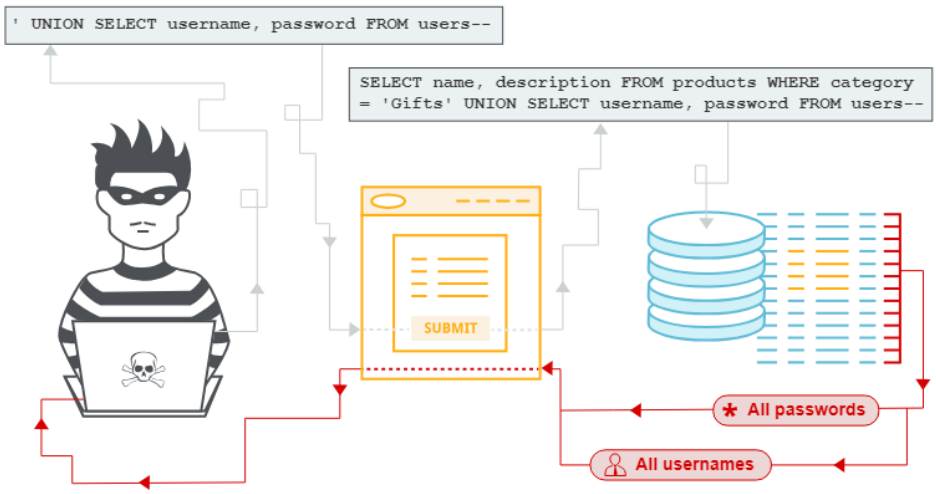

Figure 4: SQL Injection example (portswigger.net)

2.5.2 Ιστορία επιθέσεων SQL injection

Η πρώτη επίθεση SQL injection καταγράφηκε για πρώτη φορά το 1998 από τον ερευνητή και hacker Jeff Forristal. Τα ευρήματά του δημοσιεύτηκαν στο περιοδικό hacker, με όνομα Phrack. Χρησιμοποιώντας το ψευδώνυμο Rain Forest Puppy, ο Forristal εξήγησε πώς κάποιος με βασικές δεξιότητες προγραμματισμού μπορούσε να εισάγει μη εξουσιοδοτημένες εντολές SQL σε νόμιμες εντολές SQL και να ανακτήσει ευαίσθητες πληροφορίες από τη βάση δεδομένων ενός μη ασφαλούς ισότοπου.

Όταν ο Forristal ενημέρωσε τη Microsoft για το πώς η ευπάθεια επηρέαζε το δημοφιλές προϊόν SQL Server της εταιρείας, αυτοί δεν τον είδαν ως πρόβλημα. Όπως το διατύπωσε ο ίδιος ο Forristal: "*Σύμφωνα με αυτούς [τη Microsoft], αυτό που πρόκειται να διαβάσετε δεν είναι πρόβλημα, οπότε μην ανησυχείτε για να κάνετε κάτι για να το σταματήσετε*."

Αυτό που καθιστά την ανεπαρκή αντίδραση της Microsoft τόσο σοκαριστική είναι ότι πολλοί τομείς και θεσμοί εξαρτώνταν (τότε και τώρα) σοβαρά από την τεχνολογία διαχείρισης βάσεων δεδομένων της εταιρείας για να διατηρήσουν τη λειτουργία των λειτουργιών τους, συμπεριλαμβανομένων του λιανικού εμπορίου, της εκπαίδευσης, της υγείας, της τράπεζας και των ανθρωπίνων πόρων. Αυτό μας οδηγεί στο επόμενο γεγονός στο χρονοδιάγραμμα της ιστορίας του SQLI - την πρώτη μείζονα επίθεση SQLI.

Το 2007, η μεγαλύτερη αλυσίδα καταστημάτων ψιλικών στις Ηνωμένες Πολιτείες, η 7-Eleven, έπεσε θύμα μιας επίθεσης SQLI. Οι ρωσικοί hackers χρησιμοποίησαν επιθέσεις SQL injection για να χακάρουν τον ιστότοπο της 7-Eleven και να χρησιμοποιήσουν αυτόν ως πηγή στοιχείων στη βάση δεδομένων πελατών του καταστήματος. Αυτό επέτρεψε στους hackers να αναλάβουν μετά την επιστροφή στη Ρωσία. Συνολικά, οι ύποπτοι αποσπούσαν δύο εκατομμύρια δολάρια, όπως ανέφερε το περιοδικό Wired.

Δεν είναι όλες οι επιθέσεις SQLI κινητοποιημένες από τον πλούτο. Σε ένα άλλο σημαντικό παράδειγμα από το 2007, κυβερνο-εγκληματίες χρησιμοποίησαν SQLI για να κερδίσουν διαχειριστικό έλεγχο σε δύο ιστότοπους που σχετίζονταν με τον Αμερικανικό Στρατό και να ανακατευθύνουν τους επισκέπτες σε ιστότοπους με προπαγανδιστικό περιεχόμενο εναντίον των ΗΠΑ και του Ισραήλ.

Η παραβίαση δεδομένων του MySpace το 2008 κατατάσσεται ως μία από τις μεγαλύτερες επιθέσεις σε ιστότοπο καταναλωτών. Οι κυβερνο-εγκληματίες έκλεψαν emails, ονόματα και μερικούς κωδικούς πρόσβασης από σχεδόν 360 εκατομμύρια λογαριασμούς. Και αυτό είναι γιατί δεν επαναχρησιμοποιούμε κωδικούς πρόσβασης από έναν ιστότοπο στον άλλο.

Ο τίτλος για την πιο απαράδεκτη έλλειψη ασφάλειας ανήκει στην Equifax. Η παραβίαση δεδομένων της Equifax το 2017 παρήγαγε πολύ προσωπικές πληροφορίες (δηλαδή ονόματα, αριθμούς κοινωνικής ασφάλισης, ημερομηνίες γέννησης και διευθύνσεις) για 143 εκατομμύρια καταναλωτές. Για μια οργάνωση που λειτουργεί ως οι φύλακες των πληροφοριών για κάθε Αμερικανό, εκτός από εκείνους που ζουν εκτός πλέγματος, θα περίμενε κανείς ότι θα λάμβαναν μέτρα προφύλαξης ενάντια σε μια βασική επίθεση SQLI. Πριν συμβεί η παραβίαση δεδομένων, μια εταιρεία έρευνας στον κυβερνοχώρο είχε προειδοποιήσει την Equifax ότι ήταν ευάλωτη σε μια επίθεση SQLI, αλλά η πιστωτική εταιρεία δεν προέβη σε καμία δράση μέχρι να ήταν πολύ αργά.

Σε ένα από τα πιο ανατριχιαστικά hacking στην ιστορία, μια επίθεση SQLI το 2015 κατά της κατασκευάστριας παιχνιδιών Vtech, οδήγησε σε παραβίαση σχεδόν πέντε εκατομμυρίων γονέων και 200.000 παιδιών. Ο hacker που ευθύνεται δήλωσε στο Motherboard, την πολυμεσική διαδικτυακή δημοσίευση, ότι δεν είχε σχέδια για τα δεδομένα και δεν δημοσίευσε τα δεδομένα πουθενά online. Αντίθετα, ο hacker εξήγησε επίσης ότι τα δεδομένα ήταν πολύ εύκολο να κλαπούν και πως κάποιος άλλος θα μπορούσε να τα έχει πάρει πρώτα. Κρύο παρηγοριά πράγματι.

Μετακινούμαστε στο παρόν, η επίθεση SQLI εξακολουθεί να είναι μια πραγματικότητα. Κάθε τρία χρόνια, το Open Web Application Security Project (OWASP) κατατάσσει τις *10 Πιο Κρίσιμες Κινδύνους Ασφάλειας Ιστοσελίδων*. Στην πιο πρόσφατη έκδοση του 2017, η επίθεση SQLI κατατάσσεται στην πρώτη θέση.

Πέρα από τη μακροχρόνια διάρκεια της επίθεσης SQLI, το ενδιαφέρον είναι ότι οι επιθέσεις SQLI δεν έχουν αλλάξει ή εξελιχθεί με κανέναν τρόπο. Οι επιθέσεις SQLI λειτουργούν και θα συνεχίσουν να λειτουργούν μέχρις ότου οι άνθρωποι αλλάξουν τις απόψεις τους για την κυβερνοασφάλεια.

2.6 Zero-day exploit

2.6.1 Εισαγωγή

"Μηδενική ημέρα" (Zero-day) είναι ένας ευρύς όρος που περιγράφει πρόσφατες ανακαλύψεις ευπαθειών ασφαλείας που οι hacker μπορούν να χρησιμοποιήσουν για να επιτεθούν σε συστήματα. Ο όρος "μηδενική ημέρα" αναφέρεται στο γεγονός ότι ο vendor ή ο προγραμματιστής μόλις έχει μάθει το ¨ ελάττωμα ¨ - πράγμα που σημαίνει ότι έχουν "μηδενικές ημέρες" για να το διορθώσουν. Μια επίθεση zero-day λαμβάνει χώρα όταν οι hacker εκμεταλλεύονται το ελάττωμα πριν οι προγραμματιστές έχουν την ευκαιρία να το διορθώσουν.

Η επίθεση zero-day, γράφεται μερικές φορές ως 0-day. Οι λέξεις *ευπάθεια (vulnerability), εκμετάλλευση (exploit)* και *επίθεση (attack)* χρησιμοποιούνται συνήθως δίπλα στη μηδενική ημέρα, και είναι χρήσιμο να κατανοήσετε τη διαφορά:

Μια zero-day vulnerability είναι μια ευπάθεια λογισμικού που ανακαλύπτεται από τους επιτιθέμενους πριν ο vendor το γνωρίζει. Επειδή οι vendors δεν έχουν γνώση, δεν υπάρχει παράθυρο ασφαλείας για τις ευπάθειες μηδενικής ημέρας (zero-day vulnerabilities), κάτι που καθιστά τις επιθέσεις πιθανό να επιτύχουν.

Μια zero-day exploit είναι ο τρόπος που οι hacker επιτίθενται σε συστήματα με μια προηγουμένως αναγνωρισμένη ευπάθεια.

Μια zero-day attack είναι η χρήση μιας μηδενικής ημέρας εκμετάλλευση για να προκαλέσει ζημιά ή να κλέψει δεδομένα από ένα σύστημα που επηρεάζεται από μια ευπάθεια.

Το λογισμικό συχνά έχει ευπάθειες ασφαλείας που οι hacker μπορούν να εκμεταλλευτούν για να προκαλέσουν χάος. Οι προγραμματιστές λογισμικού πάντα ψάχνουν για ευπάθειες προς "επιδιόρθωση", δηλαδή να αναπτύξουν μια λύση που θα γίνει release σε μια νέα ενημέρωση.

Ωστόσο, μερικές φορές οι hackers ή κακόβουλοι δράστες παρατηρούν την ευπάθεια πριν το κάνουν οι προγραμματιστές του λογισμικού. Ενώ η ευπάθεια είναι ακόμα ανοιχτή, οι επιτιθέμενοι μπορούν να γράψουν και να υλοποιήσουν έναν κώδικα για να το εκμεταλλευτούν. Αυτό είναι γνωστό ως κώδικας εκμετάλλευσης (exploit code).

Ο κώδικας εκμετάλλευσης μπορεί να οδηγήσει σε θύματα τους χρήστες του λογισμικού, για παράδειγμα, μέσω κλοπής ταυτότητας ή άλλων μορφών cybercrime. Μόλις οι επιτιθέμενοι εντοπίσουν μια ευπάθεια μηδενικής ημέρας, χρειάζονται έναν τρόπο να φτάσουν στο ευπαθές σύστημα. Συνήθως το κάνουν μέσω ενός κοινωνικά σχεδιασμένου email, δηλαδή, ενός email ή άλλου μηνύματος που θεωρητικά προέρχεται από έναν γνωστό ή νόμιμο αποστολέα, αλλά στην πραγματικότητα προέρχεται από έναν επιτιθέμενο. Το μήνυμα προσπαθεί να πείσει έναν χρήστη να εκτελέσει μια ενέργεια όπως το άνοιγμα ενός αρχείου ή την επίσκεψη σε μια κακόβουλη ιστοσελίδα. Κάνοντας αυτό, λαμβάνει το malware του επιτιθέμενου, που διεισδύει στα αρχεία του χρήστη και κλέβει εμπιστευτικά δεδομένα.

Όταν μια ευπάθεια γίνεται γνωστή, οι προγραμματιστές προσπαθούν να την επιδιορθώσουν για να σταματήσουν την επίθεση. Ωστόσο, οι ευπάθειες ασφαλείας συχνά δεν ανακαλύπτονται αμέσως. Μερικές φορές

μπορεί να απαιτήσει μέρες, εβδομάδες ή ακόμα και μήνες πριν οι προγραμματιστές εντοπίσουν την ευπάθεια που οδήγησε στην επίθεση. Και ακόμη και αφού εγκατασταθεί ένα zero-day patch (ενημέρωση λογισμικού), δεν είναι όλοι οι χρήστες γρήγοροι στο να το εφαρμόσουν. Τα τελευταία χρόνια, οι hacker ήταν πιο γρήγοροι στο να εκμεταλλεύονται ευπάθειες σύντομα μετά την ανακάλυψή τους.

Οι εκμεταλλεύσεις (exploits) μπορούν να πωληθούν στο dark web για μεγάλα ποσά χρημάτων. Μόλις μια εκμετάλλευση εντοπιστεί και διορθωθεί, δεν αναφέρεται πλέον ως απειλή μηδενικής ημέρας (zero-day threat).

Οι επιθέσεις μηδενικής ημέρας είναι ιδιαίτερα επικίνδυνες επειδή οι μόνοι που γνωρίζουν γι' αυτές είναι οι ίδιοι οι επιτιθέμενοι. Αφού έχουν διεισδύσει σε ένα δίκτυο, οι εγκληματίες μπορούν είτε να επιτεθούν αμέσως είτε να κάθονται και να περιμένουν για την πιο ευνοϊκή στιγμή για να το κάνουν. [25]

Οι κακόβουλοι δράστες που διεξάγουν επιθέσεις μηδενικής ημέρας ανήκουν σε διαφορετικές κατηγορίες, ανάλογα με το κίνητρό τους. Για παράδειγμα (Kaspersky, Zero-Day exploit) :

- Cybercriminals - hackers οι οποίοι έχουν συνήθως ως κίνητρο τους οικονομικές αποκτήσεις
- Hacktivists - hackers που ενδιαφέρονται για πολιτικά ή κοινωνικά θέματα και θέλουν οι επιθέσεις να είναι ορατές για να τραβήξουν την προσοχή στο αίτημά τους
- Corporate espionage - hackers που κατασκοπεύουν εταιρείες για να αποκτήσουν πληροφορίες γι' αυτές
- Cyber warfare - χώρες ή πολιτικοί φορείς που κατασκοπεύουν ή επιτίθονται στο cyber infrastructure μιας άλλης χώρας

2.6.2 Ιστορία

Το 2021, η Google αναγκάστηκε να εκδόσει μια ενημέρωση μετά από επιθέσεις hacker που στόχευαν τον browser Chrome της Google. Η ευπάθεια zero-day πηγαίνει σε ένα σφάλμα στη μηχανή JavaScript V8 που

χρησιμοποιείται στο Chrome.

Το 2020, hackers ανακάλυψαν μια ευπάθεια στο Zoom, ένα δημοφιλές εργαλείο τηλεδιάσκεψης. Αυτή η ευπάθεια επέτρεπε σε έναν hacker να έχει πρόσβαση στον υπολογιστή ενός χρήστη του Zoom που χρησιμοποιούσε ακόμα μια παλιά έκδοση των Windows. Εάν ο στόχος ήταν διαχειριστής στη συνάντηση του Zoom, ο hacker μπορούσε να έχει πρόσβαση και να καταλάβει όλα τα αρχεία του.

Το 2020, το Apple iOS ήταν θύμα μιας σειράς επιθέσεων zero-day. Μία από τις επιθέσεις περιλάμβανε ένα μηδενικού-ημέρας σφάλμα που επέτρεπε σε hacker να διακινδυνεύουν τα iPhones απομακρυσμένα.

2.7 DNS Tunneling

2.7.1 Εισαγωγή

Κατά τη διάρκεια της καθημερινής αναζήτησης πληροφοριών, χρησιμοποιούμε το διαδίκτυο για να πραγματοποιήσουμε κάποιες λειτουργίες. Οι περιηγητές ιστού και το ηλεκτρονικό ταχυδρομείο χρησιμοποιούν το Σύστημα Ονομάτων τομέων (**DNS**), το οποίο επιτρέπει στις εφαρμογές να χρησιμοποιούν ονόματα για να αναπαριστούν διευθύνσεις IP, για παράδειγμα το *strathmore.edu*. Σύμφωνα με τους Bojan, Nevil και Duane (2007), το πρωτόκολλο internet δεν χρειάζεται DNS για να λειτουργήσει. Ωστόσο, η ανάγκη του χρήστη να διακρίνει μηχανές ανά ονομασία απαιτεί από το πρωτόκολλο DNS να αντιστοιχίζει ονόματα και διευθύνσεις IP. Το DNS δεν προορίζεται για τη μεταφορά δεδομένων, αλλά οι άνθρωποι μπορούν να παρεμβαίνουν για να πραγματοποιήσουν κακόβουλες επικοινωνίες ή να εξορύξουν δεδομένα από πελάτες.

Οι περισσότεροι οργανισμοί έχουν παραμελήσει το DNS ως χαμηλού κινδύνου επίθεση και επομένως δεν πραγματοποιούν παρακολούθηση αλλά εστιάζουν στην υψηλή απειλή επικοινωνίας όπως το ηλεκτρονικό ταχυδρομείο και το διαδίκτυο. Το γεγονός ότι το DNS δεν ελέγχεται κεντρικά το καθιστά ευάλωτο σε επιθέσεις ή κατάχρηση από εκτός του οργανισμού.

Επιπλέον, επιτρέπει στους επιτιθέμενους να συναλλάσσονται με ονόματα τομέων ή ακόμη και να μετακινούν γρήγορα εγγραφές ονομάτων τομέων για να αποφεύγουν το μπλοκάρισμα από διαχειριστές. Επιπλέον, οι επιτιθέμενοι μπορούν να χρησιμοποιήσουν ευπάθειες που υπάρχουν στην ασφάλεια του πελάτη, η οποία συνήθως δεν είναι αυστηρή στην κίνηση του DNS, ακόμη και σε πολύ περιορισμένα δίκτυα οργανισμών.

Το DNS tunneling επιτρέπει τη δρομολόγηση άλλων πρωτοκόλλων μέσω του DNS. Σύμφωνα με τον Beauregard (2013), το DNS tunneling είναι μια τεχνική που επιτρέπει σε επιτιθέμενους να κωδικοποιούν τα δεδομένα άλλων προγραμμάτων ή πρωτοκόλλων σε ερωτήματα και απαντήσεις DNS. Και αυτό είναι ανησυχητικό από τα τέλη της δεκαετίας του '90. Παρόλο που η αρχική πρόθεση του DNS tunneling ήταν να παρακάμψει τις περιορισμένες πύλες σε σημεία πρόσβασης Wi-Fi, με τον χρόνο η χρήση έχει επεκταθεί και έχει δημιουργήσει περισσότερους κινδύνους για τους οργανισμούς. Η πιο βασική μορφή του tunneling απαιτεί έναν πελάτη να κινδυνεύει μέσω malware, phishing ή social engineering. Ωστόσο, ο πελάτης δεν χρειάζεται απαραίτητα πρόσβαση στο διαδίκτυο για να βρεθεί σε κίνδυνο. Ο πελάτης απλώς χρειάζεται πρόσβαση σε έναν εσωτερικό διακομιστή DNS με εξωτερική πρόσβαση, ο οποίος θα προωθεί αιτήσεις και θα λαμβάνει αιτήσεις.

Σύμφωνα με τον Fruz (2014), σε ένα κανονικό σενάριο, ο χρήστης A και ο χρήστης B βρίσκονται πίσω από ένα εταιρικό τείχος προστασίας (firewall) D. Οι πολιτικές του τείχους προστασίας αποτρέπουν όλη την κίνηση εκτός από εκείνη που έρχεται μέσω της θύρας 53. Αλλά ο χρήστης A και ο χρήστης B μπορούν να έχουν πρόσβαση στο διαδίκτυο εκμεταλλευόμενοι την κίνηση DNS μέσω του tunneling. Καθώς ο διακομιστής DNS στα αριστερά έχει δυνατότητες caching, ο χρήστης A θα προσπαθήσει να έχει πρόσβαση σε οποιαδήποτε ιστοσελίδα βρίσκεται στη μνήμη cache, αλλά η αίτηση δεν θα πάει στον επαναλαμβανόμενο διακομιστή. Έτσι, όταν ο χρήστης A καλεί μια νέα αίτηση, ο διακομιστής DNS δεν θα βρει την εγγραφή του A στον

διακομιστή DNS, επομένως θα την στείλει σε έναν εξωτερικό διακομιστή DNS. [18] [20]

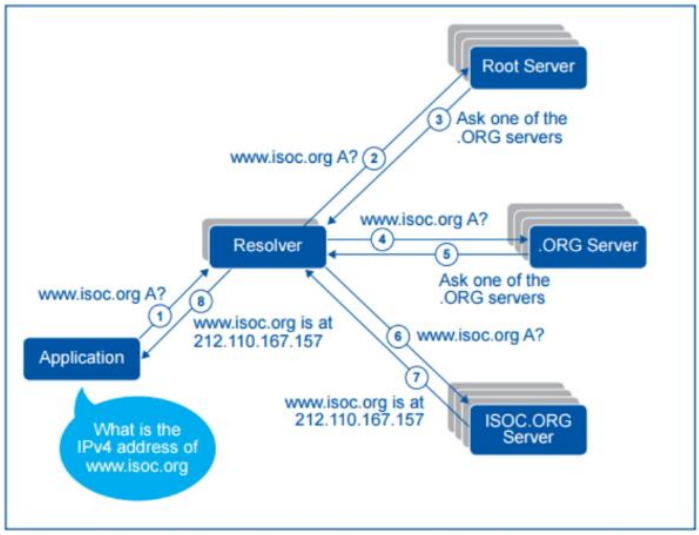

Figure 5: DNS Tunneling (Derrick Rono, 2015, researchgate.net)

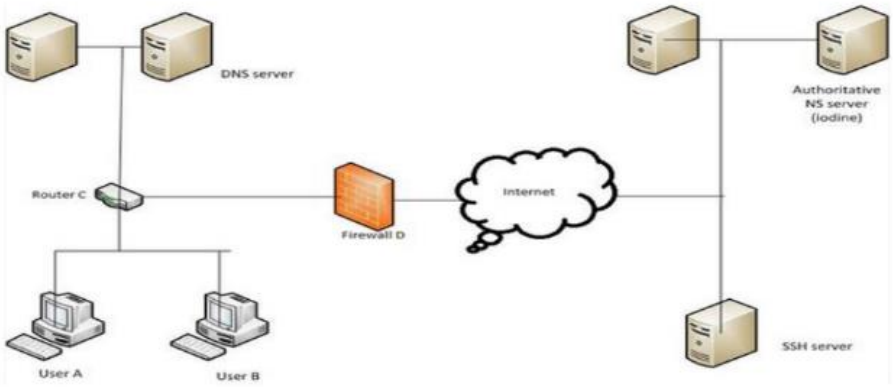

Figure 6: DNS Tunneling example (Derrick Rono, 2015, researchgate.net)

2.7.2 Ιστορία

Το DNS tunneling συζητήθηκε για πρώτη φορά στα τέλη της δεκαετίας

του ’90, και μέχρι το 2004 είχε εξαπλωθεί αρκετά ώστε να συζητηθεί στο συνέδριο Black Hat από τον Dan Kaminsky. Ο Kaminsky ήταν ο δημιουργός του Ozyman DNS, ενός από τα πρώτα εργαλεία που χρησιμοποιήθηκαν για το tunneling του DNS. Από τότε έχουν δημιουργηθεί πολλά άλλα εργαλεία, αν και η βασική μέθοδος παραμένει σχεδόν η ίδια.

Η ιστορία του DNS tunneling σχετίζεται στενά με την εξέλιξη των απειλών κυβερνοασφάλειας. Εμφανίστηκε ως μια τεχνική για την παράκαμψη περιορισμών δικτύου και την αποφυγή ανίχνευσης. Αρχικά, χρησιμοποιήθηκε για νόμιμους σκοπούς όπως η παράκαμψη περιοριστικών δικτύων ή η ανώνυμη διαδικτυακή δραστηριότητα. Ωστόσο, το DNS tunneling σταδιακά έγινε δημοφιλές μεταξύ κακόβουλων δραστών ως μυστικό κανάλι επικοινωνίας για την απομάκρυνση δεδομένων και τον έλεγχο εντολών. Τα πρώτα παραδείγματα αυτής της επίθεσης εμφανίστηκαν στις αρχές της δεκαετίας του 2000 και συχνά συνδέονταν με τη διάδοση κακόβουλου λογισμικού. Με τα χρόνια, οι επιτιθέμενοι έγιναν πιο εξελιγμένοι και οι τεχνικές τους εξελίχθηκαν. Αυτό ανάγκασε τους ειδικούς κυβερνοασφάλειας να αναπτύξουν προηγμένα μηχανισμούς παρακολούθησης και πρόληψης για την προστασία από αυτό. Ορισμένα από τα συνηθέστερα εργαλεία που χρησιμοποιούνται για το tunneling του DNS είναι το Iodine (2006), το NSTX (2000, μόνο για Linux), και το DNScat (2010).

Κεφάλαιο 3ο Διαφοροποιήσεις ως προς τον τρόπο επίθεσης

3.1 Επιθέσεις Malware

Το κακόβουλο λογισμικό αποτελεί μία από τις μεγαλύτερες απειλές ασφάλειας που αντιμετωπίζουν οι επιχειρήσεις. Τα τμήματα ασφαλείας πρέπει να παρακολουθούν ενεργά τα δίκτυα για να πιάσουν και να περιορίσουν το κακόβουλο λογισμικό πριν προκαλέσει εκτεταμένες ζημιές. Για το κακόβουλο λογισμικό, ωστόσο, η πρόληψη είναι καθοριστική. Αλλά για να προλάβουμε μια επίθεση, είναι κρίσιμο να κατανοήσουμε πρώτα τι είναι το κακόβουλο λογισμικό, μαζί με τα πιο κοινά είδη του. Οι επιτιθέμενοι χρησιμοποιούν το κακόβουλο λογισμικό, για να προκαλέσουν εσκεμμένα βλάβη και μόλυνση σε συσκευές και δίκτυα. Ο γενικός όρος περιλαμβάνει πολλές υποκατηγορίες, συμπεριλαμβανομένων των εξής:

Ιοί: Ο ιός υποκείμενος συστήνεται στις συσκευές και αναπαράγεται σε όλα τα συστήματα. Οι ιοί χρειάζονται ανθρώπινη παρέμβαση για να μεταδοθούν.

Κλεπτοκράτες (Worms): Οι κλεπτοκράτες αναπαράγονται αυτόματα και μολύνουν άλλους υπολογιστές χωρίς ανθρώπινη παρέμβαση.

Κρυπτογραφικό κακόβουλο λογισμικό (Ransomware): Το κρυπτογραφικό κακόβουλο λογισμικό κρυπτογραφεί τα αρχεία ή τις συσκευές του θύματος και απαιτεί λύτρα για την επαναφορά τους.

Ρομπότ (Bots): Ένα ρομπότ είναι αυτόματο κακόβουλο λογισμικό που εξαπλώνεται στις συσκευές, δημιουργώντας ένα δίκτυο ρομπότ.

Δούρειοι ίπποι (Trojan horses): Ένας δούρειος ίππος είναι κακόβουλο λογισμικό που εμφανίζεται ως νόμιμο στους χρήστες.

Κλειδοκράτες (Keyloggers): Οι κλειδοκράτες παρακολουθούν τα πλήκτρα που πατάνε οι χρήστες για να αποκτήσουν πρόσβαση σε ευαίσθητες πληροφορίες.

Rootkits: Ένα rootkit είναι κακόβουλο λογισμικό που επιτρέπει σε επιτιθέμενους να αποκτήσουν απομακρυσμένη πρόσβαση και έλεγχο σε μια συσκευή.

Κακόβουλο λογισμικό παρακολούθησης (Spyware):

Το κακόβουλο λογισμικό παρακολούθησης είναι κακόβουλο λογισμικό που καταγράφει δεδομένα των χρηστών χωρίς τη γνώση τους.

Μη αρχειακό κακόβουλο λογισμικό (Cryptojacking): Το μη αρχειακό κακόβουλο λογισμικό δεν εγκαθίσταται στους σκληρούς δίσκους των θυμάτων.

Καθαρισμός δεδομένων (Wiper malware): Ο καθαρισμός δεδομένων καταστρέφει τα δεδομένα του θύματος χωρίς να ζητείται λύτρα.

3.2 Διαφήμιση (Adware):

Η διαφήμιση είναι λογισμικό που εμφανίζει ή κατεβάζει ανεπιθύμητες διαφημίσεις. Δυνατή κυβερνο-ασφάλεια είναι η καλύτερη προστασία ενάντια σε επιθέσεις κακόβουλου λογισμικού.

3.3 Phishing

Μια κακόβουλη επίθεση phishing είναι μια τεχνική κυβερνοεπίθεσης που χρησιμοποιείται από τους επιτιθέμενους για να εξαπατήσουν τους χρήστες και να τους αποσπάσουν προσωπικά δεδομένα, όπως κωδικούς πρόσβασης, αριθμούς πιστωτικών καρτών, ή άλλες ευαίσθητες πληροφορίες. Οι επιτιθέμενοι συχνά προσποιούνται ότι είναι αξιόπιστες οντότητες, όπως τράπεζες, εταιρείες τεχνολογίας ή ακόμη και γνωστοί του χρήστη, και χρησιμοποιούν μέσα όπως email, μηνύματα κειμένου, ή πλαστές ιστοσελίδες για να παραπλανήσουν τα θύματα τους. Τα κύρια χαρακτηριστικά μιας επίθεσης phishing είναι τα ακόλουθα [5]:

1. Ψεύτικα Email ή Μηνύματα: Αυτά μπορεί να φαίνονται ότι προέρχονται

από μια αξιόπιστη πηγή, όπως μια τράπεζα ή μια δημοφιλή υπηρεσία, αλλά στην πραγματικότητα είναι κακόβουλα. Συχνά περιέχουν συνδέσμους που οδηγούν σε ψεύτικες ιστοσελίδες.

2. Πλαστές Ιστοσελίδες: Οι επιτιθέμενοι δημιουργούν ιστοσελίδες που μοιάζουν σχεδόν πανομοιότυπες με τις αυθεντικές, με σκοπό να παραπλανήσουν τους χρήστες να εισάγουν τα προσωπικά τους στοιχεία.

3. Αίσθηση Επείγοντος: Πολλά phishing μηνύματα περιέχουν μηνύματα επείγοντος, όπως προειδοποιήσεις ασφαλείας ή προσφορές που λήγουν σύντομα, για να παρακινήσουν τους χρήστες να δράσουν γρήγορα χωρίς να το σκεφτούν.

3.4 Man-in-the-middle attack

Μια Man-in-the-Middle (MitM) attack είναι ένας τύπος κυβερνοεπίθεσης όπου ο επιτιθέμενος παρεμβάλλεται κρυφά στη διαδικτυακή επικοινωνία μεταξύ δύο μερών (π.χ., ενός χρήστη και μιας ιστοσελίδας ή μιας συσκευής και ενός διακομιστή) χωρίς να το αντιληφθούν οι εμπλεκόμενοι. Ο επιτιθέμενος μπορεί να υποκλέψει, τροποποιήσει ή ακόμα και να εισαγάγει δεδομένα στην επικοινωνία τους [13]

3.5 Denial-of-service attack

Οι δημοφιλείς επιθέσεις πλημμύρας περιλαμβάνουν:

Επιθέσεις με υπερχείλιση μνήμης - η πιο κοινή επίθεση DoS. Η ιδέα είναι να στείλετε περισσότερη κίνηση σε μια διεύθυνση δικτύου από ό,τι έχουν κατασκευάσει οι προγραμματιστές του συστήματος να χειριστούν.

ICMP flood - εκμεταλλεύεται κακοδιαμορφωμένες δικτυακές συσκευές με την αποστολή παραποιημένων πακέτων που πραγματοποιούν ping σε κάθε υπολογιστή στο στοχευμένο δίκτυο, αντί να στοχεύει μόνο ένα συγκεκριμένο μηχάνημα. Έτσι το δίκτυο ενισχύεται για να αυξήσει την κίνηση. Αυτή η επίθεση είναι επίσης γνωστή ως επίθεση Smurf ή ping του θανάτου.

SYN flood - στέλνει αιτήματα για σύνδεση σε έναν διακομιστή, αλλά ποτέ δεν

ολοκληρώνει τη συνδεσιμότητα. Συνεχίζεται μέχρι να κατακλυστούν όλες οι ανοικτές θύρες με αιτήσεις και καμία δεν είναι διαθέσιμη για τους νόμιμους χρήστες να συνδεθούν.

Άλλες επιθέσεις DoS απλώς εκμεταλλεύονται ευπάθειες που προκαλούν το σύστημα ή την υπηρεσία στόχο να καταρρεύσουν. Σε αυτές τις επιθέσεις, αποστέλλονται εισόδους που εκμεταλλεύονται τα σφάλματα του στόχου, τα οποία στη συνέχεια καταρρέουν ή δυσταθούν το σύστημα, ώστε να μην μπορεί να προσπελαστεί ή να χρησιμοποιηθεί.

Ένα επιπλέον είδος επίθεσης DoS είναι η Διανεμημένη Επίθεση Απόρριψης Υπηρεσίας (DDoS). Μια επίθεση DDoS συμβαίνει όταν πολλά συστήματα συντονίζουν μια συγχρονισμένη επίθεση DoS σε έναν μοναδικό στόχο. Η ουσιαστική διαφορά είναι ότι αντί να επιτεθεί από μια τοποθεσία, ο στόχος επιτίθεται από πολλαπλές τοποθεσίες ταυτόχρονα. Η διανομή των υπολογιστών που καθορίζει μια DDoS παρέχει στον επιτιθέμενο πολλαπλά πλεονεκτήματα:

Μπορεί να αξιοποιήσει τον μεγαλύτερο όγκο μηχανημάτων για να εκτελέσει μια σοβαρά δυσλειτουργική επίθεση.

Η τοποθεσία της επίθεσης είναι δύσκολο να ανιχνευθεί λόγω της τυχαίας διανομής των επιτιθέμενων συστημάτων (συχνά παγκοσμίως).

Είναι πιο δύσκολο να απενεργοποιήσεις πολλά μηχανήματα από ό,τι ένα.

Είναι πολύ δύσκολο να ανιχνευθεί η πραγματική επιτιθέμενη ομάδα, καθώς κρύβονται πίσω από πολλά (κυρίως συμβιβασμένα) συστήματα.

Οι σύγχρονες τεχνολογίες ασφαλείας έχουν αναπτύξει μηχανισμούς για να αντιμετωπίζουν τα περισσότερα είδη επιθέσεων DoS, αλλά λόγω των μοναδικών χαρακτηριστικών των DDoS, εξακολουθεί να θεωρείται ως μια επικίνδυνη απειλή και αποτελεί υψηλότερη ανησυχία για οργανισμούς που φοβούνται ότι μπορεί να γίνουν στόχος μιας τέτοιας επίθεσης.

3.6 SQL Injection

Το SQL Injection είναι μια από τις πιο κοινές και επικίνδυνες τεχνικές κυβερνοεπίθεσης που στοχεύει σε βάσεις δεδομένων. Πρόκειται για μια τεχνική κατά την οποία ο επιτιθέμενος εκμεταλλεύεται κενά ασφαλείας σε εφαρμογές που χρησιμοποιούν SQL (Structured Query Language) για να εισάγει κακόβουλο SQL κώδικα, με σκοπό να αποκτήσει πρόσβαση σε δεδομένα ή να καταστρέψει δεδομένα σε μια βάση δεδομένων [3].

Λειτουργία επίθεσης SQL Injection:

Εισαγωγή Κακόβουλου Κώδικα: Ο επιτιθέμενος εισάγει κακόβουλο SQL κώδικα σε πεδία εισόδου χρήστη, όπως φόρμες σύνδεσης, αναζήτησης, ή URL παραμέτρους, τα οποία δεν έχουν επαρκή φίλτρα ασφαλείας. Ο κώδικας αυτός μπορεί να εκτελεστεί από τη βάση δεδομένων.
Εκτέλεση του Κακόβουλου Κώδικα: Εάν η εφαρμογή δεν χειριστεί σωστά τις εισόδους του χρήστη, ο κακόβουλος κώδικας θα εκτελεστεί, επιτρέποντας στον επιτιθέμενο να κάνει διάφορες κακόβουλες ενέργειες, όπως:

- Ανάκτηση δεδομένων: Ο επιτιθέμενος μπορεί να αποκτήσει πρόσβαση σε ευαίσθητα δεδομένα, όπως προσωπικά στοιχεία χρηστών, κωδικούς πρόσβασης, ή πληροφορίες πιστωτικών καρτών.
- Τροποποίηση δεδομένων: Ο επιτιθέμενος μπορεί να αλλάξει δεδομένα στη βάση, όπως να ενημερώσει ή να διαγράψει εγγραφές.
- Εκτέλεση διοικητικών εντολών: Μπορεί να αποκτήσει δικαιώματα διαχειριστή και να εκτελέσει επιβλαβείς ενέργειες στη βάση δεδομένων.

Αποφυγή εντοπισμού: Πολλοί επιτιθέμενοι χρησιμοποιούν τεχνικές για να καλύψουν τα ίχνη τους και να αποφύγουν τον εντοπισμό από τα συστήματα ασφαλείας.

Παράδειγμα SQL Injection:

Έστω ότι έχουμε μια φόρμα σύνδεσης με τα πεδία username και

password. Ο SQL κώδικας που εκτελείται όταν ο χρήστης υποβάλλει τη φόρμα είναι: SELECT * FROM users WHERE username = 'user' AND password = 'pass';

Αντί για κανονικά στοιχεία, ένας επιτιθέμενος θα μπορούσε να εισάγει τα εξής:

- Username: ' OR '1'='1
- Password: '' OR '1'='1

Αυτό θα μετατρέψει το παραπάνω query σε: SELECT * FROM users WHERE username = '' OR '1'='1' AND password = '' OR '1'='1';

Αυτό το query θα επιστρέψει όλα τα αρχεία στη βάση δεδομένων, δίνοντας ουσιαστικά στον επιτιθέμενο πρόσβαση χωρίς να γνωρίζει τον σωστό κωδικό πρόσβασης.

3.7 Zero-day exploit

Ένα zero-day exploit είναι μια ευπάθεια ή αδυναμία σε λογισμικό ή υλικό που δεν έχει ανακαλυφθεί ή δεν έχει διορθωθεί από τον προγραμματιστή ή τον κατασκευαστή του προϊόντος. Ο όρος "zero-day" αναφέρεται στο γεγονός ότι οι προγραμματιστές έχουν μηδενικές ημέρες (zero days) για να διορθώσουν το πρόβλημα πριν οι επιτιθέμενοι το εκμεταλλευτούν. Αυτές οι επιθέσεις είναι ιδιαίτερα επικίνδυνες επειδή μπορούν να χρησιμοποιηθούν από κυβερνοεγκληματίες πριν γίνει γνωστή η ευπάθεια και πριν αναπτυχθούν αντίμετρα ή διορθώσεις (patches) [29].

Λειτουργία ενός zero-day exploit:

Ανακάλυψη της Ευπάθειας: Ένας επιτιθέμενος ή ένας ερευνητής ασφαλείας ανακαλύπτει μια ευπάθεια σε ένα λογισμικό ή σε ένα σύστημα. Αυτή η ευπάθεια μπορεί να επιτρέπει σε κάποιον να παρακάμψει μέτρα ασφαλείας, να εκτελέσει κακόβουλο κώδικα, ή να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε δεδομένα.

Δημιουργία του Exploit: Ο επιτιθέμενος αναπτύσσει έναν συγκεκριμένο

κώδικα ή μέθοδο που εκμεταλλεύεται αυτήν την ευπάθεια για να επιτεθεί σε συστήματα που χρησιμοποιούν το ευάλωτο λογισμικό.

Εκμετάλλευση της Ευπάθειας: Ο επιτιθέμενος χρησιμοποιεί το zero-day exploit για να επιτεθεί σε στόχους. Αυτή η εκμετάλλευση μπορεί να γίνει μέσω email, κακόβουλων ιστοσελίδων, κακόβουλου λογισμικού, ή άλλων μεθόδων.

Καθυστερημένη Ανίχνευση και Αντίδραση: Επειδή η ευπάθεια είναι άγνωστη, τα συστήματα ασφαλείας, όπως τα antivirus, τα firewalls, και άλλες άμυνες, δεν είναι σε θέση να ανιχνεύσουν ή να μπλοκάρουν την επίθεση. Συχνά, οι οργανισμοί δεν αντιλαμβάνονται ότι έχουν πέσει θύματα επίθεσης μέχρι να έχει ήδη προκληθεί ζημιά.

Κίνδυνοι και επιπτώσεις των zero-day exploits:

- Δυσκολία στην ανίχνευση: Δεδομένου ότι η ευπάθεια είναι άγνωστη, οι επιθέσεις zero-day είναι εξαιρετικά δύσκολο να εντοπιστούν εγκαίρως.
- Μεγαλύτερες συνέπειες: Επειδή τα συστήματα δεν είναι προετοιμασμένα για τέτοιου είδους επιθέσεις, οι συνέπειες μπορεί να είναι σοβαρές, περιλαμβάνοντας απώλεια δεδομένων, παραβιάσεις ασφαλείας, ή οικονομικές ζημίες.
- Ευρεία χρήση από κακόβουλους φορείς: Οι επιτιθέμενοι που αποκτούν πρόσβαση σε ένα zero-day exploit μπορούν να το πουλήσουν στη μαύρη αγορά ή να το χρησιμοποιήσουν σε στοχευμένες επιθέσεις, όπως κυβερνοκατασκοπεία ή κυβερνοπόλεμο.

Παράδειγμα zero-day exploit:

Ένα διάσημο παράδειγμα zero-day exploit είναι το Stuxnet worm, το οποίο χρησιμοποιήθηκε για να στοχεύσει το πυρηνικό πρόγραμμα του Ιράν. Το Stuxnet εκμεταλλεύτηκε πολλαπλές zero-day ευπάθειες στα Windows για να επηρεάσει τα συστήματα ελέγχου των φυγοκεντρητών, προκαλώντας

φυσική ζημιά.

3.8 DNS Tunneling

Η επίθεση DNS tunneling εκμεταλλεύεται το πρωτόκολλο DNS και επιτυγχάνει το tunneling κακόβουλου λογισμικού ή δεδομένων, μέσω ενός μοντέλου πελάτη-εξυπηρετητή (client-server model).

Όλα ξεκινούν όταν ένας χρήστης κατεβάζει κακόβουλο λογισμικό ή ο cyber criminal, καταφέρνει να εκμεταλλευτεί μια ευπάθεια της παραβιασμένης συσκευής για να μεταφέρει ένα κακόβουλη φορτίο. Στις περισσότερες περιπτώσεις, ο κυβερνοεγκληματίας επιθυμεί να διατηρήσει μια σύνδεση με την παραβιασμένη συσκευή, δηλαδή να έχει τη δυνατότητα να εκτελεί εντολές στη συσκευή στόχο ή να εξαγάγει δεδομένα. Για τον λόγο αυτό, ο επιτιθέμενος μπορεί να καθορίσει μια σύνδεση ελέγχου-εντολών (command-and-control) (C2). Τέτοια επικοινωνία πρέπει να μπορεί να περάσει μέσα από διάφορα μέτρα ασφαλείας περιμετρικού δικτύου, ενώ πρέπει να αποφεύγει την ανίχνευση μέχρι να διασχίσει το δίκτυο στόχο.

Για τον λόγο αυτό, το DNS είναι μια κατάλληλη επιλογή για τη δημιουργία του τούνελ. Αυτός είναι ένας κοινός όρος στην ασφάλεια στον κυβερνοχώρο που σημαίνει μια σύνδεση πρωτοκόλλου που μεταφέρει ένα φορτίο που περιλαμβάνει δεδομένα (εντολές) και περνά μέσα από μέτρα ασφαλείας περιμετρικού δικτύου. Με αυτόν τον τρόπο, η επίθεση DNS tunneling καταφέρνει να κρύψει πληροφορίες μέσα σε ερωτήματα DNS και να τα στείλει σε ένα ελεγχόμενο διακομιστή από τον κυβερνοεγκληματία. Η κίνηση DNS (DNS traffic) περνά ελεύθερα μέσα από μέτρα ασφαλείας περιμετρικού δικτύου, όπως firewall.

Για τη δημιουργία του τούνελ DNS, ο κυβερνοεγκληματίας εγγράφει ένα domain name και διαμορφώνει ένα αρμόδιο εξυπηρετητή ονομάτων (authoritative name server) υπό τον έλεγχό του.

Στη συνέχεια, το κακόβουλο λογισμικό ή το φορτίο στην

παραβιασμένη συσκευή ξεκινά ένα ερώτημα DNS για ένα subdomain που ορίζει μια κωδικοποιημένη επικοινωνία. Ο αναδρομικός εξυπηρετητής DNS (DNS resolver) λαμβάνει το ερώτημα DNS και το δρομολογεί προς τον ελεγχόμενο διακομιστή. Ο διακομιστής απαντά με κακόβουλα δεδομένα DNS που περιέχουν δεδομένα (command) πίσω στην παραβιασμένη συσκευή. Με αυτόν τον τρόπο, η επίθεση περνά χωρίς να ενεργοποιήσει κανένα μέτρο ασφαλείας.

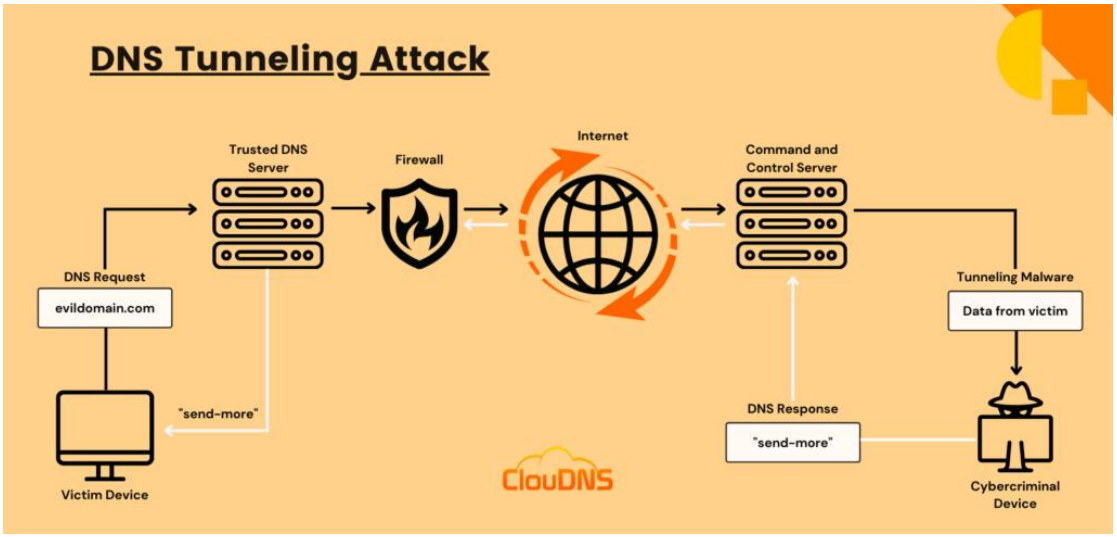

Figure 7: DNS Tunneling attack example (CloudDNS.net)

Κεφάλαιο 4ο Αδυναμίες που εκμεταλλεύονται

4.1 Επιθέσεις Malware

Οι malware ιοί εκμεταλλεύονται κυρίως τρεις κύριες αδυναμίες στα συστήματα Η/Υ και τα δίκτυα: Ελαττώματα (flaws), Χαρακτηριστικά (features) και Σφάλματα χρήστη (user errors). Τα ελαττώματα (flaws) είναι ανεπιθύμητες λειτουργίες που μπορεί να οφείλονται είτε σε κακή σχεδίαση είτε σε λάθη κατά την υλοποίηση του λογισμικού. Αυτά τα ελαττώματα μπορεί να παραμείνουν απαρατήρητα για μεγάλο χρονικό διάστημα και αποτελούν τον κυριότερο στόχο επιθέσεων. Οι zero-day ευπάθειες (zero-day vulnerabilities) ανήκουν σε αυτήν την κατηγορία και αναφέρονται σε νέες ευπάθειες που δεν έχουν ακόμα γίνει γνωστές στο ευρύ κοινό.

Τα χαρακτηριστικά (features) αναφέρονται σε επιθυμητές λειτουργίες του συστήματος που μπορούν να καταχραστούν από τον επιτιθέμενο για να παραβιάσει το σύστημα. Τα χαρακτηριστικά μπορεί να βελτιώνουν την εμπειρία του χρήστη, να βοηθούν στη διάγνωση προβλημάτων ή να βελτιώνουν τη διαχείριση, αλλά μπορούν επίσης να εκμεταλλευτούν από έναν επιτιθέμενο.

Όταν η Microsoft εισήγαγε τα macros στο σύνολο των εφαρμογών Office τη δεκαετία του '90, αυτά έγιναν σύντομα ευπάθεια, με τον ιό Melissa το 1999 να είναι ένα πρωτότυπο παράδειγμα. Τα macros είναι υπό εκμετάλλευση ακόμα και σήμερα. Το Banking Trojan Dridex που εξαπλώθηκε στα τέλη του 2014 εξαρτιόταν από spam για να παραδώσει έγγραφα του Microsoft Word που περιέχουν κακόβουλο κώδικα macros, ο οποίος στη συνέχεια κατεβάζει το Dridex στο επηρεαζόμενο σύστημα.

Το JavaScript, που χρησιμοποιείται ευρέως στο δυναμικό περιεχόμενο του ιστού, συνεχίζει να χρησιμοποιείται από επιτιθέμενους. Αυτό περιλαμβάνει την ανακατεύθυνση (diverting) του προγράμματος περιήγησης του χρήστη σε μια κακόβουλη ιστοσελίδα και το download κακόβουλου κώδικα για να περάσει απαρατήρητος από το βασικό

φιλτράρισμα του ιστού.

Τα σφάλματα χρήστη (user errors) αναφέρονται σε θέματα ασφαλείας που πηγάζουν από ανθρώπινα λάθη. Η ανθρώπινη παρέμβαση σε έναν υπολογιστή ή ένα υπολογιστικό σύστημα, μπορεί να είναι κρίσιμη για την ασφάλειά του. Ακόμα και ένας υπολογιστής που έχει σχεδιαστεί και υλοποιηθεί με προσοχή μπορεί να εκτίθεται σε ευπάθειες αν δεν ληφθούν τα κατάλληλα μέτρα προστασίας. Δυστυχώς, οι προσπάθειες αυτές μπορούν εύκολα να αναιρεθούν, ειδικά όταν ένας μη επιδέξιος διαχειριστής συστημάτων ενεργοποιεί ευπάθειες της λειτουργίας, δεν διορθώνει γνωστές ελλείψεις ή αφήνει τους προεπιλεγμένους κωδικούς πρόσβασης (credentials) αναλλοίωτους.

Γενικότερα, οι χρήστες μπορούν να αποτελέσουν σημαντική πηγή ευπαθειών. Κάνουν λάθη, όπως την επιλογή ενός κοινού ή εύκολα μαντεύσιμου κωδικού πρόσβασης, ή αφήνουν τον φορητό υπολογιστή ή το κινητό τους τηλέφωνο χωρίς προστασία από τρίτους. Ακόμα και οι πιο ενημερωμένοι χρήστες στον κυβερνοχώρο μπορούν να εξαπατηθούν και να αποκαλύψουν πληροφορίες που μπορεί να είναι χρήσιμες σε έναν επιτιθέμενο. Αυτές οι λεπτομέρειες θα επιτρέψουν σε έναν επιτιθέμενο να επιλέξει και να εκτελέσει μια επίθεση με κατάλληλο τρόπο. Εκμεταλλευόμενοι αυτές τις αδυναμίες, οι malware ιοί καταφέρνουν να εισβάλουν σε συστήματα και δίκτυα και να προκαλέσουν ζημιές.

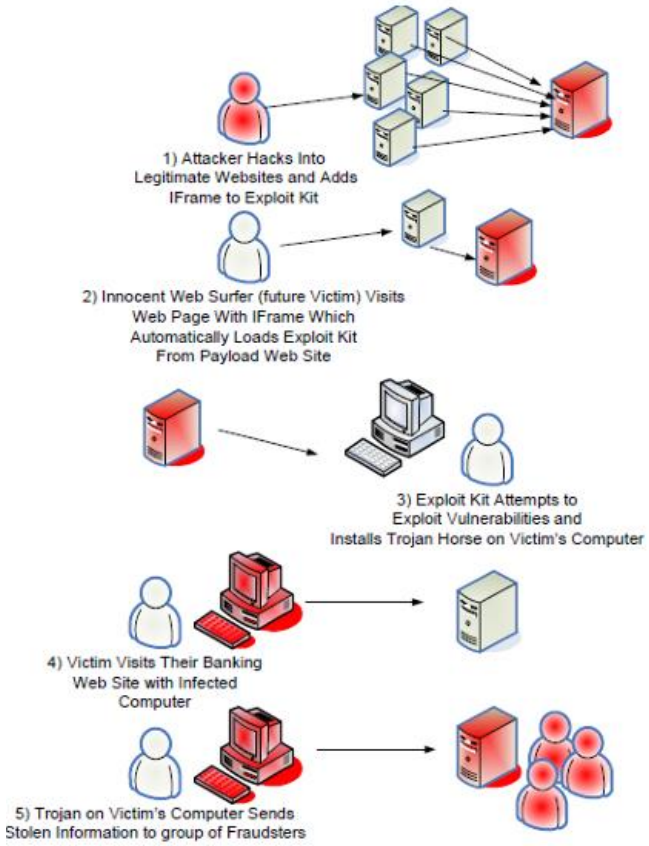

Figure 8: Malware attack scenario (Malware Risks and Mitigation Report, 2011, nist.gov)

4.2 Phishing

Οι επιθέσεις phishing εκμεταλλεύονται πολλές αδυναμίες στην ανθρώπινη συμπεριφορά και στα συστήματα πληροφορικής. Παρακάτω ακολουθεί αναλυτική παρουσίαση αυτών των ευπαθειών:

Ανθρώπινη αδυναμία στην αναγνώριση απάτης: Οι φιλικές και επειγόντως εμφανιζόμενες επιθέσεις εκμεταλλεύονται την τάση των ανθρώπων να ανταποκρίνονται σε κάτι που φαίνεται επίσημο ή επείγον. Οι χρήστες συχνά πιστεύουν ότι λαμβάνουν έγκυρα μηνύματα από οργανισμούς ή επιχειρήσεις και τελικά πέφτουν θύματα.

Αδυναμίες στα φίλτρα email: Ακόμα και οι προηγμένοι anti-phishing filters μπορεί να μην ανιχνεύουν όλα τα ανεπιθύμητα μηνύματα λόγω της σύνθετης

φύσης του phishing.

Ευκολία στη δημιουργία απατηλών ιστότοπων: Οι επιτιθέμενοι μπορούν εύκολα να δημιουργήσουν απομιμήσεις ιστοσελίδων που μοιάζουν ακριβώς με έγκυρες, προκαλώντας σύγχυση στους χρήστες.

Χρήση ψυχολογικών τεχνικών: Οι επιθέσεις phishing εκμεταλλεύονται ψυχολογικές τεχνικές όπως η ανάγκη για επείγοντα μέτρα ή η επιθυμία για επιβράβευση, προκειμένου να πείσουν τα θύματά τους να παραδώσουν προσωπικές πληροφορίες ή να κάνουν κρίσιμες ενέργειες (για παράδειγμα αποστολή χρηματικού ποσού).

Αδυναμίες στους τεχνικούς μηχανισμούς ανίχνευσης: Παρόλο που υπάρχουν τεχνικές για την ανίχνευση phishing, οι επιτιθέμενοι συνεχίζουν να βρίσκουν τρόπους να τις παρακάμψουν, όπως η χρήση προσαρμοσμένων επιθέσεων και η εξέλιξη των μεθόδων τους.

Έλλειψη ενημέρωσης και εκπαίδευσης των χρηστών: Οι χρήστες συχνά δεν έχουν επαρκή εκπαίδευση σχετικά με τις τελευταίες μεθόδους phishing και πώς να τις αντιμετωπίσουν.

Δυσκολία στην αντιμετώπιση των επιθέσεων: Λόγω της διεθνούς φύσης των επιθέσεων και της χρήσης προηγμένων τεχνικών, η αντιμετώπισή τους είναι συχνά προβληματική και δύσκολη.

Αυτές οι αδυναμίες επιτρέπουν στις επιθέσεις phishing να είναι αποτελεσματικές και να προκαλούν σημαντικές ζημίες σε επιχειρήσεις και χρήστες. Η συνεχής εκπαίδευση των χρηστών και η βελτίωση των τεχνικών ανίχνευσης αποτελούν κρίσιμα μέτρα για τη μείωση των κινδύνων που συνδέονται με το phishing.

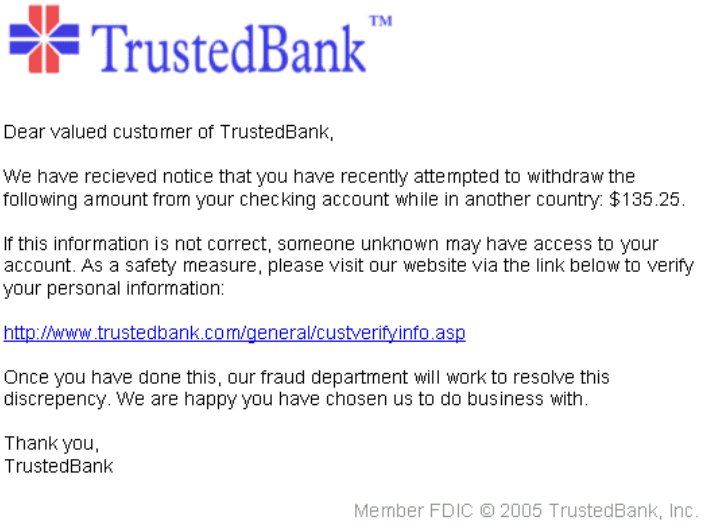

Figure 9: Phishing mail attack (slideshare.net)

4.3 Man-in-the-middle attack

Οι επιθέσεις man-in-the-middle εκμεταλλεύονται κυρίως την αδυναμία των θυμάτων να ανιχνεύσουν την παρουσία του επιτιθέμενου μεταξύ τους και του νόμιμου μέρους της επικοινωνίας. Κάποιες από τις κύριες αδυναμίες που εκμεταλλεύονται οι επιθέσεις man-in-the-middle περιλαμβάνουν:

Αδυναμία αναγνώρισης του επιτιθέμενου: Συχνά τα θύματα δεν αντιλαμβάνονται ότι η επικοινωνία τους έχει διακοπεί ή παρεμποδιστεί από έναν επιτιθέμενο.

Αναξιοπιστία των δικτυακών συστημάτων: Σε πολλές περιπτώσεις, οι επιθέσεις man-in-the-middle εκμεταλλεύονται ευπάθειες στα δικτυακά συστήματα, όπως το ARP spoofing ή το DNS spoofing, για να παρεμβάλουν τον επιτιθέμενο στην επικοινωνία.

Ελλείψεις στην κρυπτογράφηση: Η χρήση μη κρυπτογραφημένων καναλιών επικοινωνίας επιτρέπει στον επιτιθέμενο να διαβάζει και να τροποποιεί τα δεδομένα που περνούν ανάμεσα από το θύμα και το νόμιμο μέρος της επικοινωνίας.

Ανθρώπινα προγραμματιστικά λάθη: Τέλος, οι επιθέσεις man-in-the-middle μπορεί να εκμεταλλευτούν την άγνοια ή την έλλειψη εκπαίδευσης των χρηστών, οι οποίοι ενδέχεται να παραβλέψουν τα σημάδια ενός επιτιθέμενου στην επικοινωνία τους.

Οι επιθέσεις man-in-the-middle εκμεταλλεύονται την έλλειψη αναγνώρισης και προστασίας από τους χρήστες και τα δικτυακά συστήματα, καθώς και τις αδυναμίες στην κρυπτογράφηση και την ασφάλεια των δικτύων. Η κατανόηση αυτών των αδυναμιών είναι κρίσιμη για την ανάπτυξη αποτελεσματικών μέτρων προστασίας κατά των επιθέσεων man-in-the-middle.

4.4 Denial-of-service attack

Η επίθεση απόρριψης υπηρεσιών (DoS) εκμεταλλεύεται κυρίως τις αδυναμίες στον τρόπο λειτουργίας του δικτύου και των πρωτοκόλλων. Παρακάτω θα δούμε πώς εκμεταλλεύεται τις αδυναμίες σε κάθε επίπεδο του OSI reference model:

Επίπεδο Εφαρμογής (Application Layer)**:** Επιτίθεται με HTTP floods, κατανεμημένες επιθέσεις HTTP GET/POST, κ.λπ. Αυτοί οι τύποι επιθέσεων στοχεύουν συνήθως σε εφαρμογές και υπηρεσίες, κατακλύζοντάς τις με αιτήσεις που είναι δύσκολο να διαχωριστούν από την κανονική κίνηση.

Επίπεδο Παρουσίασης (Presentation Layer): Χρησιμοποιεί ανωμαλίες σε αιτήσεις SSL για να επιβαρύνει τους διακομιστές με μεγάλο υπολογιστικό φόρτο, εκμεταλλευόμενο το κόστος της διαδικασίας SSL handshake.

Επίπεδο Συνεδρίας (Session Layer): Επιτίθεται μέσω επιθέσεων Telnet, εκμεταλλευόμενο αδυναμίες στο πρωτόκολλο Telnet για να αποκλείσει τους χρήστες ή να παρεμποδίσει τις επικοινωνίες.

Επίπεδο Μεταφοράς (Transport Layer): Επιτίθεται με SYN floods, εκμεταλλευόμενο την αδυναμία του πρωτοκόλλου TCP/IP να αντιμετωπίσει μεγάλο αριθμό αιτημάτων και να εξαντλήσει τους πόρους του στόχου.

Επίπεδο Δικτύου (Network Layer): Χρησιμοποιεί ICMP floods, Smurf attacks, κ.λπ., επιδιώκοντας να κατακλύσει το δίκτυο με περισσότερη κίνηση από ό,τι μπορεί να υποστηρίξει.

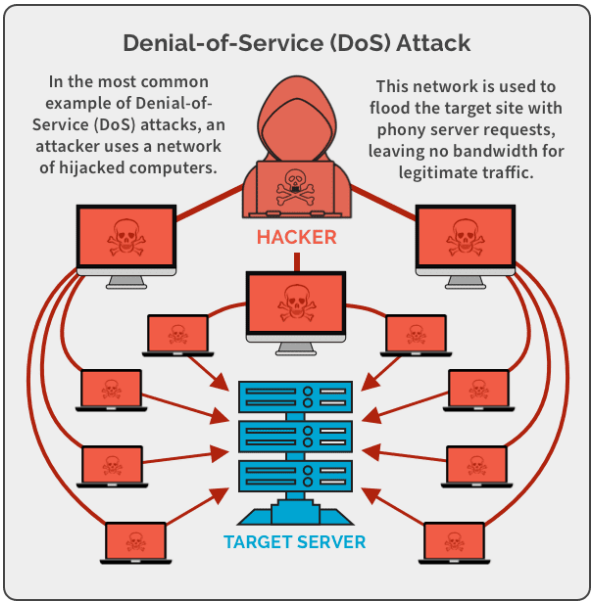

Figure 10: Denial-of-service attack structure (securityboulevard.com)

4.5 SQL Injection

Η επίθεση SQL Injection εκμεταλλεύεται πολλαπλές ευπάθειες στον τρόπο που οι εφαρμογές διαχειρίζονται τα δεδομένα των χρηστών. Αναλυτικά, οι ευπάθειες είναι οι εξής:

Εισαγωγή μη ασφαλών δεδομένων: Η επίθεση SQL Injection εκμεταλλεύεται την είσοδο μη ασφαλών δεδομένων από μη έμπιστες πηγές, όπως την είσοδο από φόρμες, URL παραμέτρους και άλλες πηγές χρήστη. Αυτά τα μη ασφαλή δεδομένα ενσωματώνονται στα SQL ερωτήματα χωρίς καμία προστασία ή επικύρωση, επιτρέποντας στον εισβολέα να εκτελέσει κακόβουλες εντολές SQL.

Κατασκευή δυναμικών ερωτημάτων SQL: Η εφαρμογή δημιουργεί δυναμικά SQL ερωτήματα χωρίς να χρησιμοποιεί ασφαλείς μηχανισμούς για τη

δημιουργία ή εκτέλεση των ερωτημάτων αυτών. Συνήθως, αυτό συμβαίνει μέσω συνένωσης σταθερών ερωτημάτων SQL με δεδομένα που παρέχονται από τον χρήστη, χωρίς ασφάλεια ή προστασία.

Έλλειψη ελέγχου επικύρωσης: Η εφαρμογή δεν εφαρμόζει επαρκείς μηχανισμούς ελέγχου για τα δεδομένα που εισάγονται από τον χρήστη, όπως έλεγχοι ακεραιότητας ή ασφαλή φιλτράρισμα των δεδομένων. Αυτό επιτρέπει στον εισβολέα να εισάγει κακόβουλα δεδομένα που μπορούν να εκτελέσουν επικίνδυνες εντολές SQL.

Αυτές οι ευπάθειες επιτρέπουν στον εισβολέα να εκτελέσει κακόβουλες εντολές SQL, όπως την ανάγνωση ευαίσθητων δεδομένων από μια database, την τροποποίηση των δεδομένων της βάσης δεδομένων, την εκτέλεση διαχειριστικών λειτουργιών στη βάση δεδομένων (όπως την απενεργοποίηση του DBMS) και άλλες επιθέσεις που απειλούν την ασφάλεια και ακεραιότητα των δεδομένων.

4.6 Zero-day exploit

Η εκμετάλλευση μιας zero-day exploit αξιοποιεί την απουσία γνώσης ή της δυνατότητας αντιμετώπισής της από τους αναπτυσσόμενους παρόχους λογισμικού. Αυτές οι ευπάθειες εκμεταλλεύονται διάφορα μέσα για να προκαλέσουν ζημιά ή να κερδίσουν πρόσβαση σε δεδομένα ή συστήματα. Παρακάτω θα εξετάσουμε αναλυτικά τις ευπάθειες που εκμεταλλεύεται ένα zero-day exploit:

Απουσία ενημέρωσης (Lack of patch): Οι zero-day exploits είναι προβλήματα στον κώδικα λογισμικού που δεν έχουν αναγνωριστεί από τους παρόχους λογισμικού, και συνεπώς δεν υπάρχει καμία πατέντα ή λύση για να τις αντιμετωπίσουν.

Ανεπάρκεια προστατευτικών μέτρων: Οι παραδοσιακοί μηχανισμοί ασφάλειας, όπως οι υπογραφές γνωστών απειλών, συχνά δεν είναι αποτελεσματικοί κατά των επιθέσεων zero-day. Αυτό συμβαίνει επειδή δεν υπάρχουν γνωστές υπογραφές που να μπορούν να ανιχνεύσουν αυτές τις

νέες ευπάθειες.

Αποτυχία έκδοσης πατέντας ή λύσης: Οι αναπτυσσόμενοι παρόχοι λογισμικού δεν έχουν προλάβει να εκδώσουν πατέντες ή λύσεις για να επιδιορθώσουν τις ευπάθειες πριν εκμεταλλευτεί κάποιος κακόβουλος την ευπάθεια.

Αναγνωρισμένοι κίνδυνοι: Οι κακόβουλοι εισβολείς αναζητούν συνεχώς νέες τεχνικές για την εκμετάλλευση ευπαθειών. Καθώς οι τεχνολογίες αναπτύσσονται, οι επιθέσεις zero-day μπορούν να εκμεταλλευτούν νέες λειτουργίες ή ευπάθειες που δεν έχουν αναγνωριστεί ακόμη.

Η αντιμετώπιση των zero-day ευπαθειών απαιτεί την υιοθέτηση πολυεπίπεδων προσεγγίσεων που συνδυάζουν τεχνολογικά μέτρα με ενημέρωση και εκπαίδευση χρηστών. Μέσω συστηματικής παρακολούθησης, ενημέρωσης και αναβάθμισης των προστατευτικών μέτρων, οι οργανισμοί μπορούν να μειώσουν τον κίνδυνο εκμετάλλευσης ευπαθειών από τους κακόβουλους εισβολείς.

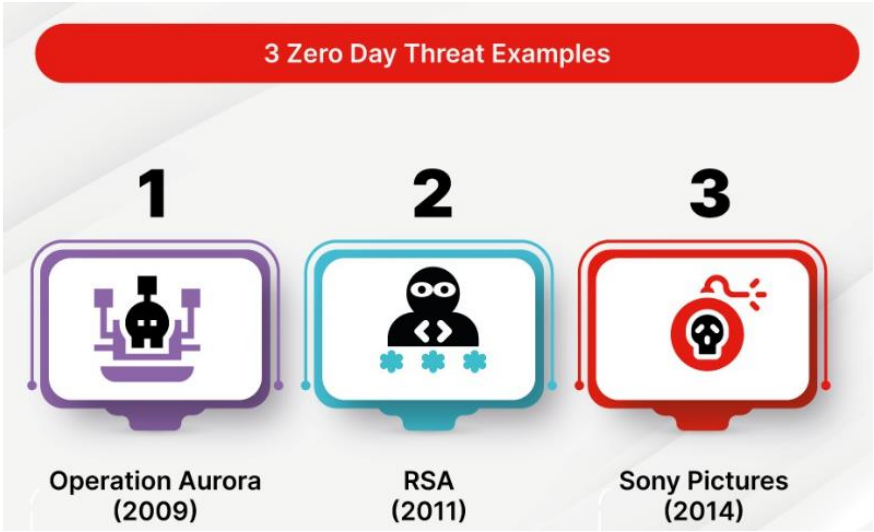

Figure 11: Zero-Day threat examples (Fortinet.com)

Κεφάλαιο 5ο Βιομηχανίες και επιθέσεις-Τρόποι αντιμετώπισης των απειλών

5.1 Επιθέσεις Malware

Η αντιμετώπιση των ιών malware απαιτεί ένα συνδυασμό τεχνικών, πολιτικών και εκπαιδευτικών μέτρων για να προστατεύσετε αποτελεσματικά το δίκτυό σας και τα συστήματά σας. Παρακάτω παρουσιάζονται προτάσεις, βήμα-προς-βήμα για την αντιμετώπιση των ιών malware:

Ενημέρωση του Λογισμικού και των Συσκευών: Η διατήρηση του λογισμικού και των συσκευών, ενημερωμένα με τις τελευταίες εκδόσεις και ενημερώσεις ασφαλείας είναι ζωτικής σημασίας. Αυτό περιλαμβάνει την ενημέρωση του λειτουργικού συστήματος, των προγραμμάτων και των antivirus software.

Εγκατάσταση και Ενημέρωση του antivirus Λογισμικού: Η χρήση antivirus λογισμικού είναι απαραίτητη. Ο χρήστης πρέπει να βεβαιωθεί ότι το λογισμικό είναι ενημερωμένο με τα τελευταία virus signatures και ορισμένα ενσωματωμένα πρόσθετα χαρακτηριστικά ανίχνευσης συμπεριφοράς (detection behavioral features).

Επικοινωνία και Ευαισθητοποίηση: Οι χρήστες πρέπει να εκπαιδεύονται ώστε να αναγνωρίζουν τις φαινομενικά κακόβουλες δραστηριότητες, όπως το άνοιγμα άγνωστων συνημμένων αρχείων ή το click σε ύποπτους συνδέσμους.

Διαχείριση της Προστασίας Πυρκαγιάς (Firewall Protection Management): Η χρήση ενεργού τείχους προστασίας πυρκαγιάς (firewall) είναι αναγκαία για το φιλτράρισμα εισερχόμενης και εξερχόμενης κίνησης στο δίκτυο των χρηστών.

Εφαρμογή Αρχής των Λιγότερων Δικαιωμάτων (Least Privilege Principle): Ο διαχειριστής πρέπει να περιορίζει τα δικαιώματα άλλων χρηστών στα συστήματα, ώστε να περιοριστεί η δυνατότητα ένας ιός malware να

προκαλέσει ζημιά.

Εφαρμογή Φίλτρων Ιστού και Email (Filtering): Ο χρήστης προτρέπεται να χρησιμοποιεί λογισμικό φιλτραρίσματος ιστού και email για τον εντοπισμό και τον αποκλεισμό κακόβουλων ιστοσελίδων και αντικειμένων.

Διαχωρισμός Δικτύου (Network Segmentation): Να διαχωρίζεται το δίκτυο σε επιμέρους τμήματα με τη χρήση διαφορετικών VLAN για να περιοριστεί η εξάπλωση των ιών malware σε περίπτωση που προκύψει μια μόλυνση.

Δημιουργία Εφεδρικών Αντιγράφων και Αποκατάσταση (Backup and Restoration): Να καθορίζεται μια πολιτική αντιγράφων ασφαλείας και αυτή να εφαρμόζεται τακτικά, προκειμένου να υπάρξει αποκατάσταση σε περίπτωση που προκύψει ένας ιός malware.

Παρακολούθηση και Ανάλυση Δραστηριότητας (Activity Monitoring and Analysis): Να χρησιμοποιείται λογισμικό παρακολούθησης και ανάλυσης δραστηριότητας για τον εντοπισμό και την αντιμετώπιση ενδεχόμενων παραβιάσεων ασφαλείας.

Ενημέρωση και Εκπαίδευση: Το προσωπικό της εταιρίας πρέπει να παραμένει ενημερωμένο και εκπαιδευμένο σχετικά με τις τελευταίες απειλές και βέλτιστες πρακτικές ασφαλείας.

Εφαρμόζοντας αυτά τα βήματα, ο χρήστης μπορεί να αυξήσει την ασφάλεια του δικτύου και να προστατεύσει τα συστήματά του από τις απειλές των ιών malware.

5.2 Phishing

Για να προστατευτεί κάποιο από επιθέσεις phishing πρέπει να ακολουθήσει τα εξής [30]:

1. Επαλήθευση Πηγής: Πριν κάνει κλικ ο χρήστης σε οποιοδήποτε σύνδεσμο ή δώσει πληροφορίες, πρέπει να επιβεβαιώσει την αυθεντικότητα του μηνύματος. Πρέπει να ελέγξει το email του αποστολέα, να αναζητήσει τυχόν

ορθογραφικά λάθη ή παράξενες διευθύνσεις URL.

2. Δεν πρέπει να γίνονται κλικ σε Υποψήφιους Συνδέσμους: Καλό είναι να πληκτρολογεί ο χρήστης τις διευθύνσεις URL απευθείας στον φυλλομετρητή του, αντί να κάνει κλικ σε συνδέσμους που του στέλνουν μέσω email.

3. Χρήση Δύο Παραγόντων Αυθεντικοποίησης (2FA): Ακόμα κι αν οι επιτιθέμενοι αποκτήσουν τον κωδικό πρόσβασής του χρήστη, η χρήση 2FA μπορεί να αποτρέψει την πρόσβασή τους στον λογαριασμό του.

4. Ενημερωμένο Λογισμικό: Πρέπει να διατηρείται το λογισμικό ενημερωμένο, καθώς οι ενημερώσεις συχνά περιέχουν επιδιορθώσεις ασφαλείας που μπορούν να προστατεύσουν από τέτοιου είδους επιθέσεις.

5.3 Man-in-the-middle attack

Οι τρόποι αντιμετώπισης από επιθέσεις MitM είναι οι ακόλουθοι [28]:

Χρήση HTTPS: Ο χρήστης πρέπει να βεβαιωθεί ότι οι ιστοσελίδες που επισκέπτεται χρησιμοποιούν το πρωτόκολλο HTTPS, το οποίο κρυπτογραφεί την επικοινωνία του με τον διακομιστή.

Αποφυγή δημόσιων Wi-Fi: Να αποφεύγονται να γίνονται ευαίσθητες συναλλαγές μέσω δημόσιων ή μη ασφαλών δικτύων Wi-Fi. Να χρησιμοποιείται ένα εικονικό ιδιωτικό δίκτυο (VPN) όταν χρειάζεται να γίνει σύνδεση σε δημόσια δίκτυα.

Ασφαλείς συνδέσεις: Ο χρήστης να επικοινωνεί μόνο μέσω εφαρμογών και υπηρεσιών που προσφέρουν ενσωματωμένη κρυπτογράφηση από άκρο σε άκρο.

Ενημέρωση λογισμικού: Ο χρήστης πρέπει να διατηρεί ενημερωμένο το λειτουργικό του σύστημα, τα προγράμματα περιήγησης και τα προγράμματα προστασίας από ιούς, για να προστατευτεί από γνωστές ευπάθειες.

Δύο Παράγοντες Αυθεντικοποίησης (2FA): Η χρήση 2FA προσθέτει ένα επιπλέον επίπεδο ασφάλειας, καθιστώντας δύσκολο για τους επιτιθέμενους

να αποκτήσουν πρόσβαση σε λογαριασμούς ακόμη κι αν έχουν υποκλέψει τον κωδικό πρόσβασης.

Οι επιθέσεις MitM είναι επικίνδυνες επειδή συχνά παραμένουν απαρατήρητες από τα θύματά τους. Ωστόσο, με την υιοθέτηση των κατάλληλων μέτρων ασφαλείας, να μπορεί ο χρήστης να μειώσει σημαντικά τον κίνδυνο αυτής της απειλής

5.4 Denial-of-service attack

Οι επιθέσεις Denial-of-Service (DoS) και Distributed Denial-of-Service (DDoS) αποτελούν σοβαρές απειλές για την ασφάλεια των δικτύων και των πληροφοριακών συστημάτων. Για την αντιμετώπισή τους, υπάρχουν διάφορες στρατηγικές και τεχνολογίες που μπορούν να εφαρμοστούν. Παρακάτω είναι μερικοί από τους βασικούς τρόπους αντιμετώπισης αυτών των επιθέσεων [15]:

1. Ανίχνευση και Παρακολούθηση Κίνησης: Η παρακολούθηση της κίνησης στο δίκτυο μπορεί να βοηθήσει στον εντοπισμό ανώμαλων μοτίβων κίνησης που μπορεί να υποδηλώνουν επίθεση DoS ή DDoS. Βασικό μέσο ανίχνευσης και παρακολούθησης είναι τα εργαλεία SIEM (Security Information and Event Management). Αυτά τα εργαλεία συγκεντρώνουν και αναλύουν δεδομένα από διάφορες πηγές σε πραγματικό χρόνο, εντοπίζοντας ενδεχόμενες επιθέσεις.

2. Φιλτράρισμα Κίνησης: Εργαλεία αναγνώρισης και διαχείρισης κινήσεων με αρνητικό αντίκτυπο για τους χρήστες είναι τα Firewall και IDS/IPS (Intrusion Detection/Prevention Systems). Αυτά τα συστήματα μπορούν να φιλτράρουν κακόβουλη κίνηση και να αποκλείσουν προσπάθειες επίθεσης πριν φτάσουν στον προορισμό τους. Επίσης υπάρχει το Web Application Firewall (WAF) το οποίο προστατεύει τις διαδικτυακές εφαρμογές από κακόβουλη κίνηση, όπως DDoS επιθέσεις που στοχεύουν συγκεκριμένες εφαρμογές.

3. Κατανομή Φορτίου και Υπερμεγέθη Υποδομές: Οι διανομείς φορτίου μπορούν να κατανείμουν την εισερχόμενη κίνηση σε πολλαπλούς διακομιστές, μειώνοντας την πιθανότητα να κατακλυστεί ένας μόνο διακομιστής. Βασικά δίκτυα κατανομής φορτίου είναι τα Content Delivery Networks (CDNs). Αυτά τα δίκτυα βοηθούν στην εξάπλωση της κίνησης σε πολλαπλές γεωγραφικές τοποθεσίες, μειώνοντας την επίπτωση μιας επίθεσης.

4. Εκπαίδευση και Ευαισθητοποίηση Προσωπικού: Το προσωπικό θα πρέπει να είναι κατάλληλα εκπαιδευμένο ώστε να αναγνωρίζει τα σημάδια μιας επίθεσης και να αντιδρά γρήγορα και αποτελεσματικά.

5. Συνεργασία με Παρόχους Υπηρεσιών: Ορισμένοι πάροχοι υπηρεσιών διαδικτύου προσφέρουν εξειδικευμένες υπηρεσίες προστασίας από DDoS επιθέσεις, όπως είναι το φιλτράρισμα της κίνησης πριν αυτή φτάσει στο δίκτυο της επιχείρησης.

6. Κανονιστική Συμμόρφωση και Ασφάλεια: Η δημιουργία και διατήρηση ενός σχεδίου αντιμετώπισης κυβερνοεπιθέσεων, που περιλαμβάνει βήματα αποκατάστασης και επικοινωνίας, είναι κρίσιμη για την αποτελεσματική διαχείριση τέτοιων απειλών.

7. Χρήση Τεχνολογιών Απορρόφησης Επίθεσης: Σε περίπτωση ανίχνευσης επίθεσης, η κίνηση μπορεί να κατευθυνθεί προς μια "μαύρη τρύπα" ή "sinkhole", όπου θα απορροφηθεί χωρίς να επηρεάσει το κύριο δίκτυο.

8. Αναβάθμιση και Ενημέρωση Λογισμικού: Τα συστήματα και τα λογισμικά πρέπει να ενημερώνονται τακτικά για να αντιμετωπίζουν νέες απειλές και να κλείνουν γνωστά κενά ασφαλείας. Η εφαρμογή αυτών των στρατηγικών μπορεί να βοηθήσει σημαντικά στην πρόληψη και την αντιμετώπιση επιθέσεων DoS/DDoS, διασφαλίζοντας την αδιάλειπτη λειτουργία των πληροφοριακών συστημάτων.

5.5 SQL Injection

Για να αντιμετωπίσει κάποιος το SQL Injection πρέπει α δώσει βαρύτητητα στα παρακάτω [6]:

Χρήση Παραμέτρων στις Εντολές SQL: Οι παραμετροποιημένες εντολές (prepared statements) είναι ασφαλέστερες επειδή διαχωρίζουν τον SQL κώδικα από τα δεδομένα εισόδου, αποτρέποντας την εκτέλεση κακόβουλων εντολών.

Επαλήθευση και Καθαρισμός Εισόδου: Πρέπει ο χρήστης να επαληθεύει όλα τα δεδομένα εισόδου των χρηστών για να διασφαλίσει ότι περιέχουν μόνο έγκυρα και αναμενόμενα δεδομένα.

Χρήση ORMs (Object-Relational Mappers): Τα ORM frameworks βοηθούν στην ασφαλή διαχείριση των βάσεων δεδομένων και μειώνουν την ανάγκη για απευθείας γραφή SQL κώδικα, περιορίζοντας τα κενά ασφαλείας.

Περιορισμός Δικαιωμάτων Βάσης Δεδομένων: Ο χρήστης να βεβαιώνεται ότι οι λογαριασμοί που χρησιμοποιούνται από την εφαρμογή για πρόσβαση στη βάση δεδομένων έχουν περιορισμένα δικαιώματα και μόνο στις απαραίτητες ενέργειες.

Χρήση Web Application Firewalls (WAFs): Τα WAFs μπορούν να αναγνωρίζουν και να μπλοκάρουν κακόβουλες προσπάθειες SQL Injection σε πραγματικό χρόνο.

Ενημέρωση και Δοκιμές Ασφαλείας: Πρέπει να διατηρούνται η εφαρμογή και η υποδομή του χρήστη ενημερωμένες με τις τελευταίες διορθώσεις ασφαλείας και να εκτελούνται τακτικές δοκιμές για να εντοπιστούν πιθανές ευπάθειες.

Η καλή πρακτική προγραμματισμού και η εφαρμογή ισχυρών μέτρων ασφαλείας μπορούν να μειώσουν σημαντικά τον κίνδυνο επιθέσεων SQL Injection.

5.6 Zero-day exploit

Η αντιμετώπιση από zero-day exploits επιτυγχάνεται τηρώντας τα ακόλουθα [8]:

Ενημέρωση Λογισμικού: Πρέπει ο χρήστης να διατηρεί όλα τα λογισμικά και τα συστήματα ενημερωμένα με τις τελευταίες ενημερώσεις ασφαλείας (patches). Οι ενημερώσεις συχνά περιέχουν διορθώσεις για γνωστές ευπάθειες.

Χρήση Αμυντικών Τεχνολογιών: Πρέπει να γίνεται χρήση προηγμένων συστημάτων ανίχνευσης εισβολών (IDS/IPS), sandboxing, και λύσεις που βασίζονται σε μηχανική μάθηση για να εντοπιστούν και να αναλυθούν κακόβουλη δραστηριότητα που μπορεί να υποδηλώνει την παρουσία ενός zero-day exploit.

Ασφάλεια σε Βάθος (Defense in Depth): Να γίνει εφαρμογή μιας πολυεπίπεδης προσέγγισης ασφαλείας που περιλαμβάνει διαφορετικά μέτρα προστασίας, όπως firewalls, antivirus, και πολιτικές πρόσβασης, για να μειωθούν οι πιθανότητες επιτυχούς επίθεσης.

Εκπαίδευση Χρηστών: Πρέπει να υπάρχει ενημέρωση και εκπαίδευση των χρηστών σχετικά με τους κινδύνους των zero-day επιθέσεων και τα σημάδια που μπορεί να υποδηλώνουν μια επίθεση.

Συνεργασία με Κοινότητες Ασφαλείας: Οι οργανισμοί μπορούν να συμμετέχουν σε κοινότητες ασφαλείας ή να συνεργάζονται με εξειδικευμένες εταιρείες ασφάλειας για να λάβουν ειδοποιήσεις σχετικά με νέες ευπάθειες και απειλές.

Οι zero-day επιθέσεις αποτελούν μία από τις μεγαλύτερες προκλήσεις στον τομέα της κυβερνοασφάλειας, αλλά με την εφαρμογή των παραπάνω πρακτικών, οι οργανισμοί μπορούν να μειώσουν τον κίνδυνο και να αντιδράσουν γρηγορότερα σε απειλές.

5.7 DNS Tunelling

Το DNS tunneling είναι μια τεχνική που χρησιμοποιείται από επιτιθέμενους

για να διοχετεύουν δεδομένα μέσω του πρωτοκόλλου DNS (Domain Name System), παρακάμπτοντας τείχη προστασίας και άλλα μέτρα ασφαλείας. Η αντιμετώπιση αυτής της απειλής απαιτεί συνδυασμό ανίχνευσης, παρακολούθησης και περιορισμού των επιθέσεων. Ακολουθούν μερικοί βασικοί τρόποι για την αντιμετώπιση των επιθέσεων DNS tunneling [27]:

1. Παρακολούθηση και Ανάλυση Κίνησης DNS: Στη διαδικασία ανίχνευσης και εντοπισμού ανωμαλιών θα πρέπει να χρησιμοποιούνται συστήματα που ανιχνεύουν ασυνήθιστη ή υπερβολική κίνηση DNS, καθώς οι επιθέσεις DNS tunneling συχνά παράγουν ανώμαλα μεγάλους όγκους κίνησης ή επαναλαμβανόμενες ερωτήσεις DNS. Επίσης είναι σημαντικό να γίνεται καταγραφή όλων των αιτημάτων και των απαντήσεων DNS για μετέπειτα ανάλυση, εντοπίζοντας ανώμαλα μοτίβα που μπορεί να υποδεικνύουν κακόβουλη δραστηριότητα.

2. Χρήση Συσκευών DNS Firewall: Τα DNS firewalls μπορούν να φιλτράρουν κακόβουλα ή μη εξουσιοδοτημένα αιτήματα DNS, αποκλείοντας τα αιτήματα που προέρχονται από γνωστούς κακόβουλους domains ή IP διευθύνσεις. Πρέπει να γίνεται εφαρμογή αυστηρών πολιτικών για να επιτρέπονται μόνο τα αιτήματα DNS που είναι απαραίτητα για τις λειτουργίες της επιχείρησης και αποκλείστε άγνωστες ή ύποπτες πηγές.

3. Χρήση DNSSEC (Domain Name System Security Extensions): Το DNSSEC βοηθά στη διασφάλιση ότι οι απαντήσεις DNS προέρχονται από έγκυρες πηγές και δεν έχουν τροποποιηθεί, μειώνοντας έτσι τον κίνδυνο κακόβουλων επιθέσεων που εκμεταλλεύονται το DNS.

4. Ανίχνευση Εξελιγμένων Τεχνικών DNS Tunneling: Εξελιγμένα εργαλεία ανίχνευσης απειλών που βασίζονται στη μηχανική μάθηση ή στην ανάλυση συμπεριφοράς μπορούν να εντοπίσουν σύνθετες επιθέσεις DNS tunneling. Ανάλυση χαρακτηριστικών των DNS queries, όπως το μήκος και η συχνότητα των αιτημάτων, βοηθούν στον εντοπισμό ανωμαλιών.

5. Περιορισμός και Έλεγχος Πρόσβασης στο DNS: Πρέπει να υπάρχει περιορισμός στα DNS queries που μπορούν να εκτελεστούν από συγκεκριμένα συστήματα ή χρήστες, επιτρέποντας μόνο εκείνα που είναι απαραίτητα για την λειτουργία τους. Αντί για δημόσιους DNS servers, πρέπει να χρησιμοποιούνται εσωτερικοί DNS servers που ελέγχονται και διαχειρίζονται, περιορίζοντας έτσι την πιθανότητα κατάχρησης.

6. Εκπαίδευση Προσωπικού: Πρέπει το προσωπικό να εκπαιδεύεται σχετικά με τις απειλές που σχετίζονται με το DNS tunneling και την σημασία της σωστής διαχείρισης των αιτημάτων DNS.

7. Συνεργασία με Παρόχους Υπηρεσιών: Ορισμένοι πάροχοι υπηρεσιών διαδικτύου και ασφάλειας προσφέρουν υπηρεσίες ανίχνευσης και αποκλεισμού DNS tunneling, οι οποίες μπορούν να ενσωματωθούν στο δίκτυο της επιχείρησης.

8. Κανονιστική Συμμόρφωση: Εφαρμογή προτύπων ασφάλειας που απαιτούνται από τη βιομηχανία ή τους κανονισμούς για την προστασία του δικτύου από επιθέσεις μέσω DNS. Η εφαρμογή αυτών των μεθόδων μπορεί να βοηθήσει στην αποτελεσματική προστασία από τις επιθέσεις DNS tunneling, διασφαλίζοντας την ασφάλεια των δεδομένων και την ακεραιότητα των συστημάτων.

Κεφάλαιο 6ο Παραδείγματα επίθεσης

6.1 Επιθέσεις Malware

Ένα παράδειγμα επίθεσης με malware είναι η περίπτωση του WannaCry ransomware το 2017, μια από τις μεγαλύτερες και πιο καταστροφικές επιθέσεις ransomware στην ιστορία. Το WannaCry ήταν ένα κακόβουλο λογισμικό τύπου ransomware, το οποίο κρυπτογραφούσε τα αρχεία σε μολυσμένα συστήματα και απαιτούσε λύτρα (συνήθως σε Bitcoin) για την αποκρυπτογράφηση τους. Το ransomware αυτό εκμεταλλεύτηκε μια ευπάθεια στα λειτουργικά συστήματα Windows, γνωστή ως EternalBlue, η οποία είχε ανακαλυφθεί από την Εθνική Υπηρεσία Ασφαλείας των ΗΠΑ (NSA) και είχε διαρρεύσει από την ομάδα χάκερ Shadow Brokers.

Το WannaCry εκμεταλλεύτηκε μια ευπάθεια στο πρωτόκολλο Server Message Block (SMB) των Windows. Η ευπάθεια αυτή επέτρεπε στους επιτιθέμενους να εκτελέσουν κακόβουλο κώδικα εξ αποστάσεως σε μη ενημερωμένα συστήματα, χωρίς να απαιτείται αλληλεπίδραση από το χρήστη. Αφού το WannaCry μόλυνε έναν υπολογιστή, αναζητούσε άλλες ευάλωτες συσκευές στο ίδιο δίκτυο και προσπαθούσε να τις μολύνει, διαδίδοντας έτσι την επίθεση σε ολόκληρο τον οργανισμό.

Το ransomware κρυπτογραφούσε όλα τα αρχεία στους μολυσμένους υπολογιστές, καθιστώντας τα μη προσβάσιμα στους χρήστες. Στη συνέχεια, εμφάνιζε ένα μήνυμα που απαιτούσε την πληρωμή λύτρων για την αποκρυπτογράφηση των αρχείων. Οι χρήστες λάμβαναν ένα μήνυμα που τους ζητούσε να πληρώσουν λύτρα σε Bitcoin για να λάβουν το κλειδί αποκρυπτογράφησης. Το ποσό αυξανόταν μετά από ένα συγκεκριμένο χρονικό διάστημα και, αν δεν γινόταν η πληρωμή, τα αρχεία απειλούνταν να διαγραφούν μόνιμα. Οι επιδράσεις της επίθεσης ήταν οι ακόλουθες (Chen & Bridges, 2017):

Παγκόσμια Διάδοση: Η επίθεση WannaCry επηρέασε εκατοντάδες χιλιάδες συστήματα σε περισσότερες από 150 χώρες. Έπληξε μεγάλους οργανισμούς,

νοσοκομεία, εταιρείες, και κυβερνητικές υπηρεσίες.

Κρίσιμες Υποδομές: Επηρέασε σοβαρά τις κρίσιμες υποδομές, όπως τα νοσοκομεία του Εθνικού Συστήματος Υγείας (NHS) στο Ηνωμένο Βασίλειο, προκαλώντας ακυρώσεις ραντεβού και καθυστερήσεις στη φροντίδα των ασθενών.

Οικονομικές Ζημιές: Οι εκτιμώμενες οικονομικές ζημίες από την επίθεση ξεπέρασαν τα 4 δισεκατομμύρια δολάρια, συμπεριλαμβανομένων των εξόδων για την αποκατάσταση των συστημάτων και τις απώλειες παραγωγικότητας.

Για να αντιμετωπιστούν επιθέσεις malware σαν το WannaCry πρέπει να ακολουθηθούν οι κάτωθι δράσεις:

Τακτικές Ενημερώσεις Λογισμικού: Η Microsoft είχε κυκλοφορήσει ένα patch για την ευπάθεια EternalBlue, αλλά πολλοί οργανισμοί δεν είχαν ενημερώσει τα συστήματά τους. Επομένως, είναι κρίσιμης σημασίας η τακτική ενημέρωση του λογισμικού και των λειτουργικών συστημάτων.

Αντίγραφα Ασφαλείας: Πρέπει να κρατούνται τακτικά αντίγραφα ασφαλείας των δεδομένων και να γίνεται αποθήκευση σε διαφορετικό φυσικό ή δικτυακό περιβάλλον για να μπορεί να γίνει επαναφορά των αρχείων σε περίπτωση επίθεσης.

Χρήση Anti-Malware Λογισμικού: Ένα αξιόπιστο λογισμικό anti-malware μπορεί να εντοπίσει και να μπλοκάρει πολλές μορφές κακόβουλου λογισμικού πριν αυτές προκαλέσουν ζημιά.

Εκπαίδευση Χρηστών: Οι χρήστες πρέπει να είναι ενημερωμένοι για τις απειλές και να αποφεύγουν το άνοιγμα ύποπτων email και την επίσκεψη σε μη ασφαλείς ιστοσελίδες.

Η επίθεση WannaCry δείχνει πόσο σημαντική είναι η προληπτική ασφάλεια στον κυβερνοχώρο και η ανάγκη για συνεχείς ενημερώσεις και εκπαίδευση.

Ένα πραγματικό παράδειγμα βιομηχανίας που επλήγη σοβαρά από το WannaCry ransomware είναι το Εθνικό Σύστημα Υγείας (NHS) του Ηνωμένου

Βασιλείου. Η επίθεση αυτή είχε καταστροφικές συνέπειες για το σύστημα υγείας της χώρας, αναδεικνύοντας τις ευπάθειες που υπάρχουν στις υποδομές των κρίσιμων υπηρεσιών. Στη συνέχεια θα δοθούν λεπτομέρειες από την επίθεση που έγινε στο NHS.

Η επίθεση σημειώθηκε στις 12 Μαΐου 2017. Περισσότερα από 80 νοσοκομεία και οργανισμοί υγειονομικής περίθαλψης σε όλη τη χώρα επλήγησαν, προκαλώντας σοβαρές διακοπές στη λειτουργία τους. Πολλά από τα υπολογιστικά συστήματα των νοσοκομείων κρυπτογραφήθηκαν, με αποτέλεσμα οι επαγγελματίες υγείας να χάσουν πρόσβαση σε αρχεία ασθενών, ιατρικά ιστορικά, και πληροφορίες για τις ιατρικές εξετάσεις. Λόγω της επίθεσης, πολλά προγραμματισμένα ραντεβού και χειρουργικές επεμβάσεις έπρεπε να ακυρωθούν ή να αναβληθούν. Οι ασθενείς που χρειάζονταν άμεση φροντίδα αντιμετώπισαν σοβαρές καθυστερήσεις. Η επίθεση είχε μεγάλο οικονομικό αντίκτυπο, όχι μόνο λόγω της άμεσης διατάραξης των υπηρεσιών, αλλά και των εξόδων που απαιτήθηκαν για την αποκατάσταση των συστημάτων και την ενίσχυση της ασφάλειας στο μέλλον. Το κόστος αποκατάστασης εκτιμήθηκε σε εκατομμύρια λίρες.

Η ευπάθεια του NHS προήλθε κυρίως από την χρήση παλαιών λειτουργικών συστημάτων, όπως τα Windows XP, τα οποία δεν υποστηρίζονταν πλέον από τη Microsoft και δεν λάμβαναν τακτικές ενημερώσεις ασφαλείας. Αν και η Microsoft είχε κυκλοφορήσει ένα έκτακτο patch για την ευπάθεια EternalBlue λίγες εβδομάδες πριν από την επίθεση, πολλά από τα συστήματα του NHS δεν είχαν ενημερωθεί εγκαίρως.

Η επίθεση στο NHS ανέδειξε την ανάγκη για άμεσες και συνεχείς ενημερώσεις ασφαλείας, ειδικά σε κρίσιμους τομείς όπως η υγειονομική περίθαλψη. Επιπλέον, η επίθεση κατέστησε σαφές ότι η εξάρτηση από παλαιά και μη υποστηριζόμενα λογισμικά μπορεί να έχει καταστροφικές συνέπειες. Μετά την επίθεση, το NHS υιοθέτησε νέες πολιτικές ασφαλείας, όπως η γρήγορη εφαρμογή ενημερώσεων και η βελτίωση της εκπαίδευσης του προσωπικού σε θέματα κυβερνοασφάλειας, ώστε να αποφευχθούν

παρόμοιες επιθέσεις στο μέλλον [7].

6.2 Phishing

Ένα χαρακτηριστικό παράδειγμα κυβερνοεπίθεσης phishing είναι η επίθεση που σημειώθηκε το 2016 κατά της εταιρείας John Podesta, ο οποίος ήταν ο επικεφαλής της προεκλογικής εκστρατείας της Hillary Clinton.

Τον Μάρτιο του 2016, ο Podesta έλαβε ένα email που φαινόταν να προέρχεται από την Google. Το email ανέφερε ότι κάποιος είχε προσπαθήσει να εισέλθει στον λογαριασμό του και τον παρότρυνε να αλλάξει τον κωδικό πρόσβασής του για λόγους ασφαλείας. Το email περιείχε έναν σύνδεσμο που φαινόταν να οδηγεί στη σελίδα αλλαγής κωδικού της Google, αλλά στην πραγματικότητα ήταν ένας κακόβουλος σύνδεσμος που οδηγούσε σε μια ψεύτικη σελίδα [10].

Ο Podesta, πιστεύοντας ότι το email ήταν γνήσιο, πάτησε τον σύνδεσμο και εισήγαγε τα στοιχεία του (όνομα χρήστη και κωδικό πρόσβασης) στη ψεύτικη σελίδα. Με αυτόν τον τρόπο, οι επιτιθέμενοι απέκτησαν πρόσβαση στον προσωπικό του λογαριασμό email.

Οι επιτιθέμενοι χρησιμοποίησαν τον κλεμμένο λογαριασμό email για να αποκτήσουν πρόσβαση σε ευαίσθητες πληροφορίες που σχετίζονταν με την προεκλογική εκστρατεία της Hillary Clinton. Το περιεχόμενο των emails του Podesta δημοσιεύτηκε αργότερα από τον ιστότοπο Wikileaks, προκαλώντας σοβαρά πλήγματα στην εκστρατεία της Clinton.

Η επίθεση στον Podesta δείχνει πόσο εύκολο είναι για μια επίθεση phishing να παραπλανήσει ακόμη και άτομα που είναι καλά ενημερωμένα. Υπογραμμίζει επίσης τη σημασία της προσοχής στη λεπτομέρεια και της επαλήθευσης των συνδέσμων και των αποστολέων πριν γίνει εισαγωγή ευαίσθητων στοιχείων.

Για να προστατευθεί κάποιος από τέτοιες επιθέσεις, είναι σημαντικό να εκπαιδεύεται το προσωπικό σχετικά με τις τεχνικές phishing, να χρησιμοποιούνται εργαλεία για την ανίχνευση κακόβουλων emails, και να εφαρμόζεται αυστηρός έλεγχος ταυτότητας, όπως η χρήση δύο παραγόντων

ταυτοποίησης (2FA)[4].

6.3 Man-in-the-middle attack

Ας υποθέσουμε ότι η Alice θέλει να επικοινωνήσει με τον Bob. Ανάμεσα στην Alice και τον Bob βρίσκεται η Mallory, που θέλει να παρακολουθήσει τη συνομιλία και πιθανώς να την παραποιήσει (χωρίς να το γνωρίζουν η Alice και ο Bob).

Στην αρχή της επικοινωνίας, η Alice ζητά από τον Bob να στείλει το δημόσιο κλειδί του. Αν ο Bob στείλει το δημόσιο κλειδί του στην Alice, η Mallory μπορεί να το υποκλέψει, εκκινώντας έτσι μια επίθεση "Man-in-the-middle". Η Mallory στέλνει ένα πλαστό μήνυμα στην Alice, αντικαθιστώντας το δημόσιο κλειδί του Bob με το δικό της δημόσιο κλειδί.

Η Alice λαμβάνει το πλαστό κλειδί της Mallory, το οποίο θεωρεί ότι ανήκει στον Bob. Κρυπτογραφεί το μήνυμα με το πλαστό κλειδί της Mallory και το στέλνει στον Bob. Η Mallory υποκλέπτει αυτό το μήνυμα, το αποκρυπτογραφεί (αν θέλει το παραποιεί) και το στέλνει κρυπτογραφημένο με το δημόσιο κλειδί του Bob, στον Bob. Όταν ο Bob λαμβάνει το πλαστογραφημένο μήνυμα από την Mallory, το αποκρυπτογραφεί χρησιμοποιώντας το ιδιωτικό του κλειδί, και θεωρεί ότι το μήνυμα έχει σταλθεί από την Alice (αγνοώντας ότι η Mallory έχει υποκλέψει και ίσως έχει παραποιήσει το μήνυμα της Alice).

Alice sends a message to Bob, which is intercepted by Mallory:

Alice "Hello Bob, I'm Alice. Give me your public key." --> Mallory Bob

Mallory forwards the message to Bob. Bob is unaware that this message did not come from Alice:

Alice Mallory "Hello Bob, I'm Alice. Give me your public key." --> Bob

Bob responds by sending his public key:

Alice Mallory <--[Bob's Public Key] Bob

Mallory replaces Bob's key with her own public key and sends it to Alice, claiming it's Bob's:

Alice <--[Mallory's Public Key] Mallory Bob

Alice encrypts the message with Mallory's key, which she believes is Bob's, assuming only Bob can decrypt it with his private key:

Alice "We'll meet at the bus stop!" [encrypted with Mallory's public key] --> Mallory Bob

Since the message was encrypted with Mallory's key, Mallory decrypts it, reads it, potentially alters it, and sends it encrypted with Bob's public key to Bob:

Alice Mallory "We'll meet at the city center!" [encrypted with Bob's public key] --> Bob

Bob considers the message to be from Alice since the communication with Alice is encrypted and secure.

Το παραπάνω παράδειγμα, δείχνει πως μια man-in-the-middle επίθεση μπορεί να επέμβει και να παραποιήσει την επικοινωνία μεταξύ δύο μερών, οδηγώντας σε πιθανώς επιβλαβείς συνέπειες.

6.4 Denial-of-service attack

Ένα πραγματικό και πολύ γνωστό παράδειγμα επίθεσης Denial-of-Service (DoS) είναι η επίθεση που έγινε τον Οκτώβριο του 2016 εναντίον της εταιρείας Dyn, ενός από τους μεγαλύτερους παρόχους υπηρεσιών DNS.
Στις 21 Οκτωβρίου 2016, η Dyn δέχθηκε μια μαζική επίθεση Distributed Denial-of-Service (DDoS), η οποία χρησιμοποιούσε το κακόβουλο λογισμικό Mirai. Η επίθεση εκμεταλλεύτηκε ένα botnet, δηλαδή ένα δίκτυο από χιλιάδες μολυσμένες συσκευές IoT (Internet of Things), όπως κάμερες

ασφαλείας και routers, για να κατακλύσει τους DNS servers της Dyn με τεράστιο όγκο αιτημάτων [14].

Η επίθεση προκάλεσε την προσωρινή διακοπή της λειτουργίας πολλών μεγάλων διαδικτυακών υπηρεσιών και ιστοσελίδων, συμπεριλαμβανομένων των Twitter, Reddit, Netflix, Airbnb, GitHub, και Spotify. Οι χρήστες σε πολλές περιοχές του κόσμου δεν μπορούσαν να έχουν πρόσβαση σε αυτές τις υπηρεσίες για αρκετές ώρες, καθώς οι DNS servers της Dyn αδυνατούσαν να διαχειριστούν τον τεράστιο όγκο των αιτημάτων.

Η επίθεση στη Dyn υπογραμμίζει την ευπάθεια των βασικών υποδομών του Διαδικτύου σε επιθέσεις DDoS. Οι επιθέσεις αυτές μπορούν να προκαλέσουν εκτεταμένες διακοπές στη λειτουργία των διαδικτυακών υπηρεσιών, επηρεάζοντας εκατομμύρια χρήστες.

Για την προστασία από τέτοιες επιθέσεις, είναι σημαντικό να χρησιμοποιούνται τεχνολογίες όπως τα Content Delivery Networks (CDNs), τα συστήματα ανίχνευσης και αποτροπής εισβολών (IDS/IPS), και τα συστήματα διανομής φορτίου (load balancers). Επιπλέον, η εφαρμογή πρακτικών ασφάλειας στα IoT συστήματα είναι κρίσιμη για την αποτροπή δημιουργίας και εκμετάλλευσης botnets όπως το Mirai [9].

6.5 SQL Injection

Αυτό το παράδειγμα δείχνει πώς ο κώδικας C# δημιουργεί δυναμικά ένα ερώτημα SQL για αναζήτηση αντικειμένων με βάση ένα καθορισμένο όνομα. Ο κώδικας δημιουργεί το ερώτημα SQL δυναμικά συνδυάζοντας σταθερό κείμενο με τιμές εισόδου του χρήστη. Αυτό μπορεί να οδηγήσει σε εκτέλεση μη ασφαλούς ερωτήματος SQL. Αν ο εισβολέας εισάγει κακόβουλο κώδικα SQL ως τιμή εισόδου, μπορεί να επηρεάσει το ερώτημα SQL και να έχει πρόσβαση σε δεδομένα που δεν θα έπρεπε να έχει. Η χρήση παραμετροποιημένων ερωτημάτων SQL μπορεί να προστατεύσει από αυτήν την επίθεση.

Το παρακάτω κομμάτι κώδικα C# δημιουργεί δυναμικά και εκτελεί

ένα ερώτημα SQL που αναζητά αντικείμενα που ταιριάζουν με ένα καθορισμένο όνομα. Το ερώτημα περιορίζει τα αντικείμενα που εμφανίζονται σε αυτά όπου ο ιδιοκτήτης ταιριάζει με το όνομα χρήστη του τρέχοντος αυθεντικοποιημένου χρήστη.

```
string userName = ctx.getAuthenticatedUserName();
string query = "SELECT * FROM items WHERE owner = '"
        + userName + "' AND itemname = '"
        + ItemName.Text + "'";
sda = new SqlDataAdapter(query, conn);
DataTable dt = new DataTable();
sda.Fill(dt);
```

6.6 Zero-day exploit

Ένα από τα πιο διάσημα παραδείγματα κυβερνοεπίθεσης με χρήση zero-day exploit είναι η επίθεση με το κακόβουλο λογισμικό Stuxnet που ανακαλύφθηκε το 2010. Το Stuxnet ήταν ένα εξαιρετικά προηγμένο κακόβουλο λογισμικό (worm) που δημιουργήθηκε με στόχο να πλήξει συγκεκριμένα βιομηχανικά συστήματα. Συγκεκριμένα, σχεδιάστηκε για να επιτεθεί σε συστήματα SCADA (Supervisory Control and Data Acquisition) που χρησιμοποιούνταν για τον έλεγχο των φυγοκεντρητών εμπλουτισμού ουρανίου στις πυρηνικές εγκαταστάσεις του Ιράν.

Το Stuxnet εκμεταλλεύτηκε πολλαπλά zero-day exploits σε λογισμικό της Microsoft Windows, τα οποία δεν είχαν αποκαλυφθεί ή επιδιορθωθεί από τη Microsoft τη στιγμή που χρησιμοποιήθηκαν. Αυτά τα zero-day exploits επέτρεψαν στο Stuxnet να διεισδύσει στα συστήματα των στόχων του χωρίς να ανιχνευτεί και να διαδοθεί σε άλλα συστήματα μέσω αφαιρούμενων

συσκευών αποθήκευσης, όπως USB drives.

Μόλις εγκατασταθεί σε ένα σύστημα, το Stuxnet αναζητούσε συγκεκριμένους τύπους προγραμματιζόμενων λογικών ελεγκτών (PLCs) της Siemens που χρησιμοποιούνταν για τον έλεγχο των φυγοκεντρητών. Αν βρισκόταν σε ένα σύστημα που χρησιμοποιούσε αυτά τα PLCs, άλλαζε τις παραμέτρους λειτουργίας των φυγοκεντρητών, προκαλώντας τους βλάβες ενώ ταυτόχρονα έστελνε ψεύτικα δεδομένα στο σύστημα παρακολούθησης, ώστε να μην ανιχνευτεί η ζημιά [26].

Το Stuxnet θεωρείται η πρώτη ψηφιακή απειλή που προκάλεσε φυσική καταστροφή και επηρέασε σημαντικά το πυρηνικό πρόγραμμα του Ιράν, επιβραδύνοντας την παραγωγή εμπλουτισμένου ουρανίου. Η επίθεση είχε ευρείες γεωπολιτικές επιπτώσεις και θεωρείται ένα σημείο καμπής στον κυβερνοπόλεμο.

Η επίθεση με το Stuxnet αναδεικνύει τους κινδύνους που ενέχουν τα zero-day exploits, τα οποία μπορούν να χρησιμοποιηθούν για την εκτέλεση εξαιρετικά στοχευμένων και καταστροφικών επιθέσεων. Υπογραμμίζει επίσης τη σημασία της ταχείας αναγνώρισης και επιδιόρθωσης των ευπαθειών λογισμικού, καθώς και της εφαρμογής ισχυρών μέτρων ασφάλειας σε κρίσιμες υποδομές.

Επίσης, δείχνει την ανάγκη για αυξημένη παρακολούθηση και έλεγχο των βιομηχανικών συστημάτων, τα οποία μπορούν να γίνουν στόχος κακόβουλων επιθέσεων που εκμεταλλεύονται άγνωστες ευπάθειες [12].

6.7 DNS Tunelling

Ένα χαρακτηριστικό παράδειγμα κυβερνοεπίθεσης μέσω DNS tunneling είναι η επίθεση που έγινε το 2018 σε μια μεγάλη τράπεζα στις Ηνωμένες Πολιτείες, γνωστή ως η "Sea Turtle" επίθεση. Η επίθεση "Sea Turtle" ήταν μια εξελιγμένη εκστρατεία κυβερνοεπιθέσεων που στόχευε κυβερνητικές υπηρεσίες, υπηρεσίες εθνικής ασφάλειας και εταιρείες σε αρκετές χώρες της Μέσης Ανατολής και της Βόρειας Αφρικής, καθώς και σε ορισμένες στην Ευρώπη και στις Ηνωμένες Πολιτείες.

Η επίθεση χρησιμοποιούσε DNS tunneling για να αποκτήσει πρόσβαση σε εσωτερικά δίκτυα των θυμάτων και να κλέψει ευαίσθητα δεδομένα. Η τεχνική DNS tunneling επέτρεπε στους επιτιθέμενους να στέλνουν δεδομένα μέσα από τις ερωτήσεις και τις απαντήσεις DNS, παρακάμπτοντας τα τείχη προστασίας και άλλα μέτρα ασφαλείας που δεν ανίχνευαν την κακόβουλη δραστηριότητα μέσα από το κανονικό DNS traffic.

Οι επιτιθέμενοι πρώτα απέκτησαν πρόσβαση στους διακομιστές DNS των στόχων μέσω προηγούμενων επιθέσεων phishing ή εκμεταλλευόμενοι ευπάθειες στα συστήματα. Μόλις απέκτησαν πρόσβαση, επανέγραψαν τις DNS εγγραφές (DNS hijacking) ώστε να ανακατευθύνουν την κίνηση των θυμάτων σε ψεύτικους διακομιστές που ελέγχονταν από τους επιτιθέμενους. Από εκεί, χρησιμοποιούσαν το DNS tunneling για να εξάγουν δεδομένα και να επικοινωνούν με το εσωτερικό δίκτυο των θυμάτων χωρίς να ανιχνευθούν. Τα δεδομένα κωδικοποιούνταν στις ερωτήσεις DNS, οι οποίες φαινομενικά φαίνονταν κανονικές, αλλά στην πραγματικότητα περιείχαν τα κλεμμένα δεδομένα που διοχετεύονταν πίσω στους επιτιθέμενους [1].

Η επίθεση αυτή είχε σοβαρές συνέπειες για τις επιχειρήσεις και τις κυβερνητικές υπηρεσίες που επηρεάστηκαν. Οι επιτιθέμενοι κατάφεραν να κλέψουν ευαίσθητα δεδομένα και να παραμείνουν ανιχνεύσιμοι για μεγάλο χρονικό διάστημα, καθώς το DNS tunneling ήταν δύσκολο να εντοπιστεί από τα παραδοσιακά συστήματα ασφάλειας.

Η επίθεση "Sea Turtle" αναδεικνύει την ευπάθεια των συστημάτων που βασίζονται στο DNS και τη σημασία της παρακολούθησης και της ανάλυσης της κίνησης DNS. Επισημαίνει επίσης την ανάγκη για πιο εξελιγμένα εργαλεία ανίχνευσης που μπορούν να εντοπίζουν κακόβουλη δραστηριότητα που χρησιμοποιεί τεχνικές DNS tunneling.

Οι οργανισμοί πρέπει να είναι σε θέση να εντοπίζουν ανώμαλες δραστηριότητες στο DNS, να χρησιμοποιούν συστήματα παρακολούθησης σε πραγματικό χρόνο και να εκπαιδεύουν το προσωπικό τους για να

κατανοούν αυτές τις απειλές. Επιπλέον, η τακτική αναθεώρηση και προστασία των DNS servers είναι κρίσιμη για την αποτροπή τέτοιων επιθέσεων.

Κεφάλαιο 7ο Συγκριτική αξιολόγηση εμπορικών και ανοικτού κώδικα λύσεων

Στην εποχή της κυβερνοεπίθεσης ως σύνθετου μέσου ληστείας, η αύξηση των φαινομένων της εξαπάτησης και πολυάριθμων εργαλείων των hacker μας κάνει υπερβολικά ευάλωτους αν δεν χρησιμοποιήσουμε και εμείς τα κατάλληλα για την προστασία μας αμυντικά λογισμικά. Υπάρχει πληθώρα εργαλείων για όλα τα είδη των επιθέσεων, ωστόσο η κρίσιμη απορία είναι πόση διαφορά έχει ένα δωρεάν λογισμικό, συγκριτικά με τα εμπορικά και αν τα επιπλέον χρήματα αξίζουν την ασφάλεια που μας προσφέρουν. Στο παρόν κεφάλαιο θα εξετάσουμε τη σύγκριση μεταξύ δωρεάν και εμπορικών λύσεων ασφαλείας, εστιάζοντας στα πλεονεκτήματα και τις αδυναμίες του κάθε τύπου. Θα αναλύσουμε τις βασικές λειτουργίες που προσφέρουν τα δωρεάν εργαλεία, όπως η αναγνώριση κακόβουλου λογισμικού και προστασία από ιούς, σε σύγκριση με τις πιο προηγμένες και εξειδικευμένες δυνατότητες που παρέχουν οι εμπορικές λύσεις, όπως η προστασία σε πραγματικό χρόνο, η ανίχνευση συνθετικών επιθέσεων, η ανάλυση συμπεριφοράς και η υποστήριξη πελατών.

7.1 Malware

Οι επιθέσεις Malware μπορούν να αντιμετωπιστούν είτε με κάποιο open source software, είτε με κάποια εμπορική επί πληρωμή λύση. Στην προκειμένη περίπτωση, θα αναλύσουμε το **ClamAV** (open source) σε σύγκριση με το **Norton** (εμπορική επί πληρωμή λύση). Το ClamAV, είναι ένα δωρεάν open source λογισμικό. Ο κύριος σκοπός του είναι να ανιχνεύσει διάφορους τύπους Malware λογισμικού, όπως worms, trojans και άλλες πιθανές απειλές. Το ClamAV δημιουργήθηκε από τον Tomasz Kojm στο Πολυτεχνείο της Βαρσοβίας το 2001. Το λογισμικό, είναι ένα CLI (Command Line Interpreter) και σαρώνει το σύστημα, δηλαδή αρχεία και φακέλους και χρησιμοποιεί φίλτρα για emails. Ένα σημαντικό του μειονέκτημα, είναι ότι η προστασία σε πραγματικό χρόνο είναι διαθέσιμη μόνο σε λειτουργικά Linux και όχι και σε Windows. Αντίθετα, ένα μεγάλο πλεονέκτημα είναι πως το λογισμικό προσφέρει συνεχείς ενημερώσεις. Λαμβάνοντας υπόψιν το παραπάνω πλεονέκτημα, το ClamAv, είναι ικανό να ανιχνεύει άμεσα πραγματικές απειλές. Το software αποτελείται από 3 βασικά χαρακτηριστικά:

- **ClamAV engine**: Το λογισμικό που ανιχνεύει το Malware λογισμικό
- **ClamAV database**: Η βάση δεδομένων που αποθηκεύονται οι υπογραφές των ιών

- **ClamAV frontend**: Οι εφαρμογές που προσφέρονται για τους χρήστες

Συμπερασματικά, το ClamAV είναι μια αρκετά καλή λύση κατά των Malware επιθέσεων καθώς το λογισμικό σαρώνει και ανιχνεύει εκατομμύρια ιούς σε αρχεία, φακέλους αλλά και σε μακροεντολές Microsoft Office. Ωστόσο, η προστασία σε πραγματικό χρόνο δεν είναι διαθέσιμη σε Windows και άλλα λειτουργικά συστήματα, αλλά μόνο σε Linux [42].

Μία εμπορική λύση, είναι αυτή που προσφέρεται από την εταιρεία **Norton**. Το **Norton Antivirus** προσφέρει ολοκληρωμένη προστασία από Malware λογισμικά σε πραγματικό χρόνο. Το λογισμικό περιλαμβάνει χαρακτηριστικά όπως firewall και VPN κάνοντας το προϊόν ελκυστικό για τους χρήστες. Ένα επιπλέον πλεονέκτημά του, είναι πως είναι εύκολο στη χρήση και έχει ένα εύκολο για τον χρήστη περιβάλλον το οποίο καθιστά το Norton εύκολο σε χρήση από άτομα χωρίς τεχνικές γνώσεις. Επίσης, το συγκεκριμένο antivirus, δεν επιβραδύνει το λειτουργικό σύστημα κατά την διάρκεια της λειτουργίας του και προσφέρει συχνές ενημερώσεις στους κατόχους του. Ωστόσο, ένα από τα μειονεκτήματά του είναι το αρκετά υψηλό κόστος το οποίο μπορεί να υπερβεί ακόμα και τα 100 ευρώ ετησίως σε ένα Premium πρόγραμμα. Ακόμη ένα μειονέκτημα είναι η ορισμένες στιγμές κατανάλωση πόρων, η οποία μπορεί να επηρεάσει σημαντικά την ταχύτητα, ειδικά σε παλαιούς υπολογιστές. Αρνητική θα μπορούσε να χαρακτηριστεί και η συνεχής ζήτηση για ενημερώσεις, πράγμα που προϋποθέτει συνεχείς συνδέσεις στο διαδίκτυο. Τέλος, συμπεραίνουμε πως το Norton Antivirus είναι ένα αποτελεσματικό λογισμικό κατά των ιών, προσφέροντας ολοκληρωμένη προστασία του Η/Υ, κοστίζοντας όμως αρκετά χρήματα στον χρήστη του.

Στο γράφημα [13], φαίνεται το market share των 2 παραπάνω λύσεων που συγκρίνονται. Γίνεται εύκολα κατανοητό πως το μεγαλύτερο πλήθος κόσμου προτιμάει την εμπορική λύση, αντί αυτής του ανοικτού κώδικα.

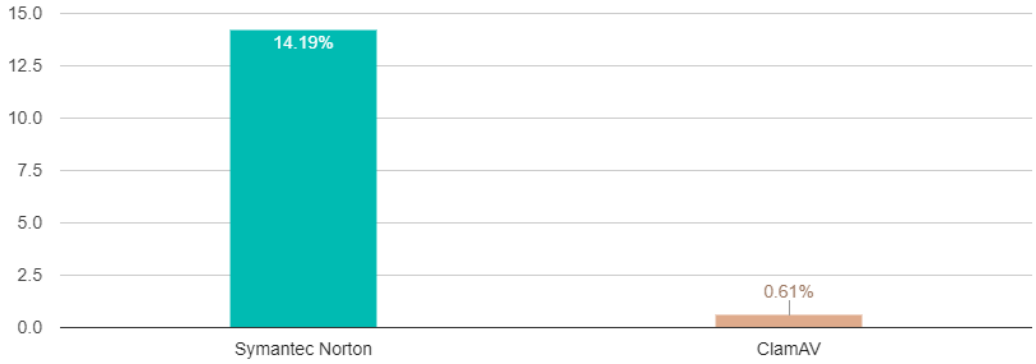

Figure 12: Market share comparison (6sense.com)

7.2 Phishing

Στην περίπτωση των επιθέσεων Phishing, οι χρήστες μπορούν μέσω του free community **PhishTank**, να κάνουν track κάποιο site που μπορεί να τους φανεί επικίνδυνο. Ο χρήστης, μπαίνοντας στο site phishtank.org, μπορεί να κάνει έλεγχο του ιστοτόπου για τον οποίο είναι υποψιασμένος ότι μπορεί να ελλοχεύει κινδύνους.

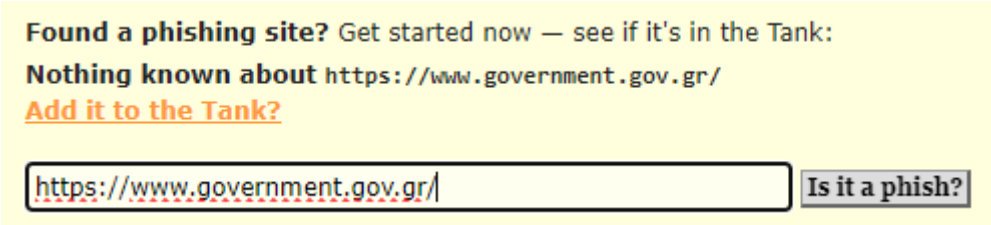

Figure 13: PhishTank search (phishtank.org)

Αντίθετα με το **PhishTanks**, μια επί πληρωμή λύση προσφέρεται από την **Proofpoint**. Η εταιρία προσφέρει λογισμικό με το ίδιο όνομα το οποίο προστατεύει από κακόβουλο λογισμικό όπως το Phishing. Το software αναγνωρίζει και αποκρούει απειλές μέσω email, αναλύοντας το περιεχόμενό τους με σκοπό να αναγνωρίσει κακόβουλη δραστηριότητα. Πλεονεκτήματα του λογισμικού Proofpoint, είναι η εξειδίκευση στην προστασία του περιεχομένου των emails. Αυτό επιτυγχάνεται με εργαλεία που βοηθούν τους χρήστες να καταλάβουν πότε κάποια ηλεκτρονική αλληλογραφία εμπεριέχει κινδύνους. Επίσης, έχοντας αναπτύξει αντίστοιχους μηχανισμούς μπορεί να αναγνωρίσει επιθέσεις που δεν εντοπίζονται με παραδοσιακές λύσεις. Αυτό επιτυγχάνεται μέσω κάποιων μηχανισμών ανάλυσης συμπεριφοράς οι οποίοι έχουν αναπτυχθεί από την εταιρία. Ωστόσο, κάποια μειονεκτήματα του συγκεκριμένου λογισμικού

μπορεί να σταθούν εμπόδιο για κάποιον χρήστη ώστε να το χρησιμοποιήσει. Ένα από αυτά είναι το κόστος, το οποίο μπορεί να αγγίξει ακόμα και τις 30.000 ευρώ, ξεκινώντας από 14.000 για μια εταιρία που θα χρησιμοποιεί ως και 200 άδειες. Μπορεί να φτάσει και τις 50.000 ευρώ για πάνω από 1000 άδειες. Ένα ακόμα μειονέκτημα είναι η διαχείριση του Proofpoint η οποία πρέπει να γίνεται αποκλειστικά από προσωπικό με γνώσεις πάνω στο αντικείμενο. Τέλος, η εταιρία παρέχει προστασία μόνο από Phishing επιθέσεις μέσω emails και όχι σε κάποια άλλη περιοχή του λειτουργικού, σε αντίθεση με το Norton για το οποίο μιλήσαμε πάνω. [43].

7.3 Man-in-the-Middle

Μια Man-in-the-Middle επίθεση συμβαίνει όταν ένας χρήστης (επιτιθέμενος) παρεμβάλλεται και μπορεί να τροποποιεί την επικοινωνία μεταξύ 2 άλλων χρηστών. Ένα open source λογισμικό που βοηθάει στην αντιμετώπιση των επιθέσεων αυτών, είναι το **Wireshark**. Μέσα από το Wireshark μπορεί να γίνει:

- **Εντοπισμός ύποπτων κινητών δεδομένων**: Το Wireshark μπορεί να συλλάβει και να αναλύσει πακέτα στα οποία μπορεί να ανιχνεύσει ασυνήθιστα πρότυπα τα οποία μπορεί να ελλοχεύουν επιθέσεις MitM.
- **Εντοπισμός μη κρυπτογραφημένων δεδομένων**: Εξετάζει τα δεδομένα που έχει συλλέξει και μέσα από αυτά μπορεί να αποκαλύψει ευαίσθητα δεδομένα που κυκλοφορούν χωρίς κρυπτογράφηση.
- **Εντοπισμός συνεδριών και επαληθεύσεις**: Το Wireshark μέσω ανάλυσης των συνεδριών του δικτύου και μπορεί να εντοπίσει ασυνήθιστες συμπεριφορές.
- **Ανίχνευση υποκρίσεων δικτύου**: Μπορούν να ανιχνευθούν υποκρισίες που σχετίζονται με την προσβασιμότητα των διακομιστών και την τροποποίηση των δεδομένων.

Το Wireshark διατίθεται στους χρήστες δωρεάν και είναι λογισμικό ανοικτού κώδικα. Επίσης, μπορεί να φιλτράρει τα δεδομένα που λαμβάνει μέσω φίλτρων που χρησιμοποιεί ο χρήστης αλλά και παρουσιάζει γραφικά τα δεδομένα που λαμβάνονται.

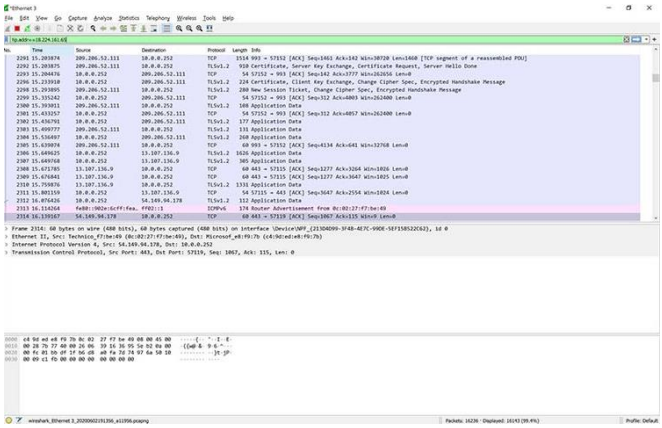

Figure 14: Γραφική αναπαράσταση στο Wireshark (comptia.org)

Για να χρησιμοποιήσει όμως κάποιος το συγκεκριμένο software, θα πρέπει να έχει καλές γνώσεις πάνω στη λειτουργία των δικτύων με σκοπό να μπορέσει να κάνει χρήση του Wireshark. Ακόμη, το software δε παρέχει ειδοποιήσεις σε περίπτωση κάποιας επίθεσης και προσφέρει περιορισμένη δυνατότητα πληροφόρησης για κάποια πιθανή κρυπτογραφημένη πληροφορία σε συνδέσεις HTTPS. Ένα ακόμα αρνητικό είναι πως δε μπορεί να επιβεβαιώσει αν μια IP είναι πραγματική ή είναι πλαστή (δηλαδή αναφέρεται σε μια διεύθυνση IP που έχει τροποποιηθεί για να παραπλανήσει τους χρήστες). Μια τεχνική πλαστής IP είναι το **IP Spoofing** που ο επιτιθέμενος τροποποιεί την IP ώστε να φαίνεται νόμιμη και αξιόπιστη [58].

Σε αντίθεση με το free Wireshark, το **Cloudflare** παρέχει NaaS (Network-as-a-Service) λύσεις. Οι λύσεις αυτές ξεκινούν από 20$ και μπορεί να φτάνουν ως και τα 200$ για τα standard πακέτα της εταιρίας. Το Cloudflare είναι μια υπηρεσία που παρέχει προστασία σε ιστότοπους και εφαρμογές. Αυτό επιτυγχάνεται μέσω του ελέγχου και της διαχείρισης της κίνησης των πακέτων στο δίκτυο και αντίστοιχα στην εφαρμογή. Ένα λογισμικό Cloudflare μετά την εγκατάστασή του μπορεί να ανιχνεύσει αυτόματα DDoS επιθέσεις, να παρέχει **Adaptive DDoS Protection**, δηλαδή αυξημένη προστασία σε εξελιγμένες DDoS επιθέσεις. Ακόμα, μέσω της **Advanced TCP** προστασίας εντοπίζει σύνθετες TCP επιθέσεις (όπως ACK, SYN, SYN-ACK) και επίσης προστατεύει από επιθέσεις DDoS που βασίζονται σε DNS [44].

Ένα πολύ μεγάλο μειονέκτημα του Cloudflare ωστόσο, είναι η εξάρτηση του χρήστη από την ίδια την εταιρία. Οποιοδήποτε πρόβλημα αντιμετωπίσει η εταιρία, μπορεί να επηρεάσει άμεσα την ιστοσελίδα του χρήστη που χρησιμοποιεί το λογισμικό. Ακόμη, ένα Cloudflare antivirus μπορεί να επιφέρει καθυστερήσεις στην απόδοση του συστήματος λόγω της δομής λειτουργίας του

συστήματος προστασίας. Ακόμη, χρησιμοποιώντας κάποιο λογισμικό της Cloudflare, σημαίνει πως όλη η κίνηση των δεδομένων του χρήστη περνάει από δίκτυο της εταιρίας, πράγμα που μπορεί να μη συμμορφώνεται με κανονισμούς όπως το GDPR ή το HIPAA [45].

7.4 Denial-of-service

Οι Denial-of-service (DDoS) επιθέσεις μπορούν να αντιμετωπιστούν είτε με λύσεις ανοικτού κώδικα, είτε με εμπορικές λύσεις.

Μια open source λύση, είναι το **Fail2ban**. Το software εγκαθίσταται σε Linux servers και προστατεύει από brute-force επιθέσεις (επιθέσεις ωμής βίας). Ο τρόπος που λειτουργεί είναι σαρώνοντας αρχεία και καταγράφοντας ύποπτες δραστηριότητες έτσι ώστε να μπορεί να μπλοκάρει δυνητικά κακόβουλες IP διευθύνσεις. Η λειτουργία του έχει ως εξής. Μετά την εγκατάστασή του, το, δωρεάν, λογισμικό σαρώνει καταγραφές από διακομιστές ή διάφορες εφαρμογές και ψάχνει για αποτυχημένες προσπάθειες σύνδεσης. Πέρα από την απλή καταγραφή, μετράει και τον αριθμό των προσπαθειών που επιχείρησε η κάθε καταγεγραμμένη IP σε ένα συγκεκριμένο χρονικό διάστημα. Εφόσον το ήδη τιθέμενο όριο αποτυχημένων συνδέσεων έχει ξεπεραστεί, τότε δημιουργεί αυτόματα firewall rule ώστε να μπλοκαριστεί η συγκεκριμένη IP. Ένα από τα πλεονεκτήματα του Fail2ban είναι το κόστος του, καθώς το software διατίθεται δωρεάν. Επίσης, είναι εύκολα ρυθμιζόμενο και μπορεί να συνεργαστεί με άλλες εφαρμογές του Η/Υ.

Το Fail2ban όμως λειτουργεί μόνο σε Linux OS, που ωστόσο δεν υποστηρίζει IPv6, κάτι που δε δίνει τη δυνατότητα σε χρήστες άλλων λειτουργικών συστημάτων να κάνουν χρήση του λογισμικού προστασίας. Επιπροσθέτως, το Fail2ban δεν υποστηρίζει τους χρήστες σε περιπτώσεις αδύναμων κωδικών πρόσβασης [46].

Figure 15: Fail2ban pros and cons (apriorit.com)

Το Akamai Kona, είναι μια ακόμα λύση για DDoS επιθέσεις. Τα κύρια χαρακτηριστικά του είναι:

- **Παροχή ολοκληρωμένης ασφάλειας**: Προστατεύει εκτός από DDoS attacks και από επιθέσεις SQL Injections, XSS και άλλες.
- **Διαχείριση των bots:** Τα εργαλεία του βοηθούν στο διαχωρισμό των bots, έτσι ώστε να κακά bots να αποτρέπονται.
- **Παρακολούθηση σε πραγματικό χρόνο:** Οι πίνακες ελέγχου του Akamai Kona επιτρέπουν την αξιολόγηση των απειλών και την λήψη των αντίστοιχων μέτρων σε πραγματικό χρόνο.

Το λογισμικό που παρέχεται από την εταιρία **Akamai**, είναι κατάλληλο για μεγάλες επιχειρήσεις οι οποίες χρειάζονται ασφάλεια στις διαδικτυακές τους εφαρμογές και τα APIs τους [56].

Η εταιρία παρέχει συνεχείς αναβαθμίσεις και αρκετά καλή τεχνική υποστήριξη. Επίσης, οι ισχυρές δυνατότητες του λογισμικού το καθιστούν αποτελεσματικό στην αποτροπή των απειλών αφού το adaptive WAF προσαρμόζεται στις απειλές σε πραγματικό χρόνο και έτσι μπορεί και εμποδίζει τις επιθέσεις. Σε αντίθεση με άλλες εμπορικές λύσεις, το Akamai Kona δεν έχει αναφορές για downtime ενώ επεξεργάζεται τεράστιο όγκο δεδομένων.

Στα μειονεκτήματά του συγκαταλέγεται η πολυπλοκότητα ρυθμίσεων που το χαρακτηρίζει, με αποτέλεσμα να μη μπορεί να γίνει η εγκατάσταση από χρήστες χωρίς εμπειρία, παρά μόνο από άτομα με γνώση της συγκεκριμένης τεχνολογίας.

Ένα ακόμη αρνητικό του προϊόντος είναι η δυσκολία στην κατανόηση από τον χρήστη, αν όλες οι ευπάθειες αποτρέπονται με τον σωστό τρόπο. Αυτό συμβαίνει γιατί οι κανόνες του WAF δεν είναι απόλυτα κατανοητοί [46].

Η χρήση του αφορά μόνο εταιρίες φυσικά, καθώς το κόστος του σύμφωνα με το https://www.applytosupply.digitalmarketplace.service.gov.uk/, ξεκινάει από τα 10.274,25$ και μπορεί να φτάσει ακόμα και τα 265.258,76$ ανά μήνα, ενώ στην αρχή παρέχεται free trial.

7.5 SQL Injection

Το **SQLmap** είναι ένα εργαλείο ανοικτού κώδικα που αποσκοπεί στον εντοπισμό των ευπαθειών SQL Injection. Η λειτουργία του ξεκινάει με την αναζήτηση ευπαθειών σε SQL Injection επιθέσεις είτε σε εφαρμογές είτε σε ιστοσελίδες. Χρησιμοποιώντας διάφορες τεχνικές, μπορεί να επιβεβαιώσει αν μια σελίδα είναι ευπαθής σε SQLi επιθέσεις. Κάποιες από τις βασικές δυνατότητες του SQLmap, είναι η αυτόματη αναγνώριση του τύπου της βάσης δεδομένων και η εξαγωγή δεδομένων από αυτή. Μπορεί επίσης να διαβάσει και να εκτελέσει αρχεία εφόσον ο χρήστης έχει δώσει τα κατάλληλα δικαιώματα, αλλά και να παρακάμψει firewall rules μέσω συγκεκριμένων script. Ένα παράδειγμα εντολής SQLmap είναι το «**sqlmap -u "http://target.com/page?id=1" –dbs**», όπου ελέγχει για πιθανό SQL injection στην παράμετρο id στο URL. Κάποια πλεονεκτήματα του είναι [50]:

- Ευχρηστία,
- Προσαρμοστικότητα στις ανάγκες κάθε επίθεσης,
- Υποστήριξη πολλών DBMS,
- Δυνατότητα Bypassing.

Μειονεκτήματα του θεωρούνται:

- **Υψηλό traffic:** Ο μεγάλος όγκος αιτημάτων μπορεί να οδηγήσει σε αποκλεισμό
- Πιθανή λανθασμένη ρύθμιση μπορεί να οδηγήσει σε σφάλματα
- Περιορισμοί με πολύπλοκες SQLi

Το **Acunetix** είναι μία εμπορική λύση που πραγματοποιεί αυτοματοποιημένους ελέγχους για πρόληψη κατά των SQL Injections. Το software ελέγχει τα διάφορα sites που χρησιμοποιούν HTTP/HTTPS πρωτόκολλο εντοπίζοντας ευπάθειες σε εφαρμογές όπως JavaScript και AJAX. Το Acunetix αναλύει την ιστοσελίδα προσπελάζοντας όλους τους συνδέσμους της και παίρνει πληροφορίες οι οποίες δεν είναι διαθέσιμες στο κοινό. Επίσης, παρέχει πληροφορίες για τις ευπάθειες

που προκύπτουν, μετά από αυτοματοποιημένους ελέγχους που πραγματοποιεί στα αρχεία.

Στα θετικά του Acunetix συγκαταλέγονται η αυξημένη ακρίβεια του και οι εκτεταμένοι έλεγχοι που πραγματοποιεί, οι πολλές γλώσσες κώδικα που υποστηρίζει (όπως PHP, .NET) και ο έλεγχος του δικτύου για πάνω από 50.000 πιθανές ευπάθειες (acunetix.com).

Το λογισμικό της ομώνυμης εταιρίας, κοστίζει από 7.000$ ως και 37.000$ για 12μηνη χρήση του, ανάλογα με το πακέτο που θα επιλέξει ο υπεύθυνος.

Πέρα από το κόστος, στα αρνητικά μπορεί να συγκαταλεχθεί και η εκπαίδευση που απαιτείται ώστε οι χρήστες να αποκτήσουν εξοικείωση με το software ώστε να μπορούν να το ρυθμίσουν κατάλληλα. Ακόμη, η υποστήριξή του σε ορισμένα frameworks, όπως το PHP, το .NET, είναι αρκετά περιορισμένη. Ένα ακόμα μειονέκτημά του είναι πως ο χρόνος σάρωσης σε μεγάλες εφαρμογές μπορεί να διαρκέσει πάρα πολύ. Τέλος, ενώ για τα web apps είναι ένα εξαιρετικά χρήσιμο εργαλείο, δε μπορούμε να πούμε το ίδιο για τα mobile apps καθώς δεν είναι η ιδανική λύση για έλεγχο ευπαθειών σε εφαρμογές για κινητά [52].

7.6 Zero-day exploit

Το **SnortML** είναι μια μηχανή ανίχνευσης βασισμένη σε αλγορίθμους μηχανικής μάθησης. Το SnortML ανιχνεύει επιθέσεις, μεταξύ των οποίων και Zero-day. Για να κατασκευαστεί το μοντέλο μηχανικής μάθησης, χρησιμοποιείται περιβάλλον Tensorflow, όπου και γίνεται η εκπαίδευση των μοντέλων. Αφού εκπαιδευτεί, χρησιμοποιεί, χρησιμοποιείται το trained μοντέλο για να ανιχνευθούν πιθανές επιθέσεις. Το training set πρέπει να αποτελείται από μηδενικά συμπληρωμένα (zero-padded) δεδομένα.

Θετικά στοιχεία:

- **Ανιχνεύει άγνωστες έως τώρα απειλές,**
- **Ευελιξία λόγω μηχανικής μάθησης,**
- **Είναι open source.**

Μειονεκτήματα:

- **Πρέπει οπωσδήποτε να εκπαιδευτεί** (χρειάζεται έμπειρος/οι χρήστες),
- **Έχει ανάλογες υπολογιστικές απαιτήσεις λόγω του machine learning,**
- **Προς το παρόν περιορίζεται σε μοντέλα δυαδικής ταξινόμησης.**

Το **Falcon** είναι μια πλατφόρμα της εταιρίας CrowdStrike. Το Falcon συνδυάζει πολλές λύσεις cybersecurity σε μια μόνο πλατφόρμα. Η εταιρία (CrowdStrike), είναι γνωστή για ταχύτητα με την οποία είναι ικανή να ανιχνεύει ενδεχόμενες απειλές και είχε καθοριστικό ρόλο σε προσπάθεια κυβερνοεπίθεσης κατά της Sony Pictures το 2014. Η πλατφόρμα εκτός από τον συνδυασμό πολλών λύσεων, προσφέρει αποδοτικότητα καθώς είναι ένα πολύ ισχυρό antivirus λογισμικό. Επίσης, είναι αρκετά 'ελαφρύ' και δεν επιβαρύνει την απόδοση του συστήματος στο οποίο είναι εγκατεστημένο η πλατφόρμα. Ακόμη, είναι σύγχρονη και προσφέρει κάλυψη σε ένα μεγάλο εύρος διαφορετικών τύπου επιθέσεων [54].

Στα αρνητικά, η πλατφόρμα μπορεί να είναι αρκετά κοστοβόρα για μικρές επιχειρήσεις καθώς το κόστος διαμοιράζεται ανά συσκευή και ξεκινάει από τα 59.99$ ανά έτος, ενώ μπορεί να φτάσει τα 184.99$ (crowdstrice.com/products). Επίσης, μεταξύ άλλων, σε παλαιότερα συστήματα μπορεί προκαλέσει σημαντικές καθυστερήσεις στη λειτουργία [48].

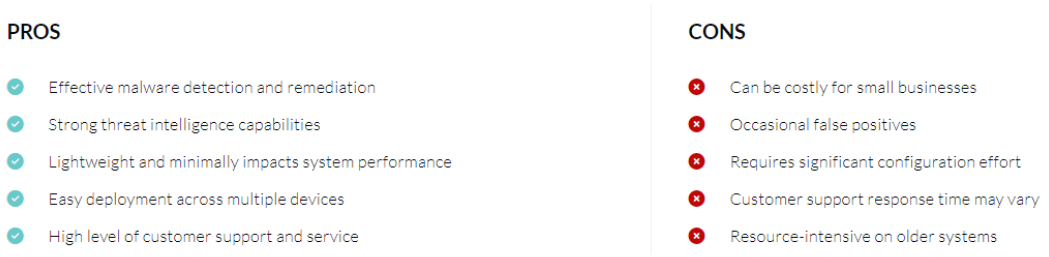

Figure 16: ClowdStrike pros and cons (peerspot.com)

Στις 19 Ιουλίου του 2024, ένα λάθος στην ενημέρωση λογισμικού από την CroudStrike, επηρέασε εκατομμύρια συστήματα με λειτουργικό Windows εμφανίζοντας την οθόνη μπλε θανάτου (BSOD) στα συστήματα αυτά. Παρόλο που το πρόβλημα διορθώθηκε γρήγορα, οι αναταραχές και τα προβλήματα που προκλήθηκαν εξ' αιτίας του ήταν πολύ μεγάλα. Το συγκεκριμένο error, προκάλεσε δυσλειτουργίες σε αεροδρόμια και αεροπορικές εταιρίες, σε ΜΜΕ και ΜΜΜ, ακόμα και σε υγειονομικές και χρηματοοικονομικές υπηρεσίες. Το πρόβλημα εντοπίστηκε και διορθώθηκε μέσα σε 79 λεπτά και χρειάστηκε φυσική πρόσβαση χρήστη σε πολλούς υπολογιστές προκειμένου να διορθωθεί [55].

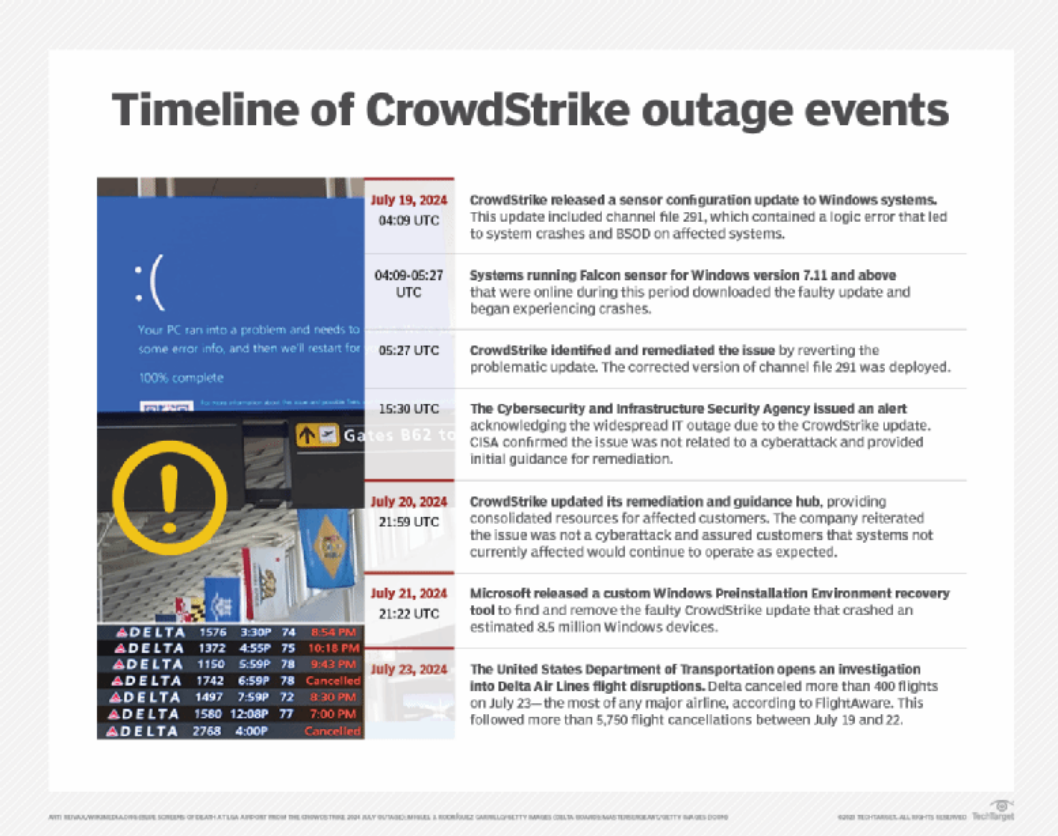

Figure 17: CrowdStrike outage events (techtarget.com)

7.7 DNS Tunneling

Το **DNSChef** είναι ένας DNS Proxy Server που παρεμβαίνει σε DNS ερωτοαπαντήσεις με σκοπό την τροποποίησή τους για δοκιμές ασφαλείας. Είναι open source και μπορεί κάθε χρήστης να το εγκαταστήσει στον υπολογιστή του μέσω της εντολής “pip”. Στα θετικά του είναι η ευέλικτη διαμόρφωσή το ανάλογα με τις ανάγκες των δοκιμών που πρέπει να γίνουν. Επίσης, χρησιμοποιείται και για δοκιμές ασφάλειας του δικτύου και αποτελεσματικότητας των firewall, αλλά και για τον αποκλεισμό ανεπιθύμητων διαφημίσεων.

Στα αρνητικά, η εγκατάσταση του DNSChef είναι σύνθετη και ένας τέτοιος server δεν είναι αξιόπιστος καθώς μπορεί να διακοπεί η λειτουργία του ανά πάσα στιγμή. Τέλος, μπορεί να μην είναι συμβατός με όλες τις συσκευές ή όλα τα routers [59].

Το **DNS Firewall** είναι μια λύση που προστατεύει τα περιβάλλοντα των ηλεκτρονικών υπολογιστών και τους χρήστες από μια ευρεία γκάμα απειλών. Η

λειτουργία τους είναι να κάνουν filter τα αιτήματα DNS και να αποκλείουν αυτά που παραβιάζουν προκαθορισμένους κανόνες και πολιτικές ασφαλείας. Ένα DNS Firewall μπορούμε να πούμε ότι λειτουργεί σαν φράγμα απέναντι στα DNS αιτήματα και μπλοκάρει την πρόσβαση του χρήση σε επικίνδυνες ιστοσελίδες. Μεταξύ άλλων επιθέσεων, το DNS Firewall αποτρέπει και τις DNS Tunneling επιθέσεις. Θετικά στοιχεία του είναι ότι προστασία κατά στοχευμένων DNS απειλών, είναι οικονομικά και απλά στην χρήση τους και βελτιώνουν την απόδοση του δικτύου κάτι που επιτυγχάνεται λόγω εξοικονόμησης του bandwidth. Ωστόσο η απόδοση ενός DNS Firewall εξαρτάται από την συνεχή ενημέρωση του ενδέχεται να χρειάζεται συνδυασμό πολλών λύσεων ασφαλείας με σκοπό να πετύχει ολοκληρωμένη προστασία [47].

Κεφάλαιο 8ο Συμπεράσματα και μελλοντικές επεκτάσεις

Αυτό που μπορούμε να συμπεράνουμε διαβάζοντας το περιεχόμενο της πτυχιακής αυτής εργασίας, είναι πως και οι open source λύσεις, αλλά και αυτές του εμπορίου μπορούν να αποτρέψουν πιθανές κυβερνοεπιθέσεις στον υπολογιστή ή σε ένα δίκτυο ηλεκτρονικών υπολογιστών. Κάθε μία από τις δύο κατηγορίες εργαλείων κατά των κυβερνοεπιθέσεων έχει τα δικά της πλεονεκτήματα και μειονεκτήματα και οι χρήστες είναι αυτοί που καλούνται να επιλέξουν το καταλληλότερο για αυτούς αμυντικό σύστημα. Οι open source λύσεις παρά το μηδαμινό τους κόστος, μπορούν εύκολα να εγκατασταθούν στους Η/Υ, είναι εύκολες στη χρήση τους και αποτελεσματικές σε πολλές περιπτώσεις. Οι λύσεις που μπορεί οποιοσδήποτε να βρει στο εμπόριο, διακρίνονται για το ψηλό τους κόστος, ωστόσο προσφέρουν μεγάλη υποστήριξη και η αμυντική τους συμπεριφορά είναι αρκετά χρήσιμη στον πόλεμο κατά των κυβερνοεγκληματιών. Ένας απλός χρήστης που λογικά δεν αποτελεί στόχο εγκληματιών, μπορεί να χρησιμοποιήσει μια open source λύση με σκοπό την προστασία του υπολογιστή του. Αντίθετα, μια μεγάλη εταιρία που είναι αρκετά πιθανό να είναι στόχος hackers, πρέπει να επενδύσει χρήματα στην προστασία του δικτύου της ώστε να αποκρουστεί η οποιαδήποτε προσπάθεια επίθεσης κατά της με σκοπό την υποκλοπή σημαντικών αρχείων αλλά και χρημάτων.

Οι τρόποι αντιμετώπισης αλλά και επίθεσης που αναλύθηκαν στα προηγούμενα κεφάλαια, οδηγούν στο συμπέρασμα πως οι χρήστες ηλεκτρονικών υπολογιστών αλλά και ολόκληρων δικτύων υπολογιστών, θα πρέπει να είναι εκπαιδευμένοι σύμφωνα με όλα τα πρότυπα και να ενημερώνονται συνέχεια για ώστε οι γνώσεις τους πάνω στην άμυνα των συστημάτων να εμπλουτίζονται συνεχώς. Ο κλάδος

του cybersecurity έχει αποδείξει ότι είναι ένας από τους σημαντικότερους στον τομέα του Computer Science καθώς χιλιάδες εταιρίες στον κόσμο έχουν υποστεί ζημίες εκατομμυρίων επειδή δεν έδιναν την απαραίτητη σημασία στην προστασία των δικτύων τους από τους hackers. Πέρα από την κατάλληλη εκπαίδευση των εργαζομένων, οι εταιρίες θα πρέπει να ενημερώνονται συνεχώς για νέους ιούς και προηγμένα αμυντικά συστήματα και οι ήδη υπάρχουσες λύσεις θα πρέπει να προσαρμόζονται στην εξέλιξη των κυβερνοεπιθέσεων με σκοπό την αποτελεσματική αντιμετώπισή τους κάθε φορά που αυτές συμβαίνουν. Η παρούσα εργασία θα μπορούσε να εμπλουτιστεί με κάποια έρευνα πάνω στην μηχανική μάθηση, σε συνάρτηση με την άμυνα στις κυβερνοεπιθέσεις. Το **Machine Learning** (**μηχανική μάθηση**) γίνεται ολοένα και πιο χρήσιμο σε κάθε τομέα της τεχνολογίας. Σε συνδυασμό με την **τεχνητή νοημοσύνη** (**AI**), μπορούν να δημιουργηθούν μοντέλα τα οποία αφού τροφοδοτηθούν με κατάλληλα δεδομένα από έως τώρα επιθέσεις, θα είναι ικανά να προβλέπουν πιθανές εισβολές από κυβερνοεγκληματίες και να αποτρέπουν τις επιθέσεις αυτές. Τα μοντέλα αυτά επίσης, θα μπορούν να ανιχνεύουν ευαίσθητα σημεία στα λογισμικά ή σε δίκτυα και να βοηθήσουν σημαντικά στην πρόβλεψη των επιθέσεων μέσα από αυτοματοποιημένες λύσεις άμυνας.

Επίσης, ένας άλλος κλάδος που θα μπορούσε να συσχετιστεί με το cybersecurity, είναι αυτός του **IoT** field. Σε ένα IoT περιβάλλον, μπορούν να υπάρχουν εκατοντάδες, ακόμα και χιλιάδες συνδεδεμένες συσκευές σε ένα δίκτυο. Αυτό, δημιουργεί την ανάγκη για ανάπτυξη λύσεων που θα προστατεύουν όλες αυτές τις συσκευές από επίδοξους hackers που θα θελήσουν να βλάψουν το περιβάλλον. Αν μια από τις συνδεδεμένες συσκευές εκτεθεί σε κάποιον ιό, τότε ο κίνδυνος για «μόλυνση» όλου του IoT συστήματος είναι κάτι παραπάνω από ορατός. Η έρευνα πάνω στο security στον τομέα του Διαδικτύου των Πραγμάτων, μπορεί να εξετάσει τους τρόπους που μπορεί ο εισβολέας να εισέλθει σε ένα τέτοιο δίκτυο υπολογιστών και μηχανών αλλά και να προτείνει εργαλεία κατάλληλα για τη απόκρουση του εχθρού.

Ακόμη, ίσως ο πιο σημαντικός παράγοντας που θα πρέπει να μελετηθεί, είναι η συνεχής εκπαίδευση και ευαισθητοποίησης των χρηστών πάνω στην πρόληψη και στην άμυνα. Η εκπαίδευσή τους, θα συμβάλλει σημαντικά στην μείωση των μολύνσεων από διαφόρων τύπων ιών, όπως το Phishing. Η έρευνα μπορεί να επικεντρωθεί στην ανάπτυξη εργαλείων που θα βοηθούν τους εργαζομένους αλλά και τους απλούς χρήστες να αποφεύγουν κάποιες ενέργειες με σκοπό την αποφυγή της εισβολής κακόβουλου λογισμικού στα λειτουργικά τους συστήματα. Επίσης, θα μπορούν να αποφεύγονται τα ανθρώπινα λάθη και η

έκθεση σε κίνδυνο από ανθρώπινο λάθος θα μπορέσει να εκμηδενιστεί. Στην έρευνα αυτή, θα μπορούσε να υπάρχει και ένας συνδυασμός εκπαίδευσης των χρηστών με το AI. Να μπορεί δηλαδή η τεχνητή νοημοσύνη να εκπαιδεύει τους ανθρώπους με σκοπό την παροχή γνώσεων που θα αποφέρουν μέγιστη ασφάλεια.

Τέλος, κάτι που σίγουρα μπορεί να μελετηθεί είναι τα οφέλη του **Penetration Testing** πάνω στα λογισμικά. Η διαδικασία αυτή, μπορεί να προσομοιώσει κυβερνοεπιθέσεις σε ένα οποιοδήποτε σύστημα ή δίκτυο υπολογιστών. Οι ειδικοί testers, πραγματοποιώντας διάφορες διαδικασίες μπορούν να εντοπίζουν τυχόν κενά στην ασφάλεια των συστημάτων και να προειδοποιήσουν τους χρήστες για τον βαθμό που το σύστημά του ή το δίκτυο είναι ευάλωτο.

Συνοψίζοντας, η πτυχιακή αυτή εργασία μπορεί να επεκταθεί με μελέτες πάνω στην ισχυροποίηση των αμυντικών μηχανισμών συνδυάζοντας το AI, το IoT και άλλους τομείς. Ακόμη, θα μπορεί να γίνει μια αναλυτική μελέτη σχετικά με άλλους ιούς που μπορούν να προσβάλλουν τα λογισμικά, αλλά και να αναλυθούν οι τρόποι της επίθεσής τους και κάποιοι πιθανοί τρόποι αντιμετώπισης των ιών αυτών.

Βιβλιογραφία

Internet Site

[31] https://222.ieeexolre.ieee.org/

[32] https://blog.havocshield.com/

[33] https://el.wikipedia.org/wiki/Malware

[34] https://portswigger.net/

[35] https://researchgate.net/

[36] https://www.cloudns.net/

[37] https://www.eset.com/gr/malware/

[38] https://www.linkedin.com/

[39] https://www.microsoft.com/

[40] https://www.secnews.gr/

[41] https://www.kaspersky.com/

[42] https://www.liquidweb.com

[43] https://www.lumificyber.com

[44] https://developers.cloudflare.com

[45] https://www.itomic.com.au

[46] https://www.apriorit.com

[47] https://www.akamai.com

[48] https://www.peerspot.com

[49] https://www.applytosupply.digitalmarketplace.service.gov.uk/

[50] https://www.vaadata.com/

[51] https://www.acunetix.com/

[52] https://www.trustradius.com/

[53] https://webhostinggeeks.com/

[54] https://www.crowdstrike.com/

[55] https://www.techtarget.com/

[56] https://www.akamai.com/

[57] https://el.wikipedia.org/wiki/Phishing

[58] https://comptia.com/

[59] https://geeksforkeeks.org/

Paper in Conference Proceedings

Journal Articles

[1] Iiascu, I. (2019). 'Sea Turtle' Campaign Focuses on DNS Hijacking to Compromise Targets.

[2] LinkedIn publish, Christopher Hong, IT Support and Project Manager

[3] Abdullayev, V., & Chauhan, A. S. (2023). SQL injection attack: Quick view. Mesopotamian Journal of CyberSecurity, 2023, 30-34.

[4] Agazzi, A. E. (2020). Phishing and Spear Phishing: examples in Cyber Espionage and techniques to protect against them. arXiv preprint arXiv:2006.00577.

[5] Alabdan, R. (2020). Phishing attacks survey: Types, vectors, and technical approaches. Future internet, 12(10), 168.

[6] Alenezi, M., Nadeem, M., & Asif, R. (2021). SQL injection attacks countermeasures assessments. Indonesian Journal of Electrical Engineering and Computer Science, 21(2), 1121-1131.

[7] Algarni, S. (2021). Cybersecurity attacks: Analysis of “wannacry” attack and proposing methods for reducing or preventing such attacks in future. In ICT Systems and Sustainability: Proceedings of ICT4SD 2020, Volume 1 (pp. 763-770). Springer Singapore.

[8] Blaise, A., Bouet, M., Conan, V., & Secci, S. (2020). Detection of zero-day attacks: An unsupervised port-based approach. Computer Networks, 180, 107391.

[9] Bonasera, W., Chowdhury, M. M., & Latif, S. (2021, October). Denial of service: A growing underrated threat. In 2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME) (pp. 1-6). IEEE.

[10] Bossetta, M. (2018). The weaponization of social media: Spear phishing and cyberattacks on democracy. Journal of international affairs, 71(1.5), 97-106.

[11] Chen, Q., & Bridges, R. A. (2017, December). Automated behavioral analysis of malware: A case study of wannacry ransomware. In 2017 16th IEEE International Conference on machine learning and applications (ICMLA) (pp. 454-460). IEEE.

[12] Chen, T. M. (2014). Cyberterrorism after Stuxnet.

[13] Javeed, D., MohammedBadamasi, U., Ndubuisi, C. O., Soomro, F., & Asif, M. (2020). Man in the middle attacks: Analysis, motivation and prevention. International Journal of Computer Networks and Communications Security, 8(7), 52-58.

[14] Magaña, J., Olvera, C. I., & Lous, P. (2019). How can we improve security against DDoS attacks? A case study: The DyN Attack in 2016.

[15] Nuiaa, R. R., Manickam, S., & Alsaeedi, A. H. (2021). Distributed reflection denial of service attack: A critical review. International Journal of Electrical and Computer Engineering, 11(6), 5327.

[16] Paper: Ferdous, J., Islam, R., Mahboubi, A., & Islam, M. Z. (2023). A State-of-the-Art Review of Malware Attack Trends and Defense Mechanism. IEEE Access.

[17] Paper: Shobana, R., & Suriakala, M. A Thorough Study On SQL Injection Attack-Detection And Prevention Techniques And Research Issues. Part time Research Scholar, University of Madras, Assistant Professor, Department of Computer Science and Applications, DKM College for Women, Vellore-1, 10(5-2020).

[18] Paper: Kumar, G. (2016). Denial of service attacks–an updated perspective. Systems science & control engineering, 4(1), 285-294.

[19] Paper: Rono, D. (2015). DNS Tunneling.

[20] Paper: Sammour, M., Hussin, B., Othman, M. F. I., Doheir, M., AlShaikhdeeb, B., & Talib, M. S. (2018). Dns tunneling: a review on features. International Journal of Engineering & Technology, 7(3.20), 1-5.

[21] Paper: Malware Attacks affecting organizations, Nimesh Silva, Florida Institute of Technology

[22] Paper: Roundtable, B. F. (2011). Malware risks and mitigation report. tech. rep., National Institute of Standards and Technology.

[23] Paper: Mallik, A. (2019). Man-in-the-middle-attack: Understanding in simple words. Cyberspace: Jurnal Pendidikan Teknologi Informasi, 2(2), 109-134.

[24] Paper: Vayansky, I., & Kumar, S. (2018). Phishing–challenges and solutions. Computer Fraud & Security, 2018(1), 15-20.

[25] Paper: Prakash, D. S. Zero-day Vulnerabilities: An In-depth analysis.

[26] Patil, A., Shinde, S., & Banerjee, S. (2021). Stuxnet-tool for zero-day attack. In Handbook of Research on Cyber Crime and Information Privacy (pp. 652-675). IGI Global.

[27] Rajendran, B. (2020, February). DNS amplification & DNS tunneling attacks simulation, detection and mitigation approaches. In 2020 International Conference on Inventive Computation Technologies (ICICT) (pp. 230-236). IEEE.

[28] Thankappan, M., Rifà-Pous, H., & Garrigues, C. (2022). Multi-Channel Man-in-the-Middle attacks against protected Wi-Fi networks: A state of the art review. Expert Systems with Applications, 210, 118401.

[29] Waheed, A., Seegolam, B., Jowaheer, M. F., Sze, C. L. X., Hua, E. T. F., & Sindiramutty, S. R. (2024). Zero-Day Exploits in Cybersecurity: Case Studies and Countermeasure.

[30] Younis, Y. A., & Musbah, M. (2020, September). A framework to protect against phishing attacks. In Proceedings of the 6th International Conference on Engineering & MIS 2020 (pp. 1-6).

Παραρτήματα

Appendix A. Terms and Definitions

Malware: malicious software, any and all software that is deployed with malicious intent

Phishing: email-born malware propagation systems

Zero-Day: modifier for the word threat or attack, meaning that the vulnerability that is used by the threat agent is not known to potential victims

URL: Universal Resource Locator

FTP: File Transfer Protocol

API: Application Programming

SYN floods: Μια μορφή επίθεσης DoS (Denial of Service) που εκμεταλλεύεται το πρωτόκολλο TCP

Telnet:Πρωτόκολλο δικτύου που επιτρέπει την απομακρυσμένη σύνδεση σε άλλους υπολογιστές ή δικτυακές συσκευές