Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και
Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή
Στην Ασφάλεια
Υπολογιστών και Δικτύων

Ransomware Protection

Θεόδωρος Χαρμπίλας

Επιβλέπων Καθηγητής
Σταύρος Σιαηλής

Μάιος 2022

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και
Εφαρμοσμένων Επιστημών

Ransomware Protection

Θεόδωρος Χαρμπίλας

Επιβλέπων Καθηγητής
Σταύρος Σιαηλής

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε
προς μερική εκπλήρωση των απαιτήσεων για απόκτηση

μεταπτυχιακού τίτλου σπουδών
στην Ασφάλεια Υπολογιστών και Δικτύων

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου

Μάιος 2022

ΛΕΥΚΗ ΣΕΛΙΔΑ

Περίληψη

Το ransomware είναι από τις πιο σημαντικές μορφές κακόβουλου λογισμικού τις τελευταίες δεκαετίες. Οι επιτιθέμενοι έχουν οργανώσει ένα καλά οργανωμένο δίκτυο εγκατάστασης κακόβουλων αρχείων ransomware ικανό να μολύνει εκατοντάδες χιλιάδες υπολογιστές σε λίγα λεπτά και με σκοπό το κέρδος. Τα τελευταία δεκαπέντε χρόνια οι στόχοι τους ως προς το προφίλ χρηστών έχει μεταβληθεί, όπως επίσης και το προφίλ των συστημάτων, και οι τρόποι μόλυνσης δικτύων και συστημάτων. Η δημιουργία ενός νέου επιχειρηματικού μοντέλου Ransomware-as-a-Service είναι σε άνοδο με σκοπό την αυτοματοποιημένη εγκατάσταση του κακόβουλου προγράμματος σε συγκεκριμένους στόχους.

Η παρούσα έρευνα καλείται να μελετήσει διεξοδικά τις οικογένειες επιθέσεων ransomware, κοινά χαρακτηριστικά και παραλλαγές στο μοντέλο επίθεσης, μέθοδοι ανάκαμψης, ανίχνευσης και αποτροπής. Ειδικά στη περίπτωση της ανίχνευσης καταγράφουμε τεχνικές που χρησιμοποιούν μηχανική μάθηση, ή τεχνητή νοημοσύνη ως πολλά υποσχόμενες τεχνικές για την εξάλειψη του προβλήματος στο μέλλον ή τεχνικές ανίχνευσης που είναι καλύτερα προετοιμασμένες στο να ανιχνεύουν άγνωστες παραλλαγές. Η έρευνα μας συνεισφέρει με μια ταξινόμησης των τεχνικών ανίχνευσης επιθέσεων ransomware και μία παρουσίαση των ερευνητικών κατευθύνσεων και ζητημάτων που πρέπει να αντιμετωπιστούν σε μελλοντικές έρευνες. Η ανάλυση και ο εντοπισμός νέων μοτίβων συμπεριφοράς που σηματοδοτούν την εμφάνιση μιας επίθεσης ransomware σε πραγματικό χρόνο, χωρίς να απαιτούνται ενέργειες από το χρήστη και χωρίς να επηρεαστεί η απόδοση του συστήματος παραμένει μία πρόκληση.

Summary

Ransomware is one of the most important forms of malware in recent decades. Attackers have organized a well-organized network of ransomware malware installations capable of infecting hundreds of thousands of computers in a matter of minutes and for profit. Over the last fifteen years their targets in terms of user profile have changed, as well as the profile of systems, and the ways of infecting networks and systems. The creation of a new Ransomware-as-a-Service business model is on the rise to automate the installation of malware on specific targets.

This research is called to study in depth the ransomware attack families, common features and variations in the attack model, recovery, detection and deterrence methods. Especially in the case of detection we list techniques using machine learning, or artificial intelligence as promising techniques to eliminate the problem in the future or detection techniques that are better prepared to detect unknown variants. Our research contributes with a classification of ransomware attack detection techniques and a presentation of research directions and issues to be addressed in future research. Analyzing and identifying new behavioral patterns that signal the occurrence of a ransomware attack in real-time, without requiring user actions and without affecting system performance remains a challenge.

Περιεχόμενα

Κεφάλαιο 1 1
Εισαγωγή 1
1.1 Σκοπός έρευνας 2
1.2 Βασικά ερευνητικά ερωτήματα 3
1.3 Αναγκαιότητα και σπουδαιότητα έρευνας 3
Κεφάλαιο 2 5
Θεωρία- βασικές κατηγορίες ransomware 5
2.1 Κακόβουλα προγράμματα (malware) 5
2.2 Κακόβουλα προγράμματα Malware 6
2.3 Ransomware 8
2.4 Διάδοση Ransomware 10
2.5 Τρεις κύριες παραλλαγές λειτουργίας κρυπτογράφησης 11
2.6 Ιστορική αναδρομή επιθέσεων ransomware 12
Κεφάλαιο 3 22
Ανατομία μίας επίθεσης ransomware – παραλλαγές επιθέσεων 22
3.1 Ανατομία επίθεσης ransomware Κακόβουλα προγράμματα (malware) 23
3.1.1 Παράδειγμα επίθεσης ransomware 26
3.2 Μοντέλο επίθεσης ransomware – βασικά χαρακτηριστικά 29
3.2.1 Στοχοποίηση χρηστών – κατηγορίες 38
3.2.2 Στοχοποίηση συστημάτων – κατηγορίες 40
3.2.3 Μέθοδοι μόλυνσης 43
3.2.4 Zero day ransomware 46
3.2.5 Σύνολο δεδομένων (Datasets) Ransomware 46
3.3 Τρόποι ανάκαμψης από επίθεσης ransomware 47
Κεφάλαιο 4 51
Μέθοδοι ανίχνευσης επιθέσεων 51
4.1 Εισαγωγή 51
4.2 Ομοιότητες μεταξύ μεθόδων ανίχνευσης 54
4.3 Μέθοδοι μηχανικής μάθησης 55
4.3.1 Μέθοδοι μηχανικής μάθησης για στατική ανάλυση 56
4.3.2 Μέθοδοι μηχανικής μάθησης για δυναμική ανάλυση 57
4.3.3 Μέθοδοι μηχανικής μάθησης για δυναμική ανάλυση σε φορητές/IoT συσκευές 60
4.3.4 Μέθοδοι μηχανικής μάθησης για δίκτυα 62
4.3.5 Μέθοδοι μηχανικής μάθησης για υβριδική ανάλυση 63
4.3.6 Μέθοδοι ανίχνευσης πολλαπλών σταδίων 65
4.3.7 Τεχνητή νοημοσύνη και Βαθειά Μάθηση 69
4.3.8 Συνελικτικά νευρωνικά δίκτυα 70

4.4 Σύνοψη 71
Κεφάλαιο 5 76
Συμπεράσματα 76
5.1 Στρατηγικές αντιμετώπισης των επιθέσεων ransomware 76
5.2 Προς ένα πλάνο ανταπόκρισης και ανάκαμψης από επιθέσεις ransomware 77
5.3 Συμπεράσματα – Μελλοντική επέκταση 80
Βιβλιογραφία 84

Κεφάλαιο 1
Εισαγωγή

Το κακόβουλο λογισμικό αποτελεί μια συνεχώς εξελισσόμενη και αυξανόμενη απειλή, ιδίως το ransomware που είναι από τις πιο σημαντικές μορφές κακόβουλου λογισμικού. Η άνοδος του ransomware ως υπηρεσία (Ransomware as a Service – RaaS) αποτελεί μία νέα τάση, και οι ερευνητές που ασχολούνται με τη συμπεριφορά κακόβουλου λογισμικού χρειάζονται τεχνικές και εργαλεία για τον γρήγορο και αξιόπιστο εντοπισμό μιας ευρύτερης πλέον κατηγορίας ransomware για την προστασία των δεδομένων ατόμων, επιχειρήσεων και σημαντικών υποδομών.

Το Ransomware είναι ένα κακόβουλο λογισμικό που έχει αποκτήσει σημαντική φήμη σε παγκόσμιο επίπεδο λόγω των πολύ σημαντικών και αμετάκλητων επιπτώσεων που μπορεί να επιφέρει στα θύματα (απλοί οικιακοί χρήστες ή οργανισμοί). Η ανεπανόρθωτη απώλεια που προκαλείται λόγω του ransomware απαιτεί την έγκαιρη ανίχνευση αυτών των επιθέσεων. Διεξάγονται πολλές μελέτες, που περιλαμβάνουν έρευνες και ανασκοπήσεις, για την εξέλιξη, ταξινόμηση, τις τάσεις, απειλές και αντίμετρα κατά του ransomware (Hassan, 2019). Χρησιμοποιείται όλο και περισσότερο από εγκληματίες στον κυβερνοχώρο για να εκβιάζουν μεγάλα χρηματικά ποσά από ιδιώτες και κυρίως από εταιρείες. Παγκοσμίως, θεωρείται από τους ερευνητές ως μια σημαντική απειλή σε μια κοινωνία που περνάει όλο και περισσότερο στη ψηφιακή εποχή (Kaspersky, 2020, McAfee, 2019; Trend Micro, 2020).

Το 2020 το Πανεπιστήμιο του Μάαστριχτ στην Ολλανδία έπεσε θύμα μόλυνσης ransomware που είχε ως αποτέλεσμα τη μη διαθεσιμότητα των συστημάτων πληροφορικής για τους φοιτητές και τους υπαλλήλους και προκάλεσε μεγάλη κοινωνική αναταραχή. Το Πανεπιστήμιο αναγκάστηκε να πληρώσει λύτρα στους επιτιθέμενους. Το 2017 το WannaCry είχε μολύνει εκατοντάδες χιλιάδες υπολογιστές σε όλο τον κόσμο. Μέσα στους οργανισμούς που είχαν επηρεαστεί ήταν και το Βρετανικό Εθνικό Σύστημα Υγείας (NHS). Ασθενείς θα μπορούσαν να είχαν πεθάνει εξαιτίας της μη διαθεσιμότητας

των απαραίτητων δεδομένων για την παροχή ιατροφαρμακευτικής φροντίδας (Ghafur et al., 2019).

Τον Σεπτέμβριο του 2020, το τοπικό ΕΚΑΒ του νοσοκομείου Ντίσελντορφ της Γερμανίας ειδοποιήθηκαν για την επιδείνωση της κατάστασης μιας 78χρονης γυναίκας που έπασχε από ανεύρυσμα αορτής. Αυτό που ξεκίνησε ως μια συνηθισμένη παραλαβή πήρε άσχημη τροπή όταν τηλεφώνησαν στο τοπικό πανεπιστημιακό νοσοκομείο για να ενημερώσουν το προσωπικό για την επικείμενη άφιξή τους. Τους είπαν ότι το τμήμα ατυχημάτων και επειγόντων περιστατικών ήταν κλειστό, οπότε δεν μπορούσαν να δεχτούν τον ασθενή. Αντ' αυτού, το ασθενοφόρο κατευθύνθηκε σε άλλο νοσοκομείο, 32 χιλιόμετρα μακριά, γεγονός που καθυστέρησε τη θεραπεία του ασθενούς κατά μία ώρα. Πέθανε λίγο αργότερα. Η τραγική αλληλουχία των γεγονότων συσχετιζόταν με μία επίθεση ransomware στο νοσοκομείο του Ντίσελντορφ.

Οι επιτιθέμενοι κρυπτογράφησαν τα δεδομένα και στη συνέχεια απαιτούσαν λύτρα για να τα ξεκλειδώσουν, και έτσι ανάγκασαν το νοσοκομείο να απομακρύνουν το ασθενοφόρο. Η επίθεση έθεσε σε κίνδυνο την ψηφιακή υποδομή στην οποία βασίζεται το νοσοκομείο για τον συντονισμό των γιατρών, των κλινών και της θεραπείας, αναγκάζοντας την ακύρωση εκατοντάδων χειρουργικών επεμβάσεων και άλλων διαδικασιών. Επίσης, περιόρισε δραστικά τη δυναμικότητα του νοσοκομείου: ενώ κανονικά νοσηλεύει περισσότερους από 1.000 ασθενείς κάθε μέρα, δεν μπορούσε να εξυπηρετήσει πάνω από τους μισούς κατά τη διάρκεια και μετά την επίθεση. Η διακοπή των νέων εισαγωγών ήταν απαραίτητη για την προστασία όσων βρίσκονταν ήδη μέσα. Το παραπάνω περιστατικό θα μπορούσε να θεωρηθεί ως η πρώτη περίπτωση θανάτου ανθρώπου από ransomware και έχει ήδη λάβει νομικές διαστάσεις.

1.1 Σκοπός έρευνας

Σκοπός της παρούσας έρευνας είναι να παρουσιάσει μία λεπτομερή βιβλιογραφική ανασκόπηση σχετικά με αυτή τη κατηγορία επιθέσεων, τις σύγχρονες παραλλαγές τους όπως και να καταγράψει τεχνικές ανίχνευσης που χρησιμοποιούν μηχανική μάθηση, ή άλλες τεχνικές τεχνητής νοημοσύνης.

Οι συνεισφορές αυτής της έρευνας παρουσιάζονται παρακάτω:

1. Παρουσίαση μιας ταξινόμησης που σκιαγραφεί τεχνικές εντοπισμού επιθέσεων ransomware τα τελευταία χρόνια.
2. Εκτενής επισκόπηση των τεχνικών ανίχνευσης ransomware που χρησιμοποιούν τεχνικές τεχνητής νοημοσύνης ή άλλες τεχνικές.
3. Παρουσίαση των ερευνητικών κατευθύνσεων και ζητημάτων που πρέπει να αντιμετωπιστούν σε μελλοντικές έρευνες.

1.2 Βασικά ερευνητικά ερωτήματα

Ορισμένα από τα ερωτήματα που θα εξετάσουμε στη παρούσα εργασία είναι:

- υπάρχουν συγκεκριμένα μοτίβα συμπεριφοράς που σηματοδοτούν την εμφάνιση μιας επίθεσης ransomware
- Έχουν καταγραφείς παραλλαγές στα υφιστάμενα μοντέλα επίθεσης που γνωρίζουμε
- Έχουν καταγραφεί νέες κατηγορίες ως προς τα γνωστά μοτίβα της συμπεριφοράς κατά την επίθεση Ransomware
- υπάρχουν συστήματα ή τεχνικές ανίχνευσης που είναι καλά σχεδιασμένα για να ανιχνεύουν άγνωστες παραλλαγές (Zero-Day) ransomware.

1.3 Αναγκαιότητα και σπουδαιότητα έρευνας

Όλο και περισσότερο λαμβάνουν χώρα κυβερνοεπιθέσεις με χρήση ransomware σε διάφορα συστήματα παγκοσμίως και ο αριθμός των παραλλαγών ransomware αυξάνεται ραγδαία κάθε χρόνο. Το 2021 είχαν λάβει χώρα 304.7 εκατομμύρια επιθέσεις 1με χρήση ransomware . Το 2021, η πιο κοινή παραλλαγή ransomware ήταν το Ryuk, το οποίο βρισκόταν πίσω από περισσότερες από 90 εκατομμύρια προσπάθειες ransomware τους πρώτους έξι μήνες του 2021. Το Cerber, ένα άλλο είδος ransomware, επιχείρησε 52,5

[1] Cyberattacks in 2021 Are at Record Levels - Consolidated Technologies, Inc. (consoltech.com)

εκατομμύρια επιθέσεις κακόβουλου λογισμικού από τον Ιανουάριο έως τον Ιούνιο του 2021.

Παρόλο που έχουν προταθεί διάφορες προσεγγίσεις ανίχνευσης και ταξινόμησης κακόβουλου λογισμικού, αυτές οι προσεγγίσεις δεν είναι κατάλληλες για άμυνα έναντι ransomware, επειδή αυτές οι προσεγγίσεις γενικά επικεντρώνονται στη διάκριση κακόβουλου λογισμικού από καλοήθη αρχεία. Κατά συνέπεια, απαιτούνται νέοι μηχανισμοί ανίχνευσης εξειδικευμένοι για ransomware και οι μηχανισμοί θα πρέπει να επικεντρώνονται σε ειδικά χαρακτηριστικά για ransomware για να διακρίνουν το ransomware από άλλους τύπους κακόβουλου λογισμικού καθώς και από καλοήθη αρχεία.

Κεφάλαιο 2 Θεωρία- βασικές κατηγορίες ransomware

2.1 Κακόβουλα προγράμματα (malware)

Κακόβουλο λογισμικό είναι κάθε λογισμικό που επηρεάζει έναν υπολογιστή/ηλεκτρονική συσκευή με κακόβουλο τρόπο. Το κακόβουλο λογισμικό μπορεί να είναι τόσο απλό όσο ένα αναδυόμενο παράθυρο που εμποδίζει τον χρήστη να έχει πρόσβαση σε μια ιστοσελίδα ή σε ένα κομμάτι λογισμικού που αντιγράφει οικονομικές πληροφορίες από τον υπολογιστή του θύματος.

Ενώ το ransomware υπάρχει εδώ και πολλά χρόνια, ξεκινώντας από την εμφάνιση του προγράμματος τύπου δούρειου ίππου (AIDS), η δημοτικότητά του μειώθηκε με την ανάπτυξη πιο προσοδοφόρων μορφών, όπως παραπλανητικές εφαρμογές, ψεύτικα προγράμματα προστασίας από ιούς και απλούστερες μορφές ransomware που κλειδώνουν τα αρχεία του συστήματος ή ενός προγράμματος περιήγησης. Ωστόσο, λόγω της αυξημένης γνώση των θυμάτων στο να γίνεται όλο και πιο δύσκολο να ξεγελαστούν από παραπλανητικές εφαρμογές και από ψεύτικα προγράμματα προστασίας από ιούς, και η έλευση των ανώνυμων διαδικτυακών νομισμάτων, δηλαδή του Bitcoin, η δημοτικότητα του ransomware έχει αντιστραφεί και πλέον αποτελεί την πιο διαδεδομένη μορφή malware.

2.2 Κακόβουλα προγράμματα Malware

Η παράδοση κακόβουλων αρχείων στο Διαδίκτυο περιλαμβάνει δύο κύριες πτυχές: τα malware payloads και τις δικτυακές υποδομές που χρησιμοποιούν οι κυβερνο- εγκληματίες για να τα εγκαταστήσουν σε υπολογιστές.

Το κακόβουλο λογισμικό αποτελεί αυξανόμενο πρόβλημα για πάνω από τρεις δεκαετίες. Προηγούμενες έρευνες επικεντρώθηκαν στη μελέτη των τρόπων με τους οποίους το κακόβουλο λογισμικό αποκρύπτεται για να αποφύγει την εύκολη ανίχνευση (Christodorescu et al, 2005), όπως με τη χρήση φθηνού λογισμικού ενθυλάκωσης του (packer) (Yan et al, 2008). Αυτή η τεχνική της απόκρυψης με δυαδικό τρόπο ονομάζεται πολυμορφισμός. Με την πάροδο των ετών, το κακόβουλο λογισμικό έχει χρησιμοποιηθεί για διάφορους λόγους: αποστολή μηνυμάτων spam (Stone et al, 2011), κλοπή σημαντικών δεδομένων από μολυσμένους υπολογιστές (Stone-Gross et al, 2009) και κρυπτογράφηση δεδομένων των θυμάτων με σκοπό τα λύτρα (Koniaris et al, 2014), για να αναφέρουμε μόνο μερικά από αυτά.

Οι ερευνητές έχουν επίσης εντοπίσει μια πληθώρα μέσων με τα οποία διανέμεται το κακόβουλο λογισμικό: μετάδοση μέσω φυσικών μέσων (Highland, 1988), με κακόβουλα συνημμένα αρχεία σε spam ηλεκτρονικά μηνύματα (Stone-Gross et al, 2011), κοινωνική μηχανική (Nelms et al, 2016) (π.χ. εξαπάτηση του θύματος ώστε να κατεβάσει το κακόβουλο λογισμικό από έναν κακόβουλο σύνδεσμο), drive-by downloads (Lee, 2018). Τα τελευταία χρόνια, ωστόσο, η ερευνητική κοινότητα έχει δείξει ότι οικογένειες από εξέχοντα κακόβουλα λογισμικά συχνά μεταφορτώνονται από droppers που ανήκουν σε υπηρεσίες pay-per-install (PPI) (Stone-Gross et al, 2011). Πρόκειται για μία από τις τελευταίες τεχνικές διανομής που αναπτύχθηκαν από τους κυβερνο-εγκληματίες.

Για να συμπληρωθεί αυτή η ήδη πολύπλευρη εικόνα της διανομής κακόβουλου λογισμικού, το οικοσύστημα του κυβερνοεγκλήματος έχει αναπτύξει πολλαπλές τεχνικές για να φέρνει σε αδιέξοδο τις διωκτικές αρχές και την ανίχνευση από τις εταιρείες ασφαλείας πιο δύσκολη. Οι κακοποιοί χρησιμοποιούν τεχνικές Fast Flux (Holz et al, 2008), στις οποίες η διεύθυνση πρωτοκόλλου Internet (IP) που σχετίζεται με έναν συγκεκριμένο τομέα αλλάζει πολύ γρήγορα. Ομοίως, για να δυσχεραίνεται ο εντοπισμός του DNS τομέα που εμπλέκεται σε μια

παράνομη επιχείρηση, οι κυβερνοεγκληματίες1 χρησιμοποιούν Domain Generation Algorithms (DGAs) (Antonakakis et al, 2012), οι οποίοι αλλάζουν με αλγοριθμικό τρόπο τα DNS domains συνεχώς, επιτρέποντας σε κακόβουλους υπολογιστές να γνωρίζουν ποιο domain να επικοινωνήσουν ανά πάσα στιγμή. Τέλος, τα κακόβουλα αρχεία αλλάζουν διαρκώς για να αποφεύγεται η εύκολη ανίχνευση, με τη χρήση τεχνικών πολυμορφισμού που είδαμε παραπάνω (Bayer et al, 2009).

Η ερευνητική κοινότητα έχει εντοπίσει δύο κύριες υποδομές που χρησιμοποιούνται από κυβερνο-εγκληματίες για την παράδοση κακόβουλου λογισμικού: exploitation kits και υπηρεσίες pay-per-install.

Τα exploit kits χρησιμοποιούνται εδώ και πολλά χρόνια για τη διάδοση κακόβουλου λογισμικού. Με λίγα λόγια, αποτελούν εργαλεία που συλλέγουν μεγάλο αριθμό από exploits που στοχεύουν σε πολλές εκδόσεις λειτουργικών συστημάτων, προγράμματα περιήγησης και πρόσθετα για προγράμματα περιήγησης για να διασφαλίσουν ότι οι εγκληματίες μπορούν να μολύνουν όσο το δυνατόν περισσότερα θύματα- υπολογιστές σε όσο το δυνατό μεγαλύτερο βαθμό (Grier et al, 2012). Ένα από τα πρώτα exploit kits είναι το MPack, βασισμένο στην γλώσσα PHP που κυκλοφόρησε στα τέλη του 2006 (Grier et al, 2012). Η κύρια λειτουργία αυτών των εργαλείων είναι η συλλογή πληροφοριών σχετικά με τον υπολογιστή του θύματος (γνωστό και ως fingerprint), να βρει ευπάθειες σε αυτόν και να καθορίσει την κατάλληλη εκμετάλλευση και, τέλος, να παραδώσει την εκμετάλλευση (π.χ., drive-by-download) και να εκτελέσει το κακόβουλο φορτίο (payload).

Η διαδικασία της εκμετάλλευσης από ένα από αυτά τα kit, σε γενικές γραμμές, ακολουθεί τα εξής βήματα: ένα θύμα επισκέπτεται μία ιστοσελίδα που είναι εκτεθειμένη, στη συνέχεια ανακατευθύνεται σε διάφορους ενδιάμεσους διακομιστές και τελικά καταλήγει σε έναν υποδοχέα με ένα exploit kit. Σήμερα, τα exploit kits αντιπροσωπεύουν την τελευταία λέξη της τεχνολογίας για αυτοματοποιημένη απομακρυσμένη μόλυνση, και έχουν εξελιχθεί μαζί με το οικοσύστημα κακόβουλου λογισμικού για κερδοσκοπικούς σκοπούς. Ως εκ τούτου, αρκετές μελέτες έχουν κατευθυνθεί προς την ανίχνευση τέτοιων exploit kits στο διαδίκτυο.

Ενώ ένα τυπικό οικοσύστημα PPI έχει τρεις κύριους φορείς: έναν πελάτη, έναν πάροχο υπηρεσιών και ένα συνεργάτη. Μια τυπική συναλλαγή PPI λειτουργεί ως εξής: οι πελάτες (π.χ. προγραμματιστές κακόβουλου λογισμικού) πληρώνουν παρόχους υπηρεσιών PPI για να εγκαταστήσουν το κακόβουλο λογισμικό τους σε έναν αριθμό θυμάτων - υπολογιστών. Αυτοί οι πάροχοι υπηρεσιών είτε εγκαθιστούν το κακόβουλο λογισμικό στις μηχανές των θυμάτων

άμεσα (δηλαδή χρησιμοποιώντας τους δικούς τους downloaders), ή χρησιμοποιούν συνεργάτες για τη διανομή κακόβουλου λογισμικού σε χρήστες-στόχους (δηλαδή αγοράζοντας εγκαταστάσεις από τρίτους). Μόλις το κακόβουλο λογισμικό εγκατασταθεί με επιτυχία και επαληθευτεί από τους πελάτες της PPI, οι συνεργάτες λαμβάνουν τις σχετικές πληρωμές από τους παρόχους υπηρεσιών.

Δεδομένης της αύξησης αυτής της κακόβουλης χρήσης των PPIs - τόσο των εμπορικών PPIs που χρησιμοποιούνται για να μεταφέρουν κακόβουλο λογισμικό μεταξύ άλλων τύπων λογισμικού, καθώς και κακόβουλα PPIs που είναι ειδικά σχεδιασμένα για κακόβουλη δραστηριότητα – έχει διεξαχθεί αρκετή έρευνα τα τελευταία χρόνια για την αποτύπωση αυτών των υπηρεσιών. Μια μελέτη (Thomas et al, 2016) υποστηρίζει ότι τα PPIs μπορούν να χωριστούν σε εμπορικά και PPIs στη μαύρη αγορά. Τα εμπορικά PPIs χρειάζονται τη συγκατάθεση του χρήστη για να λειτουργούν, ενώ οι PPI στη μαύρη αγορά εκτελούν σιωπηλές εγκαταστάσεις στους υπολογιστές-στόχους, δηλαδή εγκαταστάσεις χωρίς τη συγκατάθεση του ιδιοκτήτη του συστήματος.

Μία άλλη μελέτη (Caballero et al, 2011) παρείχε την πρώτη μεγάλης κλίμακας μέτρηση των υπηρεσιών PPI στη μαύρη αγορά. Αυτό επιτυγχάνεται με τη συγκομιδή πάνω από ένα εκατομμύριο εκτελέσιμων αρχείων πελατών χρησιμοποιώντας σημεία σε 15 χώρες. Η μελέτη διαπίστωσε ότι 12 από 20 από τις πιο διαδεδομένες οικογένειες κακόβουλου λογισμικού εκείνη την εποχή χρησιμοποιούσαν υπηρεσίες PPI για να αγοράσουν κακόβουλα προγράμματα, επιβεβαιώνοντας τις προηγούμενες έρευνες ότι οι κυβερνο-εγκληματίες συνήθως χρησιμοποιούν άλλα botnet για την παράδοση των κακόβουλων ωφέλιμων φορτίων τους.

2.3 Ransomware

Το ransomware ορίζεται σύμφωνα με διεθνούς οργανισμούς κυβερνοασφάλειας: Το Ransomware είναι λογισμικό που κρυπτογραφεί τα αρχεία του υπολογιστή έτσι ώστε οι χρήστες να μην έχουν πλέον πρόσβαση σε αυτά. Μόνο μετά την καταβολή των λύτρων τα δεδομένα ή τα έγγραφα ενδεχομένως να είναι και πάλι προσβάσιμα (MITRE, 2020; NCSC, 2020).

Το εκτελέσιμο αρχείο του ransomware είναι αυτό που αναφέρεται ως το ωφέλιμο φορτίο του κακόβουλου λογισμικού. Είναι ο κώδικας που εκτελείται στον υπολογιστή του θύματος για να πάρει τον έλεγχο των αρχείων του. Ο διακομιστής Command & Control είναι ένας απομακρυσμένος διακομιστής που ελέγχεται από τον ελεγκτή του κακόβουλου λογισμικού που παράγει εντολές και/ή ελέγχους στο εκτελέσιμο πρόγραμμα, έτσι ώστε να μπορεί να εκπληρωθεί η κύρια λειτουργία του εκτελέσιμου αρχείου (π.χ. κρυπτογράφηση των προσωπικών αρχείων του θύματος). Ο διακομιστής C&C επιτρέπει επίσης στον ελεγκτή να διατηρεί καταγραφές για κάθε εκτέλεση του ωφέλιμου φορτίου με ένα σχετικό κλειδί που ενδεχομένως επιτρέπει στο θύμα να αποκρυπτογραφήσει/ανακτήσει τα αρχεία. Ένας διακομιστής C&C δεν περνάει το ωφέλιμο φορτίο στο σύστημα του θύματος. Το ωφέλιμο φορτίο πρέπει να ενεργοποιηθεί στο σύστημα του θύματος πριν συνδεθεί με τον διακομιστή C&C για να λάβει περαιτέρω εντολές ελέγχου.

Ωστόσο, ακόμη και αν ένας οργανισμός καταβάλλει τα λύτρα δεν υπάρχει εγγύηση ότι τα αρχεία θα είναι προσβάσιμα ξανά. Τα συστήματα μολύνονται με ransomware μέσω αρχείων που ανοίγει ένας τελικός χρήστης μέσω email ή με την επίσκεψη σε ένα μολυσμένο ιστότοπο. Η μόλυνση και η περαιτέρω εξάπλωση συμβαίνουν επειδή το κακόβουλο λογισμικό εκμεταλλεύεται ευπάθειες στο λειτουργικό σύστημα, όπως το γνωστό WannaCry ransomware (Talos, 2017). Οι επιτιθέμενοι μπορούν να αναπτύξουν ransomware εναντίον πολλών διαφορετικών στόχων. Κάθε σύστημα που περιέχει πολύτιμα δεδομένα μπορεί να αποτελέσει σημαντικό στόχο και οι επιτιθέμενοι συχνά απαιτούν περισσότερα λύτρα από μεγάλες εταιρείες, κυβερνητικές υπηρεσίες ή οργανισμούς που διαθέτουν ευαίσθητα δεδομένα (Loman, 2019).

Η σύγχρονη γενιά ransomware εμφανίστηκε το 2006 και από τότε η καταστροφική του επιρροή επεκτείνεται συνεχώς. Τα τελευταία χρόνια οι εγκληματίες που δρουν στον κυβερνοχώρο έχουν εξελιχθεί και δρουν πιο στοχευμένα για το ποια συστήματα ηλεκτρονικών υπολογιστών και με ποιο τρόπο θα πρέπει να μολύνουν. Εν τω μεταξύ, όσον αφορά την ασφάλεια στον κυβερνοχώρο οι ειδικοί έχουν διαμορφώσει μεθόδους αντιμετώπισης του ransomware και μέσα από διάφορες καινοτομίες έχουν οργανώσει τις αμυντικές τους τεχνικές σε τρεις τομείς: ανάκαμψη, ανίχνευση και πρόληψη.

Η τάση δείχνει ότι το έγκλημα στον κυβερνοχώρο με επίκεντρο το ransomware θα μετριαστεί πιθανώς τις επόμενες δεκαετίες, καθώς τα εργαλεία ασφαλείας βελτιώνονται,

οι χρήστες είναι περισσότερο συνειδητοποιημένοι για τέτοιου είδους απειλές, και οι κυβερνητικές οντότητες παρεμβαίνουν για να επιβάλουν τιμωρίες.

2.4 Διάδοση Ransomware

Το Ransomware μπορεί να διαδοθεί μέσω πολλών διαφορετικών φορέων, όπως:

- Ανακατεύθυνση της κυκλοφορίας: Αυτή είναι η πιο κοινή μέθοδος για να δελεάσουν τον χρήστη σε κλικ σε κακόβουλη διαφήμιση ή ανακατεύθυνση της διαδικτυακής κίνησης του χρήστη σε άλλο ιστότοπο που περιέχει το κακόβουλο λογισμικό (exploitation kit). Συνήθως η ανακατευθυνόμενη κυκλοφορία προέρχεται από ιστοσελίδες με πορνογραφικό υλικό, μια πύλη που προσφέρει δωρεάν παιχνίδια ή αναβάθμιση εφαρμογών. Εάν ο χρήστης αποδεχτεί και κατεβάσει το δωρεάν λογισμικό, το ωφέλιμο φορτίο του κακόβουλου λογισμικού εκμεταλλεύεται ευπάθειες στον υπολογιστή του χρήστη που οδηγούν σε κλείδωμα ή κρυπτογράφηση των συστημάτων και των αρχείων τους.

- Η ανακατεύθυνση της κυκλοφορίας μπορεί επίσης να οδηγήσει σε αυτό που ονομάζεται drive-by-download όπου κακόβουλος κώδικας μεταφορτώνεται στον υπολογιστή του θύματος χωρίς να το γνωρίζει (Savage, Coogan et al. 2015).

- Συνημμένα email: Τα email που έχουν συνημμένα αρχεία ή συνδέσμους δελεάζουν τους χρήστες να τα ανοίξουν και να μπουν σε διαδικτυακές πύλες που έχουν το κακόβουλο λογισμικό. Το email στην αρχή φαίνεται να έχει νόμιμους αποστολείς, όπως ο λογαριασμός πληρωμής του ηλεκτρικού ρεύματος του χρήστη, επιστροφή φόρου από την εφορία, νομικές ειδοποιήσεις ή ακόμη και άτομα που αναζητούν εργασία και ζητούν να ανοίξουν το συνημμένο αρχείο ή κάνοντας κλικ σε έναν σύνδεσμο για να δώσουν τις τελευταίες πληροφορίες του χρήστη. Ενώ ο χρήστης

ανοίγει το συνημμένο αρχείο ή περιηγείται στον ιστότοπο, στο παρασκήνιο το κακόβουλο λογισμικό αρχίζει να μολύνει το σύστημα του χρήστη.

- Botnets: Τα botnets διανέμονται μέσω προγραμμάτων downloaders που παραβιάζουν τα συστήματα των χρηστών και στη συνέχεια λαμβάνουν το κακόβουλο λογισμικό ως δεύτερο βήμα. Οι downloaders είναι νόμιμο λογισμικό, όπως δωρεάν παιχνίδια ή εργαλεία που δεν έχουν οι ίδιοι το κακόβουλο λογισμικό- αλλά κατεβάζουν τον κώδικα του κακόβουλου λογισμικού αργότερα.

- Κοινωνική μηχανική: Κατά καιρούς το ransomware έχει μια ενσωματωμένη λειτουργία για να εξαπλωθεί σε άλλα συστήματα είτε με την αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου ή μέσω μηνυμάτων SMS. Η μέθοδος αυτή είναι αποτελεσματική καθώς το κακόβουλο λογισμικό μπορεί να εξαπλωθεί καθώς προέρχεται από νόμιμη πηγή και γίνεται αποδεκτό με εύκολο τρόπο.

- Ransomware ως υπηρεσία: παρατηρείται πλέον μία νέα τάση σε έξαρση που αφορά τους εκβιασμούς με ψηφιακά μέσα. Οι φορείς αυτού του κυβερνοεγκλήματος έχουν αρχίσει να παρέχουν ransomware ως υπηρεσία ή RaaS δηλαδή προσφέρουν την πραγματοποίηση επιθέσεων κακόβουλου λογισμικού με πληρωμή ή συμμετέχοντας στα κέρδη από τη καταβολή λύτρων (Bhardwaj, Subrahmanyam et al. 2015).

2.5 Τρεις κύριες παραλλαγές λειτουργίας κρυπτογράφησης

Αναλύουμε παρακάτω τους πιο γνωστούς τύπους ransomware. Το crypto-ransomware μπορεί να χωριστεί σε τρεις κατηγορίες με βάση τον τρόπο κρυπτογράφησης των αρχείων του θύματος. Οι κατηγορίες αυτές ορίζονται ως εξής:

- Κατηγορία 1. Το Ransomware αυτής της κατηγορίας αντικαθιστά/κωδικοποιεί τα αρχεία επιτόπου, αντιγράφει στο κρυπτογραφημένο αρχείο τα ίδια μεταδεδομένα που έχει και το αρχικό αρχείο.

- Κατηγορία 2. Το Ransomware αυτής της κατηγορίας μετακινεί το αρχικό αρχείο από τον αρχικό κατάλογο (π.χ. το φάκελο εγγράφων του θύματος) σε διαφορετικό κατάλογο όπου η κρυπτογράφηση πραγματοποιείται πριν το αρχείο μεταφερθεί πίσω στον αρχικό κατάλογο. Αυτός ο τύπος ransomware μπορεί επίσης να αλλάξει το όνομα αρχείου του κρυπτογραφημένου αρχείου έτσι ώστε τα πρωτότυπα και τα κρυπτογραφημένα αρχεία να έχουν διαφορετικά ονόματα, γεγονός που ενδεχομένως καθιστά δυσκολότερο τον εντοπισμό.

- Κατηγορία 3. Τα Ransomware αυτής της κατηγορίας δημιουργούν ένα νέο αρχείο που αντικαθιστά το αρχικό αρχείο (Scaife, Carter et al. 2016). Αυτός είναι ο τύπος ransomware που είναι πιο δύσκολο να εντοπιστεί με τη χρήση ενός συστήματος ανίχνευσης που ελέγχει για τη περίπτωση μαζικής διαγραφής αρχείων από εκτελούμενες διεργασίες. Αυτό γίνεται ακόμη πιο δύσκολο αν ο χρήστης διαγράφει μεγάλο αριθμό αρχείων σε τακτική βάση.

2.6 Ιστορική αναδρομή επιθέσεων ransomware

1989

Το πρώτο καταγεγραμμένο ransomware, το AIDS Trojan, είχε αναπτυχθεί στο Διεθνές Συνέδριο του Παγκόσμιου Οργανισμού Υγείας μέσω δισκετών 5¼ ιντσών που αποστάλθηκαν ταχυδρομικά στο συνέδριο με μία παραπλανητική ετικέτα "Ενημέρωση για το AIDS – δισκέτες προγράμματος". Το πρώτο στο είδος του, το AIDS Trojan δεν αποτελούσε στην πραγματικότητα απειλή επειδή χρησιμοποίησε απλή, συμμετρική κρυπτογραφία. Τα λύτρα καθορίστηκαν στο ποσό των $189 USD που έπρεπε να αποσταλούν σε ταχυδρομική θυρίδα στον Παναμά. Σε αντίθεση με τα περισσότερα ransomware στα οποία ο δημιουργός τους παραμένει ανώνυμος, στη περίπτωση αυτή ο δημιουργός του έγινε γνωστός: ο Joseph L Popp, ένας βιολόγος θεωρείται πλέον ο "πατέρας του ransomware" (Sjouwerman, 2015). Είναι σαφές ότι το ransomware δεν αποτελούσε απειλή ακόμα στο ξεκίνημα του. Σε αυτή την εποχή το κακόβουλο λογισμικό μπορούσε να χρησιμοποιηθεί από κάποιους για φάρσες και βανδαλισμούς με σκοπό τη φήμη (Savage et al, 2015).

1996

Οι Adam Young και Moti Yung, κρυπτογράφοι εκείνης της εποχής, περιγράψανε την έννοια του κρυπτογραφικού ransomware και το ονομάσανε κρυπτοβιολογία. Στη δημοσίευση τους αναφέρανε ότι η κρυπτογραφία - που παραδοσιακά χρησιμοποιείται για αμυντικούς σκοπούς, πχ για την προστασία της ιδιωτικής ζωής, τον έλεγχο ταυτότητας και την ασφάλεια θα μπορούσε να χρησιμοποιούνται και από επιτιθέμενους με σκοπό τον εκβιασμό. Τόνιζαν ότι η ασύμμετρη κρυπτογράφηση είναι απαραίτητη σε αυτές τις επιθέσεις και προειδοποίησαν ότι η πρόσβαση σε κρυπτογραφικά εργαλεία πρέπει να προστατευθεί (Young and Yung, 1996). Κάτι που δεν εισακούστηκε με αποτέλεσμα να ακολουθήσουν στο μέλλον ransomware επιθέσεις.

2005

Συνεχίζοντας την έρευνα τους, οι Young και Yung προτείνουν επιπλέον κάποια αντίμετρα για τους χρήστες: δημιουργία αντιγράφων ασφαλείας των δεδομένων των χρηστών, ενεργοποίηση τείχους προστασίας στη περίμετρο των δικτύων, χρήση προγραμμάτων antivirus, εγκατάσταση προγραμμάτων μόνο από αξιόπιστες πηγές (Young and Yung, 2005).

2006

Καταγράφονται οι πρώτες επιθέσεις ransomware με τις ονομασίες Archiveus Trojan και GPcode. Το GPcode μεταμφιέστηκε σε ένα κακόβουλο email στο οποίο ήταν συνημμένο ένα αρχείο για αίτηση εργασίας και στόχευε Ρώσους χρήστες του διαδικτύου. Ο προγραμματιστής του GPcode συνέχισε να βελτιώνει την έκδοση του κακόβουλου προγράμματος ενισχύοντας τον μηχανισμό κρυπτογράφησης, και κυκλοφορώντας τρεις εκδόσεις σε διάστημα πέντε ημερών. Η τρίτη έκδοση χρησιμοποιούσε κρυπτογράφηση που θα χρειαζόταν 30 χρόνια για να σπάσει ένας σύγχρονος υπολογιστής (Nazarov and Emelyanova, 2006). Το δε Archiveus Trojan απαιτούσε από τα θύματα να αγοράσουν αντικείμενα από ένα online φαρμακείο για να λάβουν το 30ψήφιο κλειδί αποκρυπτογράφησης (Sjouwerman, 2015).

2007

Στη δημοσίευσης τους, οι, ερευνητές ασφάλειας, Lou και Liao, τόνιζαν για πρώτη φορά ότι η κακή χρήση των πληροφοριακών συστημάτων από τους χρήστες είχε ως αποτέλεσμα την εκτόξευση των κυβερνοεπιθέσεων και των παραβιάσεων των προσωπικών δεδομένων. Τόνισαν επίσης την ανάγκη της προώθησης των προγραμμάτων ενημέρωσης των χρηστών σχετικά με το ransomware ως ένα μέσο πρόληψης τέτοιου είδους επιθέσεων (Luo et al, 2007). Ήταν η πρώτη φορά που οι ερευνητές σχετικά με την ασφάλεια των πληροφοριακών συστημάτων αναγνώρισαν την ανάγκη αντιμετώπισης του ransomware.

2008

Ο Gazet, ένας ειδικός στην ανάπτυξη προγραμμάτων antivirus, ανέλυσε τρεις πρώιμες οικογένειες ransomware με βάση την ποιότητα του κώδικά τους, τη λειτουργικότητα και τη κρυπτογραφική τους ισχύ. Κατέληξε στο συμπέρασμα ότι οι ερευνητές πρέπει να συνεχίσουν να παρακολουθούν την εξέλιξη των προγραμμάτων, αλλά εκείνη την εποχή δεν ήταν ώριμο και πολύπλοκο αρκετά για να απασχολήσει πιο έντονα τα μέσα ενημέρωσης. Συνεπώς ένα σχέδιο απλού ή μαζικού εκβιασμού του επιτιθέμενου θα ήταν καταδικασμένο σε αποτυχία (Gazet, 2008).

2009

Το Bitcoin εισέρχεται στην επικαιρότητα και φέρνει επανάσταση στην εξέλιξη του ransomware, μετατρέποντάς το σε μία νέα μαύρη αγορά. Μέχρι τότε, τα λύτρα έπρεπε να καταβληθούν με μη χρηματικούς τρόπους, επειδή η ηλεκτρονική πληρωμή θα ήταν ανιχνεύσιμη. Για παράδειγμα, τα θύματα θα έπρεπε να πληρώσουν στέλνοντας προπληρωμένες κάρτες, να κάνουν κλήση σε premium αριθμό υψηλής χρέωσης, ή να κάνουν παραγγελία προϊόντων από το ηλεκτρονικό κατάστημα του επιτιθέμενου (Richardson et al, 2017). Οι επιτιθέμενοι με ransomware ήταν πρόθυμοι να μεταβούν σε Bitcoin επειδή οι υπάρχουσες μέθοδοι ήταν εγγενώς ανιχνεύσιμες (Huang et al, 2018).

2013

Το CryptoLocker είναι μία σημαντική επίθεση ransomware που μολύνει χιλιάδες υπολογιστές στον κόσμο. Η βασική του μέθοδος εξάπλωσης ήταν μηνύματα ηλεκτρονικού ταχυδρομείου με συνημμένα αρχεία που είχαν αποσταλεί σε επιχειρήσεις και οργανισμούς με σκοπό να παραπλανήσει τους χρήστες και να μεταβούν σε ήδη παραβιασμένους ιστότοπους (Sjouwerman, 2015). Το CryptoLocker κατάφερε να μολύνει περίπου 500.000 υπολογιστές με εκτιμώμενα έσοδα 3 έως 27 εκατομμύρια δολάρια ΗΠΑ (Hansberry et al, 2014). Τα θύματα είχαν στη διάθεση τους τρεις ημέρες για να πληρώσουν τα λύτρα, διαφορετικά είτε θα διαγράφανε το κλειδί αποκρυπτογράφησης ή θα αυξάνανε τα λύτρα. Το CryptoLocker ήταν ο προπομπός ενός νέου επιχειρηματικού μοντέλου στο κυβερνοέγκλημα της δημιουργίας εσόδων και της μη ανιχνεύσιμης πληρωμής προς τους επιτιθέμενους. Έτσι ακολούθησαν νέες εκδόσεις ransomware (Genç, 2020) υιοθετώντας το επιχειρηματικό μοντέλο του CryptoLocker.

Το αντίκτυπο που είχε το CryptoLocker φαίνεται καλύτερα αν εξετάσουμε τον αριθμό των επιθέσεων το 2013: από τις 100.000 τον Ιανουάριο φτάσανε τις 600.000 τον Δεκέμβριο (Savage et al, 2015). Λαμβάνοντας υπόψη τον αριθμό των επιθέσεων σε τέτοια κλίμακα οι εταιρείες ασφαλείας κατάφεραν να διεισδύσουν στο δίκτυο κυβερνοεγκληματιών μέσα σε ένα χρόνο και δημιούργησαν ένα διαδικτυακό σύστημα αποκρυπτογράφησης. Μέσα από αυτή τη πύλη μπόρεσαν να βοηθήσουν θύματα και να κρατήσουν το ποσοστό καταβολής λύτρων σε χαμηλά επίπεδα (1,3%) (Hansberry et al, 2014).

2015

Μια ερευνητική ομάδα κυβερνοασφάλειας εξέτασε 1.359 δείγματα ransomware από το 2006-2014 και διαπίστωσε ότι αν και μερικά δείγματα ransomware ήταν εξελιγμένα και με σημαντικές επιπτώσεις, οι περισσότερες επιθέσεις χρησιμοποιούσαν επιφανειακές τεχνικές (Kharraz et al, 2015). Η έρευνα κατέληγε ότι η αποτροπή προηγμένων επιθέσεων ransomware ήταν απλούστερη από ότι παρουσίαζαν τα μέσα ενημέρωσης. Επίσης, για πρώτη φορά αναφέρεται σε τέτοια μελέτη ότι εφαρμόζοντας τεχνικές ανάλυσης της συμπεριφοράς του συστήματος το ransomware μπορεί να ανιχνευτεί και να ξεχωρίσει σε σχέση με φυσιολογικές εφαρμογές.

2016

Ως συνέχεια της προηγούμενης μελέτης και εφαρμόζοντας τεχνικές παρακολούθησης των προσβάσεων αρχείων και της συμπεριφοράς του συστήματος η έρευνα κατέληξε σε υψηλά ποσοστά ανίχνευσης (96,3%) (Kharraz et al, 2016). Αυτή είναι η πρώτη μελέτη που παρουσιάζει μία ολοκληρωμένη τεχνική αντιμετώπισης του κακόβουλου λογισμικού με βάση την ανίχνευση. Μελλοντικές προσπάθειες έχουν πλέον ως σημείο αναφοράς τη συγκεκριμένη μελέτη.

2017

Η χρονιά αυτή χαρακτηρίζεται από το WannaCry Ransomware που κατάφερε να μολύνει εκατομμύρια υπολογιστών σε όλο τον κόσμο. Το WannaCry αξιοποίησε ένα exploit που δημιουργήθηκε από την Εθνική Υπηρεσία Ασφαλείας (NSA) των ΗΠΑ και είχε κλαπεί και διαρρεύσει από μια ομάδα γνωστή ως Shadow Brokers. Η αρχική μόλυνση πιθανόν να συνέβη κατά τη διάρκεια μιας μη ασφαλούς δημόσιας σύνδεση Wi-Fi σε διαδικτυακό καφέ. Αυτό που έκανε το WannaCry ιδιαίτερα καταστροφικό ήταν η ικανότητά του να αυτοδιαδίδεται όπως ένας πραγματικός ιός, δηλαδή η ζημιά δεν περιοριζόταν μόνο στο μολυσμένο μηχάνημα αλλά και σε κάθε άλλο μηχάνημα στο εν λόγω δίκτυο (Chittooparambil et al, 2018). Μέσα σε λίγες ώρες το WannaCry μόλυνε εκατοντάδες χιλιάδες μηχανήματα σε περισσότερες από 150 χώρες, στοχεύοντας σε μεμονωμένους χρήστες, επιχειρήσεις, οργανισμούς και δημόσιες υπηρεσίες. Αν και δεν ήταν πολύ κερδοφόρο, το WannaCry έβαλε ως στόχο το Εθνικό Σύστημα Υγείας (NHS) του Ηνωμένου Βασιλείου, κάτι που προκάλεσε την αντίδραση της κοινωνίας ενάντια στους επιτιθέμενους (Sjouwerman, 2015).

2019

Ομάδα ερευνητών κυβερνοασφάλειας δημοσίευσε μια μελέτη για τις σύγχρονες τάσεις στις επιθέσεις ransomware και κατέληξε στο συμπέρασμα ότι διαφοροποιείται πλέον με ταχείς ρυθμούς. Για την αντιμετώπιση τους, η μελέτη πρότεινε την ανάπτυξη καλύτερων μοντέλων ανάλυσης της συμπεριφοράς του ransomware, ώστε οι μηχανισμοί άμυνας να μπορούν να ανιχνεύουν και να ανταποκρίνονται σε επιθέσεις (Hull et al, 2019). Επιπλέον, ο οργανισμός MITRE που έχει δημιουργήσει το πρότυπο ATT&CK (Adversarial

Techniques, Tactics, & Common Knowledge), αντιστοίχισε σε αυτό το μοντέλο ransomware. Με βάση αυτό το μοντέλο οι μηχανισμοί ανίχνευσης και αποτροπής παρόχων υπηρεσιών και τεχνολογιών μπορούσαν να προσαρμόσουν τις λύσεις τους (Oosthoek and Doerr, 2019).

2020

Αρκετές ομάδες εγκληματιών στο κυβερνοχώρο έχουν δραστηριοποιηθεί θέτοντας ως στόχο διαφορετικούς οργανισμούς.

Επιτιθέμενοι ξεκίνησαν τη χρονιά με μια επίθεση στην εταιρεία ανταλλαγής συναλλάγματος Travelex, αναγκάζοντας την εταιρεία να απενεργοποιήσει όλα τα συστήματα ηλεκτρονικών υπολογιστών και να βασιστεί για τις συναλλαγές σε στυλό και χαρτί. Ως αποτέλεσμα, η εταιρεία αναγκάστηκε να κατεβάσει τους ιστότοπούς της σε 30 χώρες. Μια νέα ομάδα επιτιθέμενων με την ονομασία Sodinokibi (επίσης γνωστή ως REvil) βρισκόταν πίσω από την επίθεση, απαιτώντας 6 εκατομμύρια δολάρια από την Travelex. Η συμμορία ισχυρίστηκε ότι είχε αποκτήσει πρόσβαση στο δίκτυο υπολογιστών της εταιρείας έξι μήνες νωρίτερα, επιτρέποντάς της να κατεβάσει 5 GB ευαίσθητων δεδομένων πελατών - συμπεριλαμβανομένων ημερομηνιών γέννησης και αριθμών πιστωτικών καρτών. Η ομάδα είπε ότι αν η Travelex πλήρωνε τα λύτρα, θα διέγραφε τα δεδομένα, αλλά αν όχι, τα λύτρα θα διπλασιάζονταν κάθε δύο ημέρες. Μετά από επτά ημέρες, είπαν ότι θα πωλούσαν τα δεδομένα σε άλλους εγκληματίες του κυβερνοχώρου.

Η Travelex φέρεται να κατέβαλε στη συμμορία 2,3 εκατομμύρια δολάρια σε Bitcoin και να αποκατέστησε τα online συστήματά της μένοντας εκτός λειτουργίας για δύο εβδομάδες. Τον Αύγουστο του 2020, η εταιρεία ανακοίνωσε ότι τίθεται υπό διοίκηση , λέγοντας ότι αυτό οφείλονταν σε συνδυασμό της επίθεσης ransomware και των επιπτώσεων της πανδημίας Covid-19.

Αντίστοιχα, μια επόμενη κυβερνοεπίθεση παρέλυσε ορισμένες επιχειρηματικές λειτουργίες του ομίλου ΙΝΑ, της μεγαλύτερης εταιρείας πετρελαιοειδών και της

μεγαλύτερης αλυσίδας πρατηρίων καυσίμων της Κροατίας. Η επίθεση ήταν μια επόμενη παραλλαγή ransomware που μόλυνε και στη συνέχεια κρυπτογράφησε ορισμένους από τους διακομιστές της εταιρείας. Ενώ η επίθεση δεν επηρέασε την ικανότητα της εταιρείας να παρέχει φυσικό αέριο στους πελάτες, επηρέασε την ικανότητά της να εκδίδει τιμολόγια, να καταχωρεί τη χρήση καρτών επιβράβευσης, να εκδίδει νέα κουπόνια κινητής τηλεφωνίας και να επιτρέπει στους πελάτες να πληρώνουν ορισμένους λογαριασμούς. Η επίθεση φέρεται να προκλήθηκε από μόλυνση του στελέχους Clop ransomware. Αυτή ήταν μία νέα γενιά που στοχεύουν εταιρείες για να μολύνουν τα δίκτυά τους, να κρυπτογραφήσουν δεδομένα και να απαιτήσουν εξαιρετικά μεγάλα λύτρα.

Αντίστοιχες επιθέσεις ransomware πραγματοποιήθηκαν την ίδια χρονιά σε εταιρίες που δραστηριοποιούνται στην ενέργεια (Καλιφόρνια ΗΠΑ, Ηνωμένο Βασίλειο, Πορτογαλλία), πανεπιστήμια, αυτοκινητοβιομηχανίες, παρόχους τηλεπικοινωνιακών υπηρεσιών.

2021

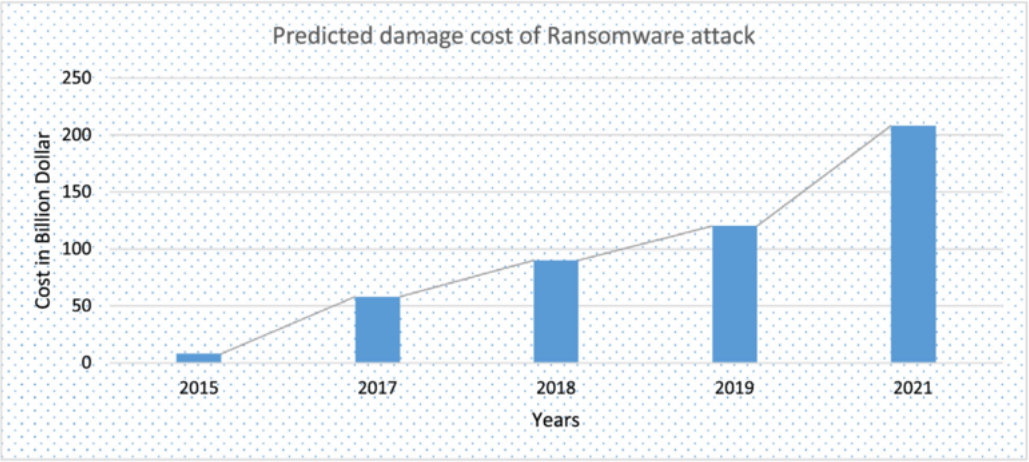
Τη χρονιά αυτή καταγράφεται παγκοσμίως αύξηση 1.885% σε επιθέσεις ransomware, ενώ μόνο ο κλάδος της υγειονομικής περίθαλψης αντιμετώπισε αύξηση 755% στις επιθέσεις αυτές. Οι επιθέσεις ransomware έπληξαν τις αλυσίδες εφοδιασμού, προκαλώντας εκτεταμένες διακοπές λειτουργίας των συστημάτων, οικονομικές απώλειες και ζημιά στη φήμη των οργανισμών.

Η επίθεση ransomware στην Colonial Pipeline στις ΗΠΑ θεωρήθηκε ως η πιο προβεβλημένη επίθεση ransomware το 2021. Η εταιρεία ήταν υπεύθυνη για τη μεταφορά σχεδόν του 50% των καυσίμων της ανατολικής ακτής των ΗΠΑ. Το περιστατικό αυτό θεωρήθηκε ως η μεγαλύτερη επίθεση ransomware με στόχο πετρελαϊκή εταιρεία στην ιστορία των ΗΠΑ. Τον Μάιο, η ομάδα DarkSide ανέπτυξε ransomware στο σύστημα υπολογιστών της εταιρείας που επιβλέπει και διαχειρίζεται τον αγωγό.

Το εκπληκτικό σε αυτό το περιστατικό είναι το πόσο εύκολα οι επιτιθέμενοι κατάφεραν να αποκτήσουν πρόσβαση στο σύστημα. Σε δεύτερο χρόνο, ο διευθύνων σύμβουλος της

Colonial Pipeline αποκάλυψε ότι η επιχείρηση δεν χρησιμοποιούσε έλεγχο ταυτότητας πολλαπλών παραγόντων, γεγονός που εξηγεί την ευκολία παραβίασης του συστήματος. Αν και η επίθεση δεν επηρέασε το λειτουργικό σύστημα της εταιρείας, επηρέασε το σύστημα χρέωσης. Αυτό ανάγκασε την Colonial Pipeline να διακόψει προσωρινά τις δραστηριότητές της. Μέσα σε λίγες ώρες από την επίθεση, η Colonial Pipeline κατέβαλε τα λύτρα ύψους 4,4 εκατομμυρίων δολαρίων ΗΠΑ με τη βοήθεια του FBI. Τον Ιούνιο, το Υπουργείο Δικαιοσύνης επικαιροποίησε το 50% των λύτρων είχαν επιστραφεί.

Το Διάγραμμα παρακάτω παρουσιάζει το εκτιμώμενο κόστος σε Δισεκατομμύρια δολάρια και το ρυθμό αύξησης του από το 2015 έως το 2021.

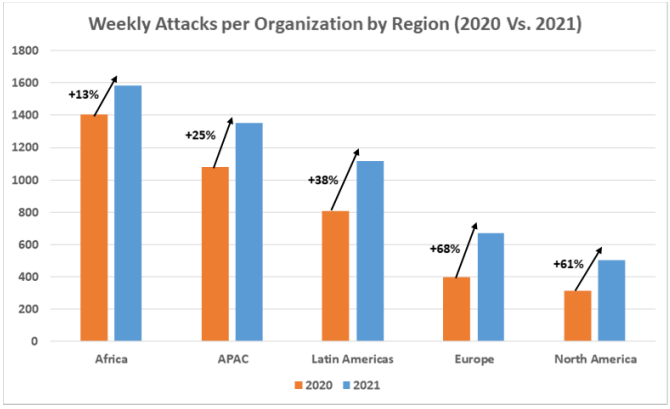


Διάγραμμα 1. Εκτιμώμενο κόστος των επιθέσεων ransomware (Humayun et al, 2022)

Αντίστοιχα παρατηρείται ότι ενώ υπήρξε μία πτώση το 2020 στο ποσό των λύτρων ανά περιστατικό το 2021 ξεπέρασε το ποσό των προηγούμενων ετών και είχε ένα μέσο όρο 6,500$.

Διάγραμμα 2. Εκτιμώμενο ποσό που πληρώθηκε σε λύτρα ανά περιστατικό[2]

Η μεγαλύτερη αύξηση των επιθέσεων το 2021 έναντι του 2020 παρατηρήθηκε στην Ευρώπη (+68%) και στη Βόρεια Αμερική (+61%).



Διάγραμμα 3. Εβδομαδιαία κατανομή επιθέσεων ανά ήπειρο (2020 / 2021)[3]

Σήμερα, πολλές βάσεις κλειδιών με κλειδιά αποκρυπτογράφησης αρχείων έχουν δημιουργηθεί στη προσπάθεια δημιουργίας μίας διεθνούς ομοσπονδίας από κρατικούς θεσμούς και ιδιωτικές επιχειρήσεις στο χώρο της ασφάλειας. Μία τέτοια βάση δεδομένων δημιουργεί σε ιστοσελίδα[4] της Europol. Μέχρι τώρα το αποθετήριο κλειδιών της Europol έχει βοηθήσει περισσότερους από έξι εκατομμύρια ανθρώπους να ανακτήσουν τα αρχεία τους χωρίς επιπλέον κόστος. Εκτιμάται ότι δεν καταβλήθηκαν με αυτό το τρόπο περίπου

[2] https://www.safetydetectives.com/blog/ransomware-statistics/
[3] https://blog.checkpoint.com/2022/01/10/check-point-research-cyber-attacks-increased-50-year-over-year/
[4] https://www.europol.europa.eu/media-press/newsroom/news/unhacked-121-tools-against-ransomware-single-website

ένα δισεκατομμύριο ευρώ στους επιτιθέμενους. Η ιστοσελίδα διαθέτει 121 εργαλεία ικανά να αποκρυπτογραφήσουν 151 οικογένειες ransomware και συνεργάζεται ήδη με 170 φορείς από τον δημόσιο και τον ιδιωτικό τομέα διαφόρων κρατών.

Κεφάλαιο 3 Ανατομία μίας επίθεσης ransomware – παραλλαγές επιθέσεων

Οι πρώτες έρευνες σχετικά με την υλοποίηση αποτελεσματικών μεθόδων ανίχνευσης κακόβουλου λογισμικού χρησιμοποιούν ένα συστημοκεντρικό μοντέλο συμπεριφοράς κατά το χρόνο εκτέλεσης (Lanzi, Balzarotti et al., 2010). Με αυτό τρόπο, λειτουργώντας στο επίπεδο του λειτουργικού συστήματος, κυρίως Windows, η παρακολούθηση των κλήσεων εισόδου/εξόδου του συστήματος μπορεί να παράγει πολύ λίγα έως μηδενικά ψευδώς θετικά αποτελέσματα ενώ μπορεί να ανιχνεύει κακόβουλες διεργασίες.

Τα αποτελέσματα αυτής της έρευνας έδειξαν ότι με την παρακολούθηση των κλήσεων εισόδου/εξόδου και των αλλαγών στο Master File Table είναι δυνατόν να ανιχνευτεί σημαντικός αριθμός επιθέσεων ransomware, και ακόμη και επιθέσεις Zero Day (Kharraz et al., 2015). Έχουν επίσης διεξαχθεί έρευνες στη χρήση ενός μοντέλου ανίχνευσης με επίκεντρο τα δεδομένα (Scaife et al., 2016), καθώς και στη χρήση δημιουργία ενός δείγματος ransomware για ερευνητικούς σκοπούς (Bazdarevic και Dubell).

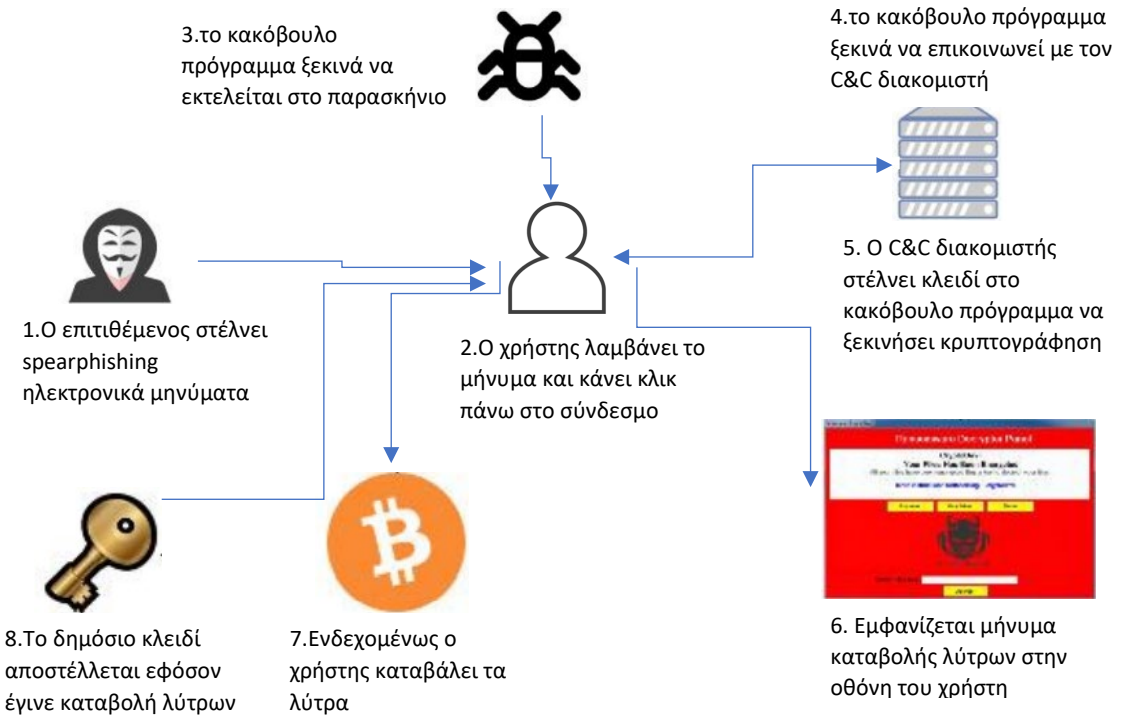
Αν και η έρευνα αυτή έχει τα πλεονεκτήματά της, δεν εξετάζει τα καθοριστικά χαρακτηριστικά στη συμπεριφορά του ransomware. Αυτές οι συμπεριφορές περιλαμβάνουν το κλείδωμα της επιφάνειας εργασίας, την παρεμπόδιση του θύματος να αποκτήσει πρόσβαση στο σύστημα, και στα μοτίβα πρόσβασης στο σύστημα αρχείων. Οι συμπεριφορές αυτές εξετάστηκαν από άλλους ερευνητές (Kharraz et al., 2016). Οι ερευνητές αναλύουν συνδυαστικά δεδομένα από την παρακολούθηση της κίνησης στο σύστημα αρχείων σε επίπεδο πυρήνα και, μία μετρική δομικής ομοιότητας εικόνων. Με τη δεύτερη μετρική συγκρίνουν στιγμιότυπα εικόνων που λαμβάνονται πριν και μετά την εκτέλεση ενός δείγματος ransomware για να αναζητήσουν το σημείωμα λύτρων που

εμφανίζεται στο θύμα. Η αναζήτηση του σημειώματος θα μπορούσε να είναι ένας από τους πιο αξιόπιστους τρόπους ανίχνευσης ransomware.

3.1 Ανατομία επίθεσης ransomware Κακόβουλα προγράμματα (malware)

Το Ransomware χρησιμοποιεί διάφορες τακτικές κοινωνικής μηχανικής για να κάνει το θύμα να φοβάται ότι θα πέσει θύμα πραγματικών συνεπειών (π.χ. καταβολή προστίμου, αντιμετώπιση σύλληψης και δίωξης), και η παράδοση ή η μόλυνση μπορεί να γίνει μέσω πολλαπλών φορέων επίθεσης, όπως exploitation kit, κακόβουλα αρχεία pdf, phishing και κακόβουλες διαφημιστικές εκστρατείες (Thomas, 2018). Το **Διάγραμμα** *4* απεικονίζει ένα τυπικό σενάριο επίθεσης ransomware.

Στις περισσότερες περιπτώσεις, το ransomware εισέρχεται στο σύστημα όταν ο χρήστης κάνει κλικ σε ένα phishing σύνδεσμο που λαμβάνει μέσω ηλεκτρονικού ταχυδρομείου. Μόλις ο χρήστης κάνει κλικ στον κακόβουλο σύνδεσμο, το κακόβουλο ωφέλιμο φορτίο μεταφορτώνεται στο παρασκήνιο και ξεκινά την εκτέλεσή του. Για να αποκρύψει την ταυτότητά του, το ransomware δεν εκτελείται ως αυτόνομη διαδικασία. Αντ' αυτού, χρησιμοποιεί ένα αρχείο υποδοχής, το λεγόμενο dropper file, το οποίο το βοηθά να κρύψει την ταυτότητά του. Για παράδειγμα, μπορεί να χρησιμοποιεί τη διεργασία εξερεύνησης των Windows μπροστά, αλλά στο παρασκήνιο, θα δημιουργήσει νόμιμη διαδικασία svchost που μοιάζει ψεύτικη. Εξασφαλίζει επίσης ότι συνεχίζει να εκτελείται σε μολυσμένα συστήματα, παραμένει σε όλες τις επανεκκινήσεις και εκτελείται ακόμη και αν το σύστημα εκκινηθεί σε "ασφαλή λειτουργία". Για να συνεχίσει να λειτουργεί παρά τις όποιες επανεκκινήσεις, κάνει προσθήκες σε κλειδιά μητρώου (στα Windows) και επίσης προσθέτει τον εαυτό του στις διαδικασίες εκκίνησης του συστήματος.



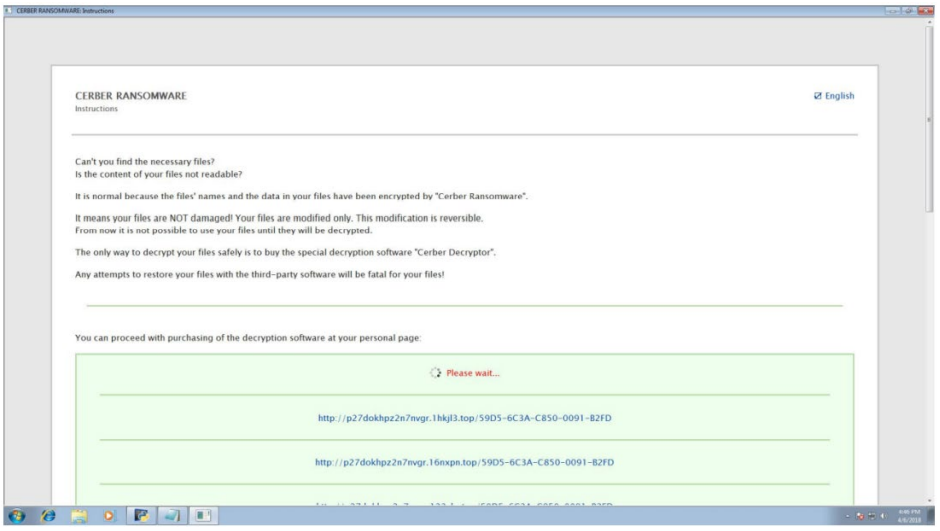
Διάγραμμα 4. Σενάριο επίθεσης ransomware

Αφού διεισδύσει στο μηχάνημα του θύματος, το ωφέλιμο φορτίο του ransomware θα επικοινωνήσει με το διακομιστή εντολών και ελέγχου (C&C), ο οποίος λειτουργεί εξ αποστάσεως από τον επιτιθέμενο. Ο διακομιστής C&C επικυρώνει την εισερχόμενη σύνδεση από το μολυσμένο μηχάνημα και παράγει ένα ζεύγος κλειδιών, αποτελούμενο από ένα δημόσιο κλειδί και ένα ιδιωτικό κλειδί. Το δημόσιο κλειδί αποστέλλεται στο payload του ransomware και χρησιμοποιείται για να κρυπτογραφηθούν τα αρχεία στο μολυσμένο μηχάνημα (Thomas, 2018). Προφανώς, τα αρχεία που έχουν κρυπτογραφηθεί με το δημόσιο κλειδί μπορούν να αποκρυπτογραφηθούν μόνο με τη χρήση του ιδιωτικού κλειδιού που βρίσκεται στον διακομιστή C&C. Οι επικοινωνίες μεταξύ του διακομιστή C&C και του μολυσμένου μηχανήματος διασφαλίζονται από ένα πρόγραμμα περιήγησης TOR.

Το ransomware δημιουργεί ένα νήμα για να κατεβάσει και να εγκαταστήσει τον πελάτη TOR για να κάνει την επικοινωνία με ανώνυμο τρόπο. Υπηρεσίες όπως το κέντρο ασφαλείας, οποιοδήποτε πρόγραμμα προστασίας από ιούς που προστατεύει το σύστημα, τα εργαλεία αναφοράς σφαλμάτων των Windows και οι ενημερώσεις των Windows απενεργοποιούνται μία προς μία (αντίστοιχα σε ένα σύστημα linux). Το κακόβουλο

λογισμικό διαγράφει επίσης όποια αντίγραφα ασφαλείας των Windows για να καταστήσει το σύστημα μη ανακτήσιμο.

Μόλις η διεργασία στο παρασκήνιο ολοκληρώσει την κρυπτογράφηση όλων των επιθυμητών αρχείων, δημιουργεί ένα μόνιμο παράθυρο στην επιφάνεια εργασίας του χρήστη που εμφανίζει ένα σημείωμα λύτρων, όπως φαίνεται στο **Διάγραμμα** *5*.



Διάγραμμα 5. Παράδειγμα ransom σημειώματος

Το σημείωμα του επιτιθέμενου ενημερώνει τον χρήστη ότι το μηχάνημά του έχει δεχθεί επίθεση και μπορεί να ανακτηθεί μόνο με την καταβολή λύτρων. Παρέχονται επίσης οι οδηγίες πληρωμής, και συνήθως, σε αυτές τις περιπτώσεις, αναφέρεται και μία διεύθυνση εικονικού νομίσματος για κάθε χρήστη για να καταστήσει τις συναλλαγές μη ανιχνεύσιμες (Kharraz et al, 2015).

Οι δημιουργοί κακόβουλου λογισμικού χρησιμοποιούν διαφορετικές τεχνικές για να μεταφορτώσουν ransomware στο εσωτερικό του δικτύου ενός οργανισμού, όπως παραβίαση του συστήματος μέσω διαδικτύου, drive-by download, phishing, εκμετάλλευση ευπαθειών, exploitation kit προγραμμάτων περιήγησης κ.α. Μερικές φορές το ransomware εξαπλώνεται με την εκμετάλλευση ευπαθειών σε ένα τοπικό δίκτυο.

Επίσης, τα πρότυπα αρχεία του Microsoft Word μπορούν να ενσωματώσουν μακροεντολές που μπορούν να εκτελέσουν κακόβουλες δραστηριότητες, όπως η λήψη κακόβουλου λογισμικού από απομακρυσμένες τοποθεσίες, και εκτέλεση εντολών στο backend (Kyurkchiev et al, 2018).

3.1.1 Παράδειγμα επίθεσης ransomware

Στην αρχή της εκτέλεσης του κακόβουλου λογισμικό, το εκτελέσιμο πρόγραμμα ransomware αντιγράφεται αμέσως στο %AppData% ή %LocalAppData% χρησιμοποιώντας τυχαίες συμβολοσειρές πεζών χαρακτήρων (π.χ., qwefghjkl.exe) (Kyurkchiev et al, 2018). Τα αρχεία των Windows μπορούν να ανακτηθούν από την ενσωματωμένη λειτουργία που παρέχεται από τα Windows που ονομάζεται shadow copy. Το ransomware ανιχνεύει τα shadow copies του σκληρού δίσκου των Windows στο σύστημα και τα διαγράφει για να καταστήσει τα δεδομένα του χρήστη μη ανακτήσιμα. Το Ransomware χρησιμοποιεί συχνά την παρακάτω εντολή για να διαγράψει τα shadow copies των windows:

%WinDir%\system32\vssadmin delete shadows /all

Το ransomware προσθέτει επίσης ορισμένα κλειδιά μητρώου στο Windows registry (στον χώρο του λειτουργικού συστήματος όπου διατηρούνται σημαντικές παράμετροι για την εκτέλεση προγραμμάτων) για να διατηρηθεί η κατάσταση του κακόβουλου λογισμικού σε όλες τις επανεκκινήσεις. Για να διασφαλίσει την πλήρη καταστροφή των αρχείων του συστήματος, το ransomware εκτελείται ακόμη και αν το σύστημα επανεκκινείται σε ασφαλή λειτουργία. Ένα παράδειγμα κλειδιού μητρώου είναι το ακόλουθο:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run "<random string>":"<full path to copied malware in %AppData%>"

Το Ransomware διασφαλίζει την παραμονή του ωφέλιμου φορτίου προσθέτοντας ένα κλειδί μητρώου, μια εργασία στο πρόγραμμα χρονοπρογραμματισμού εργασιών των Windows ή αντιγράφοντας τον εαυτό του σε μια διαδικασία εκκίνησης του λειτουργικού συστήματος. Το Ransomware μπορεί επίσης να θέσει σε κίνδυνο τη διαδικασία εκκίνησης

του λειτουργικού συστήματος. Πιο έξυπνες εκδόσεις ransomware θα προσπαθήσουν να εκτελεστούν χωρίς να γίνουν ανιχνεύσιμα από το αντι-ικό πρόγραμμα του υπολογιστή, για παράδειγμα, εισχωρώντας σε μια νόμιμη διεργασία και εκτελώντας τη από τον κατάλογο %AppData% χρησιμοποιώντας το τυπικό όνομα του εκτελέσιμου αρχείου των Windows.

Το Ransomware απαιτεί σύνδεση στο Internet για να κατεβάσει αρχεία που σχετίζονται με το ωφέλιμο φορτίο και να επικοινωνούν με τον διακομιστή εκτέλεσης εντολών και ελέγχου (C&C) για τα κλειδιά κρυπτογράφησης. Το Ransomware χρησιμοποιεί επίσης το δίκτυο ανωνυμίας TOR για να φιλοξενήσει έναν διακομιστή πληρωμών και να διευκολύνει τη πληρωμή των λύτρων με μη ανιχνεύσιμο τρόπο. Ορισμένα ransomware χρησιμοποιούν αλγορίθμους παραγωγής χιλιάδων διευθύνσεων στο διαδίκτυο (Domain Generation Algorithms - DGA) ημερησίως, προκειμένου να μπερδέψουν τα συστήματα ανίχνευσης και τους αναλυτές.

Μετά τη σύνδεση με τον διακομιστή C&C μέσω HTTP, η ανταλλαγή δημόσιου κλειδιού γίνεται μεταξύ του διακομιστή και του μολυσμένου μηχανήματος. Αυτή η επικοινωνία είναι συχνά κρυπτογραφημένη με SSL. Οι επιτιθέμενοι χρησιμοποιούν δικούς τους διακομιστές που βρίσκονται σε διαφορετικούς παρόχους υπηρεσιών διαδικτύου, οι οποίοι συχνά βρίσκονται στις χώρες του ανατολικού μπλοκ (π.χ. Ρωσία, Κίνα). Μερικές φορές, αυτοί οι διακομιστές C&C φιλοξενούνται σε νόμιμες υποδομές που διαχειρίζονται τρίτοι όπως η Amazon (Gibson and Banik, 2017).

Η διαδικασία κρυπτογράφησης ξεκινά μετά την επιτυχή επικοινωνία με τον διακομιστή C&C. Μέσα από αυτή την επικοινωνία ο διακομιστής παρέχει το δημόσιο κλειδί, το οποίο χρησιμοποιείται σε όλη τη διαδικασία κρυπτογράφησης. Οι περισσότερες από τις κατηγορίες ransomware χρησιμοποιούν πιστοποιημένα κρυπτοσυστήματα που προσφέρονται από το CryptoAPI της Microsoft, όπως το RSA και το AES. Για την κρυπτογράφηση των δεδομένων, αυτές οι οικογένειες χρησιμοποιούν τις μεθόδους RSA (CALG_RSA_KEYX) και τους αλγόριθμους AES (CALG_AES-256). Σε αυτή την περίπτωση, το ransomware καλεί το API των Windows (δηλ, GetLogicalDrive()) για την απαρίθμηση του αποθηκευτικού χώρου στους δίσκους του συστήματος. Το ransomware σαρώνει αναδρομικά όλους τους καταλόγους που παρατίθενται και επεξεργάζεται κάθε αρχείο για κρυπτογράφηση.

Υπάρχουν 3 κατηγορίες ransomware ανάλογα με τον τρόπο με τον οποίο επεξεργάζονται ένα αρχείο: κατηγορία Α, κατηγορία Β και κατηγορία C (Scaife et al, 2016). Στη Κατηγορία Α το ransomware ανοίγει το αρχικό αρχείο και αντικαθιστά αμέσως το περιεχόμενό του με κρυπτογραφημένα δεδομένα. Στη κατηγορία Β το ransomware μετακινεί πρώτα το αρχείο σε κάποια τυχαία τοποθεσία, κρυπτογραφεί το αρχείο όπως στην κατηγορία Α και στη συνέχεια μετακινεί το κρυπτογραφημένο αρχείο πίσω στην αρχική του θέση. Στη κατηγορία C το ransomware διαβάζει το αρχικό αρχείο, κρυπτογραφεί το περιεχόμενο του αρχείου, γράφει το κρυπτογραφημένο περιεχόμενο σε ένα νέο αρχείο και διαγράφει το αρχικό αρχείο.

Τα κρυπτογραφημένα δεδομένα αντικαθιστούν τα αρχικά δεδομένα στο σύστημα αρχείων, γεγονός που μειώνει την πιθανότητα της ανάκτησης αρχείων με τη χρήση εργαλείων έρευνας (forensics). Για λόγους καταγραφής των δεδομένων για μελλοντική χρήση, ο κατάλογος των κρυπτογραφημένων αρχείων αποθηκεύεται σε αρχεία HTML, αρχεία κειμένου ή ως κλειδιά μητρώου. Ενώ περνάει από κάθε κατάλογο, το ransomware δημιουργεί επιπρόσθετα αρχεία, τα οποία ενημερώνουν το χρήστη για τη πληρωμή λύτρων.

Μερικές φορές, συγκεκριμένες επεκτάσεις αρχείων είναι στόχος της επίθεσης, συνήθως το Microsoft Office, τα αρχεία πολυμέσων, τα αρχεία Adobe Photoshop και άλλα. Τέτοιες αντιπροσωπευτικές επεκτάσεις αρχείων παρουσιάζονται στον παρακάτω πίνακα:

*.docm	*.docx	*.doc	*.odb	*.odm	*.odp	*.ods	*.odt
*.pptx	*.ppt	*.xlk	*.xlsb	*.xlsm	*.xlsx	*.xls	*.wps
*.wpd	*.dxg	*.dxf	*.dwg	*.pst	*.accdb	*.mdb	*.pptm
*.ai	*.eps	*.pdd	*.psd	*.dbf	*.mdf	*.wb2	*.rtf
*.arw	*.3fr	*.dng	*.jpg	*.jpe	img_*.jpg	*.cdr	*.indd
*.erf	*.kdc	*.dcr	*.cr2	*.crw	*.bay	*.sr2	*.srf
*.rwl	*.raw	*.raf	*.orf	*.nrw	*.nef	*.mrw	*.mef

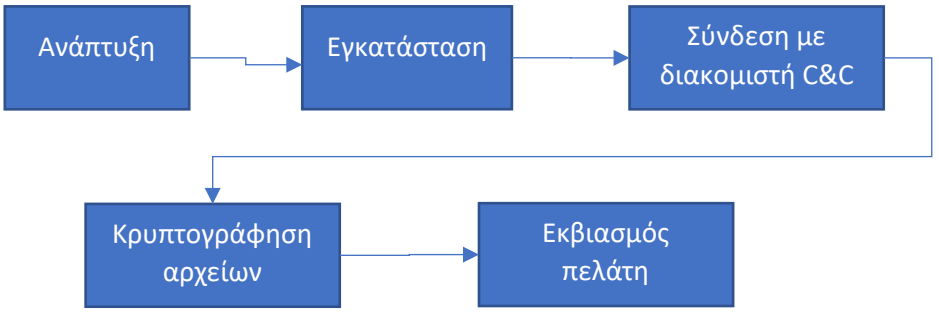
*.cer	*.der	*.x3f	*.srw	*.pef	*.ptx	*.r3d	*.rw2
*.odc	*.pdf	*.p7c	*.p7b	*.p12	*.pfx	*.pem	*.crt

Πίνακας 1. Καταλήξεις αρχείων που γίνονται στόχος επιθέσεων ransomware (Kyurkchiev et al, 2019)

Το εικονικό νόμισμα είναι πλέον μια καθιερωμένη μέθοδος πληρωμής ransomware. Οι περισσότερες από τις εκδόσεις ransomware απαιτούν λύτρα περίπου 1,5 Bitcoins. Μερικές φορές, προτιμούν επίσης προπληρωμένες κάρτες, ή άλλες μεθόδους (Kyurkchiev et al, 2019). Όλες οι συναλλαγές είναι δημόσιες εκ των προτέρων. Μερικές φορές περιλαμβάνουν επίσης οδηγίες για αγορά Bitcoins από ανταλλακτήριο. Καταχωρείται μία μοναδική διεύθυνση bitcoin για κάθε χρήστη, ώστε να κοινοποιηθεί στο θύμα και να χρησιμοποιηθεί κατά την πληρωμή. Επιπλέον, η ανακοίνωση για την απαίτηση λύτρων περιλαμβάνει επίσης τις σχετικές διευθύνσεις. Όπως αναφέραμε παραπάνω, ο χρήστης θα πρέπει να στείλει σε σχετική διεύθυνση το hash της πληρωμής των λύτρων ως απόδειξη για την αποκρυπτογράφηση των αρχείων.

3.2 Μοντέλο επίθεσης ransomware – βασικά χαρακτηριστικά

Ένα τυπικό μοντέλο επίθεσης ransomware περιλαμβάνει τις ακόλουθες φάσεις: Ανάπτυξη, εγκατάσταση του εκτελέσιμου προγράμματος στο σύστημα, σύνδεση με διακομιστή C&C, κρυπτογράφηση αρχείων και εκβιασμός του χρήστη. Στη βιβλιογραφία έχουν προσδιοριστεί ένα συγκεκριμένο σύνολο χαρακτηριστικών από την ανάλυση της συμπεριφοράς του ransomware όπως φαίνεται παρακάτω (**Διάγραμμα** *6***Διάγραμμα** *6.*).



Διάγραμμα 6. Μοντέλο επίθεσης ransomware- κύρια χαρακτηριστικά

Οι επιθέσεις Ransomware ακολουθούν το παραπάνω μοτίβο κάτι που έχει παρατηρηθεί σε κάθε οικογένεια και παραλλαγή του ransomware. Σε γενικές γραμμές, η επίθεση ransomware εξαπολύεται σε τρεις φάσεις: προ-κρυπτογράφηση, κρυπτογράφηση και μετα-κρυπτογράφηση

- Εύρεση στόχου
- Διείσδυση του φορέα μόλυνσης
- Εγκατάσταση ransomware λογισμικού
- Δημιουργία και ανάκτηση κλειδιών κρυπτογράφησης
- Πρόσβαση σε αρχεία του χρήστη
- Κρυπτογράφηση
- Λειτουργίες μετά την κρυπτογράφηση
- Απαίτηση λύτρων

API calls

Το λειτουργικό σύστημα των Windows παρέχει ένα σύνολο προγραμματιστικών διεπαφών που απλοποιούν τη διαδικασία χρήσης των API των Windows και επιτρέπει στους προγραμματιστές ελεύθερα να επικεντρωθούν στη λογική του δικού τους προγράμματος λογισμικού. Στη βιβλιογραφική έρευνα παρατηρείται ότι οι περισσότερες παραλλαγές ransomware χρησιμοποιούν τα τυπικά API κρυπτογράφησης των Windows για την κρυπτογράφηση των αρχείων. Ως εκ τούτου, η μελέτη των κλήσεων API των

Windows διαδραματίζει ζωτικό ρόλο στην ανάλυση συμπεριφοράς των επιθέσεων τύπου ransomware.

Όταν το σύστημα δέχεται επίθεση ransomware, σημαντικές αλλαγές λαμβάνουν χώρα στο σύστημα αρχείων σε πολύ σύντομο χρονικό διάστημα (κρυπτογράφηση πολλαπλών αρχείων, μαζικές διαγραφές). Ο καλύτερος τρόπος για να αποκτήσει κάποιος πρόσβαση ή να τροποποιήσει αρχεία στο λειτουργικό σύστημα Windows είναι μέσω του API των Windows. Για παράδειγμα, όταν γίνεται η κλήση συστήματος "FileOpen", το λειτουργικό σύστημα εκτελεί μια σειρά από εντολές με την ακόλουθη σειρά (Hampton et al, 2018).

1. Αρχικά, θα εντοπίσει το αρχείο, θα ελέγξει τα δικαιώματα πρόσβασης του αρχείου και θα επιστρέψει ένα δείκτη χειρισμού του αρχείου πίσω στη συνάρτηση κλήσης.
2. Το ransomware μπορεί να αντικαταστήσει το αρχείο με μία κρυπτογραφημένη έκδοση ή θα προχωρήσει σε ασφαλή διαγραφή του αρχείου χρησιμοποιώντας το σχετικό API (Secure Deletion).
3. Το ransomware ξεκινά τη διαδικασία κρυπτογράφησης χρησιμοποιώντας την συνάρτηση του API GetLogicalDrives() για να απαριθμήσει τις μονάδες δίσκου στο σύστημα και
4. ολοκληρώνει την εκτέλεση του καλώντας τη συνάρτηση CreateDesktop() του API για τη δημιουργία ενός σημειώματος σχετικά με την καταβολή λύτρων.

Ερευνητές που κάνανε ανάλυση των API κλήσεων αποκάλυψαν ότι οι API κλήσεις που σχετίζονται με δραστηριότητες του συστήματος αρχείων χρησιμοποιούνται σε μεγάλο βαθμό από ransomware σε σύγκριση με κανονικά αρχεία. Ορισμένες κλήσεις του API υπάρχουν μόνο σε προγράμματα ransomware. Ορισμένες κλήσεις του API είναι παρούσες τόσο σε κανονικά όσο και σε προγράμματα ransomware, αλλά η συχνότητα χρήσης τους ποικίλλει τόσο σε φυσιολογικές όσο και σε ransomware εφαρμογές. Αναλυτές παρατηρήσανε επίσης ότι δεν χρησιμοποιούν όλες οι οικογένειες ransomware τις ίδιες κλήσεις API για να επιτύχουν το στόχο τους. Ο παρακάτω πίνακας (Πίνακας 2) παρουσιάζει την αντιστοιχία API κλήσεων ανά αντιπροσωπευτική οικογένεια ransomware .

Οικογένεια Ransomware \ Windows Api Calls	**CTBLocker**	**Cerber**	**CryptoMix**	**CryptoShield**	**Crysis**	**Flawed**	**GlobeImposter**	**Jaff**	**Locky**	**Mole**	**Petya**	**Sage**	**Satan**	**Spora**	**Striked**	**TeslaCrypt**	**Unlock26**	**WannaCry**	**Win32.Blocker**	**Xorist**	**zeta**
MoveFileWithProgressW		x			X				x				x			x		x			
FindResourceExW	x	x							x	x		x	x		x	x	x				x
CreateDirectoryW	x	x							x	x	x	x	x	x	x	x	x	x	x		
RemoveDirectoryW																x					
LoadResource	x	x			x	x			x	x	x	x	x	x		x	x	x			x
GetSystemWindowsDirectoryW	x	x			x	x	x		x	x		x	x	x		x	x	x	x		
RegQueryValueExW	x	x			x	x	x		x	x	x	x	x	x	x	x	x	x	x		x
SizeofResource	x	x			x				x		x	x		x		x	x	x			x
NtWriteFile	x	x			x				x	x	x	x	x	x	x	x	x	x	x	X	
FindWindowExA	x	X																			
NtCreateFile	x	x			x	x	x		x	x	x	x	x	x	x	x	x	x	x	x	
GetFileAttributesW	x	x			x		x		x	x	x	x	x	x	x	x	x	x	x	x	
GetFileSize	x	x							x			x	x	x		x	x	x		X	
RegOpenKeyExA	x	X							x	x	x	x	x	x		x	x	x	x		x

Πίνακας 2. Κατανομή των Windows API κλήσεων ανά οικογένεια Ransomware (Hampton et al, 2018)

Εντροπία αρχείων

Η εντροπία στα ψηφιακά συστήματα είναι ένα μέτρο της τυχαιότητας σε ένα αρχείο (Lee et al, 2019). Ένα αρχείο συμπιέζεται με την αντικατάσταση μεγάλων μοτίβων από 0-1 τιμές (bit) με μικρότερα μοτίβα των 0-1 τιμών. Τα συμπιεσμένα και τα κρυπτογραφημένα αρχεία έχουν υψηλό βαθμό τυχαιότητας. Ο Shannon παρείχε έναν τύπο για τον

υπολογισμό του θεωρητικού μέγιστου ποσού για τη συμπίεση ψηφιακών αρχείων. Σύμφωνα με τον Shannon, η μέγιστη εντροπία συμβαίνει όταν όλα τα bytes κατανέμονται εξίσου στο αρχείο.

Η τιμή της εντροπίας είναι ένας υπολογισμός της προβλεψιμότητας του επόμενου χαρακτήρα στο αρχείο με βάση τους προηγούμενους χαρακτήρες. Μετράται σε κλίμακα από το 1 έως το 8, όπου τα κρυπτογραφημένα και συμπιεσμένα αρχεία έχουν υψηλή τιμή, ενώ τα τυπικά αρχεία με κείμενο έχουν χαμηλή τιμή. Ο τύπος της εντροπίας του Shannon επιτρέπει τον υπολογισμό του μέσου ελάχιστου αριθμού των bits που απαιτούνται για την κωδικοποίηση της συμβολοσειράς με βάση τη συχνότητα των συμβόλων και το μέγεθος του αλφάβητου. Η Εντροπία Shannon H δίνεται από τον παρακάτω τύπο (Lee et al, 2019):

$$H = -\sum_{i} p_i \log_2 p_i$$

Όπου pi είναι η πιθανότητα εμφάνισης του χαρακτήρα i στη ροή αλφαβήτου.

Για να υπολογίσουμε την εντροπία ενός αρχείου, υπολογίζουμε τη συχνότητα όλων των χαρακτήρων ASCII, οι οποίοι περιλαμβάνουν τυπικούς χαρακτήρες ASCII (0-127) και εκτεταμένους χαρακτήρες ASCII (128-255), σε ένα δεδομένο αρχείο, και στη συνέχεια χρησιμοποιείται ως πιθανότητα στον τύπο της εντροπίας Shannon.

Υπογραφή αρχείου

Τύποι φυσιολογικών αρχείων, όπως το MS Office, το 7-zip, τα αρχεία pdf είναι επίσης εξαιρετικά συμπιεσμένα και έχουν υψηλή τιμή εντροπίας. Επομένως, ο υπολογισμός της εντροπίας ενός αρχείου από μόνος του δεν βοηθά στη διάκριση μεταξύ κρυπτογράφησης που εκτελείται από τον χρήστη και κρυπτογράφησης που εκτελείται από ransomware. Ωστόσο, οι περισσότεροι τύποι αρχείων έχουν μια επικεφαλίδα, που ονομάζονται επίσης υπογραφή του αρχείου, μέσω του οποίου μπορεί να προσδιοριστεί η πραγματική μορφή του αρχείου (Aslan and Samet, 2020).

Για παράδειγμα, τα αρχεία εικόνας JPEG αρχίζουν με "FF D8" και τελειώνει με "FF D9". Οι υπογραφές αρχείων είναι τα πρώτα bytes ενός αρχείου που είναι διαφορετικά για κάθε τύπο αρχείου. Αυτά τα bytes χρησιμοποιούνται από το λειτουργικό σύστημα για να αναγνωρίσει τα αρχεία χωρίς να εξαρτάται από την επέκταση του αρχείου. Η υπογραφή ενός αρχείου δεν είναι ορατή στους χρήστες, αλλά με τη χρήση ενός επεξεργαστή δεκαεξαδικών χαρακτήρων, μπορεί να γίνει ορατή. Η αλλαγή ή η αλλοίωση αυτών των bytes καθιστά ένα αρχείο άχρηστο, καθώς είναι απαραίτητα για να ανοιχτεί ένα αρχείο από μία συμβατή εφαρμογή. Ο Πίνακας 3 παρουσιάζει τις υπογραφές για αντιπροσωπευτικούς τύπους αρχείων.

Κατάληξη	**Υπογραφή**	**Περιγραφή**
DOCX	50 4B 03 04	MS Office Open XML Format Document
7Z	37 7A BC AF 27 1C	7-zip compressed file
PDF	25 50 44 46	PDF file
RAR	52 61 72 21 1A 07 00	WinRAR compressed archive
TAR	75 73 74 61 72	Tape Archive

Πίνακας 3. Υπογραφές για αντιπροσωπευτικούς τύπους αρχείων

Συνδυάζοντας τα δύο χαρακτηριστικά της εντροπίας και της υπογραφής των αρχείων, υπάρχουν δύο ισχυρά χαρακτηριστικά του ransomware που αναλύονται παρακάτω:

1. Το Ransomware συνήθως κρυπτογραφεί ολόκληρο το αρχείο, πράγμα που σημαίνει ότι καταστρέφει επίσης την υπογραφή του αρχείου.

2. Το Ransomware εφαρμόζει γενικά έναν βασικό αλγόριθμο κρυπτογράφησης στα αρχεία. Ως αποτέλεσμα αυτής της διαδικασίας, η εντροπία του αρχείου θα είναι πολύ υψηλή.

Επομένως, τα χαρακτηριστικά που προκύπτουν από το συνδυασμό της υπογραφής του αρχείου και της εντροπίας του αρχείου μπορούν να βοηθήσουν αποτελεσματικά στον εντοπισμό κρυπτογράφησης που προκαλείται από ransomware.

Λειτουργίες διαχείρισης των κλειδιών στο μητρώο του υπολογιστή

Το μητρώο των Windows είναι μια ιεραρχική βάση δεδομένων που χρησιμοποιείται στα λειτουργικά συστήματα των Windows για τη κεντρική διαχείριση των παραμετροποιήσεων και των ρυθμίσεων του συστήματος και των επιμέρους εφαρμογών (Singh et al, 2019). Τα δεδομένα είναι δομημένα σε μορφή κλειδιού-τιμής όπου κάθε κλειδί μπορεί να έχει οποιονδήποτε αριθμό τιμών και οι τιμές μπορούν να έχουν οποιαδήποτε μορφή (π.χ. αριθμητική, συμβολοσειρά, κ.λπ.). Κάθε φορά που ο χρήστης εγκαθιστά οποιοδήποτε πρόγραμμα λογισμικού, οι αρχικές ρυθμίσεις αποθηκεύονται ως ζεύγη κλειδιών-τιμών στο μητρώο. Όταν ένας χρήστης εκτελεί το λογισμικό, τα στοιχεία του συστήματος ανακτούν τις ρυθμίσεις τους κατά τον χρόνο εκτέλεσης από τη βάση δεδομένων του μητρώου.

Ένα πρόγραμμα λογισμικού εκτελεί τέσσερις τύπους λειτουργιών ανάγνωσης, εγγραφής, τροποποίησης, διαγραφής (CRUD) κλειδιών στο μητρώο για να διατηρήσει τη μονιμότητα της εκτέλεσης του σε όλες τις επανεκκινήσεις του υπολογιστή. Οι λειτουργίες CRUD πάνω στα κλειδιά του μητρώου μπορούν να είναι μοναδικές ανά λογισμικό.

Εντολές στη γραμμή εκτέλεσης των Windows

Η γραμμή εντολών είναι μια εφαρμογή που είναι διαθέσιμη στα Windows. Χρησιμοποιείται γενικά για την αυτοματοποίηση των εργασιών, την αντιμετώπιση προβλημάτων σε θέματα λειτουργικού συστήματος ή να εκτελεί διαχειριστικές λειτουργίες. Για παράδειγμα, για να εμφανίσει ο χρήστης όλα τα αρχεία και καταλόγους που υπάρχουν σε οποιαδήποτε συγκεκριμένη τοποθεσία, ο χρήστης μπορεί να εκτελέσει

την εντολή 'dir'. Δεδομένου ότι οι περισσότεροι χρήστες χρησιμοποιούν γραφικό περιβάλλον χρήστη για ευκολία, ένα ransomware αξιοποιεί, στο παρασκήνιο, ένα τμήμα του λειτουργικού συστήματος με το οποίο οι χρήστες υπολογιστών σπάνια έρχονται σε επαφή. Το ransomware χρησιμοποιεί αυτή τη λειτουργικότητα για να επιτύχει στόχους όπως η διαγραφή του master boot record, ή διαγραφή του σκιώδους αντιγράφου των windows.

Βιβλιοθήκες (DLLs) των Windows

Μια βιβλιοθήκη δυναμικής σύνδεσης (DLL) είναι ένα πρόγραμμα που αποτελείται από συναρτήσεις και δεδομένα που μπορούν να χρησιμοποιούνται από άλλη εφαρμογή για λόγους επαναχρησιμοποίησης του κώδικα. Εκτελέσιμα των Windows ή προγράμματα μπορεί να περιέχουν διαφορετικές ενότητες, και κάθε ενότητα του προγράμματος που αναπτύσσεται διανέμεται και περιέχεται σε DLL. Με τη χρήση DLLs, οι προγραμματιστές μπορούν να αναπτύσσουν αρθρωτές εφαρμογές και η λειτουργικότητα τους μπορεί να επαναχρησιμοποιηθεί και να ενημερωθεί με εύκολο τρόπο. Τα API των Windows υλοποιούνται στο σύνολο τους ως DLL αρχεία. Στο παρασκήνιο, όλα τα API των Windows χρησιμοποιούν βιβλιοθήκες δυναμικής σύνδεσης. Συνήθως τα προγράμματα ransomware κάνουν χρήση αρκετών από αυτές τις βιβλιοθήκες (Kao et al, 2019).

Απαρίθμηση φακέλων των Windows

Κατά τη διαδικασία της κρυπτογράφησης το ransomware περνάει από όλους τους φακέλους ή ένα επιλεγμένο υποσύνολο του συστήματος αρχείων για την κρυπτογράφηση των αρχείων (Sgandurra et al, 2016). Κατά τη διάρκεια αυτής της εκτέλεσης, ο αριθμός των αλλαγών που εμφανίζονται σε επίπεδο φακέλου είναι πολύ υψηλός, επειδή το ransomware προσπαθεί να κρυπτογραφήσει όσο το δυνατόν περισσότερα αρχεία.

Mutex

Το mutex είναι ένα αντικείμενο προγράμματος που χρησιμοποιείται γενικά από ένα κακόβουλο λογισμικό ως μηχανισμός κλειδώματος για την αποφυγή ταυτόχρονης

πρόσβασης σε έναν πόρο του συστήματος (SophosLabs Research Team, 2019). Χρησιμοποιείται επίσης στον παράλληλο προγραμματισμό για να επιτρέψει σε πολλαπλά νήματα κώδικα να μοιράζονται τους ίδιους πόρους και να αποφεύγεται η μόλυνση του συστήματος περισσότερες από μία φορές. Για παράδειγμα, μόλις το κακόβουλο λογισμικό μολύνει το σύστημα, το πρώτο βήμα που κάνει είναι να λάβει ένα δείκτη χειρισμού σε ένα "ονομαστικό" mutex. Εάν η διαδικασία αποτύχει, το κακόβουλο λογισμικό εγκαταλείπει τον κώδικα.

Το mutex είναι συμβολοσειρές χαρακτήρων. Το λογισμικό προστασίας από ιούς που βασίζεται σε στατικές τεχνικές ανίχνευσης κακόβουλου λογισμικού αναζητά τα προηγούμενα γνωστά ονόματα mutex για να ελέγξει την ύπαρξη του κακόβουλου λογισμικού στο σύστημα. Για να αποφύγει την ανίχνευση, μερικές φορές κάποιο κακόβουλο λογισμικό αποφεύγει τη χρήση κοινών ονομάτων mutex και δυναμικά δημιουργεί mutexes κατά την εκτέλεση. Το ransomware χρησιμοποιεί επίσης αυτή τη λειτουργία για να αποφύγει τη μόλυνση του συστήματος περισσότερες από μία φορές.

Ενσωματωμένες συμβολοσειρές

Οι συμβολοσειρές είναι ακολουθίες χαρακτήρων ASCII και Unicode ενσωματωμένες στο εκτελέσιμο πρόγραμμα του ransomware. Η εξαγωγή της συμβολοσειράς από τη δυαδική μορφή του προγράμματος λογισμικού μπορεί να δώσει μια ένδειξη σχετικά με τη λειτουργικότητα του προγράμματος. Για παράδειγμα, εάν το κακόβουλο λογισμικό προσπαθήσει να επιλύσει το όνομα τομέα, μπορεί να αποθηκευτεί ως συμβολοσειρά στο εκτελέσιμο αρχείο. Μπορεί επίσης να δώσει σημαντικές πληροφορίες όπως διευθύνσεις IP, ονόματα αρχείων, λειτουργίες πάνω σε κλειδιά του μητρώου κ.λπ.

Άλλα χαρακτηριστικά

Το Ransomware εμφανίζει επίσης ορισμένα κοινά χαρακτηριστικά κακόβουλου λογισμικού, όπως ο έλεγχος των συντομεύσεων του πληκτρολογίου, αλλαγές στην ακολουθία εκκίνησης, κλοπή πληροφοριών από προγράμματα περιήγησης κ.λπ. Μερικά από τα πιο σημαντικά μεταξύ αυτών των χαρακτηριστικών παρουσιάζονται παρακάτω:

- Εντροπία κώδικα: Για να παρακάμψουν την ανίχνευση υπογραφών, οι προγραμματιστές του κακόβουλου λογισμικού χρησιμοποιούν τεχνικές απόκρυψης κώδικα (Kancherla et al, 2016). Υψηλές τιμές εντροπίας σε εκτελέσιμα αρχεία υποδεικνύουν τυχαία κατανομή των bytes, μια διαδεδομένη ιδιότητα σε συμπιεσμένα και κρυπτογραφημένα δεδομένα όπως αναφέραμε παραπάνω. Η υψηλή εντροπία είναι ένα από τα μέτρα για την ανίχνευση κακόβουλων εκτελέσιμων αρχείων.

- BCDEdit: Το BCDEdit είναι ένα εργαλείο γραμμής εντολών που είναι διαθέσιμο σε λειτουργικά συστήματα Windows, για τη διαχείριση δεδομένων παραμετροποίησης της διαδικασίας εκκίνησης. Το BCDEdit μπορεί να χρησιμοποιηθεί για διάφορους σκοπούς, όπως η προσθήκη μιας νέας μενού επιλογής κατά την εκκίνηση, δημιουργία νέου αποθηκευτικού χώρου, τροποποίηση υπάρχοντος αποθηκευτικού χώρου. Μερικές από τις παραλλαγές ransomware χρησιμοποιούν αυτή την επιλογή από τη γραμμή εντολών για να αλλάξουν τις επιλογές του μενού εκκίνησης (Bettany and Halsey, 2017).

- Διαγραφή του σκιώδους αντιγράφου των Windows: Το ransomware διαγράφει όλα τα αρχεία αντιγράφων ασφαλείας του συστήματος για να βεβαιωθεί ότι τα αρχεία δεν μπορούν να ανακτηθούν μετά την κρυπτογράφηση.

3.2.1 Στοχοποίηση χρηστών – κατηγορίες

Οι επιθέσεις τύπου ransomware έχουν κυρίως οικονομικά κίνητρα, οπότε η επιλογή των χρηστών που θα στοχεύσουν οι επιτιθέμενοι λαμβάνονται υπόψη σε όποια τέτοια απόφαση. Αρχικά, οι επιτιθέμενοι δεν εκτελούσαν επιθέσεις ransomware έχοντας υπόψη μία συγκεκριμένη κατηγορία χρηστών. Αντί αυτού επιλέγανε να στοχεύσουν σε ένα ευρύτερο προφίλ χρηστών(Savage et al, 2015). Αυτή η προσέγγιση λειτουργούσε αξιοποιώντας την τεράστια μάζα χρηστών στο διαδίκτυο με σκοπό να εισπράττουν σχετικά μικρά λύτρα από πολλά θύματα.

Με ένα μόνο ιό ransomware που εγκαθίσταται σε εκατομμύρια χρήστες παγκοσμίως αρκεί τότε μόνο ένα μικρό κλάσμα των χρηστών να πληρώσουν τα λύτρα για να κάνει

αυτό το σύστημα κερδοφόρο. Τα τελευταία χρόνια όμως, οι επιτιθέμενοι έχουν εστιάσει στη συλλογή μεγάλων ποσόν από λιγότερα θύματα. Έτσι αντί να στοχεύουν σε μεμονωμένα άτομα, επικεντρώνονται πλέον περισσότερο στη στόχευση επιχειρήσεων και οργανισμών.

Οι οικιακοί χρήστες έχουν δεχθεί επιθέσεις ransomware περισσότερο από ότι οι οργανισμοί. Το ransomware είχε επίπτωση κατά των οικιακών χρηστών για τρεις βασικούς λόγους. Πρώτον, επειδή σε ατομικό επίπεδο η τεχνική βοήθεια από τρίτους είναι ελάχιστη έως μηδαμινή. Δεύτερον, μεγάλο μέρος των χρηστών δεν είναι εξοικειωμένοι με την τεχνολογία. Και τρίτον, πολλοί λίγοι χρήστες είναι εξοικειωμένοι με το ransomware. Λαμβάνοντας υπόψη τους παραπάνω τρεις βασικούς λόγους, μπορεί κανείς να φανταστεί πώς ο οικιακός χρήστης – θύμα μπορεί να αισθάνεται αβοήθητος, φοβισμένος και αγχωμένος όταν ανακαλύψει την έκταση της επίθεσης.

Οι επιτιθέμενοι γνωρίζουν για αυτή τη ψυχολογική κατάσταση του χρήστη κάτι που τους δίνει μεγαλύτερες πιθανότητες να εισπράξουν λύτρα, και ως εκ τούτου, χειραγωγούν αυτά τα συναισθήματα ως μέρος μίας πρακτικής που είναι γνωστή ως κοινωνική μηχανική (Savage et al, 2015). Οι οικιακοί χρήστες έχουν συναισθηματικό δέσιμο με τα δεδομένα που έχουν κρυπτογραφηθεί επειδή μπορεί να αφορούν προσωπικά αρχεία με σημαντικές πληροφορίες και σημαντικά έγγραφα, φωτογραφικό υλικό από το αρχείο της οικογένειας, κλπ.

Τα τελευταία χρόνια, οι επιτιθέμενοι έχουν ως στόχο επιχειρήσεις και οργανισμούς, όπως εκπαιδευτικά ιδρύματα, ιατρικά ιδρύματα, κρατικές υπηρεσίες, εταιρίες διαχείρισης ενεργειακών πόρων, κ.λπ. Σε αντίθεση με ένα μεμονωμένο χρήστη, οι οργανισμοί έχουν πρόσβαση σε πολύ περισσότερους πόρους.

Αυτοί οι πόροι επιτρέπουν στους οργανισμούς να υλοποιούν μηχανισμούς ασφάλειας για την προστασία των δεδομένων, και άλλων περιουσιακών τους στοιχείων. Προσλαμβάνουν εξειδικευμένο προσωπικό που έχει τη κατάρτιση να ρυθμίσει συστήματα ασφάλειας για την προληπτική αντιμετώπιση και αποτροπή επιθέσεων.

Οι οργανισμοί μπορούν επίσης να αγοράσουν ασφαλιστικό πρόγραμμα ransomware για τον μετριασμό του οικονομικού κινδύνου μίας τέτοιας επίθεσης. Σε μία έρευνα που έγινε το 2020, το 84% των οργανισμών είχαν ένα τέτοιο ασφαλιστικό πρόγραμμα, και το 80% αυτών των πολιτικών περιλαμβάνουν το ransomware ως κάλυψη (Greengard, 2021).

Ωστόσο, τα δεδομένα μπορούν ακόμη να κλαπούν από τα συστήματα της επιχείρησης και να δεχθούν απειλές περί δημοσιοποίησης, κάτι στο οποίο η ασφαλιστική δεν θα βοηθήσει.

Από το 2015 περίπου έχει παρατηρηθεί μια εμφανής μετατόπιση των επιτιθέμενων ως προς τους στόχους τους. Αντί να στοχεύουν οικιακούς χρήστες, εστιάζανε πλέον σε επιχειρήσεις και οργανισμούς (Genç, 2020). Ο ιδιωτικός τομέας αν και δέχεται επιθέσεις συχνότερα από ό,τι ο δημόσιος τομέας, οι ιδιωτικές επιχειρήσεις δεν έχουν καμία υποχρέωση να ανακοινώσουν δημοσίως τις επιθέσεις και στην πραγματικότητα δεν έχουν το κίνητρο να τις αναφέρουν. Το 2019 το 45% των οργανισμών στο δημόσιο τομέα ανέφεραν επιθέσεις από ransomware, λιγότερο από τον παγκόσμιο μέσο όρο για κάθε τύπο οργανισμού που ήταν στο 51%, και λιγότερο από τις πιο συχνά επιτιθέμενες βιομηχανίες (πχ ψυχαγωγία) που ήταν στο 60% (Greengard, 2021).

Οι ειδικοί σε θέματα κυβερνοασφάλειας πιστεύουν ότι η τάση αυτή υπάρχει επειδή οι επιθέσεις ransomware είναι σε θέση να αποσπάσουν υψηλότερα λύτρα από μία επιχείρηση πάρα από οικιακούς χρήστες (Kok et al, 2020). Σύμφωνα με μια μελέτη που δημοσιεύτηκε το 2020 και που αναλύει τις ασφαλιστικές αποζημιώσεις προς επιχειρήσεις, το κόστος της διακοπής των επιχειρησιακών και παραγωγικών διεργασιών, η απώλεια εσόδων, ή το κόστος απαιτούμενων επισκευών υπερβαίνει συχνά τα λύτρα που ζητούνται (Dobie and Whitehead, 2020). Σε μία ολοένα και πιο ψηφιοποιημένη οικονομία μια καλά ορχηστρωμένη επίθεση στον κυβερνοχώρο μπορεί να επιβραδύνει ή να σταματήσει μεγάλης κλίμακας επιχειρηματικές λειτουργίες, αυξάνοντας τότε τη πίεση προς το θύμα (στόχο) προκειμένου να πληρώσει τα λύτρα.

3.2.2 Στοχοποίηση συστημάτων – κατηγορίες

Οι επιτιθέμενοι θέτουν ως στόχο διαφορετικούς τύπους συστημάτων. Η εγκατάσταση κακόβουλου λογισμικού είναι ο πιο συνηθισμένος τρόπος για να αποσπάσουν πολύτιμες πληροφορίες από το θύμα, για τη συνέχιση της επίθεσης οπότε επιλέγουν τον στόχο τους στρατηγικά. Σε γενικές γραμμές, οι επιτιθέμενοι στοχεύουν τέσσερα κύρια συστήματα: προσωπικούς υπολογιστές, κινητές συσκευές, διακομιστές και IoT συσκευές Internet of Things (Savage et al, 2015). Από τη φύση τους οι περισσότερες επιθέσεις ransomware απαιτούν να μπορούν να έχουν πρόσβαση σε εργαλεία κρυπτογράφησης που βρίσκονται

ήδη στο λειτουργικό σύστημα (ΛΣ) του υπολογιστή, επομένως πρέπει ο κώδικας τους να είναι συμβατός με ΛΣ.

Αρχικά, το ransomware είχε σχεδιαστεί μόνο για να στοχεύει προσωπικούς υπολογιστές, ιδίως μηχανήματα Windows. Αλλά μόλις οι κινητές συσκευές είχαν υιοθετηθεί ευρύτερα από το κοινό επέτρεψε στους προγραμματιστές κακόβουλων προγραμμάτων ή ransomware να επεκτείνουν τη λίστα των συστημάτων που ήταν στο στόχαστρο τους. Τα τελευταία χρόνια υπήρξε μια δραματική στροφή προς τις κινητές συσκευές, όπως τα κινητά τηλέφωνα και τα tablets, και IoT συσκευές, όπως κάμερες ασφαλείας και έξυπνοι θερμοστάτες. Ακόμα και στο cloud, διακομιστές και υπηρεσίες που είναι εκτεθειμένες στο ευρύ κοινό είναι πλέον στο στόχαστρο των παραπάνω επιθέσεων.

Προσωπικοί υπολογιστές, ιδίως αυτοί που τρέχουν Windows, ιστορικά είναι το κύριο ΛΣ που έχει αποτελέσει στόχο. Ο λόγος για τον οποίο τα Windows ήταν τόσο έντονα στόχος είναι επειδή οι υπολογιστές που τρέχουν σε Windows αντιπροσωπεύουν τη συντριπτική πλειοψηφία των υπολογιστών που χρησιμοποιούνται παγκοσμίως (Savage et al, 2015). Ήταν λογικό για τους επιτιθέμενους να στοχεύουν τα Windows ειδικά στο ξεκίνημα των επιθέσεων, επειδή τα περισσότερα θύματα ήταν προσβάσιμα μέσω των Windows, και αυτό συνέβη σε μια εποχή που οι οικιακοί χρήστες εξακολουθούσαν να αποτελούν τον πιο έντονο στόχο.

Όταν οι επιτιθέμενοι θέτουν στο στόχαστρο τους ένα οργανισμό, τότε στοχεύουν στους διακομιστές τους, οι οποίοι συχνά περιέχουν πολύτιμα δεδομένα ή φιλοξενούν σημαντικές διαδικτυακές υπηρεσίες. Οι επιτιθέμενοι στοχεύουν διακομιστές επειδή είναι συνήθως κρίσιμη υποδομή για την επιχείρηση, και οι οργανισμοί διακινδυνεύουν να έχουν σοβαρές απώλειες εάν δεν μπορούν να χρησιμοποιήσουν τους διακομιστές τους.

Με την ταχεία ανάπτυξη των smartphones δημιουργήθηκε μία νέα πηγή δημιουργίας εσόδων από λύτρα για τους επιτιθέμενους. Καθώς τα smartphones και άλλες κινητές συσκευές υιοθετήθηκαν ευρύτερα, έγιναν το δεύτερο πιο στοχευμένο σύστημα λόγω της πανταχού παρουσίας τους και χρήσης τους ως υπολογιστές τσέπης (Savage et al, 2015). Οι επιτιθέμενοι στόχευσαν σε αυτή την αγορά και, όπως είναι αναμενόμενο, υπήρξε για αυτούς μια αξιόπιστη μέθοδος στόχευσης μεμονωμένων χρηστών.

Οι κινητές συσκευές τείνουν να διατίθενται σε δύο λειτουργικά συστήματα, iOS ή Android (Savage et al, 2015). Το iOS για συσκευές Apple είναι αρκετά ασφαλές επειδή η Apple έχει αυστηρούς κανόνες για τους προγραμματιστές εφαρμογών και τους καταναλωτές. Αντίστοιχα, το Android είναι ένα ΛΣ ανοιχτού κώδικα και προσαρμόσιμο, καθιστώντας το πρωταρχικό στόχο για επιθέσεις σε κινητά. Επίσης, το Android έχει μεγαλύτερο μερίδιο της παγκόσμιας αγοράς, περίπου τα τρία τέταρτα των τηλεφώνων χρησιμοποιούν Android, οπότε είναι λογικό από τη σκοπιά των επιτιθέμενων να κυνηγήσουν χρήστες αυτής της κατηγορίας.

Έχουν περάσει σχεδόν δύο δεκαετίες από την αρχική κυκλοφορία του smartphone, και σε αυτό το διάστημα άλλες τεχνολογίες όπως το Διαδίκτυο των πραγμάτων (IoT) έχουν αναδυθεί και απέκτησαν φήμη σε παγκόσμιο επίπεδο. Οι συσκευές IoT είναι ηλεκτρονικές συσκευές με δυνατότητα σύνδεσης στο Διαδίκτυο για τη μεταφορά δεδομένων και να λαμβάνουν ενημερώσεις λογισμικού. Το 2018 οι συσκευές αυτές αριθμούσαν μεταξύ 18 και 35 δισεκατομμυρίων, μία σημαντική αύξηση σε σχέση με τις 2 δισεκατομμύρια συσκευές που υπήρχαν περίπου το 2010 (Alaba et al, 2017).

Μια ιδιαίτερα εντυπωσιακή κυβερνοεπίθεση σε IoT συσκευές, η οποία πραγματοποιήθηκε σε εργαστηριακό επίπεδο και όχι στον πραγματικό κόσμο είχε ως στόχο ένα αυτοκίνητο τύπου Jeep Grand Cherokee. Οι ερευνητές μπόρεσαν να πάρουν τον έλεγχο του οχήματος μέσω του Διαδικτύου, ελέγχοντας το τιμόνι, τα φρένα, το ραδιόφωνο, το σύστημα κλιματισμού, ουσιαστικά τα πάντα, αφήνοντας τον οδηγό ανίσχυρο (Miller, 2019). Το συμπέρασμα ήταν ότι εφόσον ήταν δυνατόν για τους ερευνητές, είναι δυνατόν και για επιτιθέμενους στον κυβερνοχώρο που θα μπορούσε να το κάνει και να εκβιάσει οποιονδήποτε οδηγό με σκοπό τα λύτρα αν δεν θα ήθελε να τον κατευθύνουν στην αντίθετη κατεύθυνση κυκλοφορίας.

Ένα άλλο παράδειγμα πραγματική επίθεσης αυτή τη φορά αφορούσε την εξαγωγή δεδομένων από τη βάση δεδομένων πελατών ενός καζίνο μέσω ενός μη ασφαλούς θερμόμετρου για δεξαμενή ψαριών (Niekerk et al, 2020). Αν και δεν ζητήθηκαν λύτρα, αυτή η επίθεση έδειξε την ικανότητα των επιτιθέμενων να καινοτομούν και να βρίσκουν κενά ασφαλείας στις νέες τεχνολογίες.

Η τάση για νέες καινοτόμες επιθέσεις συνεχίζεται μέχρι σήμερα, όπως αποδεικνύεται από την αύξηση των επιθέσεων προς το cloud. Πολλοί οργανισμοί επιλέγουν να

χρησιμοποιήσουν τις cloud υπηρεσίες για να αποθηκεύσουν δεδομένα, όπως Amazon Web Services ή το Microsoft Azure. Σύμφωνα με μια έρευνα του 2020 σε 5.000 διευθυντές πληροφοριακών συστημάτων σε διάφορους οργανισμούς, το 59% των επιθέσεων ransomware περιλάμβαναν κρυπτογράφηση δεδομένων που βρίσκονταν στο cloud (Greengard, 2021).

Οι απειλές για την ασφάλεια του Cloud έχουν αυξηθεί δραματικά κατά την πανδημία του κορονοϊού καθώς ανάγκασε πολλούς εργαζόμενους να εργαστούν εξ αποστάσεως σε πολύ σύντομο χρονικό διάστημα. Αυτό ανάγκασε την αναστολή των προτύπων ασφάλειας των επιχειρήσεων (Dobie and Whitehead, 2020). Μια έρευνα που διεξήχθη μετά την έναρξη της πανδημίας σε 250 επικεφαλής για την ασφάλεια των πληροφοριών σε μεγάλες εταιρείες, κατέγραψε τη χρήση του νέφους ως μία από τις τρεις μεγαλύτερες απειλές κατά τη διάρκεια της εργασίας από το σπίτι (Dobie and Whitehead, 2020). Οι επιτιθέμενοι είναι αναμφισβήτητα καιροσκόποι και θα εκμεταλλευτούν τις αλλαγές στις τεχνολογίες και τη χρήση της τεχνολογίας προς όφελός τους.

3.2.3 Μέθοδοι μόλυνσης

Μόλις ένας δημιουργός ransomware δημιουργήσει τον ιό του, θα πρέπει να διανεμηθεί σε συστήματα υπολογιστών για να υπάρχουν επιπτώσεις σε συστήματα και να παράγουν έσοδα. Οι επιτιθέμενοι έχουν πολλές επιλογές όταν αποφασίζουν πώς θα μολύνουν τα συστήματα, αλλά οι παραδοσιακές επιλογές περιλαμβάνουν την εκμετάλλευση ανθρώπινου λάθους, ή τουλάχιστον την ανθρώπινη αλληλεπίδραση. Οι τεχνικές όμως εξελίσσονται συνεχώς και οι πρόσφατες εξελίξεις έχουν παρακάμψει την ανάγκη για ανθρώπινο σφάλμα. Οι φορείς μόλυνσης με Ransomware τείνουν προς μία πιο αυτοματοποιημένη και αποτελεσματική διανομή.

Ιστορικά, οι επιτιθέμενοι έχουν στηριχθεί σε χρήστες που πρέπει να κάνουν μία ενέργεια για να μολύνουν τα ίδια τα συστήματα ή συσκευές τους. Η μόλυνση παίρνει γενικά τη μορφή ενός κακόβουλου email με ένα συνημμένο αρχείο, έναν κακόβουλο ιστότοπο που εκτελεί λήψη ενός αρχείου που δεν έχει ζητηθεί από τον χρήστη, ή κακόβουλες διαφημίσεις σε μια κατά τα άλλα αξιόπιστη ιστοσελίδα. Οι δημιουργοί του Ransomware προτιμούν αυτές τις μεθόδους, επειδή στις περισσότερες περιπτώσεις είναι πολύ πιο

εύκολο να ξεγελαστεί ένας χρήστης να κατεβάσει ένα αρχείο ή να επισκεφτεί μια ιστοσελίδα από ό,τι είναι να παρακάμψει τον χρήστη και να προσπεράσει τους ελέγχους του υπολογιστή.

Η πιο δημοφιλής μέθοδος μόλυνσης κατά τα τελευταία δεκαπέντε χρόνια ήταν κακόβουλα μηνύματα ηλεκτρονικού ταχυδρομείου μεταμφιεσμένα ως ακίνδυνα μηνύματα ηλεκτρονικού ταχυδρομείου που έχουν ως στόχο να εξαπατήσουν τον παραλήπτη να κατεβάσει ένα συνημμένο αρχείο ή να κάνει κλικ σε έναν σύνδεσμο μέσα στο μήνυμα (Hull et al, 2019). Συχνά το συνημμένο θα είναι το δυαδικό αρχείο του ransomware, οπότε μόλις κατέβει στον υπολογιστή θα αρχίσει να εκτελείται και να κρυπτογραφεί αρχεία. Στην περίπτωση ενός κακόβουλου συνδέσμου, το πιο πιθανό σενάριο είναι ότι οδηγεί σε ένα κακόβουλο ιστότοπο που πραγματοποιεί μη ζητηθείσα λήψη (γνωστό ως "drive-by download"). Η τεχνική αυτή αναφέρεται συνήθως στη βιβλιογραφία ως phishing μηνύματα ηλεκτρονικού ταχυδρομείου. Σύμφωνα με έρευνα του 2020 σε 5.000 διευθυντές πληροφοριακών συστημάτων σε διάφορους οργανισμούς, το 45% των επιθέσεων ransomware προέρχονται από phishing emails (Greengard, 2021).

Όταν οι επιτιθέμενοι στέλνουν εκατομμύρια τέτοια μηνύματα τότε αναφέρονται ως malspam. Το Malspam είναι αποτελεσματικό επειδή οι επιτιθέμενοι μπορούν να γίνουν πολύ δημιουργικοί με τα email τους, χρησιμοποιώντας μια ποικιλία ψυχολογικών τακτικών για να πείσουν τον παραλήπτη να κάνει κλικ, όπως προσφορές σε προϊόντα. Οι εγκληματίες στον κυβερνοχώρο στοχεύουν στον πιο αδύναμο κρίκο στα συστήματα ασφαλείας - τον άνθρωπο – όταν οργανώνουν phishing malspam εκστρατείες, οπότε ο μόνος αποτελεσματικός τρόπος αντιμετώπισης τέτοιων επιθέσεων είναι η εκπαίδευση των χρηστών.

Εκτός από την εξαπάτηση του χρήστη με phishing email, οι επιτιθέμενοι έχουν χρησιμοποιήσει και άλλες δύο κύριες μεθόδους για να εγκαταστήσουν τα αρχεία τους στα συστήματα των θυμάτων. Πρώτον, δημιουργούν κακόβουλους ιστότοπους με αποκλειστικό σκοπό την εκτέλεση drive-by downloads. Το μόνο που πρέπει να κάνει ο χρήστης είναι να επισκεφθεί τον ιστότοπο για να μολυνθεί η συσκευή τους, οπότε οι επιτιθέμενοι ανακατευθύνουν επισκεψιμότητα στον ιστότοπό τους. Επίσης, χρησιμοποιούν exploit kits, ειδικά εργαλεία ransomware συσκευασμένα μαζί για ευκολία, για να ανακατευθύνουν χρήστες από έναν νόμιμο ιστότοπο σε έναν κακόβουλο ιστότοπο

(Kok et al, 2020). Σε αυτό το σενάριο ένας χρήστης θα μπορούσε να κάνει κλικ σε έναν σύνδεσμο από μια σελίδα αναζήτησης αποτελεσμάτων ή ένα phishing email και, χωρίς υπαιτιότητα τους, καταλήγουν σε έναν κακόβουλο ιστότοπο.

Αυτή η τεχνική απαιτεί ενέργεια χρήστη, αλλά όχι ανθρώπινο λάθος, και ως εκ τούτου είναι δύσκολο να αντιμετωπιστεί μόνο με την εκπαίδευση των χρηστών. Δεύτερον, οι επιτιθέμενοι μπορούν να θέσουν σε κίνδυνο έναν αξιόπιστο ιστότοπο με το να εισάγουν κακόβουλο κώδικα στις διαφημίσεις που εμφανίζουν (Kok et al, 2020). Αυτές οι διαφημίσεις μπορεί να ανακατευθύνουν τους χρήστες που κάνουν κλικ στη διαφήμιση σε έναν κακόβουλο ιστότοπο, ή μπορεί να εκτελέσουν drive-by download χωρίς να χρειάζεται οι χρήστες να κάνουν καν κλικ στη διαφήμιση. Αυτή η τεχνική είναι ιδιαίτερα αποτελεσματική επειδή οι επιτιθέμενοι μπορούν να θέσουν σε κίνδυνο ιστότοπους με μεγάλη επισκεψιμότητα, όπως έγινε με το Spotify ή τους New York Times (Lee, 2018).

Τα τελευταία χρόνια, ωστόσο, οι δημιουργοί ransomware έχουν αναπτύξει τεχνικές που εξαλείφουν την ανάγκη για ενέργεια του τελικού χρήστη. Οι παλαιότερες τεχνικές εξακολουθούν να χρησιμοποιούνται κατά κόρον επειδή είναι αναμφισβήτητα αποτελεσματικές, αλλά η τάση για καινοτομία των προγραματιστών ransomware τείνει προς την αυτοματοποίηση. Τελευταίοι τύποι επιθέσεων ransomware, όπως το WannaCry, μπορούν να αυτοαναπαράγονται μέσω του δικτύου ή του διαδικτύου εκμεταλλευόμενοι ένα κενό ασφάλειας στο λειτουργικό σύστημα των Windows, επομένως κάθε συσκευή συνδεδεμένη στο ίδιο δίκτυο με τη μολυσμένη συσκευή είναι σε άμεσο κίνδυνο. Ομολογουμένως, αυτή η τεχνική εξακολουθεί να βασίζεται σε ενέργεια του χρήστη για να ξεκινήσει, αλλά μόλις συμβεί αυτό, η διάδοση έχει ξεκινήσει και είναι ανεξάρτητη από τον αρχικό χρήστη. Αυτό αποτελεί μια εντελώς νέα απειλή σε ένα επόμενο επίπεδο, διότι όταν μια συσκευή μολυνθεί, τότε οποιαδήποτε δεδομένα προσβάσιμα στο δίκτυο κινδυνεύουν.

Μια άλλη αυξανόμενη τάση στη μόλυνση υπολογιστών /συσκευών με ransomware είναι η υιοθέτηση του Ransomware as a Service (RaaS) ώς ένα σύστημα κατανομής κερδών μεταξύ συνεργατών. Το RaaS είναι ένα επιχειρηματικό μοντέλο στο κυβερνοέγκλημα όπου ένα μέρος δημιουργεί το ransomware και προσλαμβάνει άλλα μέρη για τη διανομή του ransomware (Kok et al, 2020). Αυτό το μοντέλο έχει δύο βασικά πλεονεκτήματα. Πρώτον, μοιράζεται ο κίνδυνος να συλληφθεί κάποιος μεταξύ των δύο μερών (Savage et al, 2015).

Οι δημιουργοί του Ransomware απομονώνονται από τον κίνδυνο της διανομής κάτι που αναλαμβάνει ένα άλλο μέρος της συμφωνίας (Lee et al, 2019). Οι τελευταίοι είναι κατά πάσα πιθανότητα πρόθυμοι να αναλάβουν αυτόν τον κίνδυνο διότι παίρνουν μερίδιο από τα λύτρα χωρίς να γράψουν τον κώδικα του ransomware. Δεύτερον, ο καταμερισμός εργασίας επιτρέπει στους κυβερνο-εγκληματίες να εξειδικευτούν και να επικεντρωθούν σε αυτό που κάνουν καλύτερα, είτε πρόκειται για προγραμματισμό είτε για διανομή (Savage et al, 2015).

Πολλοί κυβερνο-εγκληματίες δεν διαθέτουν τις δεξιότητες και τους απαραίτητους πόρους για να γράψουν κώδικα που μπορεί να ξεγελάσει τις σύγχρονους άμυνες κυβερνοασφάλειας, αλλά είναι ικανοί να δημιουργήσουν κώδικα για malspam και drive-by downloads τεχνικές (Savage et al, 2015). Τα exploitation kits μπορούν να αγοραστούν στο Dark Web (Kok et al, 2020). Το RaaS επιτρέπει την είσοδο νέων επιτιθέμενων σε αυτό το επιχειρηματικό μοντέλο, επεκτείνοντας την εμβέλεια που οι συγγραφείς μπορεί να έχει (Savage et al, 2015). Το Ransomware σαφώς και τείνει προς το οργανωμένο έγκλημα, επομένως οι υπεύθυνοι κυβερνοάμυνας και οι αρχές ηλεκτρονικής εγκληματικότητας πρέπει να λάβουν υπόψη τη παραπάνω τάση.

3.2.4 Zero day ransomware

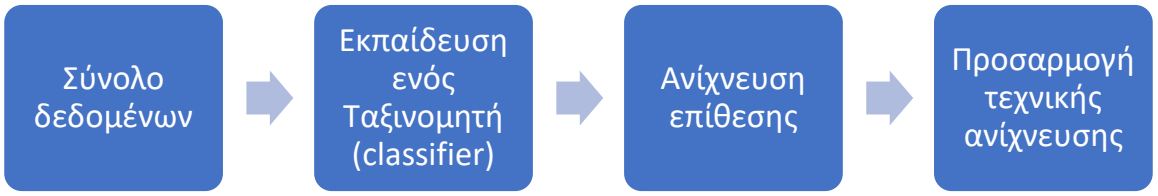
Τα Zero day ransomware είναι εκείνες οι παραλλαγές της επίθεσης που δεν έχουν ανιχνευθεί σε προηγούνενο περιστατικό. Μπορούν να ανιχνευτούν μόνο από σύστημα ανίχνευσης το οποίο είναι καλά σχεδιασμένο για να ανιχνεύει άγνωστες παραλλαγές ransomware. Ορισμένες από αυτές τις τεχνικές παρουσιάζονται στο επόμενο κεφάλαιο.

3.2.5 Σύνολο δεδομένων (Datasets) Ransomware

Το σύνολο δεδομένων και η πηγή του παίζουν καθοριστικό ρόλο στην ανάπτυξη μιας αποδοτικής μεθόδου ανίχνευσης Ransomware. Το σύνολο δεδομένων σχετίζεται άμεσα με την απόδοση και την ακρίβεια ενός συστήματος ανίχνευσης. Μέθοδοι μηχανικής μάθησης

που εκπαιδεύονται σε μη ακριβή δεδομένα θα παράγουν άκυρα αποτελέσματα. Η εκπαίδευση και ανίχνευση σχετίζονται άμεσα από το σύνολο δεδομένων εισόδου.

Οι παραλλαγές του Ransomware αναπτύσσονται σε τεράστιο βαθμό λόγω της χρήσης πολυμορφικών και μεταμορφικών τεχνικών. Το σύνολο δεδομένων είναι επίσης πολύ σημαντικό κατά την ανάπτυξη ενός συστήματος ανίχνευσης που προσαρμόζεται δυναμικά σε τέτοιες συνθήκες. Το **Διάγραμμα** *7* αποτυπώνει τη σημασία του συνόλου δεδομένων για την ανάπτυξη ενός προσαρμοστικού μοντέλου ανίχνευσης. Όσο πιο αξιόπιστο το σύνολο δεδομένων τόσο πιο αξιόπιστη η μέθοδος ταξινόμησης και ανίχνευσης.



Διάγραμμα 7. Η σημασία του συνόλου δεδομένων στην ανάπτυξη συστήματος ανίχνευσης επιθέσεων

Διαφορετικές μελέτες χρησιμοποίησαν σύνολα δεδομένων από διαφορετικά αποθετήρια. Στις περισσότερες μελέτες ανίχνευσης ransomware χρησιμοποιούνται δείγματα από το VirusTotal. Άλλα δημοφιλή αποθετήρια είναι το VirusShare, και το theZoo. Ορισμένες άλλες πηγές περιλαμβάνουν το hybridanalysis.com. Με βάση τον αριθμό των δειγμάτων που χρησιμοποιήθηκαν για ανίχνευση ransomware έναντι καλοήθες (benign) λογισμικού, πολλές μελέτες χρησιμοποίησαν διαφορετική αναλογία των δύο κατηγοριών. Στο Παράρτημα Α' παρουσιάζεται μία περίληψη των διαφόρων αποθετηρίων δεδομένων και των συνόλων δεδομένων που χρησιμοποιήθηκαν στις μελέτες ανίχνευσης από το 2019 έως 2021 για διαφορετικές πλατφόρμες και συστήματα.

3.3 Τρόποι ανάκαμψης από επίθεσης ransomware

Η ανάκτηση είναι η πιο παθητική αμυντική προσέγγιση αντιμετώπισης του ransomware, που βασίζεται στην ιδέα ότι το θύμα είναι σε θέση να ανακτήσει την πρόσβαση στα

κρυπτογραφημένα αρχεία χωρίς να πληρώσουν λύτρα (Wecksten et al, 2016). Υπάρχουν διάφορες τεχνικές που επιτρέπουν στα θύματα να ανακάμψουν από επιτυχείς επιθέσεις, που περιλαμβάνουν την αποκρυπτογράφηση ή την ανάκτηση των αρχείων από απλά αντίγραφα ασφαλείας.

Τα αντίγραφα ασφαλείας προσφέρουν μια απλή και αποτελεσματική λύση σε μία επίθεση ransomware παρέχοντας ένα σημείο ανάκτησης για το σύστημα του θύματος, επομένως τα αρχεία μπορούν να ανακτηθούν χωρίς να καταβληθούν λύτρα. Χωρίς να υπάρχει κάποια χρυσή συνταγή για όλες τις περιπτώσεις, τα αντίγραφα ασφαλείας είναι η πιο απλή πρακτική που μπορούν να εφαρμόσουν οι χρήστες. Η διατήρηση αντιγράφου των δεδομένων σε ξεχωριστά μέσα αφαιρεί αποτελεσματικά κάθε διαπραγματευτική δύναμη του επιτιθέμενου για την απαίτηση λύτρων. Επιπλέον, οι χρήστες που δημιουργούν τακτικά αντίγραφα ασφαλείας για τα δεδομένα τους έχουν μεγαλύτερη αυτοπεποίθηση ότι θα διαχειριστούν σωστά μία τέτοια επίθεση. Δυστυχώς, παρά την ευρεία διαθεσιμότητα της τεχνολογίας αντιγράφων ασφαλείας, πολλοί χρήστες δεν έχουν εφαρμόσει μια αποτελεσματική στρατηγική δημιουργίας αντιγράφων ασφαλείας για να ανακάμψει με επιτυχία από μια επίθεση ransomware.

Σύμφωνα με παλιότερες έρευνες, το 25% των οικιακών χρηστών δεν είχε ποτέ δημιουργήσει αντίγραφα ασφαλείας για τα αρχεία στο σπίτι του, ενώ το 55% έκανε αντίγραφα ασφαλείας για μερικά αρχεία αλλά όχι για το σύνολο τους στο σπίτι. Αυτή η ανησυχητική στατιστική δείχνει ότι η πλειονότητα των οικιακών χρηστών εκτίθεται, σε κάποιο βαθμό, σε επιθέσεις ransomware. Επιπλέον, μόνο το 25% των οικιακών χρηστών δημιουργούσαν αντίγραφα ασφαλείας των αρχείων τους τουλάχιστον μία φορά την εβδομάδα, πράγμα που σημαίνει ότι το 75% των οικιακών χρηστών θα έχαναν περισσότερα από τα αρχεία μιας εβδομάδας σε περίπτωση επίθεσης ransomware (Savage et al, 2015).

Η έλλειψη αντιγράφων ασφαλείας μπορεί πιθανόν να αποδοθεί στην έλλειψη ευαισθητοποίησης των χρηστών και έλλειψη εκπαίδευσης. Επομένως, η αύξηση της κατανόησης των χρηστών για την σημασία των αντιγράφων ασφαλείας, θα βοηθήσει σε μια αλλαγή στη συμπεριφορά των χρηστών προς την εφαρμογή τεχνικών ανάκαμψης.

Επιπλέον, η χρήση τεχνικών ασύμμετρης κρυπτογράφησης από τις νέες τεχνικές ransomware έκανε πολύ πιο δύσκολη την ανάκτηση αρχείων (εφόσον δεν υπήρχαν αντίγραφα ασφαλείας τους). Οι ερευνητές είχαν εντοπίσει μία μέθοδος ανάκτησης από μολύνσεις ransomware σε συστήματα Windows. Η μέθοδος αυτή βασίζεται στη δυνατότητα των Windows στη δημιουργία shadow copies. Αυτά είναι αντίγραφα ασφαλείας του συστήματος του χρήστη που αποθηκεύονται σε τακτά χρονικά διαστήματα, ώστε σε περίπτωση βλάβης του συστήματος να μπορείτε να τα επαναφέρει το σύστημα σε ένα σημείο ελέγχου αποκατάστασης (Savage et al, 2015).

Δυστυχώς για τα θύματα, οι επιθέσεις ransomware τελευταίας γενιάς είναι προηγμένες αρκετά για να διαγράψουν τα σκιώδη αντίγραφα κατά τη διάρκεια των επιθέσεών τους, χωρίς να υπάρχουν σημεία αποκατάστασης για ανάκτηση. Οι χρήστες μπορούν να αποτρέψουν τα τέσσερα πιο κοινά ransomware από τη διαγραφή των shadow copies, μετονομάζοντας το εργαλείο του συστήματος που τα χειρίζεται (Wecksten et al, 2016).

Μια άλλη μέθοδος ανάκτησης είναι ένα σύστημα key escrow που περιλαμβάνει την αποθήκευση πρόσφατων κλειδιών κρυπτογράφησης σε ασφαλές σημείο (vault) για να χρησιμοποιηθεί για την αποκρυπτογράφηση. Σε περίπτωση πετυχημένης επίθεσης ransomware το vault του χρήστη καταγράφει το κλειδί κρυπτογράφησης, καθιστώντας την ανάκτηση αρχείων μέσω αποκρυπτογράφησης μια απλή εργασία. Ένα τέτοιο εργαλείο που ονομάζεται PayBreak δημοσιεύθηκε το 2017 από μια ομάδα ερευνητών σε συνεργασία με το MITRE. Το PayBreak παρακολουθεί συνεχώς την ακεραιότητα των αρχείων στον υπολογιστή του χρήστη. Δεδομένου ότι οι περισσότερες επιθέσεις ransomware βασίζονται σε εργαλεία κρυπτογράφησης στο λειτουργικό σύστημα του υπολογιστή, το PayBreak μπορεί να αναφερθεί σε μοντέλα επίθεσης για να γνωρίζει ποιες κλήσεις συναρτήσεων είναι ύποπτες, έτσι ώστε να αποθηκεύει τα κλειδιά κρυπτογράφησης όταν αντιλαμβάνεται την έναρξη της κρυπτογράφησης (Kolodenker et al, 2017).

Το PayBreak δοκιμάστηκε με 107 δείγματα ransomware που καλύπτουν δώδεκα οικογένειες ransomware, και απέδειξε ότι μπορεί να ανακτήσει το 100% των αρχείων μετά από κάθε επίθεση (Kolodenker et al, 2017). Παρόλο που οι επιτιθέμενοι με ransomware θα μπορούσαν να αλλάξουν τις τεχνικές τους για να αποφύγουν το PayBreak, για παράδειγμα γράφοντας τις δικές τους συναρτήσεις κρυπτογράφησης αντί να

χρησιμοποιούν ό,τι είναι διαθέσιμο στο ΛΣ, το εργαλείο αυτό αυξάνει σημαντικά την απαιτούμενη προσπάθεια για να πραγματοποιηθεί μια επίθεση που δεν μπορεί να αποκατασταθεί. Το PayBreak εξαλείφει την απειλή από μια τεράστια ομάδα ransomware και με αυτόν τον τρόπο αναγκάζει τους επιτιθέμενους να χρησιμοποιούν νέες τεχνικές που οι περισσότεροι έχουν αποφύγει. Επιπρόσθετα, ο πηγαίος κώδικας του PayBreak δημοσιεύτηκε το 2017 και το εργαλείο είναι ελεύθερα διαθέσιμο στο κοινό (Kolodenker et al, 2017).

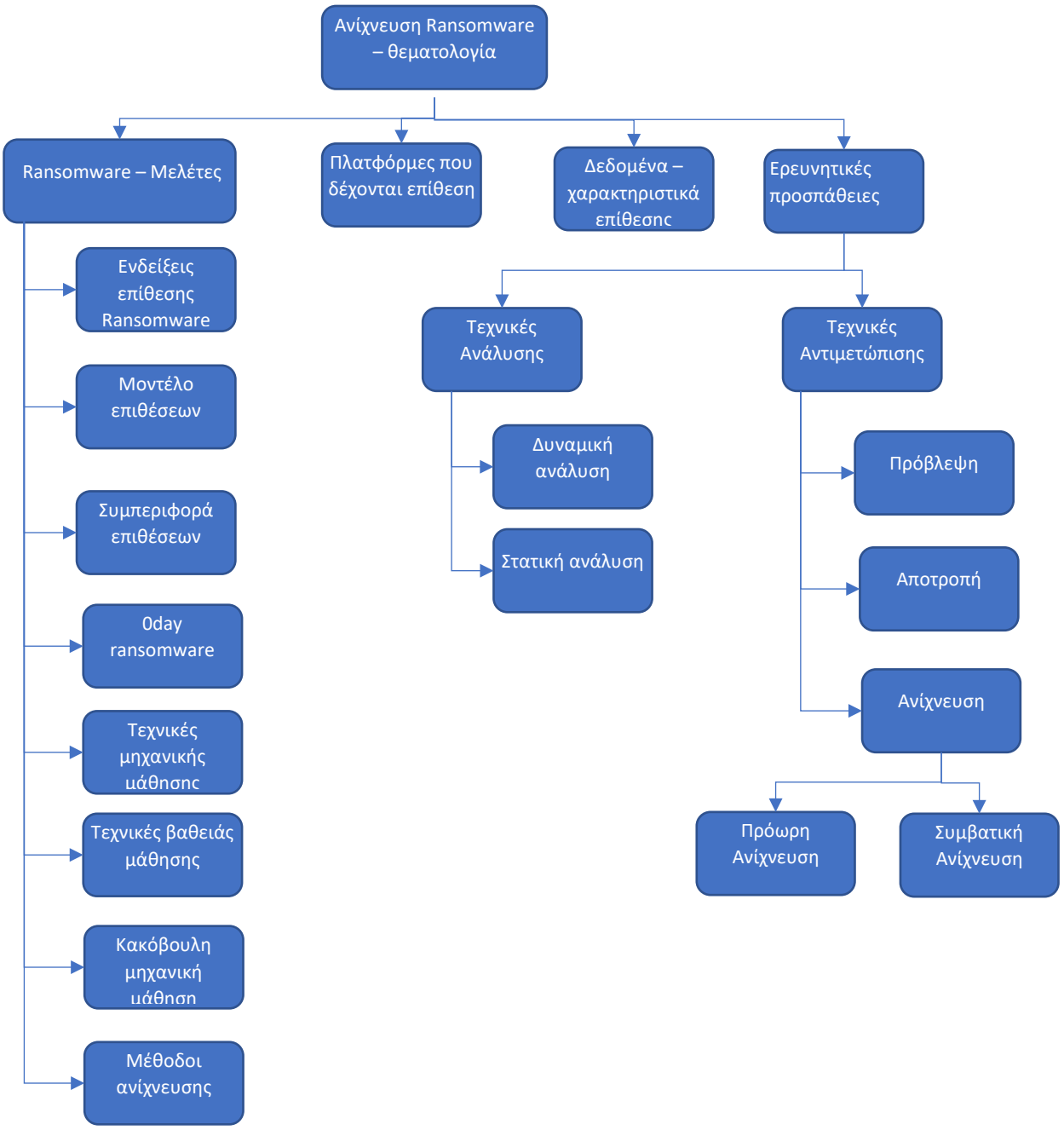
Κεφάλαιο 4 Μέθοδοι ανίχνευσης επιθέσεων

4.1 Εισαγωγή

Ο Olaimat et al (2021) παρουσιάζει μια σύντομη έρευνα σχετικά με τις κατηγορίες της επίθεσης και τεχνικές ανίχνευσης. Η μελέτη των Hu et al (2020) εστιάζει στα Android συστήματα. Οι Maigida et al (2019) παρουσιάζουν μια ανασκόπηση επιθέσεων ransomware σε συστήματα Windows και Android και αντιμετώπισης τους. Οι Bello et al (2020) παρουσιάζουν μια ολοκληρωμένη έρευνα μελετών σχετικά με τεχνικές ανίχνευσης που εφαρμόζουν τεχνικές μηχανικής μάθησης. Αντίστοιχα και οι Sneha et al (2020) καταγράφουν τεχνικές ανίχνευσης των επιθέσεων συνδυάζοντας τεχνικές μηχανικής και βαθειάς μάθησης και τεχνητής νοημοσύνης.

Το **Διάγραμμα** *8* παρουσιάζει τη ταξινόμηση διαφορετικών ερευνών σχετικά με τις επιθέσεις ransomware. Παρουσιάζει διαφορετικές πτυχές που περιλαμβάνουν παραμέτρους που αντικατοπτρίζουν την εμφάνιση σημαντικών επιθέσεων ransomware, τις φάσεις και τη συμπεριφορά της επίθεσης, zero-day επιθέσεις, τεχνικές ανίχνευσης που αρχίζουν να ωριμάζουν και να γίνονται πιο αποδοτικές όπως μηχανική μάθηση, βαθιά μάθηση, κακόβουλη μηχανική μάθηση και εναλλακτικές προσεγγίσεις ανίχνευσης μίας τέτοιας επίθεσης.

Παρέχει επίσης μία επισκόπηση με τις διαφορετικές πλατφόρμες (λειτουργικά συστήματα) που έχουν δεχθεί επιθέσεις έως σήμερα. Διαφορετικές έρευνες έχουν επίσης αποτυπώσει με λεπτομέρεια τα διαφορετικά σύνολα δεδομένων ανά επίθεση. Ενώ, διαφορετικές τεχνικές μηχανικής και βαθιάς μάθησης παρουσιάζονται στη συνέχεια του κεφαλαίου.



Διάγραμμα 8. Ταξινόμηση ερευνών σχετικά με την ανίχνευση επιθέσεων ransomware

Οι προμηθευτές προϊόντων και λύσεων anti-malware χρησιμοποιούν μεθόδους ανίχνευσης όπως σύγκριση αρχείων με βάση την υπογραφή τους (signature based matching), ευρετική ανίχνευση (heuristic detection) ή ανίχνευση με βάση τη συμπεριφορά (behavioral matching) (Amro and Alkhalifah, 2015; Sikorski and Honig, 2012). Στην πράξη, αυτές οι μέθοδοι αποδεικνύονται συχνά ανεπαρκώς αποτελεσματικές για την ανίχνευση

νέου ransomware ή παραλλαγές ενός υπάρχοντος ransomware. Οι Gilbert et al. (2019) διεξήγαγαν μια εκτεταμένη βιβλιογραφική ανασκόπηση των υφιστάμενων μεθόδων ανίχνευσης ransomware.

Υπάρχουν ορισμένα μοτίβα συμπεριφοράς που αποτελούν σημάδια επίθεσης ransomware. Οι παρακάτω ενέργειες μπορούν να χρησιμοποιηθούν ως ενδείξεις μίας τέτοιας επίθεσης:

- Άνοιγμα πολλών αρχείων.
- Η δομή των ροών εισόδου και εξόδου σε μια διεργασία είναι διαφορετική.
- Πολλές λειτουργίες εγγραφής/επανεγγραφής.
- Μια διεργασία που καλεί API κρυπτογράφησης.
- Συχνές αιτήσεις ανάγνωσης και επανεγγραφής/διαγραφής σε σύντομο χρονικό διάστημα.
- Επικοινωνία με διακομιστή command-and-control.
- Αλλαγή στα κλειδιά registry του υπολογιστή

Επί του παρόντος υπάρχουν τρεις τρόποι εντοπισμού/απόκρουσης του ransomware. Ενώ κάθε μία από τις τρέχουσες μεθόδους έχει τα δυνατά της σημεία, έχουν επίσης αδυναμίες που μπορούν να τις εκμεταλλεύονται οι επιτιθέμενοι για να κάνουν το κακόβουλο λογισμικό τους πιο δύσκολο να εντοπιστεί με αυτές τις προσεγγίσεις. Ο πρώτος τύπος είναι επικεντρωμένος στο ransomware, ο οποίος βασίζεται στον προσδιορισμό της οικογένειας/έκδοσης του ransomware που έχει μολύνει το σύστημα. Αυτό βασίζεται σε μοτίβα που βρέθηκαν στον κώδικα ή στη συμπεριφορά του ransomware (δηλαδή στις υπογραφές των αρχείων). Αυτές οι υπογραφές γίνονται για συγκεκριμένες εκδόσεις του ransomware που μπορεί να είναι διαφορετικές σε κάθε διαφορετική οικογένεια.

Ο δεύτερος τύπος είναι ο συστημοκεντρικός, ο οποίος βασίζεται στη συμπεριφορά του συστήματος σε σύγκριση με τη συμπεριφορά του ransomware. Ένα παράδειγμα αυτού του τύπου είναι ένας εταιρικός υπολογιστής που ξαφνικά εκτελεί κρυπτογράφηση σε μεγάλες λίστες αρχείων. Η ανίχνευση αυτού του τύπου μπορεί να παρεμποδιστεί εφόσον παρακολουθείται η κανονική συμπεριφορά του συστήματος.

Ο τρίτος τύπος είναι δεδομενοκεντρικός, ο οποίος βασίζεται στον προσδιορισμό της ομοιότητας/διαφοράς ανάμεσα σε δύο εκδόσεις του ίδιου αρχείου, μία πριν και μία μετά την έκδοση του αρχείου. Αν έχει αλλάξει ενεργά βοηθάει να προσδιοριστεί εάν το ransomware είναι παρόν/ενεργό στον υπολογιστή του χρήστη. Αυτός ο τύπος ανίχνευσης μπορεί επίσης να κρυφτεί πίσω από τη συνήθη συμπεριφορά ενός χρήστη στο σύστημα, όπως η ενημέρωση των προγραμμάτων του λογισμικού, εάν το πρόγραμμα ανίχνευσης εξετάζει αλλαγές στον τύπο αρχείου.

Ένας διαφορετικός τύπος τεχνικής μετριασμού που έχει μελετηθεί είναι η χρήση ενός μοντέλου δικτύωσης που καθορίζεται από το λογισμικό για τον αποκλεισμό της επικοινωνίας μεταξύ του ransomware και του C&C διακομιστή του (Cabaj and Mazurczyk 2016). Αυτός ο τύπος μετριασμού μπορεί να παρεμποδιστεί από τη δημιουργία εφεδρικού κλειδιού για χρήση όταν το ωφέλιμο φορτίο δεν μπορεί να συνδεθεί με τον διακομιστή C&C, και το κλειδί αυτό συμπεριλαμβάνεται μέσα στον κώδικα κρυπτογράφησης του ransomware. Αυτό το εφεδρικό κλειδί μπορεί ενδεχομένως να οδηγήσει σε μια κατάσταση όπου το κλειδί έχει καταστραφεί ως μέρος της "κανονικής" συμπεριφοράς του ransomware που θα καθιστούσε την ανάκτηση οποιουδήποτε κρυπτογραφημένου αρχείου με αυτό το αυτοδημιουργούμενο κλειδί αδύνατο.

4.2 Ομοιότητες μεταξύ μεθόδων ανίχνευσης

Η αναζήτηση ομοιότητας μεταξύ αρχείων χρησιμοποιώντας τις τεχνικές της εντροπίας και του κατακερματισμού για την ανίχνευση ransomware είναι από τις πιο γνωστές τεχνικές που ακολουθούνται από όλους τους προμηθευτές αντι-ικών προγραμμάτων. Ωστόσο, η ραγδαία αύξηση του κακόβουλου λογισμικού καθιστά τη μέθοδο σύγκρισης αρχείων βάσει υπογραφών μη αποτελεσματική και με περιορισμένη δυνατότητα κλιμάκωσης (Chen, 2018). Αυτό γιατί, οι προγραμματιστές του κακόβουλου λογισμικού κάνουν αλλαγές στο πρόγραμμα τους έτσι ώστε οι υπογραφές να αλλάζουν και να αποφεύγουν την ανίχνευση.

Οι (Ganapathi and Shanmugapriya, 2020; Nataraj et al., 2011) υποστηρίζουν ότι διαφορετικές κατηγορίες ransomware έχουν λειτουργικές ομοιότητες που μπορούν να βρεθούν στον κώδικα αφού αποσυμπιεστεί, καθιστώντας με αυτό το τρόπο δυνατή την

ανίχνευσή τους με βάση τα παρόμοια χαρακτηριστικά σε μία ορισμένη κατηγορία. Οι αλγόριθμοι μπορούν να μάθουν να αναγνωρίζουν τις ομοιότητες όταν τα εκτελέσιμα αρχεία κακόβουλου λογισμικού μετατρέπονται σε εικόνες, και μπορούν να προβλέψουν ότι μπορεί να αφορούν ransomware αρχεία, δεδομένου ότι είναι πάντα ένας τύπος κακόβουλου λογισμικού και ότι οι κατηγορίες ransomware έχουν επίσης ομοιότητες στον κώδικα.

4.3 Μέθοδοι μηχανικής μάθησης

Εναλλακτικά ένα κακόβουλο λογισμικό ransomware μπορεί να ανιχνευθεί και να αναγνωριστεί αξιόπιστα με τη χρήση αλγορίθμων και τεχνικών μηχανικής μάθησης (ML) (Al-rimy et al., 2018; Nataraj et al., 2011). Υπάρχουν δύο πτυχές που καθιστούν την ανίχνευση ransomware με ML αναγκαία.

Πρώτον, το ransomware εξελίσσεται όλο και περισσότερο και, λόγω της εφαρμογής καλύτερων χαρακτηριστικών για την ανίχνευση του, οι προγραμματιστές του εστιάζουν στο να γίνει πιο δύσκολο να εντοπιστεί (Dargahi et al., 2019). Δεύτερον, το ransomware εξελίσσεται τόσο γρήγορα που συχνά δεν μπορεί να εντοπιστεί αξιόπιστα χρησιμοποιώντας τρέχουσες τεχνικές ανίχνευσης. Και οι δύο παράγοντες διασφαλίζουν ότι οι προγραμματιστές κακόβουλου λογισμικού μπορούν εύκολα να παρακάμψουν την ανίχνευση και, συνεπώς, αυξάνουν την πιθανότητα μόλυνσης και ζημιάς σε υποδομές και υπηρεσίες.

Μια αξιόπιστη μέθοδος για την ανάλυση του ransomware είναι η στατική ανάλυση, κατά την οποία ένα αρχείο μετατρέπεται σε κώδικα μηχανής και στη συνέχεια ο κώδικας αναλύεται διεξοδικά από έναν ειδικό (malware reverse engineer) για να εντοπίσει γνωστά μοτίβα. Αυτό απαιτεί εξειδικευμένες γνώσεις από έναν αναλυτή και θεωρείται πολύ χρονοβόρα διαδικασία (Chen, 2018; Nataraj et al., 2011). Η μηχανική μάθηση μπορεί να υποστηρίξει τους αναλυτές στην ταξινόμηση ενός αρχείου ως καλοήθη ή κακόβουλο λογισμικό (Al-rimy et al., 2018, Johns, 2017).

Παρ' όλα αυτά, θα πρέπει να εξεταστούν περιορισμοί στη χρήση των παραδοσιακών ML αλγορίθμων εφόσον αντιμετωπίζουν την ανίχνευση κακόβουλων προγραμμάτων ως μία

εφαρμογή ταξινόμησης. Η ανάλυση και σωστή επιλογή των χαρακτηριστικών που θα ληφθούν υπόψη κατά την ταξινόμηση είναι η πιο σημαντική πρόκληση. Οι αλγόριθμοι μηχανικής μάθησης βασίζονται σε μεγάλο βαθμό στην ανάλυση και επιλογή χαρακτηριστικών. Οι τεχνικές διαχείρισης τους απαιτούν εκτεταμένη γνώση ανά τομέα εφαρμογής (Vinayakumar et al., 2019).

Παραδοσιακοί αλγόριθμοι μηχανικής μάθησης βασίζονται στη γραμμική παλινδρόμηση, διανυσματικές μηχανές (SVM) και kNN (Nearest Neighborhood) και συχνά εφαρμόζονται ως τεχνικές ανίχνευσης κακόβουλου λογισμικού. Σε γενικές γραμμές, υπάρχουν δύο τύποι τεχνικών ML που μπορούν να βοηθήσουν τους αναλυτές στον εντοπισμό κακόβουλου λογισμικού (Vu et al., 2019):

1. Τεχνικές ταξινόμησης χαρακτηριστικών που βασίζονται στον κώδικα μηχανής ή/και στη συμπεριφορά (Kolosnjaji et al., 2017)
2. Τεχνικές συσχετισμού εικόνων (image based) χωρίς την ταξινόμηση χαρακτηριστικών (Han et al., 2013)

4.3.1 Μέθοδοι μηχανικής μάθησης για στατική ανάλυση

Μία από τις πρώτες έρευνες στη χρήση μηχανικής μάθησης για την ανίχνευση κακόβουλου λογισμικού (Knebel et al, 2022) αφορούσε την εφαρμογή πληροφοριών στη μορφή φορητών, εκτελέσιμων συμβολοσειρών. Οι ακολουθίες των δεδομένων σε δυαδική μορφή αποτέλεσαν δεδομένα εισόδου στον αλγόριθμο ταξινόμησης Naïve Bayes. Σε μία αντίστοιχη προσέγγιση των (Kolter and Maloof, 2006), εφαρμόστηκαν n-gram byte ακολουθίες με διαφορετικούς αλγορίθμους ταξινόμησης, όπως naïve Bayes, δέντρα απόφασης, SVM και Boosting για την ταξινόμηση δυαδικών αρχείων κακόβουλου λογισμικού. Ο συνδυασμός των αλγορίθμων των Δέντρων Απόφασης και Boosting είχε την καλύτερη απόδοση με ποσοστό σε True Positives (TPR) 98% και False Positives (FPR) 5%.

Σε μία άλλη μελέτη, οι Jerome et al (2014) εξήγαγαν ακολουθίες δυαδικών δεδομένων από εκτελέσιμα προγράμματα κακόβουλου λογισμικού και τα μετέτρεψαν σε μια ακολουθία από opcodes. Μέσα από αυτή τη προσέγγιση, μπόρεσαν να αντληθούν μοτίβα (signatures)

κακόβουλου λογισμικού που βοήθησαν στη βελτίωση του False Positives ποσοστού. Η προτεινόμενη μέθοδος αξιοποίησε επίσης τη τεχνική Information Gain για να εστιάσει σε συγκεκριμένα χαρακτηριστικά και εφάρμοσε τον αλγόριθμο ταξινόμησης SVM. Τα πειράματα τους παρουσίασαν ποσοστό σε True Positives (TPR) 81,40% και False Positives (FPR) 2,67%.

Το κύριο μειονέκτημα των τεχνικών στατικής ανάλυσης είναι ότι δεν μπορούν να ανιχνεύσουν νέες παραλλαγές ενός κακόβουλου λογισμικού. Μελέτες εμφάνισαν ότι ένα χαμηλό μέσο όρο στην απόδοση των τεχνικών στατικής ανάλυσης με μία στις έξι επιτυχείς προσπάθειες ανίχνευσης (Kharraz et al, 2015). Ένα άλλο μειονέκτημα αυτών των τεχνικών είναι ότι μπορούν να παρακαμφθούν χρησιμοποιώντας τεχνικές απόκρυψης κώδικα (Moser et al., 2007). Επίσης, όταν φορητά εκτελέσιμα αρχεία τροποποιούνται, η απόδοση της στατικής ανάλυσης μειώνεται (Hampton et al, 2018).

Προκειμένου να ξεπεραστούν τα μειονεκτήματα των παραπάνω signature-based τεχνικών, η έρευνα εστίασε περισσότερο στις δυναμικές τεχνικές ανίχνευσης ransomware.

4.3.2 Μέθοδοι μηχανικής μάθησης για δυναμική ανάλυση

Σε μελέτη 15 διαφορετικών κατηγοριών ransomware από το 2006 έως το 2014 (Kharraz et al, 2015) προέκυψε ότι σχεδόν το 94% των δειγμάτων κακόβουλων προγραμμάτων ransomware εφαρμόζει απλές τεχνικές κλειδώματος ή κρυπτογράφησης. Η μελέτη κατέληγε ότι παρακολουθώντας στενά τη δραστηριότητα του συστήματος αρχείων και τους τύπους των πακέτων κλήσεων με δεδομένα εισόδου/εξόδου προς το σύστημα αρχείων, είναι δυνατή η ανίχνευση επιθέσεων ransomware. Παρατήρησαν επίσης ότι οι διευθύνσεις Bitcoin που χρησιμοποιούνται για τη συλλογή λύτρων από τα θύματα μοιράζονται παρόμοια αρχεία συναλλαγών, όπως μικρό αριθμό συναλλαγών, μικρά ποσά Bitcoin, μικρή περίοδο δραστηριότητας κ.λπ. Ωστόσο, παρά τις προτεινόμενες στρατηγικές για την ανίχνευση ransomware, δεν υπήρξε συγκεκριμένη αξιολόγηση υπό τη μορφή πειράματος στα πλαίσια της παραπάνω έρευνας.

Σε ένα τέτοιο πειραματικό πλαίσιο κινήθηκε (Kharraz et al, 2017) το σύστημα ανίχνευσης ransomware UNVEIL. Το UNVEIL εξετάζει το επίπεδο του συστήματος αρχείων για να εντοπίσει τη τυπική συμπεριφορά ενός ransomware. Χρησιμοποιεί τεχνικές ανάλυσης κειμένου για τον εντοπισμό απειλητικών σημειωμάτων ransomware και εξάγει συνεχώς στιγμιότυπα της οθόνης της επιφάνειας εργασίας για να ελέγχει για τυχόν κλείδωμα της οθόνης. Χρησιμοποιεί επίσης στατιστική ανάλυση με βάση τη χρήση της μνήμης, τη χρήση του επεξεργαστή και τους ρυθμούς I/O του δίσκου για τον εντοπισμό μη φυσιολογικής συμπεριφοράς από τυχόν παραλλαγές ransomware. Πειράματα με αυτό το σύστημα είχαν ακρίβεια 96,3% στην ανίχνευση ransomware. Παρά την επίτευξη σχετικά υψηλού ποσοστού ακρίβειας, το μοντέλο δεν έχει τη δυνατότητα έγκαιρης ανίχνευσης για επιθέσεις ransomware ούτε παρέχει μηχανισμό δημιουργίας αντιγράφων ασφαλείας. Επίσης, το προτεινόμενο σύστημα δεν εμφανίζει ικανοποιητικά αποτελέσματα στην ανίχνευση νεότερων γενιών ransomware.

Το ShieldFS, ήταν ένα άλλο εναλλακτικό σύστημα του UNVEIL (Continella et al, 2016). Αποτελεί ένα σύστημα ανίχνευσης που έχει τη δυνατότητα της μη επιβλεπόμενης μάθησης και επιτρέπει στο σύστημα να επιστρέψει σε μία προηγούμενη κατάσταση πριν τις αλλαγές που ενδεχομένως προκάλεσε ένα κακόβουλο λογισμικό. Παρακολουθεί εσωτερικά και σε χαμηλό επίπεδο τις δραστηριότητες του συστήματος αρχείων και υπολογίζει την εντροπία των λειτουργιών εγγραφής και της συχνότητας ανάγνωσης, εγγραφής και καταχώρισης φακέλων, για παράδειγμα στο σύστημα αρχείων της επιχείρησης. Ψάχνει επίσης τις περιοχές μνήμης κάθε διεργασίας που θεωρείται "δυνητικά κακόβουλη", αναζητώντας συγκεκριμένα χρονοδιαγράμματα και μπλοκ κλειδιών κρυπτογράφησης.

Το σύστημα συνδυάζει τη δυνατότητα αυτόματης ανίχνευσης και ανάκτησης αρχείων με διαφάνεια και παρέχεται ως ένα πρόγραμμα έτοιμο προς εγκατάσταση και χρήση σε εταιρικά δίκτυα. Ωστόσο, και αυτή η τεχνική έχει ορισμένους περιορισμούς, καθώς νέες παραλλαγές του ransomware τείνουν να κρυπτογραφούν ή να διαγράφουν το shadow copy του συστήματος αρχείων των Windows, καθιστώντας τις πιθανότητες ανάκτησης του αρχείου σχεδόν μηδενικές. Επιπλέον, το σύστημα επικεντρώνεται περισσότερο σε λειτουργίες που σχετίζονται μόνο με τη διαχείριση αρχείων σε ένα μηχάνημα. Η σάρωση της μνήμης είναι χρονοβόρα και υποφέρει από το γεγονός ότι υπάρχουν μικρές πιθανότητες να βρεθεί μπλοκ κλειδιών σε περιοχή της μνήμης.

Το CryptoDrop (Scaife et al, 2016) ήταν ένα σύστημα έγκαιρης προειδοποίησης για την ειδοποίηση των χρηστών σε περίπτωση ανίχνευσης ύποπτων δραστηριοτήτων σε αρχεία. Το σύστημα επικεντρώθηκε κυρίως στην παρακολούθηση αλλαγών σε αρχεία διακρίνοντας το ransomware σε τρεις μεγάλες κατηγορίες: κατηγορία Α, κατηγορία Β και κατηγορία Γ με βάση τον τρόπο με τον οποίο κρυπτογραφούν τα αρχεία χρήστη. Χρησιμοποιεί συναρτήσεις ομοιότητας για τη σύγκριση μεταξύ των αρχικών και των κρυπτογραφημένων περιεχομένων των αρχείων ωστόσο δεν μπορεί να διακρίνει κακόβουλες από μη κακόβουλες προθέσεις στις αλλαγές των αρχείων. Για παράδειγμα, το σύστημα δεν μπορεί να διακρίνει μία διαδικασία κρυπτογράφησης που ξεκινάει από τον ίδιο τον χρήστη έναντι της κρυπτογράφησης που προκαλείται από το ransomware.

Ένα εναλλακτικό σύστημα, EldeRan (Sgandurra et al, 2016), παρακολουθεί αρχικά ένα σύνολο δραστηριοτήτων που εκτελείται από τις εφαρμογές και ελέγχει για χαρακτηριστικά του ransomware. Σε ένα δεύτερο στάδιο, χαρακτηριστικά όπως κλήσεις API, αρχεία που απορρίπτονται, ενημερώσεις στις εγγραφές του μητρώου του υπολογιστή και απαριθμήσεις καταλόγων τροφοδοτούνται σε μοντέλο μηχανικής μάθησης για την εκμάθηση προτύπων με στόχο τη διάκριση μεταξύ κακόβουλων και μη κακόβολων εφαρμογών. Η πειραματική αξιολόγηση του συστήματος βασίστηκε σε ένα σύνολο δεδομένων που περιλάμβανε ransomware εγγραφές από 11 διαφορετικές κατηγορίες. Εφαρμόζοντας ένα περιορισμένο αριθμό χαρακτηριστικών, η ακρίβεια της δυναμικής ανάλυσης με τη βοήθεια της δυναμικής μάθησης ήταν στο 96,3%.

Ωστόσο, το EldeRan δεν μπορεί να αναλύσει χαρακτηριστικά όταν το ransomware τρέχει στο παρασκήνιο για σύντομο ή μεγάλο χρονικό διάστημα. Τα περισσότερα από τα χαρακτηριστικά που λαμβάνονται υπόψη από το σύστημα είναι σε δυαδική μορφή και πεπερασμένα. Ωστόσο, νέες παραλλαγές ransomware χρησιμοποιούν άλλα χαρακτηριστικά και έτσι καθιστούν το προτεινόμενο μοντέλο ανίχνευσης αναποτελεσματικό. Για παράδειγμα, μια εγγραφή κλειδιού μητρώου που χρησιμοποιείται σε μια παραλλαγή ransomware ενδέχεται να μην χρησιμοποιείται από άλλες παραλλαγές ή νέες εκδόσεις του ransomware.

Οι Chen et al. (2018) πρότειναν μια προσέγγιση για την ανίχνευση ransomware με βάση τη διαμόρφωση ενός δυναμικού γραφήματος με τη ροή API κλήσεων παρακολουθώντας τις ακολουθίες API κλήσεων του κακόβουλου λογισμικού. Χρησιμοποίησαν διάφορους

αλγορίθμους ταξινόμησης δεδομένων, όπως Random Forest, SVM, Naive Baysian και Λογιστική Παλινδρόμηση. Η λογιστική παλινδρόμηση πέτυχε την υψηλότερη ακρίβεια 98,2% με False Positive Rate (FPR) 1,2%. Ωστόσο, η τεχνική αυτή εστίασε σε ένα μόνο χαρακτηριστικό για την ανίχνευση ransomware και η αξιολόγηση βασίστηκε σε ένα μικρό δείγμα από ransomware αρχεία.

Οι Lanzi et al. (2010) ανέλυσαν έναν μεγάλο αριθμό συστημικών κλήσεων από απλούς χρήστες και μελέτησαν την ποικιλομορφία των συστημικών και API κλήσεων. Παρατήρησαν ότι οι αλληλεπιδράσεις των κανονικών (μη κακόβουλων) προγραμμάτων με το λειτουργικό σύστημα είναι διαφορετικές από εκείνες των κακόβουλων προγραμμάτων. Επίσης, οι Vinayakumar et al. (2019) αξιοποίησαν τις API κλήσεις για να δημιουργήσουν ένα νευρωνικό δίκτυο πολλαπλών επιπέδων perceptron (MLP). Η πειραματική αξιολόγηση του προτεινόμενου μοντέλου σε ένα σύνολο δεδομένων από 7 διαφορετικές περιπτώσεις ransomware πέτυχε ικανοποιητικά ποσοστά ακρίβειας (98%).

Οι Poudyal et al. (2019) ανέπτυξαν ένα πλαίσιο αντίστροφης μηχανικής για την ανίχνευση κακόβουλου λογισμικού. Το πλαίσιο συμβάλλει στη πραγματοποίηση πολυεπίπεδης ανάλυσης κώδικα μηχανής, κλήσεων σε συναρτήσεις προγραμμάτων ή βιβλιοθήκες του λειτουργικού συστήματος και εφαρμόζει διάφορες τεχνικές μηχανικής μάθησης με επίβλεψη (Bayesian Network, Random Forest, SMO και J48). Η πειραματική αξιολόγηση απέδωσε ακρίβεια ανίχνευσης σε ransomware δείγματα που κυμάνθηκε από 76% έως 97% ανάλογα με τη τεχνική μηχανικής μάθησης που εφαρμόστηκε.

4.3.3 Μέθοδοι μηχανικής μάθησης για δυναμική ανάλυση σε φορητές/IoT συσκευές

Mobile ransomwares στοχοποιούν τα κινητά τηλέφωνα των χρηστών, για παράδειγμα τύπου Android. Αυτές οι επιθέσεις ξεκινούν όταν ο χρήστης κατεβάσει και εγκαταστήσει ένα trojan ή μια ψεύτικη εφαρμογή από ένα ευρετήριο εφαρμογών. Η οθόνη του κινητού τηλεφώνου κλειδώνει και όλα τα δεδομένα του κινητού κρυπτογραφούνται, συμπεριλαμβανομένης της λίστας επαφών και ο χρήστης καλείται να πληρώσει λύτρα. Τα θύματα απειλούνται με την απώλεια των δεδομένων στο κινητό τους, της διαρροής στο

διαδίκτυο προσωπικών δεδομένων και του ιστορικού περιήγησης στις επαφές τους. Το Android.Lockdroid.E είναι ένα χαρακτηριστικό παράδειγμα mobile ransomware.

Οι Karimi και Moattar (2017) παρουσίασαν μια προσέγγιση που μετατρέπει μια ακολουθία εκτελέσιμων αρχείων σε μια εικόνα σε κλίμακα του γκρι. Στη συνέχεια, χρησιμοποίησαν Linear Discrimant Analysis (LDA) που είναι μια στατιστική μέθοδος για το διαχωρισμό δύο ή περισσότερων κλάσεων με τη τεχνική της μείωσης των διαστάσεων για τη βελτίωση της απόδοσης του μοντέλου. Η αξιολόγηση του προτεινόμενου μοντέλου πραγματοποιήθηκε μέσω δύο διαφορετικών πειραμάτων. Το πρώτο πείραμα διεξήχθη χρησιμοποιώντας ένα σύνολο δεδομένων από 140 δείγματα ransomware από δύο περιπτώσεις και 20 καλοήθη δείγματα, αποδίδοντας 97% ακρίβεια. Στο δεύτερο πείραμα, το μοντέλο πέτυχε ακρίβεια 97,3% με ένα σύνολο δεδομένων που αποτελείται από 230 δείγματα ransomware από τις οικογένειες Locker και Koler και 30 καλοήθη δείγματα.

Οι Andronio et al (2015) μελέτησαν οικογένειες ransomware για κινητά τηλέφωνα με λειτουργικό σύστημα Android και ανέπτυξαν τη μέθοδο HelDroid, για την ανίχνευση ransomware. Το HellDroid παρακολουθεί και ανιχνεύει τη συμπεριφορά του ransomware στο επίπεδο εφαρμογής και χρησιμοποιεί την επεξεργασία φυσικής γλώσσας (NLP) για την αναγνώριση απειλητικών φράσεων.

Η αξιολόγηση του συστήματος πέτυχε ακρίβεια άνω του 97% με ένα σύνολο δεδομένων που αποτελείται από 650 ransomware και περίπου 81.000 καλοήθη δείγματα. Ωστόσο, η ανίχνευση απειλητικών φράσεων δεν είναι πολύ χρήσιμη, καθώς μέχρι να εμφανιστεί στην οθόνη του χρήστη το σημείωμα για τα λύτρα, τα δεδομένα έχουν ήδη κρυπτογραφηθεί.

Το R-PackDroid, είναι ένα άλλο σύστημα ανίχνευσης ransomware με βάση το Android. Βασίζεται σε τεχνικής εποπτευόμενης μηχανικής μάθησης ωστόσο σε πραγματικές συνθήκες δεν απέδωσε τα αναμενόμενα αποτελέσματα.

Μια άλλη τεχνική βασισμένη σε formal methods για την ανίχνευση mobile ransomware, ακολουθεί μεθοδολογία στατικής ανάλυσης και εξετάζει την κακόβουλη συμπεριφορά σε bytecode επίπεδο. Η τεχνική αυτή δεν έχει την ικανότητα ανάλυσης του δείγματος του κακόβουλου προγράμματος σε πλήρη αποσύνθεση του κώδικα. Για την επίλυση του προβλήματος χρησιμοποιήθηκε μικρότερος αριθμός μορφοποιημένων δειγμάτων. Τα δείγματα που χρησιμοποιήθηκαν ήταν από 10 αντιπροσωπευτικές οικογένειες επιθέσεων.

Επίσης, το Διαδίκτυο των Πραγμάτων (IoT), που είναι ένα σύστημα διασυνδεδεμένων υπολογιστικών συσκευών με περιορισμένη επεξεργαστική ισχύ και μνήμη, έχει στοχοποιηθεί από ανάλογες επιθέσεις. Έχουν προταθεί τεχνικές ανίχνευσης ransomware που βασίζονται κυρίως σε νευρωνικά δίκτυα (πχ τύπου CNN, LSTM και OCSVM) (Alrawashdeh and Purdy, 2018). Αρχικά γίνεται ανάλυση της συμπεριφοράς του κακόβουλου προγράμματος από ένα στρώμα νευρωνικών δικτύων (πχ OCSVM) για να αναγνωριστεί η οικογένεια επιθέσεων στην οποία ανήκει. Στη συνέχεια, επόμενα στρώματα από νευρωνικά δίκτυα (πχ CNN, LSTM) επαληθεύουν ότι η ύποπτη συμπεριφορά σχετίζεται με επίθεση ransomware.

Άλλες τεχνικές βασίστηκαν επίσης σε μεθόδους βαθειάς μάθησης (Deep Belief Network - DBN) σε επίπεδο υλικού για την ανίχνευση ransomware σε συσκευές IoT και ενσωματωμένα συστήματα (Homayoun et al, 2019). Οι μέθοδοι αυτές πραγματοποιούν ανάλυση της συμπεριφοράς του εκάστοτε κώδικα που φορτώνεται στη μνήμη της συσκευής. Σε άλλες τεχνικές εφαρμόστηκε μία υβριδική μηχανική χαρακτηριστικών (Al-Hawawreh and Sitnikova, 2019). Για τη μείωση της διάστασης των δεδομένων και την εξαγωγή των απαραίτητων χαρακτηριστικών για την ανάλυση χρησιμοποιήθηκαν κλασικοί και μεταβλητοί κωδικοποιητές. Η αξιολόγηση της συμπεριφοράς γινόταν σε συνδυασμό της εφαρμογής νευρωνικών δικτύων τύπου DNN και BN.

4.3.4 Μέθοδοι μηχανικής μάθησης για δίκτυα

Λόγω της εξέλιξης των σύγχρονων επιθέσεων ransomware, η μέθοδος ανάλυσης σε επίπεδο δικτύου τύπου packet inspection δεν είναι πλέον αρκετή. Για τον εντοπισμό του ransomware, θα πρέπει να αναπτυχθεί ένα σύστημα παρακολούθησης της κακόβουλης δραστηριότητας σε επίπεδο δικτύου.

Ένα τέτοιο σύστημα που βασίζεται σε Honeypots είχε προταθεί από τον (Moore, 2016). Honeypots είχαν εγκατασταθεί σε κάθε σταθμό εργασίας για να ανιχνεύεται κακόβουλη συμπεριφορά τόσο σε επίπεδο μηχανήματος και συνολικά στο δίκτυο. Μόλις παρατηρηθεί μια κακόβουλη συμπεριφορά, ο διαχειριστής του δικτύου απενεργοποιεί το λογαριασμό

χρήστη και το μηχάνημα για να απομονώσει την κακόβουλη κίνηση από το δίκτυο. Παρόλα αυτά, το συγκεκριμένο σύστημα δεν μπορούσε να αποτρέψει μία επίθεση στο ξεκίνημα της, πράγμα που θα οδηγούσε σε απώλεια δεδομένων σε περίπτωση επίθεσης. Αντίστοιχο σύστημα είχε προταθεί από τους Cabaj et al (2015).

Σε ένα εναλλακτικό μοντέλο ανίχνευσης ransomware, η ανίχνευση μπορούσε να πραγματοποιηθεί σε δύο στάδια (Cusack et al, 2018). Αρχικά το σύστημα εντόπιζε μοτίβα ύποπτής κίνησης στο δίκτυο. Στη συνέχεια ο χρήστης ενημερωνόταν όταν παρατηρούνταν κακόβουλη συμπεριφορά. Ο χρήστης μπόρεσε να διακόψει τη σύνδεση και να ελέγξει τη διεύθυνση σύνδεσης με σκοπό να τη διακόψει και να εμποδίσει την ανταλλαγή κλειδιών και την κρυπτογράφηση.

4.3.5 Μέθοδοι μηχανικής μάθησης για υβριδική ανάλυση

Οι Hasan και Rahman (2017) πρότειναν ένα σύστημα με την ονομασία RansHunt που συνδυάζει στατική και δυναμική ανάλυση για τον εντοπισμό ransomware. Το προτεινόμενο μοντέλο αξιολογήθηκε χρησιμοποιώντας συνολικά 1.283 διαφορετικά προγράμματα που περιλάμβαναν 360 προγράμματα ransomware από 21 διαφορετικές οικογένειες και 923 κανονικά προγράμματα, επιτυγχάνοντας ακρίβεια 97,1%. Το σύστημα προσδιόρισε νέα χαρακτηριστικά στη δυναμική ανάλυση που σχετίζονται με τη δικτυακή κίνηση, η οποία δεν συνέβαλε σημαντικά στη βελτίωση του ποσοστού ανίχνευσης. Επίσης, τα χαρακτηριστικά που χρησιμοποιήθηκαν για τη δυναμική ανάλυση ήταν σχεδόν παρόμοια με τα χαρακτηριστικά του EldeRan συστήματος. Το μοντέλο δεν ανταποκρίθηκε αποτελεσματικά σε νέες παραλλαγές ransomware.

Οι Shaukat and Ribeiro (2018) παρουσίασαν ένα πολυεπίπεδο σύστημα ανίχνευσης για την προστασία από επιθέσεις ransomware. Συνδύασαν τόσο τη στατική όσο και τη δυναμική ανάλυση για να δημιουργήσουν ένα υβριδικό σύστημα. Το επίπεδο δυναμικής ανίχνευσης παρακολουθεί τις λειτουργίες του συστήματος αρχείων και τις τροποποιήσεις με τη μέθοδο της εντροπίας για να εντοπίσουν μαζικές δραστηριότητες κρυπτογράφησης. Εφόσον τα αρχεία τροποποιούνται από ύποπτες διεργασίες, το σύστημα δημιουργεί

αντίγραφα ασφαλείας τους σε άλλο ασφαλή φάκελο για τη διατήρηση των δεδομένων έως ότου οι διεργασίες ταξινομηθούν ως ransomware ή ως καλοήθεις.

Το προτεινόμενο μοντέλο αξιολογήθηκε χρησιμοποιώντας ένα σύνολο δεδομένων που αποτελείται από 574 δείγματα ransomware από 12 διαφορετικές οικογένειες ransomware. Η αξιολόγηση απέδωσε ακρίβεια 98,25%. Ωστόσο, όπως και στα άλλα συστήματα, η δυναμική ανάλυση εξαρτάται σε μεγάλο βαθμό από τις API κλήσεις και τις λειτουργίες του συστήματος αρχείων. Τα εκτελέσιμα προγράμματα ransomware που χρησιμοποιούν προσαρμοσμένες λειτουργίες αντί για τα προεπιλεγμένα API των Windows είναι δύσκολο να ανιχνευτούν με αυτό το σύστημα.

Ένα άλλο εργαλείο είναι το PEDA (Pre-Encryption Detection Algorithm) που αναπτύχθηκε από τους Kok et al. το 2020. Το PEDA βασίζεται σε προηγούμενες μεθόδους ανίχνευσης και πρόληψης και υλοποιεί ένα σύστημα ανίχνευσης δύο επιπέδων ικανό να εντοπίζει γνωστό και άγνωστο ransomware (Kok et al, 2020). Το επίπεδο ανάλυσης συμπεριφοράς λειτουργεί χρησιμοποιώντας ένα μοντέλο μηχανικής μάθησης που εκπαιδεύεται στις κλήσεις συναρτήσεων του λειτουργικού συστήματος που πραγματοποιούνται από το πιθανό δείγμα ransomware. Όλες οι κλήσεις συστήματος καταγράφονται έως ότου γίνει κλήση σε μια συνάρτηση κρυπτογράφησης, οπότε ο κατάλογος των κλήσεων που εξάγονται τροφοδοτείται στο μοντέλο για την δημιουργία της πρόβλεψης (Kok et al, 2020). Προκειμένου να συλλέξει τις κλήσεις συστήματος που πραγματοποιούνται χωρίς να τίθεται σε κίνδυνο το σύστημα του χρήστη, το PEDA εκτελεί την ανάλυση του δείγματος σε ένα ασφαλές εικονικό περιβάλλον (sandbox).

Το PEDA είναι ένα ιδιαίτερα προηγμένο εργαλείο ανίχνευσης ικανό να ανιχνεύει ransomware χωρίς να προκαλεί ζημιά στα αρχεία του χρήστη, αλλά η γενική του αποτελεσματικότητα περιορίζεται από το υψηλό υπολογιστικό κόστος της εκτέλεσης του sandbox. Το PEDA πετυχαίνει ποσοστά αναγνώρισης μίας επίθεσης 99,9% αποδεικνύοντας ότι είναι ένα ισχυρό σύστημα, αλλά το πιο σημαντικό είναι ότι μία σχετική μελέτη εντόπισε τρεις κλήσεις συστήματος που χρησιμοποιούνται από τα περισσότερα ransomware (Kok et al, 2020). Αυτές οι τρεις κλήσεις συστήματος έχουν σίγουρα ενσωματωθεί στα μοντέλα ανίχνευσης ransomware και θα συνεχίσουν να αποτελούν τη βάση των αμυντικών μηχανισμών τα επόμενα χρόνια.

4.3.6 Μέθοδοι ανίχνευσης πολλαπλών σταδίων

Σε πολύπλοκες επιθέσεις, στις οποίες το ransomware είναι ένα μόνο ένα μέρος τους, η ερμηνεία των συμβάντων και η χαρτογράφηση τους σε στόχους δεν έχει αποτυπωθεί επί του παρόντος στη βιβλιογραφία σε βάθος, ακρίβεια και αυτοματοποίηση, γεγονός που δυσχεραίνει την κατανόηση των πολύπλοκων επιθέσεων. Τα περισσότερα συστήματα ταξινόμησης είτε δεν είναι διαφανή ως προς τον τρόπο λειτουργίας τους είτε δεν μπορούν να ερμηνεύσουν σε βάθος την εσωτερική λειτουργία μιας κακόβουλης διαδικασίας ή ενός κακόβουλου προγράμματος. Τα εργαλεία ανίχνευσης που βασίζονται σε μοτίβα διαθέτουν συνήθως μια χειροκίνητα συμπληρωμένη, σημαντικά περιορισμένη βάση δεδομένων με συμβάντα που αντιστοιχίζει μία απομονωμένη συμπεριφορά π.χ. σε μια περιγραφική λέξη-κλειδί. Αυτό συχνά δεν είναι αρκετό για την πραγματική κατανόηση της επίθεσης στο σύνολό της. Οι ανωμαλίες, από την άλλη πλευρά, προσφέρουν συνήθως ελάχιστα άλλα εκτός από ένα όριο (threshold) που, όταν ξεπεραστεί, θα προκαλέσει μια ειδοποίηση (Luh et al, 2016).

Ένα τέτοιο σύστημα πολλαπλών σταδίων είναι ικανό να ανιχνεύει και να ταξινομεί ανώμαλες συμπεριφορές στα πλαίσια μίας διαδικασίας σε επίπεδο χρήστη (user session) παρατηρώντας και αναλύοντας όσες διεργασίες εκτελούνται στον πυρήνα του συστήματος. Για παράδειγμα ένα τέτοιο σύστημα ταξινομεί τη συμπεριφορά του συστήματος για την ανίχνευση ανωμαλιών με τη χρήση των μεθόδων Random Forest (RF) και SVM. Οι υποψήφιες εφαρμογές που είναι κατάλληλες για συνεχή παρακολούθηση από το σύστημα επιλέγονται αρχικά μέσω μιας προσαρμοσμένης διαδικασίας εξόρυξης (sentiment mining score) που βασίζεται στον λόγο λογαριθμικής πιθανότητας (log likelihood ratio - LLR) (Luh et al, 2017).

Για τη διαφανή ανίχνευση ανωμαλιών σε ένα χρονικό παράθυρο με σχετικά συμβάντα, οι ερευνητές του προτεινόμενου συστήματος χρησιμοποιούν δομές τύπου αστέρα που είναι μια διμερή αναπαράσταση σχεδιασμένη να προσεγγίζει την απόσταση επεξεργασίας μεταξύ γραφημάτων. Τα πρότυπα που αποτυπώνουν την συμπεριφορά του συστήματος δημιουργούνται αυτόματα και χρησιμοποιούνται για τον υπολογισμό τόσο του sentiment mining score (για το αν εντοπίζεται ανωμαλία ή όχι) όσο και μια έκθεση που περιέχει όλα

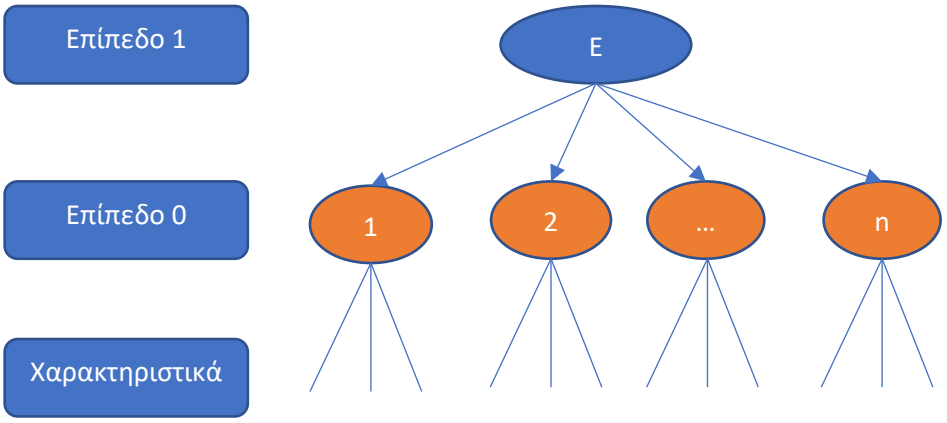
τα συναφή συμβάντα. Όπως αναφέρθηκε παραπάνω, οι ανωμαλίες που εξάγονται ταξινομούνται με τη χρήση της μεθόδου Random Forest και SVM.

Κατόπιν, τα πρόσφατα χαρακτηρισμένα μοτίβα αντιστοιχίζονται σε ένα ειδικό μοντέλο επιτιθέμενου-αμυνόμενου που εξετάζει στόχους, ενέργειες, δράστες, καθώς και τα πληροφοριακά στοιχεία που εμπλέκονται, γεφυρώνοντας έτσι το χάσμα μεταξύ των δεικτών επίθεσης και της λεπτομερούς σημασιολογίας της απειλής. Αυτό επιτρέπει τόσο την αξιολόγηση κινδύνου όσο και την υποστήριξη αποφάσεων για τον μετριασμό των στοχευμένων επιθέσεων.

Τα αποτελέσματα της παραπάνω έρευνας έδειξαν ότι το πρωτότυπο σύστημα είναι σε θέση να αναγνωρίσει το 99,8% όλων των ανωμαλιών στην δομή τύπου αστέρα ως καλοήθεις ή κακόβουλες. Σε σενάρια πολλαπλών κατηγοριών που επιδιώκουν να συσχετίσουν κάθε ανωμαλία με ένα ξεχωριστό μοτίβο επίθεσης που ανήκει σε ένα συγκεκριμένο στάδιο της επίθεσης, είχε επιτευχθεί σταθερή ακρίβεια 95,7%. Επιπλέον, αποδείχθηκε ότι το 88,3% των παρατηρούμενων επιθέσεων θα μπορούσε να αναγνωριστεί με την ανάλυση και ταξινόμηση μιας μόνιμης διαδικασίας στο σύστημα των Windows για μόλις 10 δευτερόλεπτα, εξαλείφοντας έτσι την ανάγκη παρακολούθησης κάθε (άγνωστης) εφαρμογής που εκτελείται σε ένα σύστημα.

Σε μία ανάλογη ερευνητική προσέγγιση χρησιμοποιήθηκαν πολλαπλοί ταξινομητές Logistic Regression (LR) σε δύο στάδια. Το πρώτο βήμα αποτελείται από n μοντέλα LR, όπου n είναι ο αριθμός των πιθανών κλάσεων. Κάθε μοντέλο εκπαιδεύεται για να εξάγει την πιθανότητα ένα δείγμα να ανήκει σε μία από τις n κλάσεις, με τη μεθοδολογία one-vs-all (δηλαδή ένα δείγμα είτε ανήκει στην Cn είτε όχι), έχοντας ως είσοδο τα πρωτογενή δεδομένα και χαρακτηριστικά τους.

Το δεύτερο βήμα είναι πανομοιότυπο με το LR, αλλά τώρα λαμβάνει ως χαρακτηριστικά την έξοδο κάθε ταξινομητή από το προηγούμενο επίπεδο, βγάζοντας την πιθανότητα ένα δείγμα να είναι κακόβουλο λογισμικό (**Διάγραμμα** *9*).



Διάγραμμα 9. Αναπαράσταση μοντέλου πολλαπλών επιπέδων

Έχοντας ορίσει το παραπάνω μοντέλο, ρυθμίζονται οι n κλάσεις που ενδιαφέρουν τους χρήστες του συστήματος. Οι κλάσεις δεν επισημαίνουν απλά αν ένα πρόγραμμα είναι καλό ή κακόβουλο, αλλά προσδιορίζουν και κάποια υποκλάση. Για παράδειγμα, χαρακτηριστικές κατηγορίες κακόβουλου λογισμικού: για παράδειγμα, ιός, trojan, worm, ransom, spyware και άλλες ορίζονται ως τυπικές κατηγορίες. Επιπλέον υπάρχει η κλάση goodware για να επισημαίνεται η εκτέλεση μη κακόβουλου προγράμματος.

Πέρα από την στατική ανάλυση των χαρακτηριστικών που εμφανίζει αρκετούς περιορισμούς, ειδικά εάν ένα δείγμα είναι συμπιεσμένο, κρυπτογραφημένο ή συσκευασμένο, εφαρμόζεται δυναμική ανάλυση μέσω του εργαλείου Cuckoo. Δεδομένου ότι το Cuckoo εκτελεί τα παρεχόμενα δείγματα μέσα σε μια εικονική μηχανή, παρακολουθεί το δείγμα από δυναμική άποψη. Αυτή η παρακολούθηση περιλαμβάνει πληροφορίες όπως η ακολουθία των κλήσεων βιβλιοθήκης και οι κατηγορίες και η δραστηριότητα στο δίκτυο και των αρχείων προς επεξεργασία. Για παράδειγμα, όταν το Cuckoo εκτελεί και παρακολουθεί ένα δείγμα, καταγράφει κάποιες κλήσεις βιβλιοθήκης χαμηλού επιπέδου, τις οποίες στη συνέχεια αναθέτει σε μια κατηγορία. Υπάρχουν συνολικά 14 διαφορετικές κατηγορίες που ορίζονται από το Cuckoo: *anomaly, device, filesystem, hooking, misc, network, process, registry, services, socket, synchronization, system, threading and windows*.

Ο δεύτερος τύπος πληροφόρησης μέσα από τη δυναμική ανάλυση είναι ο αριθμός των εκτελέσεων στις ρουτίνες βιβλιοθήκης, οι οποίες σχετίζονται στενά με τις κατηγορίες των εκτελέσεων παραπάνω. Ενώ οι κατηγορίες των εκτελέσεων παρέχουν τον αριθμό των εκτελέσεων ν για μια δεδομένη κατηγορία, οι κλήσεις σε ρουτίνες της βιβλιοθήκης παρέχουν τον αριθμό για κάθε εκτέλεση ρουτίνας στη βιβλιοθήκη. Κάθε κατηγορία από το προηγούμενο χαρακτηριστικό περιέχει ένα σύνολο από ρουτίνες της βιβλιοθήκης του λειτουργικού συστήματος, επομένως κάθε εκτέλεση στη βιβλιοθήκη αντιστοιχεί σε κάποια κατηγορία. Το Cuckoo καταγράφει τον αριθμό των εκτελέσεων για 163 διαφορετικές λειτουργίες, που κυμαίνονται από το άνοιγμα και το κλείσιμο αρχείων, μέχρι το άνοιγμα και το κλείσιμο sockets.

Το τρίτο και τελευταίο βήμα της δυναμικής ανάλυσης, περιλαμβάνει τις προσαρμοσμένες υπογραφές αρχείων του Cuckoo. Αυτές οι υπογραφές αρχείων δημιουργούνται από ορισμένες δραστηριότητες που το Cuckoo θεωρεί κακόβουλες ή ύποπτες. Για παράδειγμα, αν ένα δείγμα κατανέμει μνήμη και στη συνέχεια την καθιστά εκτελέσιμη, μπορεί να υποδηλώνει κάποια τεχνική packing ή obfuscation που παρουσιάσαμε σε προηγούμενη ενότητα. Παρόλο που ορισμένες υπογραφές ορίζονται από μια ακολουθία κλήσεων στη βιβλιοθήκη, η οποία θα μπορούσε επίσης να επιτευχθεί δημιουργώντας n-gramms του προηγουμένως καθορισμένου χαρακτηριστικού, η χρήση των ήδη καθορισμένων υπογραφών Cuckoo μειώνει τον χρόνο εκπαίδευσης. Για παράδειγμα, η δημιουργία bi-gramms με κλήσεις στη βιβλιοθήκη, δεδομένου ότι υπάρχουν 144 μοναδικές κλήσεις, θα απέδιδε πάνω από 20.000 πιθανά χαρακτηριστικά, κάτι που γίνεται εξαιρετικά μη πρακτικό όταν εξετάζεται ένας υψηλότερος βαθμός των n-gramms.

Η παραπάνω τεχνική μπορεί να εφαρμοστεί και σαν ένα χειροκίνητο εργαλείο (online ή μη) ανίχνευσης malware (ransomware). Σε πρόσφατη ανάλυση με δείγματα του petya malware το επίπεδο ακρίβειας των αποτελεσμάτων του εργαλείου ήταν στο 78.73%. Μία δεύτερη εφαρμογή, που είναι ακόμα σε στάδιο υλοποίησης, αλλά εκτελείται με αυτοματοποιημένο τρόπο, είναι η σάρωση συνημμένων μηνυμάτων ηλεκτρονικού ταχυδρομείου για την ανίχνευση κακόβουλου λογισμικού. Το εργαλείο μπορεί να τοποθετηθεί στο διακομιστή αλληλογραφίας ως πρόγραμμα σάρωσης για το φιλτράρισμα και τη σάρωση των μηνυμάτων ηλεκτρονικού ταχυδρομείου. Η υλοποίηση αυτή λειτουργεί με τη δημιουργία ενός προσαρμοσμένου σαρωτή ιών, ο οποίος λαμβάνει συνημμένα μηνύματα ηλεκτρονικού ταχυδρομείου και τα στέλνει στην υπηρεσία

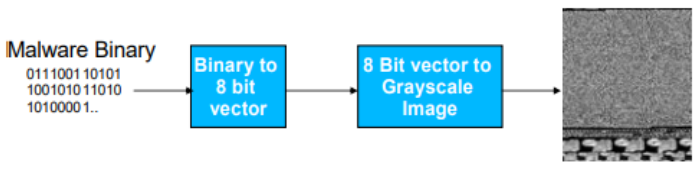
ανίχνευσης κακόβουλου λογισμικού που περιγράφηκε προηγουμένως. Μετά τη λήψη των αποτελεσμάτων, ο προσαρμοσμένος σαρωτής τροποποιεί το αντικείμενο ηλεκτρονικού ταχυδρομείου ώστε να περιλαμβάνει τα αποτελέσματα της ταξινόμησης.

4.3.7 Τεχνητή νοημοσύνη και Βαθειά Μάθηση

Η Βαθειά Μάθηση, ως μία άλλη τεχνική τεχνητής νοημοσύνης, είναι μια άλλη κατηγορία τεχνικών μηχανικής μάθησης που εκμεταλλεύεται πολλά επίπεδα επεξεργασίας μη γραμμικής πληροφορίας για εξαγωγή και μετατροπή χαρακτηριστικών καθώς και την ανάλυση και ταξινόμηση μοτίβων με εποπτευόμενο ή μη εποπτευόμενο τρόπο (Deng and Yu, 2013).

Η βαθιά μάθηση χρησιμοποιεί νευρωνικά δίκτυα (Neural Networks – NN) πολλαπλών επιπέδων. Αυτή η μορφή νευρωνικών δικτύων (NN) προσομοιώνει τη λειτουργία των νευρωνικών δικτύων του ανθρώπινου εγκεφάλου (Krohn et al., 2020). Με τη χρήση βαθιάς μάθησης, είναι δυνατή η ανάπτυξη αλγορίθμων που μπορούν να εφαρμοστούν για την επίλυση (πολλαπλών) προβλημάτων ταξινόμησης, όπως η διάκριση μεταξύ καλού και κακόβουλου λογισμικού και η διάκριση διαφορετικών κατηγοριών κακόβουλου λογισμικού χωρίς να χρειάζεται να εφαρμοστεί εκ των προτέρων μηχανική χαρακτηριστικών, η οποία, όπως αναφέρθηκε παραπάνω, είναι απαραίτητη για τους παραδοσιακούς αλγορίθμους ML (Hardy et al., 2016; Krohn et al., 2020).

Αρκετές μέθοδοι ταξινομούν βαθιάς μάθησης εστιάζουν στην ανίχνευση κακόβουλο λογισμικό με βάση μια εικόνα. Οι μέθοδοι αυτές προέρχονται από τον τομέα της επεξεργασίας εικόνων (image processing), που αναλύουν την εικόνα ενός δυαδικού αρχείου (Vu et al., 2019; Yan et al., 2018) και τα μοτίβα που περιέχει. Ένα παράδειγμα αυτής της διαδικασίας παρουσιάζεται στο **Διάγραμμα** *10*.

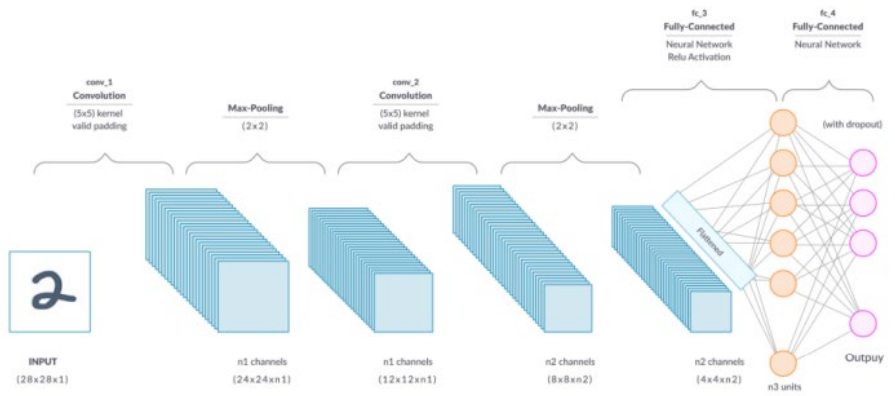


Διάγραμμα 10. Περιγραφή διαδικασίας σε υψηλό επίπεδο μετατροπής ενός δυαδικού αρχείου σε εικόνα (Hassan, 2019)

4.3.8 Συνελικτικά νευρωνικά δίκτυα

Το συνελικτικό νευρωνικό δίκτυο (Convolutional Neural Network – CNN) είναι μια αρχιτεκτονική Νευρωνικών Δικτύων που αναπτύσσεται σε διάφορους τομείς, ο πιο γνωστός από τους οποίους είναι η ταξινόμηση φωτογραφιών ή εικόνων (Cawsey, 1998, Krizhevsky et al., 2012). Η αρχιτεκτονική του CNN βασίζεται στη λειτουργία του ανθρώπινου οπτικού φλοιού (Krohn et al., 2020) και παρουσιάζεται στην **Error! Reference source not found.**. Οι αλγόριθμοι βαθιάς μάθησης με αρχιτεκτονική CNN αναφέρονται σε αρκετές μελέτες (Hardy et al., 2016- Vu et al., 2019- Yan et al., 2018) ως μια αξιόπιστη εφαρμογή μηχανικής μάθησης για τη ταξινόμηση αρχείων σε κακόβουλα ή όχι χρησιμοποιώντας τεχνικές ανάλυσης χαρακτηριστικών, όπως τεχνικές τύπου gists και SIFT (Xie et al., 2017).

Επειδή αυτοί οι τύποι Νευρωνικών Δικτύων προορίζονται κυρίως για την αναγνώριση μοτίβων στα δεδομένα χρησιμοποιώντας τις προαναφερθείσες τεχνικές, το NN μαθαίνει" από μόνο του τα χαρακτηριστικά των δεδομένων εισόδου χρησιμοποιώντας μία τεχνική που ονομάζεται back propagation (Géron, 2019; Krohn et al., 2020).



Διάγραμμα 11. Αρχιτεκτονική Συνελικτικού Νευρωνικού Δικτύου (Keras, 2020)

Το CNN είναι μια αρχιτεκτονική δικτύου με διάφορα κρυφά στρώματα μεταξύ του στρώματος εισόδου και του στρώματος εξόδου. Γενικά, τα κρυφά στρώματα αποτελούνται από στρώματα συνέλιξης, συγκέντρωσης (pooling) και πλήρως συνδεδεμένα στρώματα. Αυτά τα κρυφά στρώματα είναι υπεύθυνα για την εξαγωγή χαρακτηριστικών, όπου τα χαρακτηριστικά μαζί σχηματίζουν ένα μέρος ή ένα ολόκληρο μοτίβο που μπορεί να αναγνωριστεί από τον αλγόριθμο προκειμένου να ταξινομηθεί ένα δείγμα ως καλοήθη ή κακόβουλο λογισμικό (Géron, 2019; Krohn et al., 2020).

Τα νευρωνικά δίκτυα που βασίζονται στη Βαθιά Μάθηση όπως τα CNN έχουν καλύτερη ακρίβεια από τα Νευρωνικά Δίκτυα που βασίζονται σε ρηχές μεθόδους μηχανικής μάθησης (Simonyan and Zisserman, 2015; Bhodia et al., 2019). Αυτό γιατί η πρώτη κατηγορία μπορεί να εξάγει περισσότερα χαρακτηριστικά και παραμέτρους για χρήση στο μοντέλο εκπαίδευσης. Το μειονέκτημα τους ωστόσο είναι οι υψηλές απαιτήσεις για εκπαιδευτικά δεδομένα και πόρους CPU/GPU για την αποτελεσματική εκπαίδευσή τους.

4.4 Σύνοψη

Ο παρακάτω πίνακας συνοψίζει τις μεθόδους που παρουσιάσαμε στις προηγούμενες ενότητες αυτού του κεφαλαίου. Παρουσιάζει τα κύρια χαρακτηριστικά της κάθε μεθόδου, το ποσοστό ακρίβειας που καταγράφηκε σε πρόσφατες δημοσιεύσεις, τους απαιτούμενους πόρους και τον χρόνο ανίχνευσης.

Μέθοδος	**Χαρακτηριστικά**	**Ακρίβεια**	**Απαιτούμενοι πόροι**	**Χρόνος ανίχνευσης**
Στατική ανάλυση	μετατροπή σε κώδικα μηχανής, ανάλυση κώδικα από malware reverse engineer	<50%	malware reverse engineer	Μερικές ώρες ή ημέρες
Τεχνικές ταξινόμησης χαρακτηριστικών που βασίζονται στον κώδικα μηχανής ή/και	Νευρωνικό Δίκτυο (CNN, RNN), Μοντέλο ακολουθίας συστημικών κλήσεων κακόβουλου λογισμικού	85.6%	Εκπαίδευση του Νευρωνικού Δικτύου με τη χρήση εργαλείων Tensorflow, Theano	Ενημέρωση σε πραγματικό χρόνο μετά από εκπαίδευση του μοντέλου

στη συμπεριφορά			Χρήση γραφικών επεξεργαστών (GPUs)	
Τεχνικές συσχετισμού εικόνων (image based) χωρίς την ταξινόμηση χαρακτηριστικών	Δημιουργία πινάκων συσχετισμού εικόνων ως αποτέλεσμα της ανάλυσης κώδικα	98.4% στην ίδια κατηγορία ransomware, 30.9% μεταξύ διαφορετικών κατηγοριών	Εργαλεία μετατροπής κώδικα μηχανής (IDA Pro ή OllyDbg), Εργαλεία γραφικής ανάλυσης	Μετά την εκτέλεση του προγράμματος
Αλγόριθμοι Μηχανικής Μάθησης και Τεχνικές Εξόρυξης	Εφαρμογή αλγορίθμων naive Bayes, decision trees, support vector machines, και boosting	99.6%	Εφαρμογή των αλγορίθμων σε 291 δείγματα κακόβουλου λογισμικού	Μετά την εκτέλεση του προγράμματος
Αλγόριθμοι Μηχανικής Μάθησης	Εφαρμογή αλγορίθμων SVM για signature-based matching και Information Gain για εξαγωγή ορισμένων χαρακτηριστικών	81,40%	Genome Project's dataset of Android applications	Μετά την εκτέλεση του προγράμματος
UNVEIL	τεχνικές ανάλυσης κειμένου και εξαγωγή στιγμιότυπων της οθόνης της επιφάνειας εργασίας. στατιστική ανάλυση με βάση τη χρήση της μνήμης, τη χρήση του επεξεργαστή και τους ρυθμούς I/O του δίσκου για τον εντοπισμό μη φυσιολογικής συμπεριφοράς	96,3%	Cuckoo Sandbox	Μετά την εκτέλεση του προγράμματος
ShieldFS	παρακολούθηση σε χαμηλό επίπεδο των δραστηριοτήτων του συστήματος αρχείων (shadowing) υπολογισμός της εντροπίας των λειτουργιών εγγραφής και της συχνότητας ανάγνωσης, εγγραφής και καταχώρισης φακέλων	0,9985+%	Περιβάλλον προσομοίωσης με εικονικά μηχανήματα	Ενημέρωση σχεδόν σε πραγματικό χρόνο
CryptoDrop	παρακολούθηση αλλαγών σε αρχεία διακρίνοντας το ransomware σε τρεις μεγάλες κατηγορίες	100% σε δοκιμή με 5,099 αρχεία – ανίχνευση 492	Υλοποίηση αρχιτεκτονικής του προγράμματος σε Windows	Ενημέρωση σχεδόν σε πραγματικό χρόνο

	συναρτήσεις ομοιότητας	κακόβουλων αρχείων		
EldeRan	Δυναμική ανάλυση σε ένα sandboxed περιβάλλον τα ίχνη δειγμάτων που προέρχονται από δύο σύνολα δεδομένων ransomware και goodware. Εφαρμογή Regularized Logistic Regression classifier για Ανάλυση χαρακτηριστικών: (i) κλήσεων API των Windows , (ii) λειτουργιών κλειδιών μητρώου, (iii) λειτουργιών συστήματος αρχείων, (iv) λειτουργιών αρχείων που εκτελούνται ανά επέκταση αρχείου, (v) κατάλογο Λειτουργιών καταλόγου, (vi) Απορριφθείσα Αρχεία , και vii) Συμβολοσειρές	96.3%	Υλοποίηση του αλγορίθμου σε Matlab για τη πραγματοποίηση των πειραμάτων	Ενημέρωση σχεδόν σε πραγματικό χρόνο
ACGAN	ταξινόμησης δεδομένων με βάση μηχανική μάθηση όπως Random Forest, SVM, Naive Baysian και Λογιστική Παλινδρόμηση	98,2%	Πρόγραμμα προσομοίωσης	Ενημέρωση σχεδόν σε πραγματικό χρόνο
ScaleMalNet	νευρωνικό δίκτυο πολλαπλών επιπέδων perceptron για την ανίχνευση, ταξινόμηση και κατηγοριοποίηση κακόβουλων προγραμμάτων zeroday.	98%	Ember dataset και πρόγραμμα υλοποίησης νευρωνικού δικτύου	Ενημέρωση σχεδόν σε πραγματικό χρόνο
Ransomware Detection Framework	Μηχανή παραγωγής χαρακτηριστικών με τεχνικές αντιστροφής κώδικα και προ-επεξεργασίας (μέθοδοι σύγκρισης ομοιότητας) Μοντέλο Μηχανικής Μάθησης	98%	Εφαρμογή προγράμματος σε δείγματα από Virus Total, Virus Share και theZoo	Μετά την εκτέλεση του προγράμματος

Reduced Opcode Sequence And Image Similarity	Μετατροπή ακολουθίας εκτελέσιμων αρχείων σε μια εικόνα σε κλίμακα του γκρι. Εφαρμογή Linear Discrimant Analysis (LDA) για το διαχωρισμό δύο ή περισσότερων κλάσεων με τη τεχνική της μείωσης των διαστάσεων για τη βελτίωση της απόδοσης του μοντέλου	97.3%	Εφαρμογή προγράμματος σε επιλεγμένα δείγματα	Μετά την εκτέλεση του προγράμματος
HelDroid	Τεχνικές ανάλυσης κειμένου σε επίπεδο εφαρμογής	97%	Εφαρμογή προγράμματος σε επιλεγμένα δείγματα	Μετά την εκτέλεση του προγράμματος
Memory-Assisted-Stochastic-Dynamic-Fixed-Point	Deep Belief Network (DBN) κατηγοριοποίησης χαρακτηριστικών τεσσάρων επιπέδων	91%	Εφαρμογή προγράμματος σε επιλεγμένα δείγματα	Ενημέρωση σε πραγματικό χρόνο μετά από εκπαίδευση του μοντέλου
DRTHIS	Εφαρμογή τεχνικών Long Short-Term Memory (LSTM) και Convolutional Neural Network	97.2%	Keras deep learning framework. Εφαρμογή προγράμματος σε επιλεγμένα δείγματα	Ενημέρωση σε πραγματικό χρόνο μετά από εκπαίδευση του μοντέλου
RansHunt	στατική και δυναμική ανάλυση για τη δημιουργία υβριδικού συνόλου χαρακτηριστικών: Function Length Frequency, Printable String Information	97.1%	IDAPro code analyzer Cuckoo sandbox Εφαρμογή προγράμματος σε επιλεγμένα δείγματα	Ενημέρωση σε πραγματικό χρόνο
RansomWall	στατική και δυναμική ανάλυση για τη δημιουργία υβριδικού συνόλου χαρακτηριστικών σε πολλαπλά επίπεδα: - Static Analysis Engine - Honey Files & Trap Layer - Dynamic Analysis Engine - File Backup Layer - Machine Learning Engine	98.25%	Sandbox περιβάλλον	Ενημέρωση σε πραγματικό χρόνο

PEDA	1ο επίπεδο αλγορίθμου: μοντέλο μηχανικής μάθησης που εκπαιδεύεται στις κλήσεις συναρτήσεων του λειτουργικού συστήματος 2ο επίπεδο: σύγκριση υπογραφής κακόβουλου προγράμματος με το Signature Repository	99.9%	ανάλυση του δείγματος σε ένα ασφαλές εικονικό περιβάλλον (sandbox).	Ενημέρωση σε πραγματικό χρόνο
Anomaly-based Threat Detection & Explication System	Ανίχνευση ανώμαλων συμπεριφορών σε επίπεδο χρήστη αναλύοντας διεργασίες στον πυρήνα του συστήματος.	99,8%	Υλοποίηση των αλγορίθμων Random Forest (RF) και SVM και διαδικασίας εξόρυξης sentiment mining score	Ενημέρωση σε πραγματικό χρόνο

Πίνακας 4. Περίληψη μεθόδων μηχανικής μάθησης που εφαρμόζουν στατική, δυναμική ή υβριδική ανάλυση

Κεφάλαιο 5
Συμπεράσματα

5.1 Στρατηγικές αντιμετώπισης των επιθέσεων ransomware

Η παρούσα εργασία παρουσιάζει ένα ολιστικό πλαίσιο επεξήγησης του θεωρητικού υπόβαθρου των επιθέσεων ransomware και της μοντελοποίησης τους ως απειλή (attack vector) στα προηγούμενα κεφάλαια. Επιπλέον, παρουσιάζει μια ταξινόμηση των τεχνικών εντοπισμού επιθέσεων ransomware τα τελευταία χρόνια εστιάζοντας σε νέες τεχνικές που χρησιμοποιούν μεθόδους τεχνητής νοημοσύνης ή άλλες τεχνικές.

Επιπλέον, η παρούσα εργασία προτείνει στρατηγικές αντιμετώπισης των επιθέσεων ransomware με σκοπό την άμεση ανταπόκριση των οργανισμών και την άμεση ανάκαμψη τους.

Πράγματι, οι σύγχρονοι οργανισμοί πρέπει να υπερασπιστούν επαρκώς τις υπολογιστικές τους υποδομές και τους τελικούς τους χρήστες. Λαμβάνοντας υπόψη το αντίστοιχο πλαίσιο με τίτλο Framework for Critical Infrastructure Cybersecurity[5] που προτείνει το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST) των ΗΠΑ ο κάθε οργανισμός μπορεί να καταρτίσει ένα σχέδιο αντιμετώπισης τέτοιων επιθέσεων. Αυτό περιλαμβάνει πέντε βήματα:

Το πρώτο βήμα καλεί τους υπεύθυνους ασφαλείας να προσδιορίσουν τα περιουσιακά στοιχεία που διατρέχουν κίνδυνο εντός του οργανισμού. Μετά τη διενέργεια αξιολόγησης κινδύνου, πρέπει να καταβληθούν προσπάθειες για την προστασία των οντοτήτων που

[5] https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11

διατρέχουν κίνδυνο. Αυτό μπορεί να επιτευχθεί ως δεύτερο βήμα με την εφαρμογή μέτρων που κυμαίνονται από τις παραδοσιακές άμυνες σε επίπεδο δικτύου, όπως τα τείχη προστασίας, μέχρι και την εκπαίδευση του προσωπικού για την πλοήγηση στον κυβερνοχώρο. Το τρίτο βήμα της διαδικασίας απαιτεί την ανάπτυξη και την εφαρμογή μιας υποδομής ανίχνευσης απειλών. Πρέπει να τεθούν σε λειτουργία συστήματα για την ανίχνευση απειλών που στοχεύουν την ευρύτερη IT, Cloud, OT υποδομή και τους τελικούς χρήστες.

Μόλις ανιχνευθεί η απειλή και εντοπιστεί, οι αρμόδιες ομάδες του οργανισμού πρέπει να ανταποκριθούν. Ένα επιτυχημένο σχέδιο αντιμετώπισης, ως τέταρτο βήμα, θα πρέπει να ενημερώνει για τις ενέργειες που συσχετίζονται με μια συγκεκριμένη απειλή. Βασικό στοιχείο της αντιμετώπισης απειλών είναι η ικανότητα να περιορίσει την απειλή, μετριάζοντας την πρόσθετη ζημιά στο δίκτυο.

Το τελικό (πέμπτο) βήμα του πλαισίου κυβερνοασφάλειας του NIST είναι η ανάκαμψη. Οι διαχειριστές των συστημάτων πρέπει να έχουν την ικανότητα να αποκαθιστούν οποιεσδήποτε υπηρεσίες ενδέχεται να έχουν επηρεαστεί λόγω της επίθεσης. Όταν πρόκειται για δίκτυα που υποστηρίζουν υποδομές ζωτικής σημασίας, κάθε χρονικό διάστημα κατά το οποίο οι υπηρεσίες είναι εκτός λειτουργίας μπορεί να είναι καταστροφικό. Για το λόγο αυτό, η έγκαιρη ενημέρωση είναι υψίστης σημασίας όταν γίνεται ανάκαμψη από μια εντοπισμένη απειλή.

5.2 Προς ένα πλάνο ανταπόκρισης και ανάκαμψης από επιθέσεις ransomware

Τέλος, η παρούσα εργασία προτείνει ένα σχέδιο αντίδρασης και ανάκαμψης ανεξάρτητα από τα χαρακτηριστικά μίας επίθεσης ransomware με σκοπό ο οργανισμός να ανακάμψει λειτουργικά και να αποφύγει την πληρωμή των λύτρων. Κατά συνέπεια, η ανίχνευση της απειλής δεν είναι τόσο υψίστης σημασίας όσο είναι να υπάρχει ένα σχέδιο που να επιτρέπει σε υποδομές ζωτικής σημασίας να είναι σε θέση να ανταποκριθούν κατάλληλα σε επιθέσεις ransomware και να ανακάμψουν από αυτές.

Ένα θύμα μιας επίθεσης ransomware θα πρέπει πρώτα να παρατηρήσει την τρέχουσα κατάσταση του συστήματος πριν λάβει μια απόφαση. Πρέπει να γίνουν συγκρίσεις μεταξύ του τι ο επιτιθέμενος ισχυρίζεται ότι έχει παραβιάσει και τι πραγματικά έχει επηρεαστεί. Σε ορισμένες περιπτώσεις, ο αμυνόμενος μπορεί να μην είναι σε θέση να επιβεβαιώσει ή

να διαψεύσει τους ισχυρισμούς του επιτιθέμενου. Ως αποτέλεσμα, ο αμυνόμενος μπορεί να αναγκαστεί να υποθέσει το χειρότερο σενάριο. Μετά τον καθορισμό της τρέχουσας κατάστασης του συστήματος, οι διαχειριστές κρίσιμων υποδομών μπορούν να αρχίσουν να αναπτύσσουν τρόπους αντίδρασης είτε για να ικανοποιήσουν τις απαιτήσεις του επιτιθέμενου είτε για να ακυρώσουν την επίθεση. Οι αποφάσεις θα πρέπει να συνδέονται με δύο τουλάχιστον μετρικές:

- Κόστος: το ποσό του κεφαλαίου που απαιτείται για την υλοποίηση της λύσης.
- Χρόνος: ο χρόνος που απαιτείται για την εφαρμογή της λύσης (μη διαθεσιμότητα του συστήματος).

Οι διαχειριστές των πληροφοριακών, βιομηχανικών συστημάτων και άλλων κρίσιμων υποδομών μπορούν να επιλέξουν να χρησιμοποιήσουν είτε μέτρα αντίδρασης είτε προληπτικά μέτρα. Τα μέτρα αντίδρασης δεν απαιτούν από τον αμυνόμενο να επενδύσει χρήματα ή χρόνο εκ των προτέρων. Εάν η υπολογιστική ή βιομηχανική υποδομή ή οι τελικοί χρήστες έχουν επηρεαστεί από μία επίθεση ransomware, οι διαχειριστές των συστημάτων μπορούν να επιχειρήσουν να επαναφέρουν τα συστήματα στην αρχική τους λειτουργία. Για το λόγο αυτό, θα πρέπει να διατηρούν εφεδρικά αντίγραφα σε διαφορετικά επίπεδα.

Για παράδειγμα, σε μία βιομηχανική υποδομή μπορεί να χρειαστεί ο επαναπρογραμματισμός της PLC υποδομής. Εάν ο επαναπρογραμματισμός του PLC αποτύχει, οι διαχειριστές πρέπει να εξετάσουν το ενδεχόμενο αντικατάστασης του PLC. Ωστόσο το κόστος αντικατάστασης είναι πολύ υψηλό, αλλά και ο χρόνος που απαιτείται είναι σημαντικός. Οι διαχειριστές πρέπει να διασφαλίσουν ότι μία απειλή ransomware έχει εξουδετερωθεί πριν να εξετάσουν το ενδεχόμενο αντικατάστασης του PLC. Διαφορετικά μία μόνιμη απειλή στο βιομηχανικό δίκτυο μπορεί να θέσει σε κίνδυνο το νέο ελεγκτή. Αντίστοιχα παραδείγματα μπορεί να προκύψουν σε μία υπολογιστική υποδομή: οι διαχειριστές μπορεί να χρειαστεί να δημιουργήσουν νέους εξυπηρετητές (πχ Domain Controllers) αν δεν έχουν εφεδρικά τους αντίγραφα ή δεν διαθέτουν εφεδρική υποδομή (Disaster Recovery site).

Οι διαχειριστές μπορούν να επιταχύνουν τη διαδικασία αντίδρασης και ανάκαμψης επενδύοντας πόρους σε ένα προληπτικό σύστημα κυβερνοάμυνας για την αντιμετώπιση επιθέσεων ransomware. Ένα παράδειγμα ενός προληπτικού αμυντικού σχήματος είναι η

εφαρμογή της ασφάλειας μέσω πλεονασμού. Έτσι, για παράδειγμα στα πλαίσια ενός βιομηχανικού δικτύου, οι ιδιοκτήτες μπορούν να επιλέξουν να επενδύσουν σε εφεδρικά PLC. Αντίστοιχα σε μία υπολογιστική υποδομή οι ιδιοκτήτες μπορούν να επενδύσουν σε εφεδρικές υποδομές ή εξοπλισμό δημιουργίας αντιγράφων ασφαλείας. Ο πλεονασμός δεν υπερασπίζεται μόνο μία καταστροφή από κυβερνο επιθέσεις /εισβολείς, αλλά προστατεύει επίσης το σύστημα από βλάβες υλικού.

Τα εφεδρικά συστήματα μπορούν να διαμορφωθούν σε έναν από τους δύο τρόπους λειτουργίας:

- hot standby: Το δευτερεύον βιομηχανικό ή πληροφοριακό σύστημα είναι πάντα ενεργοποιημένο και έχει τη δυνατότητα να αποκτήσει τον έλεγχο του συστήματος ακαριαία.
- cold standby: Το δευτερεύον σύστημα παραμένει απενεργοποιημένο έως ότου ενεργοποιηθεί για να ελέγξει το κύριο σύστημα.

Κάθε επιλογή έχει πλεονεκτήματα και μειονεκτήματα. Το κύριο πλεονέκτημα της χρήσης ενός hot standby είναι η δυνατότητα της άμεσης εναλλαγής του εφεδρικού συστήματος στο ρόλο του πρωτεύοντος. Επειδή το εφεδρικό είναι πάντα ενεργοποιημένο, έχει γνώση της τρέχουσας και προηγούμενης κατάστασης του συστήματος. Ωστόσο, επειδή το δευτερεύον σύστημα είναι πάντα ενεργοποιημένο, ο επιτιθέμενος μπορεί να είναι σε θέση να ανιχνεύσει την παρουσία του στο δίκτυο και να υποβαθμίσει τη διαθεσιμότητα του.

Αντί της χρήσης ενός συστήματος εφεδρικής λειτουργίας, οι διαχειριστές μπορούν να επιλέξουν να χρησιμοποιήσουν έναν cold standby σύστημα. Σε αυτή τη περίπτωση, ο επιτιθέμενος έχει μεγαλύτερη πρόκληση εντοπισμό του δευτερεύοντος συστήματος λόγω του ότι το εφεδρικό σύστημα απενεργοποιείται όταν δεν βρίσκεται σε χρήση. Ένα μειονέκτημα της χρήσης cold standby είναι ο χρόνος που χρειάζεται το σύστημα για να εκκινήσει και να αποκτήσει τον πλήρη έλεγχο της διαδικασίας. Ο χρόνος αυτός ποικίλλει ανάλογα με την πολυπλοκότητα της ελεγχόμενης διαδικασίας. Η ασφάλεια μέσω πλεονασμού μπορεί να είναι μια αποτελεσματική επιλογή κατά την άμυνα των πληροφοριακών ή βιομηχανικών συστημάτων (IoT) και των τελικών χρηστών, ωστόσο το κόστος είναι σχετικά υψηλό (για παράδειγμα στο βιομηχανικό δίκτυο, οι οργανισμοι πρέπει να επενδύσουν σε πρόσθετους ελεγκτές και μηχανισμούς εναλλαγής).

5.3 Συμπεράσματα – Μελλοντική επέκταση

Οι επιθέσεις Ransomware είναι μια αυξανόμενη απειλή, και αναμφισβήτητα οι επιτιθέμενοι θα συνεχίζουν να καινοτομούν. Καθώς έχουν βάλει ως στόχο κυρίως οργανισμούς και επιχειρήσεις που μπορούν να τους αποσπάσουν τεράστια ποσά ως αμοιβή, βρίσκουν συνεχώς νέους τρόπους να προκαλούν επιπτώσεις στα συστήματα τους.

Αποδεδειγμένες μέθοδοι μόλυνσης όπως το phishing ή το malspam και τεχνικές προώθησης σε ιστότοπους διευκολύνονται από exploitation kits και νέες τεχνικές Ransomware-as-a-Service (RaaS). Παράλληλα με αυτές τις μεθόδους, νέες πιο αποτελεσματικές παραλλαγές ransomware εξαπλώνονται ως ιός χωρίς την αλληλεπίδραση του χρήστη έχουν προστεθεί στο οπλοστάσιο των επιτιθέμενων. Σαφώς το ισχυρό οικονομικό κίνητρο για τους επιτιθέμενους τους έχει προτρέψει να αναπτύξουν νέες τεχνικές για να μεγιστοποιήσουν τα έσοδά τους από την εκμετάλλευση των χρηστών.

Το σύγχρονο ransomware βρίσκεται στην ακμή του από τη γέννηση του το 2006. Εμφανίστηκε τη στιγμή που η παγκόσμια κοινότητα ήταν εντελώς απροετοίμαστη να το αντιμετωπίσει και έτσι με πολλούς τρόπους εξακολουθεί να εκμεταλλεύεται το στοιχείο του αιφνιδιασμού. Οι κυβερνο-εγκληματίες είναι πάντα ένα βήμα μπροστά γιατί όταν αναπτύσσουν νέες και δημιουργικές μέθοδοι επίθεσης χρειάζεται χρόνος για τους ειδικούς στην κυβερνο-ασφάλεια να σχεδιάσουν και να εφαρμόσουν νέες τεχνικές άμυνας. Το γεγονός ότι η επιφάνεια επίθεσης για τους δημιουργούς ransomware επεκτείνεται ταχύτατα καθώς ο κόσμος ψηφιοποιείται και διασυνδέονται μεταξύ τους όλο και περισσότερες συσκευές (πχ IoT) δυσκολεύει περισσότερο τις παραπάνω προσπάθειες. Επιπλέον, οι επιτιθέμενοι χρησιμοποιούν επιχειρηματικά μοντέλα για να εξειδικεύουν την εργασία τους, επιτρέποντας την ταχύτερη ανάπτυξη από όλο και πιο ισχυρούς προγραμματιστές και με πιο απειλητικούς τρόπους διανομής. Για τους παραπάνω λόγους το ransomware δεν πρόκειται να εξαφανιστεί άμεσα.

Η αποτελεσματικότητα των τεχνικών άμυνας ενάντια στο Ransomware τείνει να αυξάνεται και στους τρεις πυλώνες της ανάκτησης, ανίχνευσης και προτροπής, καθώς όλο και περισσότερη έρευνα και ανάπτυξη αφιερώνεται σε αυτά. Για περίπου δεκαπέντε χρόνια οι ερευνητές ασφαλείας δεν είχαν άλλη επιλογή από το να αντιδράσουν στις επιθέσεις και να αναλύουν τις μεθόδους τους. Αλλά τα τελευταία χρόνια λεπτομερή,

ολοκληρωμένα μοντέλα έχουν γνωστοποιηθεί, επιτρέποντας στους ειδικούς να εργάζονται προληπτικά για τη βελτίωση των μεθόδων αντίδρασης. Οι όποιοι μηχανισμοί τίθενται σε ισχύ δεν θα ήταν σε θέση να κατανοήσουν τις τεχνικές της επίθεσης χωρίς την ανάλυση της συμπεριφοράς που θέτει τις βάσεις για την ανάπτυξη μοντέλων επίθεσης με εκτεταμένα οφέλη, όπως η αποτελεσματικότητα των βασικών συστημάτων key escrow. Επίσης τεχνικές honeypot (με decoy files) επιτρέπουν καλύτερο εντοπισμό επιθέσεων με ελάχιστη ζημιά σε συστήματα. Παρόλα αυτά, τα αντίγραφα ασφαλείας αρχείων είναι ίσως ο πιο αποτελεσματικός τρόπος για να αποτραπούν επιθέσεις ransomware, και οι επιτιθέμενοι έχουν λίγες επιλογές για την αντιμετώπιση αυτής της απλής μεθόδου άμυνας.

Οι τρέχουσες μέθοδοι ανίχνευσης ransomware βασίζονται στη δυναμική και στατική ανάλυση. Η στατική ανάλυση βασίζεται σε μεθόδους ευρετικής ανάλυσης, σύγκρισης υπογραφών αρχείων και στην εξειδικευμένη γνώση αναλυτών. Σε διαδικασίες προσομοίωσης, οι αναλυτές εστιάζουν στη συμπεριφορά του ransomware που αλληλεπιδρά με το σύστημα- στόχο. Αναλύοντας τις μεθόδους ανίχνευσης ransomware που βασίζονται σε ταξινόμηση εικόνων, προκύπτει ότι η τεχνική αυτή είναι ακόμη σχετικά νέα σε αυτόν τον τομέα έρευνας. Δεν υπάρχουν αρκετές αναφορές στη βιβλιογραφία σχετικά με αυτή τη προσέγγιση.

Οι τρέχουσες μέθοδοι ανίχνευσης στοχεύουν στο πρόβλημα του κακόβουλου λογισμικού ως ένα πρόβλημα ταξινόμησης χωρίς οι τρέχουσες λύσεις να μπορούν να εξετάσουν σε επιμέρους υποκατηγορίες και ιδιαιτερότητες των διαφορετικών περιπτώσεων ransomware. Οι σύγχρονες προσεγγίσεις μηχανικής μάθησης τείνουν να χρειάζονται σημαντικό αριθμό τεχνικών χαρακτηριστικών και γνώσεων ανά τομέα. Η σύγχρονη πρόκληση είναι να μπορούμε με περιορισμένο αριθμό χαρακτηριστικών, να εφαρμόζουμε πιο αποτελεσματικές τεχνικές στον εντοπισμό κακόβουλου λογισμικού και να είμαστε σε θέση να ταξινομήσουμε διαφορετικές ransomware περιπτώσεις. Για αυτό και οι σύγχρονες μέθοδοι – τουλάχιστον σε ερευνητικό επίπεδο – εστιάζουν στο να περιοριστεί η ανάγκη για εκτεταμένο σχεδιασμό χαρακτηριστικών, και να περιοριστεί το πρόβλημα ταξινόμησης ransomware σε πρόβλημα ταξινόμησης εικόνων.

Για την επίλυση προβλημάτων ταξινόμησης εικόνων, τα Νευρωνικά Δίκτυα (Βαθιάς Μάθησης, Συνελικτικού τύπου) έχουν αποδειχθεί ότι είναι αποτελεσματικά στον τομέα της αναγνώρισης εικόνων και της μηχανικής όρασης. Ωστόσο, χρειάζονται ένα τεράστιο

αριθμό δειγμάτων για την εκπαίδευση του μοντέλου. Ωστόσο, αν και υπάρχει πλέον ευρύτερη γνώση για το τι αποτελεί ένα κακόβουλο λογισμικό τύπου ransomware, δεν υπάρχει διαθέσιμο εκπαιδευμένο μοντέλο. Ως εκ τούτου, η ταξινόμηση της εικόνας ενός αρχείου που θεωρείται ransomware έχει τη πρόκληση ότι βασίζεται σε μοντέλα που έχουν εκπαιδευτεί σε φυσικές εικόνες. Παρόλα αυτά, η βαθιά μάθηση, σε αντίθεση με παραδοσιακές ρηχές μέθοδοι μάθησης, φαίνεται να είναι μια βιώσιμη λύση και μπορεί να βοηθήσει στο μέλλον τους ερευνητές στην ανάπτυξη πιο αποτελεσματικών μηχανισμών ανίχνευσης.

Το Ransomware μάλλον δεν θα εξαφανιστεί ποτέ εντελώς, αλλά ενισχύοντας όλο και περισσότερο τους τωρινούς μηχανισμούς άμυνας μπορεί να μετριαστεί μέχρι να εξαλειφτεί. Με την πάροδο του χρόνου οι επιτιθέμενοι έχουν αλλάξει τις προτιμήσεις τους ως προς ποιους χρήστες, ποια συστήματα να στοχεύουν και πώς να μολύνουν τα θύματα τους. Νέες και δημιουργικές μέθοδοι επίθεσης θα αναδύονται πάντα, αλλά οι τεχνικές άμυνας βελτιώνουν όλο και περισσότερο την κατανόηση και τον μετριασμό των απειλών τέτοιων επιθέσεων.

Τόσο η ερευνητική κοινότητα όσο και εταιρείες που δρουν στο χώρο της κυβερνοασφάλειας μαζί με κρατικές αρχές έχουν αρχίσει να δρουν συλλογικά για να αντιστρέψουν την κατάσταση. Οι μέθοδοι πρόληψης, οι συνεργασίες μεταξύ φορέων στην ανταλλαγή πληροφοριών για απειλές (threat intelligence) θα εξουδετερώσει και τον ανταγωνιστικό χαρακτήρα τέτοιων επιθέσεων καθώς οι προγραμματιστές ransomware βρίσκονται πάντα σε ανώνυμο ανταγωνισμό μεταξύ τους. Ακόμη και συνεργατικά εγκληματικά συστήματα στον κυβερνοχώρο, όπως το Ransomware as a Service θα διαλυθεί σύντομα από νέους αμυντικούς τρόπους παρακολούθησης των πληρωμών.

Η σημασιολογία (ερμήνευση) μιας επίθεσης αποτελεί σημαντικό παράγοντα για τον εντοπισμό και την ανάλυση απειλών. Στην εποχή των Advanced Persistent Threats (APTs), είναι συνετό οι ερευνητές να απομακρυνθούν από τα συστήματα που απλά παρουσιάζουν τα ευρήματά τους (black box) ως ασαφείς αριθμούς και να εργαστούν προς την κατεύθυνση της επεξηγηματικότητας. Δυστυχώς, τα περισσότερα υπάρχοντα συστήματα δεν παρουσιάζουν τα δεδομένα συμπεριφοράς των επιτιθέμενων στον αναλυτή και συμβάλλουν ελάχιστα στην ερμηνεία μιας επίθεσης. Εάν το κάνουν, ο σημασιολογικός εμπλουτισμός γίνεται συχνά μέσω σταθερών μοτίβων, παρόμοιων με τα

σενάρια ανίχνευσης κακόβουλης χρήσης, τα οποία αντιμετωπίζουν το ίδιο φάσμα προβλημάτων.

Έτσι, η μείωση του σημασιολογικού χάσματος μεταξύ συγκεκριμένων προτύπων/ανωμαλιών και σημασιολογικών ιδιοτήτων των επιθέσεων, όπως το κίνητρο, ο στόχος, οι εμπλεκόμενοι φορείς, το στοχευόμενο σύστημα και οι συγκεκριμένες τεχνικές που χρησιμοποιούνται είναι ένα ζωτικής σημασίας επόμενο βήμα για τον ολιστικό μετριασμό των απειλών σε συστήματα.

Βιβλιογραφία

Robert Luh, Stefan Marschalek, Manfred Kaiser, Helge Janicke, and Sebastian Schrittwieser (2016). Semantics-aware detection of targeted attacks: a survey. Journal of Computer Virology and Hacking Techniques, pages 1–39, 2016.

Robert Luh, Sebastian Schrittwieser, Stefan Marschalek, Helge Janicke, and Edgar Weippl (2017). Design of an anomaly-based threat detection & explication system. In Proceedings of the 3rd International Conference on Information Systems Security and Privacy (ICISSP), pages 397–402. SCITEPRESS,2017.

Andronio N., Zanero S., Maggi F. (2015) HelDroid: Dissecting and Detecting Mobile Ransomware. In: Bos H., Monrose F., Blanc G. (eds) Research in Attacks, Intrusions, and Defenses. RAID 2015. Lecture Notes in Computer Science, vol 9404. Springer, Cham. https://doi.org/10.1007/978-3-319-26362-5_18

Singh A., Ikuesan A.R., Venter H.S. (2019) Digital Forensic Readiness Framework for Ransomware Investigation. In: Breitinger F., Baggili I. (eds) Digital Forensics and Cyber Crime. ICDF2C 2018. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 259. Springer, Cham. https://doi.org/10.1007/978-3-030-05487-8_5

Bettany A., Halsey M. (2017) Manually Removing Malware. In: Windows Virus and Malware Troubleshooting. Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-2607-0_6

SophosLabs Research Team (2019), Emotet exposed: looking inside highly destructive malware, Network Security, Volume 2019, Issue 6, 2019, Pages 6-11, ISSN 1353-4858, https://doi.org/10.1016/S1353-4858(19)30071-6.

Kancherla, K., Donahue, J. & Mukkamala, S. (2016) Packer identification using Byte plot and Markov plot. J Comput Virol Hack Tech 12, 101–111 (2016). https://doi.org/10.1007/s11416-015-0249-8

Ö. A. Aslan and R. Samet (2020), "A Comprehensive Review on Malware Detection Approaches," in IEEE Access, vol. 8, pp. 6249-6271, 2020, doi: 10.1109/ACCESS.2019.2963724.

D. Kao, S. Hsiao and R. Tso (2019), "Analyzing WannaCry Ransomware Considering the Weapons and Exploits," 2019 21st International Conference on Advanced Communication Technology (ICACT), 2019, pp. 1098-1107, doi: 10.23919/ICACT.2019.8702049.

K. Lee, S. -Y. Lee and K. Yim (2019), "Machine Learning Based File Entropy Analysis for Ransomware Detection in Backup Systems," in IEEE Access, vol. 7, pp. 110205-110215, 2019, doi: 10.1109/ACCESS.2019.2931136.

M. M. Hasan and M. M. Rahman (2017), "RansHunt: A support vector machines based ransomware analysis framework with integrated feature set," 2017 20th International Conference of Computer and Information Technology (ICCIT), 2017, pp. 1-7, doi: 10.1109/ICCITECHN.2017.8281835.

S. K. Shaukat and V. J. Ribeiro (2018), "RansomWall: A layered defense system against cryptographic ransomware attacks using machine learning," 2018 10th International Conference on Communication Systems & Networks (COMSNETS), 2018, pp. 356-363, doi: 10.1109/COMSNETS.2018.8328219.

Bhardwaj, A., et al. (2015). Ransomware: A Rising Threat of new age Digital Extortion. Cornel University.

Kyurkchiev, Nikolay & Iliev, Anton & Rahnev, Asen & Terzieva, Todorka. (2019). A New Analysis of Cryptolocker Ransomware and Welchia Worm Propagation Behavior. Some Applications. III. Communications in Applied Analysis. 23. 359-382. 10.12732/caa.v23i2.7.

N. Scaife, H. Carter, P. Traynor, and K. R. B. Butler (2016). CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data. Proc. - Int. Conf. Distrib. Comput. Syst., vol. 2016-Augus, pp. 303–312, 2016.

C. P. Gibson and S. M. Banik (2017). Analyzing the Effect of Ransomware Attacks on Different Industries. 2017 International Conference on Computational Science and Computational Intelligence (CSCI), 2017, pp. 121-126, doi: 10.1109/CSCI.2017.20.

A. Kharraz, W. Robertson, D. Balzarotti, L. Bilge, and E. Kirda (2015). Cutting the gordian knot: A look under the hood of ransomware attacks. Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 9148, pp. 3–24, 2015.

Olaimat, M.N.; Maarof, M.A.; Al-rimy, B.A.S. (2021). Ransomware Anti-Analysis and Evasion Techniques: A Survey and Research Directions. In Proceedings of the 2021 3rd International Cyber Resilience Conference (CRC), Langkawi Island, Malaysia, 29–31 January 2021; pp. 1–6

Hu, J.W.; Zhang, Y.; Cui, Y.P. (2020). Research on Android ransomware protection technology. In Journal of Physics: Conference Series; IOP Publishing: Bristol, UK, 2020; p. 012004.

Maigida, A.M.; Olalere, M.; Alhassan, J.K.; Chiroma, H.; Dada, E.G. (2019). Systematic literature review and metadata analysis of ransomware attacks and detection mechanisms. J. Reliab. Intell. Environ. 2019, 5, 67–89

Bello, I.; Chiroma, H.; Abdullahi, U.A.; Gital, A.Y.u.; Jauro, F.; Khan, A.; Okesola, J.O.; Shafi'i, M.A. (2020). Detecting ransomware attacks using intelligent algorithms: Recent development and next direction from deep learning and big data perspectives. J. Ambient. Intell. Humaniz. Comput. 2020, 12, 8699–8717.

Sneha, M.; Arya, A.; Agarwal, P. (2020). Ransomware Detection techniques in the Dawn of Artificial Intelligence: A Survey. In Proceedings of the 2020 the 9th International Conference on Networks, Communication and Computing, Tokyo, Japan, 18–20 December 2020; pp. 26–33.

Al-rimy, B.A.S., Maarof, M.A., Shaid, S.Z.M. (2018). Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. Comput. Secur. 74, 144–166. https://doi.org/10.1016/j.cose.2018.01.001

Amro, S.A., Alkhalifah, A. (2015). A Comparative Study of Virus Detection Techniques 9, 8.

Baltrušaitis, T., Ahuja, C., Morency, L.-P., 2018. Multimodal machine learning: A survey and taxonomy. IEEE Trans. Pattern Anal. Mach. Intell. 41, 423–443.

Bhodia, N., Prajapati, P., Di Troia, F., Stamp, M. (2019). Transfer Learning for Image-Based Malware Classification. ArXiv190311551 Cs Stat.

Cawsey, A., 1998. The essence of artificial intelligence, Essence of computing series. Prentice Hall, Harlow, England ; New York.

Chen, C.-M., Wang, S.-H., Wen, D.-W., Lai, G.-H., Sun, M.-K. (2019). Applying Convolutional Neural Network for Malware Detection, in: 2019 IEEE 10th International Conference on Awareness Science and Technology (ICAST). IEEE, pp. 1–5.

Chen, L., (2018). Deep Transfer Learning for Static Malware Classification. ArXiv181207606 Cs Stat.

Dargahi, T., Dehghantanha, A., Bahrami, P.N., Conti, M., Bianchi, G., Benedetto, L. (2019). A Cyber-Kill-Chain based taxonomy of crypto-ransomware features. J. Comput. Virol. Hacking Tech. 15, 277–305. https://doi.org/10.1007/s11416-019-00338-7

Deng, L., Yu, D. (2013). Deep Learning: Methods and Applications. Deep Learn. 7, 197.

Ganapathi, P., Shanmugapriya, D. (Eds.), 2020. Handbook of Research on Machine and Deep Learning Applications for Cyber Security:, Advances in Information Security, Privacy, and Ethics. IGI Global. https://doi.org/10.4018/978-1-5225-9611-0

Géron, A. (2019). Hands-on machine learning with Scikit-Learn, Keras, and TensorFlow: concepts, tools, and techniques to build intelligent systems. O'Reilly Media, Inc, Sebastopol, CA.

Ghafur, S., Kristensen, S., Honeyford, K., Martin, G., Darzi, A., Aylin, P. (2019). A retrospective impact analysis of the WannaCry cyberattack on the NHS. NPJ Digit.

Med. 2, 1–7.

Gibert, D., Mateu, C., Planes, J. (2020). The rise of machine learning for detection and classification of malware: Research developments, trends and challenges. J. Netw. Comput. Appl. 153, 102526. https://doi.org/10.1016/j.jnca.2019.102526

Guthrie, W.F. (2020). NIST/SEMATECH e-Handbook of Statistical Methods (NIST Handbook 151). https://doi.org/10.18434/M32189

Han, K., Lim, J.H., Im, E.G. (2013). Malware analysis method using visualization of binary files, in: Proceedings of the 2013 Research in Adaptive and Convergent Systems. pp. 317–321.

Hardy, W., Chen, L., Hou, S., Ye, Y., Li, X. (2016). DL4MD: A deep learning framework for intelligent malware detection, in: Proceedings of the International Conference on Data Mining (DMIN). The Steering Committee of The World Congress in Computer Science, Computer, p. 61.

Hassan, N.A., 2019. Ransomware Families, in: Ransomware Revealed. Springer, pp. 47–68.

Johns, J., 2017. Representation Learning for Malware Classification 23.

Humayun, Mamoona & Zaman, Noor & Alsayat, Ahmed & Ponnusamy, Vasaki. (2020). Internet of things and ransomware: Evolution, mitigation and prevention. Egyptian Informatics Journal. 22. 10.1016/j.eij.2020.05.003.

Kaspersky, 2020. IT threat evolution Q3 2019. Statistics. https://securelist.com/it-threat-evolution-q3-2019/95268/ (ημ. Προσπέλασης 06/03/2022).

keras, 2020. Keras. https://keras.io (ημ. Προσπέλασης 06/03/2022).

Kolosnjaji, B., Eraisha, G., Webster, G., Zarras, A., Eckert, C., 2017. Empowering convolutional networks for malware classification and analysis, in: 2017 International Joint Conference on Neural Networks (IJCNN). IEEE, pp. 3838–3845.

Krizhevsky, A., Sutskever, I., Hinton, G.E., 2012. Imagenet classification with deep convolutional neural networks, in: Advances in Neural Information Processing Systems. pp. 1097–1105.

Krohn, J., Beyleveld, G., Bassens, A., 2020. Deep learning illustrated: a visual, interactive guide to artificial intelligence.

Lo, W.W., Yang, X., Wang, Y., 2019. An Xception Convolutional Neural Network for Malware Classification with Transfer Learning, in: 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS).

Loman, M., 2019. How Ransomware Attacks.

Masters, D., Luschi, C., 2018. Revisiting Small Batch Training for Deep Neural Networks. ArXiv180407612 Cs Stat.

McAfee, 2019. McAfee Labs Threats Report August 2019.

MITRE, 2020. Data Encrypted for Impact. https://attack.mitre.org/techniques/T1486/ (ημ. Προσπέλασης 06/03/2022).

Nataraj, L., Karthikeyan, S., Jacob, G., Manjunath, B., 2011. Malware images: visualization and automatic classification, in: Proceedings of the 8th International Symposium on Visualization for Cyber Security. pp. 1–7.

Sikorski, M., Honig, A., 2012. Practical malware analysis: the hands-on guide to dissecting malicious software. No Starch Press, San Francisco.

Simonyan, K., Zisserman, A., 2015. Very Deep Convolutional Networks for Large-Scale Image Recognition. ArXiv14091556 Cs.

Trend Micro, 2020. THE SPRAWLING REACH OF COMPLEX THREATS 2019 ANNUAL SECURITY ROUNDUP. https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/the-sprawling-reach-of-complex-threats#:~:text=Complex%20and%20persistent%20threats%20riddled,came%20up%20with%20novel%20subterfuges (ημ. Προσπέλασης 06/03/2022).

Vinayakumar, R., Alazab, M., Soman, K., Poornachandran, P., Venkatraman, S. (2019). Robust intelligent malware detection using deep learning. IEEE Access 7, 46717–46738.

Vu, D.-L., Nguyen, T.-K., Nguyen, T.V., Nguyen, T.N., Massacci, F., Phung, P.H., 2019. A

convolutional transformation network for malware classification. ArXiv Prepr. ArXiv190907227.

Xie, B., Qin, J., Xiang, X., Li, H., Pan, L., 2017. An Image Retrieval Algorithm Based on GIST and SIFT Features 8.

Savage, Kevin, Peter Coogan, and Hon Lau. (2015). *The evolution of ransomware*. https://its.fsu.edu/sites/g/files/imported/storage/images/information-security-and-privacy-office/the-evolution-of-ransomware.pdf (ημ. Προσπέλασης 06/03/2022).

Scaife, N., et al. (2016). Cryptolock (and drop it): stopping ransomware attacks on user data. Distributed Computing Systems (ICDCS), 2016 IEEE 36th International Conference on, IEEE.

Lanzi, A., et al. (2010). AccessMiner: using system-centric models for malware protection. Proceedings of the 17th ACM conference on Computer and communications security. Chicago, Illinois, USA, ACM: 399-412.

Kharraz, A., et al. (2015). Cutting the gordian knot: a look under the hood of ransomware attacks. International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, Springer.

Kharraz, A., et al. (2016). UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware. 25th USENIX Security Symposium (USENIX Security 16).

Thomas, J. E. (2018). Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks. International Journal of Business Management, 12(3). 1-23. doi:10.5539/ijbm.v13n6p1

Knebel, S., Schultz, M.D. and Seele, P. (2022). "Cyberattacks as “state of exception” reconceptualizing cybersecurity from prevention to surviving and accommodating", Journal of Information, Communication and Ethics in Society, Vol. 20 No. 1, pp. 91-109. https://doi.org/10.1108/JICES-01-2021-0015

J. Z. Kolter and M. A. Maloof (2006). Learning to Detect Malicious Executables, Mach. Learn. Data Min. Comput. Secur., vol. 1, no. 212, pp. 47–63, 2006.

Q. Jerome, K. Allix, R. State, and T. Engel (2014), “Using opcode-sequences to detect malicious Android applications,” 2014 IEEE Int. Conf. Commun. ICC 2014, pp. 914–919, 2014.

A. Kharraz, W. Robertson, D. Balzarotti, L. Bilge, and E. Kirda (2015), “Cutting the gordian knot: A look under the hood of ransomware attacks,” Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 9148, pp. 3–24, 2015.

A. Moser, C. Kruegel, and E. Kirda (2007), “Limits of Static Analysis for Malware Detection - IEEE Conference Publication.”

Nikolai Hampton, Zubair Baig, Sherali Zeadally (2018), Ransomware behavioural analysis on windows platforms, Journal of Information Security and Applications, Volume 40, 2018, Pages 44-51, ISSN 2214-2126, https://doi.org/10.1016/j.jisa.2018.02.008.

A. Continella et al. (2016), “ShieldFS,” Proc. 32nd Annu. Conf. Comput. Secur. Appl. - ACSAC ’16, pp. 336– 347, 2016

D. Sgandurra, L. Muñoz-González, R. Mohsen, and E. C. Lupu (2016), “Automated Dynamic Analysis of Ransomware: Benefits, Limitations and use for Detection,” 2016.

S. Poudyal, K. P. Subedi, and D. Dasgupta (2019), “A Framework for Analyzing Ransomware using Machine Learning,” Proc. 2018 IEEE Symp. Ser. Comput. Intell. SSCI 2018, pp. 1692–1699, 2019.

A. Karimi and M. H. Moattar (2017), “Android ransomware detection using reduced opcode sequence and image similarity,” 2017 7th Int. Conf. Comput. Knowl. Eng. ICCKE 2017, vol. 2017-Janua, no. Iccke, pp. 229–234, 2017.

D. Y. Huang, M. M. Aliapoulios, V. G. Li, L. Invernizzi, K. McRoberts, E. Bursztein, J. Levin, K. Levchenko, A. C. Snoeren, and D. McCoy (2018). *Tracking Ransomware End-to-end*. 2018 IEEE Symposium on Security and Privacy, pp. 618–631, 2018.

G. Hull, H. John, and B. Arief (2019). *Ransomware deployment methods and analysis: views from a predictive model and human responses*. Crime Science, vol. 8, no. 1, 2019.

K. Savage, P. Coogan, and H. Lau (2015). *The evolution of ransomware*. Symantec, 2015.

S. Kok, A. Abdullah, and N. Jhanjhi (2020). *Early detection of crypto-ransomware using pre-encryption detection algorithm.* Journal of King Saud University Computer and Information Sciences, 2020.

Richardson, Ronny and North, Max M. (2017). *Ransomware: Evolution, Mitigation and Prevention*. Faculty Publications. 4276.

S. Sjouwerman (2015). *Ransomware.* KnowBe4, 2015.

A. L. Young and Moti Yung (1996). *Cryptovirology: extortion-based security threats and countermeasures*. Proceedings 1996 IEEE Symposium on Security and Privacy, Oakland, CA, USA, 1996, pp. 129-140, doi: 10.1109/SECPRI.1996.502676.

A. L. Young and M. Yung (2005). An Implementation of Cryptoviral Extortion Using Microsoft's Crypto API. Cryptovirology, 2005.

D. Nazarov and O. Emelyanova (2006). *Blackmailer: the story of Gpcode*. Securelist, 26-Jun-2006. [Online]. Available: https://securelist.com/blackmailer-the-story-of-gpcode/36089/. [ημ. προσπέλασης 20/03/2022].

Luo, Robert & Liao, Qinyu. (2007). *Awareness Education as the Key to Ransomware Prevention*. Information Systems Security. 16. 195-202. 10.1080/10658980701576412.

A. Gazet (2008). *Comparative analysis of various ransomware virii*. Journal in Computer Virology, vol. 6, no. 1, pp. 77–90, Jul. 2008.

A Hansberry, A Lasse, A Tarrh (2014). *Cryptolocker: 2013's most malicious malware*. [online] https://cs-web.bu.edu/~goldbe/teaching/HW55815/cryptolockerEssay.pdf [ημ. προσπέλασης 20/03/2022].

Z. A. Genç (2020). *Analysis, Detection, and Prevention of Cryptographic Ransomware.* Dissertation, University of Luxembourg Library, 2020.

Kharraz A., Robertson W., Balzarotti D., Bilge L., Kirda E. (2015). *Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks*. In: Almgren M., Gulisano V., Maggi F. (eds) Detection of Intrusions

and Malware, and Vulnerability Assessment. DIMVA 2015. Lecture Notes in Computer Science, vol 9148.

Springer, Cham. https://doi-org.proxy.lib.pdx.edu/10.1007/978-3-319-20550-2_1

Chittooparambil H.J., Shanmugam B., Azam S., Kannoorpatti K., Jonkman M., Samy G.N. (2019). *A Review of Ransomware Families and Detection Methods*. In: Saeed F., Gazem N., Mohammed F., Busalim A. (eds) Recent Trends in Data Science and Soft Computing. IRICT 2018. Advances in Intelligent Systems and Computing, vol 843. Springer, Cham. https://doi.org/10.1007/978-3-319-99007-1_55

Oosthoek K., Doerr C. (2019) *SoK: ATT&CK Techniques and Trends in Windows Malware*. In: Chen S., Choo KK., Fu X., Lou W., Mohaisen A. (eds) Security and Privacy in Communication Networks. SecureComm 2019. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 304. Springer, Cham. https://doi.org/10.1007/978-3-030-37228-6_20

S. Greengard (2021). *The worsening state of ransomware*. Commun. ACM 64, 4 (April 2021), 15–17. DOI:https://doi.org/10.1145/3449054

G. Dobie and J. Whitehead (2020). *AGCS-Cyber-Risk-Trends-2020*. Allianz Global Corporate & Specialty SE, Munich, Oct-2020.

F. A. Alaba, M. Othman, I. A. T. Hashem, F. Alotaibi (2017). *Internet of Things security: A survey, Journal of Network and Computer Applications*, Volume 88, 2017, Pages 10-28, ISSN 1084-8045, https://doi.org/10.1016/j.jnca.2017.04.002.

C. Miller (2019). *Lessons learned from hacking a car.* in IEEE Design & Test, vol. 36, no. 6, pp. 7-9, Dec. 2019, doi: 10.1109/MDAT.2018.2863106.

van Niekerk, Brett; Jansen, Joey; Ramluckan, Trishana (2020). *Special Issue: Legal, Social, and Technical Considerations for Cyber Security in the Digital Revolution*. Journal of Information Warfare; Yorktown Vol. 19, Iss. 3, (2020): I-III.

M. Lee (2018). *An Overview of Malicious Advertising*. [online] https://www.cs.tufts.edu/comp/116/archive/spring2018/mlee.pdf [ημ. προσπέλασης 20/03/2022].

S. Lee, H. K. Kim, and K. Kim (2019). *Ransomware protection using the moving target defense perspective*. Computers & Electrical Engineering, vol. 78, pp. 288–299, Sep. 2019.

M. Wecksten, J. Frick, A. Sjostrom, and E. Jarpe (2016). *A novel method for recovery from Crypto Ransomware infections*. 2016 2nd IEEE International Conference on Computer and Communications (ICCC), pp. 1354–1358, 2016.

E. Kolodenker, W. Koch, G. Stringhini, and M. Egele (2017). PayBreak. Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security, 2017.

M. Christodorescu, S. Jha, S. A. Seshia, D. Song, and R. E. Bryant (2005). *Semantics-aware malware detection*. In IEEE Symposium on Security and Privacy, 2005.

W. Yan, Z. Zhang, and N. Ansari (2008). *Revealing packed malware*. ieee security & PrivaCy, 6(5):65–69, 2008.

B. Stone-Gross, T. Holz, G. Stringhini, and G. Vigna (2011). *The underground economy of spam: A botmaster's perspective of coordinating large-scale spam campaigns*. LEET, 11:4–4, 2011.

B. Stone-Gross, M. Cova, L. Cavallaro, B. Gilbert, M. Szydlowski, R. Kemmerer, C. Kruegel, and G. Vigna (2009). *Your botnet is my botnet: analysis of a botnet takeover*. In ACM conference on Computer and communications security (CCS), 2009.

I. Koniaris, G. Papadimitriou, P. Nicopolitidis, and M. Obaidat (2014). *Honeypots deployment for the analysis and visualization of malware activity and malicious connections*. In 2014 IEEE International Conference on Communications (ICC), pages 1819–1824, June 2014.

H. J. Highland (1988). The brain virus: fact and fantasy. Computers & Security, 7(4):367–370, 1988

T. Nelms, R. Perdisci, M. Antonakakis, and M. Ahamad (2016). Towards measuring and mitigating social engineering software download attacks. In USENIX Security Symposium, pages 773–789, 2016.

T. Holz, C. Gorecki, K. Rieck, and F. C. Freiling (2008). Measuring and Detecting Fast-Flux Service Networks. In Network and Distributed Systems Security Symposium (NDSS), 2008

M. Antonakakis, R. Perdisci, Y. Nadji, N. Vasiloglou, S. Abu-Nimeh, W. Lee, and D. Dagon (2012). From throw-away traffic to bots: detecting the rise of DGAbased malware. In USENIX Security Symposium, 2012.

U. Bayer, I. Habibi, D. Balzarotti, E. Kirda, and C. Kruegel (2009). A view on current malware behaviors. In LEET, 2009.

C. Grier, L. Ballard, J. Caballero, N. Chachra, C. J. Dietrich, K. Levchenko, P. Mavrommatis, D. McCoy, A. Nappa, A. Pitsillidis, et al (2012). Manufacturing compromise: the emergence of exploit-as-a-service. In Proceedings of the 2012 ACM conference on Computer and communications security, pages 821–832. ACM, 2012

K. Thomas, J. A. E. Crespo, R. Rasti, J.-M. Picod, C. Phillips, M.-A. Decoste, C. Sharp, F. Tirelo, A. Tofigh, M.-A. Courteau, et al (2016). Investigating commercial pay-per-install and the distribution of unwanted software. In USENIX Security Symposium, pages 721–739, 2016.

J. Caballero, C. Grier, C. Kreibich, and V. Paxson (2011). Measuring pay-per-install: the commoditization of malware distribution. In Usenix security symposium, pages 13–13, 2011

Alrawashdeh, K.; Purdy, C (2018). Ransomware detection using limited precision deep learning structure in fpga. In Proceedings of the NAECON 2018-IEEE National Aerospace and Electronics Conference, Dayton, OH, USA, 23–26 July 2018; pp. 152–157.

Homayoun, S.; Dehghantanha, A.; Ahmadzadeh, M.; Hashemi, S.; Khayami, R.; Choo, K.-K.R.; Newton (2019). D.E. DRTHIS: Deep ransomware threat hunting and intelligence system at the fog layer. Future Gener. Comput. Syst. 2019, 90, 94–104.

Al-Hawawreh, M.; Sitnikova, E (2019). Industrial Internet of Things based ransomware detection using stacked variational neural network. In Proceedings of the 3rd International Conference on Big Data and Internet of Things, Melbourn, Australia, 22–24 August 2019; pp. 126–130.

Moore, C (2016). Detecting ransomware with honeypot techniques. In Proceedings of the 2016 Cybersecurity and Cyberforensics Conference (CCC), Amman, Jordan, 2–4 August 2016; pp. 77–81.

Cusack, G.; Michel, O.; Keller, E (2018). Machine learning-based detection of ransomware using SDN. In Proceedings of the 2018 ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization, Tempe, AZ, USA, 21 March 2018; pp. 1–6.

Cabaj, K.; Gawkowski, P.; Grochowski, K.; Osojca, D (2015). Network activity analysis of CryptoWall ransomware. Prz. Elektrotech. 2015, 91, 201–204.

Ahmed, Y.A.; Koçer, B.; Huda, S.; Al-rimy, B.A.S.; Hassan, M.M (2020). A system call refinement-based enhanced Minimum Redundancy Maximum Relevance method for ransomware early detection. J. Netw. Comput. Appl. 2020, 167, 102753.

Bae, S.I.; Lee, G.B.; Im, E.G (2020). Ransomware detection using machine learning algorithms. Concurr. Comput. Pract. Exp. 2020, 32, e5422.

Al-Hawawreh, M.; Sitnikova, E (2019). Industrial Internet of Things based ransomware detection using stacked variational neu- ral network. In Proceedings of the 3rd International Conference on Big Data and Internet of Things, Melbourn, Australia,

22–24 August 2019; pp. 126–130.

Homayoun, S.; Dehghantanha, A.; Ahmadzadeh, M.; Hashemi, S.; Khayami, R.; Choo, K.-K.R.; Newton (2019), D.E. DRTHIS: Deep ransomware threat hunting and intelligence system at the fog layer. Future Gener. Comput. Syst. 2019, 90, 94–104.

Ashraf, A.; Aziz, A.; Zahoora, U.; Rajarajan, M.; Khan, A (2019). Ransomware Analysis using Feature Engineering and Deep Neural Networks. arXiv 2019, arXiv:1910.00286.

Roy, K.C.; Chen, Q (2020). DeepRan: Attention-based BiLSTM and CRF for Ransomware Early Detection and Classifcation. Inf. Syst. Front. 2020, 23, 299–315.

Lee, K.; Lee, S.-Y.; Yim, K (2019). Machine learning based file entropy analysis for ransomware detection in backup systems. IEEE Access 2019, 7, 110205–110215.

Al-rimy, B.A.S.; Maarof, M.A.; Shaid, S.Z.M (2019). Crypto-ransomware early detection model using novel incremental bagging with enhanced semi-random subspace selection. Future Gener. Comput. Syst. 2019, 101, 476–491.

Alam, M.; Sinha, S.; Bhattacharya, S.; Dutta, S.; Mukhopadhyay, D.; Chattopadhyay, A (2020). RAPPER: Ransomware prevention via performance counters. arXiv 2020, arXiv:2004.01712.

Zuhair, H.; Selamat, A (2019). RANDS: A Machine Learning-Based Anti-Ransomware Tool for Windows Platforms. In Advancing Technology Industrialization Through Intelligent Software Methodologies, Tools and Techniques; IOS Press: Amsterdam, The Netherlands, 2019; pp. 573–587.

Kok, S.; Azween, A.; Jhanjhi, N (2020). Evaluation metric for crypto-ransomware detection using machine learning. J. Inf. Secur. Appl. 2020, 55, 102646.

Fernandez Maimo, L.; Huertas Celdran, A.; Perales Gomez, A.L.; Garcia Clemente, F.J.; Weimer, J.; Lee, I (2019). Intelligent and dynamic ransomware spread detection and mitigation in integrated clinical environments. Sensors 2019, 19, 1114.

Adamu, U.; Awan, I (2019). Ransomware prediction using supervised learning algorithms. In Proceedings of the 2019 7th International Conference on Future Internet of Things and Cloud (FiCloud), Istanbul, Turkey, 26–28 August 2019; pp. 57–63.

Kok, S.; Abdullah, A.; Jhanjhi, N (2020). Early detection of crypto-ransomware using pre-encryption detection algorithm. J. King Saud Univ.-Comput. Inf. Sci. 2020, in press.

Chen, Q.; Islam, S.R.; Haswell, H.; Bridges, R.A (2019). Automated ransomware behavior analysis: Pattern extraction and early detection. In Proceedings of the International Conference on Science of Cyber Security, Nanjing, China, 9–11 August 2019; pp. 199–214.

Pundir, N.; Tehranipoor, M.; Rahman, F (2020). RanStop: A Hardware-assisted Runtime Crypto-Ransomware Detection Technique. arXiv 2020, arXiv:2011.12248.

Almashhadani, A.O.; Kaiiali, M.; Sezer, S.; O'Kane, P (2019). A multi-classifier network-based crypto ransomware detection system: A case study of locky ransomware. IEEE Access 2019, 7, 47053–47067.

Ahmadian, M.M.; Shahriari, H.R.; Ghaffarian, S.M (2015). Connection-monitor & connection-breaker: A novel approach for prevention and detection of high survivable ransomwares. In Proceedings of the 2015 12th International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC), Rasht, Iran, 8–10 September 2015; pp. 79–84.

Bahrani, A.; Bidgly, A.J (2019). Ransomware detection using process mining and classification algorithms. In Proceedings of the 2019 16th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC), Mashhad, Iran, 28–29 August 2019; pp. 73–77.

Poudyal, S.; Dasgupta, D (2020). AI-Powered Ransomware Detection Framework. In Proceedings of the 2020 IEEE Symposium Series on Computational Intelligence (SSCI), Canberra, Australia, 1–4 December 2020; pp. 1154–1161.

Ahmed, Y.A.; Kocer, B.; Al-rimy, B.A.S (2020). Automated Analysis Approach for the Detection of High Survivable Ransomware. KSII Trans. Internet Inf. Syst. 2020, 14, 2236–2257.

Zuhair, H.; Selamat, A.; Krejcar, O (2020). A Multi-Tier Streaming Analytics Model of 0-Day Ransomware Detection Using Machine Learning. Appl. Sci. 2020, 10, 3210.

Kok, S.; Abdullah, A.; Jhanjhi, N.; Supramaniam, M (2019). Prevention of crypto-ransomware using a pre-encryption detection algorithm. Computers 2019, 8, 79.

Al-Hawawreh, M.; Sitnikova, E (2019). Leveraging deep learning models for ransomware detection in the industrial internet of things environment. In Proceedings of the 2019 Military Communications and Information Systems Conference (MilCIS), Canberra, Australia, 12–14 November 2019; pp. 1–6.

Yang, C.-Y.; Sahita, R (2020). Towards a Resilient Machine Learning Classifier-a Case Study of Ransomware Detection. arXiv 2020, arXiv:2003.06428.

AbdulsalamYa'u, G.; Job, G.K.; Waziri, S.M.; Jaafar, B.; SabonGari, N.A.; Yakubu, I.Z (2019). Deep Learning for Detecting Ransomware in Edge Computing Devices Based On Autoencoder Classifier. In Proceedings of the 2019 4th International Conference on Electrical, Electronics, Communication, Computer Technologies and Optimization Techniques (ICEECCOT), Mysuru, India,

13–14 December 2019; pp. 240–243.

Basnet, M.; Poudyal, S.; Ali, M.; Dasgupta, D (2021). Ransomware Detection Using Deep Learning in the SCADA System of Electric Vehicle Charging Station. arXiv 2021, arXiv:2104.07409.

Ganfure, G.O.; Wu, C.-F.; Chang, Y.-H.; Shih, W.-K (2020). DeepGuard: Deep Generative User-behavior Analytics for Ransomware Detection. In Proceedings of the 2020 IEEE International Conference on Intelligence and Security Informatics (ISI), Arlington, VA, USA, 9–10 November 2020; pp. 1–6.

Sharmeen, S.; Ahmed, Y.A.; Huda, S.; Koçer, B.S¸.; Hassan, M.M (2020). Avoiding future digital extortion through robust protection against ransomware threats using deep learning based adaptive approaches. IEEE Access 2020, 8, 24522–24534.

Nurnoby, M.F.; El-Alfy, E.-S.M (2019). Overview and Case Study for Ransomware Classification Using Deep Neural Network. In Proceedings of the 2019 2nd IEEE Middle East and North Africa COMMunications Conference (MENACOMM), Manama, Bahrain, 19–21 November 2019; pp. 1–6.

Ullah, F.; Javaid, Q.; Salam, A.; Ahmad, M.; Sarwar, N.; Shah, D.; Abrar, M (2020). Modified Decision Tree Technique for Ransomware Detection at Runtime through API Calls. Sci. Program. 2020, 2020, 8845833.

Qin, B.; Wang, Y.; Ma, C (2020). API Call Based Ransomware Dynamic Detection Approach Using TextCNN. In Proceedings of the 2020 International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE), Fuzhou, China, 12–14 June 2020; pp. 162–166.

Aurangzeb, S.; Rais, R.N.B.; Aleem, M.; Islam, M.A.; Iqbal, M.A (2021). On the classification of Microsoft-Windows ransomware using hardware profile. PeerJ. Comput. Sci. 2021, 7, e361.

Abdullah, Z.; Muhadi, F.W.; Saudi, M.M.; Hamid, I.R.A.; Foozy, C.F.M (2020). Android ransomware detection based on dynamic obtained features. In Proceedings of the International Conference on Soft Computing and Data Mining, Langkawi, Malaysia, 22–23 January 2020; pp. 121–129.

Ahmed, M.E.; Kim, H.; Camtepe, S.; Nepal, S (2021). Peeler: Profiling Kernel-Level Events to Detect Ransomware. arXiv 2021, arXiv:2101.12434.

Ayub, M.A.; Continella, A.; Siraj, A (2020). An I/O Request Packet (IRP) Driven Effective Ransomware Detection Scheme using Artificial Neural Network. In Proceedings of the 2020 IEEE 21st International Conference on Information Reuse and Integration for Data Science (IRI), Las Vegas, NV, USA, 11–13 August 2020; pp. 319–324.

Jethva, B.; Traoré, I.; Ghaleb, A.; Ganame, K.; Ahmed, S (2020). Multilayer ransomware detection using grouped registry key operations, file entropy and file signature monitoring. J. Comput. Secur. 2020, 28, 337–373.

Godinho J.F. (2018). Malware Detection via Machine Learning. MSc thesis in Information Systems and Computer Engineering. Tecnico Lisboa. Portugal. [ημ. προσπέλασης 10/04/2022]
https://fenix.tecnico.ulisboa.pt/downloadFile/844820067125659/Thesis.pdf

Παράρτημα Α’

Ransomware data sets

Α/Α	Αναφορά	Εργαλείο	Πλατφόρμα	Σύνολο δεδομένων	Κατηγορία επίθεσης	Πηγή δεδομένων	# δειγμάτων
1	Ahmed et al, 2020	Cuckoo	Desktop Windows	Ransomware		VirusShare VirusTotal	1354
				Benign		Software-informer System 32	1358
2	Bae et al, 2020	Intel Pin 3.2	Desktop Windows	Malware		VirusTotal	300
				Benign		Windows 7 system directory	582
3	Al-Hawawreh et al, 2019		Industrial IoT	Ransomware		VirusTotal	582
				Benign		Windows application	942
4	Homayoun et al, 2019	DRTHIS	Fog Layer	Ransomware		VirusTotal	660
				Benign		NA	219
5	Ashraf et al, 2019	Cuckoo	Windows	Static Dataset 3646	Ransomware	VirusTotal VirusShare	1700
					Goodware	Window 7	1946
				Dynamic Dataset 3444	Ransomware	VirusTotal VirusShare	1455
					Goodware	Window 7	1989
6	Roy and Chen 2020	Log Parser	Networks Bare metal server	Ransomware		PC host logs	17
				Benign		PC host logs	103,330
7	Lee at al, 2019		Industrial IoT	Ransomware	Sgundara	NA	582
				Benign	Sgundara	NA	942
8	Al-rimy et al, 2019	Cuckoo Sandbox		Ransomware		VirusShare	8152
				Benign		Informer.com	1000
9	Alam et al, 2020	Cuckoo sandbox	Windows	Ransomware	Wannacry Vipasana Locky	NA	NA

					Petya		
				Benign		NA	NA
10	Zuhair et al. 2019	Virtual testbed	Windows	Ransomware	AiDS RaaS GpCode CryptoLocker Archiveus CryptoWall WinLock Reveton	VirusTotal Malware Blacklist	400 310 800 720 1500 3250 2620 400
				Benign		Website	500
11	Kok et al, 2020	Cuckoo	Windows	Ransomware		VirusTotal Sgandurra theZoo	357 491 56
				Benign		Sgandurra	942
12	Fernandez et al, 2019	Flow exporter Flow controller	IoT	Ransomware	Wannacry Petya BadRabbit PowerGhost		50,537
				Benign		Network Traffic generated by Integrated Clinical Environment (ICE)	100,000
13	Adamu and Awan 2019		Windows	Ransomware		RISS of ICL machine	582
				Goodware		learning online repository	942
14	Kok et al, 2020	Cuckoo	Windows	Ransomware	Sgandurra	VirusShare VS malware repository theZoo	995
				Goodware		NA	942
15	Chen et al, 2019	Cuckoo	Host in Security Operation Centre	Ransomware attacked logs	WannaCry DBGer Defray	Infected System logs	NA

					Locky Cerber GandCrab nRansom		
				Non attacked Logs		Uninfected logs	NA
16	Pundir et al, 2020	Monitoring of micro-architectural events using hardware performance counter	Windows	Ransomware		VirusShare	80
				Goodware		OpenSSL C programs	76
17	Almashhadani et al, 2019	Python script and MATLAB	Networks	Dataset created by the network traffic of Malware Capture Facility Project (MCFP)			
18	Ahmadian et al, 2015	User client software	Backup Systems	Encrypted files	System files Documents Images Source code Executables Compressed		600
				Normal files	System files Documents Images Source code Executables Compressed		600
19	Bahrani et al, 2019	Virtual machine, Disco, and process monitoring	Windows	Ransomware			
				Benign		VirusShare	NA
20	Poudyal et al, 2020	Sandbox	Windows	Ransomware		VirusTotal	550
				Benign		Windows 10 Open Source Software	540
21		Cuckoo	Windows	Ransomware	TeslaCrypt	VirusShare	96

	Ahmed et al, 2020				Petya Pgpcoder Reveton CryptoWall Kollah Kovter Citroni Trojan CryptLocker Torrent Locker Cerber WannaCry Dirty Decrypt	VirusTotal	89 46 50 151 73 23 67 82 173 171 74 108 51
				Benign		Software.informer System32 of Win7 Pro	NA
22	Zuhair et al, 2020	Weka and Python code		Ransomware	Archiveus CryptoLocker AiDS RaaS Zeus Locky GpCode CryptoWall Crysis WinLock WannaCry Sopra Reveton Cerber	VirusTotal VirusShare	1500 1720 4000 1300 1500 2000 8000 3250 1320 3620 1300 1570 2400 1535
				Malware			500
23	Kok et al, 20219	Cuckoo	Windows	Ransomware	CryptoLocker Reveton Kovter Critroni	Resilient Information System Security (RISS) dataset	107 90 64 50

					TeslaCrypt Locker CryptoWall MATSNU KOLLAH GPCODER Trojan- Ransom		6 97 46 59 25 4 34
				Goodware			942
24	Al-Hawawreh et al, 2019	Cuckoo	Windows	Ransomware		VirusShare	1139
				Goodware		Softonic	22000
25	Yang et al, 2020	Cuckoo Sandbox	Windows	Ransomware		VirusShare	22000
				Goodware		Windows	100
26	AbdulsalamYa'u et al, 2019	Cuckoo	Edge Computing	Ransomware		Resilient Information Security System (RISS)	582
				Goodware			942
27	Sharmeen et al, 2020	Cuckoo Sandbox	Windows	Ransomware	CryptoWall Trojan Ransom TeslaCrypt Kollah Reveton Citroni TorrentLocker Pgpcoder Dirty Decrypt Kovter CryptoLocker Petya Cerber WannaCry	VirusShare VirusTotal Malwarebytes OffensiveComputing	151 82 74 73 50 67 108 46 51 23 173 89 171 74
				Benign		Software-informer System 32 of	1308

						Windows 7 Pro	
28	Basnet et al, 2021	Python program PIN tool and Custom	Supervisory control data acquisition systems (SCADA)	Ransomware		VirusTotal	561
				Benign		Windows	447
29	Ganfure et al, 2020	Cuckoo	Windows	Ransomware		VirusShare	2000
				Benign		System logs	2000
30	Nurnoby and Alfy, 2019	Cuckoo Sandbox	Windows/Mac/Mobile	Ransomware		VirusShare	2000
				Benign		System logs	2000
31	Ullah et al, 2020	Cuckoo Sandbox	Desktop	Ransomware		VirusTotal	35,369
				Benign			43,191
32	Qin et al, 2020	Cuckoo	Windows	Ransomware		Sangfor Technologies Incorporation	1000
				Benign			1000
33	Aurangzeb et al, 2021	Cuckoo Sandbox	Windows	Ransomware		NA	80
				NonRansomware		NA	80
34	Abdullah et al, 2020	Genymotion	Android	Ransomware		VirusTotal	400
				Benign		GooglePlay Store	400
35	Ahmed et al, 2021	I/O patterns observation from Process execution patterns	Windows	Ransomware	Cerber Sodinokibi GoldenEye Sage Locky Dharma dotExe WannaCry Xorist Virlock.Gen.5 LockScree.AGU Alphabet Other	VirusTotal MalwareBazaar theZoo Malware samples from github	33 14 12 5 5 3 3 3 2 83 12 2 29
				Benign			
36	Ayub et al, 2020		Windows	Ransomware	CryptoWall	VirusTotal	17 2

					Deshacop CryptoDefense Upatre Zbot Critroni Yakes Crowti Others		6 56 6 2 150 23 10
				Benign		Windows 7, 8.1, 10 logs	NA
37	Jethva et al, 2020	Cuckoo Sandbox	Windows	Ransomware	TeslaCrypt CryptoShield Cerber Crysis Sage Unlock26 Locky CryptoMix Petya WannaCry Flawed	VirusTotal	348 4 122 8 5 3 129 2 2 1 1
				Benign		Software repository Website	103