ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

“Advanced Persistent Threats (2015-2022)”

Ευγένιος Γκρίτσης

ΑΜ: P3190045

Εποπτεύων: **Δημήτρης Γκρίτζαλης**

ΑΘΗΝΑ, ΣΕΠΤΕΜΒΡΙΟΣ 2022

Περιεχόμενα

Περίληψη

Είναι κοινά παραδεκτό ότι τα τελευταία χρόνια το πλήθος των επιθέσεων στον κυβερνοχώρο αυξάνεται εκθετικά. Δεδομένου των ολοένα και αυξανόμενων ποσοστών χρήσης του διαδικτύου που οφείλονται στην ραγδαία «ψηφιοποίηση» του τρόπου ζωής και της πρόσφατης παγκόσμιας πανδημίας COVID-19, η οποία δημιούργησε την ανάγκη για μετάβαση από τον υλικό στον ψηφιακό κόσμο (π.χ. τηλεργασία), φυσικό ακόλουθο αποτελεί η αλματώδης αύξηση των κυβερνοεπιθέσεων και της πολυπλοκότητάς τους.

Ένα υποσύνολο στοχευμένων επιθέσεων διακρίνεται για την δεξιότητα και την πολυπλοκότητα των μεθόδων που χρησιμοποιούν, την άρτια οργάνωση και τεχνική κατάρτιση των ομάδων που φέρνουν εις πέρας τέτοιες επιθέσεις, καθώς και για την πιθανή χρηματοδότηση και εμπλοκή κυβερνητικών φορέων. Αυτό το σενάριο απειλής, περιγράφεται ως Προηγμένη Επίμονη Απειλή (Advanced Persistent Threat, APT). Αρχικά, κύριος στόχος τους ήταν κυβερνητικοί φορείς και κρίσιμες υποδομές, ενώ με την πάροδο του χρόνου φαίνεται πως επεκτάθηκε η ζώνη στόχου τους και πλέον περιλαμβάνει οργανισμούς, επιχειρήσεις, και απλούς πολίτες. Όντας κρατικά χορηγούμενοι, οι φορείς APT έχουν στην διάθεση τους εξαιρετικά εξελιγμένα εργαλεία και λογισμικά. Αυτό αποδεικνύεται από τα προηγμένα κακόβουλα λογισμικά και τεχνικές που χρησιμοποιούν για πετύχουν τους καλά καθορισμένους στόχους τους.

Οι επιθέσεις τύπου APT αποτελούν σήμερα από τις σημαντικότερες απειλές στον κυβερνοχώρο. Αυτό έχει ως αποτέλεσμα, κυβερνήσεις και οργανισμοί να κάνουν επίμονες προσπάθειες να αμυνθούν έναντι τέτοιων απειλών, χωρίς να έχουν καταφέρει να μειώσουν το χάσμα ανάμεσα στις εξελιγμένες μεθοδολογίες επίθεσης και στις αντίστοιχες άμυνας.

Σκοπός της παρούσας εργασίας είναι η καταγραφή, η ανάλυση και μελέτη των επιθέσεων που οφείλονται σε προηγμένες επίμονες απειλές, στο χρονικό διάστημα 2015-2022, με σκοπό την εξαγωγή μορφότυπων επίθεσης (attack patterns), καθώς και ενδεικτικών μέτρων προστασίας. Αυτή η έρευνα αποτελεί συνέχεια προηγούμενων παρόμοιων μελετών που έχουν πραγματοποιηθεί τα τελευταία έτη. Ωστόσο η χρησιμότητα της έγκειται στο γεγονός πως περιλαμβάνονται εξελιγμένες και σύγχρονες επιθέσεις, καθώς η απότομη εξέλιξη της τεχνολογίας επιβάλλει την συνεχή επιτήρηση και ανάλυση των νέων δεδομένων. Σύμφωνα με τα προαναφερθέντα, η παρούσα μελέτη μπορεί να συνεισφέρει περισσότερο στην πιο αποτελεσματική ικανότητα ανάλυσης μορφότυπων και ανάπτυξης μέτρων προστασίας έναντι σε προηγμένες επίμονες απειλές.

Abstract

It is widely acknowledged that in recent years the number of cyber-attacks has increased exponentially. Given the ever-increasing rates of internet usage due to the rapid "digitalization" of lifestyles and the recent global pandemic COVID-19 which created the need to transition from the physical to the digital world (e.g. telecommuting), a natural corollary is the exponential increase in cyber-attacks and their sophistication.

A subset of targeted attacks is distinguished by the skill and sophistication of the methods used, the highly organized and technically skilled teams that carry out such attacks, and the potential funding and involvement of government agencies. This threat scenario is described as an Advanced Persistent Threat (APT). Initially, their main target was government agencies and critical infrastructure, but over time their target zone appears to have expanded to include organizations, businesses, and ordinary citizens. Being state-sponsored, APT actors have highly sophisticated tools and software at their disposal. This is evidenced by the advanced malware and techniques they use to achieve their well-defined objectives.

APT attacks are one of the most significant cyber threats today. As a result, governments and organizations have been making persistent efforts to defend against such threats, but have not been able to narrow the gap between sophisticated attack and defense methodologies.

The purpose of this paper is to document, analyze and study attacks due to advanced persistent threats, over the period 2015-2022, in order to derive attack patterns and indicative protection measures. This research is a continuation of previous similar studies carried out in recent years. However, its usefulness lies in the fact that it includes sophisticated and modern attacks, as the sudden evolution of technology requires continuous monitoring and analysis of new data. In line with the aforementioned, this study can further contribute to a more effective ability to analyze patterns and develop protection measures against advanced persistent threats.

1. Εισαγωγή

Η ασφάλεια στον κυβερνοχώρο είναι η τέχνη της προστασίας των δικτύων, των συσκευών και των δεδομένων από μη εξουσιοδοτημένη πρόσβαση ή εγκληματική χρήση και η πρακτική της διασφάλισης της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών [1]. Αναλυτικότερα, με τον όρο εμπιστευτικότητα εννοούμε την αποφυγή της αποκάλυψης μιας πληροφορίας χωρίς την άδεια του ιδιοκτήτη της, ως ακεραιότητα ορίζεται η αποφυγή της μη εξουσιοδοτημένης τροποποίησης μιας πληροφορίας και διαθεσιμότητα ονομάζεται η αποφυγή της αδικαιολόγητης καθυστέρησης ενός εξουσιοδοτημένου χρήστη να αποκτήσει προσπέλαση σε πληροφορίες ή υπολογιστικούς πόρους [2].

Είναι ευρέως αποδεκτό ότι με την τεχνολογική πρόοδο των τελευταίων δύο δεκαετιών η κοινωνία άλλαξε και συνεχώς αλλάζει μορφή με την ολοένα και αυξανόμενη «ψηφιοποίηση» του τρόπου ζωής. Η ραγδαία αλλαγή έχει επηρεάσει κάθε οντότητα, από τους απλούς πολίτες έως τους οργανισμούς και τις κυβερνήσεις, καθώς ένα μεγάλο μέρος της καθημερινότητας βασίζεται πλέον στους υπολογιστές και στο διαδίκτυο. Η επικοινωνία, η ψυχαγωγία, οι μεταφορές, οι αγορές, η ιατρική και οι υπηρεσίες που προσφέρονται απ' τις επιχειρήσεις και τα κράτη στηρίζονται στην αποθήκευση και επεξεργασία τεράστιων όγκων εμπιστευτικών δεδομένων και πληροφοριών σε πληροφοριακά συστήματα και ψηφιακές υποδομές που επικοινωνούν και βασίζονται στο διαδίκτυο.

Με την συνεχή ραγδαία αύξηση του όγκου και της πολυπλοκότητας των κυβερνοεπιθέσεων [3], αλλά και με την τρομερή αύξηση του αριθμού των παγκόσμιων χρηστών του διαδικτύου (από 2,48 δις το 2014 στα 4,95 δις το 2022 [4]), η ασφάλεια στον κυβερνοχώρο αποτελεί πλέον αναγκαία συνθήκη για την διασφάλιση της ευδαιμονίας και της ομαλής λειτουργίας των πραγμάτων. Πλέον υπάρχουν ποικίλα είδη επιθέσεων που αξιοποιούν εκατοντάδες διαφορετικές μεθοδολογίες, τεχνικές και τεχνολογίες για να διεισδύσουν και να μολύνουν τα συστήματα των στόχων τους. Οι επιθέσεις μπορεί να στοχεύουν στην συλλογή πληροφοριών, στην κατασκοπεία, στην κλοπή χρημάτων, στην πρόκληση οικονομικών και φυσικών ζημιών, στην διαταραχή υπηρεσιών και λειτουργιών, στο σαμποτάζ, στην προώθηση πολιτικών ιδεών κ.α.

Όλοι οι χρήστες και ιδιοκτήτες οποιασδήποτε συσκευής που συνδέεται στο διαδίκτυο αποτελούν εν δυνάμει στόχο κυβερνοεπίθεσης. Μερικά από τα πιο γνωστά είδη επιθέσεων στον κυβερνοχώρο αποτελούν οι επιθέσεις που εκμεταλλεύονται "zero-day" (προηγουμένως άγνωστες στην κοινότητα της κυβερνοασφάλειας και των ειδικών) τρωτότητες, επιθέσεις με την χρήση μεθόδων κοινωνικής μηχανικής (social engineering), όπως phishing και spear-phishing, οι επιθέσεις με ιομορφικό λογισμικό όπως, με πρόγραμμα ιό (virus), λυτρισμικό (ransomware), δούρειο ίππο (trojan), αναπαραγωγό (worm), λογισμικό κατασκοπείας (spyware), οι επιθέσεις DoS (Denial of Service), DDoS (Distributed Denial of Service), MitM (Man-in-the-middle), XSS (Cross-Site Scripting), SQL Injections και πολλές άλλες [5].

Το έγκλημα στον κυβερνοχώρο όχι μόνο έχει εξελιχθεί σε τεράστιο βαθμό τα τελευταία χρόνια, αλλά από την αρχή του 2020 λόγω της παγκόσμιας πανδημίας COVID-19 πολλά άτομα, επιχειρήσεις και κρατικοί φορείς αναγκάστηκαν να υιοθετήσουν και να βασιστούν σε ακόμη

περισσότερες ψηφιακές τεχνολογίες και υπηρεσίες. Αυτό είχε ως αποτέλεσμα την εντυπωσιακή αύξηση κατά 600% των κυβερνοεγκλημάτων από την αρχή της πανδημίας [6]. Σύμφωνα με ειδικούς [7], αναμένεται να αυξάνεται κατά 15% ετησίως το παγκόσμιο κόστος που προκλήθηκε από κυβερνοεγκλήματα έως το 2025, φθάνοντας τα 10,5 τρις δολάρια ετησίως το 2025 από τα 3 τρις δολάρια που καταγράφηκαν το 2015.

Ωστόσο, ένα μικρό υποσύνολο των παραπάνω επιθέσεων διαφέρει από τις υπόλοιπες κατηγορίες. Πλέον, οι χώρες με τεχνολογικά προηγμένες κυβερνήσεις ακολουθώντας τις στρατιωτικές πολιτικές τους, έχουν αρχίσει να δίνουν μεγαλύτερη βαρύτητα στην ενίσχυση των επιθετικών και αμυντικών δυνατοτήτων τους στον κυβερνοχώρο. Η επιθυμία αυτή, δηλαδή να είναι προετοιμασμένες να αμυνθούν απέναντι σε οποιαδήποτε απειλή αλλά ταυτόχρονα να οργανώνουν και να επιτίθονται με μεγάλης κλίμακας καταστροφικές επιχειρήσεις και εκστρατείες στον κυβερνοχώρο απέναντι σε πολιτικούς «αντιπάλους», ώθησε στην δημιουργία εξαιρετικά προηγμένων και άρτια οργανωμένων τεχνικών ομάδων που συνήθως δρουν με την υποστήριξη των υπηρεσιών ασφάλειας των κυβερνήσεων.

Επιθέσεις τέτοιου είδους, ονομάζονται προηγμένες επίμονες απειλές (Advanced Persistent Threat - APT) και συγκριτικά με μια κοινή επίθεση διαφέρουν σε πολλά σημεία, όπως για παράδειγμα στους στόχους, στα κίνητρα, στις μεθοδολογίες, στην πολυπλοκότητα των εργαλείων και των τεχνολογιών που χρησιμοποιούνται, στην κλίμακα και στις ζημιές που προκαλούν. Αντικείμενο της παρούσας εργασίας αποτελούν οι παραπάνω επιθέσεις.

Πιο συγκεκριμένα, οι έννοιες, οι ορισμοί, τα χαρακτηριστικά και άλλα σημαντικά σημεία των APTs θα παρουσιαστούν και θα θεμελιωθούν στο 2ο κεφάλαιο, ενώ στο 3ο και 4ο κεφάλαιο θα παρουσιαστούν και αναλυθούν καταγεγραμμένες επιθέσεις τύπου APT, όπου με βάση αυτές θα εξαχθούν οι συνηθισμένοι μορφότυποι αυτών των επιθέσεων, καθώς και μέτρα προστασίας και αντιμετώπισης.

2. Εννοιολογική θεμελίωση

2.1 Ορισμός APT

Ο όρος «προηγμένη επίμονη απειλή» (Advanced Persistent Threat – APT) εμφανίζεται για πρώτη φορά σε μια αίτηση διπλώματος ευρεσιτεχνίας των ΗΠΑ που κατατέθηκε το 2007 και δημοσιεύτηκε το 2008 [8], [9], η οποία περιγράφει τον όρο ως εξής:

«Η επόμενη φάση στην εξέλιξη των απειλών είναι μια πιο προηγμένη, επίμονη απειλή. Χαρακτηρίζεται από μεγαλύτερη πολυπλοκότητα και δεξιότητα, ταχεία συνεργασία και ολοένα και πιο δομημένες σχέσεις για την εξουδετέρωση των πολύπλοκων μηχανισμών ασφαλείας του δικτύου – πολλές φορές εκ των έσω. Τα κίνητρά τους γίνονται όλο και περισσότερο επικεντρωμένα στο κέρδος και ο τρόπος δράσης τους περιλαμβάνει επιμονή και μυστικότητα. Πιθανώς περιλαμβάνουν κρατικά χρηματοδοτούμενους φορείς, τα αποτελέσματα των οποίων συμβάλλουν σε μακροπρόθεσμες εκστρατείες επιρροής και εκμετάλλευσης, καθώς και σε καταστροφικά αποτελέσματα για τη διευκόλυνση της στρατιωτικής δράσης. Οι υπογραφές τους περιλαμβάνουν τη χρήση zero-day εκμεταλλεύσεων, κατανεμημένων δικτύων πρακτόρων (distributed agent networks), προηγμένων τεχνικών κοινωνικής μηχανικής (social engineering), όπως το spear-phishing, και η μακροπρόθεσμη εξόρυξη και εξαγωγή δεδομένων. Η ευελιξία τους και το ισχυρό κιτ εργαλείων και τεχνικών που διαθέτουν καθιστά τις προηγμένες απειλές ιδιαίτερα δύσκολο να νικηθούν επιτυχώς με την σημερινή τεχνολογικά βαριά εστίαση στην ασφάλεια δικτύων».

Στην παραπάνω περιγραφή του όρου, γίνεται λόγος για την πιθανή ανάμιξη κρατικά χρηματοδοτούμενων φορέων. Ακόμη και σε αυτό το αρχικό στάδιο, ο όρος χρησιμοποιούταν για να περιγράψει ένα σενάριο απειλής σε αντίθεση με έναν συγκεκριμένο επιτιθέμενο.

Ο ορισμός του APT δεν είναι αυστηρά καθορισμένος και υπάρχουν πολλές διαφορετικές εκδοχές του, αλλά κυρίως καλύπτει απειλές με μια σειρά από κοινά χαρακτηριστικά. Σύμφωνα με το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NISP) [10] των Ηνωμένων Πολιτειών της Αμερικής, ο ορισμός του έχει ως εξής:

«Ένας αντίπαλος με εξελιγμένα επίπεδα εμπειρογνωμοσύνης και σημαντικούς πόρους, που του επιτρέπει μέσω της χρήσης πολλαπλών διαφορετικών φορέων επίθεσης (π.χ., στον κυβερνοχώρο, τη φυσική κατάσταση και την παραπλάνηση) να δημιουργεί ευκαιρίες για την επίτευξη των στόχων του, οι οποίοι είναι συνήθως η εγκαθίδρυση και η επέκταση ερεισμάτων εντός της υποδομής τεχνολογίας πληροφοριών των οργανισμών με σκοπό τη συνεχή εξαγωγή πληροφοριών και/ή την υπονόμευση ή την παρεμπόδιση κρίσιμων πτυχών μιας αποστολής, ενός προγράμματος ή ενός οργανισμού, ή να βρεθεί σε θέση να το πράξει στο μέλλον. Επιπλέον, η προηγμένη επίμονη απειλή επιδιώκει τους στόχους της επανειλημμένα για παρατεταμένο χρονικό διάστημα, προσαρμόζεται στις προσπάθειες του αμυνόμενου να της αντισταθεί και με αποφασιστικότητα διατηρεί το επίπεδο αλληλεπίδρασης που απαιτείται για την εκτέλεση των στόχων της».

Από τους παραπάνω ορισμούς, συμπεραίνουμε πως αυτό το σενάριο απειλής ονομάζεται «προηγμένη επίμονη απειλή» διότι [11]:

- **Προηγμένη** σημαίνει πως ο επιτιθέμενος μπορεί να λειτουργήσει σε όλο το φάσμα της εισβολής σε έναν υπολογιστή. Μπορεί να χρησιμοποιήσει το πιο πρόσφατο δημόσια διαθέσιμο exploit μιας γνωστής τρωτότητας ή μπορεί να αναπτύξει προσαρμοσμένα exploits αναλόγως την φύση του στόχου του.
- **Επίμονη** σημαίνει πως ο αντίπαλος έχει αναλάβει να φέρει εις πέρας μια αποστολή. Δεν είναι ευκαιριακός εισβολέας. Λαμβάνει οδηγίες και εργάζεται για να ικανοποιήσει καλά ορισμένους στόχους. Το επίμονο δεν σημαίνει απαραίτητα ότι πρέπει να εκτελεί συνεχώς κακόβουλες ενέργειες στους υπολογιστές των θυμάτων του, αλλά αντιθέτως σημαίνει να διατηρεί το επίπεδο αλληλεπίδρασης που απαιτείται για την εκτέλεση των στόχων του.
- **Απειλή** σημαίνει πως ο επιτιθέμενος δεν είναι αποτελεί ένα κομμάτι «άμυαλου» κώδικα. Πολλές φορές ο όρος «απειλή» χρησιμοποιείται για την περιγραφή ενός ιομορφικού λογισμικού. Όμως, εάν το λογισμικό αυτό δεν επικοινωνούσε με τον δράστη για να ελέγχει τις ενέργειες και να διαβάζει τα κλεμμένα δεδομένα, τότε το μεγαλύτερο μέρος του κακόβουλου λογισμικού θα ήταν ελάχιστα ανησυχητικό (εφόσον δεν υποβαθμίζει ή δεν αρνείται δεδομένα). Αντίθετα, ο επιτιθέμενος αποτελεί απειλή διότι είναι εξειδικευμένος και οργανωμένος, χρηματοδοτείται και έχει κίνητρα.

Ο όρος APT χρησιμοποιείται συχνά καταχρηστικά. Σε πολλές περιπτώσεις, σε μια προσπάθεια αιτιολόγησης ενός περιστατικού ασφαλείας, οργανισμοί και επιχειρήσεις αποδίδουν τις ευθύνες σε μια προηγμένη επίμονη απειλή, λέγοντας πως το περιστατικό δεν μπορούσε να αποφευχθεί, λόγω των προηγμένων επιθετικών δυνατοτήτων του επιτιθέμενου. Ωστόσο, οι διαφορές μεταξύ μιας λιγότερο εξελιγμένης κυβερνοεπίθεσης και μιας επίθεσης τύπου APT δεν είναι πάντα σαφής. Ενδεικτικό στοιχείο για επιθέσεις APT αποτελεί η χρήση εξελιγμένων τεχνικών, νέων μεθόδων και προσαρμοσμένου κακόβουλου λογισμικού. Όμως, αξίζει να σημειωθεί πως έχουν υπάρξει περιπτώσεις επιθέσεων που αξιοποίησαν πολύ λιγότερο εξελιγμένα εργαλεία και τεχνικές, αλλά εξακολουθούν να θεωρούνται APT. Οι επιτιθέμενοι δεν θα δαπανήσουν πόρους για την ανάπτυξη προηγμένων εργαλείων εάν μπορούν να επιτύχουν τους στόχους τους χρησιμοποιώντας δημοσίως διαθέσιμα. Το γεγονός αυτό, καθιστά πολύ πιο δύσκολη την απόδοση ευθυνών, καθώς οι δράστες εκμεταλλεύονται εργαλεία τα οποία μπορούν να χρησιμοποιηθούν από οποιονδήποτε [12].

2.2 Ταξινομία επιθέσεων APT

Έχουν αναπτυχθεί και προταθεί πολλές ταξινομίες για την ανάλυση των δραστών APT, παραδείγματα αποτελούν έρευνες από τους Chen και άλλοι [13], Lemay και άλλοι [14], Bahrami και άλλοι [15]. Οι παρακάτω πληροφορίες σχετικά με την ταξινομία των επιθέσεων πάρθηκαν από την έρευνα του Ν. Βιρβίλη [12] καθώς κρίθηκε βοηθητική για μια εφ' όλης της ύλης σύνοψη. Συγκεκριμένα, οι επιθέσεις τύπου APT με βάση το μονοπάτι επίθεσης που θα ακολουθήσουν, διακρίνονται σε εξωτερικές, εσωτερικές και έμμεσες.

Εξωτερικές Επιθέσεις

Η πλειονότητα των γνωστών επιθέσεων APT εμπίπτει σε αυτήν την κατηγορία. Σε αυτές, ο δράστης προσπαθεί να θέσει σε κίνδυνο την υποδομή του στόχου του εξ αποστάσεως. Αυτό συνήθως επιτυγχάνεται μέσω της χρήσης τεχνικών κοινωνικής μηχανικής, όπως η αποστολή ενός έξυπνα διαμορφωμένου μηνύματος ηλεκτρονικού ταχυδρομείου σε έναν συγκεκριμένο αριθμό χρηστών που εργάζονται στην υποδομή-στόχο (spear-phishing attack). Δεν είναι ασυνήθιστο για τον επιτιθέμενο να πραγματοποιεί εκ των προτέρων εκτεταμένη συλλογή πληροφοριών για να αυξήσει την πιθανότητα επιτυχίας του. Αυτό μπορεί να επιτευχθεί με την εκμετάλλευση των κοινωνικών δικτύων προκειμένου να βρεθούν οι πιθανοί στόχοι, τα ενδιαφέροντα, την τεχνογνωσία και την θέση τους στον οργανισμό ή μέσω υπηρεσιών πληροφοριών (για επιθέσεις που χρηματοδοτούνται από κυβερνήσεις). Ανεξάρτητα από τον τρόπο που σχεδιάστηκε η επίθεση, όσο περισσότερες πληροφορίες διαθέτει ο φορέας APT, τόσο πιο πιθανό είναι η αρχική προσπάθεια εκμετάλλευσης να είναι επιτυχής.

Σε αυτόν τον τύπο επιθέσεων, ο δράστης έχει το πλεονέκτημα πως μπορεί να εκτελέσει τις κακόβουλες ενέργειες του μέσω του διαδικτύου από μια απομακρυσμένη και ασφαλή τοποθεσία. Λόγω αυτής της απομακρυσμένης φύσεως, ο κίνδυνος να αποδοθούν οι ευθύνες σε ένα συγκεκριμένο άτομο είναι αρκετά χαμηλός, ακόμη και εάν κατά την διάρκεια της έρευνας ανακτηθούν οι πραγματικές διευθύνσεις IP του δράστη. Επιπλέον, η ταυτοποίηση είναι σχεδόν απίθανη, όχι μόνο για τις προηγμένες επίμονες απειλές, αλλά και για λιγότερο εξελιγμένες και πιο καθημερινές επιθέσεις, καθώς υπάρχουν πολλαπλές μέθοδοι απόκρυψης της διεύθυνσης IP (π.χ. TOR network, Proxychains, VPN κ.α.). Ακόμη και σε περιπτώσεις που έχουν αποδοθεί ευθύνες, εάν η επιχείρηση ήταν χρηματοδοτούμενη από κρατικούς κυβερνητικούς φορείς, τότε είναι πολύ δύσκολο να αντιμετωπίσουν οι υπεύθυνοι οποιεσδήποτε κυρώσεις.

Εσωτερικές Επιθέσεις / Εσωτερική Απειλή

Σύμφωνα με τον CISA [16], η εσωτερική επίθεση ή αλλιώς απειλή εκ των έσω, είναι το ενδεχόμενο ένας εσωτερικός κακόβουλος υπάλληλος (insider) να χρησιμοποιήσει την εξουσιοδοτημένη πρόσβαση ή κατανόηση ενός οργανισμού για να βλάψει τον οργανισμό. Αυτές είναι είτε επιθέσεις που σχεδιάζονται και διεξάγονται από τον insider, είτε επιθέσεις στις οποίες ο insider ενεργεί ως συνεργός μιας μεγαλύτερης ομάδας. Η ζημιά που προκαλεί μπορεί να περιλαμβάνει κακόβουλες, αυθαίρετες ή ακούσιες πράξεις που επηρεάζουν αρνητικά την ακεραιότητα, την εμπιστευτικότητα και την διαθεσιμότητα των πληροφοριακών συστημάτων του οργανισμού. Συγκεκριμένα, μπορεί να προκληθούν ζημιές σε αποστολές, πόρους, εγκαταστάσεις, προσωπικό, πληροφορίες, εξοπλισμό, δίκτυα, συστήματα και άλλα. Η απειλή αυτή, μπορεί να εκδηλωθεί με τις παρακάτω συμπεριφορές ενός insider:

- Κατασκοπεία
- Τρομοκρατία
- Μη εξουσιοδοτημένη αποκάλυψη πληροφοριών
- Διαφθορά, συμπεριλαμβανόμενης της συμμετοχής σε διεθνώς οργανωμένο έγκλημα

- Σαμποτάζ
- Βία στον εργασιακό χώρο
- Ηθελημένη ή αθέλητη απώλεια ή υποβάθμιση των πόρων ή των δυνατοτήτων ενός τμήματος του οργανισμού
- Κλοπή

Σημαντικές επιθέσεις εκ των έσω, αποτελούν οι περιπτώσεις της Chelsea Manning και του Edward Snowden. Πιο συγκεκριμένα, η Chelsea Manning ήταν πρώην στρατιώτης του αμερικανικού στρατού και καταδικάστηκε για την διαρροή πολλών χιλιάδων απόρρητων εγγράφων, καθώς στις αρχές του Ιανουαρίου του 2010, κατέβασε εμπιστευτικές πληροφορίες σχετικά με τους πολέμους στο Ιράκ και το Αφγανιστάν και τις διέρρευσε στον γνωστό ιστότοπο WikiLeaks. Αργότερα, η ίδια δήλωσε πως τα κίνητρά της ήταν ανθρωπιστικά και πολιτικά. Από την άλλη πλευρά, ο Edward Snowden είναι πρώην εργολάβος της NSA (National Security Agency) και στις αρχές του 2013 δημοσιοποίησε χιλιάδες απόρρητα έγγραφα, αποκαλύπτοντας παρεμβατικά προγράμματα παγκόσμιας παρακολούθησης, εκτεθειμένα κρυπτοσυστήματα και πολλαπλά εργαλεία και τεχνικές επίθεσης που χρησιμοποιούσε η NSA για την εκτέλεση μαζικών προγραμμάτων παρακολούθησης.

Έμμεσες Επιθέσεις

Ο όρος «έμμεσες επιθέσεις» αναφέρεται σε επιθέσεις στον κυβερνοχώρο κατά τις οποίες ο δράστης εφαρμόζει πολυεπίπεδες τακτικές για να κλέψει, διαταράξει ή να καταστρέψει δεδομένα μέσω ενδιάμεσων τρίτων πηγών [17]. Αναλυτικότερα, οι επιθέσεις αυτού του είδους έχουν ως τελικό στόχο την εκμετάλλευση ενός συγκεκριμένου θύματος, αλλά αντί να επιτεθεί ο δράστης άμεσα στην υποδομή και στα συστήματα αυτού, στοχεύει τρίτους, όπως παρόχους και υπηρεσίες που χρησιμοποιούνται από το αρχικό θύμα-στόχο. Με την εκμετάλλευση αυτών των παρόχων και υπηρεσιών, διευκολύνεται η πρόσβαση και η μόλυνση των συστημάτων του στόχου, λόγω της σχέσης εμπιστοσύνης μεταξύ των δύο.

2.3 Ανατομία και μεθοδολογία επιθέσεων APT

Κάθε επίθεση προηγμένης επίμονης απειλής ενεργεί με διαφορετικό τρόπο και οι μεθοδολογίες και τεχνικές που χρησιμοποιούνται προσαρμόζονται αναλόγως με το επιλεγμένο θύμα. Υπάρχουν πολλαπλές διαφορετικές προσεγγίσεις για την σειρά των φάσεων-βημάτων μιας επίθεσης APT. Στα πλαίσια της συγκεκριμένης έρευνας, θα παρουσιαστούν τα βήματα αναλυτικά σύμφωνα με το μοντέλο της Dell SecureWorks [18] και με επιπρόσθετες πληροφορίες που πάρθηκαν από άλλες πηγές [19], [20].

Εικόνα 1. *Κύκλος ζωής μιας προηγμένης επίμονης απειλής [21].*

Οι φάσεις μιας επίθεσης APT διακρίνονται σε 6 κατηγορίες:

1. Προετοιμασία (Preparation).
2. Αρχική διείσδυση (Initial Intrusion).
3. Επέκταση (Expansion).
4. Επιμονή (Persistence).
5. Αναζήτηση και εξαγωγή πληροφοριών (Search and exfiltration).
6. Κάλυψη των ιχνών / Καθαρισμός (Covering the tracks / Clean Up).

Προετοιμασία (Preparation)

Η φάση προετοιμασίας περιλαμβάνει τις εξής πτυχές του κύκλου ζωής:

- Καθορισμός στόχου (Define target).

- Εύρεση και οργάνωση συνεργατών (Find and organize accomplices).
- Ανάπτυξη ή απόκτηση εργαλείων (Build or acquire tools).
- Έρευνα στόχου/υποδομών/εργαζομένων (Research target).
- Δοκιμή για ανίχνευση (Test for detection).

Οι επιθέσεις τύπου APT συνήθως περιλαμβάνουν υψηλό βαθμό προετοιμασίας. Στην φάση αυτή, οι δράστες πραγματοποιούν μια πλήρη μελέτη σχετικά με τον στόχο τους με σκοπό να χαρτογραφήσουν όσο το δυνατόν καλύτερα τα πληροφοριακά συστήματα τους και να αναζητήσουν τρωτότητες εντός τους. Στην μελέτη αυτή, τα στοιχεία που συλλέγονται περιλαμβάνουν υποδομές, εργαλεία, δεδομένα, πληροφορίες για το περιβάλλον των στόχων, τοπολογίες δικτύου, domains, διακομιστές DNS και DHCP, περιοχές διευθύνσεων IP, θύρες κ.α. Επιπλέον, συλλέγονται και κρίσιμες πληροφορίες σχετικά με τους ελέγχους και διαδικασίες ασφαλείας που έχουν υιοθετήσει οι στόχοι με σκοπό την αποφυγή τους.

Η υποδομή που απαιτείται για την διεξαγωγή μιας επιχείρησης ποικίλλει ανάλογα με τον στόχο, αλλά το στάδιο αυτό αποτελεί απαραίτητη προϋπόθεση για μια επιτυχημένη επίθεση, καθώς όση περισσότερη γνώση αποκτά ένας κυβερνοεγκληματίας σε ένα στοχευμένο δίκτυο, τόσο μεγαλύτερες είναι οι πιθανότητες επιτυχούς διείσδυσης και ανάπτυξης κακόβουλου λογισμικού.

Αρχική διείσδυση (Initial Intrusion)

Η φάση της αρχικής διείσδυσης περιλαμβάνει τις εξής πτυχές του κύκλου ζωής:

- Ανάπτυξη (Deployment).
- Αρχική εισβολή (Initial intrusion).
- Έναρξη εξερχόμενης σύνδεσης (Outbound connection initiated).

Το επόμενο βήμα της επιχείρησης APT είναι η προσπάθεια εισβολής στο περιβάλλον του στόχου. Ο επιτιθέμενος πλέον μελετάει τις άμυνες και τις λύσεις ασφαλείας που διαθέτει ο στόχος, με αποτέλεσμα να χρησιμοποιήσει προσαρμοσμένες τεχνικές για να διεισδύσει στα συστήματα του θύματος. Μια εξαιρετικά συνηθισμένη τακτική εισόδου είναι η χρήση spear-phishing μηνυμάτων που περιέχουν έναν σύνδεσμο URL ή συνημμένο αρχείο. Οι σύνδεσμοι ηλεκτρονικού ταχυδρομείου συνήθως οδηγούν σε μολυσμένους ιστότοπους, στους οποίους όταν συνδεθεί το θύμα, ο δράστης θα καταφέρει μέσω διαφόρων τεχνικών εκμετάλλευσης ή μέσω μεθόδων κοινωνικής μηχανικής, ο δράστης θα καταφέρει να αποκτήσει πρόσβαση σε στοιχεία του στόχου. Τα συνημμένα αρχεία είναι συνήθως ένα κακόβουλο λογισμικό το οποίο βρίσκεται εντός ενός άλλου αρχείου (π.χ. ZIP), ή έγγραφα τύπου Office, Adobe, PDF τα οποία εκμεταλλεύονται ορισμένες τρωτότητες στις εφαρμογές του θύματος για να εκτελεστεί το κακόβουλο λογισμικό στον υπολογιστή του.

Τα μηνύματα ηλεκτρονικού ταχυδρομείου phishing μπορεί να είναι πολύ πειστικά και να είναι δύσκολο να διακριθούν από τα νόμιμα μηνύματα. Μόλις ο στόχος ανοίξει το κακόβουλο αρχείο χρησιμοποιώντας ευάλωτο λογισμικό, το κακόβουλο λογισμικό εκτελείται και πλέον ο επιτιθέμενος έχει πρόσβαση στα συστήματα του στόχου του. Συνήθως αποτελεί ένα trojan

απομακρυσμένης πρόσβασης και λειτουργεί ως ένα απλό πρόγραμμα λήψης των επόμενων προγραμμάτων και στοιχείων της επίθεσης και ξεκινάει μια σύνδεση επικοινωνίας με τους διακομιστές C2 του επιτιθέμενου.

Επέκταση (Expansion)

Η φάση της επέκτασης περιλαμβάνει τις ακόλουθες πτυχές του κύκλου ζωής:

- Επέκταση πρόσβασης και απόκτηση διαπιστευτηρίων (Expand access and obtain credentials).
- Ενίσχυση των ερεισμάτων (Strengthen foothold).

Συνήθως, ένας από τους στόχους του επιτιθέμενου, είναι να αποκτήσει όσο περισσότερα δικαιώματα γίνεται και να καταφέρει να εισχωρήσει σε πολλαπλά συστήματα. Σε αυτές τις περιπτώσεις η επέκταση πρόσβασης αποτελεί μια από τις αμέσως επόμενες ενέργειες που εκτελούνται μετά την αρχική εισβολή.

Για να αποκτηθούν τα διαπιστευτήρια σύνδεσης και να επιτευχθεί κλιμάκωση προνομίων (escalation of privileges), ο επιτιθέμενος χρησιμοποιεί τεχνικές και λογισμικά όπως keyloggers, ARP spoofing και εργαλεία hooking. Αναλυτικότερα, με τα keyloggers καταγράφονται όλα τα πλήκτρα που πατιούνται στο παραβιασμένο μηχάνημα με αποτέλεσμα να καταγράφονται και εμπιστευτικά στοιχεία, όπως οι κωδικοί χρηστών. Τα εργαλεία ARP spoofing κατασκοπεύουν συνομιλίες μεταξύ δύο ή περισσοτέρων συστημάτων μέσω ενός παραποιημένου ARP (Address Resolution Protocol) ώστε να κλέψουν διαπιστευτήρια. Τα εργαλεία hooking ουσιαστικά «αγκιστρώνουν» λειτουργίες που σχετίζονται με τον έλεγχο ταυτότητας κωδικών πρόσβασης, ενώ υπάρχει πληθώρα εργαλείων (π.χ. Mimikatz, Windows Credential Editor, Magipet, Lslsass, Gsecdump, CacheDump) όπως το Pwdump που κατεβάζει κατακερματισμένους κωδικούς πρόσβασης από το μητρώο των Windows. Επιπροσθέτως, συχνά χρησιμοποιούνται και άλλες τεχνικές όπως brute force και “pass the hash”.

Επιμονή (Persistence)

Σε αυτήν την φάση, ο επιτιθέμενος προσπαθεί να εδραιώσει την παρουσία του στο εσωτερικό του δικτύου του στόχου παρακάμπτοντας τις περιμετρικές του άμυνες. Γνωρίζει πολύ καλά, πως οι περισσότεροι οργανισμοί χρησιμοποιούν προϊόντα και λύσεις ασφαλείας όπως τα antivirus, επομένως λαμβάνει τα κατάλληλα μέτρα για να διασφαλίσει πως τα εργαλεία και οι μέθοδοι που θα χρησιμοποιήσει δεν θα ανιχνευτούν. Αυτό συνήθως σημαίνει πως ο επιτιθέμενος θα αναπτύξει προσαρμοσμένο κακόβουλο λογισμικό ή θα χρησιμοποιήσει ευρέως γνωστά εργαλεία τα οποία θα ανακατασκευάσει κατάλληλα (π.χ. psexec, password dumpers κ.α.). Έπειτα, δοκιμάζεται το λογισμικό που θα χρησιμοποιηθεί με σύγχρονα εργαλεία προστασίας από ιούς για να αξιολογηθεί η ικανότητα του να παραμείνει «αόρατο». Αυτή η διαδικασία είναι αποτελεσματική καθώς ο δράστης είναι πιθανό να έχει πρόσβαση στα περισσότερα προϊόντα ασφαλείας που κυκλοφορούν στην αγορά.

Κάθε οργανισμός, μόλις εντοπίσει ένα περιστατικό παραβίασης των συστημάτων του, θα ακολουθήσει ορισμένες διαδικασίες και τεχνικές με στόχο την ανάκτηση του κακόβουλου λογισμικού, την ανάλυση της κυκλοφορίας του δικτύου και την συλλογή δεικτών παραβίασης. Ωστόσο, ο επιτιθέμενος είναι εξοικειωμένες με αυτές τις τεχνικές απόκρισης και μέσω της αξιοποίησης πολλαπλών προσαρμοσμένων κακόβουλων λογισμικών με την μορφή πρόσθετων εκτελέσιμων αρχείων και υπηρεσιών καταφέρνει να καθυστερήσει και να δυσκολέψει τις προσπάθειες των οργανισμών να ανακτήσουν δείκτες παραβίασης. Επιπλέον, λόγω της παρακολούθησης της δικτυακής κυκλοφορίας από τους οργανισμούς, ο επιτιθέμενος συχνά δεν ενεργοποιεί όλο το κακόβουλο λογισμικό ταυτόχρονα, αλλά πολλές φορές ενεργοποιείται μετά από ένα μεγάλο χρονικό διάστημα και επικοινωνεί με διάφορους κεντρικούς διακομιστές C2.

Συμπληρωματικά, η εγκατάσταση του κακόβουλου λογισμικού σε μη παραδοσιακές τοποθεσίες αποτελεί μια συχνή και δύσκολα ανιχνεύσιμη μεθοδολογία που ακολουθούν φορείς APT. Προσθέτοντας το λογισμικό σε νόμιμους διακομιστές, δρομολογητές, τείχη προστασίας (firewalls), εκτυπωτές και άλλα σημεία τα οποία δεν είναι τόσο πιθανό να εξεταστούν για μόλυνση, καταφέρνει ο δράστης να διατηρήσει την πρόσβασή του. Τέλος, σε περιπτώσεις που αναμένονται να διεξαχθούν εγκληματολογικές έρευνες στα μολυσμένα συστήματα, ο επιτιθέμενος προετοιμάζει την πλήρη απομάκρυνσή του, διαγράφοντας και καταστρέφοντας όλα τα αποδεικτικά στοιχεία ενώ καθιστά και το σύστημα μη λειτουργικό.

Αναζήτηση και εξαγωγή πληροφοριών (Search and exfiltration)

Σε αυτό το στάδιο, ο δράστης APT στοχεύει στην μη εξουσιοδοτημένη μεταφορά ευαίσθητων πληροφοριών από το δίκτυο ενός στόχου σε εξωτερική τοποθεσία την οποία ελέγχει ο ίδιος. Αφού ανακαλύψει τα δεδομένα που τον ενδιαφέρουν, τα συγκεντρώνει σε ένα αρχείο και στην συνέχεια τα συμπιέζει και κρυπτογραφεί. Αυτό έχει ως αποτέλεσμα την απόκρυψη του περιεχομένου του αρχείου από επιθεωρήσεις πακέτων σε βάθος (deep packet inspection) και από τεχνικές πρόληψης απώλειας δεδομένων (data loss prevention techniques).

Οι οργανισμοί και οι επιχειρήσεις αναγκάζονται καθημερινά να επιτηρούν την διαδικτυακή κυκλοφορία τεράστιων όγκων δεδομένων και δραστηριοτήτων με αποτέλεσμα η ανίχνευση της παράνομης μεταφοράς των κλεμμένων δεδομένων στους διακομιστές του δράστη να είναι πολύ δύσκολη. Μόλις συγκεντρωθούν οι ευαίσθητες πληροφορίες, τα δεδομένα του αρχείου διοχετεύονται σε έναν εσωτερικό διακομιστή προετοιμασίας, όπου τεμαχίζονται, συμπιέζονται και συχνά κρυπτογραφούνται για την μετάδοση σε εξωτερικές τοποθεσίες ανάκτησης από τον δράστη. Ορισμένα εργαλεία που αξιοποιούνται για τέτοιου είδους λειτουργίες και διαδικασίες είναι το Lz77 το οποίο χρησιμοποιείται για την συμπίεση, το ZXProxy και το ZXPortMap που βοηθάνε στην ανακατεύθυνση συνδέσεων HTTP/HTTPS για την απόκρυψη της πηγής της σύνδεσης, το LSB-Steganography το οποίο αξιοποιεί τεχνικές στεγανογραφίας για την ενσωμάτωση αρχείων σε εικόνες, το ZXHttpServer που είναι ένας μικρός ευέλικτος διακομιστής HTTP και άλλα.

Κάλυψη των ιχνών / Καθαρισμός (Covering the tracks / Cleanup)

Στο τελευταίο στάδιο του κύκλου ζωής μιας επίθεσης τύπου APT, ο δράστης επικεντρώνεται στην αποφυγή εντοπισμού, στην αφαίρεση αποδεικτικών στοιχείων της εισβολής και στην εξάλειψη στοιχείων σχετικά με το ποιος βρίσκεται πίσω από την επίθεση. Σε μερικές περιπτώσεις [22], ο επιτιθέμενος χρησιμοποιεί τακτικές "False Flags" με σκοπό να εξαπατήσει τα θύματα και τις ομάδες ασφαλείας καθιστώντας πολύ δύσκολη την απόδοση ευθυνών. Όσο καλύτερα ο φορέας APT καλύψει τα ίχνη του, τόσο πιο δύσκολο θα είναι για τα θύματα να αξιολογήσουν τον αντίκτυπο της παραβίασης.

3. Μελέτη και ανάλυση νέων επιθέσεων (2015-2022)

Σε αυτό το κεφάλαιο, παρουσιάζονται και αναλύονται πολύπλοκες και άρτια οργανωμένες επιθέσεις σε κρίσιμες υποδομές και κυβερνητικούς φορείς στο χρονικό διάστημα 2015-2022, με σκοπό την εξαγωγή μορφότυπων και συμπερασμάτων. Οι κυβερνοεπιθέσεις αυτές, επιλέχθηκαν λόγω της εντυπωσιακής πολυπλοκότητας των μεθόδων και εργαλείων που εκμεταλλεύτηκαν, καθώς και των καταστροφικών ζημιών που προκάλεσαν. Στην συνέχεια του κεφαλαίου βρίσκεται ο πίνακας σύγκρισης των λογισμικών, τεχνικών και μεθόδων 21 επιθέσεων που οφείλονται σε προηγμένες επίμονες απειλές και έπειτα -μέσω του πίνακα- εξάγονται σημαντικά κοινά χαρακτηριστικά και μορφότυποι.

Μεθοδολογία

Δεδομένα, πληροφορίες και τεχνικές λεπτομέρειες που αξιοποιήθηκαν στα πλαίσια αυτής της έρευνας, συλλέχθηκαν κυρίως από εταιρείες κυβερνοασφάλειας που ειδικεύονται σε τέτοιου είδους επιθέσεις (π.χ. MITRE, Mandiant, Kaspersky, ESET, CrowdStrike, Dragos, CheckPoint κ.α.), από αναφορές κρατικών υπηρεσιών ασφάλειας (π.χ. FBI, CISA κ.α.) και από άλλα μέσα ενημέρωσης όπως διαδικτυακά άρθρα και forums.

Συνολικά συγκεντρώθηκαν πληροφορίες και υλικό σχετικά με 21 κυβερνοεπιθέσεις, ωστόσο από αυτές επιλέχθηκαν οι 15 προς παρουσίαση και ανάλυση, ενώ οι υπόλοιπες 6 διαδραματίζουν συμπληρωματικό ρόλο στην εξαγωγή συμπερασμάτων και περιλαμβάνονται τα κύρια χαρακτηριστικά τους στον πίνακα σύγκρισης.

3.1 Παρουσίαση επιλεγμένων επιθέσεων

3.1.1 Ukraine Power Grid Cyberattack

Περιγραφή επίθεσης

Η κυβερνοεπίθεση στο ηλεκτρικό δίκτυο της Ουκρανίας που έλαβε χώρα στις 23 Δεκεμβρίου του 2015 αποτέλεσε την πρώτη γνωστοποιημένη επίθεση ενάντια σε λειτουργίες ηλεκτρικού δικτύου και σηματοδότησε ένα επαναστατικό γεγονός για τους διαχειριστές ηλεκτρικών δικτύων. Για να επιτευχθεί αυτής της κλίμακας καταστροφή οι δράστες εισέβαλαν στα δίκτυα τριών περιφερειακών εταιρειών διανομής ηλεκτρικής ενέργειας, καθώς και σε τρεις κρίσιμους οργανισμούς, μολύνοντάς τους με το BlackEnergy3 trojan. Από εκεί, κατάφεραν να μετακινηθούν και να αποκτήσουν πρόσβαση και στα δίκτυα SCADA των εταιρειών ηλεκτρικής ενέργειας, με αποτέλεσμα, να μπορέσουν να αποσυνδέσουν υποσταθμούς διανομής ηλεκτρισμού, χρησιμοποιώντας νόμιμες διαδικασίες, αφήνοντας περισσότερους από 225.000 πελάτες δίχως ρεύμα για 1 έως και 6 ώρες, μέχρις ότου να επαναφέρουν το ρεύμα χειροκίνητα οι πάροχοι [23].

Σύμφωνα με τον CISA [24], η κυβερνοεπίθεση ήταν συγχρονισμένη και συντονισμένη, ενώ πιθανότατα ακολούθησε εκτεταμένη αναγνώριση και παρακολούθηση των δικτύων των

θυμάτων, καθώς οι επιθέσεις στις εταιρείες σημειώθηκαν με διαφορά 30 λεπτών η μια από την άλλη και επηρέασαν πολλαπλές κεντρικές και περιφερειακές εγκαταστάσεις. Κατά την διάρκεια των επιθέσεων, πραγματοποιήθηκαν πολλαπλές κακόβουλες απομακρυσμένες λειτουργίες διακοπτών χρησιμοποιώντας είτε υπάρχοντα εργαλεία απομακρυσμένης διαχείρισης σε επίπεδο λειτουργικού συστήματος είτε από λογισμικό βιομηχανικού ελέγχου μέσω συνδέσεων εικονικού ιδιωτικού δικτύου (Virtual Private Network).

Αρχική μόλυνση - προσβολή

Την άνοιξη του 2015 οι δράστες στόχευσαν διαχειριστές και προσωπικό του τμήματος πληροφορικής των τριών εταιρειών διανομής ηλεκτρικής ενέργειας, χρησιμοποιώντας τεχνικές spear-phishing. Πιο συγκεκριμένα, η δράση τους πραγματοποιήθηκε με την αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου τα οποία περιείχαν αρχεία Office με κακόβουλες μακροεντολές. Μόλις ένα μέλος του προσωπικού άνοιγε ένα από αυτά τα μηνύματα, ένα αναδυόμενο παράθυρο του ζητούσε να τις ενεργοποιήσει. Η ενεργοποίηση της λειτουργίας μακροεντολών στο Office επέτρεψε στο BlackEnergy3 να φορτωθεί στο σύστημα του θύματος [25].

Κακόβουλο λογισμικό - μέθοδοι

Στο πρώτο μέρος της επίθεσης αξιοποιήθηκε μια ενημερωμένη έκδοση του κακόβουλου λογισμικού BlackEnergy [26], [27] με το οποίο οι δράστες ανέκτησαν διαπιστευτήρια διαχειριστή και κατάφεραν να αποκτήσουν πρόσβαση στα δίκτυα των υποσταθμών ενέργειας. Κατά την διάρκεια της δεύτερης φάσης χρησιμοποιήθηκε το καταστροφικό λογισμικό KillDisk, το οποίο έκανε τα συστήματα με Windows μη λειτουργικά, διαγράφοντας ή τροποποιώντας το master boot record, ενώ σε άλλα συστήματα απλώς διέγραφε τα logs [23]. Σαν τελική φάση της επίθεσης, οι δράστες εξαπέλυσαν μια επίθεση TDoS στοχεύοντας στην άρνηση της διαθεσιμότητας του τηλεφωνικού κέντρου εξυπηρέτησης πελάτων, εμποδίζοντας τους καλούντες να αναφέρουν την διακοπή ηλεκτρικής ενέργειας [26].

Τύπος PE

Ο τύπος PE των αρχείων που αξιοποιήθηκαν από το κακόβουλο λογισμικό και από τους επιτιθέμενους στα πλαίσια αυτής της επίθεσης είναι DLL.

Επικοινωνία με C&C / C2 servers

Κατά την εγκατάσταση του, το BlackEnergy3 επιχειρούσε να συνδεθεί με την IP του C2. Δεν έχουν αναγνωριστεί οι διευθύνσεις IP των servers που χρησιμοποιήθηκαν κατά την επίθεση αλλά είναι πιθανό οι δράστες να μετακινήθηκαν σχετικά σύντομα από τους αρχικούς C2 servers [23].

Τεχνικές αποφυγής ανίχνευσης

Οι εταιρείες πιστεύουν πως οι δράστες απέκτησαν νόμιμα διαπιστευτήρια πριν από την κυβερνοεπίθεση [24] με αποτέλεσμα να μειώνεται σημαντικά η πιθανότητα να ανιχνευτεί παράνομη δραστηριότητα εντός των συστημάτων των εταιρειών.

Κρυπτογράφηση

Δεν βρέθηκαν πληροφορίες σχετικά με την κρυπτογράφηση.

Στόχος επίθεσης

Ο στόχος της επίθεσης ήταν η διαταραχή του ηλεκτρικού δικτύου και της παροχής ρεύματος.

Απόδοση ευθυνών

Η κυβέρνηση των Ηνωμένων Πολιτειών Αμερικής αποδίδει την εν λόγω δραστηριότητα σε Ρωσικούς εθνικούς κυβερνοπαράγοντες [24].

3.1.2 CRASHOVERRIDE / Industroyer

Περιγραφή επίθεσης

Το CRASHOVERRIDE ή αλλιώς γνωστό και ως Industroyer αποτελεί το δεύτερο γνωστοποιημένο κακόβουλο λογισμικό που σχεδιάστηκε με σκοπό την διατάραξη συστημάτων βιομηχανικού ελέγχου (ICS). Αν και έχουν ξανά υπάρξει επιθέσεις που στόχευαν ηλεκτρικά δίκτυα (π.χ. Ουκρανία 2015), καμία από αυτές δεν χρησιμοποίησε κακόβουλο λογισμικό το οποίο να προκαλεί άμεσα την ζημιά στα συστήματα των ηλεκτρικών δικτύων ή των ICS. Οι δράστες που δημιούργησαν αυτό το λογισμικό κατέχουν βαθιά γνώση και κατανόηση των βιομηχανικών συστημάτων ελέγχου και ειδικότερα των πρωτοκόλλων που χρησιμοποιούνται σε αυτά.

Αποτέλεσμα της επίθεσης μέσω του CRASHOVERRIDE ήταν η απώλεια ηλεκτροδότησης του Κιέβου της Ουκρανίας για περίπου μια ώρα, αισθητά μικρότερης κλίμακας και διάρκειας από την επίθεση του 2015. Κύρια διαφορά μεταξύ των δυο, αποτελεί το γεγονός πως το 2015 οι δράστες χειραγώγησαν χειροκίνητα τα συστήματα μέσω παραβιασμένων απομακρυσμένων συνδέσεων σε σταθμούς ελέγχου του συστήματος, ενώ στο συμβάν του 2016 οι δράστες αξιοποίησαν το CRASHOVERRIDE framework για την χειραγώγηση των βιομηχανικών συστημάτων ελέγχου [28]. Πιο συγκεκριμένα, οι επιτιθέμενοι είχαν την δυνατότητα μέσω κατάλληλων ακολουθιών εντολών να χειραγωγήσουν την φυσική κατάσταση ορισμένων διακοπτών με αποτέλεσμα την υποβάθμιση της αξιοπιστίας του ηλεκτρικού δικτύου [29].

Αρχική μόλυνση – προσβολή

Η αρχική διείσδυση στο περιβάλλον-στόχο κατά πάσα πιθανότητα επιτεύχθηκε μέσω ενός phishing campaign το οποίο είχε ήδη ξεκινήσει από τον Ιανουάριο του 2016 και σύμφωνα με αποδεικτικά στοιχεία που εντοπίστηκαν, οι δράστες απέκτησαν αρχική πρόσβαση στο δίκτυο του στόχου το αργότερο τον Οκτώβριο του 2016 [28].

Κακόβουλο λογισμικό - μέθοδοι

Το CRASHOVERRIDE από μόνο του αποτελεί ένα framework σχεδιασμένο για την ανάπτυξη πολλαπλών κακόβουλων φορτίων (payloads) για συγκεκριμένα πρωτόκολλα ICS, με στόχο την διατάραξη της διανομής ηλεκτρικής ενέργειας. Ειδικότερα το λογισμικό περιέχει τα εξής δομικά στοιχεία [30]:

- *Κύρια κερκόπορτα (Main backdoor)*: Αποτελεί το βασικό συστατικό του κακόβουλου λογισμικού και χρησιμοποιείται για τον έλεγχο όλων των υπολοίπων οντοτήτων και στοιχείων. Επίσης, κατεβάζει στο σύστημα-στόχο την πρόσθετη κερκόπορτα και το πρόγραμμα εκκίνησης.
- *Πρόσθετη κερκόπορτα (Additional backdoor):* Παρέχει έναν εναλλακτικό μηχανισμό persistence που επιτρέπει στους χάκερς να αποκτήσουν πρόσβαση στο δίκτυο σε περίπτωση που εντοπιστεί ή/και απενεργοποιηθεί η κύρια κερκόπορτα. Η κερκόπορτα αυτή, είναι μια trojanized έκδοση της εφαρμογής Notepad των Windows.
- *Πρόγραμμα εκκίνησης (Launcher component):* Αποτελεί ένα ξεχωριστό εκτελέσιμο αρχείο που είναι υπεύθυνο για την εκκίνηση των φορτιών 101, 104, 61850, OPC DA και της μονάδας Data wiper. Το πρόγραμμα λειτουργούσε σαν time bomb καθώς εκκινούσε 2 νήματα εκτέλεσης των παραπάνω στοιχείων αφότου 2 συγκεκριμένες ημερομηνίες είχαν περάσει.
- *Μονάδα διαγραφής δεδομένων (Data wiper component):* Αποτελεί μια καταστροφική μονάδα που χρησιμοποιείται στο τελικό στάδιο της επίθεσης με στόχο να δυσχεράνουν τον εντοπισμό τους και την ανάκτηση των δεδομένων.

Δεδομένου της λειτουργικότητας του, το λογισμικό αυτό πρέπει να φορτωθεί σε κάποιο τερματικό σύστημα εντός του δικτύου-στόχου το οποίο πρέπει να έχει την δυνατότητα να χειρίζεται ή να επικοινωνεί απευθείας με τον εξοπλισμό ελέγχου ICS.

Τύπος PE

Ο τύπος PE των αρχείων που αξιοποιήθηκαν από το κακόβουλο λογισμικό και από τους επιτιθέμενους στα πλαίσια αυτής της επίθεσης είναι DLL και EXE.

Επικοινωνία με C&C / C2 servers

Η κύρια κερκόπορτα συνδέεται με τον απομακρυσμένο διακομιστή C2 χρησιμοποιώντας το πρωτόκολλο HTTPS και λαμβάνει εντολές από τους επιτιθέμενους. Οι περισσότεροι από τους διακομιστές που χρησιμοποιήθηκαν ανήκουν στο δίκτυο Tor και παράλληλα η επικοινωνία γίνεται μόνο ώρες εκτός του ωραρίου εργασίας, με αποτέλεσμα να δυσχεραίνεται η ανίχνευση της παράνομης κίνησης [30].

Τεχνικές αποφυγής ανίχνευσης

Οι επιτιθέμενοι χρησιμοποίησαν μια trojanized έκδοση της γνωστής εφαρμογής Notepad των Windows. Αναλυτικότερα, πρόκειται για μια πλήρως λειτουργική έκδοση της εφαρμογής, αλλά οι συγγραφείς του κακόβουλου λογισμικού έχουν εισάγει κακόβουλο κώδικα που εκτελείται κάθε φορά που η εφαρμογή εκτελείται [30].

Κρυπτογράφηση

Δεν βρέθηκαν πληροφορίες σχετικά με την κρυπτογράφηση.

Στόχος επίθεσης

Η λειτουργικότητα του CRASHOVERRIDE framework δεν εξυπηρετεί σκοπούς κατασκοπείας, αλλά αξιοποιείται για επιθέσεις που μπορούν να οδηγήσουν σε διακοπές ρεύματος [28].

Απόδοση ευθυνών

Μετά την ανάλυση του CRASHOVERRIDE στα μέσα του 2017, ερευνητές του Dragos [31] απέδωσαν την ευθύνη στην ομάδα Electrum και συμπλήρωσαν πως υπάρχει το ενδεχόμενο να υπηρέτησαν ως μονάδα ανάπτυξης δυνατοτήτων ICS για την APT ομάδα Sandworm, η οποία εξυπηρετεί Ρωσικά κυβερνητικά συμφέροντα. Ενώ πολλές πτυχές της δραστηριότητας της Electrum παραμένουν αβέβαιες, οι διαθέσιμες πληροφορίες υποδεικνύουν ότι η ομάδα διαθέτει εξειδικευμένες ικανότητες ανάπτυξης ειδικού λογισμικού ICS και παραμένει ενεργή.

3.1.3 Bangladesh Bank Cyber Heist

Περιγραφή επίθεσης

Η κυβερνοεπίθεση ενάντια στην κεντρική τράπεζα του Μπαγκλαντές τον Φεβρουάριου του 2016 θεωρείται από τις μεγαλύτερες και πιο καλοσχεδιασμένες επιθέσεις σε συστήματα

SWIFT. Το SWIFT (Society for Worldwide Interbank Financial Telecommunications) είναι μια ασφαλή υπηρεσία ανταλλαγής μηνυμάτων που χρησιμοποιείται για την μετάδοση οικονομικών μηνυμάτων μεταξύ τραπεζών σε όλο τον κόσμο. Τον Μάιο του 2015, οι επιτιθέμενοι δημιούργησαν πολλαπλούς τραπεζικούς λογαριασμούς, χρησιμοποιώντας πλαστές ταυτότητες και κατέθεσαν στον καθένα από αυτούς το ποσό των 500 δολαρίων. Μόλις οι επιτιθέμενοι απέκτησαν πρόσβαση στα συστήματα της τράπεζας, εκμεταλλεύτηκαν αξιόπιστο λογισμικό των Windows ώστε να παρακολουθήσουν τους εργαζομένους και τις δραστηριότητες τους. Αξιοποιώντας πληροφορίες που συγκέντρωσαν οι δράστες, κατάφεραν να κινηθούν σε όλα τα εσωτερικά συστήματα της τράπεζας αναζητώντας εκείνα που συνδέονταν άμεσα με το SWIFT. Με την πρόσβαση στα συστήματα SWIFT, οι επιτιθέμενοι πλέον είχαν την δυνατότητα να παρακολουθήσουν τους υπαλλήλους, να κλέψουν διαπιστευτήρια και να ετοιμάσουν κατάλληλο λογισμικό το οποίο θα επιτίθεται σε εφαρμογές SWIFT Alliance Access παρακάμπτοντας τα μέτρα ασφαλείας και αφαιρώντας τις αποδείξεις.

Συνολικά 35 συναλλαγές SWIFT αξίας 951.000.000 δολαρίων πραγματοποιήθηκαν. Οι 30 από αυτές απορρίφθηκαν διότι αποστέλλονταν σε ένα υποκατάστημα της RCBC σε οδό με όνομα "Jupiter". Το όνομα αυτό προκάλεσε κυρώσεις στην Ομοσπονδιακή Τράπεζα των ΗΠΑ λόγω εντελώς διαφορετικών κυρώσεων κατά μιας εταιρείας πετρελαιοφόρων με την επωνυμία "Jupiter Seaways Shipping" η οποία συνδεόταν με προσπάθειες του Ιράν να αποφύγει ναυτιλιακές κυρώσεις. Από τις άλλες 5 συναλλαγές, η μία απορρίφθηκε λόγω ορθογραφικού λάθους, ενώ οι υπόλοιπες εγκρίθηκαν και 81.000.000 δολάρια μεταφέρθηκαν στους 4 λογαριασμούς που αναφέρθηκαν παραπάνω [32]. Εάν δεν γινόντουσαν τα παραπάνω σφάλματα, τα οποία οδήγησαν στο να απορριφθούν οι 30 συναλλαγές, οι δράστες θα κατάφερναν να εξάγουν περισσότερα από 950 εκατομμύρια δολάρια, καθιστώντας την κυβερνο-ληστεία ως «την πιο καταστροφική κυβερνοεπίθεση όλων των εποχών» [33].

Αρχική μόλυνση – προσβολή

Κατά την διάρκεια του Ιανουαρίου και Φεβρουαρίου του 2015, πολλαπλά μηνύματα ηλεκτρονικού ταχυδρομείου στάλθηκαν σε εργαζομένους της τράπεζας. Τα μηνύματα αυτά περιείχαν ένα βιογραφικό σημείωμα και μία συνοδευτική επιστολή εντός ενός αρχείου .zip. Μέσω αυτού του spear-phishing campaign κατάφεραν οι δράστες να αποκτήσουν αρχική πρόσβαση στα υπολογιστικά συστήματα της τράπεζας τον Μάρτιο του 2015 [32].

Κακόβουλο λογισμικό

Οι δράστες αρχικά εγκατέστησαν το λογισμικό στον SWIFT Alliance Software Server. Το λογισμικό έψαχνε ανάμεσα σε όλες τις διεργασίες του διακομιστή για να εντοπίσει αυτές που περιείχαν το "liboradb.dll" module και τους τροποποιούσε 2 bytes έτσι ώστε να αναγκάζεται η εφαρμογή να εγκρίνει πάντα τους ελέγχους εγκυρότητας, με αποτέλεσμα να παρέχονται στο κακόβουλο λογισμικό δικαιώματα εκτέλεσης συναλλαγών στην βάση δεδομένων της τράπεζας [32].

Τύπος PE

Ο τύπος PE των αρχείων που αξιοποιήθηκαν από το κακόβουλο λογισμικό και από τους επιτιθέμενους στα πλαίσια αυτής της επίθεσης είναι EXE.

Επικοινωνία με C&C / C2 servers

Η επικοινωνία των επιτιθέμενων με το κακόβουλο λογισμικό γινόταν μέσω του πρωτοκόλλου HTTP.

Τεχνικές αποφυγής ανίχνευσης

Οι επιτιθέμενοι χρησιμοποίησαν αξιόπιστο λογισμικό των Windows για την παρακολούθηση των δραστηριοτήτων των υπαλλήλων της τράπεζας.

Κρυπτογράφηση

Δεν βρέθηκαν πληροφορίες σχετικά με την κρυπτογράφηση.

Στόχος επίθεσης

Η κυβερνοεπίθεση στην κεντρική τράπεζα του Μπαγκλαντές ουσιαστικά αποτέλεσε μια κυβερνο-ληστεία με αποκλειστικό στόχο την κλοπή μεγάλων χρηματικών ποσών.

Απόδοση ευθυνών

Σύμφωνα με το FBI [34], η επίθεση στην τράπεζα του Μπαγκλαντές ήταν αποτέλεσμα των προσπαθειών της γνωστής APT ομάδας Lazarus η οποία λειτουργεί με την υποστήριξη της κυβέρνησης της Βόρειας Κορέας.

3.1.4 Domestic Kitten

Όλα τα δεδομένα και πληροφορίες που αξιοποιήθηκαν για την ανάλυση της επίθεσης, πάρθηκαν από την έρευνα της Check Point [35].

Περιγραφή επίθεσης

Έρευνες που διεξάχθηκαν το 2018 από την Check Point, αποκάλυψαν μια εκτεταμένη και στοχευμένη επίθεση με αφετηρία το 2016 η οποία βρισκόταν ακόμη σε εξέλιξη κατά την διάρκεια της έρευνας. Συνολικά 240 χρήστες έπεσαν θύματα αυτής της εκστρατείας παρακολούθησης και

πάνω από το 97% των θυμάτων ήταν Ιρανοί. Εκτός από τους Ιρανικούς στόχους, ανακαλύφθηκαν και θύματα με προέλευση από το Αφγανιστάν, το Ιράκ, και τη Μεγάλη Βρετανία. Όμως, ο πραγματικός αριθμός ατόμων που προσβλήθηκαν από αυτήν την επίθεση ήταν πολύ μεγαλύτερος. Αυτό οφείλεται στο γεγονός πως ο πλήρης κατάλογος επαφών κάθε κινητού, συμπεριλαμβανομένων και των πλήρων ονομάτων συλλέχθηκε από τους δράστες, έχοντας ως αποτέλεσμα να παραβιαστούν οι προσωπικές πληροφορίες χιλιάδων χρηστών.

Αρχική μόλυνση – προσβολή

Μέσω της χρήσης εφαρμογών για κινητά τηλέφωνα, οι δράστες χρησιμοποίησαν ψεύτικο παραπλανητικό περιεχόμενο για να δελεάσουν τα θύματα τους να κατεβάσουν εφαρμογές οι οποίες είναι φορτωμένες με λογισμικό παρακολούθησης (spyware).

Κακόβουλο λογισμικό – μέθοδοι

Σύμφωνα με τους ερευνητές της Check Point τα θύματα παρασύρονται αρχικά στην λήψη εφαρμογών που πιστεύεται πως τους ενδιαφέρουν. Οι εφαρμογές που ανακαλύφθηκαν περιλαμβάνουν μία εφαρμογή που η κύρια λειτουργία της είναι η αλλαγή της ταπετσαρίας του κινητού με εικόνες του ISIS, μία εφαρμογή με ενημερώσεις από το πρακτορείο ειδήσεων ANF Kurdistan και μία ψεύτικη έκδοση εφαρμογής ανταλλαγής μηνυμάτων.

Όσον αφορά την εφαρμογή ειδήσεων του ANF, αποτελεί μια ανακατασκευασμένη και κακόβουλη έκδοση της νόμιμης ειδησεογραφικής ιστοσελίδας και χρησιμοποιείται για να εξαπατήσει τους στόχους των επιτιθέμενων.

Οι κακόβουλες εφαρμογές περιείχαν λειτουργίες συλλογής ευαίσθητων πληροφοριών από τις συσκευές των στόχων. Συγκεκριμένα το spyware επικεντρωνόταν στις εξής πληροφορίες:

- Μηνύματα SMS/MMS.
- Αρχεία κλήσεων τηλεφώνου.
- Λίστα επαφών.
- Ιστορικό και σελιδοδείκτες προγραμμάτων περιήγησης.
- Εξωτερικό αποθηκευτικό χώρο.
- Λίστα εφαρμογών.
- Περιεχόμενο πίνακα προσωρινής μνήμης (Clipboard).
- Γεωγραφική θέση.
- Φωτογραφίες κάμερας.
- Φωνητικές ηχογραφήσεις.

Τύπος PE

Δεν βρέθηκαν πληροφορίες σχετικά με τον τύπο PE.

Επικοινωνία με C&C / C2 servers

Όλα τα ευαίσθητα δεδομένα αποστέλλονται πίσω σε διακομιστές C2 χρησιμοποιώντας HTTP POST requests. Επιπλέον, μια από τις εφαρμογές βρέθηκε να επικοινωνεί με μία ιστοσελίδα με Ιρανική IP διεύθυνση που όμως στην συνέχεια άλλαξε σε Ρωσική. Συνολικά βρέθηκαν 4 IP διευθύνσεις και 4 domains

Τεχνικές αποφυγής ανίχνευσης

Δεν εντοπίστηκαν συγκεκριμένες τεχνικές αποφυγής.

Κρυπτογράφηση

Οι κακόβουλες εφαρμογές κωδικοποιούσαν τις επικοινωνίες τους με BASE64 και XOR αλγορίθμους. Τα κλεμμένα δεδομένα συγκεντρώνονταν σε ένα αρχείο, το οποίο στην συνέχεια συμπιέζεται και κρυπτογραφείται με AES.

Στόχος επίθεσης

Τέτοιου είδους προγράμματα παρακολούθησης χρησιμοποιούνται κατά ατόμων και ομάδων που θα μπορούσαν να αποτελέσουν απειλή για την σταθερότητα του Ιρανικού καθεστώτος. Επομένως, κύριος στόχος της επίθεσης ήταν η παρακολούθηση και η συλλογή πληροφοριών.

Απόδοση ευθυνών

Η ακριβής ταυτότητα του δράστη πίσω από την επίθεση παραμένει ανεπιβεβαίωτη. Οι ερευνητές όμως κατάφεραν να συλλέξουν σημαντικές πληροφορίες σχετικά με τους στόχους, την φύση των εφαρμογών και την υποδομή της επίθεσης με αποτέλεσμα να πειστούν πως η επιχείρηση αυτή είναι Ιρανικής προέλευσης. Σύμφωνα με εμπειρογνώμονες των υπηρεσιών πληροφοριών, Ιρανικές κυβερνητικές οντότητες όπως το IRGC και το υπουργείο εσωτερικών διεξάγουν συχνά εκτεταμένη παρακολούθηση μελών συγκεκριμένων ομάδων.

3.1.5 Operation Cloud Hopper

Περιγραφή επίθεσης

Η επιχείρηση Cloud Hopper πιθανώς είχε ήδη ξεκινήσει από το 2014, αλλά αυξήθηκε η συμμετοχή των δραστών και η ένταση της επίθεσης το 2016, αποκαλύφθηκε δημόσια το 2017 από την PwC σε συνεργασία με την εταιρεία BAE Systems [36] και παρέμεινε ενεργή και κατά την διάρκεια του 2018. Η επίθεση αυτή ταξινομείται ως “supply chain attack” και απέκτησε το όνομά

της λόγω της παραβίασης παρόχων MSP (managed service provider) των θυμάτων, αξιοποιώντας τους για να μεταπηδήσουν από το cloud των MSP στα δίκτυα των επιχειρήσεων-στόχων. Αυτό είχε ως αποτέλεσμα οι επιτιθέμενοι να αποκτήσουν πρόσβαση σε πνευματική ιδιοκτησία και ευαίσθητα δεδομένα των MSP και των πελατών τους σε παγκόσμιο επίπεδο [37].

Ειδικότερα, η επίθεση αυτή επηρέασε οργανισμούς στην Βόρεια Αμερική, την Ευρώπη, τη Νότια Αμερική, την Ασία και MSPs στο Ηνωμένο Βασίλειο, ΗΠΑ, Ιαπωνία, Καναδά, Βραζιλία, Γαλλία, Ελβετία, Νορβηγία, Φινλανδία, Σουηδία, Νότια Αφρική, Ινδία, Ταϊλάνδη, Νότια Κορέα και Αυστραλία. Στις βιομηχανίες που επηρεάστηκαν περισσότερο, περιλαμβάνονται οι κλάδοι της μηχανικής, βιομηχανικής παραγωγής, λιανικού εμπορίου, ενέργειας, φαρμάκων, τηλεπικοινωνιών και κυβερνητικών υπηρεσιών [38].

Αρχική μόλυνση – προσβολή

Οι χάκερς διείσδυσαν σε υποδομές διαχείρισης cloud αυτών των MSP χρησιμοποιώντας μεθόδους spear phishing. Συγκεκριμένα, αποστέλλοντας μηνύματα ηλεκτρονικού ταχυδρομείου που περιείχαν το κακόβουλο λογισμικό ενσωματωμένο σε έγγραφα Word [37] και μεταμφιέζοντας το με τέτοιον τρόπο, ώστε ο αποστολέας να φαίνεται πως είναι ένας νόμιμος οργανισμός, όπως μια υπηρεσία δημόσιου τομέα [38].

Κακόβουλο λογισμικό – μέθοδοι

Η πολυπλοκότητα της συγκεκριμένης επίθεσης είναι αρκετά υψηλή, καθώς οι δράστες χρησιμοποίησαν εργαλεία ανοιχτού κώδικα, τα οποία όμως τροποποίησαν με κατάλληλους τρόπους ώστε να βελτιωθεί η λειτουργικότητά τους [36]. Σύμφωνα με αναφορές της Trend Micro [38], οι επιτιθέμενοι χρησιμοποίησαν πολλαπλά κακόβουλα προγράμματα, συμπεριλαμβανομένων trojan γνωστών οικογενειών όπως PlugX, Poison Ivy, ChChes, Graftor και άλλων. Πάνω από 70 παραλλαγές trojan και κερκόπορτων βρέθηκαν. Οι δράστες χρησιμοποίησαν εργαλεία κλοπής διαπιστευτηρίων (π.χ. keyloggers) με προνόμια επιπέδου διαχειριστή για την πρόσβαση στους κοινόχρηστους χώρους των MSP και των πελατών τους. Με αυτόν τον τρόπο κατάφεραν να αποκτήσουν περαιτέρω πρόσβαση και στα δίκτυα των πελατών των MSP.

Τύπος PE

Ο τύπος PE των αρχείων που αξιοποιήθηκαν από το κακόβουλο λογισμικό και από τους επιτιθέμενους στα πλαίσια αυτής της επίθεσης είναι DLL.

Επικοινωνία με C&C / C2 servers

Τα κλεμμένα δεδομένα συγκεντρώνονται, συμπιέζονται και αποστέλλονται από το δίκτυο του MSP στην υποδομή που ελέγχεται από τους επιτιθέμενους. Η υποδομή C2 που χρησιμοποιείται βασίζεται κυρίως σε Dynamic DNS domains (DDNS) [36]. Η υπηρεσία DDNS επιτρέπει στους δράστες να λειτουργούν σε μεγάλη κλίμακα, διαθέτοντας μια δεξαμενή με πολλά domain names που δυναμικά αντιστοιχίζονται σε καινούριες διευθύνσεις IP. Με αυτόν τον τρόπο, ένα domain μπορεί να συσχετιστεί με πολλές διευθύνσεις και μια διεύθυνση IP να συσχετιστεί με πολλά domains.

Τεχνικές αποφυγής ανίχνευσης

Ορισμένοι trojan, όπως ο ARTIEF (TROJ_ARTIEF), μαζί με κακόβουλα αρχεία (TROJ_FAKEMS), προκειμένου να αποφύγουν την ανίχνευση, μιμούνται υπογραφές ή ιδιότητες αξιόπιστων και νόμιμων αρχείων της Microsoft [38].

Κρυπτογράφηση

Δεν βρέθηκαν πληροφορίες σχετικά με την κρυπτογράφηση.

Στόχος επίθεσης

Οι στόχοι της επίθεσης ήταν κυρίως βιομηχανική κατασκοπεία και σε συγκεκριμένες περιπτώσεις συλλογή πληροφοριών με πολιτικά κίνητρα [37].

Απόδοση ευθυνών

Τον Δεκέμβριο του 2018, η κυβέρνηση των ΗΠΑ απέδωσε την ευθύνη ολόκληρης της επιχείρησης Cloud Hopper στην ομάδα APT10 [39]. Η ομάδα αυτή συνδέεται με το Υπουργείο Κρατικής Ασφάλειας της Κίνας και ειδικεύεται από το 2006 στην κλοπή πνευματικής ιδιοκτησίας από βιομηχανίες στρατηγικού ενδιαφέροντος της Κίνας [37].

3.1.6 Trisis / Triton

Περιγραφή επίθεσης

Τον Δεκέμβριο του 2017, η εταιρεία κυβερνοασφάλειας Mandiant ανέφερε [40] πως πρόσφατα συνεργάστηκε με έναν βιομηχανικό φορέα του οποίου οι εγκαταστάσεις δέχτηκαν επίθεση από έναν νέο τύπο κακόβουλου λογισμικού που επιτιθόταν σε βιομηχανικά συστήματα ελέγχου (ICS). Το λογισμικό αυτό ονομάστηκε Triton αλλά είναι γνωστό και ως Trisis. Η εταιρεία

διαπίστωσε πως σχεδιάστηκε ειδικά για να αλληλεπιδρά με ελεγκτές των Safety Instrumented Systems (SIS) της Schneider Electric Triconex και ακολουθεί το Stuxnet που χρησιμοποιήθηκε κατά του Ιράν το 2010 και το Industroyer που αναπτύχθηκε κατά της Ουκρανίας το 2016. Το Triton συνάδει με αυτές τις επιθέσεις δεδομένου πως μπορεί να εμποδίσει τους μηχανισμούς ασφαλείας από το να εκτελέσουν τις προβλεπόμενες λειτουργίες τους, με αποτέλεσμα να προκληθούν φυσικές ζημιές.

Η στοχευμένη εγκατάσταση ταυτοποιήθηκε στην συνέχεια ως εργοστάσιο επεξεργασίας πετροχημικών προϊόντων της Σαουδικής Αραβίας. Οι δράστες απέκτησαν απομακρυσμένη πρόσβαση σε σταθμό εργασίας μηχανικού του SIS και αξιοποιώντας το λογισμικό Triton κατάφεραν να επαναπρογραμματίσουν τους ελεγκτές. Αυτό είχε ως αποτέλεσμα ορισμένοι ελεγκτές SIS να εισέλθουν σε κατάσταση αποτυχημένης ασφάλειας (failed safe state) [40]. Το Triton υπερβαίνει κατά πολύ τις προηγούμενες επιθέσεις και θεωρείται ορόσημο βιομηχανικής κυβερνοεπίθεσης διότι αλληλεπιδρά και ελέγχει άμεσα το SIS. Έτσι, αυξάνεται η πιθανότητα τέτοιο είδος επιθέσεων να προκαλέσουν απρόβλεπτες και επικίνδυνες συνθήκες [41].

Αρχική μόλυνση – προσβολή

Η επίθεση ξεκίνησε με την διείσδυση στο δίκτυο IT με την χρήση γνωστών και εύκολα ανιχνεύσιμων μεθόδων επίθεσης. Έπειτα, οι δράστες μετακινήθηκαν στο δίκτυο OT (Operational Technology) και από αυτό, κατάφεραν να μολύνουν τον σταθμό εργασίας μηχανικών συστημάτων SIS. Θεωρείται πιθανό η μόλυνση να επιτεύχθηκε χρησιμοποιώντας τεχνικές κοινωνικής μηχανικής (social engineering) καθώς κάποιος μηχανικός έλαβε και κατέβασε αρχείο με το φαινομενικά αξιόπιστο όνομα “trilog.exe” [41].

Κακόβουλο λογισμικό – μέθοδοι

Σύμφωνα με την έρευνα της FireEye [40], το Triton μιμείται το νόμιμο λογισμικό για Windows διαχείρισης ελεγκτών Triconex SIS Trilog. Το κακόβουλο αυτό λογισμικό είναι ένα compiled Python script που χρησιμοποιεί τον δημόσια διαθέσιμο ‘py2exe’ compiler. Αυτό επιτρέπει στο εκτελέσιμο να μπορεί να εκτελεστεί ακόμη και σε περιβάλλοντα που δεν είναι εγκατεστημένη η γλώσσα Python.

Η ανάλυση του κώδικα από την Dragos [42] έδειξε πως το script στόχευε στην αλλαγή της λογικής των μονάδων του επεξεργαστή Triconex 3008. Για να επιτευχθεί αυτή η τροποποίηση, σε πρώτη φάση παραδίδεται το trilog.exe στο θύμα. Το εκτελέσιμο αυτό αρχείο αξιοποιεί τις εντολές επικοινωνίας που περιέχονται σε ένα αρχείο .zip με όνομα library.zip και δύο δυαδικά αρχεία, τα inject.bin και imain.bin. Έχει την δυνατότητα να διαβάζει και να γράφει προγράμματα, μεμονωμένες λειτουργίες και να ζητά την κατάσταση ενός ελεγκτή SIS. Επίσης, το Triton μπορεί να επικοινωνήσει με τους ελεγκτές και να τους επαναπρογραμματίσει φορτώνοντας τους κακόβουλα φορτία (payloads) που έχουν ορίσει οι δράστες.

Τύπος PE

Ο τύπος PE των αρχείων που αξιοποιήθηκαν από το κακόβουλο λογισμικό και από τους επιτιθέμενους στα πλαίσια αυτής της επίθεσης είναι EXE.

Επικοινωνία με C&C / C2 servers

Σύμφωνα με τους ερευνητές της Madiant [43]:

- Για την μεταφορά εργαλείων και την απομακρυσμένη εκτέλεση εντολών και προγραμμάτων, οι επιτιθέμενοι βασίζονται σε κρυπτογραφημένα tunnels βασισμένες στο SSH.
- Αξιοποίηση κωδικοποιημένων διακομιστών DNS.
- Συχνές θύρες επικοινωνίας: 443, 4444, 8531, 50501.
- Το λογισμικό έψαχνε Dynamic DNS domains που ανήκουν στο afraid.org domain.
- Αξιοποίηση SSH και hard-coded OpenSSH private keys.

Τεχνικές αποφυγής ανίχνευσης

Οι επιτιθέμενοι προσπάθησαν να μειώσουν την πιθανότητα να ανιχνευτούν οι κακόβουλες δραστηριότητες τους αλληλεπιδρώντας με τους ελεγκτές σε ώρες εκτός λειτουργίας. Παράλληλα, χρησιμοποιούσαν αξιόπιστα ονόματα της Microsoft για τα αρχεία τους και διέγραφαν τα αρχεία που δεν χρειαζόντουσαν πλέον με στόχο την αποφυγή ανίχνευσης της παράνομης κίνησης τους.

Για να αποφύγει πολλών μορφών ανιχνεύσεων, το κακόβουλο λογισμικό χρησιμοποιεί τις εξής τεχνικές [44]:

- Το αρχείο inject.bin, μεταμφιέζεται σε ένα τυπικό μεταγλωττισμένο πρόγραμμα PowerPC για το Tricon.
- Το Triton απενεργοποιεί τον έλεγχο συνέπειας RAM/ROM εισάγοντας το imain.bin payload στην περιοχή μνήμης του κατάλληλου υλικολογισμικού.

Κρυπτογράφηση

Δεν βρέθηκαν πληροφορίες σχετικά με την κρυπτογράφηση.

Στόχος επίθεσης

Ο στόχος της επίθεσης ήταν η λειτουργική διαταραχή κρίσιμης υποδομής.

Απόδοση ευθυνών

Η κυβερνοεπίθεση αυτή, αποδίδεται στην APT ομάδα XENOTIME, που δραστηριοποιείται από το 2014. Η FireEye αργότερα συνέδεσε το κακόβουλο λογισμικό Triton/Trisis με το Κεντρικό Επιστημονικό Ερευνητικό Ινστιτούτο Χημείας και Μηχανικής (CNIIHM), έναν οργανισμό έρευνας που ανήκει στην Ρωσική κυβέρνηση [45].

3.1.7 NotPetya Campaign

Περιγραφή επίθεσης

Στις 27 Ιουνίου του 2017, μια μαζική επίθεση ransomware βρισκόταν σε εξέλιξη στην Ουκρανία. Χρησιμοποιήθηκε το NotPetya, το οποίο αποτελεί μια καταστροφική παραλλαγή λυτρισμικού (ransomware) που επηρέασε πάνω από 2000 Ουκρανικούς οργανισμούς και εξαπλώθηκε γρήγορα και σε όλη την Ευρώπη, χτυπώντας κυβερνήσεις, τράπεζες, εταιρείες εμπορίου και ενέργειας. Το NotPetya είχε τα χαρακτηριστικά ενός λυτρισμικού καθώς κρυπτογραφούσε κρίσιμα αρχεία και σκληρούς δίσκους και έπειτα ζητούσε 300 δολάρια σε bitcoin ως αντάλλαγμα για να ξεκλειδωθεί το μολυσμένο μηχάνημα. Ωστόσο, η διεύθυνση ηλεκτρονικού ταχυδρομείου που δόθηκε για την επικοινωνία με τους επιτιθέμενους δεν ήταν ζωντανή, επομένως δεν υπήρχε τρόπος να αποκρυπτογραφηθούν και να ανακτηθούν τα χαμένα αρχεία [46]. Αν και αρχικά φαινόταν ότι το λυτρισμικό αποτελούσε μια παραλλαγή της οικογένειας Petya, οι ερευνητές διαπίστωσαν πως δεν σχετίζονται μεταξύ τους και για αυτόν τον λόγο ονομάστηκε “NotPetya” [47].

Αρχική μόλυνση – προσβολή

Οι πρώτες μολύνσεις υποτίθεται πως προήλθαν μέσω ενός μηχανισμού ενημέρωσης της εφαρμογής M.E.Doc. Το λογισμικό αυτό αποτελεί επίσημο και εγκεκριμένο πρόγραμμα υποβολής φορολογικών δηλώσεων και ζητούσε από τους χρήστες του να ενημερώσουν την εφαρμογή. Με την ενημέρωση αυτή, οι συσκευές των θυμάτων μολύνονταν με το NotPetya. Οι δράστες με άγνωστο τρόπο απέκτησαν προνόμια διαχειριστή σε έναν από τους διακομιστές της M.E.Doc ώστε να μπορέσουν να παρέμβουν στην λειτουργία ενημέρωσης [46]. Σύμφωνα με την Talos [48], ήδη από τις 24 Απριλίου του 2017 κυκλοφόρησε ενημέρωση που περιείχε κακόβουλο κώδικα.

Κακόβουλο λογισμικό – μέθοδοι

Το NotPetya συνδυάζει χαρακτηριστικά λυτρισμικού με την ικανότητα να διαδίδεται σε ένα δίκτυο. Εξαπλώνεται σε μηχανήματα με Windows λειτουργικό σύστημα χρησιμοποιώντας διάφορες μεθόδους διάδοσης, συμπεριλαμβανομένης της εκμετάλλευσης του EternalBlue για την τρωτότητα CVE-2017-0144 της υπηρεσίας SMB. Μετά την μόλυνση του αρχικού θύματος, το NotPetya απαριθμεί όλα τα αποθηκευμένα διαπιστευτήρια SMB για να συνδεθεί σε άλλα μηχανήματα που βρίσκονται εντός του τοπικού δικτύου, ενώ ακόμη και ενημερωμένα μηχανήματα

Windows απειλούνται να μολυνθούν. Μόλις συνδεθεί σε ένα τερματικό, εκτελούνται οι εξής κακόβουλες λειτουργίες [49]:

- Κλοπή διαπιστευτηρίων.
- Πλαστοπροσωπία Token (Token impersonation).
- Απαρίθμηση κόμβων δικτύου και εκμετάλλευση τρωτότητας μέσω EternalBlue.
- Απομακρυσμένη εκτέλεση κακόβουλου λογισμικού.
- Χειραγώγηση φυσικού δίσκου.
- Κρυπτογράφηση MFT (Master File Table).
- Κρυπτογράφηση αρχείων.
- Απενεργοποίηση συστήματος.
- Anti-forensics λειτουργίες.

Το κακόβουλο αυτό λογισμικό, λειτουργεί περισσότερο ως καταστροφικό εργαλείο παρά ως πραγματικό λυτρισμικό. Πιο συγκεκριμένα, χρησιμοποιώντας το API DeviceloControl των Windows είναι σε θέση να αποκτήσει πρόσβαση ανάγνωσης και εγγραφής στον φυσικό σκληρό δίσκο, χωρίς αλληλεπίδραση με το λειτουργικό σύστημα, έχοντας την δυνατότητα να καταστρέφει δεδομένα [47].

Παράλληλα με τις υπόλοιπες λειτουργίες, το NotPetya διέθετε και ένα “kill switch”, δηλαδή έναν μηχανισμό με τον οποίο μπορούσε να αποτραπεί η εξάπλωση του. Ειδικότερα, έλεγχε για την ύπαρξη αρχείου με όνομα “perfc.dat” ή “perfc” και εάν υπήρχε τότε σήμαινε πως το σύστημα αυτό είναι ήδη μολυσμένο και διακοπτόταν η εκτέλεση της ακολουθίας, ενώ στην περίπτωση που δεν υπήρχε τέτοιο αρχείο, τότε το κακόβουλο λογισμικό διαδιδόταν αυτο-αναπαραγόμενο στον σκληρό δίσκο του θύματος [47].

Τύπος PE

Τα αναλυθέντα δείγματα του NotPetya είναι αρχεία 32-bit τύπου PE DLL των Windows με αρχικό όνομα “perfc.dat” [47], [49].

Επικοινωνία με C&C / C2 servers

Σύμφωνα με έρευνες της ESET [50], δεν χρησιμοποιούνται εξωτερικοί διακομιστές ως C2, αλλά αξιοποιούνται τα τακτικά αιτήματα ελέγχου ενημερώσεων του λογισμικού M.E.Doc προς τον επίσημο διακομιστή M.E.Doc upd.me-doc.com[.]ua. Οι πληροφορίες που συλλέγονται αποστέλλονται σε cookies.

Τεχνικές αποφυγής ανίχνευσης

Το NotPetya απαριθμεί όλες τις διεργασίες που εκτελούνται στο μηχάνημα του θύματος, αναζητώντας τρία συγκεκριμένα προϊόντα προστασίας και ανίχνευσης ιών: Kaspersky, Symantec

και Norton Security. Ανάλογα με τα προϊόντα που βρέθηκαν, το NotPetya ακολουθεί διαφορετικές διαδρομές εκτέλεσης. Στην περίπτωση που δεν υπάρχει κανένα από τα 3 προϊόντα antivirus, τότε το κακόβουλο λογισμικό τρέχει σε πλήρη λειτουργία ενεργοποιώντας τεχνικές anti-forensics, όπως η εκκαθάριση των αρχείων καταγραφής συμβάντων κ.α. Στην περίπτωση που ανιχνεύτηκε μόνο προϊόν της εταιρείας Kaspersky, εκτελείται διαφορετική διαδρομή στην οποία οι τεχνικές anti-forensics δεν συμβαίνουν [47].

Κρυπτογράφηση

Οι δράστες χρησιμοποίησαν AES-128 για να κρυπτογραφήσουν όλα τα αρχεία του συστήματος και κρυπτογράφηση Salsa20 για το MFT (Master File Table) [49]. Επίσης, αξιοποιήθηκαν τροποποιημένοι XOR αλγόριθμοι για την κρυπτογράφηση των ονομάτων των εκτελέσιμων αρχείων του NotPetya [47].

Στόχος επίθεσης

Η κυβερνοεπίθεση σκόπευε στην προσωρινή ή μόνιμη απώλεια ευαίσθητων πληροφοριών, στην διακοπή επιχειρησιακών λειτουργιών και σε οικονομικές απώλειες [51].

Απόδοση ευθυνών

Η κυβέρνηση των ΗΠΑ απέδωσε την ευθύνη της καταστροφικής αυτής κυβερνοεπίθεσης σε κυβερνητικούς παράγοντες της Ρωσίας [51].

3.1.8 Olympic Destroyer

Περιγραφή επίθεσης

Τον Φεβρουάριο του 2018, σύμφωνα με την Guardian [52], οι Ολυμπιακοί αγώνες που διεξάχθηκαν στο Pyeongchang της Νότιας Κορέας χτυπήθηκαν. Λίγο πριν την τελετή, η επίσημη ιστοσελίδα Pyeongchang 2018 σταμάτησε να λειτουργεί με αποτέλεσμα οι χρήστες να μην μπορούν να αποκτήσουν πρόσβαση σε πληροφορίες και να αδυνατούν να εκτυπώσουν τα εισιτήρια τους. Ταυτόχρονα, σταμάτησε να λειτουργεί το wifi και οι τηλεοράσεις του Ολυμπιακού σταδίου, καθώς και το διαδίκτυο του κεντρικού κέντρου Τύπου. Η πλήρης αποκατάσταση των συστημάτων ολοκληρώθηκε περίπου 12 ώρες από την στιγμή της επίθεσης. Το κακόβουλο λογισμικό που χρησιμοποιήθηκε για την κυβερνοεπίθεση αυτή, ονομάστηκε ‘Olympic Destroyer’.

Αρχική μόλυνση – προσβολή

Από τον Δεκέμβριο του 2017 έως τον Φεβρουάριο του 2018, οι δράστες μέσω spear-phishing campaigns και κακόβουλων εφαρμογών για κινητά τηλέφωνα κατάφεραν να προσβάλλουν υπολογιστές και συστήματα που σχετιζόντουσαν με την διοργάνωση των αγώνων [53]. Ειδικότερα, ανακαλύφθηκαν [54] spear phishing emails τα οποία σχετίζονταν με τους αγώνες και περιείχαν αρχεία MS Office με κακόβουλο περιεχόμενο.

Κακόβουλο λογισμικό – μέθοδοι

Το Olympic Destroyer είναι ένα κακόβουλο λογισμικό που στοχεύει Windows μηχανήματα και λειτουργεί φορτώνοντας αρχεία στο σύστημα-στόχο για την κλοπή δεδομένων, την μετάδοση του στο δίκτυο και για την καταστροφή και διαγραφή δεδομένων [55].

Σύμφωνα με την εταιρεία κυβερνοασφάλειας Talos [56], σε πρώτη φάση, όταν εκτελεστεί, ξεκινάνε διαδικασίες κλοπής διαπιστευτηρίων και κωδικών πρόσβασης που είναι αποθηκευμένοι στους περιηγητές Internet Explorer, Chrome και Firefox και ταυτόχρονα ξεκινάει μια διαδικασία ανακάλυψης δικτύου (Network discovery). Ειδικότερα, ελέγχεται το ARP (Address Resolution Protocol) table μέσω του νόμιμου Windows API GetIPNetTable και του Windows Management Instrumentation (WMI). Αφού ολοκληρωθούν αυτές οι δύο λειτουργίες, το Olympic Destroyer διαδίδεται αυτοαναπαραγώμενο στο υπόλοιπο δίκτυο χρησιμοποιώντας τα αξιόπιστα και νόμιμα εργαλεία PsExec και WMI.

Παράλληλα, το κακόβουλο λογισμικό περιέχει ένα wiper module το οποίο είναι υπεύθυνο για την καταστροφή δεδομένων. Το module αυτό, ενεργοποιείται με την εκτέλεση του Olympic Destroyer και αξιοποιεί το command prompt (cmd.exe) για να εκκινήσει το vssadmin και να διαγράψει τα shadow copies του συστήματος. Στην συνέχεια, διαγράφει το WBAdmin.exe που χρησιμοποιείται για την διαχείριση ρυθμίσεων αντιγράφων ασφαλείας και την ανάκτηση αρχείων. Τέλος, εμποδίζει την κονσόλα ανάκτησης των Windows να προσπαθήσει να επιδιορθώσει και να ανακτήσει τα αρχεία του μολυσμένου συστήματος και διαγράφει το αρχείο καταγραφής συμβάντων των Windows System & Security [54], [55], [56].

Τύπος PE

Ο τύπος αρχείων PE που εκμεταλλεύεται το κακόβουλο λογισμικό και οι επιτιθέμενοι σε αυτή την επίθεση είναι EXE.

Επικοινωνία με C&C / C2 servers

Ανακαλύφθηκε κακόβουλη κίνηση προς έναν C2 server με διεύθυνση IP 131.25.*.* ο οποίος βρίσκεται στην Αργεντινή. Οι συνδέσεις προς αυτόν τον διακομιστή γινόντουσαν μέσω των θυρών: 443, 4443, 8080, 8081, 8443, 8880 [54].

Τεχνικές αποφυγής ανίχνευσης

Οι επιτιθέμενοι χρησιμοποιούν πολλαπλές τεχνικές για να αποφύγουν την ανίχνευση του κακόβουλου λογισμικού. Αναλυτικότερα, αξιοποιούν νόμιμα και έμπιστα εργαλεία των Windows, αλλάζουν τα ονόματα των κακόβουλων αρχείων που φορτώνουν τα modules και διαγράφουν τα αρχεία καταγραφής συμβάντων.

Κρυπτογράφηση

Οι επιτιθέμενοι χρησιμοποίησαν τους αλγορίθμους κρυπτογράφησης RC4 & BASE64 [54].

Στόχος επίθεσης

Πρωταρχικός στόχος της επίθεσης ήταν η διατάραξη της διοργάνωσης και η καταστροφή αρχείων. Πιστεύεται πως η επιχείρηση αυτή δεν επιδίωκε οικονομικά οφέλη ή συλλογή πληροφοριών, αλλά απώτερος σκοπός της ήταν να προκληθεί χάος [53].

Απόδοση ευθυνών

Σύμφωνα με έρευνες [54], [57], οι επιτιθέμενοι σκοπίμως χρησιμοποίησαν false flags εντός του κακόβουλου λογισμικού και των μεθόδων που χρησιμοποίησαν, προκειμένου να αποδοθεί η επίθεση στην γνωστή ομάδα APT Lazarus. Ωστόσο, το Ηνωμένο Βασίλειο [58] και οι Ηνωμένες Πολιτείες Αμερικής [59] αποδίδουν τις ευθύνες στην GRU (Main Directorate of the General Staff of the Armed Forces of the Russian Federation).

3.1.9 Operation ShadowHammer

Περιγραφή επίθεσης

Το Ιανουάριο του 2019, το Kaspersky Lab ανακάλυψε [60] μια προηγμένη επίθεση supply chain που αφορούσε το ASUS Live Update Utility. Οι επιτιθέμενοι παραποίησαν παλαιότερες εκδόσεις λογισμικού της ASUS, εισάγοντας τον δικό τους κακόβουλο κώδικα. Η επίθεση πραγματοποιήθηκε μεταξύ Ιουνίου και Νοεμβρίου του 2018 και εκτιμάται πως επηρεάστηκαν περισσότεροι από ένα εκατομμύριο χρήστες παγκοσμίως. Το ASUS Live Update Utility είναι για ένα προεγκατεστημένο βοηθητικό πρόγραμμα των περισσοτέρων νέων υπολογιστών ASUS, για αυτόματες ενημερώσεις BIOS, UEFI, drivers και εφαρμογών.

Αρχική μόλυνση – προσβολή

Το πώς αρχικά μολύνθηκαν τα συστήματα της ASUS παραμένει ακόμη άγνωστο.

Κακόβουλο λογισμικό – μέθοδοι

Σύμφωνα με έρευνα της Kaspersky [61], το κακόβουλο αρχείο που μόλυνε τους υπολογιστές των πελατών της ASUS αποτελούσε μια trojanized έκδοση του ASUS Live Updater file και είχε το όνομα "setup.exe". Η υποτιθέμενη λειτουργία του ήταν η ενημέρωση του ίδιου του εργαλείου ενημέρωσης, ενώ στην πραγματικότητα αποτελούσε ένα αρχείο ενημέρωσης ASUS που κυκλοφόρησε το 2015, στο οποίο είχε προστεθεί ο κακόβουλος κώδικας. Η χρήση μιας παλιάς έκδοσης του λογισμικού που περιείχε ψηφιακή υπογραφή της ASUSTek Computer Inc σημαίνει πως οι επιτιθέμενοι είχαν πρόσβαση στον διακομιστή όπου η ASUS υπέγραφε αρχεία, αλλά όχι στον διακομιστή κατασκευής νέων αρχείων [62].

Οι επιτιθέμενοι αντικατέστησαν την συνάρτηση WinMain του αρχικού δυαδικού αρχείου με μια νέα κακόβουλη συνάρτηση κατά την οποία αντιγράφεται μια κερκόπορτα στο heap memory και σε άλλη στιγμή χρησιμοποιείται ένα hardcoded offset για την ενεργοποίηση της. Το κακόβουλο εκτελέσιμο PE (Portable Executable) δημιουργήθηκε με το εργαλείο Microsoft Visual C++ 2010.

Επίσης, ερευνητές της Kaspersky ανακάλυψαν πως ο κώδικας κάθε κερκόπορτας, περιείχε έναν πίνακα με hardcoded MAC addresses. Μόλις ενεργοποιούταν η κερκόπορτα στο μηχάνημα του θύματος, ξεκινούσε μια διαδικασία επαλήθευσης της διεύθυνσης MAC του σε σχέση με τον πίνακα. Εάν η διεύθυνση MAC ταίριαζε με μια από τις εγγραφές του πίνακα, το κακόβουλο λογισμικό κατέβαζε το επόμενο στάδιο του κακόβουλου κώδικα, ενώ σε διαφορετική περίπτωση έμενε σε κατάσταση αδράνειας χωρίς να εκτελέσει παράνομες ενέργειες. Συνολικά, οι ειδικοί κατάφεραν να εντοπίσουν περισσότερες από 600 διευθύνσεις MAC [63].

Τύπος PE

Ο τύπος αρχείων PE που εκμεταλλεύεται το κακόβουλο λογισμικό και οι επιτιθέμενοι σε αυτή την επίθεση είναι EXE.

Επικοινωνία με C&C / C2 servers

Οι ερευνητές της Kaspersky ανακάλυψαν 6 διευθύνσεις IP των C2 διακομιστών.

Τεχνικές αποφυγής ανίχνευσης

Η επαλήθευση ψηφιακής υπογραφής είναι μια μέθοδος που χρησιμοποιείται για τον έλεγχο ακεραιότητας αξιόπιστων εκτελέσιμων αρχείων. Στην συγκεκριμένη επίθεση οι επιτιθέμενοι κατάφεραν να υπογράφουν ψηφιακά τον κώδικα τους με πιστοποιητικό μεγάλου προμηθευτή. Ειδικότερα, 2 από τα πιστοποιητικά που χρησιμοποιήθηκαν έχουν χρησιμοποιηθεί στο παρελθόν για την υπογραφή τουλάχιστον 3000 νόμιμων αρχείων ASUS, γεγονός που τους έκανε ως επί το πλείστον αόρατους στην συντριπτική πλειοψηφία των προϊόντων ασφάλειας [61], [63].

Κρυπτογράφηση

Εντός του κώδικα του κακόβουλου λογισμικού αξιοποιήθηκε ένας προσαρμοσμένος block-chaining XOR αλγόριθμος [61].

Στόχος επίθεσης

Με την επίθεση αυτή, οι επιτιθέμενοι κατάφεραν να μολύνουν μια μεγάλη ομάδα χρηστών. Για να εντοπίσουν τους πραγματικούς τους στόχους, το κακόβουλο λογισμικό διέθετε λίστες με MAC διευθύνσεις και έλεγχε εάν η διεύθυνση MAC των adapter των δικτύων των θυμάτων, ταίριαζε με κάποια διεύθυνση της λίστας στόχων τους. Παρ ’όλα αυτά, παραμένουν άγνωστα τα κίνητρα και τα τελικά θύματα αυτής της επίθεσης [61].

Απόδοση ευθυνών

Οι ερευνητές δεν απέδωσαν την επίθεση σε καμία ομάδα APT [62]. Όμως, έχουν βρεθεί ορισμένα στοιχεία [61] που συνδέουν την επιχείρηση ShadowHammer με το περιστατικό ShadowPad το 2017, το οποίο η Microsoft αποδίδει [64] στην ομάδα APT BARIUM.

3.1.10 Operation SolarWinds

Περιγραφή επίθεσης

Σύμφωνα με το US Senate Republican Policy Committee [65] η επιχείρηση SolarWinds είναι μια από τις πιο εξελιγμένες και μεγάλης κλίμακας κυβερνοεπιθέσεις που έχουν εντοπιστεί ποτέ. Κατηγοριοποιείται ως digital supply chain attack κατά την οποία οι επιτιθέμενοι εισάγουν κακόβουλο κώδικα σε αξιόπιστο λογισμικό τρίτου, μολύνοντας όλους τους πελάτες του. Η εταιρεία-στόχος SolarWinds, από την οποία πήρε και το όνομα της η επίθεση, παρέχει λογισμικό και υπηρεσίες διαχείρισης υποδομών τεχνολογίας πληροφοριών μεγάλης κλίμακας σε επιχειρήσεις και κυβερνητικούς οργανισμούς.

Τον Δεκέμβριο του 2020, η εταιρεία κυβερνοασφάλειας FireEye, αποκάλυψε την επιχείρηση SolarWinds κατά την οποία οι δράστες εισήγαγαν κακόβουλο κώδικα στην ενημερωμένη πλατφόρμα διαχείρισης δικτύων Orion της SolarWinds. Η πρώτη παραβίαση των συστημάτων της SolarWinds συνέβη τον Σεπτέμβριο του 2019 και μετά από αρκετούς μήνες που οι δράστες παρέμειναν απαρατήρητοι, τον Φεβρουάριο του 2020 εισήγαγαν την κερκόπορτα στο λογισμικό της εταιρείας με αποτέλεσμα κατά τους μήνες Μάρτιο και Απρίλιο του 2020 το κακόβουλο λογισμικό να μολύνει πολλαπλές επιχειρήσεις και οργανισμούς.

Περίπου 18.000 πελάτες της SolarWinds χτυπήθηκαν από το κακόβουλο λογισμικό, συμπεριλαμβανομένων και κυβερνητικών φορέων, όπως τα υπουργεία Εμπορίου, Άμυνας, Ενέργειας, Δικαιοσύνης, Εργασίας, Εξωτερικών, Οικονομικών, καθώς και η υπηρεσία Homeland Security και τα Εθνικά Ινστιτούτα υγείας. Η συνολική ζημιά υπολογίζεται ότι έφτασε έως και τα 100 δισεκατομμύρια δολάρια [66].

Αρχική μόλυνση – προσβολή

Ο αρχικός τρόπος μόλυνσης των συστημάτων της SolarWinds παραμένει άγνωστος.

Κακόβουλο λογισμικό – μέθοδοι

Σύμφωνα με την FireEye [67], [68], το SolarWinds.Orion.Core.BusinessLayer.dll είναι ένα ψηφιακά υπογεγραμμένο στοιχείο του λογισμικού Orion, το οποίο περιέχει μια κερκόπορτα. Η trojanized έκδοση αυτού του plugin του λογισμικού ονομάστηκε SUNBURST. Το αρχείο ενημέρωσης αποτελεί ένα τυπικό αρχείο Windows Installer Patch και μόλις εκτελεστεί το κακόβουλο αρχείο τύπου PE DLL θα φορτωθεί από το νόμιμο SolarWinds.BusinessLayerHost(x64).exe.

Μετά από μια αρχική περίοδο αδράνειας έως και 2 εβδομάδων, το SUNBUSRT μπορεί να ανακτήσει και να εκτελέσει τις εξής εντολές:

- Μεταφορά αρχείων.
- Εκτέλεση διαδικασιών και αρχείων.
- Σκιαγράφηση συστήματος.
- Επανεκκίνηση συστήματος.
- Απενεργοποίηση υπηρεσιών συστήματος.

Επιπροσθέτως, εντός των διαφορετικών payloads που χρησιμοποιούσε το SUNBURST, ανακαλύφθηκε και το κακόβουλο λογισμικό TEARDROP, το οποίο πιστεύεται πως αξιοποιήθηκε για την εκτέλεση ενός προσαρμοσμένου Cobalt Strike beacon.

Τέλος, το SUNBURST διέθετε και ένα “kill switch” το οποίο προκαλούσε την απενεργοποίηση του λογισμικού και των λειτουργιών του. Ανακαλύφθηκαν ορισμένα DNS responses που είχαν αυτήν την δυνατότητα.

Τύπος PE

Ο τύπος αρχείων PE που εκμεταλλεύεται το κακόβουλο λογισμικό και οι επιτιθέμενοι σε αυτή την επίθεση είναι DLL.

Επικοινωνία με C&C / C2 servers

Το SUNBURST χρησιμοποιεί έναν ενδιάμεσο συντονιστή C2 για να ανακτήσει τον τελικό διακομιστή C2. Ο συντονιστής υλοποιείται ως authoritative DNS server για κάποιο domain και η λειτουργία του είναι να ανακατευθύνει το κακόβουλο λογισμικό στον τελικό διακομιστή C2 μέσω εγγραφών DNS CNAME. Κατά την επικοινωνία με τον συντονιστή C2, η κερκόπορτα παράγει συνεχώς domains μέσω του DGA (Domain Generation Algorithm) και καθυστερεί την εκτέλεση για τυχαία χρονικά διαστήματα μεταξύ της δημιουργίας των domains. Η καθυστέρηση αυτή, μπορεί να φτάσει έως και τις 9 ώρες.

Η κερκόπορτα χρησιμοποιεί ένα πρωτόκολλο C2 2 τμημάτων που αξιοποιεί τα πρωτόκολλα DNS και HTTP. Στην «παθητική» λειτουργία, η κερκόπορτα επικοινωνεί με τον ενδιάμεσο συντονιστή C2 μέσω DNS και λαμβάνει ενημερώσεις υψηλού επιπέδου για την κατάσταση της. Όταν βρίσκεται η κερκόπορτα σε «ενεργή» λειτουργία, επικοινωνεί μέσω HTTP με τον τελικό C2 και λαμβάνει τις κακόβουλες εντολές.

Ο διακομιστής C2 επίσης χρησιμοποιεί στεγανογραφία για την απόκρυψη δεδομένων μέσα στο σώμα μηνυμάτων απόκρισης HTTP και προσπαθεί να εμφανιστεί ως XML.

Τεχνικές αποφυγής ανίχνευσης

Το κακόβουλο λογισμικό μεταμφιέζει την κυκλοφορία δικτύου του ως πρωτόκολλο Orion Improvement Program (OIP) και αποθηκεύει δεδομένα σε νόμιμα αρχεία ρυθμίσεων, επιτρέποντας του να αναμειγνύεται με την νόμιμη δραστηριότητα της SolarWinds. Παράλληλα, πραγματοποιεί πολυάριθμους ελέγχους πριν προχωρήσει σε κακόβουλη δραστηριότητα για διασφαλίσει πως δεν υπάρχουν εργαλεία ανάλυσης και λογισμικά AV (anti-virus). Επιπρόσθετα, αξιοποιούνται obfuscated blocklists για την αναγνώριση λογισμικών ασφάλειας και τεχνικές anti-sandboxing.

Κρυπτογράφηση

Οι επιτιθέμενοι χρησιμοποίησαν πολλαπλές παραλλαγές του αλγορίθμου XOR, καθώς και BASE64.

Στόχος επίθεσης

Αρχικές αναλύσεις, έδειχναν πως η επίθεση αυτή δεν είχε στόχο την διατάραξη και καταστροφή δικτύων και συστημάτων, αλλά μάλλον την συλλογή πληροφοριών. Δεδομένων των μεθόδων που χρησιμοποίησαν οι επιτιθέμενοι για να αποφύγουν την ανίχνευση τους, η κυβερνοεπίθεση φαίνεται να σχεδιάστηκε για να μολύνει πολλαπλά δίκτυα και για να συλλέξει πληροφορίες και δεδομένα [69], [70].

Απόδοση ευθυνών

Σύμφωνα με το FBI, τον CISA και την NSA [70], για την κυβερνοεπίθεση SolarWinds ευθύνεται ένας φορέας προηγμένης επίμονης απειλής (APT) Ρωσικής προέλευσης.

3.1.11 Operation North Star

Περιγραφή επίθεσης

Το καλοκαίρι του 2020, η εταιρεία McAfee ανακάλυψε [71] μια επίμονη εκστρατεία κυβερνο-κατασκοπείας με στόχο άτομα υψηλής σημασίας που έχουν στην κατοχή τους υψηλής αξίας πνευματική ιδιοκτησία του αμυντικού τομέα και άλλες εμπιστευτικές πληροφορίες. Η επιχείρηση North Star κατά την διάρκεια των πρώτων μηνών του 2020 εκμεταλλεύτηκε ιστότοπους κοινωνικής δικτύωσης και πολλαπλές τεχνικές για να πλησιάσει τα προσεκτικά επιλεγμένα θύματα του. Συγκεκριμένα, επιθέσεις δέχτηκαν οργανισμοί στην Νότια Κορέα, Αυστραλία, Ινδία, Ισραήλ και Ρωσία, συμπεριλαμβανομένων και αμυντικών εργολάβων με έδρα την Ινδία και τη Ρωσία.

Αρχική μόλυνση – προσβολή

Σύμφωνα με την McAfee [72], οι επιτιθέμενοι ανέπτυξαν ξεχωριστό και προσαρμοσμένο περιεχόμενο για το κάθε θύμα και το προσέγγιζαν μέσω ιστότοπων κοινωνικής δικτύωσης όπως το LinkedIn. Χρησιμοποιήθηκε νόμιμο περιεχόμενο πρόσληψης θέσεων εργασίας από δημοφιλείς ιστοσελίδες μεγάλων εργολάβων του αμυντικού και αεροδιαστημικού τομέα των ΗΠΑ με σκοπό να δελεάσουν τους ενδιαφερόμενους-στόχους να ανοίξουν τα επισυναπτόμενα spear phishing emails. Τα μηνύματα ηλεκτρονικού ταχυδρομείου περιείχαν κακόβουλα έγγραφα Word τα οποία κατέβαζαν εξωτερικά Word templates με κακόβουλες μακροεντολές. Η τεχνική αυτή ονομάζεται “template injection attack”. Η περίοδος αποστολής των εγγράφων στα θύματα ήταν από τις 31 Μαρτίου έως τις 18 Μάϊου 2020.

Κακόβουλο λογισμικό – μέθοδοι

Τα αρχεία DOTM (Office template filetype) είναι υπεύθυνα για την φόρτωση των κακόβουλων αρχείων τύπου PE DLL στον υπολογιστή του θύματος-στόχου για την συλλογή πληροφοριών για τον δίσκο και τον ελεύθερο του χώρο, το όνομα του υπολογιστή και των χρηστών, καθώς και πληροφορίες για τις διεργασίες του συστήματος. Τα DOTM αρχεία υπάρχουν σε απομακρυσμένους διακομιστές που έχουν παραβιάσει οι επιτιθέμενοι και το έγγραφο Word περιέχει ενσωματωμένο έναν σύνδεσμο που παραπέμπει στην θέση αυτού του αρχείου. Όταν το θύμα ανοίξει το έγγραφο Word θα φορτωθεί το απομακρυσμένο αρχείο DOTM που περιέχει έναν κώδικα μακροεντολών Visual Basic και θα φορτώσει τα κακόβουλα αρχεία τύπου PE DLL.

Στην συνέχεια, χρησιμοποιήθηκε ένα σύνολο κανόνων λογικής για να αξιολογηθούν τα δεδομένα που συλλέχθηκαν με σκοπό να παρθεί η απόφαση για το εάν θα εγκατασταθεί ένα νέο implant με όνομα “Torisma”. Το Torisma, αποτελεί ένα προηγουμένως άγνωστο, ειδικά σχεδιασμένο implant που εξειδικεύεται στην παρακολούθηση συστημάτων υψηλής σημασίας. Αναλόγως με τα προφίλ των συστημάτων των θυμάτων-στόχων, το Torisma εκτελεί διαφορετικές ενέργειες παρακολούθησης και εκτελεί payloads βασισμένα στα παρατηρούμενα συμβάντα [73].

Τύπος PE

Ο τύπος αρχείων PE που εκμεταλλεύεται το κακόβουλο λογισμικό και οι επιτιθέμενοι σε αυτή την επίθεση είναι DLL.

Επικοινωνία με C&C / C2 servers

Χρησιμοποιήθηκαν νόμιμα domains για την φιλοξενία των C2 διακομιστών συμπεριλαμβανομένων και domains με βάση την Ιταλία και τις ΗΠΑ. Με αυτόν τον τρόπο πιθανώς παρακάμφθηκαν διάφοροι έλεγχοι ασφαλείας, καθώς οι περισσότεροι οργανισμοί δεν μπλοκάρουν αξιόπιστους ιστότοπους [71], [73].

Τεχνικές αποφυγής ανίχνευσης

Οι επιτιθέμενοι χρησιμοποίησαν πολλαπλές τεχνικές για να αποφύγουν να εντοπιστούν. Μια από αυτές αποτελούσε η ίδια η αρχική μόλυνση, κατά την οποία με template injection attack παρακάμπτονται μέθοδοι στατικής ανάλυσης κακόβουλων εγγράφων, καθώς οι μακροεντολές είναι ενσωματωμένες στο κατεβασμένο template. Επίσης, οι επιτιθέμενοι επιχείρησαν να καλύψουν την κακόβουλη δικτυακή δραστηριότητα τους, μιμούμενοι τον ίδιο User-Agent του συστήματος. Μέσω της χρήσης του API ObtainUserAgentString των Windows, κατάφεραν να αποφύγουν τα συστήματα ανίχνευσης, με αποτέλεσμα η εξερχόμενη κυκλοφορία να μην φαίνεται ύποπτη [71].

Κρυπτογράφηση

Εντός των αρχείων τύπου PE DLL και του Torisma χρησιμοποιήθηκαν πολλαπλές κρυπτογραφικές τεχνικές όπως: BASE64, AES, VEST algorithm, XOR.

Στόχος επίθεσης

Οι ερευνητές που μελέτησαν την επιχείρηση, κατέληξαν στο συμπέρασμα πως στόχος της επίθεσης ήταν η δημιουργία μιας μακροπρόθεσμης, επίμονης εκστρατείας κατασκοπείας σημαντικών ατόμων από χώρες-κλειδιά σε όλο τον κόσμο.

Απόδοση ευθυνών

Σύμφωνα με την McAfee δεν είναι δυνατή η απόδοση της ευθύνης σε μια συγκεκριμένη ομάδα μόνο. Κατά την διάρκεια της έρευνας βρέθηκαν στοιχεία που συνδέουν την επιχείρηση North Star με μια εκστρατεία το 2019 που αποδόθηκε στην ομάδα Hidden Cobra. Η ομάδα αυτή, χρησιμοποιείται από τους ειδικούς κυβερνοασφάλειας για να αναφερθούν σε ομάδες που συνδέονται και υπηρετούν συμφέροντα της κυβέρνησης της Βόρειας Κορέας και αποτελείται από τις ομάδες Lazarus, Kimsuky, KONNI και APT37.

3.1.12 Operation Spalax

Όλα τα δεδομένα και πληροφορίες που αξιοποιήθηκαν για την ανάλυση της επίθεσης, πάρθηκαν από την έρευνα της ESET [74].

Περιγραφή επίθεσης

Κατά την διάρκεια του 2020, η εταιρεία κυβερνοασφάλειας ESET παρατήρησε πολλαπλές επιθέσεις σε Κολομβιανούς φορείς. Οι επιθέσεις επικεντρώνονται τόσο σε κυβερνητικά ιδρύματα όσο και σε ιδιωτικές εταιρείες, οι τομείς που επηρεάστηκαν περισσότερο περιλαμβάνουν αυτούς της ενέργειας και της μεταλλουργίας. Οι δράστες βασίστηκαν στην χρήση trojan για την απομακρυσμένη πρόσβαση στα συστήματα των θυμάτων με πιθανό στόχο την κατασκοπεία και την συλλογή πληροφοριών.

Αρχική μόλυνση – προσβολή

Οι επιτιθέμενοι με spear phishing μηνύματα ηλεκτρονικού ταχυδρομείου προσέγγιζαν τους στόχους τους με σκοπό να τους πείσουν να κατεβάσουν τα κακόβουλα αρχεία. Στις περισσότερες περιπτώσεις τα μηνύματα περιείχαν ένα έγγραφο PDF, το οποίο παρείχε στον παραλήπτη έναν σύνδεσμο προς νόμιμες υπηρεσίες φιλοξενίας αρχείων, όπως το OneDrive ή το MediaFire, οι οποίες φιλοξενούσαν ένα αρχείο RAR. Ο στόχος έπρεπε να κατεβάσει το αρχείο

RAR, να εξάγει χειροκίνητα το κακόβουλο εκτελέσιμο που βρισκόταν εντός του, και τέλος, να το εκτελέσει για να μολυνθεί το σύστημα του.

Ειδικότερα, τα μηνύματα ηλεκτρονικού ταχυδρομείου που βρέθηκαν αφορούσαν θέματα όπως ειδοποιήσεις σχετικά με παράβαση οδήγησης, υποχρεωτική εξέταση COVID-19, συμμετοχή σε δικαστική ακρόαση, έρευνα κατά του παραλήπτη για κατάχρηση δημοσιών πόρων και σχετικά με εμπάργκο τραπεζικών λογαριασμών του θύματος.

Κακόβουλο λογισμικό – μέθοδοι

Το αρχικό αρχείο dropper που εισάγεται στο σύστημα του στόχου περιέχει το κρυπτογραφημένο RAT (Remote Access Trojan) με όνομα Bonehead και ένα αρχείο τύπου PE DLL με όνομα ShoonCataclysm.dll που αποκρυπτογραφεί και εκτελεί το trojan. Το payload που χρησιμοποιήθηκε στις περισσότερες περιπτώσεις ήταν το RemcosRAT, αλλά βρέθηκαν και επιθέσεις που αξιοποίησαν το njRAT και το AsyncRAT. Αυτά τα payloads παρέχουν διάφορες δυνατότητες στους επιτιθέμενους, όπως καταγραφή οθόνης, keylogging, δυνατότητα λήψης και εκτέλεσης άλλου κακόβουλου λογισμικού, εξαγωγή δεδομένων και αρχείων και άλλα.

Επιπροσθέτως, αξίζει να σημειωθεί πως κανένα από τα παραπάνω εργαλεία απομακρυσμένης πρόσβασης δεν αναπτύχθηκε από τους επιτιθέμενους. Το RemcosRAT μπορεί να αγοραστεί στο διαδίκτυο με νόμιμες διαδικασίες, το njRAT μπορεί να βρεθεί σε forums και τέλος το AsyncRAT αποτελεί λογισμικό ανοιχτού κώδικα.

Τύπος PE

Ο τύπος αρχείων PE που εκμεταλλεύεται το κακόβουλο λογισμικό και οι επιτιθέμενοι σε αυτή την επίθεση είναι EXE και DLL.

Επικοινωνία με C&C / C2 servers

Οι ερευνητές κατά το δεύτερο εξάμηνο του 2020 ανακάλυψαν περίπου 70 διαφορετικά domains που χρησιμοποιήθηκαν για C2 και αντιστοιχούν σε 24 διευθύνσεις IP. Ταυτοποιήθηκαν ακόμα 160 domains από το 2019 τα οποία αντιστοιχούν σε επιπλέον 40 διευθύνσεις IP. Επιπροσθέτως παρατηρήθηκε πως σχεδόν όλες οι διευθύνσεις IP που βρέθηκαν βρίσκονταν στην Κολομβία. Παράλληλα, τα RATs που χρησιμοποιήθηκαν, επικοινωνούν με τους C2 διακομιστές μέσω συνδέσεων TCP και αναλόγως με το RAT που χρησιμοποιήθηκε, αλλάζουν και οι θύρες επικοινωνίας.

Τεχνικές αποφυγής ανίχνευσης

Οι επιτιθέμενοι χρησιμοποίησαν πολλαπλές τεχνικές για να αποφύγουν την ανίχνευση του κακόβουλου λογισμικού, συγκεκριμένα:

- Χρησιμοποίησαν obfuscated αρχεία.
- Αξιοποίησαν τεχνικές στεγανογραφίας.
- Ενσωμάτωσαν τα κακόβουλα payloads σε νόμιμες και αξιόπιστες διεργασίες όπως η RegAsm.exe, MSBuild.exe και άλλες.
- Εκτελούν ελέγχους anti-analysis για τον εντοπισμό εργαλείων ανίχνευσης και sandboxes.

Κρυπτογράφηση

Κατά κύριο λόγο, οι επιτιθέμενοι χρησιμοποιούσαν αλγορίθμους βασισμένους στην πράξη XOR για την κρυπτογράφηση στοιχείων του λογισμικού, ενώ για την επικοινωνία με τους C2 servers χρησιμοποιήθηκαν RC4 και BASE64.

Στόχος επίθεσης

Η επιχείρηση Spalax αποτελεί μια εκστρατεία κατασκοπείας οντοτήτων Κολομβιανής προέλευσης. Αυτό φαίνεται από τις λειτουργίες και δυνατότητες του κακόβουλου λογισμικού, καθώς κύριος στόχος τους ήταν η συλλογή πληροφοριών και η παρακολούθηση του θύματος.

Απόδοση ευθυνών

Σύμφωνα με τους ερευνητές της ESET, οι επιθέσεις που καταγράφηκαν κατά την διάρκεια του 2020 έχουν κάποια κοινά στοιχεία με παλαιότερες επιθέσεις από ομάδες που στόχευαν την Κολομβία, αλλά ταυτόχρονα διαφέρουν σε πολλά σημεία, καθιστώντας την απόδοση δύσκολη.

3.1.13 PseudoManuscrypt

Όλα τα δεδομένα και πληροφορίες που αξιοποιήθηκαν για την ανάλυση της επίθεσης, πάρθηκαν από την έρευνα της Kaspersky [75].

Περιγραφή επίθεσης

Τον Ιούνιο του 2021, ερευνητές της Kaspersky ανακάλυψαν μια σειρά επιθέσεων με στόχο οργανισμούς σε όλο τον κόσμο, συμπεριλαμβανομένων κυβερνητικών οργανισμών και βιομηχανικών επιχειρήσεων. Αρχικά, το κακόβουλο λογισμικό που χρησιμοποιήθηκε εντοπίστηκε από λύσεις προστασίας που εξειδικεύονται στην ανίχνευση δραστηριοτήτων της ομάδας APT

Lazarus, καθώς ο loader του λογισμικού παρουσίαζε πολλαπλές ομοιότητες με το γνωστό κακόβουλο λογισμικό Manuscrypt που χρησιμοποιείται έντονα από την Lazarus. Όμως, η ομάδα αυτή δεν είχε καμία σχέση με τις επιθέσεις και για αυτόν τον λόγο οι ειδικοί του έδωσαν το όνομα PseudoManuscrypt.

Κατά την περίοδο από τις 20 Ιανουαρίου έως τις 10 Νοεμβρίου 2021, προϊόντα της Kaspersky μπλόκαραν το PseudoManuscrypt σε περισσότερους από 35.000 υπολογιστές σε 195 χώρες. Σύμφωνα με τους ειδικούς, το 7,2% του συνόλου των συστημάτων που δέχτηκαν επίθεση αποτελούν μέρος βιομηχανικών συστημάτων ελέγχου (ICS) που χρησιμοποιούνται από οργανισμούς σε διάφορες βιομηχανίες, όπως η μηχανολογία, ο αυτοματισμός κτιρίων, ενέργεια, μεταποίηση, διαχείριση υδάτων κ.α.

Αρχική μόλυνση – προσβολή

Το PseudoManuscrypt εισέρχεται στο σύστημα του θύματος μέσω περίπλοκων αλυσίδων εγκατάστασης πολυάριθμων άλλων κακόβουλων αρχείων. Αυτές οι αλυσίδες ποικίλουν, αλλά όλες ξεκινούν με το θύμα να κατεβάζει κακόβουλα ψεύτικα αρχεία εγκατάστασης υποτιθέμενου πειρατικού λογισμικού. Τα αρχεία μπορούν να βρεθούν σε υψηλές θέσεις σελίδων αποτελεσμάτων των μεγαλύτερων μηχανών αναζήτησης, όπως της Google.

Κακόβουλο λογισμικό – μέθοδοι

Κατά την διάρκεια της έρευνας, εντοπίστηκαν περισσότερες από 100 διαφορετικές εκδόσεις του PseudoManuscrypt loader. Το κύριο module του PseudoManuscrypt διαθέτει εκτεταμένες και πολλαπλές λειτουργίες κατασκοπείας αναλόγως με την έκδοση του. Ειδικότερα, εμπεριέχονται οι εξής λειτουργίες:

- Keylogging.
- Κλοπή δεδομένων από το clipboard.
- Κλοπή δεδομένων σύνδεσης VPN, το κακόβουλο λογισμικό αποκτά δεδομένα των Windows που χρησιμοποιούνται για την αποθήκευση δεδομένων σχετικά με συνδέσεις VPN.
- Κλοπή δεδομένων καταγραφής συμβάντων του λειτουργικού συστήματος, με αποτέλεσμα να μπορούν οι δράστες να υποκλέψουν δεδομένα αυθεντικοποίησης RDP.
- Καταγραφή ήχου από μικρόφωνα.

Τον Ιούλιο του 2021, ανακαλύφθηκε μια νέα ανανεωμένη έκδοση του PseudoManuscrypt η οποία είχε επεκτείνει τις λειτουργιές κατασκοπείας προσθέτοντας τις εξής:

- Καταγραφή βίντεο της οθόνης του υπολογιστή.

- Κλοπή διαπιστευτηρίων γνωστών Ασιατικών εφαρμογών ανταλλαγής μηνυμάτων.
- Συλλογή πληροφοριών συστήματος.
- Συλλογή δεδομένων και πληροφοριών για την σύνδεση δικτύου.
- Απενεργοποίηση λύσεων antivirus (το λογισμικό προσπαθούσε να αποκτήσει τα κατάλληλα προνόμια με σκοπό να τερματίσει πολλαπλές διεργασίες antivirus).
- Συλλογή πληροφοριών σχετικά με διεργασίες που δέχονται συνδέσεις δικτύου σε θύρες TCP και UDP.
- Διαγραφή αρχείων του συστήματος και λήψη άλλων από απομακρυσμένο URL.
- Εκκαθάριση αρχείων καταγραφής συμβάντων εφαρμογών, ασφάλειας και συστημάτων των Windows.
- Ανακατεύθυνση χρήστη σε κακόβουλους διαδικτυακούς πόρους.

Τύπος PE

Ο τύπος αρχείων PE που εκμεταλλεύεται το κακόβουλο λογισμικό και οι επιτιθέμενοι σε αυτή την επίθεση είναι EXE.

Επικοινωνία με C&C / C2 servers

Για την επικοινωνία του PseudoManuscrypt με τους επιτιθέμενους βρέθηκαν 4 domains. Χρησιμοποιήθηκε μια συγκεκριμένη υλοποίηση του πρωτοκόλλου KCP για την σύνδεση με τους διακομιστές C2 και σύμφωνα με τους δημιουργούς του, το πρωτόκολλο είναι 10%-20% ταχύτερο από το γνωστό TCP.

Τεχνικές αποφυγής ανίχνευσης

Όπως αναφέρθηκε ήδη στην ενότητα του κακόβουλου λογισμικού, το PseudoManuscrypt απενεργοποιούσε τα antivirus και τις διεργασίες τους, καθώς περιείχε και λειτουργίες εκκαθάρισης αρχείων καταγραφής συμβάντων.

Κρυπτογράφηση

Δεν βρέθηκαν πληροφορίες σχετικά με την κρυπτογράφηση.

Στόχος επίθεσης

Οι ερευνητές, βάσει των λειτουργιών του PseudoManuscrypt και των τύπων δεδομένων και πληροφοριών που εξάγουν οι επιτιθέμενοι, συμπέραναν πως στόχος είναι μια μεγάλης κλίμακας επιχείρηση κατασκοπείας και συλλογής πληροφοριών.

Απόδοση ευθυνών

Οι ειδικοί της Kaspersky δεν έχουν αποδώσει κάπου την ευθύνη για τις επιθέσεις ακόμη, αλλά έχουν συγκεντρώσει ένα σύνολο στοιχείων που δείχνει πως οι δράστες είναι κινεζικής προέλευσης και λόγω της χρήσης μιας συγκεκριμένης βιβλιοθήκης για την αποστολή δεδομένων στον C2 διακομιστή, οι αναλυτές υποψιάζονται την κινεζική ομάδα APT41.

3.1.14 New Industroyer campaign

Περιγραφή επίθεσης

Στις 12 Απριλίου 2022, η CERT-UA και η ESET [76] ανέφεραν πως μια κυβερνοεπίθεση επηρέασε τις λειτουργίες του δικτύου ηλεκτρικής ενέργειας της Ουκρανίας. Στην επίθεση αυτή, αξιοποιήθηκαν πολλά κομμάτια κακόβουλου λογισμικού, συμπεριλαμβανομένης μιας νέας έκδοσης του γνωστού κακόβουλου λογισμικού ICS Industroyer (βλ. υποπαράγραφο 3.1.1) που αναπτύχθηκε από την Ρωσική ομάδα APT Sandworm για να προκαλέσει διακοπές ρεύματος στην Ουκρανία.

Σύμφωνα με την Mandiant [77], η επίθεση αυτή, αποτελεί την πρώτη περίπτωση κατά την οποία κώδικας που πάρθηκε από ευρέως γνωστό κακόβουλο λογισμικό που στοχεύει σε επιχειρησιακές τεχνολογίες (operational technology), επαναχρησιμοποιήθηκε εναντίον νέου θύματος. Ουσιαστικά, οι δράστες προσάρμοσαν το ίδιο εργαλείο με σκοπό να προσεγγίσουν νέους στόχους και για αυτόν τον λόγο ονομάστηκε Industroyer2 ή Industroyer v2.

Εκτός από το Industroyer2, οι επιτιθέμενοι χρησιμοποίησαν διάφορες οικογένειες καταστροφικών λογισμικών, συμπεριλαμβανομένων των CaddyWiper, ORCSHRED, SOLOSHRED και AWFULSHRED. Ειδικότερα, το CaddyWiper χρησιμοποιήθηκε κατά την διάρκεια του Μαρτίου και Απριλίου εναντίον μιας Ουκρανικής τράπεζας και κυβερνητικών οντοτήτων ενώ μια παραλλαγή του αξιοποιήθηκε σε μια επίθεση κατά ενός Ουκρανικού παρόχου ενέργειας. Τα ORCHSRED, SOLOSHRED ΚΑΙ AWFULSHRED επίσης βρέθηκαν στα συστήματα της εταιρείας παροχής ενέργειας.

Αρχική μόλυνση – προσβολή

Προς το παρόν, δεν έχει αναγνωριστεί ο τρόπος με τον οποίο οι επιτιθέμενοι παραβίασαν το αρχικό θύμα ούτε πως μετακινήθηκαν στα δίκτυα ICS [78].

Κακόβουλο λογισμικό – μέθοδοι

Για την παρακάτω ανάλυση των κακόβουλων λογισμικών που αξιοποιήθηκαν στις πρόσφατες επιθέσεις, χρησιμοποιήθηκαν δεδομένα και πληροφορίες από τις τεχνικές αναλύσεις των εταιρειών κυβερνοασφάλειας ESET [76, p. 2] *και Mandiant* [77, p. 2].

Industroyer2

Το Industroyer2 αναπτύχθηκε ως ένα ενιαίο εκτελέσιμο πρόγραμμα των Windows με όνομα 108_100.exe και εκτελέστηκε με χρήση προγραμματισμένης εργασίας (Scheduled Task) στις 8 Απριλίου 2022. Σύμφωνα με την χρονοσφραγίδα του, η σύνταξή του έγινε στις 23 Μαρτίου, γεγονός που σημαίνει πως οι επιτιθέμενοι σχεδίαζαν την επίθεση για περισσότερες από 2 εβδομάδες.

Εντός του κακόβουλου λογισμικού, εφαρμόζεται μόνο ένα πρωτόκολλο για την επικοινωνία με βιομηχανικό εξοπλισμό και πρόκειται για μια μικρή αλλαγή σε σχέση με το αρχικό Industroyer του 2016, το οποίο περιείχε πολλαπλά payloads για διαφορετικά πρωτόκολλα ICS. Επίσης, το Industroyer2 μοιράζεται αρκετές ομοιότητες στον κώδικα του, με το payload 104.dll του Industroyer, γεγονός που υποδεικνύει πως το νέο λογισμικό κατασκευάστηκε χρησιμοποιώντας τον ίδιο πηγαίο κώδικα.

Το Industroyer2 είναι γραμμένο σε C++ και υλοποιεί το πρωτόκολλο IEC-104 για την τροποποίηση της κατάστασης των απομακρυσμένων τερματικών μονάδων (RTUs). Το κακόβουλο λογισμικό αποτελεί ένα αυτοτελές εκτελέσιμο πρόγραμμα, όπου ο χειριστής του μπορεί να ρυθμίσει παραμέτρους διαμόρφωσης για να στοχεύσει συγκεκριμένους απομακρυσμένους σταθμούς, να ορίσει επιλογές εκτέλεσης και να χρησιμοποιήσει ενσωματωμένες καταχωρήσεις δεδομένων ASDU (Application Service Data Unit) για να δημιουργήσει μια συγκεκριμένη εντολή για την τροποποίηση της κατάστασης του IOA (Information Object Addresses) του στοχευμένου απομακρυσμένου σταθμού είτε σε ON είτε σε OFF με στόχο την διακοπή παροχής ρεύματος.

CaddyWiper

Σε συνδυασμό με την φόρτωση του Industroyer2 στο δίκτυο ICS, οι επιτιθέμενοι ανέπτυξαν μια νέα έκδοση του καταστροφικού λογισμικού CaddyWiper. Σύμφωνα με τους ειδικούς, είχε στόχο να επιβραδύνει την διαδικασία ανάκτησης των συστημάτων και να εμποδίσει τους χειριστές της εταιρείας ενέργειας να ανακτήσουν τον έλεγχο των κονσολών ICS. Ταυτόχρονα, κάλυπτε τα ίχνη που άφηνε το Industroyer2 και για αυτόν τον λόγο χρησιμοποιήθηκε και στα ίδια μηχανήματα που επιτιθόταν το Industroyer2.

Το CaddyWiper διαγράφει δεδομένα χρηστών και τις πληροφορίες των συνδεδεμένων σκληρών δίσκων των μηχανημάτων που μολύνει, καθιστώντας το σύστημα μη λειτουργικό και μη ανακτήσιμο.

Linux and Solaris destructive malware (ORCSHRED, SOLOSHRED, AWFULSHRED)

Επιπροσθέτως, στο δίκτυο της στοχευμένης εταιρείας παροχής ενέργειας, βρέθηκε καταστροφικό λογισμικό υπολογιστών με λειτουργικά συστήματα Linux και Solaris. Βρέθηκαν 2 συστατικά στοιχεία της επίθεσης, ένας αναπαραγωγός (worm) και ένας wiper. Όλα τα κακόβουλα λογισμικά αναπτύχθηκαν σε Bash.

Το πρώτο συστατικό της επίθεσης είναι ο αναπαραγωγός. Το αρχείο του ονομαζόταν sc.sh και στόχος αυτού του bash script ήταν να ξεκινήσει μια προγραμματισμένη εργασία για την εκκίνηση του κακόβουλου wiper μια συγκεκριμένη ημερομηνία και ώρα.

Το δεύτερο συστατικό της επίθεσης, αναλόγως με το λειτουργικό σύστημα, ήταν το Linux ή Solaris Wiper. Αυτό που στόχευε στα Linux μηχανήματα, κατέστρεφε ολόκληρο το περιεχόμενο των δίσκων που ήταν συνδεδεμένοι στο σύστημα. Το λογισμικό απενεργοποιούσε τις υπηρεσίες HTTP και SSH και διέγραφε σημαντικά αρχεία υπηρεσιών με σκοπό να καταστήσει το σύστημα μη λειτουργικό ταχύτερα. Τέλος, οδηγούσε τον υπολογιστή σε αναγκαστική επανεκκίνηση με την χρήση του SysRq και λόγω του ότι οι δίσκοι έχουν γεμίσει με τυχαία δεδομένα, δεν μπορούσε να φορτωθεί κανένα λειτουργικό σύστημα για να ανοίξει ο υπολογιστής.

Το Solaris Wiper, για να εμποδίσει τους χειριστές της εταιρείας ενέργειας να ανακτήσουν τον έλεγχο των υποσταθμών και να ανατρέψουν τις κακόβουλες διαδικασίες του Industroyer2, έψαχνε όλες τις υπηρεσίες του συστήματος και απενεργοποιούσε αυτές που περιείχαν τις λέξεις κλειδιά ssh, http, apache και ora_ ή oracle. Επιπλέον, η καταστροφή αρχείων γινόταν μέσω της διαγραφής των βάσεων δεδομένων και ολοκληρωνόταν με την αντικατάσταση των δεδομένων των σκληρών δίσκων. Τέλος, το script αυτοκαταστρεφόταν.

Τύπος PE

Ο τύπος αρχείων PE που εκμεταλλεύεται το κακόβουλο λογισμικό και οι επιτιθέμενοι σε αυτή την επίθεση είναι EXE.

Επικοινωνία με C&C / C2 servers

Δεν βρέθηκαν πληροφορίες σχετικά με τον τρόπο επικοινωνίας με τους C2 διακομιστές.

Τεχνικές αποφυγής ανίχνευσης

Ο κώδικας του Industroyer2 περιέχει περιορισμένες μεθόδους αποφυγής ανίχνευσης [77].

Κρυπτογράφηση

Οι επιτιθέμενοι χρησιμοποίησαν τον αλγόριθμο κρυπτογράφησης XOR.

Στόχος επίθεσης

Ο στόχος της επίθεσης ήταν η διαταραχή του ηλεκτρικού δικτύου και παροχής ρεύματος.

Απόδοση ευθυνών

Οι ερευνητές της ESET εκτιμούν με μεγάλη βεβαιότητα πως η ρωσική ομάδα APT Sandworm είναι υπεύθυνη για την επίθεση [76, p. 2].

3.1.15 Pegasus Project

Περιγραφή επίθεσης

Σύμφωνα με την εταιρεία κυβερνοασφάλειας Kaspersky [79], οι επιθέσεις με το κατασκοπευτικό λογισμικό (spyware) Pegasus, το οποίο δημιουργήθηκε από την Ισραηλινή εταιρεία NSO Group, αποτελούν τις πιο εξελιγμένες επιθέσεις που έχουν παρατηρηθεί ποτέ σε οποιοδήποτε τερματικό. Το Pegasus, σχεδιάστηκε για να παραβιάζει και να κατασκοπεύει υπολογιστές και κινητές συσκευές δίχως την συγκατάθεση του χρήστη και ιδιοκτήτη τους. Ωστόσο, οι δημιουργοί του ισχυρίζονται [80] πως το Pegasus προορίζεται μόνο για κυβερνητικές αρχές και συγκεκριμένα για να τις βοηθήσει να αντιμετωπίσουν εγκληματικές και τρομοκρατικές ενέργειες με νόμιμες διαδικασίες. Παραδείγματα κυβερνητικών οργανώσεων που έχουν χρησιμοποιήσει το κατασκοπευτικό λογισμικό αποτελούν το FBI και η CIA [81].

Σε αντίθεση με τους ισχυρισμούς της NSO Group, έρευνες [82] έδειξαν πως το λογισμικό της NSO Group μπορεί να αποτελέσει μεγάλο κίνδυνο για τα ανθρώπινα δικαιώματα σε παγκόσμιο επίπεδο. Συγκεκριμένα, τουλάχιστον 6 χώρες που χρησιμοποίησαν το Pegasus για μεγάλες επιχειρήσεις κατασκοπείας έχουν κατηγορηθεί για την κατάχρηση του, καθώς στόχευαν πολίτες. Επιπροσθέτως, το λογισμικό χρησιμοποιείται αρκετά από χώρες με ιστορικό καταχρηστικής συμπεριφοράς από τις κρατικές υπηρεσίες ασφάλειας με αποτέλεσμα να τίθεται υπό αμφισβήτηση το κατά πόσο η τεχνολογία αυτή χρησιμοποιείται σε νόμιμες διαδικασίες ποινικών ερευνών. Παράλληλα, ανακαλύφθηκαν επιθέσεις με το Pegasus σε 45 χώρες παγκοσμίως και στα θύματα περιλαμβάνονται δικηγόροι, δημοσιογράφοι, ακτιβιστές, πολιτικοί, μέλη του Ευρωκοινοβουλίου και άλλα άτομα υψηλής σημασίας.

Πρόσφατα, εκπρόσωποι της εξεταστικής επιτροπής του Ευρωπαϊκού Κοινοβουλίου επισκέφθηκαν το Ισραήλ και έμαθαν πως η εταιρεία συνεργάζεται πλέον με 22 οργανισμούς ασφαλείας και επιβολής του νόμου στην Ευρωπαϊκή Ένωση. Σύμφωνα με την NSO, έχουν συνεργαστεί με 14 χώρες της Ε.Ε στο παρελθόν και τουλάχιστον 12 εξακολουθούν να χρησιμοποιούν το Pegasus για την νόμιμη υποκλοπή κλήσεων κινητής τηλεφωνίας [83].

Αρχική μόλυνση – προσβολή

Για την μόλυνση ενός συστήματος με το Pegasus, πρέπει ο χρήστης να κάνει κλικ σε έναν ειδικά διαμορφωμένο κακόβουλο σύνδεσμο, ο οποίος όταν πατηθεί εκμεταλλεύεται μια αλυσίδα από zero-day exploits (προηγουμένως άγνωστες από την κοινότητα κυβερνοασφάλειας) με αποτέλεσμα να διεισδύσει το λογισμικό στο σύστημα χωρίς την συγκατάθεση και την γνώση του χρήστη-στόχου. Για να ωθήσουν οι επιτιθέμενοι το θύμα στο να πατήσει τον σύνδεσμο,

χρησιμοποιούνται τεχνικές spear phishing [82], ενώ με μια νέα έκδοση του Pegasus έχουν παρατηρηθεί και περιπτώσεις κατά τις οποίες μολύνεται η συσκευή του θύματος με εξελιγμένα "zero-click" exploits κατά τα οποία δεν απαιτείται από το θύμα να πατήσει κάποιον κακόβουλο σύνδεσμο ή να κατεβάσει κάτι, αλλά αρκεί μια αναπάντητη κλήση ή ένα μήνυμα για να μολυνθεί.

Εντοπίστηκε για πρώτη φορά τον Αύγουστο του 2016, όταν απέτυχε να εγκατασταθεί στο iPhone ενός ακτιβιστή ανθρωπίνων δικαιωμάτων από τα Ηνωμένα Αραβικά Εμιράτα. Αναλυτικότερα, οι επιτιθέμενοι έστειλαν μια σειρά από μηνύματα SMS που υπόσχονταν πληροφορίες που γνώριζαν πως θα ενδιέφεραν τον ακτιβιστή και του ζητούσαν να ανοίξει διάφορους κακόβουλους συνδέσμους URL [84].

Κακόβουλο λογισμικό – μέθοδοι

Το Pegasus παρέχει στους πελάτες-χρήστες του απεριόριστη πρόσβαση στις κινητές συσκευές του στόχου. Συγκεκριμένα, μπορεί να μολύνει συσκευές με iOS, BlackBerry OS, Symbian και μερικές από τις προσφερόμενες λειτουργίες του είναι οι εξής [85]:

- Παρακολούθηση φωνητικών κλήσεων και κλήσεων VoIP σε πραγματικό χρόνο.
- Συλλογή πληροφοριών, όπως επαφές, αρχεία, κωδικοί πρόσβασης, SMS, Emails, φωτογραφίες κάμερας, μικρόφωνο, ημερολόγιο κλπ.
- Παράκαμψη μεθόδων κρυπτογράφησης και πρωτοκόλλων (π.χ. SSL) που ασφαλίζουν τις επικοινωνίες και τα δεδομένα του θύματος.
- Παρακολούθηση πολλαπλών εφαρμογών, συμπεριλαμβανομένου του Skype, WhatsApp, Viber, Facebook, Blackberry, Telegram, Signal, Messenger κ.α.
- Παρακολούθηση και εντοπισμός ακριβών πληροφοριών σχετικά με την τοποθεσία του θύματος χρησιμοποιώντας GPS.
- Αυτοκαταστροφή σε περίπτωση έκθεσης και εντοπισμού του λογισμικού.
- Ανάκτηση οποιοδήποτε αρχείου από μια συσκευή για βαθύτερη ανάλυση.

Τύπος PE

Δεν βρέθηκαν πληροφορίες σχετικά με τον τύπο PE.

Επικοινωνία με C&C / C2 servers

Από το 2016 έως τα μέσα του 2018, ερευνητές [82] εντόπισαν 1.091 διευθύνσεις IP και 1.014 domain names που σχετίζονται με το κατασκοπευτικό λογισμικό Pegasus. Τα domain names των διακομιστών C2 επιλύονται σε cloud-based εικονικούς ιδιωτικούς διακομιστές που αποκαλούνται front-end και ενοικιάζονται είτε από την NSO Group είτε από τον πελάτη-επιτιθέμενο. Οι front-end διακομιστές έπειτα προωθούν την κυκλοφορία μέσω μιας αλυσίδας άλλων διακομιστών σε άλλους τελικούς διακομιστές που ονομάζονται back-end Pegasus

διακομιστές. Το Pegasus χρησιμοποιεί το πρωτόκολλο HTTPS για την επικοινωνία με τους διακομιστές C2 και τα domain names μερικές φορές υποδύονται παρόχους κινητής τηλεφωνίας, κυβερνητικές υπηρεσίες, τράπεζες και διαδικτυακές υπηρεσίες με στόχο να φανούν αξιόπιστα.

Τεχνικές αποφυγής ανίχνευσης

Το Pegasus εκμεταλλεύεται πολλαπλά zero-day exploits και τεχνολογίες, όπως το "zero-click". Αυτό έχει ως αποτέλεσμα να μην ανιχνεύεται η προσβολή του συστήματος από τις λύσεις ασφαλείας, καθώς οι μέθοδοι που χρησιμοποιούνται δεν είναι γνωστές και επομένως δεν έχουν ενημερωθεί οι συσκευές των στόχων.

Κρυπτογράφηση

Δεν βρέθηκαν πληροφορίες σχετικά με την κρυπτογράφηση.

Στόχος επίθεσης

Ο στόχος της επίθεσης ήταν η συλλογή δεδομένων και η κατασκοπεία χρηστών.

Απόδοση ευθυνών

Το Pegasus αναπτύχθηκε και διανέμεται από την Ισραηλινή εταιρεία NSO Group.

3.2 Σύγκριση Προηγμένων Επίμονων Απειλών

Ο παρακάτω πίνακας περιλαμβάνει ορισμένα κύρια χαρακτηριστικά και πληροφορίες σχετικά με συνολικά 21 επιθέσεις που καταγράφηκαν και αναλύθηκαν κατά την διάρκεια αυτής της έρευνας. Όπως προαναφέρθηκε και στην αρχή του κεφαλαίου, οι επιθέσεις με τίτλο Operation PZCHAO, Operation Rocket Man, Operation Dream Job, ThreatNeedle campaign, Attack on a telecommunications company in Kazakhstan και Unknown APT group has targeted Russia repeatedly since Ukraine invasion, έχουν συμπληρωματικό ρόλο στην διεξαγωγή των αποτελεσμάτων και των κοινών χαρακτηριστικών των κυβερνοεπιθέσεων.

Αναλυτικότερα, εμπεριέχονται στον πίνακα σημαντικές πληροφορίες για κάθε επίθεση, όπως η έναρξη της, η χρονική στιγμή που ανιχνεύτηκε, ο τύπος PE (Portable Executable) του κακόβουλου λογισμικού που αξιοποιήθηκε, η αρχική μόλυνση, η ικανότητα του κακόβουλου λογισμικού να διαδίδεται αυτοαναπαραγώμενο, η ύπαρξη λειτουργίας keylogging, εάν χρησιμοποιήθηκαν μέθοδοι αποφυγής ανίχνευσης, αλγόριθμοι κρυπτογράφησης, τεχνικές επικοινωνίας με διακομιστές C2 και τέλος ο στόχος της επίθεσης.

Επιπροσθέτως, είναι σημαντικό να τονιστεί πως τα κελιά με ‘-’ δηλώνουν πως δεν βρέθηκαν δεδομένα για το συγκεκριμένο χαρακτηριστικό στα πλαίσια της έρευνας.

Εικόνα 2. *Σύγκριση Προηγμένων Επίμονων Απειλών (1)*

Characteristics	Ukraine Power Grid Cyberattack	CRASHOVERRIDE / Industroyer	Bangladesh bank cyber heist	Domestic Kitten	Operation Cloud Hopper	Trisis / Triton	NotPetya Campaign
Active Since	Spring 2015	Oct-16	January-February 2015	2016	2014	At least 2014	Late 2016 - Early 2017
Detected	23-Dec-15	mid-2017	-	2018	Apr-17	Dec-17	27-Jun-17
PE Type	DLL	EXE & DLL	EXE & DLL	Mobile Application	DLL	EXE	DLL
Initial Infection	Spear-phishing campaign, malicious MS Office documents	Phishing campaign	Spear-phishing campaign	Victims are lured into downloading applications	Spear-phishing campaign, malicious Word document	Possibly phishing email, malicious executable	Unknown
Replication	No	No	No	No	No	No	Yes
Key logging	Yes	No	-	Yes	Yes	No	No
Evasion	Yes	Yes	Yes	-	Yes	Yes	Yes
Encryption	-	-	-	BASE64, XOR, AES	-	-	XOR, Salsa20, AES-128
C&C / C2	Attackers moved quickly away from their initial vulnerable C2s in an effort to blend into the target's systems as authorized users.	HTTPS, Tor software, Communication only outside of work hours	-	HTTP POST requests	Dynamic-DNS domains, Domains closely resemble legitimate organizations, Sensitive data is exfiltrated via MSP networks	Encrypted SSH-based tunnels, off-hour interactions with the target	-
Target	Power grid disruption	Electric grid disruption	Money theft	Information gathering, Espionage	Industrial espionage, Information gathering	Disruption	Disruption

***Εικόνα 3**. Σύγκριση Προηγμένων Επίμονων Απειλών (2)*

Characteristics	Olympic Destroyer	Operation ShadowHammer	Operation SolarWinds	Operation North Star	Operation Spalax	PseudoManuscrypt campaign	New Industroyer campaig
Active Since	Dec-17	June - November 2018	4-Sep-19	Feb-20	2020 (Active to this day)	Jan-20	Early 2022
Detected	Feb-18	29-Jan-19	Dec-20	-	2020	Jun-21	12-Apr-22
PE Type	EXE	EXE	DLL	DLL	EXE & DLL	EXE	EXE
Initial Infection	Spear-phishing campaign, malicious MS Office documents, malicious mobile applications	Unknown	Unknown	Social media, spear-phishing emails, malicious Word documents	Spear-phishing emails, pdf containing link to OneDrive or Mediafire containing malicious RAR.	Fake pirated software installer archives	Unknown
Replication	Yes	No	No	No	Yes	No	No
Key logging	No	No	Yes	Yes	Yes	Yes	No
Evasion	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Encryption	RC4 & BASE64	Custom block-chaining XOR algorithm	XOR	BASE64, VEST, AES, XOR	XOR, RC4, BASE64	-	XOR
C&C / C2	Ports used: 443, 4443, 8080, 8081, 8443, 8880, Malicious server in Argentina	First stage of C2 servers would provide the backdoor with an encrypted next stage C2 domain, Hard-coded URL for C2 communication, Use of publicly editable online Google documents	Two-part C2 protocol that involved DNS and HTTP	C2 infrastructure consisted of compromised domains in different countries	70 different domains used for C&C, at least 24 IP addresses, Dynamic DNS services, RC4 encryption for C2 communications, TCP used for communications	A specific implementation of the KCP is used to connect to the server	-
Target	Disruption, Sabotage	Unknown	Information gathering	Espionage	Information gathering, Espionage	Information gathering, Espionage	Electric grid disruption

Εικόνα 4. *Σύγκριση Προηγμένων Επίμονων Απειλών (3)*

Characteristics	Pegasus Project	Operation PZCHAO	Operation Rocket Man	Operation Dream Job	ThreatNeedle campaign	Attack on a telecommunications company in Kazakhstan	Unknown APT group has targeted Russia repeatedly since Ukraine invasion
Active Since	At least 2011 (Active to this day)	-	Group has been active since 2013	2019	May-20	2019	Feb-22
Detected	Aug-16	17-Jul-17	Aug-18	June-August2020	mid-2020	Oct-21	Feb-22
PE Type	-	EXE & DLL & SYS	EXE	EXE & DLL & SYS	SYS	EXE & DLL	EXE & DLL
Initial Infection	Spear-phishing SMS or emails, malicious links, zero-click exploits	Highly targeted SPAM campaigns, malicious VBS attachment	Spear-phishing, infected website disguised as the attached file image	Social media impersonation, Social engineering methods, Spear-phishing attachment	Spear-phishing emails, malicious Word document	-	Social engineering, disguising malware as an interactive map of Ukraine, Spear-phishing emails, malicious PDF & DOCX attachments, Social media
Replication	No	No	No	No	No	No	No
Key logging	Yes	Yes	No	Yes	Yes	Yes	No
Evasion	Yes	Yes	Yes	Yes	Yes	No	Yes
Encryption	-	AES	XOR	XOR	RC4, AES, XOR	dynamic XOR, XOR method with random bytes, AES-128, RC4	XOR
C&C / C2	1.091 IP Addresses and 1.014 Domain names are associated with Pegasus C2 servers. Domain names sometimes impersonate mobile providers, online services, banks, government services etc. HTTPS, 2 layers of C2 servers	Accessed on port 8555. Five subdomains hosting communication and control servers, each one is used for a well-defined purpose. Rat.pzchao.com used for receiving instructions, centruriosa.info used for receiving instructions, zll855.no-ip.info used for receiving new C&C addresses. Malware hosting server: HTTP FILE SERVER, over 12000 downloads for the main payloads	Command communication (C2) communication is proceeded via PubNub channel. An attacker uses a legitimate IaaS service for communication, so that it is quite difficult to detect the malicious traffic	Two-part C2 protocol that involved DNS and HTTP	Custom SSH tunnels from several compromised server hosts, Binary encryption, HTTP POST requests	GET requests to server, Heartbeat requests, Establishing a connection to the server mimics the creation of a TLS1.0 connection	HTTPS, SSL
Target	Information gathering, Espionage	Espionage, Information gathering	-	Espionage, Money theft	Espionage	Information gathering	Unknown

3.3 Μορφότυποι

Από την παραπάνω ανάλυση και τον πίνακα σύγκρισης προηγμένων επίμονων απειλών, προκύπτουν ορισμένα κοινά χαρακτηριστικά και μονοπάτια των επιθέσεων τύπου APT. Στην παρούσα ενότητα, βάσει τα παραπάνω, εξάγονται μορφότυποι και κοινές μεθοδολογίες σχετικά με διάφορες πτυχές του κύκλου ζωής μιας τέτοιας απειλής. Πιο συγκεκριμένα, εξάγονται συμπεράσματα για τα αρχικά στάδια της ανίχνευσης και της συλλογής πληροφοριών, τους αρχικούς φορείς των επιθέσεων, την εγκαθίδρυση ερεισμάτων, την επέκταση, την επικοινωνία με διακομιστές C&C, τις μεθοδολογίες για την αποφυγή ανίχνευσης, την χρήση κρυπτογράφησης, τους τύπους PE των κακόβουλων λογισμικών, καθώς και για τους στόχους και τα κίνητρα των φορέων APT.

3.3.1 Ανίχνευση και συλλογή πληροφοριών

Όπως παρουσιάστηκε και στο 2ο κεφάλαιο, ένα από τα πρώτα βήματα μιας επίθεσης APT είναι το στάδιο της προετοιμασίας που περιλαμβάνει την συλλογή πληροφοριών σχετικά με τον οργανισμό-στόχο. Όσες περισσότερες πληροφορίες συλλέξουν οι επιτιθέμενοι, τόσο αυξάνονται οι πιθανότητες η επίθεση να είναι επιτυχής και να εκπληρωθούν οι στόχοι τους. Η ανίχνευση και συλλογή πληροφοριών περιλαμβάνουν συνήθως τεχνικές κοινωνικής μηχανικής, εργαλεία ανίχνευσης και σάρωσης θυρών, υπηρεσιών και δικτύων, καθώς και τεχνικές OSINT (Open Source Intelligence) κατά τις οποίες συλλέγονται και αναλύονται δεδομένα και πληροφορίες από δημόσιες πηγές. Συνήθως, οι πληροφορίες που επιλέγουν οι επιτιθέμενοι να εντοπίσουν αφορούν το δίκτυο του στόχου, τις περιοχές διευθύνσεων IP, τα σημεία πρόσβασης, τις ανοιχτές θύρες, τους δρομολογητές, τους μεταγωγείς, τα ενεργά μηχανήματα, λεπτομέρειες υποδομών, καθώς και στοιχεία για τους εργαζομένους όπως η κοινωνική τους ζωή, ιστοσελίδες που επισκέπτονται συχνά και πολλά άλλα.

Παράλληλα, ανιχνεύονται κρίσιμες πληροφορίες, όπως η ύπαρξη λύσεων προστασίας όπως λογισμικά anti-virus, sandboxes, firewalls, IDS, IPS και γίνονται προσπάθειες για εντοπισμό ιστότοπων στο δίκτυο-στόχο που έχουν τρωτότητες υψηλού κινδύνου, όπως cross-site scripting (XSS), SQL injections (SQLI). Στις επιθέσεις APT, η διαδικασία αναγνώρισης των υποδομών και των στοιχείων του θύματος είναι παθητική, καθώς συλλέγουν πληροφορίες που θα τους εξυπηρετήσουν αργότερα σε επόμενα στάδια [86].

Τέλος, είναι σημαντικό να επισημανθεί πως η προέλευση των δραστηριοτήτων αναγνώρισης, ανίχνευσης και συλλογής πληροφοριών είναι γενικά δύσκολη να εντοπιστεί.

3.3.2 Αρχική διείσδυση

Από τις 21 επιθέσεις που βρίσκονται στον πίνακα της ενότητας 3.2, οι 15 (71,4%) ξεκίνησαν με μεθόδους κοινωνικής μηχανικής (social engineering). Πιο συγκεκριμένα, οι 14 (66.6%) αξιοποίησαν phishing, spear-phishing ή/και SPAM μηνύματα ηλεκτρονικού ταχυδρομείου τα οποία περιείχαν κακόβουλα συνημμένα αρχεία MS Office, Word, PDF και σε

μια περίπτωση μολυσμένη ιστοσελίδα μεταμφιεσμένη σε φωτογραφία. Επιπλέον, σε 3 επιθέσεις (14,2%) χρησιμοποιήθηκαν και τα μέσα κοινωνικής δικτύωσης για να προσεγγίσουν τους στόχους τους υποδύοντας έμπιστα πρόσωπα. Ενώ, για 4 επιθέσεις (19%) οι αρχικές μέθοδοι μόλυνσης δεν έχουν προσδιοριστεί ακόμα.

Γίνεται, επομένως, εύκολα αντιληπτό ότι πλέον ένα μεγάλο ποσοστό των επιθέσεων τύπου APT χρησιμοποιούν τεχνικές κοινωνικής μηχανικής και κατά κύριο λόγο ξεκινάνε με spear-phishing μηνύματα ηλεκτρονικού ταχυδρομείου. Αναλυτικότερα, μέσω των πληροφοριών που κατάφεραν οι επιτιθέμενοι να συλλέξουν από το προηγούμενο στάδιο της επίθεσης, αποστέλλουν έξυπνα και κατάλληλα προσαρμοσμένα μηνύματα ηλεκτρονικού ταχυδρομείου που περιέχουν κακόβουλο συνημμένο αρχείο (συνήθως αρχεία Office, ZIP, Adobe, PDF κ.α.). Αυτά τα μηνύματα είναι σχεδιασμένα για να δελεάσουν τον παραλήπτη να κατεβάσει τα αρχεία και αφότου συμβεί αυτό, το κακόβουλο λογισμικό εκμεταλλεύεται κάποια τρωτότητα των εφαρμογών που χρησιμοποιούνται για το άνοιγμα των αρχείων, με αποτέλεσμα την μόλυνση του μηχανήματος του υπαλλήλου-στόχου και στην συνέχεια ολόκληρου του δικτύου του οργανισμού. Επιπροσθέτως, τα μηνύματα μπορεί να περιέχουν συνδέσμους URL κακόβουλων ιστότοπων, τους οποίους όταν επισκέπτεται ο χρήστης αυτομάτως ξεκινάει μια διαδικασία λήψης κακόβουλου λογισμικού δίχως να το καταλάβει ο ίδιος. Παρακάτω θα αναφερθούν μερικές ακόμη από τις πιο συνηθισμένες τεχνικές που χρησιμοποιούνται από φορείς APT σε αυτό το στάδιο, σύμφωνα με την έρευνα [86]:

1. *Εκμετάλλευση γνωστών τρωτοτήτων σημείων εφαρμογών*: Οι γνωστές τρωτότητες που είναι συνήθως εκτεθειμένες, μπορούν να ληφθούν από δημοσίως γνωστές τεράστιες βάσεις δεδομένων τρωτοτήτων όπως η Common Vulnerabilities and Exposures List (CVE), η Open Source Vulnerability Database (OSVDB) και η NIST National Vulnerability Database (NVD). Επιπλέον, ο φορέας APT μπορεί να συλλέξει πληροφορίες σχετικά με τρωτότητες και exploits και από το "dark web" και σχετικά forums.
2. *Κακόβουλο λογισμικό:* Σύμφωνα με την Threat Intelligence πλατφόρμα AV-ATLAS [87], από το 1984 έως και σήμερα, έχουν υπάρξει περισσότερα από 1,2 δισεκατομμύρια προγράμματα κακόβουλου λογισμικού. Μόνο το 2022 (έως και τον Αύγουστο) έχουν εντοπιστεί 72 εκατομμύρια προγράμματα κακόβουλου λογισμικού. Επιπροσθέτως, είναι σημαντικό να τονιστεί πως το κακόβουλο λογισμικό μπορεί να μεταδοθεί με τεχνικές spear-phishing, μέσω συσκευών USB και με την λήψη του από το διαδίκτυο.
3. *Zero-day τρωτότητα:* Ο όρος "zero-day" αναφέρεται σε ένα σφάλμα λογισμικού που είτε ο κατασκευαστής του δεν γνωρίζει την ύπαρξη του, είτε γνωρίζει αλλά δεν μπορεί να το επιδιορθώσει προτού ο επιτιθέμενος το εκμεταλλευτεί. Ο δράστης APT, στην φάση της συλλογής δεδομένων για τον στόχο του, ανακαλύπτει σημαντικές πληροφορίες σχετικά με τα συστήματα του στόχου, όπως τα λειτουργικά συστήματα και τις εκδόσεις προγραμμάτων, με αποτέλεσμα να έχει την δυνατότητα είτε να εντοπίσει zero-day τρωτότητες και να τις εκμεταλλευτεί μέσω ανάπτυξης κατάλληλων exploit, είτε να τις αγοράσει από το διαδίκτυο σε πολύ υψηλές τιμές.
4. *Επίθεση Watering*-Hole: Σε αντίθεση με τις επιθέσεις phishing, η επίθεση "watering-hole" περιλαμβάνει την μόλυνση ενός ή περισσοτέρων από τους ιστότοπους που επισκέπτονται συχνά οι εργαζόμενοι του οργανισμού-στόχου. Αυτό επιτυγχάνεται μέσω της εκμετάλλευσης τρωτοτήτων των επιλεγμένων -συχνά επισκεπτόμενων- ιστότοπων με

σκοπό την εισαγωγή κακόβουλου κώδικα. Έτσι, ο φορέας APT καταφέρνει να μολύνει τα συστήματα υπαλλήλων του στόχου του.

3.3.3 Εγκαθίδρυση ερεισμάτων

Η εδραίωση περιλαμβάνει διαδικασίες με τις οποίες οι επιτιθέμενοι εξασφαλίζουν τον έλεγχο των συστημάτων του στόχου και την επικοινωνία από μια απομακρυσμένη τοποθεσία. Συνήθως, αφότου εγκατασταθεί το κακόβουλο λογισμικό στο μηχάνημα του αρχικού στόχου, δημιουργείται μια κερκόπορτα η οποία συνδέεται με τους απομακρυσμένους διακομιστές εντολών και ελέγχου C&C με σκοπό την επικοινωνία και την λήψη εντολών. Η τακτική κατά την οποία η κερκόπορτα ξεκινάει μια εξωτερική σύνδεση αποτελεί μια καλή και συνηθισμένη τεχνική, καθώς η κακόβουλη δικτυακή δραστηριότητα που προέρχεται από το εσωτερικό του δικτύου του στόχου εντοπίζεται πιο δύσκολα. Συνήθως, οι κερκόπορτες που φορτώνονται στα συστήματα των αρχικών στόχων έχουν την δυνατότητα να κατεβάζουν, να διαγράφουν, να εκτελούν, να δημιουργούν αρχεία και προγράμματα, να απαριθμούν τους χρήστες και το δίκτυο, μερικές φορές να καταγράφουν το πληκτρολόγιο και να αποθηκεύουν στιγμιότυπα της οθόνης κ.α.

3.3.4 Επέκταση

Σε αυτό το σημείο, ο φορέας APT αφότου έχει αποκτήσει πρόσβαση στο σύστημα του στόχου του, επιθυμεί να εξαπλωθεί σε ολόκληρο το δίκτυο και στα υπόλοιπα συστήματα του εσωτερικού περιβάλλοντος του θύματος. Συνήθως, για να επιτευχθεί η επέκταση αυτή, γίνονται προσπάθειες κάθετης κλιμάκωσης προνομιών κατά τις οποίες οι επιτιθέμενοι επιχειρούν να αποκτήσουν δικαιώματα επιπέδου διαχειριστή και μέσω αυτών να μεταπηδήσουν και να μολύνουν εκ νέου πολλαπλά μηχανήματα με κερκόπορτες και άλλα κακόβουλα λογισμικά. Αυτές οι προσπάθειες περιλαμβάνουν την απόκτηση στοιχείων και διαπιστευτηρίων μέσω λογισμικών όπως το mimikatz, keyloggers, τεχνικών όπως pass-the-hash και επιθέσεων brute force, κατά τις οποίες οι δράστες προσπαθούν να πετύχουν τον σωστό συνδυασμό συνθηματικών ελέγχοντας συστηματικά πολλούς πιθανούς συνδυασμούς.

3.3.5 Επικοινωνία με C2 και εξαγωγή δεδομένων

Σύμφωνα με την TrendMicro [88], ένας διακομιστής εντολών και ελέγχου (C2, C&C) είναι ένας υπολογιστής που ελέγχεται από τους επιτιθέμενους και χρησιμοποιείται για την αποστολή εντολών σε συστήματα που έχουν παραβιαστεί από κακόβουλο λογισμικό και για την λήψη κλεμμένων δεδομένων από ένα δίκτυο-στόχο. Κατά κύριο λόγο, ο φορέας APT αξιοποιεί διακομιστές C2 για την απομακρυσμένη επικοινωνία και πρόσβαση στο εσωτερικό περιβάλλον του στόχου του με σκοπό την εκτέλεση κακόβουλων εντολών και την εξαγωγή κλεμμένων δεδομένων. Η διαδικασία επικοινωνίας με τα κέντρα C2 αποτελεί ζωτικό βήμα των προηγμένων επίμονων απειλών, καθώς χωρίς αυτά δεν θα μπορούσαν οι επιτιθέμενοι ούτε να κινηθούν πλευρικά εντός ενός δικτύου, ούτε θα κατάφερναν να αποσπάσουν κρίσιμα δεδομένα και πληροφορίες που ίσως ήταν και απώτερος σκοπός της επιχείρησης.

Όπως φαίνεται από επιθέσεις που αναλύθηκαν σε αυτό το κεφάλαιο, τα κακόβουλα λογισμικά που αξιοποιήθηκαν σχεδόν σε όλες τις περιπτώσεις κατάφεραν να δημιουργήσουν κανάλια επικοινωνίας με τους διακομιστές των επιτιθέμενων. Ειδικότερα, τα δικτυακά πρωτόκολλα που εμφανίζονται περισσότερο είναι το Hyper Text Transport Protocol (HTTP), το HTTP Secure (HTTPS), το Secure Shell (SSH), το Domain Name System (DNS) και το Dynamic DNS (DDNS). Παράλληλα, σε πολλές από τις αναλυθέντες επιθέσεις οι δράστες χρησιμοποιούσαν και επιπλέον τεχνικές αποφυγής εντοπισμού της παράνομης διαδικτυακής κίνησης. Μερικές από τις πιο συνηθισμένες ήταν ο περιορισμός της επικοινωνίας με το κακόβουλο λογισμικό μόνο σε ώρες εκτός λειτουργίας των οργανισμών-στόχων, η χρήση του Tor και η αξιοποίηση πολλαπλών και διαφορετικών διακομιστών στα διαφορετικά στάδια της επίθεσης.

3.3.6 Μέθοδοι αποφυγής ανίχνευσης

Συνολικά 19 (90%) επιθέσεις χρησιμοποίησαν πολύπλοκες τεχνικές σκοπεύοντας να αποτρέψουν την ανίχνευση ή να δυσκολέψουν την ανάλυση του κακόβουλου λογισμικού. Κατά κύριο λόγο, οι επιτιθέμενοι επιθυμούν να παραμείνουν «αόρατοι» εντός των συστημάτων του θύματος για όσο μεγαλύτερο διάστημα γίνεται. Βέβαια, η επιθυμία αυτή έχει να κάνει με τον βασικό στόχο που έχει τεθεί από την αρχή της επίθεσης, εάν για παράδειγμα η επίθεση αποτελεί μια εκστρατεία παρακολούθησης και συλλογής πληροφοριών, τότε συνηθίζεται να δίνεται μεγαλύτερη έμφαση στην επιμονή και στην κάλυψη ιχνών, ενώ μια επίθεση με λυτρισμικό εντοπίζεται άμεσα από το θύμα.

Με βάση τα ευρήματα, σε πολλές περιπτώσεις οι επιτιθέμενοι εκμεταλλευόντουσαν νόμιμα λογισμικά, αξιόπιστες υπογραφές (σε κάποιες περιπτώσεις τις μιμούνταν ενώ σε άλλες διέθεταν κλεμμένες αυθεντικές), εργαλεία, ονόματα και ιδιότητες αρχείων των Windows και της Microsoft κάνοντας την ανίχνευση πολύ δύσκολη. Παράλληλα, παρατηρούνται σε έντονο βαθμό και τεχνικές αναζήτησης και παράκαμψης (anti-analysis, anti-forensics, anti-sandboxing) προϊόντων Antivirus και Sandbox, κατά τις οποίες το κακόβουλο λογισμικό αναλόγως με το είδος του λογισμικού ασφάλειας άλλαζε την συμπεριφορά του με σκοπό να μην εντοπιστεί. Επιπροσθέτως, αξιοποιούνται συχνά και λειτουργίες διαγραφής αρχείων καταγραφής συμβάντων, καθώς και πολλαπλά επίπεδα κρυπτογράφησης και obfuscation καθιστώντας την επιτυχία των εγκληματολογικών ερευνών δύσκολη.

3.3.7 PE Type

Ο τύπος PE EXE και DLL χρησιμοποιήθηκε στην πλειοψηφία των κακόβουλων λογισμικών των επιθέσεων, συγκεκριμένα σε 13 (61,9%) και 12 (57,1%) επιθέσεις αντίστοιχα. Ωστόσο παρατηρήθηκαν και 3 περιπτώσεις (14,2%) που ο τύπος PE ήταν SYS.

3.3.8 Χρήση κρυπτογράφησης

Από τον πίνακα της ενότητας 3.2, φαίνεται πως σε 11 επιθέσεις (52,3%) οι δράστες βασίστηκαν στην κρυπτογράφηση με την πράξη XOR για να αποτρέψουν την ανίχνευση και να περιπλέξουν την ανάλυση του κακόβουλου λογισμικού και της κυκλοφορίας του δικτύου. Παράλληλα, χρησιμοποιήθηκαν και άλλοι αλγόριθμοι όπως ο AES σε 6 επιθέσεις (28,5%), οι RC4 και BASE64 σε 4 (19%) και τέλος οι VEST και SALSA20 σε 1 επίθεση (4,7%) ο καθένας.

3.3.9 Στόχος επίθεσης

Σύμφωνα με την ανάλυση, 11 από τις 21 επιθέσεις (52,3%) στόχευαν είτε στην επίμονη και μακροχρόνια κατασκοπεία και παρακολούθηση του στόχου, είτε στην συλλογή πληροφοριών, ενώ μόλις 6 κυβερνοεπιθέσεις (28,5%) είχαν ως στόχο την διαταραχή λειτουργιών και υπηρεσιών και την πρόκληση ζημιών. Επιπροσθέτως, σε 2 περιπτώσεις (9,5%) παρατηρήθηκαν και οικονομικά κίνητρα, καθώς οι επιτιθέμενοι κατάφεραν να αποσπάσουν χρηματικά ποσά από τα θύματα τους. Τέλος, για 2 επιθέσεις (9,5%) δεν έχουν προσδιοριστεί ακόμη τα κίνητρα και οι στόχοι των δραστών.

4. Άμυνα και αντίμετρα

Η χρήση προσαρμοσμένου ιομορφικού λογισμικού, η εκμετάλλευση άγνωστων μη καταγεγραμμένων τρωτοτήτων (zero-day), οι προηγμένες μέθοδοι και τεχνικές, καθώς και οι πιθανές κρατικές χρηματοδοτήσεις των επιτιθέμενων έχουν ως αποτέλεσμα κανένα μεμονωμένο προϊόν ασφαλείας να μην προσφέρει αποτελεσματική προστασία. Για αυτόν τον λόγο, απαιτείται ένα ευρύ φάσμα αντιμέτρων ασφαλείας και διαδικασιών hardening για να καταστεί δυνατή μια πολυεπίπεδη και ισχυρή άμυνα [89]. Στο κεφάλαιο αυτό, αρχικά παρουσιάζονται ενδεικτικά μέτρα προστασίας για την κοινωνική μηχανική και στην συνέχεια προτείνονται μέτρα προστασίας για την παρακολούθηση, την ανίχνευση και την μετρίαση μιας επίθεσης APT, που προτάθηκαν, κατηγοριοποιήθηκαν και αναλύθηκαν από τους Alshamrani κ.α [86].

4.1 Αντίμετρα κοινωνικής μηχανικής

Στα πλαίσια αυτής της έρευνας, διαπιστώθηκε πως ο αρχικός φορέας της πλειοψηφίας των επιθέσεων τύπου APT ήταν τεχνικές κοινωνικής μηχανικής. Είναι ευρέως αποδεκτό από την κοινότητα της κυβερνοασφάλειας πως ο άνθρωπος -από την αρχή- αποτελεί έναν από τους πιο αδύναμους κρίκους στην αλυσίδα της κυβερνοασφάλειας [90]. Η εταιρεία τηλεπικοινωνιών Verizon στην έκθεση της με τίτλο "2022 Data Breach Investigation Report (DBIR)" [91] αποκάλυψε πως φέτος το 82% των παραβιάσεων αφορούσαν το ανθρώπινο στοιχείο, συμπεριλαμβανομένων των κοινωνικών επιθέσεων, των σφαλμάτων και της κατάχρησης. Πιο συγκεκριμένα, κυριαρχούν οι επιθέσεις με phishing καθώς αποτελεί ένα από τα τέσσερα κύρια σημεία εισόδου σε έναν οργανισμό.

Δεδομένου πως στην απέναντι πλευρά βρίσκεται μια άρτια οργανωμένη και ικανή ομάδα ειδικών που έπειτα από έντονη παρακολούθηση και συλλογή πληροφοριών στοχεύει στην εκμετάλλευση του ανθρώπινου παράγοντα για να διεισδύσει στον οργανισμό-θύμα, κρίνεται απαραίτητη η υιοθέτηση κατάλληλων διαδικασιών και μέτρων ασφαλείας. Παράλληλα, αξίζει να τονιστεί ότι ο φορέας αυτός δεν μπορεί να εξαλειφθεί, αλλά τα μέτρα προστασίας αυξάνουν τις πιθανότητες να αποφευχθεί ή να γίνει αντιληπτή νωρίς μια παραβίαση πριν προκληθούν σοβαρές ζημιές στους οργανισμούς. Εύκολα, λοιπόν, οδηγούμαστε στο συμπέρασμα ότι η τεχνολογία από μόνη της δεν αποτελεί λύση για επιθέσεις που αξιοποιούν τεχνικές κοινωνικής μηχανικής.

Ακολουθώντας την ταξινόμηση των αντιμέτρων που ορίζεται από το NIST Cybersecurity Framework [92], οι στρατηγικές άμυνας απέναντι σε επιθέσεις κοινωνικής μηχανικής κατηγοριοποιούνται σε τρείς κύριες κατηγορίες: Προστασία, Ανίχνευση, Αντίδραση.

Προστασία

Το αποτελεσματικότερο μέσο ασφάλειας απέναντι σε τέτοιες απειλές είναι η ενημέρωση και η κατάρτιση. Το ανθρώπινο δυναμικό των οργανισμών θα πρέπει μέσω κατάλληλων προγραμμάτων να ενημερώνεται και να εκπαιδεύεται για το πώς να αντιμετωπίσει επιθέσεις αυτής

της μορφής. Αναλυτικότερα, αναλόγως με την ειδικότητα και τις δεξιότητες του κάθε υπαλλήλου τα προγράμματα αυτά οφείλουν να εξοικειώσουν τους ενδιαφερόμενους με τα διάφορα μονοπάτια επίθεσης και τις πολλαπλές τεχνικές που μπορούν να αξιοποιήσουν οι επιτιθέμενοι. Συμπληρωματικά, μπορούν να περιλαμβάνουν διαλέξεις ή εικονικά εργαστήρια τα οποία προσομοιώνουν σενάρια επιθέσεων στα οποία οι εργαζόμενοι καλούνται να διαχειριστούν και να αντιμετωπίσουν συγκεκριμένες ελεγχόμενες καταστάσεις. Πιο συγκεκριμένα, στις προσομοιωμένες επιθέσεις αποστέλλονται κακόβουλα μηνύματα ηλεκτρονικού ταχυδρομείου σε διάφορα μέλη του οργανισμού για να κριθεί σε τι βαθμό μπορούν οι εργαζόμενοι να εντοπίσουν και να διακρίνουν κακόβουλα μηνύματα. Ένα γνωστό πρόγραμμα εκπαίδευσης του ανθρώπινου δυναμικού οργανισμών που χρησιμοποιείται έως και σήμερα, αποτελεί το SETA (Security Education, Education and Awareness) και στοχεύει στην μείωση ανθρώπινων σφαλμάτων και στην αύξηση της ευαισθητοποίησης των εργαζομένων σε θέματα ασφάλειας [93].

Απαραίτητο μέσο προστασίας αποτελεί και ο έλεγχος προσπέλασης (Access Control). Ο έλεγχος προσπέλασης σε ένα πληροφοριακό σύστημα περιλαμβάνει τα τεχνικά μέτρα και τις διαδικασίες με τις οποίες μπορεί να αποδειχθεί, με κάποιο βαθμό ακρίβειας, η ταυτότητα του λογικού υποκειμένου που ζητεί να προσπελάσει το φυσικό περιβάλλον ή τους υπολογιστικούς πόρους του συστήματος αυτού [2]. Με αυτόν τον τρόπο, περιορίζεται η πρόσβαση του κάθε εργαζομένου μόνο στους απαραίτητους για αυτόν πόρους, ελαχιστοποιώντας την επιφάνεια της επίθεσης στην οποία εκθέτει κάθε εργαζόμενος τον οργανισμό του [94].

Επιπροσθέτως, μπορούν να δημιουργηθούν και να εφαρμοστούν διάφορες πολιτικές και διαδικασίες ασφαλείας. Για παράδειγμα, μπορεί να εφαρμοστεί ορισμένη πολιτική κωδικών πρόσβασης με σκοπό την δημιουργία ενός ισχυρού προτύπου που στοχεύει στην μείωση των περιστατικών παραβίασης των συστημάτων λόγω αδύναμων κωδικών. Άλλες χρήσιμες πολιτικές ασφαλείας αποτελούν οι κανόνες φυσικής πρόσβασης στις εγκαταστάσεις ενός οργανισμού, οι πολιτικές αποκάλυψης πληροφοριών καθώς και πολιτικές σχετικά με τις συσκευές που θα χρησιμοποιούνται εντός του (π.χ. BYOD, Bring Your Own Device) [90].

Είναι απαραίτητο να επισημανθεί πως ένας οργανισμός μπορεί να χρησιμοποιήσει και προστατευτικές τεχνολογίες για να μειώσει σημαντικά τις πιθανότητες να υπάρξει παραβίαση από ανθρώπινο σφάλμα. Τέτοιες τεχνολογίες μπορεί να είναι οι μαύρες λίστες (Blacklists), τα τείχη προστασίας εφαρμογών (Application firewalls) καθώς και λογισμικά που εμποδίζουν την πρόσβαση σε κακόβουλες ιστοσελίδες [94]. Τέλος, ένα πολύ σημαντικό αντίμετρο αποτελεί και η κρυπτογράφηση. Μέσω αυτής, όλα τα αποθηκευμένα δεδομένα ενός οργανισμού είναι διασφαλισμένα καθώς υπάρχουν πολλαπλοί διαφορετικοί ασφαλείς αλγόριθμοι κρυπτογράφησης. Έτσι, ακόμη και να καταφέρουν οι επιτιθέμενοι να υποκλέψουν εμπιστευτικά δεδομένα και πληροφορίες ενός οργανισμού, εφόσον βρίσκονται σε κρυπτογραφημένη μορφή, δεν θα μπορέσουν να τα αποκρυπτογραφήσουν καθιστώντας τα κλεμμένα δεδομένα άχρηστα [90].

Ανίχνευση

Οι στρατηγικές ανίχνευσης αναφέρονται σε τεχνικές και μη λύσεις που αποσκοπούν στην ανακάλυψη phishing δραστηριοτήτων πριν την εκδήλωση τους [95]. Οι οργανισμοί οφείλουν να

διαθέτουν μια διαδικασία ανίχνευσης επιθέσεων κοινωνικής μηχανικής, συμπεριλαμβανομένων του phishing και των τηλεφωνικών απατών. Η διαδικασία αυτή παρέχει δυνατότητες συνεχούς παρακολούθησης με στόχο την ανίχνευση ύποπτων συμπεριφορών στο δίκτυο ενός οργανισμού. Τα εργαλεία παρακολούθησης και φιλτραρίσματος του δικτύου που χρησιμοποιούνται σε αυτήν την διαδικασία αποσκοπούν στον εντοπισμό προσπαθειών παραποίησης ιστότοπων [94].

Αντίδραση

Οι στρατηγικές αντίδρασης αναφέρονται στην ικανότητα έγκαιρης ανταπόκρισης σε επιθέσεις κοινωνικής μηχανικής, με κυριότερη το phishing και είναι ζωτικής σημασίας για τους οργανισμούς. Η έγκαιρη αναφορά περιστατικών αποτελεί ένα σημαντικό μέσο για την μείωση της επίδρασης της επίθεσης. Μεγάλοι οργανισμοί, όπως τράπεζες ή χρηματοπιστωτικοί φορείς, πολλές φορές απασχολούν ομάδες απόκρισης, των οποίων ο στόχος είναι να αναλύουν και να μετριάζουν τις εισερχόμενες επιθέσεις. Οι ομάδες αυτές συνήθως λειτουργούν σε κέντρα επιχειρήσεων ασφαλείας και βασίζονται σε τεχνολογίες ανίχνευσης προκειμένου να αντιδράσουν στην επίθεση [94].

4.2 Μέθοδοι επιτήρησης και παρακολούθησης συστημάτων

Σύμφωνα με τους συγγραφείς, κρίνεται απαραίτητη η παρακολούθηση και η επιτήρηση ολόκληρου του συστήματος δικτύου του οργανισμού που επιθυμεί να αμυνθεί, σε πολλαπλά σημεία, με στόχο την κάλυψη της επιφάνειας του. Για αυτόν τον λόγο, προτείνονται τα παρακάτω αντίμετρα:

Παρακολούθηση Δίσκων

Κάθε οργανισμός οφείλει να επιτηρεί κάθε τελικό του σύστημα για τυχόν κακόβουλη συμπεριφορά μέσω τεχνολογιών όπως το antivirus, τα firewalls, λογισμικά φιλτραρίσματος περιεχομένου κ.α. Με αυτόν τον τρόπο, ελαχιστοποιείται το πλήθος των πιθανών σημείων εισόδου για έναν εισβολέα αφαιρώντας τρωτότητες που διαφορετικά θα επέτρεπαν την εξάπλωση του ιομορφικού λογισμικού σε άλλα συστήματα εντός του δικτύου. Παράλληλα, προτείνεται και η παρακολούθηση της χρήσης της CPU, καθώς μπορεί να διευκολύνει στον εντοπισμό ύποπτων δραστηριοτήτων τελικών συστημάτων.

Παρακολούθηση Μνήμης

Έπειτα από την ανάλυση των επιθέσεων στο κεφάλαιο 3, διαπιστώθηκε πως μια από τις βασικές τεχνικές που αξιοποιούν οι δράστες για να αποφύγουν την ανίχνευση του κακόβουλου λογισμικού που έχουν εισάγει στο σύστημα του οργανισμού-στόχου, είναι η προσθήκη του σε κάποια νόμιμη διεργασία ή/και εφαρμογή. Με αυτόν τον τρόπο, δεν υπάρχει ξεχωριστό αρχείο

από το οποίο εκτελείται το λογισμικό, καθώς η εκτέλεσή του συμβαίνει στα πλαίσια της ήδη εκτελούμενης διεργασίας-ξενιστή, έχοντας ως αποτέλεσμα να μην υπάρχει κανένα ίχνος ανώμαλης συμπεριφοράς πέρα από την απροσδόκητη χρήση μνήμης. Λόγω αυτών των προηγμένων τεχνικών, οι Alshamrani κ.α απαριθμούν πολλαπλούς τρόπους που έχουν ήδη προταθεί από τους ειδικούς κυβερνοασφάλειας και βασίζονται σε διάφορες τεχνολογίες όπως μηχανική μάθηση, εργαλεία ανάλυσης των φαινομενικά αξιόπιστων λογισμικών και σε σύγχρονες κάρτες γραφικών.

Παρακολούθηση Πακέτων

Η πιο κρίσιμη φάση του κύκλου ζωής μιας επίθεσης τύπου APT είναι η επικοινωνία με το κέντρο διοίκησης και ελέγχου (C2, C&C). Μέσω αυτής της επικοινωνίας, οι δράστες καταφέρνουν και καθοδηγούν το κακόβουλο λογισμικό δίνοντας τις κατάλληλες εντολές ενώ παράλληλα επιτυγχάνεται και η μεταφορά των κλεμμένων δεδομένων και πληροφοριών. Η παρακολούθηση σε επίπεδο τελικού συστήματος για τυχόν πακέτα δικτύου με ασυνήθιστες διευθύνσεις προορισμού, πακέτα με μη φυσιολογικό μέγεθος payload και μεγάλο αριθμό πακέτων που αποστέλλονται σε συγκεκριμένη διεύθυνση IP, θα βοηθούσε στον εντοπισμό οποιασδήποτε παράνομης δραστηριότητας και συμπεριφοράς από το εσωτερικό του δικτύου του οργανισμού-στόχου.

Παρακολούθηση αρχείων καταγραφής

Στην έρευνα, οι συγγραφείς προτείνουν ως ακόμη ένα μέτρο προστασίας από επιθέσεις τύπου APT τα αρχεία καταγραφής (Logs). Κρίνουν πως η αξία τους δεν περιορίζεται μόνο στα πλαίσια μια εγκληματολογικής ανάλυσης και έρευνας, αλλά αν χρησιμοποιηθούν κατάλληλα μπορούν να βοηθήσουν στην ανίχνευση και στην πρόληψη επιθέσεων στα αρχικά τους στάδια. Τα αρχεία αυτά, καταγράφουν πληροφορίες σχετικά με την μνήμη, την χρήση CPU, εφαρμογές, το σύστημα και άλλα, με αποτέλεσμα να παρέχουν έναν τεράστιο όγκο χρήσιμων πληροφοριών που θα βοηθούσαν στην άμυνα των συστημάτων και των δικτύων του οργανισμού απέναντι σε άγνωστες επιθέσεις.

4.3 Μέθοδοι ανίχνευσης

Οι τεχνικές για την ανίχνευση APT ταξινομούνται σε αυτές που βασίζονται στην ανίχνευση ανωμαλιών και σε αυτές που βασίζονται στην ανίχνευση με αντιστοίχιση προτύπων.

Ανίχνευση ανωμαλιών

Η ανίχνευση ανωμαλιών είναι ο εντοπισμός εκείνων των γεγονότων που δεν συμμορφώνονται με ένα αναμενόμενο μοτίβο άλλων στοιχείων σε ένα σύνολο δεδομένων. Ο

κύριος στόχος της ανίχνευσης ανωμαλιών είναι η στόχευση οποιουδήποτε συμβάντος που δεν εμπίπτει σε ένα προκαθορισμένο σύνολο φυσιολογικών συμπεριφορών. Οι τεχνικές μηχανικής μάθησης διαδραματίζουν σημαντικό ρόλο στην δημιουργία φυσιολογικών προφίλ και για αυτό χρησιμοποιούνται πολύ στην ανίχνευση εισβολών σε συστήματα όπου εφαρμόζονται τεχνικές ανίχνευσης ανωμαλιών. Υπάρχουν επιβλεπόμενες και μη επιβλεπόμενες τεχνικές ανίχνευσης. Οι μη επιβλεπόμενες τεχνικές ανίχνευσης ανωμαλιών απαιτούν μη επισημασμένα (unlabeled) δεδομένα δοκιμής, με την υπόθεση ότι πολλές από τις περιπτώσεις στο σύνολο δεδομένων είναι φυσιολογικές, αναζητώντας περιπτώσεις που φαίνεται να ταιριάζουν λιγότερο με το υπόλοιπο του συνόλου δεδομένων. Ενώ οι τεχνικές ανίχνευσης ανωμαλιών με επίβλεψη απαιτούν ένα σύνολο δεδομένων με ετικέτες που έχουν επισημανθεί ως «κανονικό» και «κακόβουλο» και περιλαμβάνει την εκπαίδευση ενός ταξινομητή [96].

Στο προηγούμενο κεφάλαιο, εξάχθηκε το πόρισμα πως οι δράστες APT είναι κατάλληλα καταρτισμένοι και ικανοί ώστε να προσαρμόζονται στις προσπάθειες του θύματος να αμυνθεί. Παράλληλα, παρατηρήθηκε πως σε αρκετές περιπτώσεις τα ιομορφικά λογισμικά που φορτώθηκαν στα συστήματα των οργανισμών-στόχων, εμπεριείχαν μηχανισμούς αναζήτησης των λύσεων ασφαλείας του μολυσμένου μηχανήματος, με σκοπό την κατάλληλη προσαρμογή του κώδικα τους ώστε να αποφύγουν να εντοπιστούν. Αδιαμφισβήτητα, λόγω της προηγμένης φύσης μιας τέτοιας επίθεσης, πάντα οι δράστες θα βρίσκουν τρόπο να παρακάμψουν της κλασσικές μεθόδους άμυνας. Για παράδειγμα, στην πλειοψηφία των αναλυθέντων επιθέσεων του 3^{ου} κεφαλαίου, εντοπίστηκαν νόμιμες ψηφιακές υπογραφές που κατάφερναν να παρακάμψουν εργαλεία anti-malware. Επομένως, κρίνεται απαραίτητη η ύπαρξη αμυντικών μεθόδων οι οποίες να συλλέγουν δεδομένα από διάφορες πηγές, να μαθαίνουν από αυτά και να κάνουν προβλέψεις επί των συλλεχθέντων δεδομένων, με σκοπό να εκτιμηθεί και να ανταποκριθεί σε μια μελλοντική πιθανή επίθεση. Όσο νωρίτερα εντοπιστούν οι επιθέσεις τύπου APT, τόσο καλύτερη θα είναι και η κατάσταση του οργανισμού-στόχου.

Μέσω της αυτοματοποίησης των μεθόδων ανίχνευσης ανωμαλιών που παρακολουθούν, μαθαίνουν, εκπαιδεύουν και ενημερώνουν συνεχώς τα μοντέλα μάθησης, είναι δυνατό να εντοπιστούν ακόμη και μικρές αλλαγές που είναι εξαιρετικά δύσκολο να παρατηρηθούν από ανθρώπινους φορείς. Τεχνικές όπως η μηχανική μάθηση, τα Perceptrons, τα νευρωνικά δίκτυα, τα Centroids, τα δυαδικά δέντρα αποφάσεων, η βαθιά μάθηση και άλλα, μπορούν να βοηθήσουν στην επεξεργασία εκατομμυρίων σημείων δεδομένων κάθε λεπτό για να καθορίσουν την κανονική συμπεριφορά και τις ανωμαλίες. Ωστόσο, οι συγγραφείς τονίζουν πως δεν αρκεί μόνο μια τεχνική ή μέθοδος ανίχνευσης ανωμαλιών για να ανιχνευτούν οι επιθέσεις APT.

Ανίχνευση με αντιστοίχιση προτύπων

Η αντιστοίχιση προτύπων είναι μια παλιά τεχνική που χρησιμοποιούν τα συστήματα Intrusion Detection (IDS) και Intrusion Prevention (IPS). Η ανίχνευση λειτουργεί εντοπίζοντας κακόβουλες συμπεριφορές και δραστηριότητες μέσω της παρατήρησης των μοτίβων της συμπεριφορά μιας διεργασίας ή εφαρμογής. Στην συνέχεια, οι συγγραφείς απαριθμούν ενδεικτικές μεθόδους που έχουν προταθεί από την επιστημονική κοινότητα οι οποίες βασίζονται σε τεχνικές

επεξεργασίας φυσικής γλώσσας (Natural Language Processing, NLP), σε αρχεία καταγραφής συμβάντων, σε δείκτες επιπέδου κινδύνου και εμπιστοσύνης κ.α.

4.4 Προληπτικές τεχνικές μετριασμού

Οι προληπτικές μέθοδοι μετριασμού βασίζονται σε τεχνικές που μπορούν να εξαπατήσουν τον επιτιθέμενο ή να αλλάξουν την επιφάνεια της επίθεσης με σκοπό να αυξηθούν τα επίπεδα δυσκολίας και πολυπλοκότητας για τον δράστη. Συγκεκριμένα, οι τεχνικές κατηγοριοποιούνται σύμφωνα με τους συγγραφείς της έρευνας στις εξής ομάδες: Honeypot & Honeynet, Moving Target Defense (MTD).

Στρατηγικές Honeypot & Honeynet

Το Honeypot είναι ένας μηχανισμός κυβερνοασφάλειας που χρησιμοποιεί έναν κατασκευασμένο στόχο επίθεσης για να παρασύρει τους επιτιθέμενους μακριά από τους πραγματικούς στόχους τους. Παράλληλα, συλλέγουν πληροφορίες σχετικά με την ταυτότητα, τις μεθόδους και τα κίνητρα των αντιπάλων. Αυτή η τεχνολογία, μπορεί να διαμορφωθεί με πολλαπλούς τρόπους, συμπεριλαμβανομένων εφαρμογών, λογισμικών, διακομιστών κ.α. Σχεδιάζεται σκόπιμα ώστε να μοιάζει με τον νόμιμο πραγματικό στόχο και προσπαθεί να πείσει τους επιτιθέμενους πως έχουν καταφέρει να αποκτήσουν πρόσβαση στα πραγματικά συστήματα του οργανισμού-στόχου τους. Ομοίως, ένα honeynet αποτελεί ένα δίκτυο δόλωμα που περιέχει όλα τα χαρακτηριστικά ενός πραγματικού δικτύου, όπως δρομολογητές, βάσεις δεδομένων, διακομιστές και άλλα ψηφιακά περιουσιακά στοιχεία. Στόχος του, όπως και του honeypot, είναι να προσελκύσει και να ξεγελάσει τους επιτιθέμενους με σκοπό την συγκέντρωση διαφόρων πολύτιμων πληροφοριών [97].

Σε αυτήν την προτεινόμενη μεθοδολογία άμυνας, οι συγγραφείς θεωρούν πως η εξαπάτηση των επιτιθέμενων με την δημιουργία δολωμάτων πολλαπλών μορφών μπορεί να οδηγήσει στην ευκολότερη ανίχνευση προηγμένων επίμονων απειλών που κινούνται στο δίκτυο των συστημάτων του οργανισμού. Πιο συγκεκριμένα, παρουσιάζονται λύσεις όπως η αυτοματοποιημένη δημιουργία και προσθήκη εγγράφων δολωμάτων σε συστήματα-δολώματα όπου όταν ανοιχτούν με ψεύτικα διαπιστευτήρια θα ενεργοποιηθεί ένας κατάλληλος συναγερμός που θα προδώσει τον κακόβουλο χρήστη.

Είναι χρήσιμο να τονιστεί επίσης ότι υπάρχουν ποικίλα είδη και τύποι honeypot που μπορούν να αξιοποιηθούν για τον εντοπισμό διαφορετικών τύπων απειλών. Αναλυτικότερα [98], υπάρχουν οι παγίδες ηλεκτρονικού ταχυδρομείου ή παγίδες spam οι οποίες τοποθετούν μια ψεύτικη διεύθυνση ηλεκτρονικού ταχυδρομείου σε μια κρυφή θέση όπου μόνο ένας αυτόματος συλλέκτης διευθύνσεων μπορεί να βρει. Με αυτόν τον τρόπο, οποιοδήποτε μήνυμα σταλθεί στην συγκεκριμένη διεύθυνση κατευθείαν αναγνωρίζεται ως spam. Επίσης, χρήσιμα μπορούν να φανούν και τα honeypot κακόβουλου λογισμικού, τα οποία μιμούνται εφαρμογές και API που

προσκαλούν επιθέσεις με κακόβουλο λογισμικό και με αυτόν τον τρόπο γίνεται ευκολότερος ο εντοπισμός και η ανάλυση τους.

Σύμφωνα με την εταιρεία κυβερνοασφάλειας Kaspersky [98], παρά τα πολλαπλά θετικά τους στοιχεία και την χρησιμότητα τους, υπάρχουν και ορισμένα αρνητικά. Είναι σύνηθες πολλοί οργανισμοί να θεωρούν πως επειδή τα honeypots, honeynets κλπ. που έχουν αξιοποιήσει, δεν έχουν καταγράψει κάποιο ίχνος απειλής, η απειλή δεν υφίσταται. Επιπροσθέτως, ένας έξυπνος επιτιθέμενος θα μπορούσε να χρησιμοποιήσει ένα honeypot ως σημείο εισόδου στα συστήματα ενός οργανισμού και για αυτόν τον λόγο τα αντίμετρα αυτά δεν μπορούν και ούτε πρέπει να αντικαταστήσουν άλλους επαρκείς ελέγχους ασφαλείας όπως τα firewalls και τα IDS.

Moving Target Defense

Οι άμυνες κινητού στόχου (MTD) είναι μια συλλογή τεχνολογιών που επιδιώκουν την βελτίωση της ασφάλειας και την αύξηση της ανθεκτικότητας και της διαθεσιμότητας μιας εφαρμογής μέσω της αύξησης της ποικιλομορφίας των διαδρομών λογισμικού και δικτύου. Αυτό επιτυγχάνεται αλλάζοντας δυναμικά το λογισμικό που χρησιμοποιείται για διαφορετικά επίπεδα της στοίβας του συστήματος ενώ εκτελείται μια εφαρμογή. Αυτό δίνει στους επιτιθέμενους μια τυχαία και διαρκώς μεταβαλλόμενη άποψη του υποκείμενου συστήματος, αυξάνοντας έτσι την δυσκολία των επιτυχημένων εκμεταλλεύσεων και την απαιτούμενη προσπάθεια, ενώ ταυτόχρονα καθιστά την επιμονή πιο δύσκολη και τελικά τους αποτρέπει από περαιτέρω επιθέσεις. Το διεπιστημονικό ερευνητικό κέντρο επιστήμης και μηχανικής Argonne έχει επί του παρόντος αναπτύξει πολλαπλά έργα MTD που στοχεύουν σε διάφορα επίπεδα του συστήματος [99]. Ενδεικτικά μοντέλα που ανέπτυξαν και προτείνουν ακολουθούν παρακάτω:

- *Multiple Operating System Rotational Environment (MORE)*: Το MORE είναι ένα πρόγραμμα που ελέγχει πολλαπλές μηχανές που εκτελούν ένα διαφορετικό σύνολο λειτουργικών συστημάτων. Αυτά τα λειτουργικά συστήματα εξυπηρετούν το ίδιο περιεχόμενο καθιστώντας την εναλλαγή τους διαφανή για τον τελικό χρήστη. Σε περίπτωση που ένας επιτιθέμενος καταφέρει να εκμεταλλευτεί επιτυχώς ένα από τα μηχανήματα που σερβίρουν περιεχόμενο, θα τεθεί εκτός εναλλαγής προκειμένου να απομονωθεί η περαιτέρω αλληλεπίδραση οποιουδήποτε χρήστη με ένα ευάλωτο μηχάνημα.
- *Dynamic Application Rotation Environment (DARE)*: Το DARE είναι ένα έργο που εναλλάσσει το λογισμικό που παρέχει την ίδια υπηρεσία σε έναν κεντρικό υπολογιστή. Η τρέχουσα έρευνα του Argonne περιλαμβάνει την εναλλαγή διακομιστών ιστού προκειμένου να παρέχεται ανθεκτικότητα απέναντι σε εκμεταλλεύσεις που θέτουν σε κίνδυνο την απόδοση ή την ασφάλεια. Με την εναλλαγή του λογισμικού που εξυπηρετεί τους χρήστες, μια εκμετάλλευση ενός από τα κομμάτια του λογισμικού που εναλλάσσονται μπορεί να μετριαστεί με την μείωση της έκθεσης του ευάλωτου λογισμικού σε επιτιθέμενους.
- *Stream Splitting:* Σκοπός του διαχωρισμού ροής είναι η διερεύνηση και ο σχεδιασμός μιας τεχνικής άμυνας κινούμενου στόχου TCP με τον διαχωρισμό του ωφέλιμου φορτίου

δεδομένων σε πολλαπλές ροές TCP, καθιστώντας δύσκολο για τον επιτιθέμενο να αποκτήσει πρόσβαση σε ολόκληρο το ωφέλιμο φορτίο επικοινωνίας και να αποκτήσει σημαντικές πληροφορίες. Είναι ένα έργο που στέλνει δεδομένα σε πολλαπλά διαφορετικά μέσα (κυψελοειδή, οπτικές ίνες, ραδιόφωνο, DSL) προκειμένου να παρέχει πλεονάζουσες συνδέσεις με το διαδίκτυο, να αποτρέπει τη συσχέτιση της κίνησης μεταξύ των κεντρικών υπολογιστών με την χρήση ενδιάμεσων κόμβων και τον μετριασμό της χρήσιμης κίνησης εμποδίζοντας κάθε σύνδεσμο από το να έχει όλα τα περιεχόμενα μιας δικτυακής επικοινωνίας. Στο σενάριο όπου ένας από τους συνδέσμους περιορίζεται ή αποτυγχάνει, ο διαχωρισμός ροής έχει την δυνατότητα να ανακατευθύνει αυτόματα την κυκλοφορία μέσω συνδέσμων υψηλότερου εύρους ζώνης, έτσι ώστε να διατηρηθεί η συνδεσιμότητα και η διαθεσιμότητα. Ο διαχωρισμός ροής καθιστά πιο δύσκολο για έναν εισβολέα να αποκτήσει όλα τα κομμάτια μιας επικοινωνίας, καθώς απαιτείται να έχει πρόσβαση σε όλους τους συνδέσμους που χρησιμοποιούνται στην διαίρεση της ροής, προκειμένου να επανασυνθέσουν το πλήρες μήνυμα.

- *Honeybadger*: Η προληπτική άμυνα Honeybadger χρησιμοποιεί έναν μεταγωγέα SDN (Software Defined Networking) για να αναλύει την κυκλοφορία των χρηστών και να εκτρέπει την κυκλοφορία των επιτιθέμενων σε ένα δίκτυο honeypot για να περιορίσει την αλληλεπίδραση τους με ευάλωτους διακομιστές παραγωγής και την πιθανή τους εκμετάλλευση.

Τέλος, ένας τρόπος ταξινόμησης των τεχνικών MTD που βασίζεται στην υλοποίηση της στοίβας πρωτοκόλλων είναι ο εξής [86]:

- *Network Level MTD*: Περιλαμβάνει την αλλαγή στην τοπολογία του δικτύου, π.χ. αλλαγή και μεταπήδηση διευθύνσεων IP, απόκρυψη κίνησης κλπ.
- *Host Level MTD*: Απαιτεί την αλλαγή στους πόρους του host, στο λειτουργικό σύστημα, μετονομασία ρυθμίσεων κ.α.
- *Application Level MTD*: Περιλαμβάνει την αλλαγή του πηγαίου κώδικα, της αντίστοιχης μνήμης και έκδοσης λογισμικού εφαρμογών.

4.5 Αντίμετρα επιθέσεων Supply-Chain

Σύμφωνα με τον CISA [100], μια επίθεση στην αλυσίδα εφοδιασμού λογισμικού συμβαίνει όταν ένας επιτιθέμενος διεισδύσει στο δίκτυο ενός προμηθευτή λογισμικού και χρησιμοποιεί κακόβουλο κώδικα για να θέσει σε κίνδυνο το λογισμικό πριν ο πωλητής το στείλει στους πελάτες του. Το παραβιασμένο λογισμικό θέτει στην συνέχεια σε κίνδυνο τα δεδομένα ή το σύστημα του πελάτη. Το νεοαποκτηθέν λογισμικό μπορεί να είναι εξαρχής εκτεθειμένο σε κίνδυνο, ή ο κίνδυνος μπορεί να προκύψει από κάποια ενημέρωση. Αυτού του είδους οι επιθέσεις επηρεάζουν όλους τους χρήστες του εκτεθειμένου λογισμικού και μπορεί να έχουν εκτεταμένες συνέπειες σε κυβερνήσεις, κρίσιμες υποδομές και για πελάτες λογισμικού του ιδιωτικού τομέα.

Λόγω της δυσκολίας μετριασμού των συνεπειών μετά από μία επίθεση, οι αμυνόμενοι θα πρέπει να τηρούν τις βέλτιστες πρακτικές ασφαλείας πριν από την εκδήλωση μιας τέτοιας

επίθεσης. Η εφαρμογή βέλτιστων πρακτικών θα ενισχύσει την ικανότητα ενός οργανισμού να προλαμβάνει, να μετριάζει και να ανταποκρίνεται σε επιθέσεις supply-chain. Παρακάτω παρουσιάζονται ενδεικτικά αντίμετρα και ενέργειες που προτείνονται για την αντιμετώπιση παρόμοιων επιθέσεων [101]:

1. Οι αμυνόμενοι οργανισμοί θα πρέπει να υιοθετήσουν τους πιο πρόσφατους αμυντικούς μηχανισμούς, όπως τα λογισμικά ανίχνευσης και προστασίας ιών (anti-virus), τείχη προστασίας, τεχνολογίες ασφάλειας τερματικών σημείων, βασισμένα στην τεχνητή νοημοσύνη συστήματα ανίχνευσης ανωμαλιών, αυτόματους και συνεχείς ελέγχους διείσδυσης. Παράλληλα, πρέπει να βεβαιώνονται πως όλα τα λογισμικά που χρησιμοποιούνται εντός του οργανισμού είναι ενημερωμένα για την επιδιόρθωση τυχόν τρωτοτήτων που μπορούν να οδηγήσουν σε παραβιάσεις δεδομένων.
2. Σοφή χρήση των σύγχρονων τεχνολογιών. Οι πιο σύγχρονες τεχνολογίες πλέον εξαρτώνται σε τεράστιο βαθμό από την τεχνητή νοημοσύνη και την μηχανική μάθηση για την ανάλυση μεγάλων όγκων δεδομένων για την παροχή χρήσιμων πληροφοριών στους ειδικούς.
3. Προστασία δεδομένων. Ακόμη ένα σημαντικό αντίμετρο που έχει αναφερθεί και στις προηγούμενες ενότητες αποτελεί η κρυπτογράφηση όλων των δεδομένων, είτε βρίσκονται σε κατάσταση «ηρεμίας» είτε μεταφέρονται ενεργά. Ωστόσο, για την μέγιστη ασφάλεια, οφείλουν και οι συνεργάτες/πάροχοι/συνέταιροι του οργανισμού που αμύνεται να εφαρμόσουν τα ίδια πρότυπα ασφαλείας.
4. Υιοθέτηση decentralized τεχνικών ανταλλαγής δεδομένων όπως τα blockchains που παρέχουν ένα ασφαλές δίκτυο για την ανταλλαγή δεδομένων με την πρόσθετη ασφάλεια της αμεταβλητότητας και της ανθεκτικότητας.
5. Ασφαλής αποθήκευση δεδομένων. Αποθήκευση κρίσιμων δεδομένων σε ασφαλείς τοποθεσίες με κατάλληλη προστασία (π.χ. πιστοποίηση ταυτότητας, έλεγχος πρόσβασης).

Επιπροσθέτως, η εταιρεία UpGuard προτείνει τους εξής τρόπους αντιμετώπισης επιθέσεων supply-chain [102]:

6. Ασφαλής διαχείριση προνομιακής πρόσβασης. Με στόχο την διατάραξη της κοινής πορείας (αναζήτηση προνομιακών λογαριασμών και πλευρικές κινήσεις) που ακολουθούν οι περισσότεροι κυβερνοεγκληματίες αφότου έχουν εισβάλλει σε έναν οργανισμό, προτείνεται ένα αποτελεσματικό πλαίσιο διαχείρισης προνομιακών δικαιωμάτων πρόσβασης (Privileged Access Management – PAM).
7. Ανίχνευση διαρροών δεδομένων προμηθευτών. Με την εφαρμογή μιας τέτοιας λύσης, οι διαρροές των προμηθευτών μπορούν να εντοπιστούν και να αποκατασταθούν πριν έχουν την ευκαιρία να αξιοποιηθούν από επιτιθέμενους για επιθέσεις αλυσίδας εφοδιασμού.
8. Εφαρμογή αρχιτεκτονικής μηδενικής εμπιστοσύνης (ZTA). Μια αρχιτεκτονική μηδενικής εμπιστοσύνης υποθέτει ότι όλες οι δραστηριότητες δικτύου είναι εξ

ορισμού κακόβουλες. Μόνο αφότου κάθε αίτημα σύνδεσης περάσει από έναν αυστηρό κατάλογο πολιτικών, επιτρέπεται η πρόσβαση σε πνευματική ιδιοκτησία.

9. Τακτικό Risk Assessment από τρίτους. Οι αξιολογήσεις κινδύνου από τρίτους βοηθούν στην καλύτερη κατανόηση της κατάστασης της ασφάλειας ενός οργανισμού και αποκαλύπτονται και τυχόν τρωτότητες που χρήζουν διόρθωση και αποκατάσταση.

5. Συμπεράσματα και προτάσεις για μελλοντική έρευνα

Στην παρούσα έρευνα, μελετήθηκαν σε βάθος οι έννοιες γύρω από τον όρο «προηγμένη επίμονη απειλή», συμπεριλαμβανομένου του μοντέλου του κύκλου ζωής, της ανατομίας και των μεθόδων του. Παρουσιάστηκαν και αναλύθηκαν επιλεγμένες επιθέσεις κατά την διάρκεια 2015-2022 και βάσει αυτών ερευνήθηκαν οι διάφορες μεθοδολογίες, τεχνικές και στρατηγικές που οι επιτιθέμενοι προσεκτικά επέλεγαν κατά το πέρασμα του χρόνου. Δεδομένου των πολλαπλών μονοπατιών επίθεσης που παρατηρήθηκαν, στο τέλος της έρευνας προτάθηκαν ενδεικτικά αντίμετρα που βασίζονται στα μοτίβα των διαδικασιών των APT που εξάχθηκαν.

Διαπιστώθηκε από την πρώτη στιγμή, πως οι επιθέσεις τύπου APT είναι εξελιγμένες, συγκεκριμένες και βρίσκονται συνεχώς σε μια ροή ανάπτυξης. Οι τεχνικές και μεθοδολογίες που χρησιμοποιούνται διακρίνονται για την πολυπλοκότητά τους και αποδεικνύουν το εντυπωσιακό τεχνικό και γνωστικό επίπεδο των φορέων που αναλαμβάνουν επιθέσεις τέτοιου είδους και κλίμακας. Στην παρούσα έρευνα, έπειτα από ανάλυση, εντοπίστηκαν κοινά μονοπάτια και χαρακτηριστικά μεταξύ αυτών των επιθέσεων. Πιο συγκεκριμένα, διαπιστώθηκε πως οι επιτιθέμενοι προτιμούσαν τεχνικές κοινωνικής μηχανικής και OSINT για να συλλέξουν κρίσιμα δεδομένα και πληροφορίες σχετικά με τους στόχους τους και πως στην συντριπτική πλειοψηφία των επιθέσεων, το δημοφιλέστερο μέσο μετάδοσης του κακόβουλου λογισμικού ήταν το spear-phishing. Με αυτά τα κατάλληλα προσαρμοσμένα μηνύματα ηλεκτρονικού ταχυδρομείου, οι φορείς APT κατάφερναν να ξεγελάσουν τα θύματα τους στο να ανοίξουν και να τρέξουν το κακόβουλο συνημμένο αρχείο. Μόλις εκτελεστεί, το κακόβουλο λογισμικό εκμεταλλεύεται μια τρωτότητα της εφαρμογής ανοίγματος του αρχείου, με αποτέλεσμα οι επιτιθέμενοι να αποκτούν πρόσβαση στα συστήματα του στόχου.

Σε δεύτερη φάση, παρατηρήθηκε η τάση των δραστών να επιχειρούν να εδραιώσουν την παρουσία τους στα μολυσμένα μηχανήματα. Συνήθως, αφότου έχει εγκατασταθεί το κακόβουλο λογισμικό στο μηχάνημα-στόχο, οι επιτιθέμενοι δημιουργούν κατάλληλες κερκόπορτες που υποστηρίζουν πολλαπλές χρήσιμες λειτουργίες, συμπεριλαμβανομένης και της επικοινωνίας με τους διακομιστές διοίκησης και ελέγχου (C2). Παρατηρήθηκε πως σχεδόν σε όλες τις επιθέσεις, το κακόβουλο λογισμικό κατάφερε να δημιουργήσει κανάλια επικοινωνίας με τους διακομιστές C2 των επιτιθέμενων, καθώς αποτελεί ένα βήμα ζωτικής σημασίας για μια επίθεση APT. Επιπλέον, εντοπίστηκαν πολλαπλές τεχνικές αποφυγής ανίχνευσης της παράνομης διαδικτυακής δραστηριότητας μεταξύ των κερκόπορτων και των διακομιστών C2, όπως η επικοινωνία μέσω Tor, μέσω πρωτοκόλλων HTTP, HTTPS, SSH, DNS, DDNS, ο περιορισμός της επικοινωνίας μόνο σε ώρες εκτός λειτουργίας κ.α. Παράλληλα, μια συνηθισμένη και σημαντική τακτική που παρατηρήθηκε είναι η επέκταση της πρόσβασης των επιτιθέμενων σε ολόκληρο το δίκτυο του στόχου και περιλάμβανε τεχνικές κάθετης κλιμάκωσης προνομίων, κλοπή στοιχειών και διαπιστευτηρίων, χρήση κατάλληλων λογισμικών κ.α.

Εν συνεχεία, εξάχθηκαν και μεθοδολογίες που φαίνεται πως οι περισσότεροι φορείς APT χρησιμοποιούσαν έντονα για να αποφύγουν την ανίχνευση τους από τις διάφορες λύσεις και προϊόντα ασφαλείας των στόχων τους. Ειδικότερα, σε πολλές από τις αναλυθέντες επιθέσεις οι δράστες εκμεταλλευόντουσαν νόμιμες εφαρμογές και υπογραφές των Windows και της Microsoft, με αποτέλεσμα να δυσχεραίνεται η ανίχνευση κακόβουλης δραστηριότητας. Επιπροσθέτως, εντός

των κακόβουλων λογισμικών εντοπίστηκαν και προηγμένες λειτουργίες anti-analysis, anti-forensics, anti-sandboxing, καθώς και λειτουργίες διαγραφής αρχείων καταγραφής συμβάντων. Αξίζει, επιπλέον, να αναφερθεί η έντονη χρήση κρυπτογράφησης στην πλειοψηφία των επιθέσεων που καταγράφηκαν. Με επικρατέστερη μέθοδο κρυπτογράφησης αυτή με την χρήση της πράξης XOR, οι δράστες κρυπτογραφούσαν τις επικοινωνίες και τα κακόβουλα λογισμικά τους. Επιπλέον, εξάχθηκε και το πόρισμα πως στην πλειοψηφία τους οι επιθέσεις στόχευαν στην συλλογή πληροφοριών και στην μακροχρόνια κατασκοπεία και παρακολούθηση του στόχου. Βέβαια, σε πολλές κυβερνοεπιθέσεις οι στόχοι δεν είναι πάντοτε προφανείς και συνήθως δεν εμπίπτουν μονάχα σε μια κατηγορία.

Είναι προφανές πως οι προηγμένες επίμονες απειλές υπήρχαν, υπάρχουν, και θα συνεχίσουν να υφίστανται μελλοντικά. Αποτελούν έναν τεράστιο κίνδυνο που παραμονεύει οποιαδήποτε χρονική στιγμή και απειλεί ταυτόχρονα κυβερνήσεις, οργανισμούς, επιχειρήσεις, πολίτες, ενώ παράλληλα ο αντίκτυπος μιας επίθεσης τέτοιας κλίμακας και είδους πέρα από ψηφιακές, μπορεί να προκαλέσει και φυσικές ζημιές, πάντοτε με τον κίνδυνο να χαθούν ακόμη και ανθρώπινες ζωές. Ολοένα και περισσότερες άρτια οργανωμένες, συνεχώς εξελισσόμενες και πιθανώς κρατικά χορηγούμενες επιθέσεις λαμβάνουν χώρα στον κυβερνοχώρο καθημερινά, και δεδομένου του επιπέδου της κατάρτισης των φορέων που αναλαμβάνουν τέτοιες επιχειρήσεις είναι λογικό να μην αποτελεί ρεαλιστικό σενάριο η πλήρης άμυνα και αντιμετώπιση τέτοιων απειλών. Ακόμη και κυβερνητικοί φορείς και οργανισμοί μεγάλης κλίμακας αδυνατούν να αντιμετωπίσουν τις πολύπλοκες μεθόδους και τεχνικές όπως η εκμετάλλευση μιας τρωτότητας zero-day. Τα συνηθισμένα προϊόντα και όλες οι πρακτικές ασφαλείας που υιοθετούν αυτοί οι οργανισμοί μπορεί να τύχει να ανιχνεύσουν έγκαιρα ή και να μετριάσουν τον αντίκτυπο μιας τέτοιας επίθεσης, παρόλα αυτά, κανένα σύστημα δεν μπορεί να θεωρηθεί «ασφαλές».

Βάσει των παραπάνω συμπερασμάτων, το πρώτο και κυριότερο μέτρο ενάντια στις προηγμένες επίμονες απειλές είναι η σωστή και πλήρης εφαρμογή των τυπικών μέτρων ασφαλείας. Ωστόσο, η επιστημονική κοινότητα και οι ειδικοί της ασφάλειας στον κυβερνοχώρο, έχουν την δυνατότητα να επεκτείνουν τις έρευνες επάνω στην ανίχνευση και την μετρίαση επιθέσεων τύπου APT. Ήδη, υπάρχουν πολλών ειδών έρευνες και τεχνολογίες οι οποίες αξιοποιούν τον κλάδο της τεχνητής νοημοσύνης και συγκεκριμένα τεχνικές μηχανικής και βαθιάς μάθησης που στοχεύουν στον έγκαιρο εντοπισμό ανωμαλιών. Παρόλα αυτά, απαιτείται ένα ολοκληρωμένο πολυδιάστατο πλαίσιο, το οποίο να εμπεριέχει τα πλεονεκτήματα όλων των σύγχρονων προϊόντων ασφαλείας με τα οποία θα κάλυπτε μια σημαντικά μεγαλύτερη επιφάνεια επίθεσης και ταυτόχρονα θα βοηθούσε τα κέντρα επιχειρήσεων ασφαλείας να διερευνούν και να ανταποκρίνονται ταχύτερα και πιο αποτελεσματικά στα διάφορα στάδια των προηγμένων απειλών που εμφανίζονται. Επιπροσθέτως, η συλλογή και ανάλυση των πολλαπλών μεθοδολογιών και τακτικών που αξιοποιούν οι δράστες APT, με σκοπό την συνεχή ενημέρωση και τροποποίηση των γνωστών αντιμέτρων, κρίνεται απαραίτητη και αποτελεί ένα σημαντικό μέρος της αντιμετώπισης των προηγμένων επίμονων απειλών.

Βιβλιογραφία

[1] "What is Cybersecurity? | CISA." https://www.cisa.gov/uscert/ncas/tips/ST04-001 (accessed Jul. 23, 2022).

[2] "Ασφάλεια Πληροφοριακών Συστημάτων." https://www.infosec.aueb.gr/index.php/2009-01-24-13-20-46/2009-01-24-14-53-55/2015-12-20-19-16-12 (accessed Jul. 23, 2022).

[3] "Microsoft report shows increasing sophistication of cyber threats," *Microsoft On the Issues*, Sep. 29, 2020. https://blogs.microsoft.com/on-the-issues/2020/09/29/microsoft-digital-defense-report-cyber-threats/ (accessed Aug. 27, 2022).

[4] "How Many People Use the Internet in 2022? [Feb 2022 Update]." https://www.oberlo.com/statistics/how-many-people-use-internet (accessed Jul. 23, 2022).

[5] "Top 14 Most Common Cyber Attacks Today | CrowdStrike," *crowdstrike.com*. https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-cyberattacks/ (accessed Jul. 23, 2022).

[6] "2022 Must-Know Cyber Attack Statistics and Trends | Embroker," Sep. 18, 2019. https://www.embroker.com/blog/cyber-attack-statistics/ (accessed Jul. 23, 2022).

[7] "Cybercrime To Cost The World $10.5 Trillion Annually By 2025," *Cybercrime Magazine*, Dec. 08, 2018. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/ (accessed Jul. 23, 2022).

[8] R. Schmidt, G. J. Rattray, and C. J. Fogle, "Methods and apparatus for developing cyber defense processes and a cadre of expertise," US20080167920A1, Jul. 10, 2008 Accessed: Jul. 25, 2022. [Online]. Available: https://patents.google.com/patent/US20080167920A1/en

[9] A. Ahmad, J. Webb, K. C. Desouza, and J. Boorman, "Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack," *Comput. Secur.*, vol. 86, pp. 402–418, Sep. 2019, doi: 10.1016/j.cose.2019.07.001.

[10] C. C. Editor, "advanced persistent threat (APT) - Glossary | CSRC." https://csrc.nist.gov/glossary/term/advanced_persistent_threat (accessed Jul. 25, 2022).

[11] "What Is APT and What Does It Want?," *What Is APT and What Does It Want?* https://taosecurity.blogspot.com/2010/01/what-is-apt-and-what-does-it-want.html (accessed Jul. 25, 2022).

[12] N. Virvilis-Kollitiris, "Fighting an unfair battle: unconventional defenses against advanced persistent threats," Οικονομικό Πανεπιστήμιο Αθηνών, Τμήμα Πληροφορικής, 2015. doi: 10.12681/eadd/36514.

[13] P. Chen, L. Desmet, and C. Huygens, "A Study on Advanced Persistent Threats," in *Communications and Multimedia Security*, Berlin, Heidelberg, 2014, pp. 63–72.

[14] A. Lemay, J. Calvet, F. Menet, and J. M. Fernandez, “Survey of publicly available reports on advanced persistent threat actors,” *Comput. Secur.*, vol. 72, pp. 26–59, Jan. 2018, doi: 10.1016/j.cose.2017.08.005.

[15] P. Nikkhah Bahrami, A. Dehghantanha, T. Dargahi, R. Parizi, K.-K. R. Choo, and H. Haj Seyyed Javadi, “Cyber Kill Chain-Based Taxonomy of Advanced Persistent Threat Actors: Analogy of Tactics, Techniques, and Procedures,” *J. Inf. Process. Syst.*, vol. 15, Mar. 2021, doi: 10.3745/JIPS.03.0126.

[16] “Defining Insider Threats | CISA.” https://www.cisa.gov/defining-insider-threats (accessed Jul. 26, 2022).

[17] “Protecting Against an Indirect Attack in Cyber Security,” *Verizon Enterprise*. https://enterprise.verizon.com/resources/articles/s/protecting-against-an-indirect-attack-in-cyber-security/ (accessed Jul. 26, 2022).

[18] Dell SecureWorks, “Lifecycle of the Advanced Persistent Threat.” http://docs.media.bitpipe.com/io_10x/io_105022/item_550605/Lifecycle_of_the_Advanced_Persistent_Threat%5B1%5D.pdf

[19] J. Ashiq, “Anatomy of an APT attack: Step by step approach,” *Infosec Resources*, 2018. https://resources.infosecinstitute.com/topic/anatomy-of-an-apt-attack-step-by-step-approach/ (accessed Feb. 23, 2022).

[20] “APT1: Exposing One of China’s Cyber Espionage Units,” *Mandiant*. https://www.mandiant.com/resources/apt1-exposing-one-of-chinas-cyber-espionage-units (accessed Jul. 25, 2022).

[21] “Home.” https://www.gsa.gov/ (accessed Sep. 02, 2022).

[22] “Threat Actors Master ‘False Flags’ Tactics to Deceive Victims and Security Teams,” *usa.kaspersky.com*, May 26, 2021. https://usa.kaspersky.com/about/press-releases/2016_threat-actors-master--false-flags-tactics-to-deceive-victims-and-security-teams (accessed Jul. 26, 2022).

[23] D. U. Case, “Analysis of the cyber attack on the Ukrainian power grid,” *Electr. Inf. Shar. Anal. Cent. E-ISAC*, vol. 388, pp. 1–29, 2016.

[24] “Cyber-Attack Against Ukrainian Critical Infrastructure | CISA.” https://www.cisa.gov/uscert/ics/alerts/IR-ALERT-H-16-056-01 (accessed Jun. 27, 2022).

[25] “Ukrainian Power Grid Attack - Blog,” *GlobalSign*, Oct. 28, 2020. https://www.globalsign.com/en/blog/cyber-autopsy-series-ukranian-power-grid-attack-makes-history (accessed Jun. 26, 2022).

[26] “Power grid cyberattack in Ukraine (2015),” *International cyber law: interactive toolkit*, Jun. 04, 2021. https://cyberlaw.ccdcoe.org/wiki/Power_grid_cyberattack_in_Ukraine_(2015) (accessed Jun. 26, 2022).

[27] J. Cox, “The Malware That Led to the Ukrainian Blackout,” *Vice*, Jan. 26, 2016. https://www.vice.com/en/article/wnx5yz/the-malware-that-led-to-the-ukrainian-blackout (accessed Jun. 30, 2022).

[28] J. Slowik, “Anatomy of an Attack: Detecting and Defeating CRASHOVERRIDE,” p. 23, 2018.

[29] “CrashOverride Malware | CISA.” https://www.cisa.gov/uscert/ncas/alerts/TA17-163A (accessed Jun. 28, 2022).

[30] A. Cherepanov, “A new threat for industrial control systems,” p. 17.

[31] “ELECTRUM | Dragos,” May 30, 2020. https://www.dragos.com/threat/electrum/ (accessed Jun. 28, 2022).

[32] “ANALYSIS: ATTACKING AND DEFENDING SWIFT SYSTEMS - SWIFT systems and the SWIFT Customer Security Program.” https://www.readkong.com/page/analysis-attacking-and-defending-swift-systems-swift-9666737 (accessed Aug. 20, 2022).

[33] “International Banks Are in Trouble: Bangladeshi Bank Attacks,” *Cybersecurity | Digital Forensics | Crypto Investigations*. https://ermprotect.com/blog/malware-bangladesh-bank-heist/ (accessed Jun. 29, 2022).

[34] “North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions,” Sep. 06, 2018. https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and (accessed Jun. 29, 2022).

[35] “Checkpoint_Domestic-Kitten-Iranian-Surveillance-Operation(09-07-2018).pdf | Powered by Box.” https://app.box.com/s/48z6mq7k6xlzicxbj9360eskrta92fbm (accessed Jun. 30, 2022).

[36] “Operation Cloud Hopper,” p. 25.

[37] A. Bendiek and M. Schulze, “Attribution: a major challenge for EU cyber sanctions: an analysis of WannaCry, NotPetya, Cloud Hopper, Bundestag Hack and the attack on the OPCW,” *SWP Res. Pap.*, 2021, doi: 10.18449/2021RP11.

[38] “Operation Cloud Hopper: What You Need to Know - Wiadomości bezpieczeństwa.” https://www.trendmicro.com/vinfo/pl/security/news/cyber-attacks/operation-cloud-hopper-what-you-need-to-know (accessed Jul. 04, 2022).

[39] “Chinese Hackers Indicted,” *Federal Bureau of Investigation*. https://www.fbi.gov/news/stories/chinese-hackers-indicted-122018 (accessed Jul. 04, 2022).

[40] “Attackers Deploy New ICS Attack Framework ‘TRITON’ and Cause Operational Disruption to Critical Infrastructure | Mandiant.” https://www.mandiant.com/resources/attackers-deploy-new-ics-attack-framework-triton (accessed Jul. 02, 2022).

[41] ro D. P.-Y. D. Aless, “TRITON: The First ICS Cyberattack on Safety Instrument Systems,” p. 28.

[42] “TRISIS: Analyzing Safety System Targeting Malware | Dragos,” Dec. 14, 2017. https://www.dragos.com/resource/trisis-analyzing-safety-system-targeting-malware/ (accessed Jul. 02, 2022).

[43] “TRITON Actor TTP Profile, Custom Attack Tools, Detections, and ATT&CK Mapping,” *Mandiant*. https://www.mandiant.com/resources/blog/triton-actor-ttp-profile-custom-attack-tools-detections (accessed Aug. 20, 2022).

[44] “Triton, Software S1009 | MITRE ATT&CK®.” https://attack.mitre.org/software/S1009/ (accessed Jul. 02, 2022).

[45] “NJCCIC Threat Profile TRISIS/TRITON.” https://www.cyber.nj.gov/threat-center/threat-profiles/ics-malware-variants/trisis-triton (accessed Jul. 02, 2022).

[46] C. Krasznay, “Case Study: The NotPetya Campaign,” 2020, pp. 485–499.

[47] LogRhythm, “NotPetya Technical Analysis,” *LogRhythm*, Jun. 30, 2017. https://logrhythm.com/blog/notpetya-technical-analysis/ (accessed Jul. 05, 2022).

[48] N. Biasini, “The MeDoc Connection.” http://blog.talosintelligence.com/2017/07/the-medoc-connection.html (accessed Jul. 05, 2022).

[49] “NotPetya Ransomware Attack [Technical Analysis].” https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/ (accessed Jul. 05, 2022).

[50] “Analysis of TeleBots’ cunning backdoor,” *WeLiveSecurity*, Jul. 04, 2017. https://www.welivesecurity.com/2017/07/04/analysis-of-telebots-cunning-backdoor/ (accessed Jul. 05, 2022).

[51] “Petya Ransomware | CISA.” https://www.cisa.gov/uscert/ncas/alerts/TA17-181A (accessed Jul. 05, 2022).

[52] S. Ingle, “Winter Olympics was hit by cyber-attack, officials confirm,” *The Guardian*, Feb. 11, 2018. Accessed: Jul. 06, 2022. [Online]. Available: https://www.theguardian.com/sport/2018/feb/11/winter-olympics-was-hit-by-cyber-attack-officials-confirm

[53] “Olympic Destroyer (2018),” *International cyber law: interactive toolkit*, Aug. 17, 2021. https://cyberlaw.ccdcoe.org/wiki/Olympic_Destroyer_(2018) (accessed Jul. 06, 2022).

[54] “OlympicDestroyer is here to trick the industry.” https://securelist.com/olympicdestroyer-is-here-to-trick-the-industry/84295/ (accessed Jul. 06, 2022).

[55] “NJCCIC Threat Profile Olympic Destroyer.” https://www.cyber.nj.gov/threat-center/threat-profiles/trojan-variants/olympic-destroyer (accessed Jul. 06, 2022).

[56] W. Mercer, “Olympic Destroyer Takes Aim At Winter Olympics.” http://blog.talosintelligence.com/2018/02/olympic-destroyer.html (accessed Jul. 06, 2022).

[57] “The devil’s in the Rich header.” https://securelist.com/the-devils-in-the-rich-header/84348/ (accessed Jul. 07, 2022).

[58] “UK exposes series of Russian cyber attacks against Olympic and Paralympic Games,” *GOV.UK*. https://www.gov.uk/government/news/uk-exposes-series-of-russian-cyber-attacks-against-olympic-and-paralympic-games (accessed Jul. 07, 2022).

[59] “Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace,” Oct. 19, 2020.

https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and (accessed Jul. 06, 2022).

[60] "Operation ShadowHammer." https://securelist.com/operation-shadowhammer/89992/ (accessed Jul. 09, 2022).

[61] "Operation ShadowHammer: A High Profile Supply Chain Attack." https://securelist.com/operation-shadowhammer-a-high-profile-supply-chain-attack/90380/ (accessed Jul. 09, 2022).

[62] ISSP, "Operation ShadowHammer," *ISSP Global*, Mar. 27, 2019. https://www.issp.com/post/operation-shadowhammer (accessed Jul. 09, 2022).

[63] "Operation ShadowHammer: new supply chain attack threatens hundreds of thousands of users worldwide," *www.kaspersky.com*, May 26, 2021. https://www.kaspersky.com/about/press-releases/2019_operation-shadowhammer-new-supply-chain-attack (accessed Jul. 09, 2022).

[64] "ShadowPad Malware Analysis." https://www.secureworks.com/research/shadowpad-malware-analysis (accessed Jul. 09, 2022).

[65] "The SolarWinds Cyberattack." https://www.rpc.senate.gov/policy-papers/the-solarwinds-cyberattack (accessed Jul. 08, 2022).

[66] "Cleaning up SolarWinds hack may cost as much as $100 billion," *Roll Call*, Jan. 11, 2021. https://www.rollcall.com/2021/01/11/cleaning-up-solarwinds-hack-may-cost-as-much-as-100-billion/ (accessed Jul. 08, 2022).

[67] "Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor | Mandiant." https://www.mandiant.com/resources/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor (accessed Jul. 08, 2022).

[68] "SUNBURST Additional Technical Details | Mandiant." https://www.mandiant.com/resources/sunburst-additional-technical-details (accessed Jul. 08, 2022).

[69] M. Willett, "Lessons of the SolarWinds Hack," *Survival*, vol. 63, no. 2, pp. 7–26, Mar. 2021, doi: 10.1080/00396338.2021.1906001.

[70] "Joint Statement by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA) | CISA." https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure (accessed Jul. 08, 2022).

[71] "Operation (노스 스타) North Star A Job Offer That's Too Good to be True?," *McAfee Blog*, Jul. 30, 2020. https://www.mcafee.com/blogs/other-blogs/mcafee-labs/operation-north-star-a-job-offer-thats-too-good-to-be-true/ (accessed Jul. 10, 2022).

[72] "Operation North Star: Summary Of Our Latest Analysis | McAfee Blogs." https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/operation-north-star-summary-of-our-latest-analysis.html (accessed Jul. 10, 2022).

[73] “Operation North Star: Behind The Scenes | McAfee Blogs.” https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/operation-north-star-behind-the-scenes.html (accessed Jul. 10, 2022).

[74] “Operation Spalax: Targeted malware attacks in Colombia,” *WeLiveSecurity*, Jan. 12, 2021. https://www.welivesecurity.com/2021/01/12/operation-spalax-targeted-malware-attacks-colombia/ (accessed Jul. 11, 2022).

[75] “PseudoManuscrypt: a mass-scale spyware attack campaign | Kaspersky ICS CERT,” Dec. 16, 2021. https://ics-cert.kaspersky.com/publications/pseudomanuscrypt-a-mass-scale-spyware-attack-campaign/ (accessed Jul. 12, 2022).

[76] “Industroyer2: Industroyer reloaded,” *WeLiveSecurity*, Apr. 12, 2022. https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ (accessed Jul. 13, 2022).

[77] “INDUSTROYER.V2: Old Malware Learns New Tricks | Mandiant.” https://www.mandiant.com/resources/industroyer-v2-old-malware-new-tricks (accessed Jul. 13, 2022).

[78] “Industroyer2: Industroyer reloaded | WeLiveSecurity | #linux | #linuxsecurity,” *NATIONAL CYBER SECURITY NEWS TODAY*, Apr. 12, 2022. https://nationalcybersecuritynews.today/industroyer2-industroyer-reloaded-welivesecurity-linux-linuxsecurity/ (accessed Jul. 13, 2022).

[79] “Pegasus: The ultimate spyware for iOS and Android.” https://www.kaspersky.com/blog/pegasus-spyware/14604/ (accessed Jul. 14, 2022).

[80] “What is Pegasus Spyware and How It Works?,” *GeeksforGeeks*, Jul. 29, 2021. https://www.geeksforgeeks.org/what-is-pegasus-spyware-and-how-it-works/ (accessed Jul. 14, 2022).

[81] S. Shankland, “Pegasus Spyware and Citizen Surveillance: What You Need to Know,” *CNET*. https://www.cnet.com/tech/mobile/pegasus-spyware-and-citizen-surveillance-what-you-need-to-know/ (accessed Jul. 14, 2022).

[82] B. Marczak, J. Scott-Railton, S. Mckune, R. Deibert, and B. Abdulrazzak, *HIDE AND SEEK Tracking NSO Group’s Pegasus Spyware to Operations in 45 Countries*. 2018. doi: 10.13140/RG.2.2.33325.95204.

[83] “Pegasus Spyware Maker NSO Has 22 Clients in the European Union. And It’s Not Alone,” *Haaretz*. Accessed: Aug. 10, 2022. [Online]. Available: https://www.haaretz.com/israel-news/security-aviation/2022-08-09/ty-article/.premium/israeli-spyware-maker-nso-has-22-customers-in-12-eu-countries-and-its-not-alone/00000182-8403-df1d-a3a7-ae9bce800000

[84] A. Chawla, “Pegasus Spyware – ‘A Privacy Killer.’” Rochester, NY, Jul. 21, 2021. doi: 10.2139/ssrn.3890657.

[85] “Pegasus spyware: A complete guide to what it does and how it can be used to infiltrate all aspects of your digital life- Technology News, Firstpost,” *Tech2*, 15:55:45 +05:30. https://www.firstpost.com/tech/news-analysis/pegasus-spyware-a-complete-guide-to-how-it-can-be-used-to-infiltrate-your-phone-7585931.html (accessed Jul. 14, 2022).

[86] A. Alshamrani, S. Myneni, A. Chowdhary, and D. Huang, “A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities,” *IEEE Commun. Surv. Tutor.*, vol. 21, no. 2, pp. 1851–1877, 2019, doi: 10.1109/COMST.2019.2891891.

[87] A.-T.-T. I. I.-S. Institute, “AV-ATLAS - Malware & PUA,” *AV-ATLAS - Malware & PUA*. https://portal.av-atlas.org/malware (accessed Aug. 28, 2022).

[88] “Command and Control [C&C] Server - Definition.” https://www.trendmicro.com/vinfo/us/security/definition/command-and-control-server (accessed Aug. 17, 2022).

[89] N. Virvilis and D. Gritzalis, “The Big Four - What We Did Wrong in Advanced Persistent Threat Detection?,” in *2013 International Conference on Availability, Reliability and Security*, Sep. 2013, pp. 248–254. doi: 10.1109/ARES.2013.32.

[90] V. S. D. Selvam, “Human Error in IT Security.” arXiv, May 08, 2020. doi: 10.48550/arXiv.2005.04163.

[91] “2022 Data Breach Investigation Report (DBIR),” *Verizon Enterprise Solutions*. https://www.verizon.comhttps://www.verizon.com/business/resources/dbir/2022-data-breach-investigations-report-dbir.pdf (accessed Aug. 08, 2022).

[92] “Cybersecurity Framework,” *NIST*, Nov. 2013, Accessed: Aug. 08, 2022. [Online]. Available: https://www.nist.gov/cyberframework

[93] S. D. Hight, “The importance of a security, education, training and awareness program (November 2005),” p. 5.

[94] L. Allodi, T. Chotza, E. Panina, and N. Zannone, “On the Need for New Antphishing Measures Against Spear Phishing Attacks,” *IEEE Secur. Priv.*, vol. PP, Sep. 2019, doi: 10.1109/MSEC.2019.2940952.

[95] A.-D. M.m, B. N, and S. M.m, *Security awareness training: A review*. Newswood Limited, 2017. Accessed: Aug. 08, 2022. [Online]. Available: http://localhost:8080/jspui/handle/123456789/1880

[96] E. Nkiru, “MASTER OF SCIENCE DEGREE IN COMPUTER SCIENCE,” p. 82.

[97] “What is a Honeypot? How It Can Trap Cyberattackers | CrowdStrike,” *crowdstrike.com*. https://www.crowdstrike.com/cybersecurity-101/honeypots-in-cybersecurity-explained/ (accessed Aug. 10, 2022).

[98] “What is a honeypot?,” *www.kaspersky.com*, Mar. 30, 2022. https://www.kaspersky.com/resource-center/threats/what-is-a-honeypot (accessed Aug. 10, 2022).

[99] “Moving Target Defenses – The Cyber Team.” https://coar.risc.anl.gov/research/moving-target-defense/ (accessed Aug. 11, 2022).

[100] “Defending Against Software Supply Chain Attacks,” p. 16.

[101] N. F. Syed, S. W. Shah, R. Trujillo-Rasua, and R. Doss, “Traceability in supply chains: A Cyber security analysis,” *Comput. Secur.*, vol. 112, p. 102536, Jan. 2022, doi: 10.1016/j.cose.2021.102536.

[102] “11 Ways to Prevent Supply Chain Attacks in 2022 (Highly Effective) | UpGuard.” https://www.upguard.com/blog/how-to-prevent-supply-chain-attacks (accessed Aug. 11, 2022).