ΠΟΛΥΤΕΧΝΕΙΟ ΚΡΗΤΗΣ

Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών
Εργαστήριο Μικροεπεξεργαστών και Υλικού

Διπλωματικη Εργασια

Χρήση Honeytokens για προστασία σε Ransomware

Συντάκτης:
Ιωάννης ΣΤΑΜΑΤΕΛΟΣ

Επιτροπή:
Καθ. Σωτήριος ΙΩΑΝΝΙΔΗΣ
Καθ. Απόστολος ΔΟΛΛΑΣ
Καθ. Μιχαήλ Γ.ΛΑΓΟΥΔΑΚΗΣ

Διπλωματική εργασία που υποβλήθηκε στο πλαίσιο της ολοκλήρωσης των απαιτήσεων για την απόκτηση του διπλώματος Ηλεκτρολόγου Μηχανικού και Μηχανικού Υπολογιστών

Χανιά, Οκτώβριος 2024

ΠΟΛΥΤΕΧΝΕΙΟ ΚΡΗΤΗΣ

Σχολή Ηλεκτρολόγων Μηχανικών & Μηχανικών Υπολογιστών

Περίληψη

Διπλωματική Εργασία

Χρήση Honeytokens για προστασία σε Ransomware

Ιωάννης ΣΤΑΜΑΤΕΛΟΣ

Το Ransomware είναι ένας τύπος κακόβουλου λογισμικού που έχει αναδειχθεί ως μία από τις πιο διάχυτες και επιζήμιες απειλές στον κυβερνοχώρο τα τελευταία χρόνια, προκαλώντας σημαντικές οικονομικές απώλειες και παραβιάσεις δεδομένων σε διάφορους τομείς, εκτός εάν καταβληθούν λύτρα. Δεδομένου ότι οι μέθοδοι ανίχνευσης βελτιώνονται συνεχώς για τον εντοπισμό και την αντιμετώπιση του ransomware, το ίδιο το ransomware γίνεται εξίσου καλύτερο για την αποφυγή των μηχανισμών ανίχνευσης. Η εργασία ξεκινά με την ανάλυση της τρέχουσας κατάστασης των απειλών στον κυβερνοχώρο και στη συνέχεια εστιάζει στο ransomware, καθώς είναι μια από τα πιο δημοφιλείς απειλές. Συνεχίζει με την εξέλιξη του ransomware από τις πρώτες του μορφές στις πιο σύγχρονες, εξελιγμένες μορφές, επισημαίνοντας βασικά ορόσημα και αλλαγές στις τεχνικές επίθεσης. Μια προσέγγιση στον κύκλο ζωής του ransomware παρέχει πληροφορίες για το πώς αυτά τα κακόβουλα προγράμματα διαδίδονται, κρυπτογραφούν τα δεδομένα και απαιτούν λύτρα, ρίχνοντας φως στον τρόπο λειτουργίας τους. Η ενότητα ταξινόμησης κατηγοριοποιεί τις παραλλαγές ransomware με βάση τα χαρακτηριστικά, τους μηχανισμούς διάδοσης και τις τεχνικές κρυπτογράφησης. Αυτή η ταξινόμηση βοηθά στην κατανόηση των διαφόρων ransomware. Τέλος, προτείνεται μια μέθοδος ανίχνευσης ransomware με χρήση HoneyTokens. Τα HoneyTokens είναι αρχεία που έχουν στρατηγικά τοποθετηθεί για να προσελκύουν ransomware, παρέχοντας έναν προληπτικό αμυντικό μηχανισμό. Η μελέτη προσφέρει μια ολοκληρωμένη ανάλυση της εφαρμογής και της αποτελεσματικότητας αυτής της προσέγγισης στον εντοπισμό και τον μετριασμό των απειλών ransomware.

TECHNICAL UNIVERSITY OF CRETE

School of Electrical and Computer Engineering

Abstract

Diploma Thesis

Honeytokens for the fight against ransomware

Ioannis STAMATELOS

Ransomware is a type of malware that has emerged as one of the most pervasive and damaging cyber threats in recent years, causing significant financial losses and data breaches across various sectors, unless a ransom is paid. Since detection methods are constantly improving in order to detect and mitigate ransomware, the ransomware itself becomes equally better in avoiding detection mechanisms. This thesis begins by analyzing the current state of cyberthreats and then focuses on ransomware, as it is one of most popular ones. It continues with the evolution of ransomware from its early origins to its contemporary, sophisticated forms, highlighting key milestones and shifts in attack techniques. A deep dive into the ransomware lifecycle provides insights into how these malicious programs propagate, encrypt data, and demand ransoms, shedding light on their operational dynamics. The classification section categorizes ransomware variants based on their characteristics, propagation mechanisms, and encryption techniques. This taxonomy aids in understanding the diverse landscape of ransomware. Finally, a method for ransomware detection using HoneyTokens is implemented. HoneyTokens are strategically-placed decoy files designed to attract ransomware attackers, providing a proactive defense mechanism. The study offers a comprehensive analysis of the implementation and effectiveness of this approach in identifying and mitigating ransomware threats.

Ευχαριστίες

Με την παρούσα διπλωματική εργασία ολοκληρώνονται οι σπουδές μου στο προπτυχιακό πρόγραμμα σπουδών στο Πολυτεχνείο Κρήτης στη Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών.

Στο σημείο αυτό θα ήθελα να ευχαριστήσω τον Καθηγητή Σωτήριο Ιωαννίδη και τον συνεργάτη του Γεώργιο Χατζηβασίλη για την επίβλεψη της διπλωματικής μου εργασίας.

Επίσης, θα ήθελα να ευχαριστήσω τους φίλους, μου αλλά και τους συναδέλφους μου για την ανοχή, την κατανόηση και την υπομονή που επέδειξαν όλο αυτό το διάστημα.

Κλείνοντας, ευχαριστώ τους γονείς μου και τα αδέρφια μου για την κατανόηση, υποστήριξη και ενθάρρυνση που μου παρείχαν σε όλη τη διάρκεια του προπτυχιακού προγράμματος.

Περιεχόμενα

Πίνακας Εικόνων

Chapter 1

Εισαγωγή

1.1 Ασφάλεια στο Κυβερνοχώρο

Με την αυξανόμενη εξάρτηση από την τεχνολογία και την επικράτηση του Διαδικτύου, η ασφάλεια στον κυβερνοχώρο έχει αναδειχθεί ως ένας κρίσιμος παράγοντας που επιδιώκει να προστατεύσει ιδιώτες, οργανισμούς, ακόμα και εθνικές υποδομές, από κακόβουλες επιθέσεις. Αυτή η διπλωματική εργασία στοχεύει να ρίξει φως στις επιθέσεις στο κυβερνοχώρο και τον αντίκτυπό τους, να τονίσει τη σημασία της κυβερνοασφάλειας και να διερευνήσει την δυνατότητα αντιμετώπισης του Ransomware με την χρήση HoneyTokens.

Μια επίθεση στον κυβερνοχώρο αναφέρεται σε οποιαδήποτε μη εξουσιοδοτημένη απόπειρα απόκτησης πρόσβασης, διακοπής συστημάτων ή δικτύων υπολογιστών, συνήθως με κακόβουλη πρόθεση. Αυτές οι επιθέσεις έρχονται σε διάφορες μορφές, όπως κακόβουλο λογισμικό, phishing, επιθέσεις άρνησης υπηρεσίας (DoS), ransomware. Στοχεύουν τα πάντα, από προσωπικούς υπολογιστές έως υποδομές δικτύου μεγάλης κλίμακας, δημιουργώντας σημαντικές διαταραχές στην εύρυθμη λειτουργία των παραπάνω συστημάτων, ζημιές και οικονομικές απώλειες.

Μία από τις πιο σημαντικές επιπτώσεις των επιθέσεων στον κυβερνοχώρο είναι η απώλεια ευαίσθητων πληροφοριών. Οι χάκερ, οι εγκληματίες ή ακόμη και οι κρατικοί φορείς στοχεύουν συχνά βάσεις δεδομένων που περιέχουν προσωπικές, οικονομικές πληροφορίες. Τέτοιες παραβιάσεις σε προσωπικά δεδομένα έχουν σοβαρές συνέπειες για τα άτομα, συμπεριλαμβανομένης της οικονομικής καταστροφής και της προσωπικής φήμης [39].

Επιπλέον, οι επιθέσεις στον κυβερνοχώρο μπορούν να υπονομεύσουν κρίσιμες υποδομές και να διαταράξουν βασικές υπηρεσίες. Για παράδειγμα, οι επιθέσεις σε δίκτυα ηλεκτρικής ενέργειας, εγκαταστάσεις επεξεργασίας νερού ή συστήματα μεταφοράς υδρογονανθράκων μπορεί να έχουν σοβαρές συνέπειες για τη δημόσια ασφάλεια και ευημερία. Αυτές οι επιθέσεις μπορεί να οδηγήσουν σε διακοπές ρεύματος, μόλυνση του νερού ή αστοχίες μεταφοράς του, θέτοντας σε κίνδυνο ζωές

και προκαλώντας σημαντικές οικονομικές απώλειες [40].

Ο αντίκτυπος των επιθέσεων στον κυβερνοχώρο δεν περιορίζεται σε άτομα και υποδομές, επεκτείνεται και στις κυβερνήσεις και την εθνική ασφάλεια κρατών. Φορείς εθνικών κρατών συχνά εμπλέκονται σε κυβερνοπόλεμο ή κατασκοπεία, εξαπολύοντας επιθέσεις σε συστήματα άλλων χωρών για να αποκτήσουν πληροφορίες, να διαταράξουν υπηρεσίες ή να υπονομεύσουν κρίσιμες εθνικές υποδομές. Τέτοιες επιθέσεις όχι μόνο θέτουν σε κίνδυνο την εθνική ασφάλεια, αλλά μπορεί να οδηγήσει στη κλιμάκωση των εντάσεων μεταξύ εθνών, οδηγώντας σε διασυνοριακές συγκρούσεις [41].

Δεδομένης της σοβαρότητας των απειλών στον κυβερνοχώρο, η σημασία της κυβερνοασφάλειας δεν μπορεί να υποτιμηθεί. Η κυβερνοασφάλεια αναφέρεται στην πρακτική της προστασίας ψηφιακών συστημάτων, δικτύων και ευαίσθητων δεδομένων από μη εξουσιοδοτημένη πρόσβαση, επιθέσεις και ζημιές.

Πρώτον και κύριον, η κυβερνοασφάλεια συμβάλλει στην προστασία του απορρήτου και των προσωπικών πληροφοριών των ατόμων. Εφαρμόζοντας αποτελεσματικά μέτρα ασφαλείας, οι οργανισμοί μπορούν να προστατεύσουν τα δεδομένα των πελατών τους, αποτρέποντας μη εξουσιοδοτημένη πρόσβαση σε αυτά. Αυτό, με τη σειρά του, ενισχύει την εμπιστοσύνη μεταξύ των χρηστών και εταιρειών, διασφαλίζοντας μια θετική διαδικτυακή εμπειρία.

Επιπλέον, η κυβερνοασφάλεια είναι ζωτικής σημασίας για την οικονομική ευημερία των επιχειρήσεων. Σύμφωνα με μια μελέτη που διεξήχθη από την Hiscox, οι επιθέσεις στον κυβερνοχώρο κόστισαν στις μικρές και μεσαίες επιχειρήσεις κατά μέσο όρο 200.000 $ το 2019, και ο αριθμός αυτός αυξάνεται σταθερά [42]. Η εφαρμογή ισχυρών μέτρων κυβερνοασφάλειας συμβάλλει στην ελαχιστοποίηση των κινδύνων και δίνει τη δυνατότητα στις επιχειρήσεις να λειτουργούν με ασφάλεια, διασφαλίζοντας τη συνεχή ανάπτυξή τους.

Η κυβερνοασφάλεια είναι επίσης ζωτικής σημασίας για την προστασία των υποδομών ζωτικής σημασίας και της δημόσιας ασφάλειας. Όπως αναφέρθηκε προηγουμένως, οι επιθέσεις σε δίκτυα ηλεκτρικής ενέργειας, εγκαταστάσεις επεξεργασίας νερού ή συστήματα μεταφοράς μπορεί να έχουν τρομερές συνέπειες. Επενδύοντας σε ισχυρά μέτρα κυβερνοασφάλειας, οι κυβερνήσεις και οι φορείς εκμετάλλευσης υποδομών μπορούν να ενισχύσουν την άμυνά τους έναντι πιθανών επιθέσεων στον κυβερνοχώρο, διασφαλίζοντας τη σταθερότητα και την ασφάλεια βασικών υπηρεσιών.

Αναγνωρίζοντας τη σημασία και την αυξανόμενη απειλή των επιθέσεων στον κυβερνοχώρο, η αγορά της κυβερνοασφάλειας έχει δει εκθετική ανάπτυξη τα τελευταία χρόνια. Η παγκόσμια αγορά κυβερνοασφάλειας αποτιμήθηκε σε 147,42

δισεκατομμύρια δολάρια το 2022 και προβλέπεται να φτάσει τα 256,60 δισεκατομμύρια δολάρια έως το 2028 [43]. Αυτή η ανάπτυξη μπορεί να αποδοθεί σε διάφορους παράγοντες, όπως ο αυξανόμενος αριθμός και η πολυπλοκότητα των επιθέσεων στον κυβερνοχώρο, η αυξανόμενη υιοθέτηση υπηρεσιών cloud και οι αυστηροί κανονισμοί προστασίας δεδομένων που επιβάλλονται από τις κυβερνήσεις παγκοσμίως.

Η αγορά της κυβερνοασφάλειας παρουσιάζει σημαντικές ευκαιρίες για διάφορους ενδιαφερόμενους, από παρόχους τεχνολογίας έως ειδικούς στον τομέα της κυβερνοασφάλειας. Εταιρείες που ειδικεύονται σε λύσεις κυβερνοασφάλειας, όπως λογισμικά προστασίας από ιούς, τείχη προστασίας, συστήματα ανίχνευσης και πρόληψης εισβολών και εργαλεία κρυπτογράφησης, έχουν σημειώσει αξιοσημείωτη ανάπτυξη και ζήτηση. Επιπλέον, οι επαγγελματίες της κυβερνοασφάλειας με εξειδίκευση σε τομείς, όπως το ηθικό hacking, η αξιολόγηση τρωτότητας και η αντιμετώπιση επιθέσεων, έχουν μεγάλη ζήτηση, καθώς οι οργανισμοί επιδιώκουν να ενισχύσουν τις δυνατότητες αντιμετώπισης επιθέσεων στον κυβερνοχώρο.

Συμπερασματικά, οι επιθέσεις στον κυβερνοχώρο αποτελούν σοβαρές απειλές για ιδιώτες, οργανισμούς ακόμα και κρατικούς φορείς. Ο αντίκτυπος αυτών των επιθέσεων κυμαίνεται από την απώλεια ευαίσθητων πληροφοριών έως τη διακοπή παροχής υπηρεσιών ζωτικής σημασίας. Ως αποτέλεσμα, η σημασία της κυβερνοασφάλειας έχει αυξηθεί πάρα πολύ. Αποτελεσματικά μέτρα κυβερνοασφάλειας προστατεύουν τις προσωπικές πληροφορίες, προστατεύουν τις επιχειρήσεις και διασφαλίζουν τη σταθερότητα των βασικών υπηρεσιών. Η αυξανόμενη αγορά για την ασφάλεια στον κυβερνοχώρο παρουσιάζει σημαντικές ευκαιρίες, τόσο για τους παρόχους τεχνολογίας, όσο και για τους επαγγελματίες της κυβερνοασφάλειας.

1.2 Συνήθεις τύποι κυβερνοεπιθέσεων

Σε αυτή την ενότητα θα αναπτυχθούν εν συντομία οι πιο κοινές επιθέσεις στον κυβερνοχώρο. Επίθεση στον κυβερνοχώρο ή Cyber Attack ορίζεται κάθε μη εξουσιοδοτημένη προσπάθεια πρόσβασης, διακοπής ή πρόκλησης βλάβης σε ένα σύστημα υπολογιστών, δίκτυα ή ψηφιακές συσκευές.

1.2.1 Επίθεση Man In the Middle (MITM)

Η επίθεση MITM αποτελεί μία από τις παλαιότερες επιθέσεις και αφορά την παρακολούθηση της επικοινωνίας μεταξύ δύο οντοτήτων από έναν επιτιθέμενο (hacker) με σκοπό την τροποποίηση ή την συλλογή δεδομένων (π.χ. προσωπικών, οικονομικών) [1]. Η επίθεση αυτή μπορεί να υλοποιηθεί με πολλούς τρόπους,

οι οποίοι μπορούν να ενταχθούν σε δύο ευρύτερες μεθόδους, την προσπάθεια παράκαμψης ή χειραγώγησης των πρωτόκολλων ασφαλείας όπως το SSL/TLS που χρησιμοποιούνται για την ασφάλεια του καναλιού επικοινωνίας μεταξύ του Client και του Server, και την υποκλοπή της μεταξύ τους επικοινωνίας ανακατευθύνοντας όλη τη κίνηση των δεδομένων μέσα από ένα κόμβο που ελέγχεται από τους επιτιθέμενους [1]. Οι κατηγορίες αυτού του τύπου επιθέσεων περιγράφονται παρακάτω.

1.2.1.1 HTTPS Spoofing

Είναι μία ιδιαίτερη περίπτωση καθώς ορισμένοι ειδικοί λένε ότι πρόκειται για μία επίθεση Phishing, ενώ άλλοι ότι πρόκειται για MITM. Η τακτική είναι η δημιουργία ενός domain που μοιάζει πολύ με αυτόν του κανονικού ιστότοπου. Αυτή η τακτική είναι γνωστή και ώς "homograph attack", όπου οι χαρακτήρες στο όνομα του domain στόχου αντικαθίστανται με χαρακτήρες που δεν είναι ASCII αλλά μοιάζουν σε εμφάνιση. Έτσι ο ανυποψίαστος χρήστης είναι πιθανό να μην δει την διαφορά και να χρησιμοποιήσει την ιστοσελίδα κανονικά [1].

1.2.1.2 SSL Session Hijacking

Το Session hijacking, γνωστό και ως cookie side-jacking, είναι μια μορφή επίθεσης που θα δώσει σε έναν χάκερ πλήρη πρόσβαση σε έναν διαδικτυακό λογαριασμό. Όταν συνδεόμαστε σε ένα διαδικτυακό λογαριασμό η εφαρμογή μας επιστρέφει ένα "session cookie", δηλαδή ένα τμήμα δεδομένων που προσδιορίζει τον χρήστη στο διακομιστή, του δίνει πρόσβαση στον λογαριασμό του και παραμένει ενεργό μέχρι ο χρήστης να αποσυνδεθεί από την εφαρμογή. Σε αυτή την επίθεση, ο κυβερνοεγκληματίας κλέβει το διακριτικό περιόδου λειτουργίας του χρήστη και το χρησιμοποιεί για να αποκτήσει πρόσβαση στον λογαριασμό του [1].

1.2.1.3 SSL Stripping

Η επίθεση είναι γνωστή και ως downgrade attack, καθώς ο επιτιθέμενος προσπαθεί να υποβαθμίσει το επίπεδο ασφαλείας στις επικοινωνίες των μερών, αφαιρώντας την κρυπτογράφηση. Όταν ένα θύμα θέλει να συνδεθεί σε έναν διακομιστή, ο επιτιθέμενος υποκλέπτει το αίτημα και δημιουργεί μια ανεξάρτητη, νόμιμη σύνδεση με τον διακομιστή μέσω πρωτοκόλλου HTTPS. Στην συνέχεια, όταν ο επιτιθέμενος λάβει την απάντηση του διακομιστή, την αναμεταδίδει στο θύμα σε μη κρυπτογραφημένη μορφή, παριστάνοντας τον διακομιστή [1].

1.2.1.4 IP Spoofing

Τα δεδομένα στο διαδίκτυο μεταφέρονται μέσω πακέτων. Τα πακέτα περιέχουν την ταυτότητα του αποστολέα και του παραλήπτη με την μορφή διευθύνσεων IP. Σε αυτή την περίπτωση, ο επιτιθέμενος στέκεται ανάμεσα σε δύο μέρη που επικοινωνούν, πλαστογραφώντας τις διευθύνσεις τους. Με αυτόν τον τρόπο, κάθε ένα από τα θύματα στέλνει τα πακέτα του δικτύου του στον εισβολέα, αντί να τα στείλει απευθείας στον πραγματικό του προορισμό. Αυτή η τακτική μπορεί να χρησιμοποιηθεί και σε επιθέσεις Distributed Denial of Service (DDoS) [2].

1.2.1.5 DNS Spoofing

Το DNS είναι ένα πρωτόκολλο για την αντιστοίχιση της διεύθυνσης IP προορισμού, όταν υποβάλλεται αίτημα από έναν πελάτη. Όταν υποβάλλεται ένα αίτημα για έναν συγκεκριμένο ιστότοπο, το πρόγραμμα περιήγησης και το λειτουργικό σύστημα αναζητούν μια αντίστοιχη καταχώρηση από την προσωρινή μνήμη ή τον εσωτερικό χώρο αποθήκευσης της συσκευής. Εάν δεν το βρει εκεί, τότε θέτει το ερώτημα (queries) για αναζήτηση αυτής της διεύθυνσης IP. Όταν βρει την αντίστοιχη διεύθυνση IP, συνδέει τον πελάτη με αυτήν. Ο επιτιθέμενος αντικαθιστά μια νόμιμη διεύθυνση IP στα αρχεία ενός διακομιστή DNS και με αυτόν τον τρόπο μπορεί να ανακατευθύνει και να συλλέξει τα δεδομένα που στέλνει ο πελάτης και ο διακομιστής [3].

1.2.1.6 ARP Spoofing

Η πλαστογράφηση ARP είναι ένας τύπος επίθεσης κατά την οποία ένας επιτιθέμενος στέλνει παραποιημένα μηνύματα ARP μέσω ενός τοπικού δικτύου. Αυτό έχει ως αποτέλεσμα τη σύνδεση της διεύθυνσης MAC του με τη διεύθυνση IP ενός νόμιμου υπολογιστή ή διακομιστή στο δίκτυο. Μόλις η διεύθυνση MAC συνδεθεί με μια αυθεντική διεύθυνση IP, ο επιτιθέμενος θα αρχίσει να λαμβάνει όλα τα δεδομένα που προορίζονται για αυτήν τη διεύθυνση IP. Η πλαστογράφηση ARP μπορεί να επιτρέψει στους κυβερνοεγκληματίες να υποκλέψουν, να τροποποιήσουν ή ακόμα και να σταματήσουν τη μεταφορά δεδομένων. Οι επιθέσεις αυτού του τύπου μπορούν να συμβούν μόνο σε τοπικά δίκτυα που χρησιμοποιούν το ARP [3].

1.2.1.7 Μέτρα προστασίας απέναντι σε επιθέσεις MITM

Ορισμένα μέτρα που μπορούν να ληφθούν για την αποφυγή τέτοιου είδους επιθέσεων είναι [1]:

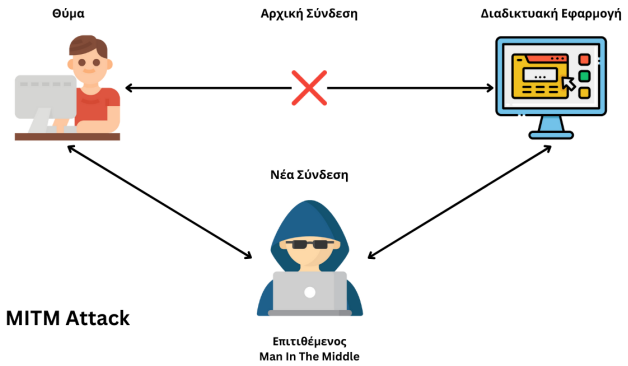

FIGURE 1.1: MITM Attack

- Η αποφυγή της χρήσης Wi-Fi χωρίς κωδικό πρόσβασης.
- Η αποφυγή ανταλλαγής ευαίσθητων πληροφοριών και χρηματικών συναλλαγών σε δημόσια δίκτυα.
- Χρήση μόνο HTTPS ιστοσελίδων.

1.2.1.8 Χαρακτηριστικές MITM επιθέσεις

- **Superfish**: Το 2015 οι υπολογιστές Lenovo κυκλοφόρησαν με προεγκατεστημένο adware που έκανε τους χρήστες ευάλωτους σε επιθέσεις MiTM. Αυτό το λογισμικό, γνωστό ως Superfish Visual Search, εισήγαγε διαφημίσεις στις ιστοσελίδες που επισκέπτονταν ο χρήστης. Μια ενημέρωση του Microsoft Windows Defender τον Φεβρουάριο του 2015 αφαίρεσε αυτήν την ευπάθεια [44].
- **DigiNotar**: Ο εκδότης ψηφιακών πιστοποιητικών ασφαλείας παραβιάστηκε το 2011 όταν ένας επιτιθέμενος απέκτησε πρόσβαση σε 500 πιστοποιητικά για ιστότοπους, όπως η Google και το Skype. Ο επιτιθέμενος χρησιμοποίησε την τακτική μιας επίθεσης MiTM εξαπατώντας τους χρήστες να εισάγουν κωδικούς πρόσβασης σε ψεύτικους ιστότοπους που υποδύονταν τους πραγματικούς. Η DigiNotar υπέβαλε τελικά αίτηση πτώχευσης για να ανακάμψει από τις απώλειες αυτής της παραβίασης δεδομένων [45].

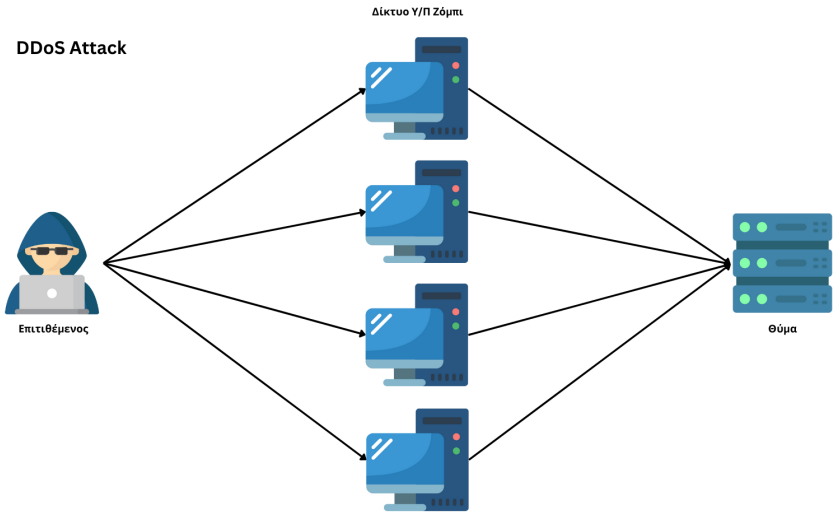

FIGURE 1.2: DDoS Attack

1.2.2 Distributed Denial of Service (DDoS) Attack

Είναι μία επίθεση κατά την οποία το σύστημα ή ο υπολογιστής σταματάει να ανταποκρίνεται σε οποιαδήποτε εντολή από τον κάτοχό του (denial of service). Αυτό συμβαίνει όταν ένας κακόβουλος χρήστης αποκτά ένα δίκτυο υπολογιστών ζόμπι για να σαμποτάρει έναν συγκεκριμένο ιστότοπο ή διακομιστή. Ο κακόβουλος χρήστης δίνει την εντολή σε όλους τους υπολογιστές ζόμπι να επικοινωνούν με έναν συγκεκριμένο ιστότοπο ή διακομιστή ξανά και ξανά [4]. Οι επιθέσεις DDoS ταξινομούνται σε δύο τύπους με βάση το επίπεδο προτοκόλου που στοχεύουν, όπως περιγράφονται παρακάτω.

1.2.2.1 Application Layer

Σε αυτή την επίθεση γίνεται προσπάθεια εξάντλησης των πόρων του διακομιστή (Sockets, CPU, memory, disk/database bandwidth, and I/O bandwidth) μέσω φαινομενικά νόμιμων και μη κακόβουλων αιτημάτων και συνήθως καταναλώνουν λιγότερο bandwith [4].

1.2.2.2 Network or Transport Layer

Ο στόχος της επίθεσης είναι να κορεστούν οι δομές του δικτύου (servers, routers, switches) μέσω της δημιουργίας μεγάλης κίνησης στο δίκτυο [4].

1.2.2.3 Μέτρα προστασίας απέναντι σε επιθέσεις DDoS

Ορισμένα μέτρα που μπορούν να ληφθούν για την αποφυγή τέτοιου είδους επιθέσεων είναι [5]:

- Εφαρμογή φίλτρων στο router για απόρριψη πακέτων από ύποπτες πηγές.
- Συνεχής παρακολούθηση της εισερχόμενης κίνησης που πλήττει τον διακομιστή. Όσο πιο γρήγορα εντοπιστεί μια ασυνήθιστη αύξηση στην κυκλοφορία που φαίνεται ύποπτη, τόσο πιο γρήγορα μπορεί να ξεκινήσει η έρευνα.
- Περιορισμός στον αριθμό των αιτημάτων που μπορεί να δεχθεί ο διακομιστής και εφαρμογή τείχους προστασίας σε διαδικτυακές εφαρμογές (Web application firewall - WAF).

1.2.2.4 Χαρακτηριστικές DDos επιθέσεις

- **AWS DDoS Attack**: Η Amazon Web Services, χτυπήθηκε από μια γιγαντιαία επίθεση DDoS τον Φεβρουάριο του 2020. Στόχευε έναν αγνώστων στοιχείων πελάτη AWS χρησιμοποιώντας μια τεχνική που ονομάζεται Connectionless Lightweight Directory Access Protocol (CLDAP). Αυτή η τεχνική βασίζεται σε ευάλωτους διακομιστές CLDAP τρίτων και ενισχύει τον όγκο των δεδομένων που αποστέλλονται στη διεύθυνση IP του θύματος κατά 56 έως 70 φορές. Η επίθεση διήρκεσε τρεις ημέρες και στην κορύφωση έφτασε στα 2,3 terabyte ανά δευτερόλεπτο [46].
- **GitHub Attack**. Το 2018,το GitHub δέχτηκε επίθεση DDoS με όγκο δεδομένων που έφτασε τα 1,35 terabit ανά δευτερόλεπτο (Tbps) στέλνοντας πακέτα με ρυθμό 126,9 εκατομμύρια ανά δευτερόλεπτο [47].

1.2.3 Phishing attacks

Η επίθεση phishing είναι η πρακτική της αποστολής μηνυμάτων ηλεκτρονικού ταχυδρομείου,σε κοινωνικά δίκτυα αλλά και προσωπικά μηνύματα που φαίνεται να προέρχονται από αξιόπιστες πηγές με στόχο την απόκτηση προσωπικών πληροφοριών των χρηστών. Συνδυάζει κοινωνική μηχανική (social engineering) και τεχνικές ικανότητες. Μπορεί να είναι από ένα συνημμένο σε ένα email που φορτώνει κακόβουλο λογισμικό στον υπολογιστή ή να είναι ένας σύνδεσμος προς έναν ιστότοπο που μοιάζει αξιόπιστος ώστε να κατεβάσει το θύμα κακόβουλο λογισμικό [6]. Βασικές υποκατηγορίες κατηγορίες του Phishing περιγράφονται παρακάτω.

1.2.3.1 Spear Phishing

Ο επιτιθέμενος αφιερώνει κάποιο χρόνο ώστε να συγκεντρώσει περισσότερες πληροφορίες για το υποψήφιο θύμα του για να κάνει την επίθεση πιο εστιασμένη και άρα να έχει περισσότερες πιθανότητες επιτυχίας [6].

1.2.3.2 Whaling

Ο επιτιθέμενος, όπως και στο spear phishing, αφιερώνει αρκετό χρόνο για να μαζέψει πολλές πληροφορίες για το θύμα του όπου συνήθως είναι CEO και άλλα υψηλόβαθμα στελέχη μεγάλων επιχειρήσεων. Είναι ιδιαίτερα επικίνδυνος τύπος επίθεσης καθώς αυτά τα στελέχη έχουν πρόσβαση σε πολλά δεδομένα της κάθε εταιρείας [6].

1.2.3.3 Vishing

Ο επιτιθέμενος τηλεφωνεί στο υποψήφιο θύμα και ζητά προσωπικές πληροφορίες παριστάνοντας ότι τηλεφωνεί από έγκυρη πηγή π.χ μία τράπεζα. Μπορεί να είναι και αυτοματοποιημένο ηχητικό μήνυμα [6].

1.2.3.4 Smishing

Ο επιτιθέμενος στέλνει SMS στα υποψήφια θύματα παριστάνοντας ότι είναι έγκυρη πηγή και τα καθοδηγεί να εκτελέσουν συγκεκριμένες όπως το άνοιγμα παγιδευμένων συνδέσμων όπου μπορούν να κλαπούν διαπιστευτήρια εισόδου της πραγματικής σελίδα [6].

1.2.3.5 Μέτρα προστασίας σε επιθέσεις Phishing

Ορισμένα μέτρα που μπορούν να ληφθούν για την αποφυγή τέτοιου είδους επιθέσεων είναι [6]:

- Εκπαίδευση και κριτική σκέψη για την αποδοχή και το άνοιγμα ύποπτων μηνυμάτων.
- Άνοιγμα ύποτπων μηνυμάτων σε εικονικό περιβάλλον.
- Μη αποστολή ευαίσθητων πληροφοριών μέσω email.

1.2.3.6 Χαρακτηριστικές Phishing επιθέσεις:

- **Phish Phry**: Το 2009 κυβερνοεγκληματίες έστειλαν μηνύματα ηλεκτρονικού ταχυδρομείου σε θύματα προσποιούμενα ότι προέρχονται από τράπεζες. Τα θύματα στη συνέχεια καθοδηγούνταν στο να επισκεφτούν ιστοσελίδες

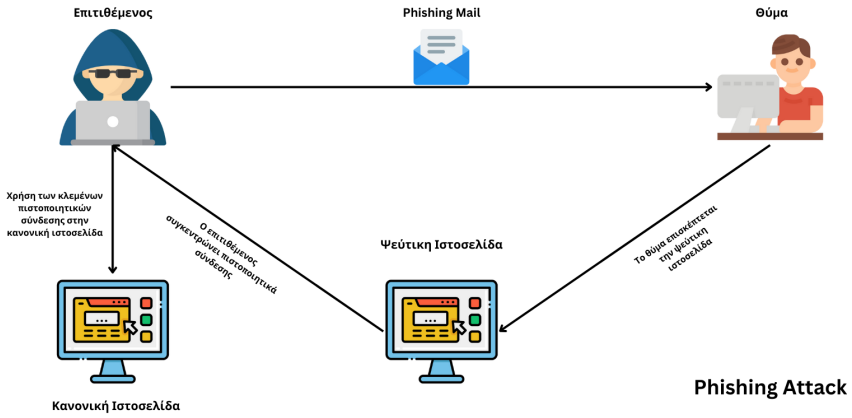

FIGURE 1.3: Phishing Attack

παρόμοιες με αυτές των τραπεζών τους, ώστε κατά την εισαγωγή των πιστοποιητικών εισόδου σε αυτές οι κυβερνοεγκληματίες να τα αποσπάσουν. Με αυτόν τον τρόπο κλάπηκαν πάνω από 1.5 εκατομμύρια δολάρια [48].

- **Nordea**: Το 2007, η σουηδική τράπεζα Nordea έχασε πάνω από 7 εκατομμύρια κορώνες όταν οι phishers κατάφεραν να στείλουν δόλια μηνύματα ηλεκτρονικού ταχυδρομείου στους πελάτες της τράπεζας, δελεάζοντάς τους να εγκαταστήσουν το "haxdoor" Trojan μεταμφιεσμένο ως λογισμικό προστασίας από ανεπιθύμητα μηνύματα [49].

1.2.4 SQL injection

Η έγχυση (SQLi) είναι μια ευπάθεια ασφαλείας που επιτρέπει σε έναν εισβολέα να παρεμβαίνει στα ερωτήματα (queries) που κάνει μια εφαρμογή στη βάση δεδομένων της. Γενικά επιτρέπει σε έναν εισβολέα να αποκτά πρόσβαση σε δεδομένα που συνήθως δεν είναι σε θέση να ανακτήσει. Αυτό μπορεί να περιλαμβάνει δεδομένα που ανήκουν σε άλλους χρήστες ή οποιαδήποτε άλλα δεδομένα στα οποία μπορεί να έχει πρόσβαση η ίδια η εφαρμογή. Σε πολλές περιπτώσεις, ένας εισβολέας μπορεί να τροποποιήσει ή να διαγράψει αυτά τα δεδομένα, προκαλώντας μόνιμες αλλαγές στο περιεχόμενο ή τη συμπεριφορά της εφαρμογής [50]. Κατηγορίες SQLi είναι οι εξής:

1.2.4.1 In-band SQLi

Ο επιτιθέμενος χρησιμοποιεί το ίδιο κανάλι επικοινωνίας για να πραγματοποιήσει τις επιθέσεις του και να συλλέξει τις πληροφορίες/αποτελέσματα αυτής. Οι δύο συνηθισμένοι τύποι in-band SQLi είναι:

Error-based SQL injection: Ο επιτιθέμενος εκτελεί ορισμένες ενέργειες που προκαλούν τη δημιουργία μηνυμάτων σφάλματος στη βάση δεδομένων. Χρησιμοποιώντας το μήνυμα σφάλματος είναι δυνατός ο προσδιορισμός του τύπου βάσης δεδομένων που χρησιμοποιείται, την έκδοση κ.λπ.

Union-based SQL injection: Ο επιτιθέμενος χρησιμοποιεί τον τελεστή UNION για να συνδυάσει μια δήλωση SQL με μια κακόβουλη δήλωση. Η κακόβουλη δήλωση πρέπει να χρησιμοποιεί τις ίδιες στήλες και τύπους δεδομένων με την αρχική δήλωση. Μια ευάλωτη βάση δεδομένων επεξεργάζεται τη συνδυασμένη πρόταση και εκτελεί τον κακόβουλο κώδικα.

1.2.4.2 Blind SQLi

Ονομάζεται Blind(τυφλή) γιατί ο επιτιθέμενος δεν βλέπει τα αποτελέσματα της επίθεσης αμέσως. Υποκατηγορίες είναι:
Boolean-based SQL Injection: Εδώ, ο εισβολέας θα στείλει ένα ερώτημα SQL στη βάση δεδομένων ζητώντας από την εφαρμογή να επιστρέψει ένα διαφορετικό αποτέλεσμα ανάλογα με το αν το ερώτημα επιστρέφει True ή False.

Time-based SQL Injection: Ο επιτιθέμενος στέλνει ένα ερώτημα SQL στη βάση δεδομένων, το οποίο κάνει τη βάση δεδομένων να περιμένει ένα συγκεκριμένο χρονικό διάστημα πριν κοινοποιήσει το αποτέλεσμα. Ο χρόνος απόκρισης βοηθά τον εισβολέα να αποφασίσει εάν ένα ερώτημα είναι Σωστό ή Λάθος.

1.2.4.3 Out-of-bound SQL Injection

Ο επιτιθέμενος δεν μπορεί να χρησιμοποιήσει το ίδιο κανάλι επικοινωνίας για να υλοποιήσει μια επίθεση και να συγκεντρώσει τις πληροφορίες/αποτελέσματα.

1.2.4.4 Μέτρα προστασίας σε επιθέσεις SQLi

Ορισμένα μέτρα που μπορούν να ληφθούν για την αποφυγή τέτοιου είδους επιθέσεων είναι:

- Prepared Statements και Parameterized Queries διασφαλίζουν ότι οι παράμετροι που στέλνονται στην βάση δεδομένων είναι ορθοί.
- Εφαρμογή κατακερματισμού (hashing) στους κωδικούς πρόσβασης.

FIGURE 1.4: SQLi Attack

- Escaping inputs: είναι μια μέθοδος κατά την οποία οι συναρτήσεις διαφυγής χαρακτήρων που παρέχονται από το DBMS χρησιμοποιούνται για έλεγχο των στοιχείων που παρέχονται από το χρήστη.

1.2.4.5 Χαρακτηριστικές SQLi τρωτότητες:

Ευπάθεια Tesla—το 2014, ερευνητές ασφαλείας δημοσίευσαν ότι κατάφεραν να παραβιάσουν τον ιστότοπο της Tesla χρησιμοποιώντας SQLi, καταφέρνοντας να αποκτήσουν δικαιώματα διαχειριστή και να κλέψουν δεδομένα χρηστών [51].

Ευπάθεια Cisco—το 2018, βρέθηκε μια ευπάθεια SQLi στο Cisco Prime License Manager. Η ευπάθεια επέτρεψε στους εισβολείς να αποκτήσουν πρόσβαση φλοιού (shell access) στα συστήματα. Η Cisco έχει επιδιορθώσει την ευπάθεια [52].

1.2.5 Malware

Malware ή αλλιώς malicious software είναι ένα κακόβουλο λογισμικό το οποίο έχει ώς στόχο να εισχωρήσει και να καταστρέψει μια συσκευή ή ένα δίκτυο. Ανάλογα με τρόπο λειτουργίας του εκάστοτε προγράμματος αυτό μπορεί να ταξινομηθεί σε μία από τις παρακάτω κατηγορίες.

1.2.5.1 Virus

Virus ή ιός είναι ένα κακόβουλο λογισμικό το οποίο παίρνει την μορφή κώδικα που έχει τοποθετηθεί σε μία εφαρμογή ή ένα πρόγραμμα. Παραμένει ανενεργός μέχρι

να ενεργοποιηθεί για πρώτη φορά από τον ίδιο τον χρήστη. Έπειτα μπορεί να πολλαπλασιαστεί και να προσβάλει περισσότερα αρχεία του συστήματος αλλά και το ίδιο το σύστημα. Μπορεί να προκαλέσει απώλεια δεδομένων ,δυσλειτουργία εφαρμογών, αργή λειτουργία του υπολογιστή. Ο πιο σύνηθες τρόπος για να προσβληθεί ένα σύστημα από ιό είναι μέσω συνημμένων αρχείων σε ύποπτα email και λήψη αρχείων από μη έγκυρες πηγές [7].

Ένας από τους πιο γνωστούς ιούς αποτελεί ο ILOVEYOU [53]. Ο ιός μεταδόθηκε μέσω του ηλεκτρονικού ταχυδρομείου όπου υποδύονταν ένα ερωτικό γράμμα με όνομα "LOVE-LETTER-FOR-YOU.TXT.vbs" και θέμα "I love you".Ήταν ένα Microsoft Visual Basic Script και διέγραφε προσωπικά και αρχεία του συστήματος.Υπολογίζεται ότι οι ζημιές που προκάλεσε μπορεί να αγγίζουν τα 15 δις.

1.2.5.2 Worm

Worm ή αλλιώς σκουλήκι είναι ένα κακόβουλο λογισμικό που μοιάζει με τους ιούς αλλά σε αντίθεση με αυτούς μπορεί να εξαπλωθεί μόνο του κάνοντας χρήση της υπάρχουσας δικτυακής υποδομής ή υπηρεσιών του διαδικτύου. Τα λογισμικά αυτού του τύπου δεν προσκολλώνται σε άλλα αρχεία προκειμένου να επιβιώσουν αλλά λειτουργούν ως αυτόνομα προγράμματα. Για την εξάπλωση τους χρησιμοποιούν από απλές μεθόδους όπως η αποστολή email αλλά και πιο περίπλοκες όπως η εκμετάλλευση ευπαθειών του λειτουργικού συστήματος. Μπορούν να προκαλέσουν απώλεια δεδομένων, δημιουργία backdoor, να βοηθήσουν στην εξάπλωση άλλων κακόβουλων λογισμικών όπως spyware κλπ [7].

Χαρακτηριστικό παράδειγμα Worm είναι το σκουλήκι Morris που κυκλοφόρησε το 1988 και θεωρείται ως το πρώτο σκουλήκι υπολογιστή [54]. Το σκουλήκι Morris ήταν το έργο του Robert Tappan Morris Jr., ενός μεταπτυχιακού φοιτητή στο Cornell, ο οποίος φέρεται να προσπαθούσε να απαριθμήσει όλα τα συστήματα που ήταν συνδεδεμένα στο δίκτυο ARPANET. Στοχεύοντας τα τρωτά σημεία σε πολλά διαφορετικά προγράμματα Unix, το worm Morris ήταν ικανό να μολύνει ένα σύστημα περισσότερες από μία φορές. Το σκουλήκι επηρέασε έως και το 10% από τα 60.000 συστήματα που πιστεύεται ότι είναι συνδεδεμένα με το ARPANET.

1.2.5.3 Trojan

Trojans είναι ένας τύπος κακόβουλου λογισμικού που μεταμφιέζεται ως καλόπιστο λογισμικό, εφαρμογές ή αρχεία για να παραπλανήσει τους χρήστες να το κατεβάσουν και εν αγνοία τους να παραχωρήσουν τον έλεγχο των συσκευών τους. Μόλις εγκατασταθεί, ένα trojan μπορεί να εκτελέσει την ενέργεια για την οποία σχεδιάστηκε όπως διαγραφή αρχείων,παρακολούθηση δραστηριότητας

χρηστών,έλεγχος συσκευής .Το κακόβουλο λογισμικό trojan διαδίδεται συχνά μέσω συνημμένων ηλεκτρονικού ταχυδρομείου και ύποπτης λήψης από ιστότοπο. Όπως και οι ιοί, απαιτεί την ενέργεια του χρήστη για να ενεργοποιηθεί με τη διαφορά ότι τα Trojans δεν αυτο-αναπαράγονται [7].

Γνωστό λογισμικό Trojan είναι το ZeuS/Zbot [55]. Υπολογίζεται ότι έχει μολύνει πάνω από 3,6 εκατομμύρια υπολογιστές στις ΗΠΑ, συμπεριλαμβανομένων μηχανημάτων που ανήκουν στη NASA, την Bank of America και το Υπουργείο Μεταφορών των ΗΠΑ. Το ZeuS μολύνει υπολογιστές με λειτουργικό Windows και στέλνει δεδομένα από τον υπολογιστή του θύματος στο διακομιστή ZeuS. Το αδύνατο σημείο του συστήματος αυτού είναι ο ενιαίος διακομιστής C&C, ο οποίος αποτέλεσε το πρωταρχικό στόχο για τις υπηρεσίες επιβολής του νόμου.

1.2.5.4 Fileless Malware

Σε αντίθεση με το κοινό κακόβουλο λογισμικό, το οποίο χρησιμοποιεί εκτελέσιμα αρχεία για να μολύνει συσκευές, το κακόβουλο λογισμικό χωρίς αρχεία χρησιμοποιεί την μνήμη του συστήματος. Εκμεταλλεύεται αντικείμενα που δεν είναι αρχεία αλλά ήδη υπάρχων προεγκατεστημένο λογισμικό, όπως μακροεντολές του Microsoft Office, PowerShell, WMI. Επειδή δεν υπάρχει εκτελέσιμο αρχείο, είναι δύσκολο να εντοπιστεί από τα συστήματα ασφαλείας [8].

Ένα αξιοσημείωτο παράδειγμα επίθεσης κακόβουλου λογισμικού χωρίς αρχεία ήταν το Operation Cobalt Kitty, στο οποίο η ομάδα OceanLotus διείσδυσε σε πολλές εταιρείες και παρακολουθούσε την δραστηριότητα τους για διάστημα έξι μηνών πριν εντοπιστεί [56].

1.2.5.5 Adware

Το Adware, όπως υποδηλώνει το όνομα, είναι κακόβουλο λογισμικό που σχετίζεται με τις διαφημίσεις που συναντάμε στο διαδίκτυο. Το λογισμικό αυτό εμφανίζει ανεπιθύμητες διαφημίσεις στον υπολογιστή σας, μερικές φορές με τη μορφή αναδυόμενων διαφημίσεων. Αυτές οι ανεπιθύμητες διαφημίσεις μπορεί να οδηγήσουν τους χρήστες να κατεβάσουν κάποιο κακόβουλο λογισμικό κατα λάθος, να συλλέξουν δεδομένα που σχετίζονται με το ιστορικό αναζήτησης, με δεδομένα εισόδου σε ηλεκτρονικές υπηρεσίες και να τα πουλήσουν σε τρίτους [7].

Χαρακτηριστική περίπτωση Adware αποτελεί το Fireball. Έγινε γνωστό το 2017, όταν μια μελέτη που παραγγέλθηκε από μια ισραηλινή εταιρεία λογισμικού διαπίστωσε ότι περισσότεροι από 250 εκατομμύρια υπολογιστές και το ένα πέμπτο των εταιρικών δικτύων σε όλο τον κόσμο είχαν μολυνθεί από αυτό [57].

1.2.5.6 Spyware

Το Spyware είναι ένα κακόβουλο πρόγραμμα που όταν εγκαθίσταται σε ένα υπολογιστή, καταγράφει και μεταδίδει προσωπικές πληροφορίες του χρήστη. Το λογισμικό αυτό επιτρέπει στο διαχειριστή του να παρακολουθεί όλες τις μορφές επικοινωνίας στη στοχευμένη συσκευή. Τέτοια λογισμικά χρησιμοποιούνται συχνά από τις αρχές επιβολής του νόμου, κυβερνητικές υπηρεσίες και οργανισμούς ασφάλειας για την παρακολούθηση των επικοινωνιών υπόπτων. Το spyware είναι επίσης διαθέσιμο στους καταναλωτές, επιτρέποντας στους αγοραστές του να κατασκοπεύουν από αντίπαλες εταιρείες μέχρι και πρόσωπα του στενού τους περιβάλλον [7].

Γνωστά λογισμικά Spyware:

Pegasus: σχεδιάστηκε από την Ισραηλινή NSO Group και είναι ένα από τα πιο πρόσφατα ευρείας χρήσης spyware. Αν και το Pegasus αρχικά αναπτύχθηκε για την καταπολέμηση της τρομοκρατίας, τα στοιχεία δείχνουν ότι πολλοί πελάτες χρησιμοποιούν το Pegasus για να κατασκοπεύουν δημοσιογράφους, πολιτικούς αντιπάλους και σχεδόν όποιον επιθυμεί ο πελάτης. Αγοραστές και χρήστες του συγκεκριμένου λογισμικού έχουν υπάρξει κυβερνήσεις της Γαλλίας, της Ουγγαρίας, των Ηνωμένων Αραβικών Εμιράτων, της Σαουδικής Αραβίας, της Ινδίας και άλλων [58].

FinSpy: είναι μια προηγμένη σουίτα εργαλείων παρακολούθησης που χρησιμοποιούν υπηρεσίες επιβολής του νόμου και υπηρεσίες πληροφοριών. Το FinSpy λειτουργεί σε λειτουργικά συστήματα Windows, macOS, Linux, Android και iOS. Οι δυνατότητές του ποικίλλουν ανάλογα με την πλατφόρμα. Έχει την δυνατότητα να ενεργοποιεί κρυφά τα μικρόφωνα για την εγγραφή συνομιλιών, την ενεργοποίηση της κάμερας, την εγγραφή και μετάδοση εικόνων, τη μετάδοση χρήσης πλήκτρων, την τροποποίηση αρχείων [59].

1.2.5.7 Botnet

Ο όρος botnet αποτελείται από το “bot” και από το “net”. Το bot προέρχεται από το robot το οποίο είναι ένα λογισμικό το οποίο θέτει έναν υπολογιστή, ένα κινητό ακόμα και ένα ολόκληρο διακομιστή υπό τον έλεγχο κυβερνοεγκληματιών. Το net δηλώνει ότι πρόκειται για ένα ολόκληρο δίκτυο από ηλεκτρονικές συσκευές που έχουν μολυνθεί από bot malware και ελέγχεται από το “botherder”. Ο επιτιθέμενος μπορεί να δώσει εντολή σε κάθε υπολογιστή στο botnet του να πραγματοποιήσει μια συντονισμένη επίθεση. Η κλίμακα ενός botnet (πολλά αποτελούνται από εκατομμύρια bot) επιτρέπει στον εισβολέα να εκτελεί επιθέσεις

μεγάλης κλίμακας που προηγουμένως ήταν αδύνατες με χρήση ενός μόνο υπολογιστή. Δεδομένου ότι τα botnet παραμένουν υπό τον έλεγχο ενός απομακρυσμένου εισβολέα, τα μολυσμένα μηχανήματα μπορούν να λαμβάνουν ενημερώσεις και να αλλάζουν τη συμπεριφορά τους αμέσως. Συχνά οι bot-herders νοικιάζουν τμήματα του botnet τους στη μαύρη αγορά. Μερικές επιθέσεις που μπορούν να προκαλέσουν είναι DDoS, Click fraud, SpamBot [9].

Γνωστά Botnet αποτελούν :

Storm: το Storm ήταν ένα από τα πρώτα peer-to-peer botnets — δηλαδή, ελέγχονταν από πολλούς διαφορετικούς διακομιστές. Το δίκτυο ήταν τεράστιο, κυμαίνοταν από 250.000 έως 1 εκατομμύριο μολυσμένους υπολογιστές και μπορούσε να ενοικιαστεί. Εξαιτίας αυτού, το Storm συμμετείχε σε ένα ευρύ φάσμα εγκληματικών δραστηριοτήτων, από επιθέσεις DDoS έως κλοπής δεδομένων. Μερικοί από τους διακομιστές του Storm έκλεισαν το 2008 και σήμερα το botnet θεωρείται λίγο πολύ ανενεργό [60].

Mirai: Το Mirai Botnet βρισκόταν πίσω από μια μαζική επίθεση άρνησης υπηρεσίας (DDoS) που άφησε μεγάλο μέρος του Διαδικτύου απρόσιτο στην ανατολική ακτή των ΗΠΑ. Ωστόσο, αυτό που έκανε το Mirai αξιοσημείωτο ήταν ότι ήταν το πρώτο μεγάλο botnet που μόλυνε τις μη ασφαλείς συσκευές IoT. Στο απόγειό του, μόλυνε περισσότερες από 600.000 συσκευές. Το botnet δημιουργήθηκε από μια ομάδα φοιτητών κολλεγίου που ήθελε να έχει πλεονέκτημα στο Minecraft [61].

1.2.5.8 RootKits

Το όνομα "rootkit" προέρχεται από τα λειτουργικά συστήματα Unix και Linux, όπου ο πιο προνομιακός διαχειριστής λογαριασμού ονομάζεται "root". Οι εφαρμογές που επιτρέπουν μη εξουσιοδοτημένη πρόσβαση root ή σε επίπεδο διαχειριστή στη συσκευή είναι γνωστές ως "kit". Αν και τα περισσότερα rootkits επηρεάζουν το λογισμικό και το λειτουργικό σύστημα, ορισμένα μπορούν επίσης να μολύνουν το hardware και το firmware του υπολογιστή. Τα Rootkit είναι ικανά να δρουν χωρίς να εντοπίζονται. Μόλις αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε υπολογιστές, τα rootkits επιτρέπουν στους κυβερνοεγκληματίες να κλέβουν προσωπικά δεδομένα, να εγκαταστήσουν άλλα κακόβουλα λογισμικά ή να χρησιμοποιούν υπολογιστές ως μέρος ενός botnet [10].

Το Necurs rootkit είναι ένα από τα μεγαλύτερα ενεργά botnets αυτή τη στιγμή και είναι υπεύθυνο για τη διάδοση του Locky ransomware καθώς και του κακόβουλου λογισμικού Dridex. Το rootkit Necurs προστατεύει άλλους τύπους κακόβουλου

λογισμικού που καθιστούν έναν υπολογιστή μέρος ενός botnet, διασφαλίζοντας έτσι ότι η μόλυνση δεν μπορεί να αφαιρεθεί [62].

1.2.6 Cryptojacking

Cryptojacking είναι η κυβερνοεπίθεση κατά την οποία συσκευές όπως υπολογιστές, tablet, smartphone ακόμα και διακομιστές χρησιμοποιούνται για την εξόρυξη κρυπτονομισμάτων χωρίς την γνώση ή τη συγκατάθεση των χρηστών. Έχουν σχεδιαστεί ώστε να μένουν κρυφά χωρίς να σημαίνει όμως ότι δεν έχουν κόστος. Η χρήση των πόρων μιας συσκευής οδηγεί στην επιβράδυνση της, την κατανάλωση μεγαλύτερης ποσότητας ενέργειας και την μείωση της διάρκειας ζωής της [11]. Το cryptojacking ανάλογα με τον τρόπο που λειτουργεί χωρίζεται σε δύο κατηγορίες όπως περιγράφονται παρακάτω.

1.2.6.1 Browser Cryptojacking

Η τεχνική είναι γνωστή και ως drive-by cryptomining και γίνεται κατά την επίσκεψη ιστοσελίδων μέσω του περιηγητή (browser). Οι cryptjackers ορισμένες φορές δημιουργούν ιστότοπους στους οποίους ενσωματώνουν κώδικα JavaScript υπεύθυνο για cryptomining ή ακόμα και σε ήδη υπάρχουσες ιστοσελίδες μέσω των διαφημίσεων. Αξίζει να σημειωθεί ότι πολλοί ιστότοποι ενημερώνουν τους επισκέπτες τους ότι χρησιμοποιούν αντίστοιχα cryptomining JavaScript με σκοπό την απόκτηση εσόδων για την λειτουργία τους. Σε αυτή την περίπτωση δεν αποθηκεύεται κάποιος κώδικας στη συσκευή και αυτός εκτελείται μόνο όσο ο επισκέπτης βρίσκεται στο συγκεκριμένο ιστότοπο [11].

1.2.6.2 Host cryptojacking

Host cryptojacking ή αλλιώς file based γίνεται μέσω ενός κακόβουλου λογισμικού (malware) το οποίο χρησιμοποιεί τους πόρους ενός συστήματος για την εξόρυξη κρυπτονομισμάτων. Ο τρόπος με τον οποίο τοποθετείται στις συσκευές των θυμάτων γίνεται όπως και με τα περισσότερα malware, δηλαδή μέσω phishing υπό την μορφή email, εγκατάσταση προγραμμάτων και εφαρμογών ακόμα και από αξιόπιστες πηγές όπως το Google Play Store, και κάποια παρουσιάζουν δυνατότητες σκουληκιών (worm) [11].

1.2.6.3 Μέτρα για την αποφυγή τέτοιου είδους επιθέσεων είναι:

Ορισμένα μέτρα που μπορούν να ληφθούν για την αποφυγή τέτοιου είδους επιθέσεων είναι [11]:

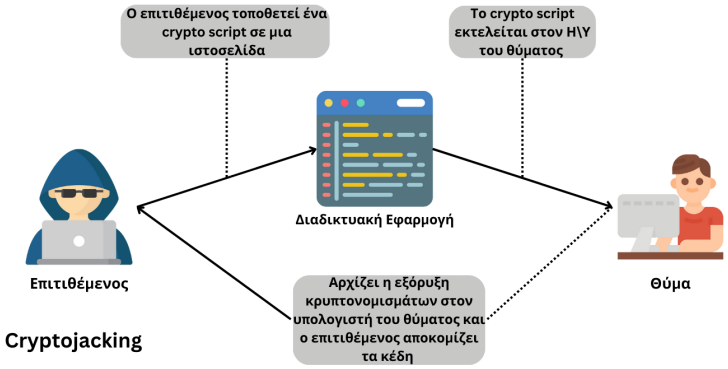

FIGURE 1.5: Cryptojacking

- Συνεχής παρακολούθηση των πόρων του συστήματος.
- Χρήση ad blocker και απενεργοποίηση της δυνατότητας εκτέλεσης JavaScript κώδικα.
- Φραγή σε ιστότοπους που είναι γνωστό ότι χρησιμοποιούν cryptomining scripts.

1.2.6.4 Γνωστές περιπτώσεις Cryptojacking:

- **Coinhive**: Το Coinhive ήταν μια υπηρεσία εξόρυξης κρυπτονομισμάτων που κυκλοφόρησε το 2017. Επέτρεπε στους ιδιοκτήτες ιστοτόπων να ενσωματώσουν έναν κώδικα JavaScript στους ιστότοπούς τους, ο οποίος θα χρησιμοποιούσε τον υπολογιστή του επισκέπτη του ιστότοπου για την εξόρυξη του κρυπτονομίσματος Monero. Το Coinhive σχεδιάστηκε για να είναι ένας νόμιμος τρόπος για να δημιουργούν έσοδα οι κάτοχοι ιστότοπων χωρίς να βασίζονται σε διαφημίσεις. Ωστόσο, δεν άργησε να αξιοποιηθεί από κακόβουλους χρήστες για χρήση χωρίς τη γνώση ή τη συγκατάθεσή των επισκεπτών [63].
- **WannaMine**: Το WannaMine ανακαλύφθηκε για πρώτη φορά το 2018 και είναι ένας τύπος κακόβουλου λογισμικού που χρησιμοποιείται σε επιθέσεις cryptojacking. Ο πιο κοινός τρόπος μετάδοσής γίνεται με phishing email. Όταν το θύμα ανοίγει το συνημμένο αρχείο, το κακόβουλο λογισμικό WannaMine εγκαθίσταται στον υπολογιστή του. Στη συνέχεια, χρησιμοποιεί

τον υπολογιστή του θύματος για την εξόρυξη του κρυπτονομίσματος Monero. Εκτός από την εξόρυξη κρυπτονομισμάτων, το WannaMine είναι σχεδιασμένο να εξαπλώνεται σε άλλους υπολογιστές που βρίσκονται στο ίδιο δίκτυο. Το WannaMine v4.0 είναι η πιο πρόσφατη έκδοση του κακόβουλου λογισμικού WannaMine. Εμφανίστηκε το 2020 και είναι γνωστό ότι χρησιμοποιεί πολλαπλές μεθόδους για την αποφυγή εντοπισμού. Είναι επίσης σε θέση να κλέβει ευαίσθητες πληροφορίες από τον υπολογιστή του θύματος [63].

1.3 Διάρθρωση εργασίας

Στο δεύτερο κεφάλαιο με τίτλο **Αναλύοντας το Ransomware**, θα παρουσιαστεί η εξέλιξη του ransomware, αναλύοντας τον κύκλο ζωής του και ταξινομώντας το. Στο τρίτο κεφάλαιο με τίτλο **Σχετικές Εργασίες**, θα εξεταστούν αντίστοιχες έρευνες σχετικά με την ανίχνευση ransomware. Έπειτα, στο τέταρτο κεφάλαιο με τίτλο **Προσέγγιση του Προβλήματος**, θα περιγραφεί η μέθοδος που ακολουθήθηκε για την ανίχνευση του ransomware. Εδώ θα παρουσιαστούν λεπτομέρειες της διαδικασίας, της μεθοδολογίας, και των εργαλείων που χρησιμοποιήθηκαν. Τέλος, στο πέμπτο κεφάλαιο **Συμπεράσματα και Επόμενα Βήματα**, θα παρουσιαστούν τα συμπεράσματα της έρευνας και θα αναφερθούν τα επόμενα βήματα που πρέπει να ακολουθηθούν.

Chapter 2

Αναλύοντας το Ransomware

2.1 Γιατί επιλέχθηκε το Ransomware

Η κυβερνοασφάλεια είναι ένας τομέας ο οποίος αλλάζει συνεχώς, ωστόσο λίγες απειλές έχουν συγκεντρώσει τόση προσοχή όσο το ransomware. Το ransomware είναι ένα κακόβουλο λογισμικό το οποίο μπορεί να προκαλέσει καταστροφές και αναστάτωση σε μεμονωμένα άτομα, επιχειρήσεις και οργανισμούς. Η λειτουργία του είναι απλή αλλά καταστροφική, εισβάλει σε ένα σύστημα και προσπαθεί να κρυπτογραφήσει τα δεδομένα του θύματος απαιτώντας λύτρα για την αποκρυπτογράφησή τους. Οι δράστες εκμεταλλευόμενοι τον φόβο των θυμάτων έχουν μετατρέψει το ransomware σε μια προσοδοφόρα εγκληματική επιχείρηση επινοώντας συνεχώς νέες μεθόδους εκβιασμού [64].

Οι επιθέσεις ransomware στοχεύοντας πλέον οργανισμούς όλων των μεγεθών, από πολυεθνικές μέχρι και κυβερνήσεις, έχουν γίνει πολλές και πρωτοσέλιδα. Πρόσφατο χαρακτηριστικό παράδειγμα είναι η επίθεση σε αγωγό της Colonial Pipeline στο Τέξας των ΗΠΑ [65]. Η επίθεση έδειξε την αδυναμία ακόμα και μεγάλων οργανισμών να αμυνθούν απέναντι στα ransomware αναγκάζοντας τον Πρόεδρο των ΗΠΑ να εκδώσει διάταγμα για την ενίσχυση της κυβερνοασφάλειας [65]. Από την άλλη πλευρά η Ευρωπαϊκή Ένωση μέσω του οργανισμού ENISA (Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών) έχει επανειλημμένα τοποθετήσει το ransomware ως μια από τις κυριότερες απειλές στον κυβερνοχώρο [66, 67, 68, 69, 64].

Συνεπώς η κατανόηση της φύσης των ransomware και των τακτικών αποτελεί σημαντικό πρωταρχικό μέλημα για την αντιμετώπιση του. Η αντιμετώπιση της απειλής του ransomware απαιτεί μια πολύπλευρη προσέγγιση που συνδυάζει προληπτικά μέτρα, προληπτικές πρακτικές ασφάλειας στον κυβερνοχώρο και μια σαφή στρατηγική αντίδρασης. Είναι απαραίτητο να δοθεί προτεραιότητα στην ευαισθητοποίηση και την εκπαίδευση για την ασφάλεια στον κυβερνοχώρο σε όλα τα

επίπεδα ενός οργανισμού ή για μεμονωμένους χρήστες μιας και ένα από τα ευρήματα του ENISA ήταν ότι 84% των κυβερνοεπιθέσεων βασίζεται σε μορφές κοινωνικές μηχανικής [70]. Η εφαρμογή ισχυρών συστημάτων δημιουργίας αντιγράφων ασφαλείας, η τακτική ενημέρωση λογισμικού και η χρήση ισχυρών μεθόδων κρυπτογράφησης και ελέγχου ταυτότητας είναι ζωτικής σημασίας βήματα για τη μείωση της ευπάθειας. Επιπλέον, είναι σημαντικό να εξεταστούν εναλλακτικές λύσεις αντί της πληρωμής λύτρων, καθώς η πληρωμή δεν εγγυάται την ανάκτηση δεδομένων και τροφοδοτεί την συνεχιζόμενη εγκληματική δράση στο κυβερνοχώρο [64].

Αυτή η εισαγωγή θέτει το έδαφος για μια βαθύτερη εξερεύνηση του ransomware, συμπεριλαμβανομένης της προέλευσης του, τον τρόπο δράσης, τις κατηγορίες του και τέλος ορισμένες προσεγγίσεις που έχουν γίνει για την αντιμετώπιση του. Σε αυτό ευελπιστούμε ότι θα συνεισφέρει και η δική μας εργασία κάνοντας χρήση HoneyToken με την μορφή Honeyfile.

2.2 Εξέλιξη Ransomware

Το AIDS trojan εμφανίστηκε το 1989 και ήταν το πρώτο κακόβουλο λογισμικό που κρυπτογράφησε δεδομένα και απαίτησε πληρωμή λύτρων για την αποκρυπτογράφησή τους. Το κακόβουλο λογισμικό διανεμήθηκε αρχικά με την μορφή δισκέτας και κρυπτογραφούσε μόνο τα ονόματα των αρχείων σε έναν υπολογιστήθύμα. Τέλος, το AIDS trojan χρησιμοποιούσε συμμετρική κρυπτογράφηση, δηλαδή οι πληροφορίες αποκρυπτογράφησης ήταν διαθέσιμες στη συσκευή του θύματος [12]. Κατά τη διάρκεια της δεκαετίας του 1990 υπήρξαν ανάλογες επιθέσεις όπου οι επιτιθέμενοι απέκτησαν πρόσβαση στα δεδομένα -ή τουλάχιστον έτσι υποστήριζαν- των υπολογιστών των θυμάτων και απαιτούσαν πληρωμή για την αποκρυπτογράφησή τους ή ακόμη και για την μη δημοσιοποίηση αυτών.

Το 1996, ερευνητές του Πανεπιστημίου Κολούμπια πρότειναν την χρήση του συνδυασμού συμμετρικής και ασύμμετρης κρυπτογραφίας σε αντίστοιχες επιθέσεις [13].Στη σημερινή εποχή πολλές παραλλαγές ransomware χρησιμοποιούν τον συνδιασμό συμμετρικής και ασύμμετρης κρυποτγράφησης δημιουργόντας ισχυρά και ασφαλή κλειδιά αποκρυπτογράφησης [14]. Από τη δεκαετία του 1990 έως τις αρχές της δεκαετίας του 2010, τα ransomware συχνά είτε προσποιούνταν ότι κρυπτογραφούσαν δεδομένα είτε η κρυπτογράφηση εφαρμόστηκε εσφαλμένα με αποτέλεσμα τα θύματα να μην απολέσουν τα δεδομένα τους [15]. Ωστόσο αξίζει να σημειωθεί ότι το 2005 οι ίδιοι καθηγητές του Πανεπιστημίου Κολούμπια υλοποίησαν την ιδέα που είχαν παρουσιάσει παλαιότερα και προειδοποίησαν ξανά για τους κινδύνους της ασύμμετρης κρυπτογράφησης παρουσιάζοντας ορισμένα αντίμετρα όπως τη δημιουργία αντιγράφων ασφαλείας των δεδομένων, ένα ισχυρό

τείχος προστασίας και προστασία από ιούς και λήψη μόνο από αξιόπιστες πηγές [16]. Έτσι, λίγο αργότερα το 2006, ήρθε η πρώτη επίθεση με ransomware που χρησιμοποίησε ασύμμετρη κρυπτογράφηση. Το GPcode μεταμφιέστηκε σε άκακο συνημμένο email αίτησης εργασίας που στόχευε Ρώσους χρήστες του Διαδικτύου [17]. Ο δημιουργός του GPcode συνέχισε να βελτιώνει το ransomware ενισχύοντας την κρυπτογράφηση, κυκλοφορώντας πολλαπλές εκδόσεις σε διάστημα λίγων ημερών Cracking-the-code. Η τρίτη έκδοση χρησιμοποιούσε κρυπτογράφηση που θα χρειαζόταν 30 χρόνια για να τη σπάσει ένας σύγχρονος υπολογιστής. Το trojan απαιτούσε από τα θύματα να πληρώσουν με ένα είδος προπληρωμένης κάρτας [17].

Η επόμενη σημαντική εξέλιξη συνέβη το 2013 με το ransomware CryptoLocker. Το CryptoLocker συνδύαζε κρυπτογράφηση δημόσιου κλειδιού που αποθηκεύονταν στον C&C server που ελέγχονταν από τον επιτιθέμενο και οι πληρωμές γίνονταν σε bitcoin [18]. Πριν το CryptoLocker οι πληρωμές ransomware γινόντουσαν με τη χρήση ηλεκτρονικών πορτοφολιών, προπληρωμένων χρεωστικών καρτών, μεταφορών χρημάτων, δωροκάρτες και άλλων μορφών πληρωμής γεγονός που δυσκόλευε τους επιτιθέμενους να ζητήσουν μεγάλα λύτρα [71]. Η εμφάνιση του Bitcoin το 2009 έδωσε τη δυνατότητα γρήγορων και ψευδοανώνυμων πληρωμών καθώς και τη δημιουργία του σύγχρονου "επιχειρηματικού μοντέλο" των ransomware [71]. Ο συνδυασμός ισχυρής κρυπτογράφησης του CryptoLocker και οι πληρωμές σε Bitcoin επέτρεψαν στους κυβερνοεγκληματίες να αποσπάσουν κέρδη περίπου 27 εκατομμυρίων δολαρίων. Ωστόσο το 2016 το FBI σταματήσει την παράνομη δράση της ομάδας πίσω από το CryptoLocker [72]. Το CryptoLocker χρησιμοποίησε τακτικές όπου προσπαθούσε να μολύνει όσο το δυνατόν περισσότερα θύματα και απαιτούσε μικρό αντίτιμο. Αυτή η τακτική ονομάζεται "spray and pray" και ήταν το κυρίαρχος τρόπος μόλυνσης των υπολογιστών με ransomware πριν από το 2015.

Στα μέσα της δεκαετίας του 2000, το ransomware χρησιμοποιούνταν συνήθως κατά ιδιωτών και λιγότερο κατά επιχειρήσεων. Ωστόσο, το 2015, οι κυβερνοεγκληματίες άρχισαν να στοχεύουν επιχειρήσεις. Ζητούσαν λύτρα με βάση την εκτίμηση της ζημίας που προκαλούσε το ransomware σε αυτές. Αυτή η μετατόπιση οδήγησε σε ευρεία στόχευση των επιχειρήσεων και μεγάλων βιομηχανιών.

Το 2014, οι ομάδες πίσω από ransomware άρχισαν να πωλούν ransomware σε διαδικτυακά φόρουμ ως Ransomware-as-a-service (RaaS). Το CTB-Locker αποτέλεσε το πρώτο RaaS που εντοπίστηκε, και λειτουργούσε με ένα μοντέλο RaaS όπου οι δημιουργοί του ransomware δάνειζαν το κακόβουλο λογισμικό και οι «πελάτες» που το δανείζονταν αναλάμβαναν την ανάπτυξη του στα συστήματα

των θυμάτων. Στη συνέχεια, οι δημιουργοί έπαιρναν ένα μέρος των λύτρων που ζητήθηκαν από το θύμα. Αυτό μείωσε τον κίνδυνο για τους «πελάτες» του ransomware και αύξησε τα κέρδη για δημιουργούς του [73]. Το μοντέλο αυτό είναι η κύρια μορφή RaaS, αλλά υπάρχουν και άλλες όπου το κακόβουλο λογισμικό δίνεται σε άλλες εταιρείες χωρίς να απαιτείται από αυτές να δώσουν μέρος των λύτρων που αποκόμισαν. Ένας ακόμα τύπος RaaS περιλαμβάνει συνδρομή για «πελάτες» που χρησιμοποιούν το ransomware [74]. Όλα τα μοντέλα RaaS μείωσαν την τεχνική ικανότητα που απαιτείται για τη διεξαγωγή επιθέσεων ransomware, οδηγώντας σε αυξημένες κυβερνοεπιθέσεις αυτού του τύπου [75].

Ως επέκταση του RaaS, οι ομάδες πίσω από τα ransomware άρχισαν να αναθέτουν σε άλλες ομάδες την ανάπτυξη ορισμένων πόρων που απαιτούνται για την υλοποίηση των επιθέσεων τους. Αυτοί οι πόροι είναι κρίσιμοι σε διάφορα στάδια του κύκλου του ransomware όπως η χρήση domains για την υποστήριξη C&C server, λογαριασμοί email για phishing attacks ως μέρος της αρχικής πρόσβασης ή κλοπή πιστοποιητικών σύνδεσης σε διάφορους λογαριασμούς. Το 2017, το Jaff ransomware άρχισε να νοικιάζει το Necurs spam botnet για την αποστολή malspam σε εκατομμύρια πιθανά θύματα [76]. Το 2018,το Ryuk ransomware άρχισε να συνεργάζεται με το Emotet botnet για αποστολή μολυσμένων εγγράφων Word στα θύματα από παραβιασμένους λογαριασμούς email. Οι χειριστές του Ryuk στη συνέχεια χρησιμοποιούσαν αυτή τη πρόσβαση για να μολύνουν τα θύματα με ransomware. Αυτού του είδος αμοιβαία επωφελούς εταιρική σχέση μεταξύ πολλαπλών ειδικευμένων κυβερνοεγκληματιών συνεχίζεται και είναι υπεύθυνη για πολλά από τα πιο επιζήμια ransomware.

Μια μορφή εξυπηρέτησης πελατών όπου πελάτες είναι τα θύματα αποτελεί ένα ακόμα χαρακτηριστικό του τρόπου δράσης των ransomware . Η ομάδα πίσω από το CryptoLocker ήταν μια από τις πρώτες που ανταποκρίθηκε στα αιτήματα των θυμάτων μέσω φόρουμ για παροχή βοήθειας. Άλλες ομάδες πίσω από ransomware έχουν διαπραγματευτεί με τα θύματα ή τους έχουν προσφέρει καθοδήγηση σχετικά απόκτηση bitcoin για την καταβολή των λύτρων [77]. Πολλές φορές οι επιτιθέμενοι δίνουν τη δυνατότητα στα θύματα να μην δημοσιοποιήσουν πως δέχτηκαν επίθεση και πλήρωσαν λύτρα, καταβάλλοντας ένα επιπλέον κόστος.

Το επιχειρηματικό μοντέλο των ransomware έχει οδηγήσει στο να δημιουργηθούν άλλες στρατηγικές δημιουργίας εσόδων κατά τη διάρκεια της επίθεσης. Αυτές οι στρατηγικές μπορούν να σπάσουν σε τρεις μεγάλες κατηγορίες:

- Μόλυνση επιπλέον θυμάτων
- διαστρωμάτωση κυβερνοεπιθέσεων
- κλοπή δεδομένων και/ή δημοσιοποίηση αυτών

Σε ορισμένες πρώιμες μορφές ransomware τα θύματα απαιτήθηκαν είτε να πληρώνουν λύτρα είτε να μολύνουν άλλα δύο τα θύματα να ξεκλειδώσουν τα δεδομένα τους [78]. Αυτή η στρατηγική μόλυνσης επιπλέον θυμάτων συνεχίζει να υπάρχει μέχρι σήμερα αν και η μορφή της έχει αλλάξει. Όταν οι κυβερνοεγκληματίες έχουν διεισδύσει στα δίκτυα και τα συστήματα των θυμάτων, ενδέχεται να χρησιμοποιήσουν κάποιο παραβιασμένο λογαριασμό email για την αποστολή email που περιέχει κακόβουλο λογισμικό στις επαφές τους.

Ένας ακόμα τρόπος δημιουργίας περισσοτέρων κερδών περιλαμβάνει την εξαπόλυση πολλαπλών τύπων κυβερνοεπιθέσεων. Μερικοί κυβερνοεγκληματίες πριν από την κρυπτογράφηση ενδέχεται να κάνουν Cryptojacking δηλαδή να αξιοποιήσουν την επεξεργαστική ισχύ των συστημάτων του θύματος για την εξόρυξη κρυπτονομισμάτων. Έτσι ακόμα και εάν τα θύματα πληρώσουν τα λύτρα για να ανακτήσουν την πρόσβαση στα αρχεία τους, υπάρχει το ενδεχόμενο να συνεχιστεί η διαδικασία εξόρυξης κρυπτονομισμάτων δημιουργώντας επιπλέον έσοδα στους επιτιθέμενους. Άλλες ομάδες επιτιθέμενων αφού έχουν εξαπολύσει την πρώτη επίθεση υλοποιούν επιθέσεις τύπου DDoS ζητώντας επιπλέον λύτρα από τα θύματα προκειμένου να σταματήσει. Το 2020, παρατηρήθηκε ένα τρίτο επίπεδο στην διαστρωμάτωση των επιθέσεων καθώς ορισμένοι κυβερνοεγκληματίες φέρεται να τοποθέτησαν είτε το ίδιο ransomware ή άλλες παραλλαγές ransomware αναγκάζοντας τα θύματα να καταβάλουν ακόμα μεγαλύτερα λύτρα [79].

Τέλος, μια ακόμα στρατηγική δημιουργίας επιπλέον εσόδων αποτελεί η κλοπή δεδομένων και/ή δημοσιοποίηση αυτών. Αυτό γίνεται με την πώληση των πιστοποιητικών εισόδου σε τρίτους. Αν τα θύματα δεν αλλάξουν τους κωδικούς τους τότε οι λογαριασμοί τους ενδέχεται να παραβιαστούν. Σε άλλες περιπτώσεις δεδομένα που έχουν κλαπεί μπορεί να πωληθούν είτε να δημοσιοποιηθούν προκαλώντας ζημιά στην εικόνα των επιχειρήσεων. Καθώς οι μολύνσεις με ransomware έγιναν όλο και πιο συχνές, οι ομάδες πίσω από αυτά άρχισαν να εκβιάζουν τα θύματα προκειμένου να μην γνωστοποιήσουν ότι υπήρξαν θύματα κυβερνοεπίθεσης. Αυτό έχει οδηγήσει πολλές επιχειρήσεις και οργανισμούς να πληρώσουν μεγάλα ποσά προκειμένου να διατηρήσουν το κύρος τους. Σε αυτές τις περιπτώσεις, οι κυβερνοεγκληματίες απαιτούσαν και επιπλέον πληρωμή για την μη δημοσιοποίηση των δεδομένων που κλάπηκαν. Αυτό έγινε σύνηθες τεχνική στα ransomware το 2019, όταν το καρτέλ Maze ανακοίνωσε έναν ιστότοπο όπου κυβερνοεγκληματίες μπορούσαν να ανεβάσουν τα δεδομένα που έκλεψαν [80]. Πολλές ομάδες πίσω από τα ransomware υιοθέτησαν την ίδια μέθοδο και διοχετεύουν τα δεδομένα στο dark web.

Το μοντέλο RaaS είναι το κυρίαρχο business model των σημαντικότερων σύγχρονων ransomware, αλλά δεν είναι το μόνο. Ορισμένες από αυτές είναι η

εφάπαξ αγορά ransomware και των πόρων που χρειάζεται για την ανάπτυξή του ενώ άλλες ομάδες συνεχίζουν να εφαρμόζουν τακτικές "spray and pray".

2.3 Τρόπος δράσης Ransomware

Ο τρόπος δράσης τους ransomware ακολουθεί ορισμένα βήματα τα οποία ορίζονται ως έξης:

1. Αρχική είσοδος στον υπολογιστή
2. Μόλυνση του υπολογιστή
3. Ειδοποίηση του θύματος για την δράση του ransomware
4. Δίλημμα πληρωμής
5. Επιπλέον κακόβουλες ενέργειες

2.3.1 Αρχική είσοδος στον υπολογιστή

Το πρώτο στάδιο της επίθεσης από ransomware είναι η διείσδυση στο σύστημα του θύματος. Ο ανθρώπινος παράγοντας είναι ο σημαντικότερος λόγος που τα περισσότερα ransomware καταφέρνουν να διεισδύσουν σε ένα σύστημα. Αυτό μπορεί να οφείλεται σε:

- Έλλειψη εκπαίδευσης και κριτικής σκέψης
- Μη χρήση αντικών προγραμμάτων
- Μη ενημερωμένο λογισμικό π.χ. Λειτουργικού συστήματος, Java, περιηγητή δικτύου

Ένας από τους πιο κλασικούς τρόπους που επιτιθέμενοι προσπαθούν να εισβάλουν σε έναν υπολογιστή είναι μέσω φαινομενικά ακίνδυνων μηνυμάτων ηλεκτρονικού ταχυδρομείου (phishing) όπου υπάρχει κάποιο συνημμένο αρχείο ή κάποια ηλεκτρονική διεύθυνση όπου γίνεται λήψη του κακόβουλου λογισμικού. Ιδιαίτερο ενδιαφέρον αποτελεί ότι περίπου το 45% των επιθέσεων ransomware σε μεγάλους οργανισμούς γίνεται με αυτό τον τρόπο [81]. Παρά το γεγονός ότι αυτή η τεχνική είναι αρκετά αποτελεσματική, όπως μας το επιβεβαιώνουν και τα στατιστικά, τα πιο σύγχρονα ransomware είναι πολύ πιο αυτοματοποιημένα καθώς μπορούν να "αναπαράγονται" μέσο του διαδικτύου και να εκμεταλλεύονται κενά ασφαλείας λειτουργικών όπως τα Windows. Τέλος μία ακόμα μέθοδος είναι η "drive-by download" όπου οι χρήστες κατεβάζουν ένα ransomware ενα αγνοία και χωρίς την

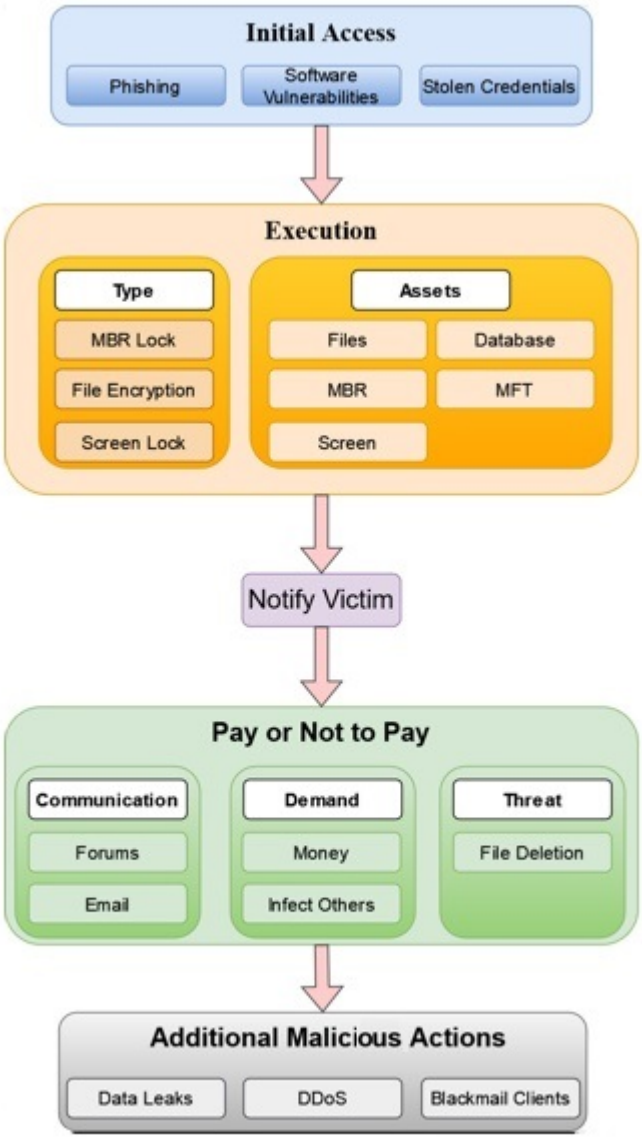

FIGURE 2.1: Κύκλος δράσης Ransomware

εξουσιοδότηση τους. Τέτοιες μορφές αποτελούν το Cross Site Scripting (XSS), Adware που περιγράφησαν στην προηγούμενη ενότητα.

2.3.2 Μόλυνση του Υπολογιστή

Από την στιγμή που θα καταφέρει να περάσει τις άμυνες του συστήματος, το ransomware ξεκινά τη κακόβουλη δράση του. Το διάστημα αυτό μπορεί να ποικίλει καθώς το ransomware ως ένας τύπος malware μπορεί να προκαλεί και άλλες βλάβες, π.χ., να είναι μέρος ενός botnet που λαμβάνει ενημερώσεις ή κάνει κάποιο DDoS. Παρόλα αυτά κάποια στιγμή θα επικοινωνήσει με τον Server των επιτιθέμενων για την δημιουργία των κρυπτογραφικών κλειδιών όπου ένα από τα οποία

αποθηκεύεται στον server του κυβερνοεγκληματία και ένα στέλνεται στον υπολογιστή του θύματος για την κρυπτογράφηση των αρχείων. Ανάλογα με το τρόπο δράσης του ransomware μπορεί να χαρακτηριστεί ως [19]:

- MBR ransomware: Το Master Boot Record (MBR) επιτρέπει στον υπολογιστή να εκκινεί. Η κρυπτογράφηση αυτών των αρχείων αλλάζει τον τρόπο εκκίνησης και προβάλλει το αίτημα για τα λύτρα
- Lock screen ransomware: Αυτό του είδους ransomware "κλειδώνει" την οθόνη του θύματος χωρίς να κρυπτογραφεί τα αρχεία αλλά περιορίζει την χρήση του υπολογιστή.
- File encryption ransomware: Τα αρχεία του υπολογιστή κρυπτογραφούνται και απαιτείται η χρήση του κλειδιού για την αποκρυπτογράφηση τους.

2.3.3 Ειδοποίηση του θύματος

Σε αυτό το στάδιο το θύμα ειδοποιείται για την ύπαρξη ransomware στον υπολογιστή του και ζητούνται λύτρα για να μπορέσει να αποκτήσει έλεγχο στο σύστημα. Συχνά το μήνυμα είναι γραμμένο στη γλώσσα του θύματος.

2.3.4 Δίλημμα πληρωμής

Στο τέταρτο στάδιο το θύμα πρέπει να αποφασίσει αν θα πληρώσει ή όχι για να αποκτήσει πίσω τα αρχεία του. Εδώ θα πρέπει να τονίσουμε πως πέρα από την αξία των αρχείων που χάνει κάποιος, θα πρέπει να υπολογίσει πως οι συναλλαγές με εγκληματίες δεν είναι αξιόπιστες και υπάρχει ο κίνδυνος να μην κρατήσουν τον λόγο τους, συνεπώς να μη του δώσουν το κλειδί για την αποκρυπτογράφηση των αρχείων του. Οι πληρωμές πλέον γίνονται κατά κύριο λόγο με κρυπτονομίσματα καθώς αυτά παρέχουν ανωνυμία, ασφάλεια και ταχύτητα. Παρόλα αυτά η διαδικασία μετατροπής των κρυπτονομισμάτων σε κανονικά χρήματα ενέχει κινδύνους για την αποκάλυψη της ταυτότητας των κυβερνοεγκληματιών και για αυτό συχνά κατά την διαδικασία της μετατροπής ανακατεύουν πληρωμές από διαφορετικά θύματα [20].

2.3.5 Επιπλέον κακόβουλες ενέργειες

Σε μια τυπική επίθεση ransomware, ο εισβολέας κρυπτογραφεί τα δεδομένα του οργανισμού και στη συνέχεια, απαιτεί πληρωμή με αντάλλαγμα την αποκατασταθείσα πρόσβαση. Αυτός ο τύπος κρυπτογράφησης αντιπροσωπεύει τον "μονό εκβιασμό" ή "single extortion".

FIGURE 2.2: Η ειδοποίηση που λάμβαναν τα θύματα που είχαν μολυνθεί απο το Reveton Ransomware.

Ωστόσο, στην περίπτωση του διπλού εκβιασμού (double extortion), ο δράστης απειλεί ότι θα δημοσιεύσει ευαίσθητα δεδομένα των θυμάτων εάν δεν πληρώσουν. Ως εκ τούτου, ο διπλός εκβιασμός περιλαμβάνει κλοπή δεδομένων(exfiltration), η οποία είναι η πρακτική της αντιγραφής και μεταφορά ευαίσθητων πληροφοριών. Η απειλή της δημόσιας έκθεσης τους ασκεί πρόσθετη πίεση στο θύμα προκειμένου να υποκύψει στην πληρωμή των λύτρων. Το ransomware Maze πρωτοστάτησε σε αυτήν την προσέγγιση το 2019. Αυτή η πρακτική υιοθετήθηκε και από άλλα ransomware καθώς σύμφωνα με την έκθεση του Coveware για το Q4 του 2020, το 70 τοις εκατό όλων των επιθέσεων ransomware κατά τη διάρκεια εκείνου του τριμήνου περιλάμβανε την πρακτική double extortion, που αντιπροσωπεύει 43% αύξηση από το τρίτο τρίμηνο του 2020 [82].

Υπάρχουν επιπλέον επίπεδα εκβιασμού πέρα από τον διπλό εκβιασμό. Ο "τριπλός εκβιασμός" (triple extortion) συμβαίνει όταν οι χάκερ ξεκινούν μια επίθεση άρνηση υπηρεσίας DDoS που προκαλεί άρνηση πρόσβασης στους ιστότοπους του θύματος, απειλούν να αποκαλύψουν εμπιστευτικές πληροφορίες και κρυπτογραφούν τις πληροφορίες που κατέχει το θύμα. Οι επιθέσεις DDoS κατακλύζουν τους διακομιστές του θύματος με νέα αιτήματα, με αποτέλεσμα να δημιουργείται κυκλοφοριακή συμφόρηση που καθιστά τον ιστότοπο απρόσιτο σε άλλους. Η τακτική

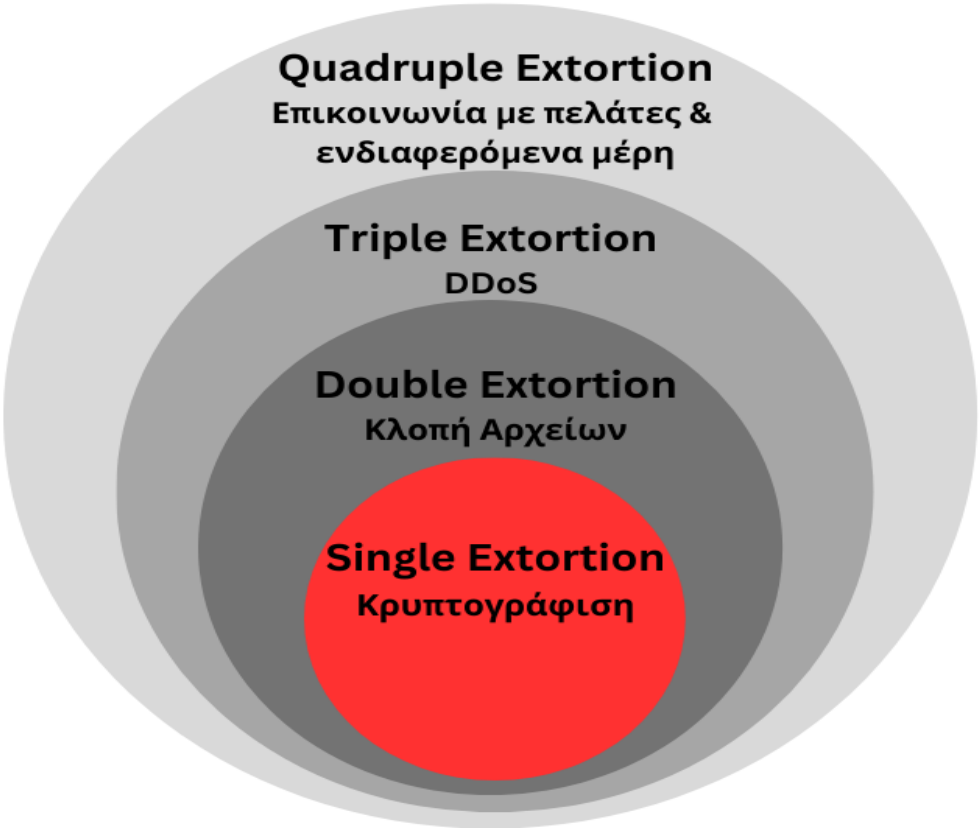

FIGURE 2.3: Τα στάδια εκβιασμού των Ransomware

του τριπλού εκβιασμού ασκεί πρόσθετη πίεση στην εταιρεία-θύμα προκειμένου να πληρώσουν τα λύτρα, αφού οι πελάτες/χρήστες δεν μπορούν να έχουν πρόσβαση στον ιστότοπο της εταιρείας για όσο διάστημα κρατάει η επίθεση.

Ο "τετραπλός εκβιασμός" (quadruple extortion) συμβαίνει όταν οι χάκερ διεξάγουν τριπλό εκβιασμό αλλά παράλληλα εκβιάζουν άμεσα τους πελάτες ή τις συνεργαζόμενες εταιρείες με βάση τα δεδομένα που κατάφεραν να αποκτήσουν από την εταιρεία που υπέστη παραβίαση. Είναι ένα πρόσφατο φαινόμενο που παρατηρήθηκε για πρώτη φορά τον Οκτώβριος του 2020, όταν οι χάκερ απέκτησαν πρόσβαση στα αρχεία ψυχοθεραπείας της Φινλανδίας. Ασθενείς της εταιρείας ψυχοθεραπείας Vastaamo ανέφεραν ότι έλαβαν μηνύματα ηλεκτρονικού ταχυδρομείου που απαιτούσαν 200 ευρώ σε bitcoin για να αποτρέψουν τη δημοσιοποίηση ευαίσθητων συνομιλιών με τους ψυχοθεραπευτές τους [83]. Η γρήγορη άνοδος της διπλής, τριπλής και τετραπλής εκβίασης οδηγεί σε νέα τεχνικές για την άσκηση πρόσθετης πίεσης στις εταιρείες-θύματα. Με αυτό τον τρόπο το ransomware δεν επηρεάζει μόνο την ίδια την εταιρεία, αλλά μπορεί να έχει μεγάλο αντίκτυπο στην ιδιωτικότητα και την ασφάλεια των πελατών επίσης. Αυτό εν μέρει εξηγεί γιατί τα καταβληθέντα ποσά λύτρων έχουν αυξηθεί δραστικά.

2.4 Ταξινόμιση Ransomware

Το Ransomware μπορεί να ταξινομηθεί με διάφορους τρόπους. Σε αυτή την ενότητα ταξινομούμε το ransomware με βάση το στόχο τους, τη μέθοδο μόλυνσης, τον τρόπο επικοινωνίας με τον Command and Control (C&C) server, τον τρόπο δράσης, δυνατότητα διαγραφής αρχείων και μεθόδου εκβιασμού.

2.4.1 Ταξινόμηση ανά στόχο

Τα ransomware μπορούν να ταξινομηθούν σε δύο κατηγορίες: i) το είδος του θύματος και ii) την πλατφόρμα/λειτουργικό.

2.4.1.1 Θύματα Ransomware

Αναλύοντας τους τύπους θυμάτων του ransomware μπορούν να εξαχθούν πολύτιμες πληροφορίες για το σχεδιασμό αμυντικών μηχανισμών προσαρμοσμένο στις ανάγκες της κάθε ομάδας.Τα θύματα του ransomware χωρίζονται σε δύο ομάδες: τους τελικούς χρήστες και οργανισμούς.

Τελικοί χρήστες

Οι τελικοί χρήστες ήταν οι αρχικοί στόχοι για τα πρώτα ransomware. Η έλλειψη ενημέρωσης για τις απειλές του διαδικτύου αλλά και τεχνικών γνώσεων καθιστούν το ransomware ιδιαίτερα αποτελεσματικό έναντι των τελικών χρηστών [84]. Ένα crypto-ransomware μπορεί να κρυπτογραφήσει σημαντικά αρχεία που είναι αποθηκευμένα στις προσωπικές συσκευές (π.χ., υπολογιστές, φορητοί υπολογιστές, smartphone, κ.λ.π.), ενώ ένα locker-ransomware ενδέχεται να κλειδώσει τις συσκευές και να αποτρέψτε την πρόσβαση σε αυτές εκτός εάν καταβληθούν τα λύτρα. Το ποσό που ζητείται από τους τελικούς χρήστες είναι αρκετά μικρότερο από ότι στους οργανισμούς και για αυτό, τέτοιου είδους ransomware μολύνουν αρκετούς χρήστες για να είναι αποδοτικά [21].

Μεγάλοι Οργανισμοί

Οι οργανισμοί δεν ήταν αρχικά οι κύριοι στόχοι του ransomware. Ωστόσο, καθώς το ransomware εξελίσσονταν διαφορετικοί τύποι οργανισμών, συμπεριλαμβανομένων κυβερνήσεων, επιχειρήσεων, δομών υγείας, κ.λ.π [85] στοχοποιήθηκαν. Σε αυτές τις επιθέσεις, οι εγκληματίες του κυβερνοχώρου επιλέγουν τους στόχους τους και προσπαθήσουν να προκαλέσουν όσο το δυνατόν μεγαλύτερη ζημιά με την ελπίδα αποκόμισης περισσότερων λύτρων [86]. Σε μία τέτοια περίπτωση ένας οργανισμός μπορεί να χάσει σημαντικά δεδομένα, να σταματήσει την λειτουργία του και/ή να εκβιαστεί ότι θα δημοσιοποιήθουν τα δεδομένα που κλάπηκαν.

2.4.1.2 Πλατφόρμες στόχου Ransomware

Ένα άλλο σημαντικό σημείο για την κατανόηση της συμπεριφοράς του ransomware είναι η πλατφόρμα στόχος. Τις περισσότερες φορές, ένα ransomware είναι ειδικά σχεδιασμένο για μια πλατφόρμα και ένα λειτουργικό σύστημα επειδή συχνά αξιοποιεί τις βιβλιοθήκες/λειτουργίες του συγκεκριμένου λειτουργικού συστήματος (όπως κλήσεις συστήματος) για να εκτελέσει τις κακόβουλες ενέργειές του [84]. Έτσι έχουμε τις τρεις μεγαλύτερες κατηγορίες PC, έξυπνα κινητά τηλέφωνα (mobile devices) και Internet of Things (IoT)/ Cyber-physical systems CPS.

PC

Οι πιο συνηθισμένοι στόχοι ransomware είναι οι υπολογιστές. Λόγω της δημοτικότητας μεταξύ των χρηστών [87], η πλειονότητα των ransomware στοχεύει υπολογιστές με Windows OS. Επιπλέον, υπάρχουν ορισμένες οικογένειες ransomware που στοχεύουν άλλα λειτουργικά συστήματα, όπως το KeRanger για macOS και το LinuxEncoder για πλατφόρμες GNU/Linux. Τα θύματα μπορούν να αντιμετωπίσουν επιθέσεις ransomware τύπου locker με την επανεγκατάσταση του λειτουργικού τους συστήματος. Από την άλλη, ένα κρυπτογραφικό ransomware είναι δύσκολο να αντιμετωπιστεί και να ανακτηθούν τα αρχεία λόγω χρήσης προηγμένων τεχνικών κρυπτογραφίας [22].

Κινητές συσκευές

Η αυξανόμενη δημοτικότητα των κινητών συσκευών στην σύγχρονη εποχή κάνει τις κινητές συσκευές όπως τα smartphone ιδανικούς στόχους για ransomware. Όσον αφορά τις κινητές συσκευές τόσο οι πλατφόρμες Android όσο και iOS αποτελούν στόχο των ransomware, καθώς αυτές οι πλατφόρμες ελέγχουν το μεγαλύτερο μερίδιο της παγκόσμιας αγοράς κινητών συσκευών. Η Apple διαθέτει ένα αυστηρά ελεγχόμενο οικοσύστημα όπου οι εφαρμογές ελέγχονται διεξοδικά πριν εγκριθούν προς διάθεση στους πελάτες. Πιθανώς για αυτόν τον λόγο, οι χρήστες iOS δεν έχουν επηρεαστεί τόσο από επιθέσεις ransomware [88]. Από την άλλη το Android αποτελεί ένα ανοιχτό οικοσύστημα και ως εκ τούτου το ransomware αποτελεί σοβαρή απειλή για τους χρήστες Android. Έτσι, το πρώτο Locker ransomware για Android κινητές συσκευές, το Android Defender, εμφανίστηκε το 2013 και τον επόμενο χρόνο εμφανίστηκε το πρώτο κρυπτογραφικό ransomware, το Simplocker [89]. Παρόλο που για Η/Υ τα crypto-ransomware είναι περισσότερο απειλητικά από το locker-ransomware, στις κινητές συσκευές συμβαίνει το ακριβώς αντίθετο.

Συσκευές IoT/CPS

Οι συσκευές IoT και CPS δεν είναι οι κύριοι στόχοι των ransomware αυτή στιγμή. Ωστόσο, τέτοιες συσκευές αποκτούν όλο και περισσότερες εφαρμογές σε τομείς όπως έξυπνες συσκευές για σπίτια, υγεία, μεταφορές, έξυπνες πόλεις, έξυπνα εργοστάσια, κ.λ.π. [90]. Στην πραγματικότητα, βιομηχανικές συσκευές IoT και CPS (π.χ., PLC, RTU, RIO, κ.λ.π.) χρησιμοποιούνται ήδη σε δίκτυα νερού και σωλήνες αερίου, πυρηνικά και χημικά εργοστάσια. Αν και δεν υπάρχον διαδεδομένα ransomware [91] για τέτοια συσκευές αυτή τη στιγμή, δεν αποκλείεται να αποτελέσουν στόχους στο μέλλον.

2.4.2 Ταξινόμηση με βάση τον τρόπο μόλυνσης

Οι μέθοδοι μόλυνσης του ransomware μπορούν να κατηγοριοποιηθούν σε πέντε κύριες ομάδες: κακόβουλα e-mail, SMS ή άμεσα μηνύματα (IMs), κακόβουλες εφαρμογές, drive-by-download, και ευπάθειες.

2.4.2.1 Κακόβουλα e-mail

Τα κακόβουλα e-mail είναι ο πιο συχνά χρησιμοποιούμενος τρόπος μόλυνσης με κακόβουλο λογισμικό ransomware. Οι επιτιθέμενοι στέλνουν spam e-mail όπου τα συνημμένα αρχεία περιέχουν ransomware [92]. Τέτοια ανεπιθύμητα μηνύματα μπορούν να διανεμηθούν χρησιμοποιώντας botnets [86].

2.4.2.2 SMS/IM

Τα μηνύματα SMS ή τα μηνύματα IM χρησιμοποιούνται συχνά για την μόλυνση κινητών με ransomware. Σε αυτό του είδους επιθέσεις, οι επιτιθέμενοι στέλνουν μηνύματα SMS ή IM στα θύματα και τους καθοδηγούν να περιηγηθούν σε ένα κακόβουλο ιστότοπο για λήψη ransomware στις συσκευές τους [89, 92].

2.4.2.3 Κακόβουλες Εφαρμογές

Οι δημιουργοί ransomware αναπτύσσουν φαινομενικά καλοήθης εφαρμογές για κινητά. Ωστόσο όταν δεν υπάρχει ο κατάλληλος έλεγχος μπορει να τοποθετήσουν ransomware που να μολύνει την συσκευή [89, 92].

2.4.2.4 Drive-by-download

Η drive-by-download πραγματοποιείται όταν ένας χρήστης επισκέπτεται εν αγνοία του έναν μολυσμένο ιστότοπο ή κάνει κλικ σε μια κακόβουλη διαφήμιση και στη

συνέχεια γίνει λήψη και εγκατάσταση του κακόβουλου λογισμικού εν αγνοία του [93].

2.4.2.5 Vulnerabilities

Τρωτά σημεία στην πλατφόρμα του θύματος, όπως ευπάθειες στα λειτουργικά συστήματα [23], προγράμματα περιήγησης [94], ή στο λογισμικό που μπορεί να χρησιμοποιηθεί από τους δημιουργούς ransomware ως φορέας μόλυνσης. Οι επιτιθέμενοι μπορεί να χρησιμοποιήσουν βοηθητικές εφαρμογές, exploit kits, για να εκμεταλλευτούν γνωστές ευπάθειες ή τις ευπάθειες μηδενικής ημέρας.

2.4.3 Ταξινόμηση με βάση την επικοινωνία του C&C

Οι C&C servers χρησιμοποιούνται συχνά από τους δημιουργούς ransomware για την επικοινωνία και τη τροποποίηση του κακόβουλου λογισμικού. Πιο συγκεκριμένα οι διακομιστές C&C χρησιμοποιούνται κυρίως από οικογένειες κρυπτογραφικών ransomware για την αποστολή ή λήψη του κλειδιού κρυπτογράφησης που χρησιμοποιείται για την κρυπτογράφηση των αρχείων ή/και των εφαρμογών του θύματος. Τα ransomware χρησιμοποιούν κυρίως πρωτόκολλα HTTP ή HTTPS για αυτόν τον σκοπό [95]. Μπορούν να συνδεθούν στον διακομιστή C&C είτε μέσω hard-coded IP addresses ή domains, ή dynamically με fast-fluxed/generated/shifted domain names χρησιμοποιώντας Domain Generation Algorithms (DGA).

2.4.3.1 Hard-coded IPs/Domains

Ορισμένα ransomware μπορούν να ενσωματώσουν διευθύνσεις IP ή domains στα δυαδικά αρχεία τους για την δημιουργία σύνδεσης με τον διακομιστή C&C. Σε αυτήν την προσέγγιση, η διεύθυνση IP ή το domain παραμένει το ίδιο για κάθε επίθεση και παρέχει μια αξιόπιστη επικοινωνία για τους επιτιθέμενους. Ωστόσο, οι πληροφορίες που έχουν τοποθετηθεί στα δυαδικά αρχεία, μπορούν να χρησιμοποιηθούν από αναλυτές κυβερνοεπιθέσεων για τη δημιουργία προτύπων συμπεριφοράς ransomware που βοηθούν στην ανίχνευση του ransomware σε μελλοντική επίθεση.

2.4.3.2 Dynamic Domains

Οι DGA χρησιμοποιούνται από ransomware προκειμένου να επικοινωνούν δυναμικά με τους διακομιστές C&C. Αυτοί οι αλγόριθμοι παρέχουν ένα μοναδικό domain name στο διακομιστή για κάθε επικοινωνία μέσω fast-fluxing/generating/shifting των domain names. Αυτή η μορφή της επικοινωνίας

είναι πιο ασφαλής και τα τείχη προστασίας δεν μπορούν το εντοπίσουν εύκολα [24].

2.4.4 Ταξινόμηση κατά κακόβουλη ενέργεια

Οι κακόβουλες ενέργειες που μπορούν που υλοποιούνται από τα ransomware μπορούν να χωριστούν σε δύο ομάδες: κρυπτογράφηση και κλείδωμα.

2.4.4.1 Κρυπτογράφηση

Κρυπτογράφηση είναι η κακόβουλη ενέργεια που πραγματοποιείται από κρυπτογραφικά ransomware έχοντας στόχο να καταστήσουν τα αρχεία ενός θύματος μη προσβάσιμα, εκτός εάν καταβληθούν λύτρα. Το ransomware προετοιμάζει πρώτα τα κλειδιά και τότε ξεκινά η διαδικασία κρυπτογράφησης. Τα πρώτα ransomware κρυπτογραφούσαν αποκλειστικά τα αρχεία που βρίσκονται σε συγκεκριμένο τμήμα του σκληρού δίσκου [12]. Με την πάροδο του χρόνου, οι δημιουργοί ransomware ξεκίνησαν να στοχεύουν συγκεκριμένους τύπους αρχείων (δηλαδή, .doc, .zip, .pdf) που ενδέχεται να περιέχουν πολύτιμες πληροφορίες για τα θύματα. Μετά τη διαδικασία κρυπτογράφησης, το ransomware μπορεί να προκαλέσει επιπλέον βλάβες στα αρχεία θυμάτων, όπως διαγραφή ή αντικατάσταση. Σε αυτή την υποενότητα, αρχικά εξηγούμε τις κρυπτογραφικές τεχνικές που χρησιμοποιούνται από το ransomware.

2.4.4.2 Τεχνικές κρυπτογράφησης

Το Ransomware μπορεί να χρησιμοποιήσει τεχνικές συμμετρικής, ασύμμετρης ή υβριδικής κρυπτογράφησης. Για να εκτελέσει τη λειτουργία κρυπτογράφησης, το ransomware μπορεί να χρησιμοποιήσει API του συστήματος ή αλγόριθμους κρυπτογράφησης που βρίσκονται στον κώδικα του ransomware [25].

Κρυπτογράφηση συμμετρικού κλειδιού

Μόνο ένα κλειδί χρησιμοποιείται για την κρυπτογράφηση και αποκρυπτογράφηση αρχείων στη συμμετρική κρυπτογράφηση. Σε σύγκριση με την κρυπτογράφηση ασύμμετρου κλειδιού, απαιτεί μικρότερος αριθμός πόρων για την κρυπτογράφηση μεγάλου αριθμού αρχείων, ώστε το ransomware να μπορεί να κρυπτογραφήσει τα αρχεία των θυμάτων γρηγορότερα [96]. Ωστόσο, ο εισβολέας πρέπει να διασφαλίσει ότι το κλειδί δεν είναι προσβάσιμο στο θύμα μετά την κρυπτογραφική διαδικασία [84]. Το κλειδί κρυπτογράφησης είτε δημιουργείται στο σύστημα προορισμού είτε ενσωματώνεται στο πηγαίο κώδικα του ransomware. Μετά την κρυπτογράφηση, το ransomware στέλνει το κλειδί κρυπτογράφησης στον επιτιθέμενο μέσω επικοινωνίας του C&C. Αν και τα ransomware χρησιμοποιούν διαφορετικούς αλγόριθμους

κρυπτογράφησης συμμετρικού κλειδιού, ο Advanced Encryption Standard AES είναι ο πιο δημοφιλής αλγόριθμος.

Κρυπτογράφηση ασύμμετρου κλειδιού

Σε αυτή τη μέθοδο, το ransomware χρησιμοποιεί ένα ζεύγος κλειδιών, δηλαδή δημόσια και ιδιωτικά κλειδιά, για κρυπτογράφηση και αποκρυπτογράφηση αρχείων. Αν και δεν είναι αποτελεσματικός τρόπος για την κρυπτογράφηση μεγάλου αριθμού αρχείων, η κρυπτογράφηση ασύμμετρου κλειδιού επιλύει το πρόβλημα προστασίας του κλειδιού, καθώς απαιτούνται ξεχωριστά κλειδιά για κρυπτογράφηση και αποκρυπτογράφηση. Οι εισβολείς μπορούν να ενσωματώσουν το δημόσιο κλειδί στο πηγαίο κώδικα όπως στο TeslaCrypt [26] που επιτρέπει στο ransomware να ξεκινήσει την κρυπτογράφηση χωρίς σύνδεση στο C&C. Μπορούν επίσης να δημιουργήσουν τα κλειδιά στα συστήματα θυμάτων όπως στο CryptoLocker [97]. Σε ορισμένες οικογένειες ransomware, όπως π.χ, WannaCry [23], το δημόσιο κλειδί του εισβολέα παραδίδεται μέσω επικοινωνίας του C&C, καθιστώντας την σύνδεση απαραίτητη προκειμένου να αρχίσει η κρυπτογράφηση. Επιπλέον, ορισμένα ransomware μπορούν να δημιουργήσουν μοναδικά ζεύγη κλειδιών δημόσιο-ιδιωτικό για κάθε θύμα. Αυτό επιτρέπει στον εισβολέα να αποκρυπτογραφήσει τα αρχεία του θύματος χωρίς να αποκαλυφθεί το ιδιωτικό κλειδί που θα μπορούσε επίσης να χρησιμοποιηθεί για την αποκρυπτογράφηση αρχείων σε άλλα θύματα [84]. Ο Rivest–Shamir–Adleman (RSA) είναι ο πιο συχνά χρησιμοποιούμενος αλγόριθμος ασύμμετρου κλειδιού.

Υβριδική κρυπτογράφηση

Τα πλεονεκτήματα και των δύο τεχνικών κρυπτογράφησης συνδυάζονται από τους εισβολείς με την μορφή της υβριδικής κρυπτογράφησης. Σε αυτή την περίπτωση, το ransomware χρησιμοποιεί πρώτα την κρυπτογράφηση συμμετρικού κλειδιού για να κρυπτογραφήσει γρήγορα τα αρχεία του θύματος. Μετά, κρυπτογραφεί το χρησιμοποιούμενο συμμετρικό κλειδί με το δημόσιο κλειδί του εισβολέα. Γενικά, το δημόσιο κλειδί του εισβολέα είναι ενσωματωμένο στο λογισμικό του ransomware, έτσι ώστε να μην απαιτείται η σύνδεση με τον διακομιστή C&C κατά τη διάρκεια της επίθεσης.

2.4.4.3 Καταστροφή αρχείων

Το ransomware μπορεί να εμφανίσει διάφορες καταστροφικές συμπεριφορές μετά την ολοκλήρωση της διαδικασίας κρυπτογράφησης. Ορισμένες οικογένειες ransomware κρυπτογραφούν τα αρχεία επιτόπου έτσι ώστε να αντικαθιστούν το αρχικό αρχείο με τις κρυπτογραφημένες εκδόσεις. Αφ 'ετέρου, ορισμένες οικογένειες

διαγράφουν τα αρχικά αρχεία του θύματος τροποποιώντας τον Master File Table (MFT) και δημιουργούν ένα νέο αρχείο που περιέχει την κρυπτογραφημένη έκδοση του αρχικού αρχείου [15]. Για την εξάλειψη της πιθανότητα επαναφοράς των αρχείων από στιγμιότυπα του συστήματος, ορισμένα ransomware όπως το Locky, διαγράφει τα Shadow copies των Windows μετά τη μόλυνση [98].

2.4.4.4 Locker-ransomware

Οι οικογένειες locker-ransomware κλειδώνουν τους πόρους του συστήματος για να αποτρέψουν την πρόσβαση των θυμάτων. Το locker-ransomware μπορεί να χωριστεί σε τρεις κατηγορίες: κλειδώματος οθόνης, κλειδώματος προγράμματος περιήγησης, και κλείδωμα του Master Boot Record (MBR).

Screen Locking ransomware

Το ransomware κλειδώνει τη γραφική διεπαφή του συστήματος του χρήστη και εμποδίζει την πρόσβαση στο σύστημα απαιτώντας λύτρα για την άρση του περιορισμού. Μπορούν να κλειδώσουν την οθόνη του θύματος χρησιμοποιώντας διαφορετικές μεθόδους, συμπεριλαμβανομένης της χρήσης λειτουργιών του λειτουργικού συστήματος (π.χ. CreateDesktop) για τη δημιουργία μιας νέας επιφάνειας εργασίας [15]. Ορισμένες οικογένειες ransomware όπως το Reveton [99] μπορούν να κάνουν λήψη εικόνων ή σελίδες HTML από διακομιστές C&C και δημιουργούν το banner κλειδώματος τους δυναμικά. Τέτοιου τύπου ransomware στοχεύουν και κινητές συσκευές. Για παράδειγμα το LockerPin ransomware παραμετροποιεί συγκεκριμένες παραμέτρους του API Android συσκευών ενώ άλλα όπως το WipeLocker απενεργοποιεί τα συγκεκριμένα κουμπιά (π.χ. Κουμπί Home) των κινητών συσκευών [27].

MBR Locking ransomware

Τα ransomware που κλειδώνουν το MBR, όπως το Seftad [100], στοχεύουν τα MBR του συστήματος. Το MBR ενός συστήματος περιέχει τις απαιτούμενες πληροφορίες για την εκκίνηση του λειτουργικού συστήματος. Ετσι, το αποτέλεσμα μιας τέτοιας κακόβουλης ενέργειας έχει ως στόχο να εμποδίσει το σύστημα να φορτώσει τον κωδικό εκκίνησης αντικαθιστώντας το αρχικό MBR με ένα τροποποιημένο MBR.

Browser Locking ransomware

Οι οικογένειες ransomware που κλειδώνουν το πρόγραμμα περιήγησης κλειδώνουν το πρόγραμμα περιήγησης ιστού του θύματος και ζητούν λύτρα. Οι εισβολείς κλειδώνουν τα προγράμματα περιήγησης των θυμάτων ανακατευθύνοντας τα θύματα

σε μια ιστοσελίδα που περιέχει ένα κακόβουλο κώδικας JavaScript. Σε αντίθεση με άλλες τακτικές κακόβουλου ransomware, η ανάκτηση από τα Browser Locking ransomware είναι σχετική πρακτικά απλή. Για να τρομάξουν τα θύματα, ένα τέτοιο ransomware μπορεί να εμφανίσει ένα μήνυμα λύτρων που δηλώνει ότι το υπολογιστής έχει μπλοκαριστεί λόγω παραβίασης του νόμου.

2.4.4.5 Εξαγωγή δεδομένων

Εκτός από την κρυπτογράφηση και την καταστροφή, ορισμένες οικογένειες ransomware, ειδικά τα πιο πρόσφατα, προσπαθούν να κλέψουν δεδομένα του θύματος (π.χ., πληροφορίες πιστωτικής κάρτας , εταιρικά έγγραφα, προσωπικά αρχεία) [90]. Έτσι μερικά ransomware απαιτούν δύο πληρωμές λύτρων. Μία πληρωμή για την αποστολή του κλειδιού για την αποκρυπτογράφηση των αρχείων, και μία για την αποτροπή δημοσίευσης των κλεμμένων πληροφοριών [101]. Στόχος είναι να απαιτήσουν περισσότερα λύτρα από τα θύματα και να επιταχύνουν τη διαδικασία πληρωμής.

2.4.5 Ταξινόμηση με βάση τρόπο πληρωμής

Ο κύριος στόχος του ransomware είναι η πληρωμή των λύτρων από τα θύματα. Βασικό χαρακτηριστικό των μεθόδων πληρωμής είναι η ανωνυμία. Τρόποι πληρωμής όπως προπληρωμένα κουπόνια ή προπληρωμένες κάρτες Paysafe έχουν χρησιμοποιηθεί καθώς προσφέρουν ανωνυμία αλλά δεν είναι προσφέρονται για την αποπληρωμή μεγάλων ποσών. Ωστόσο, τα κρυπτονομίσματα όπως το Bitcoin είναι η πιο προτιμώμενη μέθοδος καθώς προσφέρουν ψευδο- ανωνυμία, ταχύτητα και δυνατότητα κάλυψης οποιουδήποτε ποσού.

Chapter 3

Σχετικές Εργασίες

Μέσω της έρευνας στη σχετική βιβλιογραφια των τελευταίων εργαλείων anti-ransomware, εντοπίστηκαν πολλές διαφορετικές μέθοδοι ανίχνευσης. Σε αυτό το κεφάλαιο παρουσιάζονται άλλες εργασίες και τα αποτελέσματα τους.

3.1 Detection

3.1.1 RWGuard

Το RWGuard ενοποιεί τεχνικές που προτάθηκαν σε παλαιότερες εργασίες σε ένα μόνο εργαλείο για να αντιμετωπίσει τα ransomware [28]. Για τον εντοπισμό ransomware, το RWGuard αξιοποιεί μεμονωμένα module για να:

- ελέγξει εάν έχει τροποποιηθεί ένα αρχείο δόλωμα
- παρακολουθεί την συμπεριφορά ορισμένων processes
- εντοπίζει μη φυσιολογικές αλλαγές αρχείων
- ξεχωρίζει πότε μια κρυπτογραφική διαδικασία γίνεται από ransomware ή από τον χρήστη
- ελέγχει την κρυπτογραφική διαδικασία τοποθετόντας hooks στο CryptoAPI για την εκτέλεση τροποποιημένων συναρτήσεων

Το εργαλείο RWGuard χρησιμοποιεί τα πρωτότυπα αρχεία του χρήστη για την δημιουργεία των HoneyFiles. Οι συγγραφείς δηλώνουν ότι τα ονόματα των αρχείων HoneyFIles που δημιουργούνται είναι παρόμοια με τα γνήσια αρχεία χρηστών και με τέτοιο τρόπο ώστε τα HoneyFiles να ξεχωρίζουν, χωρίς ωστόσο, η ακριβής διαδικασία να περιγράφεται. Ο αριθμός των αρχείων δόλωμα καθορίζεται από τον χρήστη, η λίστα των τύπων των αρχείων είναι στατική (.txt, .doc, .pdf, .ppt και .xls) και τα περιεχόμενά τους δημιουργούνται με αντιγραφή από τα γνήσια αρχεία

του χρήστη. Τα μεγέθη των αρχείων HoneyFIle επιλέγονται τυχαία, ενώ το συνολικό μέγεθος των αρχείων decoy περιορίζεται στο 5% των κανονικών αρχείων.

3.1.2 Rlocker

Πρόκειται για ένα λογισμικό που ανιχνεύει την ύπαρξη ransomware σε λειτουργικά συστήματα Unix. Το R-Locker [29] χρησιμοποιεί HoneyFiles αλλά με ένα διαφορετικό από το συνηθισμένο τρόπο. Η προτεινόμενη προσέγγιση είναι η δημιουργία ενός κεντρικού αρχείου HoneyFile στο Home directory του χρήστη, το οποίο είναι στην πραγματικότητα ένα ειδικό αρχείο FIFO, δηλαδή ένα named pipe. Στη συνέχεια, το R-Locker γράφει μερικά byte σε αυτό το αρχείο FIFO, τα οποία δεν θα διαβαστούν έως ότου μια διεργασία αποκτήσει πρόσβαση στο named pipe. Κατά συνέπεια, οποιαδήποτε διαδικασία προσπαθεί να διαβάσει το named pipe θα ενεργοποιήσει το μηχανισμό προστασίας και θα ανιχνευθεί. Οι συγγραφείς προτείνουν να τοποθετηθούν πολλαπλά symbolic links που δείχνουν προς το κεντρικό αρχείο HoneyFile, σε διάφορα directories του συστήματος ώστε να μειωθεί ο χρόνος ανίχνευσης ransomware.

Σε αντίθεση με τα άλλα συστήματα anti-ransomware, το R-Locker ερμηνεύει οποιοδήποτε προσπάθεια read access στα αρχεία δόλωμα ως δραστηριότητα ransomware. Το ψευδώς θετικό ποσοστό αυτής της προσέγγισης, δηλαδή η συχνότητα εμφάνισης read access από μία νόμιμη διαδικασία, δεν αξιολογείται.

3.1.3 CryptDrop

Το CryptoDrop σχεδιάστηκε ώστε να παρακολουθεί σε πραγματικό χρόνο τις αλλαγές στα δεδομένα του χρήστη για τον εντοπισμό επίθεσης ransomware [30]. Το CryptoDrop έχει τρεις επιμέρους τρόπους αναγνώρισης της επίθεσης ransomware προκειμένου να μειωθεί ο αριθμός των ψευδώς θετικών ειδοποιήσεων (false positives) ενώ ταυτόχρονα προσπαθεί να κρατήσει τον αριθμό των κρυπτογραφημένο αρχείων από το ransomware στο ελάχιστο.

Τύπος αρχείου: Τα αρχεία σπάνια αλλάζουν τον τύπο ή τη μορφοποίησή τους, εκτός από την περίπτωση που έχουν κρυπτογραφηθεί. Επομένως η αλλαγή στους τύπους αρχείων θα μπορούσε να αποτελέσει ένδειξη ότι ένα σύστημα είναι υπό επίθεση, αν και μια μεμονωμένη αλλαγή σε έναν τύπο αρχείου δεν είναι επαρκής. Συνεπώς χρειάζονται αρκετές αλλαγές σε μικρό χρονικό διάστημα για να βεβαιωθούμε ότι υπάρχει επίθεση. Έτσι για να βρεθεί το σημείο που δεν προκύπτουν πολλά ψευδώς θετικά αποτελέσματα απαιτούνται πολλές δοκιμές με διαφορετικά ransomware.

Κατακερματισμός ομοιότητας: Δεδομένου ότι τα κρυπτογραφημένα αρχεία δεν είναι καθόλου όμοια με τα αρχικά αρχεία το περιεχόμενο αυτών των αρχείων μπορεί να συγκριθεί με κάποιο μέτρο ομοιότητας. Χρησιμοποιώντας similarity-preserving hash functions μπορεί κανείς να δει πόσο διαφορετικό είναι ένα αρχείο πριν και μετά την εγγραφή [31]. Αν η ομοιότητα κατακερματισμού είναι πολύ ανόμοια σε πολλά αρχεία εντός συγκεκριμένου χρονικού διαστήματος, τότε ίσως υπάρχει κάποια δραστηριότητα που να οφείλεται σε ransomware.

Εντροπία Shannon: Η υποτιθέμενη τιμή της πληροφορίας σε ένα μήνυμα ονομάζεται Εντροπία Shannon. Δεδομένου ότι τα κρυπτογραφημένα δεδομένα έχουν πάντα υψηλή εντροπία, αυτό σημαίνει ότι εάν πολλά αρχεία έχουν υψηλή εντροπία Shannon ως αποτέλεσμα της κρυπτογράφησης, τότε αυτό θα μπορούσε να υποδεικνύει ότι μια επίθεση ransomware βρίσκεται σε εξέλιξη.

Αυτές οι τρεις μέθοδοι είναι οι κύριες μέθοδοι που χρησιμοποιεί το CryptoDrop για τον εντοπισμό επιθέσεων ransomware. Επιπλέον, το CryptoDrop ειδοποιεί εάν υπάρχει διαγραφή πολλών αρχείων, καθώς αυτό θα μπορούσε επίσης να υποδεικνύει κακόβουλη δραστηριότητα. Το πλεονέκτημα του συνδυασμού αυτών των μεμονωμένων μεθόδων ανίχνευσης είναι ότι εάν ransomware δεν εντοπιστεί από μία, υπάρχει πιθανότητα να εντοπιστεί από μία άλλη [30].

3.1.4 Monitoring of the File System Activity (SSDT)

Ο εντοπισμός μιας επίθεσης ransomware είναι δυνατόν να επιτευχθεί παρακολουθώντας τη δραστηριότητα αρχείων του συστήματος [0]. Η προτεινόμενη μέθοδος χρησιμοποιώντας το System Service Descriptor Table (SSDT) φιλτράρει τα αιτήματα εισόδου/εξόδου (I/O) και τα χαρακτηριστικά τους, όπως όνομα διεργασίας, αναγνωριστικό διεργασίας κ.λ.π. Έτσι, εάν υπάρξει ένα πλήθος από ύποπτα αιτήματα I/O είναι πολύ πιθανόν να οφείλονται σε κακόβουλες διεργασίες. Τέλος βρίσκοντας μία κακόβουλη διεργασία που ίσως να οφείλεται σε ένα ransomware, είναι δυνατόν να εντοπιστεί η διεργασία γονέα (parent process) του κακόβουλου λογισμικού αλλά και κάθε επιπλέον διεργασία ή αρχείο που έχει δημιουργήσει το ransomware. Στη συνέχεια, όλες αυτές οι διεργασίες τερματίζονται και όλα τα αρχεία διαγράφονται.

Ο SSDT είναι ένας "internal dispatch table" των Windows και χρησιμοποιείται για να αντιστοιχεί system calls σε διευθύνσεις των kernel function. Οι πληροφορίες που επιστράφηκαν από τα system calls μπορούν να διαβαστούν ή να αλλάξουν εφαρμόζοντας μία τεχνική που ονομάζεται "hooking into the SSDT". Αυτή η τεχνική χρησιμοποιείται συχνά από rootkits και λογισμικά προστασίας από ιούς.

Αυτή η προσέγγιση υποστηρίζει ότι εφαρμόζοντας την παραπάνω τεχνική είναι πολύ δύσκολο να μην βρεθεί κάποια ύποπτη δραστηριότητα ακόμα και από μελλοντικά ransomware. Εκτός από αυτό οποιαδήποτε προσπάθεια να σταματήσει η λειτουργία παρακολούθησης των αρχείων είναι αδύνατη καθώς θα μπορεί να τερματίζεται από το ίδιο το σύστημα. Έτσι εκτός από αρκετά αποδοτικός τρόπος εντοπισμού ύποπτων διεργασιών, έχει τέτοια δομή που δεν μπορεί να παρακαμφθεί εύκολα από ένα ransomware.

3.2 Mitigation

Στην προηγούμενη ενότητα καλύψαμε τον τρόπο ανίχνευσης μιας επίθεσης από ransomware, ωστόσο, μόλις εντοπιστεί η επίθεση θα πρέπει να αντιμετωπιστεί. Στο κομμάτι της αντιμετώπισης της επίθεσης δεν υπάρχει εκτεταμένη έρευνα καθώς ο τρόπος αντιμετώπισης του ransomware είναι πολύ συγκεκριμένος. Οι δύο κύριοι τρόποι για να σταματήσουμε μια επίθεση είναι είτε να τερματίσουμε την λειτουργεία του συστήματος είτε να αναστείλουμε τη κακόβουλη διεργασία.

Η αναστολή ύποπτων διεργασιών (process) είναι μια καλή πρακτική καθώς δίνει την δυνατότητα για την επιπλέον ανάλυση και μελέτη αυτών. Η ανάλυση μπορεί να γίνει είτε αυτόματα είτε από κάποιο χρήστη. Με την εμπλοκή του χρήστη μπορεί επιπλέον να διασφαλιστεί ότι η διεργάσια δεν αποτελεί κάποιο κίνδυνο για το σύστημα. Στον αντίποδα αν ο χρήστης δεν έχει την κατάλληλη εμπειρία ή γνώση μπορεί να πάρει λάθος αποφάσεις και για παράδειγμα να μην τερματίσει κάποιες διεργασίες που τελικά είναι κακόβουλες ή να τερματίσει κάποιες άλλες που δεν είναι.

Το πλεονέκτημα του άμεσου τερματισμού ύποπτων διαδικασιών, είναι ότι η κακόβουλη διαδικασία τερματίζεται αμέσως, χωρίς να παρεμβαίνει ο χρήστης, ελαχιστοποιώντας το περιθώριο λάθους. Βέβαια εδώ θα πρέπει να τονιστεί ότι η αποτελεσματικότητα της αναγνώρισης κακόβουλων ή μη εργασιών από την εφαρμογή ασφάλειας παίζει σημαντικό ρόλο καθώς ο τερματισμός μιας μη κακόβουλης διεργασίας μπορεί να οδηγήσει σε απώλεια δεδομένων ή αστάθεια του συστήματος.

Τέλος, στην περίπτωση του τερματισμού λειτουργείας θα πρέπει να δώσουμε προσοχή καθώς έχουν παρατηρηθεί αντίποινα από ορισμένα ransomware. Ένα τέτοιο παράδειγμα αποτελεί το Jigsaw που μπορεί να διαγράψει έως και 1000 αρχεία κατά την επανεκκίνηση μετά τον εντοπισμό του[102].

Chapter 4

Προσέγγιση του Προβλήματος

4.1 Honeypots

Τα Honeypots είναι συστήματα που δουλεύουν ως δόλωμα καθώς προσελκύουν τους επιτιθέμενους και τους ξεγελούν για να αλληλεπιδράσουν με αυτά. Αυτά ορίζονται ως εξής:

Το honeypot είναι ένας πόρος υπολογιστών που παρακολουθείται στενά και θέλουμε να διερευνηθει ή να παραβιαστεί [32].

Ένας χρήστης θα πρέπει να αναζητήσει συγκεκριμένα τέτοια συστήματα. Αυτό σημαίνει ότι, εξ ορισμού, οποιαδήποτε επαφή με αυτά θεωρείται ύποπτη. Γενικά, αυτό οδηγεί σε πολύ χαμηλά ποσοστά ανίχνευσης ψευδώς θετικών ειδοποιήσεων, καθώς υποτίθεται ότι δεν υπάρχει πρόσβαση σε αυτούς τους πόρους από τους νόμιμους χρήστες και από τις εφαρμογές που χρησιμοποιούν. Επίσης, τα honeypots μπορούν να βοηθήσουν στην παραπλάνηση των επιτιθέμενων, κάνοντάς τους να χάσουν χρόνο εξετάζοντας ένα εικονικό σύστημα αντί να επιτίθενται σε σημαντικότερα συστήματα. Κατά την αλληλεπίδραση με αυτά δεν παραβιάζεται κανένα πραγματικό σύστημα και οι υπάλληλοι ασφαλείας έχουν αρκετό χρόνο για να λάβουν τα κατάλληλα αντίμετρα.

Υπάρχουν διάφοροι τύποι honeypot, με διαφορετικές δυνατότητες, απαιτήσεις. Ενώ υπάρχουν πολλές ταξινομήσεις τέτοιων συστημάτων, οι ακόλουθες τρεις είναι οι πιο διαδεδομένες:

- Low and High-Interaction honeypots [33]
- Server and Client-based honeypots [34]
- Physical and Virtual honeypots [35]

4.1.1 Low- and High-Interaction honeypots

Τα Honeypots μπορούν να ομαδοποιηθούν με βάση την αλληλεπίδραση μεταξύ του εισβολέα και του συστήματος σε τρεις κατηγορίες: low, medium and high-interaction honeypots [33].

4.1.1.1 Low-Interaction honeypots

Τα honeypot χαμηλής αλληλεπίδρασης προσομοιώνουν μια συγκεκριμένη υπηρεσία, ένα σύστημα αρχείων ή μια διεπαφή σε ένα προσομοιωμένο περιβάλλον [33]. Παρέχουν περιορισμένη πρόσβαση στο λειτουργικό σύστημα ή το hardware διατηρώντας την δυνατότητα πρόσβασης σε αυτά απο τον επιτιθέμενο. Έχουν σχεδιαστεί με τέτοιο τρόπο που ενεργοποιούνται μόνο όταν ο επιτιθέμενος αλληλεπιδράσει με αυτά. Τέλος, είναι εύκολο να αναπτυχθούν σε ένα σύστημα και δεν απαιτούν πολύ επεξεργαστική ισχύ.

4.1.1.2 High-Interaction honeypots

Ένα honeypot υψηλής αλληλεπίδρασης αποτελείται από ένα πραγματικό λειτουργικό σύστημα και υπηρεσίες [33]. Η ιδέα είναι να παρέχουμε σε έναν εισβολέα ένα πραγματικό σύστημα και να παρακολουθούμε την αλληλεπίδραση μαζί του. Δεδομένου ότι τα honeypot υψηλής αλληλεπίδρασης λειτουργούν σε πραγματικά λογισμικό, τυχόν σφάλματα και τρωτά σημεία στο λειτουργικό σύστημα ή σε οποιαδήποτε εφαρμογή μπορεί να χρησιμοποιηθούν για να θέσουν σε κίνδυνο όλο το σύστημα. Αυτό μπορεί να οδηγήσει σε πλήρη πρόσβαση στο μηχάνημα, το οποίο μπορεί στη συνέχεια να χρησιμοποιηθεί για να εξαπολύσει επιθέσεις εναντίον άλλων συστηματων.

Γενικά, αυτή η προσέγγιση αποδίδει ακριβέστερα δεδομένα για την ανάλυση της επίθεσης όμως είναι πιο δύσκολο να εγκατασταθούν, απαιτούν σημαντικό όγκο επεξεργαστικής ισχύς και συνεχής παρακολούθηση.

4.1.1.3 Medium-Interaction honeypots

Τα honeypots μέσης αλληλεπίδρασης βρίσκονται εννοιολογικά μεταξύ των παραπάνω και δεν θεωρούνται πάντα δική τους κατηγορία [33]. Συνήθως, δεν προσομοιώνουν πλήρως ένα λειτουργικό σύστημα, αλλά υλοποιούν ένα application layer ώστε να καταγράφονται οι αλληλεπιδράσεις με το σύστημα.

4.1.2 Server- and Client-based

Η διάκριση μεταξύ των honeypot που βασίζονται σε διακομιστή και πελάτη είναι απαραίτητη, καθώς περιγράφουν δύο πολύ διαφορετικά μοντέλα αλληλεπίδρασης και περιπτώσεις χρήσης [34]. Διακομιστές honeypot έχουν ως στόχο να προσελκύσουν επιτιθέμενους, περιμένοντας παθητικά για κάποια πρόσβαση. Εξαιτίας αυτής της λειτουργικότητας, οποιαδήποτε σύνδεση με αυτά μπορεί να θεωρηθεί ύποπτη. Αυτό συμπίπτει με τον «παραδοσιακό» ορισμό των honeypots που δίνεται παραπάνω. Από την άλλη πλευρά, τα honeypots πελατών προσομοιώνουν έναν πελάτη, συνήθως ένα πρόγραμμα περιήγησης ιστού και συνδέονται σε διακομιστή όπου ελέγχονται ύποπτες δραστηριότητες. Σε σύγκριση με τα server honeypot, πρέπει να ορίσουν τι θεωρείται ύποπτη κίνηση. Αυτό επιτυγχάνεται με τη χρήση στατικής ανάλυσης, όπως αντιστοίχιση υπογραφών.

4.1.3 Physical vs. Virtual

Η τρίτη ταξινόμηση των honeypot χωρίζεται σε φυσικά και εικονικά honeypot [35]. Ο πρώτος τύπος τρέχει σε ένα πραγματικό μηχάνημα, το οποίο προσφέρεται για πιο ρεαλιστικές επιθέσεις. Από την άλλη πλευρά, η ανάπτυξη αυτού του τύπου είναι πιο ακριβή, γιατί για κάθε νέο honeypot απαιτείται επιπλέον μηχάνημα. Συνεπώς, τα physical honeypots δεν είναι κατάλληλα για μεγαλύτερου εύρους εφαρμογές, πρέπει να διαχειρίζονται χειροκίνητα και ως εκ τούτου έχουν περιοριστεί μόνο στη χρήση για ερευνητικές μελέτες μεγάλης κλίμακας. Ωστόσο, τα φυσικά συστήματα honeypot εξακολουθούν να υπάρχουν και χρησιμοποιούνται για περιπτώσεις ειδικής χρήσης, όπως το HoneyDroid, ένα honeypot που τρέχει σε Android τηλέφωνα. Δεδομένου ότι τα εικονικά περιβάλλοντα έχουν γίνει περισσότερο διαδεδομένα και οικονομικά λόγο της αύξησης της επεξεργαστικής ισχύς, τα περισσότερα honeypots στις μέρες μας τρέχουν σε εικονικές μηχανές. Τα κύρια πλεονεκτήματα είναι ευκολότερη ανάπτυξη και ευκολότερη επεκτασιμότητα. Ένα φυσικό μηχάνημα μπορεί να διαχειρίζεται πολλαπλές εικονικές μηχανές που με τη σειρά τους αναπτύσσουν πολλαπλά honeypot. Επιπλέον, η πλειοψηφία των μηχανών που χρησιμοποιούνται στο υπολογιστικό νέφος είναι εικονικές παρέχοντας επιπλέον ασφάλεια [36].

4.2 Μέθοδος αντιμετώπισης

4.2.1 Σχεδιασμός

Για τον σχεδιασμό της στρατηγικής που θα ακολουθηθεί απέναντι στα ransomware απαιτείται να γίνει πλήρως αντιληπτός ο τρόπος δράσης τους αφού καταφέρουν να περάσουν από τις άμυνες του συστήματος. Τα ransomware, ανάλογα και με την οικογένεια στην οποία ανήκουν, στοχεύουν ένα ευρύ φάσμα από τύπους αρχείων και αυτά μπορεί να είναι ".txt", ".doc",".docx", ".xls", ".xlsx", ".ppt", ".pptx", ".odt", ".png", ".csv",".sql", ".mdb", ".sln", ".php", ".asp", ".aspx", ".html" , ".xml", ".psd" [37]. Τα αρχεία που αποτελούν πιθανούς στόχους του ransomware είτε κρυπτογραφούνται με το που εντοπιστούν, είτε αποθηκεύεται η θέση τους στον δίσκο για να κρυπτογραφηθούν στο τέλος όλα μαζί. Επίσης έχει παρατηρηθεί ότι τα ransomware ελέγχουν για τους διαθέσιμους δίσκους του συστήματος, το είδος τους (εξωτερικός δίσκος, εσωτερικός δίσκος, RAM, κ.λ.π.) καθώς και τον διαθέσιμο ελεύθερο χώρο. Γενικά, στοχεύουν περισσότερο τους διαθέσιμους εσωτερικούς δίσκους και επιλέγουν μονοπάτια στο δίσκο όπως C:/Users/ και τους υποφακέλους [37] ενώ αποφεύγουν directories όπως Windows, Program Files, $Recycle.bin [38]. Η σειρά με την οποία γίνεται η κρυπτογράφηση των αρχείων καθώς και η διάσχιση των μονοπατιών του δίσκου είναι σε Windows-1252 ή αντίστροφα, ορισμένες φορές με βάση το μέγεθος ή τυχαία [37]. Τέλος, υπάρχουν τρεις τρόποι με τους οποίους γίνεται η κρυπτογράφηση των αρχείων i) Write-in-place, ii) Rename-and-encrypt, και iii) Create-encrypt-and-delete [103].

- Write-in-place: δημιουργεί ένα προσωρινό αρχείο και κρυπτογραφεί το φάκελο στόχο, γράφει τα κρυπτογραφημένα δεδομένα του φακέλου στόχου στο νέο φάκελο, και τέλος επανεγγράφει στο φάκελο στόχο το περιεχόμενο του καινούριου φακέλου και στην συνέχεια τον διαγράφει.
- Rename-and-encrypt: αλλάζει το όνομα του φακέλου στόχου, κρυπτογραφεί τα δεδομένα όπως στην περίπτωση Write-in-place και τέλος αλλάζει το όνομα του αρχείου στόχου στην αρχική του ονομασία.
- Create-encrypt-and-delete: δημιουργεί ένα αρχείο και κρυπτογραφεί σε αυτό τα δεδομένα του αρχείου στόχου και διαγράφει τον φάκελο στόχο.

Λαμβάνοντας όλα αυτά υπόψη για να έχουμε όσο το δυνατόν καλύτερα και ταχύτερα αποτελέσματα τα HoneyTokens μας θα πρέπει:

- να αποτελούνται από αρχεία που θα τοποθετηθούν κυρίως στο μονοπάτι C:/Users/ του δίσκου

- να αποτελούνται από ποικίλους τύπους αρχείων, (".txt", ".doc",".docx", ".xls" κ.λ.π)
- να έχουν όνομα έτσι εάν αν σειρά κρυπτογράφησης που ακολουθείται είναι σε Windows-1252, να κρυπτογραφούνται πρώτα ή αντίστροφα
- να έχουν μέγεθος αντίστοιχο της σειράς κρυπτογράφησης (π.χ. κρυπτογράφηση σε αύξουσα σειρά θα πρέπει το μέγεθος του αρχείου να είναι μικρό)

Τέλος, το πρόγραμμα που θα υλοποιηθεί θα πρέπει να δίνει έμφαση στο άνοιγμα των αρχείων καθώς και οι τρεις τρόποι κρυπτογράφησης απαιτούν την πρόσβαση στα περιεχόμενα του. Παράλληλα θα πρέπει να δοθεί προσοχή στη μετονομασία, στη δημιουργία, και στη διαγραφή αρχείων.

4.2.2 Restart Manager

Αρχικά, θα πρέπει να βρεθεί ένας μηχανισμός ο οποίος θα μπορεί να παρακολουθεί τις αλλαγές που γίνονται στα HoneyTokens που έχουν τοποθετηθεί στο δίσκο. Για τον λόγο αυτό επιλέχθηκε η χρήση του API Restart Manager. Το Restart Manager είναι μια βιβλιοθήκη που σχεδιάστηκε για τη μείωση των απαιτούμενων επανεκκινήσεων του λειτουργικού συστήματος κατά τις ενημερώσεις λογισμικού. Τα αρχεία που ενδέχεται να τροποποιηθούν κατά τη διάρκεια μιας ενημέρωσης μπορεί να έχουν "κλειδωθεί" από εφαρμογές, εμποδίζοντας τη διαδικασία της ενημέρωσης. Αυτό μπορεί να οδηγήσει σε επανεκκίνηση του συστήματος αναγκάζοντας τις εφαρμογές να απελευθερώσουν τα αρχεία που έχουν κλειδώσει. Σε αντίθεση, το Restart Manager επιτρέπει στις διεργασίες να απελευθερώσουν τα αρχεία τερματίζοντας τις διαδικασίες που τα χρησιμοποιούν, εάν πληρούνται οι απαιτούμενες προϋποθέσεις [104].

4.2.2.1 Προέλευση

Κάθε λειτουργικό σύστημα (OS) έχει έναν μοναδικό τρόπο χειρισμού της ταυτόχρονης πρόσβασης σε αρχεία. Στην περίπτωση των Windows, ανάλογα με το πώς έχει ανοίξει ένα αρχείο, μια διεργασία μπορεί να έχει αποκλειστική πρόσβαση στο αρχείο, όπως στην περίπτωση του file mapping ή αρχείων που έχουν ανοιχτεί χωρίς τη λειτουργεία FILE_SHARE_READ | FILE_SHARE_WRITE. Σε τέτοιες περιπτώσεις, το αρχείο μπορεί να «κλειδωθεί» από τη διαδικασία, οδηγώντας στην απόρριψη άλλων διαδικασιών που ζητούν πρόσβαση ανάγνωσης ή εγγραφής σε αυτό το αρχείο. Εάν άλλες διεργασίες χρειάζονται πρόσβαση σε ένα "κλειδωμένο αρχείο", μπορούν να ζητήσουν επανεκκίνηση ολόκληρου του συστήματος

για να ελευθερωθεί το αρχείο προκαλώντας διακοπή των λειτουργιών του χρήστη. Για να λυθεί αυτό το πρόβλημα, ξεκινώντας από τα Windows Vista, η Microsoft παρουσίασε το Restart Manager, επιτρέποντας στις εφαρμογές να τερματίζουν διαδικασίες που κλειδώνουν τους πόρους χωρίς να απαιτείται επανεκκίνηση.

4.2.2.2 Χρήση του Restart Manager

Το Restart Manager υλοποιείται στα Windows μέσω της βιβλιοθήκης "RstrtMgr.dll", που βρίσκεται στο C:\Windows\System32\. Οι διεργασίες αλληλεπιδρούν με το Restart Manager μέσω των “sessions”. Στο κάθε “session” καταχωρείται ένα σύνολο πόρων (αρχεία, processes, services) και λαμβάνονται πληροφορίες που σχετίζονται με αυτές. Οι παραπάνω πόροι αντιπροσωπεύουν στόχους που πρέπει να προσπελαστούν από μια διαδικασία. Ο ρόλος του Restart Manager είναι να προσδιορίζει ποιες διεργασίες μπλοκάρουν αυτήν τη στιγμή έναν συγκεκριμένο πόρο, που αναφέρεται ως επηρεαζόμενη εφαρμογή, και να αποθηκεύει τις πληροφορίες σχετικά με τις εφαρμογές σε μια λίστα. Με αυτόν τον τρόπο είναι δυνατόν να σχεδιαστεί ένα πρόγραμμα όπου μέσω Restart Manager session, να καταχωρούνται ένα σύνολο αρχείων, διεργασιών ή υπηρεσιών που πρέπει να χρησιμοποιηθούν, για να προσδιοριστεί ποιες διεργασίες εμποδίζουν την πρόσβασή τους. Εάν υπάρχουν, το Restart Manager θα παρέχει τη λίστα των εφαρμογών που επηρεάζονται και το πρόγραμμα μπορεί να ζητήσει τον τερματισμό λειτουργίας αυτών των εφαρμογών. Μία προέκταση αυτού του προγράμματος είναι η παρακολούθηση πόρων που θα λειτουργούν ώς HoneyTokens και όταν παρατηρηθεί κάποια δραστηριότητα (π.χ. άνοιγμα και κρυπτογράφηση) σε αυτά να τερματίζεται κάθε διεργασία.

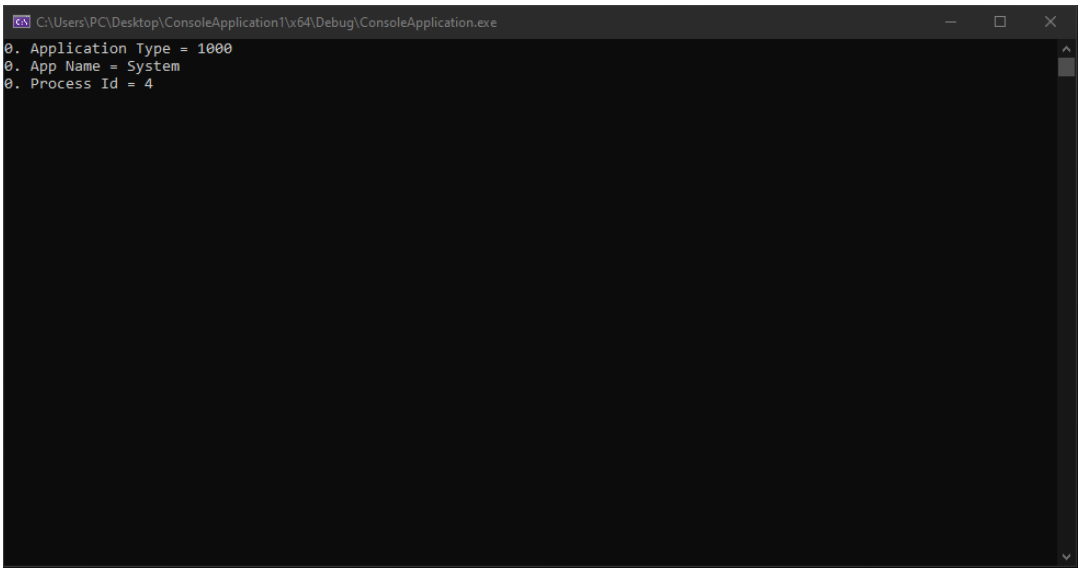

Figure 4.1: RM APP TYPE 1000

4.2.3 Υλοποίηση

Το πρώτο βήμα για την υλοποίηση της εφαρμογής είναι η κλήση της συνάρτησης RmStartSession για την δημιουργία του Restart Manager session. Η συνάρτηση επιστρέφει ένα session handle και ένα session key τα οποία είναι απαραίτητα στα επόμενα βήματα. Αφού έχει δημιουργηθεί το session μπορούν να καταχωρηθούν οι πόροι του συστήματος που θα παρακολουθούνται κάνοντας κλήση της συνάρτησης RmRegisterResources. Ένας πόρος μπορεί να είναι ένα αρχείο, ένα process ή ένα service. Στην περίπτωση αυτή θα χρησιμοποιήσουμε αρχεία καθώς αυτά στοχεύουν τα περισσότερα ransomware, αν και έχει παρατηρηθεί ότι ορισμένα ransomware πριν απο την κρυπτογράφηση τερματίζουν συγκεκριμένα Windows Services [105]. Στη συνέχεια αφού έχουν καταχωρηθεί με επιτυχία οι πόροι που θα παρακολουθούνται, τότε με τη χρήση της συνάρτησης RmGetList επιστρέφεται μία λίστα με δομές RM_PROCESS_INFO καθώς και ο αριθμός των process που χρησιμοποιούν τα HoneyFiles. Όσο ο αριθμός είναι μηδέν αυτό σημαίνει ότι δεν υπάρχει κάποια πρόσβαση. Αν όμως αλλάξει τότε πιθανόν να υπάρχει παραβίαση του συστήματος. 'Ετσι, διασχίζοντας τα στοιχεία της λίστας που επιστρέφει η συνάρτηση RmGetList μπορεί να βρεθεί το ID του εκάστοτε process της. Το ID είναι πληροφορία που βρίσκεται στη δομή RM_PROCESS_INFO. Αποκτώντας πρόσβαση σε ένα process object γίνεται να βρεθεί η θέση του μονοπατιού μέσα στον δίσκο στο οποίο βρίσκεται η εφαρμογή που χρησιμοποιεί τον πόρο μας, δηλαδή η θέση στον δίσκο όπου βρίσκεται το ransomware, και να την τερματίσει όπως φαίνεται και στην Εικόνα 4.3. Εδώ πρέπει να σημειωθεί ότι υπάρχουν 7 τύποι RM_APP_TYPE εκ των οποίων ο ένας χαρακτηρίζεται critical και δεν είναι δυνατόν να τερματιστεί παρά μόνο με τερματισμό του συστήματος. Αυτό φαίνεται στην Εικόνα 4.1 όπου βλέπουμε ότι ο τύπος της εφάρμογής είναι 1000, δηλαδή critical και πρόκειται για εντολή κρυπτογράφησης openSSL που εκτελέστηκε σε Ubuntu terminal environment με τη χρήση του Windows Subsystem for Linux (WSL). Έτσι, όποτε προκύπτει κάποια αλλαγή στα HoneyFiles ενημερώνεται ο νόμιμος χρήστης του συστήματος. Αυτό γίνεται αξιοποιώντας την υπηρεσία Canary Token. Το Canary Token δίνει την δυνατότητα υλοποίησης διαφορετικών ειδών Token όπως Microsoft Word Document, PDF, QRCode, SQL SERVER και DNS Token το οποίο χρησιμοπιήθηκε [106]. Η ειδοποίηση γίνεται μέσω Email, Εικόνα 4.2.

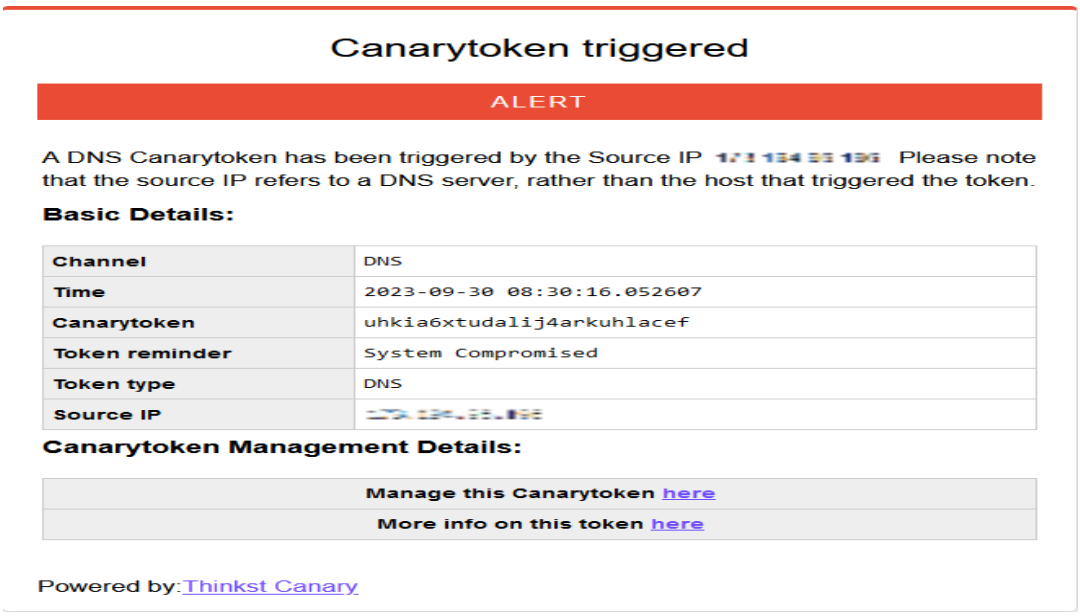

FIGURE 4.2: Canary Token Triggered

Ωστόσο μετά από πειράματα που έγιναν τα οποία αποτελούνταν από script που προσομοιώνουν μία τυπική λειτουργία του ransomware, παρατηρήθηκαν δύο αδυναμίες. Η πρώτη και σημαντικότερη μπορεί να γίνει αντιληπτή τόσο πειραματικά όσο και λογικά. Έχει να κάνει με τον τρόπο που κρυπτογραφεί τα δεδομένα το ransomware. Αν το ransomware ακολουθεί τη διαδικασία Rename-and-encrypt, δηλαδή να αλλάξει το όνομα του HoneyFile πριν την κρυπτογράφηση, επειδή έχει καταχωρηθεί το HoneyFile στην λίστα των πόρων που παρακολουθούνται με διαφορετικό όνομα και μονοπάτι, δεν είναι δυνατός ο εντοπισμός της κακόβουλης διεργασίας σε ένα πόρο που δεν υπάρχει. Η δεύτερη αδυναμία έχει να κάνει με το μέγεθος του HoneyFile. Αν είναι πολύ μικρό το μέγεθος του HoneyFile (<10MB) το άνοιγμα και η κρυπτογράφηση γίνονται πολύ γρήγορα και το πρόγραμμα δεν μπορεί να ανιχνεύσει το process. Αυτό βέβαια αλλάζει από υπολογιστή σε υπολογιστή καθώς εξαρτάται από τα χαρακτηριστικά και τις επιδόσεις του. Συγκεκριμένα οι παραπάνω πειραματισμοί έγιναν σε μηχάνημα με CPU: AMD Ryzen 5 2600, RAM: 16GB 2600Hz CL 16-18-18, Storage: SSD Read Speed 560 MB/s Write Speed 510 MB/s Maximum 4KB Random Write 90000 IOPS, OS Windows 10.

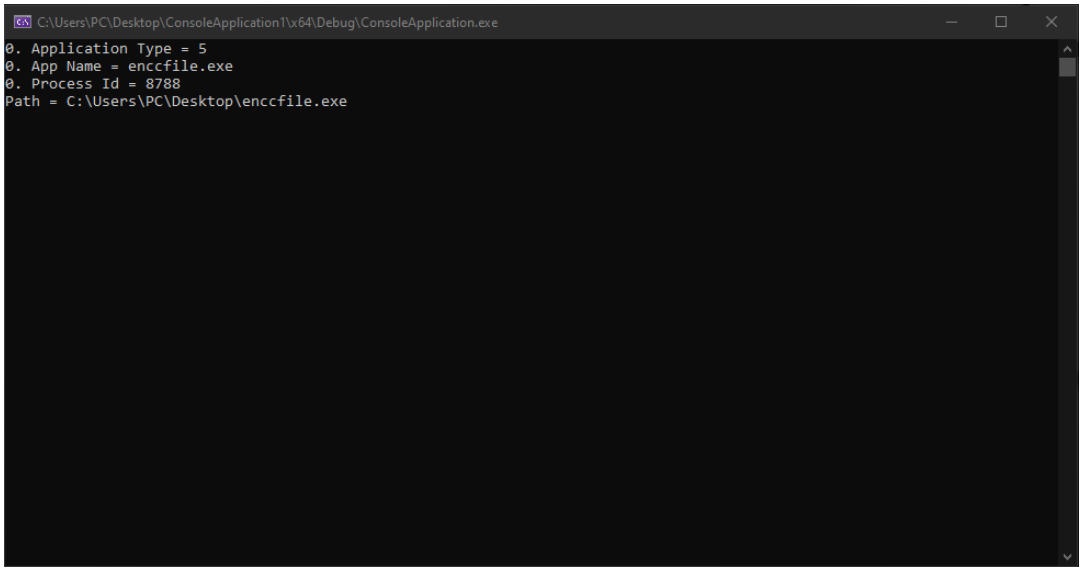

FIGURE 4.3: Encryption Process Found And Terminated

4.2.4 Αντιμετώπιση περιορισμών

Για την αντιμετώπιση της αδυναμίας εντοπισμού του ransomware όταν έχει προηγηθεί αλλαγή του ονόματος του HoneyFile η λύση δόθηκε με την χρήση της κλάσης System.IO.FileSystemWatcher [107]. Η κλάση αυτή υποστηρίζει ότι δίνει την δυνατότητα να παρακολουθούνται αλλαγές όπως άνοιγμα/ διαγραφή /μετονομασία σε ένα μονοπάτι του δίσκου. Μια επιπλέον δυνατότητα της κλάσης είναι ότι μπορεί να ορίσει φίλτρα στα αρχεία που παρακολουθούνται. Τέτοια φίλτρα μπορεί να είναι ονόματα και τύποι αρχείων. Αξιοποιώντας και αξιολογώντας την κλάση παρατηρήθηκε ότι δεν είναι δυνατόν να ορισθεί ώς μονοπάτι ένας ολόκληρος δίσκος αλλά ένα τμήμα του. Αυτό δεν αποτελεί μεγάλο περιορισμό καθώς όπως αναφέρθηκε προηγουμένως τα περισσότερα ransomware στοχεύουν το μονοπάτι C:/Users/... το οποίο και είναι δυνατόν να παρακολουθηθεί. Ένας ακόμα περιορισμός που πρέπει να αντιμετωπιστεί είναι πως θα ξεχωρίζει το σύστημα παρακολούθησης τα HoneyFiles από τα αρχεία που χρησιμοποιεί ο χρήστης ή μη κακόβουλες εφαρμογές του συστήματος. Αυτό γίνεται για την αποφυγή όσο το δυνατόν περισσότερων ψευδών θετικών παραβιάσεων. Η λύση που δόθηκε είναι τα αρχεία που παρακολουθούνται θα πρέπει να περιέχουν μια κοινή συμβολοσειρά στο όνομα τους τέτοια όμως που δεν θα αντιλαμβάνεται το ransomware ότι τα αρχεία είναι HoneyFiles (π.χ. Honeybait.odt, ransomwarebait.txt). Για την λύση του προβλήματος καθώς και για να αποδειχθεί ότι είναι δυνατή η λύση που σχεδιάστηκε χρησιμοποιήθηκε το όνομα "test*". Έτσι κάθε αραχείο που το όνομα του θα περιέχει την λέξη/συμβολοσειρά test θα παρακολουθείται. Η απόδοση αυτής της προσέγγισης επιβεβαιώθηκε τρέχοντας Script που προσομοιώνουν

τους τρεις διαφορετικούς τρόπους με τους οποίους μπορεί να κρυπτογραφεί ένα αρχείο. Πιο συγκεκριμένα, στην Εικόνα 4.4 βλέπουμε το αποτέλεσμα από ένα script το οποίο κρυπτογραφεί ένα αρχείο με την μέθοδο Rename-and-encrypt. Αρχικά μετανομάζει το HoneyFile από "test create.txt" σε "test rename.txt" και έπειτα το διαγράφει.

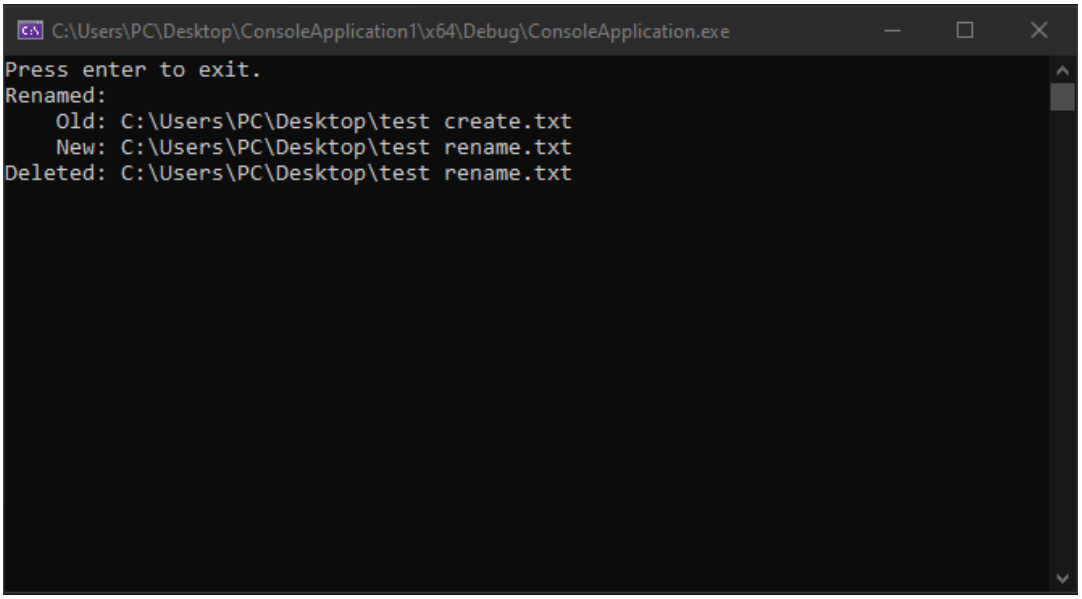

FIGURE 4.4: Rename-Delete Action Detected On Desktop

Ωστόσο ο σχεδιασμός anti-ransomware εφαρμογών πρέπει να προβλέπει και τους πιθανούς τρόπους με τους οποίους μπορούν να παρακαμφθούν οι μηχανισμοί ανίχνευσης. Στην περίπτωση αυτή δεδομένου ότι χρησιμοποιούνται HoneyFiles θα πρέπει να εξεταστεί πως μπορεί ένα ransomware να καταλάβει αν ένα αρχείο είναι HoneyFile. Έτσι για να είναι πιο αποδοτικά τα HoneyFiles θα πρέπει:

1. Το μέγεθος τους δεν θα πρέπει να είναι πολύ μεγάλο ή πολύ μικρό. Τέτοια συμπεριφορά έχει παρατηρηθεί σε ένα Android ransomware, το SLocker, όπου δεν κρυπτογραφούνταν αρχεία μικρότερα από 150KB και μεγαλύτερα από 50MB.

2. Το HoneyFiles ανεξάρτητα από το μέγεθος τους δεν θα πρέπει να μην είναι γεμάτα με μηδενικά γιατί είναι εύκολο να το αντιληφθεί το ransomware.

3. Τα ransomware πριν αρχίσουν να κρυπτογραφούν τα αρχεία ενός συστήματος στόχου μπορεί να παραμείνουν αδρανή. Σε αυτό το διάστημα μπορούν να παρατηρούν ποια αρχεία χρησιμοποιεί ο χρήστης και ποια όχι. Αυτό μπορεί να οδηγήσει ένα ransomware να πιθανολογήσει ότι τα τελευταία αποτελούν HoneyFiles. Αν ένα ransomware αξιοποιήσει ένα μηχανισμο αντίστοιχο

του FileSystemWatcher ή αξιοποιώντας το Master File Table (MTF), ο οποίος περιέχει τις πληροφορίες αρχείων όπως date created, last access, attributes, μπορεί να δει ποια αρχεία δεν χρησιμοποιούνται και να αποφύγει να τα κρυπτογραφήσει καθιστώντας τα HoneyFiles άχρηστα. Αυτό μπορεί να παρακαμφθεί δημιουργώντας ένα μηχανισμό ο οποίος περιοδικά και τυχαία θα αλλάζει κάποια στοιχεία όπως το last access ή θα προσομοιώνει την χρήση τους από τον χρήστη. Η αποτελεσματικότητα αυτού του μηχανισμού μπορεί να αποτελέσει αντικείμενο για περαιτέρω μελέτη.

4.3 Tests

Σε αυτό το κεφάλαιο γίνεται μια εις βάθος ανάλυση του τρόπου με τον οποίο πραγματοποιήθηκαν τα test για την αξιολόγηση του εργαλείου που σχεδιάστηκε.

4.3.1 Περιβάλλον δοκιμής

Αρχικά έπρεπε να επιλεχθεί ένα περιβάλλον δοκιμής ικανό να δοκιμάσει την μέθοδο ανίχνευσης και αντιμετώπισης του ransomware που σχεδιάστηκε. Επιπλέον θα πρέπει να παρέχει την αντίστοιχη προστασία του φυσικού υπολογιστή αλλά και να μπορεί να διαμορφωθεί σε σύντομο χρονικό διάστημα για την δοκιμή των διαφορετικών ransomware. Για τον λόγο αυτό επιλέχθηκε το Windows Sandbox. Το Windows Sandbox παρέχει ένα ελαφρύ περιβάλλον εργασίας για την ασφαλή εκτέλεση εφαρμογών σε χρήστες των Windows των εκδόσεων Pro, Enterprise, και Education. Παράλληλα διατηρεί πρόσβαση στο διαδίκτυο το οποίο είναι σημαντικό, καθώς επιτρέπει στα ενεργά ransomware να επικοινωνήσουν με τους διακομιστές τους επιτρέποντας τον πλήρη κύκλο λειτουργίας τους.

Το πλεονέκτημα του περιβάλλοντος δοκιμής ήταν ότι μπορεί να διασφαλίσει ότι τα ransomware δεν θα εξαπλωθούν ανεξέλεγκτα είτε στο φυσικό μηχάνημα είτε στο υπόλοιπο δίκτυο. Επιπλέον, δεδομένου ότι έχουν αφαιρεθεί οι επεκτάσεις από τα δυαδικά αρχεία ransomware, και η λήψη τους γίνεται απευθείας στο Sandbox δεν είναι δυνατή η τυχαία εκτέλεση των ransomware στο φυσικό μηχάνημα. Μια τυπική διαδικασία εκτέλεσης ενός test είναι:

1. Εκκίνηση Windows Sandbox
2. Λήψη όλων των απαραίτητων αρχείων συμπεριλαμβανομένου του ransomware, του εργαλείου ανίχνευσης και αντιμετώπισης, των βιβλιοθηκών που απαιτούνται για την εκτέλεση του, των Script για την μεταφορά αρχείων σε συγκεκριμένα σημεία του δίσκου,τον έλεγχο ύπαρξης αυτών μετά

την εκτέλεση του ransomware, του κεντρικού Script ελέγχου, και τέλος την εγκατάσταση εφαρμογών για να κάνουν το περιβάλλον δοκιμής πιο ρεαλιστικό.

3. Εκτέλεση του κεντρικού Script το οποίο υλοποιεί με την ακόλουθη σειρά i)του Script που μετακινεί τα αρχεία σε συγκεκριμένα σημεία του δίσκου ii)την ενεργοποίηση του εργαλείου iii)την εκτέλεση του ransomware iv) την εκτέλεση του Script ελέγχου των αρχείων
4. Αναμονή 20 λεπτών για την εκτέλεση του Script ελέγχου των αρχείων για την καταγραφή των κρυπτογραφημένων αρχείων και τον έλεγχο της αντίδρασης του εργαλείου.

Η διαδικασία είναι αρκετά αυτοματοποιημένη καθώς πέρα από την λήψη και εγκατάσταση των απαιτούμενων αρχείων, η υπόλοιπη διαδικασία ελέγχονταν από ένα κεντρικό Script όπως περιγράφηκε προηγουμένως. Πρέπει να σημειωθεί πως παρόλο που το τελικό εργαλείο δίνει την δυνατότητα ο κάθε χρήστης να εισάγει τις δικές του παραμέτρους (π.χ., CannaryToken, δημιουργία και αφαίρεση Honeytoken) στην πειραματική διαδικασία αυτά γινόντουσαν αυτόματα από το εργαλείο για την επιτάχυνση της όλης διαδικασίας. Ωστώσο, παρόλο που οι συνθήκες των test ήταν ίδιες, κάποιες φορές τα Scripts χρειάστηκαν παραμετροποίηση για να υπάρξει το επιθυμητό αποτέλεσμα ενώ άλλες φορές ορισμένα δείγματα ransomware προκαλούσαν προβλήματα με την μνήμη και τη σύνδεση με το Sandbox και το test έπρεπε να επαναληφθεί.

4.3.2 Δείγματα ransomware

Μετά την επιτυχή αντιμετώπιση των Script που προσομοιώνουν ένα ransomware αποφασίστηκε να δοκιμαστεί η αποτελεσματικότητα του εργαλείου που σχεδιάστηκε σε πραγματικά ransomware. Υπάρχουν πολλά διαδικτυακα αποθετήρια όπου μπορεί κάποιος ερευνητής να αποκτήσει ειδική πρόσβαση όπως το virusshare ή το hybrid-analysis. Ωστόσο λόγο της ειδικής πρόσβασης που απαιτείται επιλέχθηκαν άλλες ανοιχτές πηγές με εκτελέσιμα δυαδικά αρχεία ransomware από το GitHub όπως το theZoo, malware-samples, malware-sample-library, ransomware-Samples. Αυτό κατέστησε δυνατό να αποκτηθεί ένα ευρύ φάσμα από ransomware, από την αρχή έως και το 2023. Για την αποφυγή σπατάλης πόρων και χρόνου στη δοκιμή ανενεργών ransomware, και ransomware που δεν λειτουργούσαν, πραγματοποιήθηκε μια προκαταρκτική ανάλυση στα ransomware πριν από την πραγματική δοκιμή με τη μέθοδο ανίχνευσης. Σε αυτό το στάδιο

με την χρήση ενός Script κεντρικού ελέγχου αντίστοιχο ενός πραγματικού test ακολουθούνταν η εξής διαδικασία:

1. Εκκίνηση Windows Sandbox
2. Λήψη όλων των απαραίτητων αρχείων συμπεριλαμβανομένου του ransomware, των Script που δημιουργούν τυχαία αρχεία σε συγκεκριμένα σημεία του δίσκου, τον έλεγχο ύπαρξης αυτών μετά την εκτέλεση του ransomware, του κεντρικού Script ελέγχου.
3. Εκτέλεση του κεντρικού Script το οποίο υλοποιεί με την ακόλουθη σειρά i)του Script που δημιουργεί τυχαία αρχεία (όνομα,τύπος, μέγεθος) σε συγκεκριμένα σημεία του δίσκου ii)την εκτέλεση του ransomware iv) την εκτέλεση του Script ελέγχου των αρχείων που δημιουργήθηκαν
4. Αναμονή 5 λεπτών για την εκτέλεση του Script ελέγχου των αρχείων που δημιουργήθηκαν για την καταγραφή των κρυπτογραφημένων αρχείων και τον έλεγχο λειτουργίας του ransomware.

Η αναμονή επιλέχθηκε να είναι 5 λεπτά καθώς ένα ransomware ξεκινάει αμέσως την καταστροφική του δράση. Επομένως, αν σε αυτό το διάστημα δεν παρατηρηθούν αλλαγές αυτό μπορεί να οφείλεται στο ότι είτε το ransomware έχει κάποια αδρανή περίοδο, είτε παρουσιάζει αδυναμία εκτέλεσης που μπορεί να είναι αποτέλεσμα αλλοιωμένου εκτελέσιμου αρχείου ή γενικά πρόκειται για ανενεργό ransomware. Και στις δύο περιπτώσεις, δεν θα ήταν κατάλληλο για περαιτέρω δοκιμές και επομένως επισημάνθηκε ως μη ενεργό. Ο αριθμός των ενεργών ransomware ανήλθε στα 23.

4.3.3 Test Computers

Το περιβάλλοντος δοκιμής που ήταν υπεύθυνο για τη δοκιμή του ransomware αποτελείται από ένα φυσικό υπολογιστή και ένα εικονικό. Τα χαρακτηριστικά του φυσικού υπολογιστή είναι:

- CPU: AMD Ryzen 5 2600
- RAM: 16GB 2600Hz CL 16-18-18,
- Storage: SSD Read Speed 560 MB/s Write Speed 510 MB/s Maximum 4KB Random Write 90000 IOPS
- OS Windows 10 Education

Ο φυσικός υπολογιστής με τα Windows 10 Education ήταν πλήρως ενημερωμένος και η λειτουργία αναστολής λειτουργίας απενεργοποιήθηκε, για να διασφαλιστεί

ότι το περιβάλλον δοκιμής δεν θα κλείσει κατά τη διάρκεια της δοκιμής. Ο φυσικός υπολογιστής έχει δύο λειτουργίες. Η πρώτη είναι η εκτέλεση των εικονικών υπολογιστών και, δεύτερον η παροχή όλων των απαραίτητων αρχείων που αναφέρθηκαν προηγουμένως.

Στον εικονικό υπολογιστή τα χαρακτηριστικά του περιορίζονταν σε:

- RAM: 4GB
- Storage: 50GB
- 1 κοινό φάκελο για την απόκτηση των απαραίτητων αρχείων από το φυσικό υπολογιστή.

Για να φαίνεται το εικονικό σύστημα δοκιμής σαν ένα πραγματικό σύστημα, εγκαταστάθηκε ένα σύνολο προγραμμάτων που παρουσιάζονται συχνά σε ένα υπολογιστή με λειτουργικό Windows. Παραδείγματα εγκατεστημένων λογισμικό ήταν, Google Chrome, Sublime, Spotify, VLC media player, Winrar και Java. Όταν είχαν εγκατασταθεί τα παραπάνω προγράμματα το σύστημα δοκιμής ήταν έτοιμο.

4.3.4 Honeytoken

Αρχικά η ιδέα ήταν να δημιουργούνται τυχαία αρχεία (όνομα,τύπος, μέγεθος) σε όλους τους υποφακέλους του εικονικού υπολογιστή, ωστόσο, αυτή η ιδέα δεν προχώρησε για δύο λόγους: της πολυπλοκότητας μιας τέτοιας προσέγγισης και την παράβλεψη ενός χαρακτηριστικού που θα έπρπε να έχουν τα honeytokens και κατά συνέπεια και τα κανονικά αρχεία, δηλαδή να μην αποτελούνται από αρχεία που θα είναι γεμάτα με μηδενικά. Για αυτό επιλέχθηκε να χρησιμοποιηθούν κανονικά αρχεία των πιο κοινών τύπων έγγραφα word, pdf, εικόνες κ.λπ., όπου το μέγεθος ξεκινάει από μερικά kilobytes και φτάνει αρκετά megabytes. Αυτά στην συνέχεια τοποθετούνταν στους υποφακέλους Desktop, Documents, Downloads, και Videos του χρήστη των Windows, φάκελοι που όπως αναφέρθηκε προηγουμένως αποτελούν σύνηθες στόχο των ransomware. Ο αριθμός των αρχείων που τοποθετούνταν σε κάθε φάκελο είναι 100. Τα honeytoken δημιουργήθηκαν με τον ίδιο ακριβώς τρόπο και τοποθετήθηκαν στους ίδιους υποφακέλους. Ο αριθμός των honeytoken σε κάθε υποφάκελο είναι 10. Προφανώς με την χρήση των honeyfiles όσο μεγαλύτερος είναι αριθμός τους τόσο πιο πιθανό είναι να εντοπιστεί το ransomware και τα αποτελέσματα είναι γρηγορότερα. Γενικά τα honeyfiles δεν μπορούν να είναι πολλά καθώς δεσμεύουν χώρο στον δίσκο, ειδικά στην

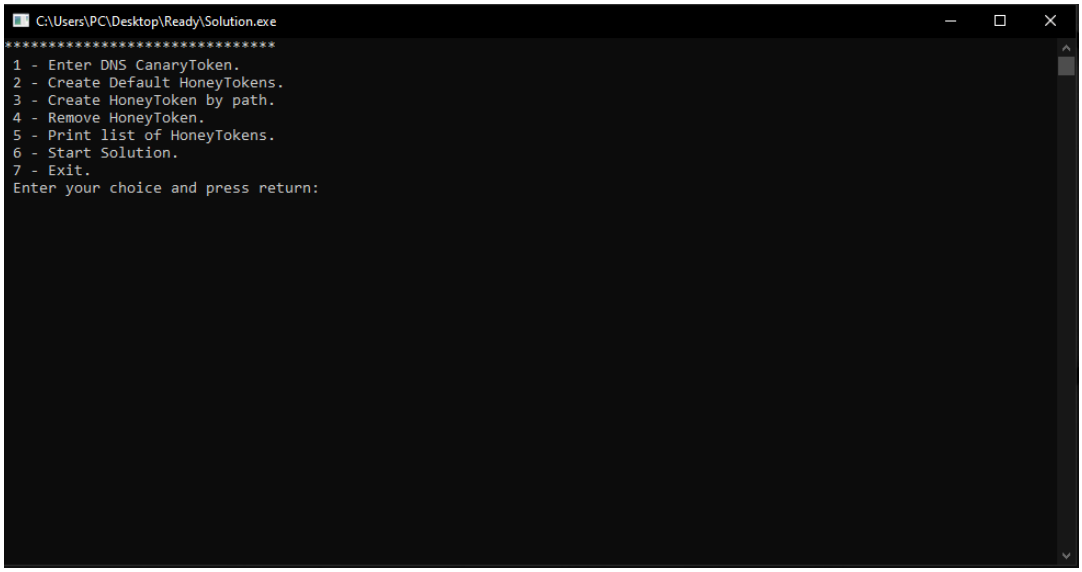

FIGURE 4.5: Μενού Επιλογών

περίπτωση μας όπου πρέπει να είναι μεγαλύτερα από 15MB. Τα ονόματα στα honeyfile δόθηκαν έτσι ώστε να βρίσκονται κατανεμημένα σε όλη την αγγλική αλφάβητο οπότε ανεξάρτητα από την σειρά κρυπτογράφησης να υπάρχει πιθανότητα να κρυπτογραφηθούν απο τα πρώτα.

4.3.5 Τυπική περίπτωση χρήσης του σχεδιασθέντος εργαλείου

Το εργαλείο που σχεδιάστηκε ελέγχεται από ένα Command Line Interface όπου ο χρήστης μπορεί να εισάγει τι δικές του παραμέτρους, όπως φαίνεται στην εικόνα 4.5. Ο χρήστης προκειμένου να ειδοποιηθεί μέσω της υπηρεσίας CannaryToken, πρέπει να δημιουργήσει το δικό του DNS CannaryToken και να το εισάγει ως παράμετρο. Σε περίπτωση που δεν το εισάγει το εργαλείο συνεχίζει να λειτουργεί κανονικά, ωστόσο ο χρήστης δεν θα λάβει ειδοποίηση στο email του. Στην εικόνα 4.6 φαίνεται η λειτουργία "1 - Enter DNS CannaryToken" όπου γίνεται εισαγωγή του CannaryToken. Στην συνέχεια ο χρήστης μπορεί να δημιουργήσει τα HoneyToken αρχεία. Έχει δύο επιλογές, ή να δημιουργήσει σε ένα φάκελο του συστήματος μία ομάδα από 8 προκαθορισμένα αρχεία ή να τα δημιουργήσει έναένα δίνοντας το θέση τους στο δίσκο ακολουθούμενα από το όνομά τους. Η λειτουργίες "2 - Create Default HoneyTokens.", " 3 - Create HoneyToken by path." που περιγράφησαν φαίνονται στην εικόνα 4.7. Και στις δύο περιπτώσεις ζητείται από τον χρήστη να δώσει το μέγεθος των αρχείων που θα δημιουργηθούν. Σε αυτό το σημείο ο χρήστης μπορεί να ενεργοποιήσει το εργαλείο για να ξεκινήσει την διαδικασία ανίχνευσης ransomware. Αφού έχει ξεκινήσει η διαδικασία

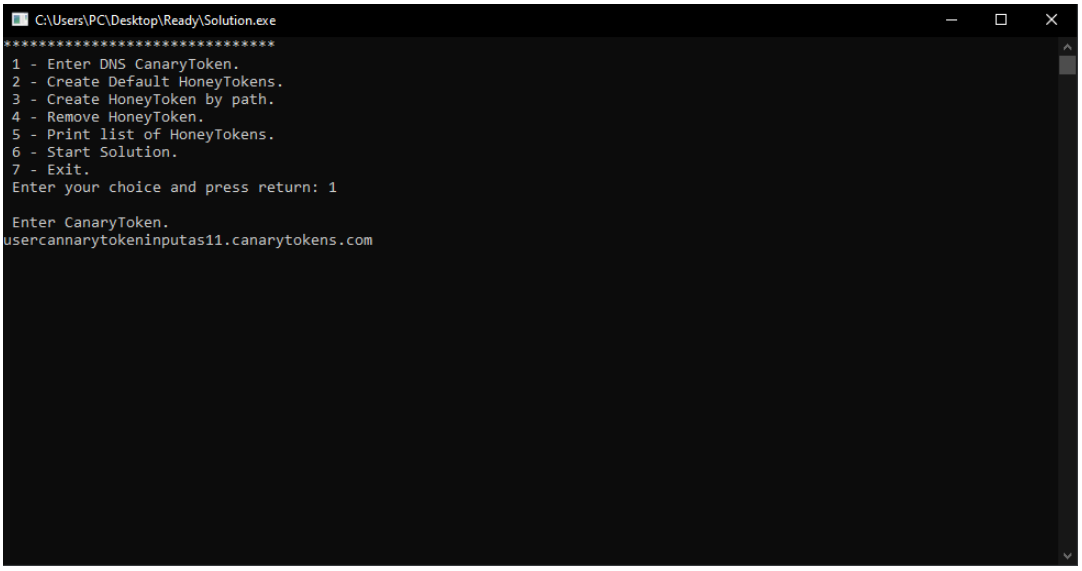

FIGURE 4.6: Εισαγωγή μοναδικού DNS CannaryToken

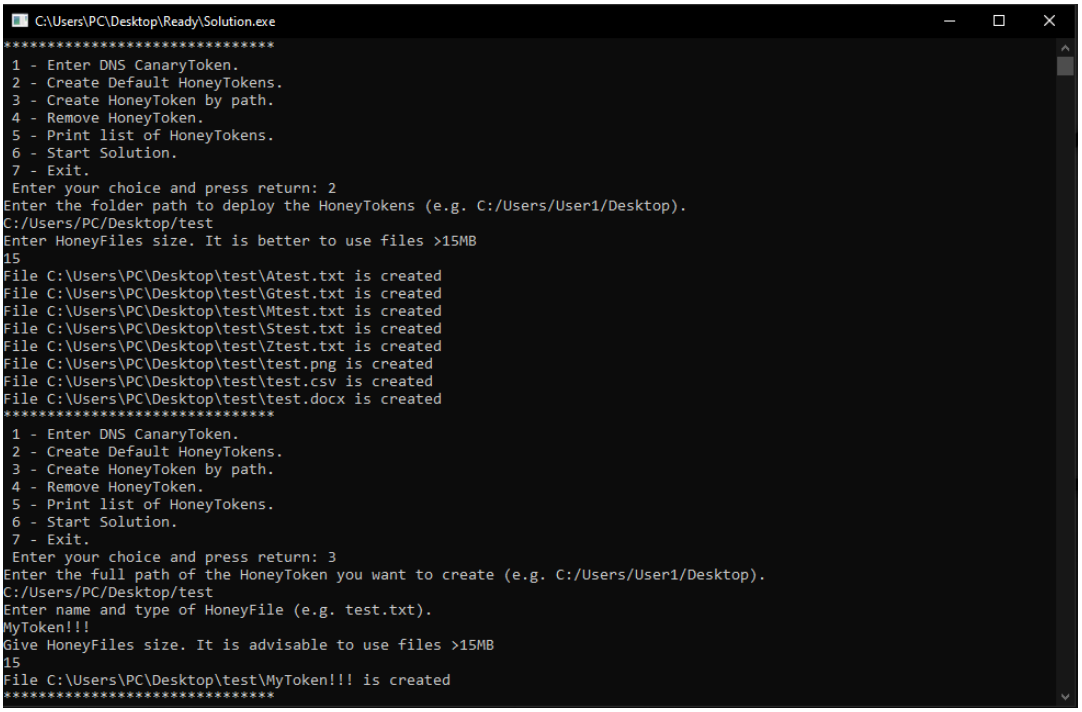

FIGURE 4.7: Δημιουργία HoneyTokens

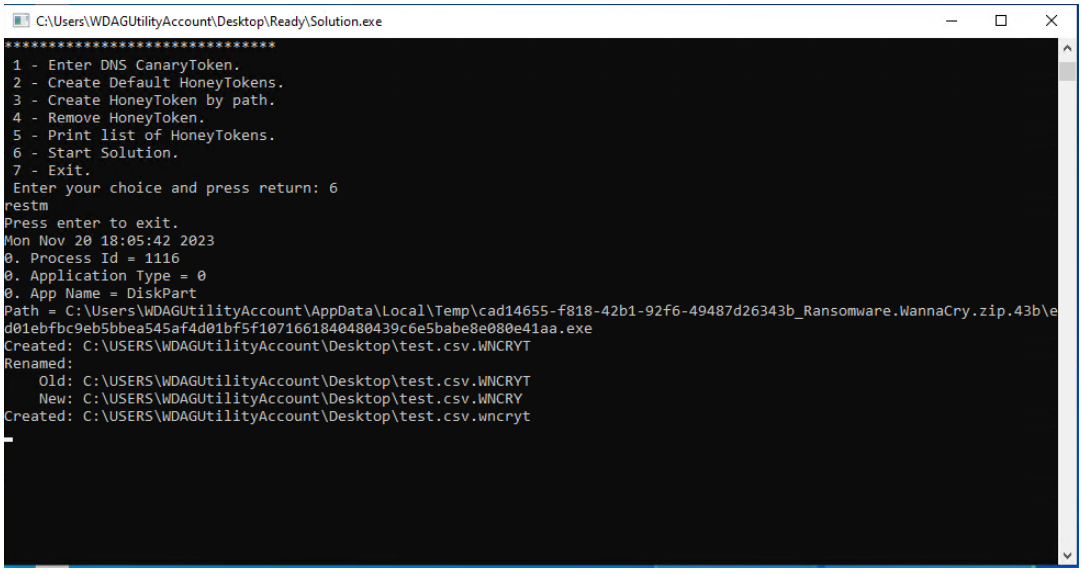

FIGURE 4.8: Στιγμιότυπο ανίχνευσης του Ransomware WannaCry

ανίχνευσης αυτή μπορεί να τερματιστεί οποιαδήποτε στιγμή πιέζοντας "Enter". Τέλος ο χρήστης μπορεί να δει το σύνολο των Honeytoken αρχείων στο σύστημα με την επιλογή "5 - Print list of HoneyTokens." αλλά και να διαγράψει όποιο από αυτά επιθυμεί, επιλογή "4 - Remove HoneyToken.".Στην εικόνα 4.8 φαίνεται μία επιτυχημένη ανίχνευση του γνωστού ransomware WannaCry.

Σε αυτό το σημείο πρέπει να αναφερθεί πως από τα 23 ενεργά ransomware που συγκεντρώθηκαν, τα 19 εντοπίστηκαν εγκαίρως με αποτέλεσμα το ransomware να μην προκαλέσει μεγάλη καταστροφή, 3 εντοπίστηκαν σε προχωρημένο στάδιο έχοντας κρυπτογραφήσει έως και 27% των συνολικών αρχείων και 1 εντοπίστηκε μετά τον πλήρη κύκλο δράσης του.

Chapter 5

Σύγκριση της προτεινόμενης μεθόδου με άλλες μεθόδους

Σε αυτό το κεφάλαιο, εξετάζονται οι προσεγγίσεις των τεσσάρων εργασιών που αναφέρθηκαν στο κεφάλαιο 3 και της πρότασης αυτής της εργασίας. Η σύγκριση θα βασίζεται σε βασικές κατηγορίες, συμπεριλαμβανομένης της Ακρίβειας Ανίχνευσης, των Ψευδών Θετικών, της Μεθοδολογίας, των Οικογενειών Ransomware που Δοκιμάστηκαν, και των Περιορισμών.

1. **Μέθοδολογία:** Κάθε μέθοδος περιγράφει την προσέγγισή της για την ανίχνευση ransomware. Αυτό μπορεί να περιλαμβάνει ψευδείς στόχους, παρακολούθηση διεργασιών, ελέγχους τύπου αρχείων κ.λπ.

2. **Οικογένειες Ransomware που Δοκιμάστηκαν:** Αναφέρονται οι συγκεκριμένες οικογένειες ransomware που χρησιμοποιήθηκαν για τις δοκιμές. Αυτό είναι σημαντικό για να κατανοήσουμε την εμβέλεια των αποτελεσμάτων.

3. **Ακρίβεια Ανίχνευσης:** Ποσοστό των δειγμάτων ransomware που ανιχνεύθηκαν σωστά από τη μέθοδο. Αυτό δίνει μια ιδέα της αποτελεσματικότητας της μεθόδου στον εντοπισμό κακόβουλου λογισμικού.

4. **Ψευδή Θετικά:** Το ποσοστό των ανιχνεύσεων που παρουσίασαν ψευδείς συναγερμούς, δηλαδή περιπτώσεις όπου η μέθοδος εντόπισε κάτι ως κακόβουλο αλλά στην πραγματικότητα δεν ήταν.

5. **Περιορισμοί και Μελλοντικές Βελτιώσεις:** Εδώ περιγράφονται τα προβλήματα και οι πιθανότητες βελτίωσης της μεθόδου. Αυτό μπορεί να περιλαμβάνει τη βελτίωση της ακρίβειας, τη μείωση των ψευδών θετικών ή την αντιμετώπιση περαιτέρω περιορισμών.

Έρευνα	**Μεθοδολογία**	**Οικογένειες Ransomware που Δοκιμάστηκαν**	**Ακρίβεια Ανίχνευσης**	**Ψευδή Θετικά**	**Περιορισμοί και μελλοντικές βελτιώσεις**
RWGuard	Ψεύτικοι στόχοι, παρακολούθηση διεργασιών, μάθηση κρυπτογράφησης χρήστη.	14 οικογένειες ransomware (Wannacry, Cerber, CryptoLocker, κ.λ.π.).	Δεν αναφέρεται ρητά αλλά περιγράφει ότι έχει μηδενικά ψευδή θετικά.	Ποσοστό ψευδών θετικών περίπου 0,1%, με ελάχιστο επιπρόσθετο κόστος απόδοσης περίπου 1,9%.	Βελτίωση χρονικής καθυστέρησης και αντιμετώπιση προσαρμοσμένης κρυπτογράφησης.
RLocker	Honeyfiles σε λειτουργικό Linux	2 δείγματα Ransomware και εργαλεία proof of concept.	100% καθώς εντοπίστηκαν όλα τα δείγματα.	Προκύπτουν Ψευδή θετικά που μπορούν να περιοριστούν με Blacklists.	Βελτίωση ψευδών θετικών και δυνατότητα εφαρμογή σε λειτουργικά Windows και Android.
CryptDrop	Έλεγχος τύπου αρχείου, κατακερματισμού ομοιότητας, και εντροπία Shannon	492 δείγματα ransomware από 14 διαφορετικές οικογένειες	100% ανίχνευση 0,2% απώλεια αρχείων.	Αδυναμία ελέγχου ψευδών θετικών.	Βελτιστοποίηση των ψευδών θετικών καθώς και πιο αποδοτικού τρόπου παρακολούθησης.
MFSA	Πρόταση παρακολούθησης SSDT για ύποπτα αιτήματα I/O.	1.389 δείγματα ransomware από 15 διαφορετικές οικογένειες	-	-	-
Εργασία	Honeypots σε λειτουργικό Windows	23 δείγματα από 8 οικογένειες	82% έγκυρη ανίχνευση.	Δεν γίνεται έλεγχος	Αποδοτικότερη παρακολούθηση, λίστα με μη κακόβουλες διεργασίες.

Table 5.1: Πίνακας σύγκρισης

Αυτή η συγκριτική ανάλυση παρέχει μια σφαιρική εικόνα των διαφορετικών προσεγγίσεων για την ανίχνευση ransomware που παρουσιάζονται στα επιλεγμένα έγγραφα. Η κατανόηση των δυνατοτήτων, των αδυναμιών και των λεπτομερειών κάθε μεθόδου είναι απαραίτητη για την καθοδήγηση μελλοντικής έρευνας και τη δημιουργία πιο αξιόπιστων και προσαρμοστικών συστημάτων ανίχνευσης ransomware.

Chapter 6

Συμπεράσματα και Επόμενα Βήματα

Με αυτήν την πτυχιακή εργασία έγινε προσπάθεια να αναδειχθεί ο όλο και αυξανόμενος κίνδυνος των κυβερνοεπιθέσεων καθώς και την ανάγκη αντιμετώπισής τους. Πολλές από αυτές τις απειλές γίνονται περισσότερο εξειδικευμένες και είναι δύσκολο να αντιμετωπιστούν. Μια από αυτές είναι και το ransomware. Αν και το ζήτημα των ransomware έχει αναλυθεί σε πολλές δημοσιεύσεις και πτυχιακές, παρόλα αυτά έγινε προσπάθεια επιπλέον συνδρομής, παρουσιάζοντας μια ακόμα λύση για ανίχνευση τους. Η προσπάθεια αυτή οδήγησε στην υλοποίηση ενός προγράμματος το οποίο όχι μόνο θα μπορεί να ανιχνεύει την ύπαρξη ransomware αλλά θα δίνει και την δυνατότητα να εντοπίζει πιο process είναι υπεύθυνο για την κρυπτογράφηση και κατα συνέπεια το ίδιο το ransomware και την θέση του στο δίσκο. Βέβαια μετά από αρκετούς πειραματισμούς για την βελτιστοποίηση και την αύξηση της αποδοτικότητας του προγράμματος έπρεπε να δοθούν λύσεις, να γίνουν ορισμένοι συμβιβασμοί και περιορισμοί στην χρήση του προγράμματος. Με την αρχική προσέγγιση, κάνοντας χρήση του Restart Manager API, δεν κατέστη δυνατή η παρακολούθηση ένος HoenyFile αν αυτό μετονομάζονταν ή το μέγεθος του ήταν μικρότερο από 10MB. Η λύση που δόθηκε ήταν η παρακολούθηση για τυχόν μετονομασίες με την χρήση της κλάσης FileSystemWatcher. Κάνοντας χρήση της FSW προέκυψαν δύο επιπλέον περιορισμοί καθώς η κλάση δεν δίνει την δυνατότητα να παρακολουθούνται πολλοί δίσκοι ταυτόχρονα αλλά μόνο subdirectories και έπρεπε να επιλεχθεί αν θα παρακολουθούνται μόνο συγκεκριμένοι τύποι αρχείων ή αρχεία με συγκεκριμένο όνομα. Έτσι έγινε συμβιβασμός με το να παρακολουθείται το subdirectory C:/Users/... το οποίο στοχεύεται από τα περισσότερα ransomware και τα ονόματα των HoneyFiles να περιέχουν μια κοινή συμβολοσειρά. Όλα αυτά είχαν ως αποτέλεσμα την δημιουργία HoneyFiles με διαφορετικα χαρακτηριστικά. Το RM API και η κλάση FSW μπορούν να δουλεύουν συνεργατικά παρακολουθώντας κοινά HoneyFiles προσφέροντας την μέγιστη δυνατή

κάλυψη αλλά και αυτόνομα. Τέλος, στην προσπάθειά να βελτιστοποιηθούν τα HoneyFiles έτσι ώστε να μην μπορούν να γίνουν αντιληπτά από τα ransomware ορίσαμε μερικούς γενικούς κανόνες οι οποίοι είναι:

- Να αποτελούνται από αρχεία διαφορετικών μεγεθών και να υπάρχει ένα HoneyFile με το μεγαλύτερο και το μικρότερο μέγεθος σε ένα φάκελο
- Να αποτελούνται από αρχεία διαφορετικών τύπων
- Το όνομα να μην προδίδει την ιδιότητα τους και να υπάρχουν HoneyFiles όπου το όνομα τους θα ξεκινάει με το πρώτο και το τελευταίο χαρακτήρα σε σειρά Windows-1252
- Να μην είναι dummy files που περιέχουν μηδενικά ή το περιεχόμενο τους είναι κρυπτογραφημένο
- Να υπάρχει μηχανισμός που θα προσομοιώνει την περιοδική τους χρήση

Η τελευταία πρόταση για τον μηχανισμό που θα προσομοιώνει την χρήση των HoneyFiles από τον χρήστη δεν έχει υλοποιηθεί και μπορεί να αποτελέσει αντικείμενο για περαιτέρω μελέτη. Ακόμα με βάση την δυνατότητα που μας δίνει το RM API να παρακολουθεί όχι μόνο αρχεία αλλά και διαδικασίες, θα ήταν αρκετά ενδιαφέρον να παρακολουθούμε διαδικασίες που συχνά τερματίζονται από ransomware, λύση η οποία εν μέρη προτάθηκε με το εργαλείο Killed Process Canary [105].

Βιβλιογραφικές Αναφορές

[1] A. Mallik et al. "Understanding Man-in-the-middle-attack through Survey of Literature". In: *Indonesian Journal of Computing, Engineering and Design (IJoCED)* 1.1 (2019), pp. 44–56. ISSN: 2656-8179. DOI: 10.35806/ijoced.v1i1.36.

[2] Toby Ehrenkranz and Jun Li. "On the State of IP Spoofing Defense". In: *ACM Trans. Internet Technol.* 9.2 (May 2009). ISSN: 1533-5399. DOI: 10.1145/1516539.1516541.

[3] P. Babu, Lalitha Bhaskari, and CH.Satyanarayana. "A Comprehensive Analysis of Spoofing". In: *International Journal of Advanced Computer Sciences and Applications* (Jan. 2011). DOI: 10.14569/IJACSA.2010.010623.

[4] Dutta Sai Eswari et al. "A survey on detection of DDoS attacks using machine learning approaches". In: *Turkish Journal of Computer and Mathematics Education (TURCOMAT)* 12.11 (2021), pp. 4923–4931. URL: https://www.turcomat.org/index.php/turkbilmat/article/view/6671.

[5] Akshat Gaurav. "A Comprehensive Survey on DDoS Attacks on various Intelligent Systems and It's Defense Techniques". In: (May 2022). DOI: 10.13140/RG.2.2.16769.12644.

[6] Ashina Sadiq et al. "A review of phishing attacks and countermeasures for internet of things-based smart business applications in industry 4.0". In: *Human Behavior and Emerging Technologies* 3 (Oct. 2021). DOI: 10.1002/hbe2.301.

[7] John Aycock. *Computer Viruses and Malware*. Springer, 2006.

[8] Vala Khushali. "A Review on Fileless Malware Analysis Techniques". In: *International Journal of Engineering Research and* V9 (May 2020). DOI: 10.17577/IJERTV9IS050068.

[9] Khlood Shinan et al. "Machine Learning-Based Botnet Detection in Software-Defined Network: A Systematic Review". In: *Symmetry* 13.5 (2021). ISSN: 2073-8994. DOI: 10.3390/sym13050866.

[10] "Tools and Techniques for Malware Detection and Analysis". In: *CoRR* abs/2002.06819 (2020). Withdrawn. arXiv: 2002.06819. URL: https://arxiv.org/abs/2002.06819.

[11] Ege Tekiner et al. "SoK: Cryptojacking Malware". In: (2021), pp. 120–139. DOI: 10.1109/EuroSP51992.2021.00019.

[12] S. Davidoff and an O'Reilly Media Company Safari. *Data Breaches: Crisis and Opportunity*. Addison-Wesley Professional, 2019. ISBN: 9780134507750.

[13] A. L. Young and M. Yung. "Cryptovirology: The Birth, Neglect, and Explosion of Ransomware". In: *International Journal of Information Technology and Computer Science(IJITCS)* V60 (July 2017), pp. 24–26. DOI: DOI:10.5815/ijitcs.2018.01.05.

[14] Fabrizio Cicala and Elisa Bertino. "Analysis of Encryption Key Generation in Modern Crypto Ransomware". In: *IEEE Transactions on Dependable and Secure Computing* 19.2 (2022), pp. 1239–1253. DOI: 10.1109/TDSC.2020.3005976.

[15] Amin Kharraz et al. "Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks". In: *Detection of Intrusions and Malware, and Vulnerability Assessment*. Ed. by Magnus Almgren, Vincenzo Gulisano, and Federico Maggi. Cham: Springer International Publishing, 2015, pp. 3–24. DOI: https://doi.org/10.1007/978-3-319-20550-2_1.

[16] Adam Young and Moti Yung. *Malicious Cryptography: Exposing Cryptovirology*. Hoboken, NJ, USA: John Wiley & Sons, Inc., 2004. ISBN: 0764549758.

[17] David Emm. "Cracking the code: The history of Gpcode". In: *Computer Fraud and Security* 2008.9 (2008), pp. 15–17. ISSN: 1361-3723. DOI: https://doi.org/10.1016/S1361-3723(08)70139-8.

[18] Samuel Greengard. "The Worsening State of Ransomware". In: *Commun. ACM* 64.4 (Mar. 2021), pp. 15–17. ISSN: 0001-0782. DOI: 10.1145/3449054.

[19] Miss. Harshada Salvi and Mr. Ravindra Kerkar. "Ransomware: A Cyber Extortion". In: *Asian Journal For Convergence In Technology (AJCT) ISSN -2350-1146* 2.2 (Dec. 2017). URL: https://asianssr.org/index.php/ajct/article/view/55.

[20] Danny Yuxing Huang et al. "Tracking Ransomware End-to-end". In: *2018 IEEE Symposium on Security and Privacy (SP)*. 2018, pp. 618–631. DOI: 10.1109/SP.2018.00047.

[21] Amir Atapour-Abarghouei, Stephen Bonner, and Andrew Stephen McGough. "Volenti non fit injuria: Ransomware and its Victims". In: *2019 IEEE International Conference on Big Data (Big Data)*. 2019, pp. 4701–4707. DOI: 10.1109/BigData47090.2019.9006298.

[22] Fei Tang et al. "RansomSpector: An introspection-based approach to detect crypto ransomware". In: *Computers And Security* 97 (2020), p. 101997. ISSN: 0167-4048. DOI: https://doi.org/10.1016/j.cose.2020.101997.

[23] Da-Yu KAO, Shou-Ching HSIAO, and Raylin TSO. "Analyzing WannaCry Ransomware Considering the Weapons and Exploits". In: *2019 21st International Conference on Advanced Communication Technology (ICACT)*. 2019, pp. 1098–1107. DOI: 10.23919/ICACT.2019.8702049.

[24] Saeid Salehi et al. "A Novel Approach for Detecting DGA-based Ransomwares". In: *2018 15th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC)*. 2018, pp. 1–7. DOI: 10.1109/ISCISC.2018.8546941.

[25] Shina Sheen and Ashwitha Yadav. "Ransomware detection by mining API call usage". In: *2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*. 2018, pp. 983–987. DOI: 10.1109/ICACCI.2018.8554938.

[26] Gavin Hull, Henna John, and Budi Arief. "Ransomware deployment methods and analysis: views from a predictive model and human responses". In: *Crime Science* 8 (Feb. 2019). DOI: 10.1186/s40163-019-0097-9.

[27] Amirhossein Gharib and Ali Ghorbani. "DNA-Droid: A Real-Time Android Ransomware Detection Framework". In: July 2017, pp. 184–198. ISBN: 978-3-319-64700-5. DOI: 10.1007/978-3-319-64701-2_14.

[28] Shagufta Mehnaz, Anand Mudgerikar, and Elisa Bertino. "RWGuard: A Real-Time Detection System Against Cryptographic Ransomware". In: *Research in Attacks, Intrusions, and Defenses*. Ed. by Michael Bailey et al. Cham: Springer International Publishing, 2018, pp. 114–136. ISBN: 978-3-030-00470-5.

[29] J.A. Gómez-Hernández, L. Álvarez-González, and P. García-Teodoro. "R-Locker: Thwarting ransomware action through a honeyfile-based approach". In: *Computers And Security* 73 (2018), pp. 389–398. ISSN: 0167-4048. DOI: https://doi.org/10.1016/j.cose.2017.11.019.

[30] Nolen Scaife et al. "CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data". In: *2016 IEEE 36th International Conference*

on Distributed Computing Systems (ICDCS). 2016, pp. 303–312. DOI: 10.1109/ICDCS.2016.46.

[31] Jesse Kornblum. "Identifying almost identical files using context triggered piecewise hashing". In: *Digital Investigation* 3 (2006). The Proceedings of the 6th Annual Digital Forensic Research Workshop (DFRWS '06), pp. 91–97. ISSN: 1742-2876. DOI: https://doi.org/10.1016/j.diin.2006.06.015.

[32] Niels Provos and Thorsten Holz. *Virtual Honeypots - From Botnet Tracking to Intrusion Detection*. Jan. 2008. ISBN: 978-0-321-33632-3.

[33] Iyatiti Mokube and Michele Adams. "Honeypots: concepts, approaches, and challenges". In: Mar. 2007, pp. 321–326. DOI: 10.1145/1233341.1233399.

[34] Christian Seifert, Ian Welch, and Peter Komisarczuk. "HoneyC - The low-interaction client honeypot". In: 2006. URL: https://api.semanticscholar.org/CorpusID:14418203.

[35] Niels Provos. "A Virtual Honeypot Framework". In: *13th USENIX Security Symposium (USENIX Security 04)*. San Diego, CA: USENIX Association, 2004. URL: https://www.researchgate.net/publication/221260586_A_Virtual_Honeypot_Framework.

[36] Michael Armbrust et al. "A View of Cloud Computing". In: *Commun. ACM* 53.4 (Apr. 2010), pp. 50–58. ISSN: 0001-0782. DOI: 10.1145/1721654.1721672.

[37] Jeonghwan Lee, Jinwoo Lee, and Jiman Hong. "How to Make Efficient Decoy Files for Ransomware Detection?" In: *Proceedings of the International Conference on Research in Adaptive and Convergent Systems*. RACS '17. Krakow, Poland: Association for Computing Machinery, 2017, pp. 208–212. ISBN: 9781450350273. DOI: 10.1145/3129676.3129713.

[38] Yassine Lemmou, Jean-Louis Lanet, and El Mamoun Souidi. "A behavioural in-depth analysis of ransomware infection". In: *IET Information Security* 15.1 (2021), pp. 38–58. DOI: https://doi.org/10.1049/ise2.12004. eprint: https://ietresearch.onlinelibrary.wiley.com/doi/pdf/10.1049/ise2.12004.

Εξωτερικοί Σύνδεσμοι

[39] *Cyber attack on ICRC: What we know*. 2022. URL: https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know.

[40] *Attacks on US Power Grids Rose to All-Time High in 2022*. 2023. URL: https://www.bloomberg.com/news/articles/2023-02-01/attacks-on-us-power-grids-rise-to-all-%20time-high-in-2022#xj4y7vzkg.

[41] *Israel-Iran Cyber War, Gas Station Attack*. 2023. URL: https://iranprimer.usip.org/blog/2021/nov/02/israel-iran-cyber-war-gas-station-attack.

[42] *Hiscox Cyber Readiness Report 2019*. 2019. URL: https://www.hiscox.com/documents/2019-Hiscox-Cyber-Readiness-Report.pdf.

[43] *Statista: Cybersecurity - Worldwide*. URL: https://www.statista.com/outlook/tmo/cybersecurity/worldwide#revenue.

[44] *Lenovo Superfish Adware Vulnerable to HTTPS Spoofing*. 2016. URL: https://www.cisa.gov/news-events/alerts/2015/02/20/lenovo-superfish-adware-vulnerable-%20https-spoofing.

[45] *Operation Black Tulip: Certificate authorities lose authority*. URL: https://www.enisa.europa.eu/media/news-items/operation-black-tulip/.

[46] *AWS mitigated a record-breaking 2.3 Tbps DDoS attack in February*. URL: https://siliconangle.com/2020/06/17/aws-mitigated-record-breaking-2-3-tbps-ddos-attack-%20february/.

[47] *February 28th DDoS Incident Report*. URL: https://github.blog/2018-03-01-ddos-incident-report/.

[48] *Operation Phish Phry*. URL: https://archives.fbi.gov/archives/news/stories/2009/october/phishphry_100709.

[49] *Nordea Bank loses 1.14 million to online fraud*. URL: https://itwire.com/business-it-news/security/nordea-bank-loses-114-million-to-online-%20fraud-update.html.

[50] *What is SQL Injection And How to Prevent SQL Injection*. URL: https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-sql-injection.

[51] *Tesla Pays 10K for Microsoft SQL Server Reporting Services Bug*. URL: https://www.bleepingcomputer.com/news/security/tesla-pays-10k-for-microsoft-sql-server-%20reporting-services-bug/.

[52] *Cisco Prime License Manager SQL Injection Vulnerability*. URL: https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-20181128-plm-sql-inject.html.

[53] *ILOVEYOU - Wikipedia*. URL: https://en.wikipedia.org/wiki/ILOVEYOU.

[54] *Morris worm - Wikipedia*. URL: https://en.wikipedia.org/wiki/Morris_worm.

[55] *Zeus Malware - Wikipedia*. URL: https://en.wikipedia.org/wiki/Zeus_(malware).

[56] *Operation Cobalt Kitty: A large-scale APT in Asia carried out by the OceanLotus Group*. URL: https://www.cybereason.com/blog/operation-cobalt-kitty-apt.

[57] *Hack Brief: Dangerous 'Fireball' Adware Infects a Quarter Billion PCs*. URL: https://www.wired.com/2017/06/hack-brief-dangerous-fireball-adware-infects-quarter-%20billion-pcs/.

[58] *Pegasus - Wikipedia*. URL: https://en.wikipedia.org/wiki/Pegasus_(spyware).

[59] *FinSpy - Wikipedia*. URL: https://en.wikipedia.org/wiki/FinFisher.

[60] *Storm botnet - Wikipedia*. URL: https://en.wikipedia.org/wiki/Storm_botnet.

[61] *Mirai Malware - Wikipedia*. URL: https://en.wikipedia.org/wiki/Mirai_(malware).

[62] *The Necurs Botnet: A Pandora's Box of Malicious Spam*. 2017. URL: https://securityintelligence.com/the-necurs-botnet-a-pandoras-box-of-malicious-spam/.

[63] *Cryptojacking*. URL: https://www.aquasec.com/cloud-native-academy/cloud-attacks/cryptojacking/.

[64] *ENISA Threat Landscape 2022*. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022.

[65] *Colonial Pipeline hack explained: Everything you need to know*. URL: https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know.

[66] *ENISA Threat Landscape Report 2017*. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017.

[67] *ENISA Threat Landscape Report 2018*. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018.

[68] *ENISA Threat Landscape 2020 - Ransomware*. URL: https://www.enisa.europa.eu/publications/ransomware.

[69] *ENISA Threat Landscape 2021*. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021.

[70] *ENISA Threat Landscape 2020 - Main Incidents*. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-main-incidents.

[71] *Modern Ransomware's Double Extortion Tactics and How to Protect Enterprises Against Them*. URL: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/modern-ransomwares-double-extortion-tactics-and-how-to-protect-enterprises-against-them.

[72] *2014: The Year Extortion Went Mainstream*. 2014. URL: https://krebsonsecurity.com/2014/06/2014-the-year-extortion-went-mainstream/.

[73] *The Current State of Ransomware*. 2015. URL: https://www.sophos.com/en-us/medialibrary/PDFs/technical%20papers/sophos-current-state-of-%20ransomware.pdf.

[74] *Ransomware as a Service (RaaS) Explained How It Works And Examples*. 2023. URL: https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/.

[75] *Ransomware as a Service*. URL: https://documents.trendmicro.com/assets/resources/ransomware-as-a-service.pdf.

[76] *This new ransomware nightmare demands a big payday to decrypt your files*. 2017. URL: https://www.zdnet.com/article/this-new-ransomware-nightmare-demands-a-big-payday-to-%20decrypt-your-files/.

[77] *Hackers are now offering 'customer support' to the victims they extort money from*. 2016. URL: https://www.businessinsider.com/ransomware-writers-offer-customer-support-to-victims-%202016-1.

[78] *Ransomware Gives Free Decryption Keys to Victims Who Infect Others*. 2016. URL: https://threatpost.com/ransomware-gives-free-decryption-keys-to-victims-who-infect-others%20/122395/.

[79] *Ransomware's Dangerous New Trick Is Double-Encrypting Your Data*. 2021. URL: https://www.wired.com/story/ransomware-double-encryption/.

[80] *Ransomware Double Extortion and Beyond: REvil, Clop, and Conti*. 2021. URL: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats%20/ransomware-double-extortion-and-beyond-revil-clop-and-conti.

[81] *Cyber Resilient Organization Study 2021*. 2021. URL: https://www.ibm.com/resources/guides/cyber-resilient-organization-study/.

[82] *Ransomware Payments Fall as Fewer Companies Pay Data Exfiltration Extortion Demands*. 2021. URL: https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020.

[83] *The Evolution of Ransomware: A 5-Year Perspective*. 2023. URL: https://www.cyber.nj.gov/informational-report/the-evolution-of-ransomware-a-5-year-%20perspective.

[84] *The Evolution of Ransomware*. 2023. URL: https://its.fsu.edu/sites/g/files/imported/storage/images/information-security-and-%20privacy-office/the-evolution-of-ransomware.pdf.

[85] *Ransomware 'Crisis' in US Schools: More Than 1,000 Hit So Far in 2019*. 2019. URL: https://www.darkreading.com/threat-intelligence/ransomware-crisis-in-us-schools-more-%20than-1-000-hit-so-far-in-2019.

[86] *Internet Security Threat Report ISTR Ransomware 2017*. 2017. URL: https://docs.broadcom.com/doc/istr-ransomware-2017-en.

[87] *Global market share held by operating systems for desktop PCs, from January 2013 to July 2023*. URL: https://www.statista.com/statistics/218089/global-market-share-of-windows-7/.

[88] *iPhone users fooled by fake ransomware*. 2017. URL: https://www.bbc.com/news/technology-39432350.

[89] *The Rise of Android Ransomware*. 2016. URL: https://web-assets.esetstatic.com/wls/2016/02/rise_of_android_ransomware.pdf.

[90] *Attackers Prefer Ransomware to Stealing Data*. 2020. URL: https://www.darkreading.com/threat-intelligence/attackers-prefer-ransomware-to-stealing-%20data.

[91] *What makes IoT ransomware a different and more dangerous threat?* 2016. URL: https://techcrunch.com/2016/10/02/what-makes-iot-ransomware-a-different-and-more-%20dangerous-threat/?guccounter=1.

[92] *ThreatList: Top 5 Most Dangerous Attachment Types*. 2019. URL: https://threatpost.com/threatlist-top-5-most-dangerous-attachment-types/144635/.

[93] *Renew Your Ransomware Defense with CISA's Updated Guidance*. 2017. URL: https://www.cisecurity.org/insights/blog/renew-your-ransomware-defense-with-cisas-updated-%20guidance.

[94] *WOOF locker: Unmasking the browser locker behind a stealthy tech support scam operation*. 2020. URL: https://www.malwarebytes.com/blog/news/2020/01/woof-locker-stealthy-browser-locker-tech-%20support-scam.

[95] *Ransomware: How an attack works*. 2023. URL: https://support.sophos.com/support/s/article/KB-000036277?language=en_US.

[96] *An Overview of Symmetric Encryption and the Key Lifecycle*. 2020. URL: https://www.cryptomathic.com/news-events/blog/an-overview-of-symmetric-encryption-and-the-%20key-lifecycle.

[97] *Cryptolocker ransomware: what you need to know*. 2013. URL: https://www.malwarebytes.com/blog/news/2013/10/cryptolocker-ransomware-what-you-need-to-%20know.

[98] *Emerging Threat on RANSOM-LOCKY*. 2019. URL: https://success.trendmicro.com/dcx/s/solution/1113859-emerging-threat-on-ransom-%20locky?language=en_US.

[99] *Reveton ransomware distributor sentenced to six years in prison in the UK*. 2019. URL: https://www.zdnet.com/article/reveton-ransomware-distributor-sentenced-to-six-years-in-%20prison-in-the-uk/.

[100] *New Seftad Ransomware Attacks Master Boot Record*. 2010. URL: https://threatpost.com/new-seftad-ransomware-attacks-master-boot-record-113010/74714/.

[101] *Ransomware Gangs Don't Need PR Help*. 2020. URL: https://krebsonsecurity.com/2020/07/ransomware-gangs-dont-need-pr-help/.

[102] *New Crypto-Ransomware JIGSAW Plays Nasty Games*. 2016. URL: https://idsirtii.or.id/securitynews/baca/504/new-crypto-ransomware-jigsaw-plays-nasty-%20games.html.

[103] *A Different View: Understand and Prevent Encrypting Ransomware*. 2015. URL: https://www.paloaltonetworks.com/blog/2015/01/different-view-understand-prevent-encrypting-ransomware/.

[104] *About Restart Manager*. URL: https://learn.microsoft.com/en-us/windows/win32/rstmgr/about-restart-manager.

[105] *Deception Engineering: exploring the use of Windows Service Canaries against ransomware*. 2021. URL: https://research.nccgroup.com/2021/03/04/deception-engineering-exploring-the-use-of-%20windows-service-canaries-against-ransomware/.

[106] *Canarytokens Guide*. URL: https://docs.canarytokens.org/guide/.

[107] *FileSystemWatcher Class*. URL: https://learn.microsoft.com/en-us/dotnet/api/system.io.filesystemwatcher?view=net-7.0.