Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών

«Πληροφορική»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Απειλές Ασφαλείας για Εφαρμογές Απομακρυσμένης Σύνδεσης** **Security Threats for Remote Connection Applications**
Ονοματεπώνυμο Φοιτητή	**Λυκούργος Καπαρέλος**
Πατρώνυμο	**Βασίλειος**
Αριθμός Μητρώου	**ΜΠΠΛ/17019**
Επιβλέπων	**Κωνσταντίνος Πατσάκης, Αναπληρωτής Καθηγητής**

Ημερομηνία Παράδοσης **Δεκέμβριος 2022**

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Κωνσταντίνος Πατσάκης Αναπληρωτής καθηγητής	Ευθύμιος Αλέπης Αναπληρωτής καθηγητής	Ευάγγελος Σακκόπουλος Αναπληρωτής καθηγητής

Αφιέρωση

Ευχαριστώ την οικογένεια μου για την στήριξη, την συμπαράσταση, την υπομονή και την κατανόηση που έδειξαν κατά την διάρκεια των σπουδών μου.

Περίληψη

Στην παρούσα μεταπτυχιακή διατριβή γίνεται αναφορά των πρωτόκολλων που μπορούν να χρησιμοποιηθούν για απομακρυσμένη πρόσβαση σε υπολογιστικά συστήματα. Συγκεκριμένα, γίνεται εκτενής αναφορά της λειτουργία του πρωτόκολλου RDP (Remote desktop protocol) και πώς αυτό θα μπορούσε από συμβατική λύση απομακρυσμένης σύνδεση να μετατραπεί σε πρωτόκολλο για επιτήδειες ενέργειες. Στο κύριο θεωρητικό μέρος της διατριβής, γίνονται αναφορές διείσδυσης για κακόβουλη χρήση του πρωτόκολλου RDP, εφαρμογές που συμβάλουν στην απομακρυσμένη ασφάλεια καθώς και αναφορά στο πρακτικό μέρος της διατριβής για έλεγχο και εξαγωγή ευρημάτων με σκοπό την ανάλυση έπειτα από επίθεση μέσω εφαρμογών που χρησιμοποιούν RDP πρωτόκολλο. Τέλος, καταλήγουμε στα συμπεράσματα του πρακτικού κομματιού, σύνδεση με άλλες εφαρμογές και προτάσεις βελτίωσης των ελέγχων.

Λέξεις - Κλειδιά

RDP, κυβερνοχώρος, Ιστός, διαδίκτυο, ασφάλεια, συσκευές, cloud, βάσεις δεδομένων, δίκτυα, εφαρμογές, κώδικας, στόχος, Ransomware

Abstract

On the below dissertation we are creating references to the protocols that can be used for Remote connection to computer devices. Specifically, we are analyzing the Remote Desktop Protocol (RDP) and how it could be transformed from a mainstream remote connectivity solution into tool for software attacks. On the main part of the dissertation, we will refer to the ways that RDP can be used for operating system attacks, applications that assist on remote security to computing devices, the dangers of remote connections as well as the script created for the purpose of data and forensic analysis after a successful remote attack. Finally, we will conclude on how this script can be made better, what are the possibilities of data extraction and how it can be implemented into know applications.

Keywords

RDP, cyberspace, web, internet, security, devices, cloud, databases, networks, applications, code, target, Ransomware

Περιεχόμενα

ΠΕΡΙΛΗΨΗ **4**

ABSTRACT **5**

ΕΙΣΑΓΩΓΗ **11**

1 ΕΦΑΡΜΟΓΕΣ ΑΠΟΜΑΚΡΥΣΜΕΝΗΣ ΣΥΝΔΕΣΗΣ **13**

1.1. Δημιουργια Tunnel 14
1.2. Εφαρμογες Πυλων 15
1.3. Προσβαση σε Εφαρμογες Σταθερου Υπολογιστη 15
1.4. Άμεση Προσβαση σε Εφαρμογες 16

2 ΚΙΝΔΥΝΟΙ ΑΣΦΑΛΕΙΑΣ ΣΕ ΕΦΑΡΜΟΓΕΣ ΑΠΟΜΑΚΡΥΣΜΕΝΗΣ ΣΥΝΔΕΣΗΣ **18**

2.1 Η ασφαλεια στον κυβερνοχωρο ως παγκοσμια προκληση 18
2.2 Ασφαλεια υποδομων ζωτικης σημασιας 18
2.3 Ασφαλεια δικτυου 19
2.4 Κινητες συσκευες 20
2.5 Διαχειριση ταυτοτητας και προσβασης 20
2.6 Ασφαλεια εφαρμογων 21
2.7 Ασφαλεια στο cloud 21
2.8 Ασφαλεια βασεων δεδομενων 22
2.9 Ασφαλεια Internet of Things 23
2.10 Ευαισθητοποιηση για την ασφαλεια στον κυβερνοχωρο 23

3 ΑΝΤΙΜΕΤΩΠΙΣΗ ΚΙΝΔΥΝΩΝ ΑΣΦΑΛΕΙΑΣ ΕΦΑΡΜΟΓΩΝ ΑΠΟΜΑΚΡΥΣΜΕΝΗΣ ΣΥΝΔΕΣΗΣ **25**

3.1 Έλεγχος Προσβασης Δικτυου (Network Access Control, NAC) 25
3.2 Εικονικο Ιδιωτικο Δικτυο (VPN) 25
3.3 Ασφαλεια δικτυου με εφαρμογες Τριτων 29
3.4 Αποστρατιωτικοποιημενη Ζωνη (DMZ) 30
3.5 Sheep-dip Δικτυου 31

4 ΣΤΑΤΙΣΤΙΚΑ ΣΤΟΙΧΕΙΑ ΕΠΙΘΕΣΕΩΝ **33**

5 ΒΙΒΛΙΟΓΡΑΦΙΚΗ ΑΝΑΣΚΟΠΗΣΗ ΜΕΛΕΤΩΝ ΑΠΟ ΔΟΚΙΜΕΣ ΔΙΕΙΣΔΥΣΗΣ ΣΕ RDP **36**

5.1 Πλαισιο Αξιολογησης Ασφαλειας Πληροφοριακων Συστηματων 36
5.2 Εγχειριδιο Μεθοδολογιας Δοκιμων Ασφαλειας Ανοικτου Κωδικα 36
5.3 Ανοιχτο Εγχειρημα Ασφαλειας Εφαρμογων Ιστου 37

6 ΒΙΒΛΙΟΓΡΑΦΙΚΗ ΑΝΑΣΚΟΠΗΣΗ ΛΟΓΙΣΜΙΚΟΥ RANSOMWARE **38**

6.1 Κακοβουλο Λογισμικο Ransomware 38

6.2 Μοτιβα Επιθεσεων 39
6.3 Human-Operated-Ransomware 40

7. ΠΡΑΚΤΙΚΟ ΜΕΡΟΣ POWERSHELL SCRIPT 43

7.1 Μεθοδολογια δημιουργιας κωδικα και Στοχος 43
7.2 Περιορισμοι και αντιμετωπιση 48

8. ΠΑΡΟΥΣΙΑΣΗ ΕΦΑΡΜΟΓΗΣ/POWERSHELL SCRIPT 51

8.1 ΠΑΡΟΥΣΙΑΣΗ ΑΠΟΤΕΛΕΣΜΑΤΩΝ POWERSHELL SCRIPT 53

9. ΠΡΟΣΘΗΚΗ ΝΕΩΝ ΛΟΓΙΣΜΙΚΩΝ ΚΑΙ ΣΥΝΔΕΣΗ ΜΕ ΑΛΛΕΣ ΕΦΑΡΜΟΓΕΣ 64

ΣΥΜΠΕΡΑΣΜΑΤΑ 66

ΒΙΒΛΙΟΓΡΑΦΙΑ 67

Κατάλογος Εικόνων / Σχημάτων

Σχημα 1. Αρχιτεκτονικη VPN απομακρυσμενης προσβασης 13
Σχημα 2. Αρχιτεκτονικη Tunneling 14
Σχημα 3. Αρχιτεκτονικη πυλης 15
Σχημα 4. Αρχιτεκτονικη προσβασης απομακρυσμενης επιφανειας εργασιας 16
Σχημα 5. Αρχιτεκτονικη αμεσης προσβασης εφαρμογης 17
Σχημα 6. Ένα VPN απομακρυσμενης προσβασης 26
Σχημα 7. Κατηγοριες/Πρωτοκολλα VPN 27
Σχημα 8. Ένα παραδειγμα DMZ 31
Σχημα 9. Ένα sheep-dip δικτυου 32
Σχημα 10. Αναφορες επιθεσεων ransomware του FBI Internet Crime Complaint Center (IC3) απο το 2016-2020. 33
Σχημα 11. Διακομιστες με υπηρεσια RDP (θυρα 3389) εκτεθειμενη στο Διαδικτυο. 34
Σχημα 12. Στατιστικα χρησης πορτας 3389 35
Σχημα 13. Στατιστικα χρησης πρωτοκολλου RDP πορτες 3389 και 3388 35
Σχημα 14. Δομη μιας επιθεσης Ransomware. 40
Σχημα 15. Διαγραμμα ροης κρυπτογραφησης ransomware εναντι αστυνομικων ransomware. 41
Σχημα 16. Κανονας Τοιχους προστασιας για RDP συνεση 45
Σχημα 17. Προσθετες επιλογες Ασφαλειας Remote Desktop connection 46
Σχημα 18. Επιλογες ενεργοποιησης απομακρυσμενης συνδεσης 47
Σχημα 19. Επιλογες συστηματος για απομακρυσμενη συνδεση 48
Σχημα 20. Windows Remote Desktop Connection 51
Σχημα 21. Teamviewer Remote connection interface 52
Σχημα 22. Anydesk Remote connection interface 52
Σχημα 23. Έλεγχος διαγραφης Event Logs 53
Σχημα 24. Επιτυχεις συνδεσεις με Remote Desktop Connection 53
Σχημα 25. Αποσυνδεσεις χρηστων με την εφαρμογη Windows RDP 54
Σχημα 26. Αποπειρες απομακρυσμενης συνδεσης με το Remote Desktop Connection 54
Σχημα 27. Συνδεση της εφαρμογης Teamviewer στους κεντρικους server 55
Σχημα 28. Συνδεσεις της τελευταιας ημερας στο Teamviewer 55
Σχημα 29. Teamviewer IDs assigned 56
Σχημα 30. Μεταφορα αρχειων μεσα απο την εφαρμογη Teamviewer 56
Σχημα 31. Προσπαθειες συνδεσης στο τερματικο μεσω Teamviewer 57
Σχημα 32. Τελευταια επιτυχημενη συνδεση στο Teamviewer 57
Σχημα 33. Τελευταια επιτυχημενη συνδεση με Anydesk 58
Σχημα 34. Προσπαθεια προσπελασης αρχειων μεσω Anydesk 59

Σχημα 35. Αρχεια τα οποια εγιναν προσπελαση 59
Σχημα 36. Αρχεια τα οποια τροποποιηθηκαν/διαγραφηκαν 60
Σχημα 37. Διεργασιες οι οποιες αρχισαν κατα το Remote connection 60
Σχημα 38. Διεργασιες που εκλεισαν κατα το Remote connection 61
Σχημα 39. Εφαρμογες οι οποιες εγκατασταθηκαν κατα την διαρκεια του remote connection 61
Σχημα 40. Εφαρμογες που απεγκαταστηθηκαν κατα την διαρκεια του remote connection 61
Σχημα 41. Αρχειο τυπου Json για τις διεργασιες που εκκινηθησαν 62
Σχημα 42. Αρχειο τυπου Json για τα αρχεια που εγινε προσπελαση 62
Σχημα 43. Αρχειο τυπου Json για τις εφαρμογες που εγιναν απεγκαταστση 63

Συντομογραφίες & Ακρωνύμια

RDP	Remote Desktop protocol
JSON	JavaScript Object Notation
VPN	Virtual Private Network
LAN	local area network
ATM	Asynchronous Transfer Mode
CIA	Confidentiality Integrity Availability
IAM	Identity and Access Management
IaaS	Identity as a Service
RAC	Rules-based Access Control
AWS	Amazon Web Services
RBAC	Roles-Based Access Control
GCP	Google Cloud Platform
DDoS	Distributed Denial of Service
IoT	Internet of Things
PPTP	point-to-point tunneling protocol
L2TP	layer two tunneling protocol
IPsec	internet protocol security
IDS	Intrusion Detection System
ISSAF	Information System Security Assessment Framework
OISSG	Open Information Systems Security Group
OSSTMM	Open Source Security Testing Methodology Manual
NIST	National Institute of Standards and Technology
OWASP	Open Web Application Security Project

Εισαγωγή

Στην παρούσα μεταπτυχιακή διατριβή, θα αναλύσουμε τις εφαρμογές απομακρυσμένης σύνδεσης και πως αυτές μπορούν να εξυπηρετήσουν εταιρίες πληροφοριών για απομακρυσμένη διαχείριση εφαρμογών και δεδομένων. Αυτό μπορεί να επιτευχθεί με διάφορους τρόπους και πρωτόκολλα επικοινωνίας, αλλά συγκεκριμένα θα αναλυθεί το πρωτόκολλο απομακρυσμένης σύνδεσης RDP (Remote Desktop protocol). Θα αναφερθούμε στην λειτουργία αυτού, πως δημιουργείται ο δίαυλος επικοινωνίας και πως μπορούμε απομακρυσμένα να έχουμε πρόσβαση σε εφαρμογές ή επιφάνειες εργασίας.

Δεδομένης της ανάγκης που δημιουργήθηκε για απομακρυσμένη πρόσβαση παγκοσμίως λόγω της πανδημίας COVID-19, αρκετές εταιρίες διαχείρισης πληροφοριών, προσπάθησαν να συμπεριλάβουν και να υιοθετήσουν υβριδικά μοντέλα εργασίας ούτος ώστε να γίνεται πιο ασφαλής η εργασία για όλους. Αυτό είχε ως αποτέλεσμα να χρησιμοποιηθούν απομακρυσμένα πρωτόκολλα και εφαρμογές που χρησιμοποιούν αυτά τα πρωτόκολλα, σε αρκετές περιπτώσεις χωρίς τις βασικές δικλείδες ασφαλείας, για διασύνδεση των εργαζομένων στις εφαρμογές και σε παραγωγικά περιβάλλοντα των εταιριών.

Οι παραπάνω αλλαγές, πέραν από το κομμάτι διευκόλυνσης και εξυπηρέτησης των εργαζομένων και κατ' επέκταση της διασφάλισης της συνέχειας των εταιριών, επέφερε και αρκετούς κίνδυνους καθώς υπήρχαν πολλά κενά ασφάλειας στις εφαρμογές που χρησιμοποιούσαν τα πρωτόκολλα αυτά όπως και «τρύπες» που αρκετοί κακόβουλοι χρήστες εκμεταλλεύτηκαν με σκοπό το κέρδος. Στην δεύτερη ενότητα του θεωρητικού κομματιού της μεταπτυχιακής διατριβής, γίνεται ανάλυση των κίνδυνων που προκύπτουν από τέτοιες εφαρμογές, πώς αποτελεί παγκόσμια πρόκληση καθώς και αντιπαραθέσεις με την ασφάλεια που μπορούν να μας παρέχουν εφαρμογές.

Στην τρίτη ενότητα της διατριβής, παρατίθενται προτάσεις βελτίωσης. Πώς μπορούν οι συγκεκριμένες εφαρμογές απομακρυσμένης πρόσβασης (κατ' επέκταση και το πρωτόκολλο RDP που πραγματευόμαστε) να γίνουν πιο ασφαλή μέσα σύνδεσης σε απομακρυσμένες επιφάνειες εργασίας και εφαρμογών. Γίνεται αναφορά των αποστρατιωτικοποιημένων ζωνών (DMZ), των εικονικών δικτύων (VPN) που υιοθετήθηκε από αρκετές εταιρίες σαν ενδιάμεσο απλό, γρήγορο και ευέλικτο βήμα σύνδεσης και απόκρυψης διαδικτυακής κίνησης. Επιπρόσθετα, γίνεται αναφορά σε λύσεις όπως και έλεγχο πρόσβασης δικτύου (NAC) με διάφορες εφαρμογές τρίτων εταιριών καθώς και Sheep-dip δικτύου, όπου ανιχνεύει εσωτερικές συνδέσεις για οτιδήποτε κακόβουλα λογισμικά εισέρχονται στο εσωτερικό δίκτυο μιας εταιρίας.

Στην τέταρτη ενότητα της παρακάτω ανάλυσης, γίνεται αναφορά στατιστικών στοιχείων μεγάλων επιθέσεων που έχουν γίνει σε αρκετές εταιρίες του κλάδου της πληροφορίας και όχι μόνο, τα αίτια που οδήγησαν σε αυτές τις επιθέσεις καθώς και τύπους επιθέσεων πέραν του γνωστού ransomware που αρκετές γνωστές εταιρίες και οργανισμοί έπεσαν θύματα και χάνοντας εκατομμύρια ευρώ και δολάρια.

Στην πέμπτη ενότητα της διατριβής, γίνεται βιβλιογραφική ανασκόπηση από δοκιμές διείσδυσης με την χρήση του πρωτοκόλλου RDP, που υπόκεινται στην πόρτα επικοινωνίας 3389. Γίνεται αναφορά στο Πλαίσιο Αξιολόγησης Ασφάλειας Πληροφοριακών Συστημάτων και πως αυτό το πλαίσιο δοκιμών ανοιχτού κώδικα ενσωματώνει μεθοδολογίες διείσδυσης, επίλυσης επιθέσεων και διασφάλισης της ασφάλειας των συστημάτων. Επιπλέον, γίνεται αναφορά στο Εγχειρίδιο Μεθοδολογίας Δοκιμών Ασφάλειας Ανοικτού Κώδικα που μπορεί να συγκριθεί και θεωρείται μια βελτιωμένη έκδοση του Πλαισίου Αξιολόγησης Ασφάλειας Πληροφοριακών Συστημάτων. Κλείνοντας την πέμπτη ενότητα, γίνεται αναφορά και στο Ανοιχτό Εγχείρημα Ασφάλειας Εφαρμογών Ιστού, ποια εργαλεία και μεθοδολογίες ακολουθεί καθώς και τις τρείς κύριες ενότητες που χωρίζεται για τους ελέγχους διείσδυσης.

Στην προτελευταία ενότητα γίνεται βιβλιογραφική αναφορά των κακόβουλων επιθέσεων, πως οι επιτήδειοι χρησιμοποιούν τέτοιους είδους λογισμικά για εκβιασμό και κέρδος καθώς και ποια μοτίβα επιθέσεων χρησιμοποιούν. Μια κατηγορία κακόβουλων λογισμικών, αποτελεί και το Human-Operated-Ransomware, όπου οι επιτιθέμενοι κυβερνοεγκληματίες προσπαθούν να αποκτήσουν πρόσβαση σε υποδομή Cloud ή τοπική υποδομή εταιρίας, να αποκτήσουν δικαιώματα διαχειριστή και έτσι να διασπείρουν το κακόβουλο λογισμικό σε ευαίσθητες πληροφορίες, συστήματα και βάσεις των εταιριών. Οι επιτιθέμενοι προσπαθούν με αυτή την απόκτηση πρόσβασης, να χτυπήσουν κομμάτι του οργανισμού και όχι ιδιαίτερα μεμονωμένες

συσκευές του δικτύου. Αυτό μπορεί να επιτευχθεί με την απόκτηση στοιχείων πρόσβασης διαχειριστών και κινήσεων μεταξύ των συστημάτων με την χρήση αυξημένων προνομίων (elevated privileges).

Στο τελευταίο κομμάτι της διατριβής, θα γίνει ανάλυση του πρακτικού μέρους το οποίο αποτελείται από την δημιουργία powershell script το οποίο ελέγχει 3 συγκεκριμένες εφαρμογές (Windows RDP connection, Teamviewer, Anydesk). Το συγκεκριμένο script, εξάγει δεδομένα για ανάλυση όπως π.χ. στοιχεία συνδεδεμένου χρήστη, διεύθυνση IP, όνομα υπολογιστή, λογισμικό που χρησιμοποιείται για την σύνδεση καθώς και στοιχεία όπως διαγραφή αρχείων συστήματος, αλλαγές σε φακέλους, αρχεία, δικαιώματα, εγγραφές μητρώου υπολογιστή κ.ο.κ όπως και εφαρμογές που εγκαταστάθηκαν, εφαρμογές που απεγκαταστάθηκαν και προσπάθειες σύνδεσης ή κακόβουλων ενεργειών. Από το παραπάνω powershell script, γίνεται εξαγωγή σε αρχεία JSON (JavaScript Object Notation) τα οποία αποτελούν αρχεία με πιο απλοποιημένη μορφοποίηση και χρησιμοποιούνται ευρέως από εφαρμογές και λογισμικά, με σκοπό να γίνει οποιουδήποτε τύπου ανάλυση έπειτα από κακόβουλη επίθεση.

Τέλος, γίνεται αναφορά των συμπερασμάτων και των αποτελεσμάτων του πρακτικού μέρους. Θα τεθούν προτάσεις που θα παρουσιάσουν πως μπορεί να αναπτυχθεί το λογισμικό, πως μπορούν να εισαχθούν νέες εφαρμογές και με ποιες υπάρχοντες εφαρμογές θα μπορούσε να συνδεθεί το script για την καλύτερη εξαγωγή δεδομένων και ανάλυση αυτών.

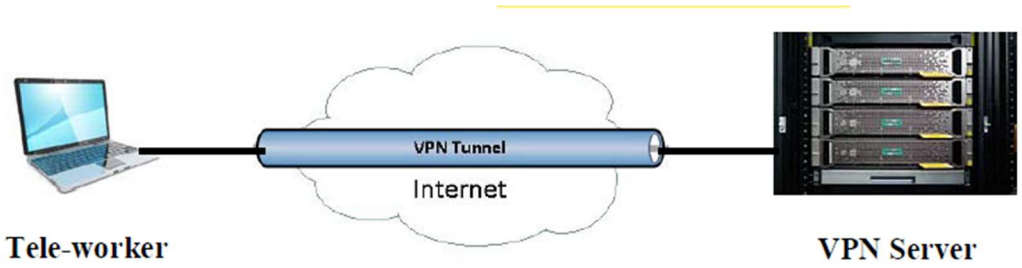
1 Εφαρμογές Απομακρυσμένης Σύνδεσης

Ένα εταιρικό δίκτυο συνήθως αποτελείται από πολλές απομακρυσμένες συνδεδεμένες εγκαταστάσεις που βρίσκονται μακριά μεταξύ τους. Παραδοσιακά, οι συνδέσεις μισθωμένων γραμμών που χρησιμοποιούν το πλαίσιο αναμετάδοσης και τη λειτουργία ασύγχρονης μεταφοράς (Asynchronous Transfer Mode, ATM) χρησιμοποιήθηκαν για την παροχή συνδεσιμότητας μεταξύ αυτών των εταιρικών τοποθεσιών. Η ανάπτυξη αυτού του δικτύου το κατέστησε μια δαπανηρή λύση και μια πρόκληση για την επεκτασιμότητα του δικτύου.

Το Εικονικό Ιδιωτικό Δίκτυο (Virtual Private Network, VPN) παρουσιάζεται ως εναλλακτική πρόταση που παρέχει ευέλικτες λύσεις, όπως η διασφάλιση της επικοινωνίας μεταξύ απομακρυσμένων τηλεργαζομένων και διακομιστών του οργανισμού, ανεξάρτητα από το πού βρίσκονται οι τηλεργαζόμενοι. Οι Alshalan et al, (2015), στο άρθρο τους περιγράφουν ένα εικονικό ιδιωτικό δίκτυο (VPN) ως την παραδοσιακή προσέγγιση για μια ασφαλή σύνδεση από άκρο σε άκρο μεταξύ δύο τελικών σημείων μέσω της χρήσης δημόσιας ή κοινής τηλεπικοινωνιακής υποδομής, διατηρώντας το απόρρητο μέσω της χρήσης ενός πρωτοκόλλου διάνοιξης σήραγγας (tunneling protocol) και των διαδικασιών ασφαλείας. Το VPN δημιουργεί σήραγγες μεταξύ διακομιστών σε ένα VPN από τοποθεσία σε τοποθεσία, πελατών και διακομιστών σε VPN από πελάτη σε τοποθεσία (Avani & Ankita, 2017). Το VPN tunneling περιλαμβάνει τη δημιουργία και τη διατήρηση μιας λογικής σύνδεσης δικτύου (σήραγγα, tunnel), όπου τα πακέτα που κρυπτογραφούνται σε συγκεκριμένο μορφότυπο πρωτοκόλλου VPN, στη συνέχεια ενσωματώνονται σε κάποιο άλλο πρωτόκολλο φορέα, μεταδίδονται στη συνέχεια μεταξύ VPN πελάτη και διακομιστή και τελικά αποκρυπτογραφούνται στην πλευρά λήψης.

Η προσέγγιση του VPN ρίχνει σημαντικό βάρος στην ασφάλεια κατά την απομακρυσμένη πρόσβαση, καθώς οι περισσότερες μεγάλες εταιρείες, εκπαιδευτικά ιδρύματα και κυβερνητικές υπηρεσίες χρησιμοποιούν τεχνολογία VPN για να επιτρέψουν στον τηλεργαζόμενο να συνδεθεί με ασφάλεια σε ένα ιδιωτικό δίκτυο. Οι τηλεργαζόμενοι μπορούν να συνδεθούν στο εταιρικό τους δίκτυο ή σε οποιοδήποτε άλλο δίκτυο έχουν δικαίωμα πρόσβασης, ανεξάρτητα από το πού βρίσκονται (Narayan et al., 2009) και μπορούν να έχουν πρόσβαση σε πόρους όπως email και έγγραφα σαν να ήταν φυσικά τοποθετημένοι σε κάποιον υπολογιστή του δικτύου της επιχείρησης.

Όλοι οι απομακρυσμένοι χρήστες ελέγχουν την ταυτότητα τους με τον διακομιστή VPN, ο οποίος προστατεύεται από ένα τείχος προστασίας. Μόλις ένας χρήστης συνδεθεί στο δίκτυο, ένα εσωτερικό τείχος προστασίας εγγυάται ότι η πρόσβαση είναι διαθέσιμη μόνο στους απαιτούμενους πόρους (Chowdhury & Gkioulos, 2021). Όταν ένα πακέτο δεδομένων μεταδίδεται από έναν απομακρυσμένο χρήστη, αυτό αποστέλλεται μέσω μιας πύλης VPN, η οποία προσθέτει μια κεφαλίδα ελέγχου ταυτότητας για δρομολόγηση και έλεγχο ταυτότητας. Στη συνέχεια, τα δεδομένα κρυπτογραφούνται και τέλος περικλείονται σε ένα Encapsulating Security Payload που περιέχει τις οδηγίες αποκρυπτογράφησης και χειρισμού.



Σχήμα 1. Αρχιτεκτονική VPN απομακρυσμένης πρόσβασης

Ο διακομιστής VPN λήψης αφαιρεί τις πληροφορίες κεφαλίδας, αποκρυπτογραφεί τα δεδομένα και τα δρομολογεί στον προορισμό τους. Ένα VPN επιτρέπει την παροχή ενός εικονικού tunnel που συνδέει τα δύο τελικά σημεία. Η κίνηση μέσα στη σήραγγα VPN είναι κρυπτογραφημένη έτσι ώστε οι άλλοι χρήστες του δημόσιου διαδικτύου να μην μπορούν να αντιληφθούν το πραγματικό περιεχόμενο ακόμα κι αν υποκλέψουν την επικοινωνία (Sobh & Aly, 2011). Με την εφαρμογή ενός VPN ένας οργανισμός όπως εταιρία, κυβερνητική υπηρεσία,

εκπαιδευτικό ίδρυμα κ.α., μπορεί να παρέχει ασφαλή πρόσβαση στο εσωτερικό ιδιωτικό δίκτυο σε συνεργάτες από όλο τον κόσμο με πρόσβαση μέσω του δημόσιου Διαδικτύου.

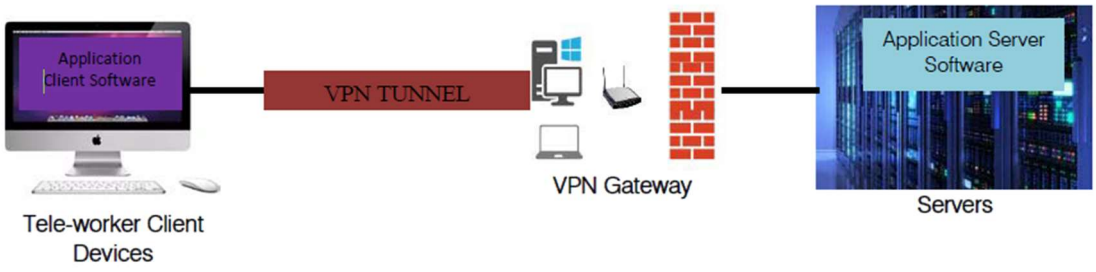
Η απομακρυσμένη πρόσβαση είναι μια από τις διαδεδομένες επιχειρηματικές τάσεις στη σημερινή εποχή των υπολογιστών, η οποία αναπτύσσει τη χρήση ασφαλούς πρόσβασης σε εταιρικούς πόρους, δημιουργώντας μια κρυπτογραφημένη σήραγγα σε όλο το δίκτυο. Είναι μια σύνδεση χρήστη σε τοπικό δίκτυο (local area network, LAN) που χρησιμοποιείται από μια εταιρεία που έχει υπαλλήλους που πρέπει να συνδεθούν στο ιδιωτικό δίκτυο από διάφορες απομακρυσμένες τοποθεσίες. Τα VPN επιτρέπουν ασφαλείς, κρυπτογραφημένες συνδέσεις απομακρυσμένης πρόσβασης μεταξύ του ιδιωτικού δικτύου μιας εταιρείας και των απομακρυσμένων χρηστών μέσω τρίτου παρόχου υπηρεσιών.

Σύμφωνα με τον Rajamohan (2014), τα VPN επιτρέπουν την ασφαλή πρόσβαση σε εταιρικούς πόρους με τη δημιουργία μιας κρυπτογραφημένης σήραγγας στο Διαδίκτυο. Ενώ ένα τείχος προστασίας προστατεύει τα συστήματα και τα δεδομένα σε ένα LAN από μη εξουσιοδοτημένη πρόσβαση, δεν μπορεί να προστατεύσει την εμπιστευτικότητα και την ακεραιότητα της κίνησης που διασχίζει το Διαδίκτυο καθ' οδόν προς και από το LAN. Αυτός είναι ο ρόλος ενός εικονικού ιδιωτικού δικτύου ή VPN. Η τεχνολογία VPN παρέχει λειτουργίες κρυπτογράφησης και σήραγγας για δικτυακή κίνηση στο Διαδίκτυο. Τα δεδομένα ενσωματώνονται σε ένα *περιτύλιγμα* IP που ταξιδεύει μέσω του Διαδικτύου. Όταν αποστέλλονται δεδομένα, πρέπει να περιτυλίγονται και να κρυπτογραφούνται από μια πύλη χρησιμοποιώντας έναν αλγόριθμο κρυπτογράφησης. Στο άλλο άκρο της σύνδεσης επικοινωνίας, η πύλη προορισμού πρέπει να "ξετυλίξει" τα δεδομένα, να τα αποκρυπτογραφήσει και να τα δρομολογήσει στον προορισμό τους.

Στη συνέχεια παρουσιάζονται οι σύγχρονες μέθοδοι απομακρυσμένης πρόσβασης VPN για τη δημιουργία εικονικού ιδιωτικού δικτύου. Οι μέθοδοι απομακρυσμένης πρόσβασης χρησιμοποιούνται συχνότερα από τηλεργαζόμενους. Στις επόμενες ενότητες περιγράφονται τέσσερις κατηγορίες με βάση τις αρχιτεκτονικές υψηλού επιπέδου και τις επιπτώσεις στην ασφάλεια. Οι κατηγορίες περιλαμβάνουν: σήραγγες, πύλες, πρόσβαση απομακρυσμένης επιφάνειας εργασίας και άμεση πρόσβαση σε εφαρμογές και δίνεται μια διερεύνηση της πρόσβασης στο VPN.

1.1. Δημιουργία Tunnel

Πολλές μέθοδοι απομακρυσμένης πρόσβασης προσφέρουν μια ασφαλή σήραγγα επικοινωνίας μέσω της οποίας μπορούν να μεταδοθούν πληροφορίες μεταξύ δικτύων, συμπεριλαμβανομένων δημόσιων δικτύων όπως το Διαδίκτυο. Σύμφωνα με τους Souppaya & Scarfone, (2016), το tunneling περιλαμβάνει τη δημιουργία μιας ασφαλούς σήραγγας επικοινωνίας μεταξύ μιας συσκευής πελάτη και ενός διακομιστή απομακρυσμένης πρόσβασης, συχνά μια πύλη εικονικού ιδιωτικού δικτύου (VPN) που χρησιμοποιεί κρυπτογραφία για την προστασία του απορρήτου και της ακεραιότητας των μεταδιδόμενων πληροφοριών μεταξύ της συσκευής-πελάτη και της πύλης VPN. Η πύλη VPN μπορεί να φροντίσει για τον έλεγχο ταυτότητας χρήστη, τον έλεγχο πρόσβασης και άλλες λειτουργίες ασφαλείας για τους απομακρυσμένους χρήστες. Η σήραγγα χρησιμοποιεί κρυπτογραφικά πρωτόκολλα όπως σήραγγες IPsec, SSL και SSH για την προστασία του απορρήτου και της ακεραιότητας των επικοινωνιών. Το (Σχήμα 2) δείχνει την αρχιτεκτονική σήραγγας που χρησιμοποιείται για τη ρύθμιση της απομακρυσμένης πρόσβασης σήραγγας.



Σχήμα 2. Αρχιτεκτονική Tunneling

Μόλις δημιουργηθεί μια σήραγγα VPN μεταξύ της συσκευής πελάτη και της πύλης VPN του οργανισμού, ο απομακρυσμένος χρήστης μπορεί να έχει πρόσβαση σε πολλούς από τους υπολογιστικούς πόρους του οργανισμού. Για να χρησιμοποιήσουν την εφαρμογή VPN, οι χρήστες πρέπει είτε να διαθέτουν το κατάλληλο λογισμικό VPN στις συσκευές τους είτε να βρίσκονται σε δίκτυο που διαθέτει σύστημα πύλης VPN σε αυτό. Η πύλη VPN μπορεί να ελέγξει την πρόσβαση στα μέρη του δικτύου και τους τύπους πρόσβασης που αποκτά ο απομακρυσμένος χρήστης μετά τον έλεγχο ταυτότητας. Για παράδειγμα ένα VPN μπορεί να επιτρέπει σε έναν χρήστη να έχει πρόσβαση μόνο σε ένα υποδίκτυο ή να εκτελεί μόνο συγκεκριμένες εφαρμογές σε ορισμένους διακομιστές στο προστατευμένο δίκτυο. Με αυτόν τον τρόπο, παρόλο που η κρυπτογραφική σήραγγα τελειώνει στην πύλη VPN, η πύλη μπορεί να προσθέσει πρόσθετη δρομολόγηση στην κίνηση του τηλεργαζόμενου για να επιτρέπει την πρόσβαση μόνο σε ορισμένα μέρη του εσωτερικού δικτύου.

1.2. Εφαρμογές Πυλών

Μια πύλη είναι ένας διακομιστής που προσφέρει πρόσβαση σε μία ή περισσότερες εφαρμογές μέσω μιας ενιαίας κεντρικής διεπαφής (Souppaya & Scarfone, 2016). Ένας απομακρυσμένος χρήστης χρησιμοποιεί έναν υπολογιστή πελάτη πύλης σε μια συσκευή πελάτη τηλεργασίας για πρόσβαση στην πύλη. Το λογισμικό πελάτη εγκαθίσταται στον διακομιστή πύλης και επικοινωνεί με τον διακομιστή εφαρμογών και την πύλη, οι πύλες μπορούν επίσης να ελέγχουν την ταυτότητα του λογισμικού των χρηστών σε διακομιστές εντός του οργανισμού. Το (Σχήμα 3) και ο περιορισμός της πρόσβασης στο εσωτερικό του οργανισμού δείχνει τη βασική αρχιτεκτονική της λύσης πύλης VPN. Η πύλη προστατεύει τις επικοινωνίες μεταξύ των συσκευών πελάτη και της πύλης και οι πύλες μπορούν επίσης να ελέγχουν την ταυτότητα των χρηστών και να περιορίζουν την πρόσβαση στους εσωτερικούς πόρους του οργανισμού.

Όσον αφορά την ασφάλεια, οι πύλες έχουν τα περισσότερα από τα χαρακτηριστικά ασφάλειας με τις σήραγγες: οι πύλες προστατεύουν τις πληροφορίες μεταξύ των συσκευών πελάτη και της πύλης και μπορούν να παρέχουν έλεγχο ταυτότητας και έλεγχο πρόσβασης. Το λογισμικό πελάτη και τα δεδομένα αρχικά βρίσκονται στον διακομιστή πύλης, στη συνέχεια μεταφέρονται στις συσκευές πελάτη, στη συνέχεια αποθηκεύονται συνήθως στις συσκευές πελάτη. Η συγκέντρωση του λογισμικού πελάτη της εφαρμογής δίνει σε έναν οργανισμό περισσότερο έλεγχο στην πολιτική ασφάλειας του λογισμικού και των δεδομένων, σε σύγκριση με τις πιο κατανεμημένες λύσεις απομακρυσμένης πρόσβασης. Οι πύλες περιορίζουν την πρόσβαση που έχει ένας τηλεργαζόμενος σε συγκεκριμένους πελάτες εφαρμογών που εκτελούνται στις λύσεις της πύλης.

Σχήμα 3. Αρχιτεκτονική πύλης

1.3. Πρόσβαση σε Εφαρμογές Σταθερού Υπολογιστή

Μια λύση πρόσβασης απομακρυσμένης επιφάνειας εργασίας δίνει στον τηλεργαζόμενο τη δυνατότητα να ελέγχει εξ αποστάσεως έναν συγκεκριμένο επιτραπέζιο υπολογιστή στον οργανισμό, τις περισσότερες φορές τον υπολογιστή του ίδιου του χρήστη στο γραφείο του οργανισμού, από μια συσκευή πελάτη τηλεργασίας. Η λύση επιτρέπει στον χρήστη να έχει πρόσβαση σε όλες τις εφαρμογές, τα δεδομένα και άλλους πόρους που είναι συνήθως διαθέσιμοι από τον υπολογιστή του στο γραφείο. Το (Σχήμα 4) δείχνει τη βασική αρχιτεκτονική πρόσβασης απομακρυσμένης επιφάνειας εργασίας.

Η πρόσβαση απομακρυσμένης επιφάνειας εργασίας χρησιμοποιεί ένα ιδιόκτητο πρωτόκολλο, το πρωτόκολλο απομακρυσμένης επιφάνειας εργασίας (remote desktop protocol, RDP) για να επιτρέπει στους χρήστες να διασυνδέονται με άλλον υπολογιστή μέσω μιας διεπαφής γραφικών. Επιτρέπει στους χρήστες να αποκτήσουν πρόσβαση στην επιφάνεια εργασίας άλλου υπολογιστή. Σύμφωνα με τους Scarfone et al. (2009), το λογισμικό πρόσβασης απομακρυσμένης επιφάνειας εργασίας προστατεύει την εμπιστευτικότητα και την ακεραιότητα των επικοινωνιών και επίσης πιστοποιεί την ταυτότητα του χρήστη για να διασφαλίσει ότι κανένας άλλος δεν συνδέεται στον εσωτερικό σταθμό εργασίας. Ωστόσο επειδή αυτό περιλαμβάνει κρυπτογράφηση από άκρο σε άκρο των επικοινωνιών σε όλη την περίμετρο του οργανισμού, τα περιεχόμενα της επικοινωνίας αποκρύπτονται από τα στοιχεία ελέγχου ασφαλείας δικτύου στην περίμετρο, όπως firewall και συστήματα ανίχνευσης εισβολής. Ένα πρόγραμμα πελάτη πρόσβασης απομακρυσμένης επιφάνειας εργασίας εγκαθίσταται σε κάθε συσκευή πελάτη τηλεργασίας και συνδέεται απευθείας με τον αντίστοιχο εσωτερικό σταθμό εργασίας του τηλεργαζόμενου στο εσωτερικό δίκτυο του οργανισμού.

Σχήμα 4. Αρχιτεκτονική πρόσβασης απομακρυσμένης επιφάνειας εργασίας

1.4.Άμεση Πρόσβαση σε Εφαρμογές

Με την άμεση πρόσβαση σε εφαρμογές, η απομακρυσμένη πρόσβαση μπορεί να επιτευχθεί χωρίς τη χρήση λογισμικού απομακρυσμένης πρόσβασης. Ένας τηλεργαζόμενος μπορεί να έχει απευθείας πρόσβαση σε μια μεμονωμένη εφαρμογή, με την εφαρμογή να παρέχει τη δική της ασφάλεια όπως κρυπτογράφηση επικοινωνιών, έλεγχος ταυτότητας χρήστη. Σύμφωνα με τους Souppaya & Scarfone (2016), ένα από τα πιο κοινά παραδείγματα άμεσης πρόσβασης εφαρμογών είναι η διαδικτυακή πρόσβαση στο email, γνωστή και ως Webmail. Ο απομακρυσμένος χρήστης χρησιμοποιεί ένα πρόγραμμα περιήγησης στο Web και συνδέεται με έναν διακομιστή Web που παρέχει πρόσβαση στο email. Ο διακομιστής Ιστού εκτελεί το HTTP μέσω SSL (HTTPS) για την προστασία των επικοινωνιών και η εφαρμογή Webmail στον διακομιστή ελέγχει την ταυτότητα του τηλεργαζόμενου πριν παραχωρήσει πρόσβαση στο email τηλεργαζόμενου. Το (Σχήμα 5) δείχνει την αρχιτεκτονική υψηλού επιπέδου για άμεση πρόσβαση σε εφαρμογές.

Το λογισμικό πελάτη εφαρμογής που είναι εγκατεστημένο στη συσκευή πελάτη τηλεργασίας ξεκινά μια σύνδεση με έναν διακομιστή, ο οποίος βρίσκεται συνήθως στην περίμετρο του οργανισμού. Η αρχιτεκτονική άμεσης πρόσβασης εφαρμογών είναι γενικά αποδεκτή μόνο εάν οι διακομιστές στους οποίους έχουν πρόσβαση οι απομακρυσμένοι χρήστες βρίσκονται στην περίμετρο του δικτύου του οργανισμού ή σε ένα δημόσιο νέφος και όχι σε εσωτερικά δίκτυα. Οι διακομιστές που είναι άμεσα προσβάσιμοι από το Διαδίκτυο θα πρέπει να είναι ήδη καλά ασφαλισμένοι για να μειωθεί η πιθανότητα παραβίασης της ασφάλειας. Πολλοί οργανισμοί επιλέγουν να παρέχουν άμεση πρόσβαση μόνο σε λίγες εφαρμογές χαμηλότερου κινδύνου που χρησιμοποιούνται ευρέως, όπως το ηλεκτρονικό ταχυδρομείο, και να χρησιμοποιούν μεθόδους σήραγγας ή πύλης για να παρέχουν πρόσβαση σε άλλες κρίσιμες εφαρμογές, ιδιαίτερα σε εκείνες που θα διέτρεχαν υπερβολικό κίνδυνο εάν ήταν άμεσα προσβάσιμες από το Διαδίκτυο.

Σχήμα 5. Αρχιτεκτονική άμεσης πρόσβασης εφαρμογής

2 Κίνδυνοι ασφάλειας σε εφαρμογές απομακρυσμένης σύνδεσης

Τα πρόσφατα ευρήματα, όπως τεκμηριώνονται σε κυβερνητικές εκθέσεις [1,2] υποδεικνύουν την απειλή φυσικών επιθέσεων και επιθέσεων που βασίζονται στον κυβερνοχώρο, οι οποίες αυξάνονται σε αριθμούς και σε πολυπλοκότητα σε δίκτυα μεταφοράς ηλεκτρικής ενέργειας και άλλα συστήματα υποδομών ζωτικής σημασίας. Η ανάπτυξη της τεχνολογίας του Διαδικτύου έχει δημιουργήσει σοβαρές προκλήσεις με την απαίτηση για ένα κατάλληλο σύστημα άμυνας στον κυβερνοχώρο για την προστασία των πολύτιμων δεδομένων που είναι αποθηκευμένα στο σύστημα.

Με τα χρόνια, σε συνδυασμό με την τεχνολογική ανάπτυξη και τις ανάγκες, η τεχνολογία του Διαδικτύου έχει αναπτυχθεί, προσφέροντας πολλές λειτουργίες και υπηρεσίες. Η προστασία του Διαδικτύου και των χρηστών του Διαδικτύου έχει γίνει αναπόσπαστο στοιχείο της ανάπτυξης νέων υπηρεσιών καθώς και της κυβερνητικής πολιτικής. Προς αυτόν τον στόχο προτείνεται η μελέτη και κατανόηση των διαφόρων κακόβουλων αντικειμένων. Οι τρεις τρόποι κακόβουλων επιθέσεων σε οποιαδήποτε υποδομή είναι οι εξής:

- επίθεση στο σύστημα.
- επίθεση από το σύστημα. και
- επίθεση μέσω του συστήματος (Ten et al., 2010).

Η καταπολέμηση του εγκλήματος στον κυβερνοχώρο χρειάζεται μια συνολική και ασφαλέστερη προσέγγιση. Ως εκ τούτου, είναι απαραίτητη μια εξίσου ολοκληρωμένη κατανόηση των πολυάριθμων τομέων της ασφάλειας στον κυβερνοχώρο. Χωρίς πλήρη συνειδητοποίηση σε όλους τους τομείς που καλύπτονται από την ασφάλεια στον κυβερνοχώρο, οποιαδήποτε στρατηγική άμυνας στον κυβερνοχώρο θα παραμείνει επιρρεπής σε τρωτά σημεία. Καθώς το πεδίο εφαρμογής της ασφάλειας στον κυβερνοχώρο είναι ευρύ, κάθε καλή στρατηγική ασφάλειας στον κυβερνοχώρο θα πρέπει να τα λαμβάνει όλα υπόψη

2.1 Η ασφάλεια στον κυβερνοχώρο ως παγκόσμια πρόκληση

Η ασφάλεια στον κυβερνοχώρο δεν μπορεί πλέον να εκληφθεί ως καθαρά τεχνικό ζήτημα ασφάλειας υπολογιστών, αλλά μάλλον ως ζήτημα συνολικής πολιτικής καθώς η παράνομη χρήση του Κυβερνοχώρου θα μπορούσε να παρεμποδίσει τις οικονομικές δραστηριότητες, τη δημόσια υγεία, την ασφάλεια και την εθνική ασφάλεια. Οι ηγέτες μια χώρας έχουν ευθύνη για τη χάραξη μιας στρατηγικής για την ασφάλεια στον κυβερνοχώρο και την προώθηση της τοπικής, εθνικής και παγκόσμιας διατομεακής συνεργασίας. Δεδομένου ότι τα τεχνικά μέτρα από μόνα τους δεν μπορούν να αποτρέψουν οποιοδήποτε έγκλημα, είναι σημαντικό να επιτραπεί στις υπηρεσίες επιβολής του νόμου να ερευνούν και να διώκουν αποτελεσματικά το έγκλημα στον κυβερνοχώρο.

Σήμερα πολλά κράτη και κυβερνήσεις επιβάλλουν αυστηρούς νόμους για την κυβερνοασφάλεια για να αποτρέψουν την απώλεια σημαντικών πληροφοριών. Ο κυβερνοχώρος δημιουργεί μοναδικές δυσκολίες λόγω της παγκόσμιας εμβέλειας των σημερινών δικτύων που συνήθως εκτείνονται σε περιοχές δικαιοδοσίας με αδύναμους νόμους και μη επιβολή τους, καθώς και στις γρήγορες ταχύτητες σύνδεσης που δίνουν στα θύματα ελάχιστο χρόνο για να αμυνθούν από επιθέσεις.

2.2 Ασφάλεια υποδομών ζωτικής σημασίας

Οι υποδομές κρίσιμης σημασίας περιλαμβάνει τα κυβερνοφυσικά συστήματα στα οποία βασίζεται η κοινωνία, συμπεριλαμβανομένου του δικτύου μεταφοράς ηλεκτρικής ενέργειας, του δικτύου

[1] Official Website of the Department of Homeland Security, https://www.dhs.gov/topic/cybersecurity

[2] Australian Cyber Security Centre, https://www.cyber.gov.au/

μεταφοράς και καθαρισμού του νερού, των χρηματοοικονομικών συναλλαγών, των φωτεινών σηματοδοτών και του συστήματος υγείας. Ενώ οι υποδομές που χαρακτηρίζονται ως ζωτικής σημασίας μπορεί να διαφέρουν από χώρα σε χώρα. Οι τυπικοί τομείς υποδομής περιλαμβάνουν τους τομείς της υγείας, του νερού, των μεταφορών, των επικοινωνιών, της κυβέρνησης, της ενέργειας, των τροφίμων, των χρηματοοικονομικών και των υπηρεσιών έκτακτης ανάγκης.

Η πολυπλοκότητα των υποδομών παρέχει μεγάλες δυνατότητες για λειτουργία, έλεγχο, επιχειρηματική δραστηριότητα και ανάλυση. Ταυτόχρονα εκθέτει τις υποδομές αυτές σε ένα μεγάλο σύνολο κινδύνων είτε από φυσικές, είτε από ανθρώπινες πηγές, με αυξανόμενο κίνδυνο κακόβουλης κυβερνοεπίθεσης. Η αποτελεσματική προστασία από αυτές τις επιθέσεις απαιτεί ευέλικτες λύσεις. Λύσεις που να μπορούν να προσαρμοστούν στα μοναδικά βιομηχανικά περιβάλλοντα και τις προκλήσεις τους, ενώ ταυτόχρονα θα είναι αρκετά ισχυρές ώστε να κρατούν μακριά ακόμα και τον πιο επίμονο ή προηγμένο αντίπαλο.

Όλοι οι τομείς υποδομής ζωτικής σημασίας βασίζονται σε φυσική υποδομή όπως κτίρια, δρόμοι, δίκτυα, εγκαταστάσεις και αγωγοί. Όλο και περισσότερο, οι κρίσιμοι τομείς βασίζονται επίσης στον Κυβερνοχώρο και στις Τεχνολογίες Πληροφορικής και Επικοινωνιών (ΤΠΕ) που επιτρέπουν την αυτοματοποιημένη λειτουργία τους. Η Υποδομή Κρίσιμων Πληροφοριών (Critical Information Infrastructure, CII) θα πρέπει να λειτουργεί και να ελέγχει τους κρίσιμους τομείς και τα φυσικά στοιχεία τους. Κατά συνέπεια, η διασφάλιση της αξιόπιστης λειτουργίας του Κυβερνοχώρου αποτελεί στρατηγικό στόχο για κάθε χώρα, διότι η έλλειψη εμπιστοσύνης στη χρήση των ΤΠΕ θα μπορούσε να εμποδίσει την καθημερινή ζωή, το εμπόριο και την εθνική ασφάλεια.

Η ηλεκτρονική ασφάλεια είναι εξίσου σημαντική με τη φυσική ασφάλεια λόγω του πιθανού αντίκτυπου που μπορεί να προκληθεί μέσω των λειτουργιών κρίσιμων στοιχείων στον κυβερνοχώρο. Η εξέλιξη των συστημάτων Εποπτικού Ελέγχου και Απόκτησης Δεδομένων (Supervisory Control and Data Acquisition, SCADA) έχει επίσης εγείρει ανησυχίες σχετικά με τα τρωτά σημεία που σχετίζονται με τον κυβερνοχώρο (Safa et al., 2016). Τα συστήματα SCADA είναι κρίσιμα βιομηχανικά συστήματα λόγω της λειτουργικότητάς τους στην επίβλεψη και τον έλεγχο μεγάλων και παγκόσμιων βιομηχανικών δικτύων, όπως τα δίκτυα διανομής ηλεκτρικής ενέργειας και φυσικού αερίου (Elhady et al., 2017).

Επιπλέον, οι αλληλεξαρτήσεις μεταξύ των υπολογιστών, των υποδομών επικοινωνίας και ενέργειας έχουν αυξήσει τους κινδύνους λόγω της πολυπλοκότητας των ολοκληρωμένων υποδομών σύμφωνα με τους Amin & Wollenberg (2005). Ενώ οι τεχνολογικές εξελίξεις μπορούν να βοηθήσουν στη μείωση των ελλείψεων των σημερινών συστημάτων ισχύος και επικοινωνίας (Wu et al., 2005), η τεχνολογική πολυπλοκότητα μπορεί επίσης να οδηγήσει σε παραβιάσεις της ασφάλειας που είναι επιρρεπείς σε ηλεκτρονικές εισβολές.

Μια επιτυχημένη εισβολή στα δίκτυα ελέγχου μπορεί να οδηγήσει σε ανεπιθύμητες λειτουργίες μεταγωγής που εκτελούνται από εισβολείς, με αποτέλεσμα εκτεταμένες διακοπές ρεύματος. Άλλα πιθανά σενάρια είναι η εισβολή σε έναν ή περισσότερους υποσταθμούς και η αλλαγή των ρυθμίσεων του συστήματος προστασίας, που θα μπορούσε να οδηγήσει σε ανεπιθύμητη ενεργοποίηση των αυτόματων διακοπών.

Τα περισσότερα συστήματα άμυνας στον κυβερνοχώρο κατά τη λειτουργία τους γενικά δημιουργούν επιβαρύνσεις, όπως να επιβραδύνουν την απόδοση του υπάρχοντος συστήματος, να αυξάνουν το μήκος του πακέτου ή να απαιτούν περισσότερο χρόνο για σύγκριση. Χρειάζεται λοιπόν η παροχή ενός συστήματος κυβερνοάμυνας, το οποίο δεν θα δημιουργεί περισσότερες επιπλέον επιβαρύνσεις. Και οι δύο τύποι αμυντικών συστημάτων (για την πρόληψη επίθεσης και για την ανάκτηση μετά από επίθεση) θα πρέπει να είναι αρκετά προβλέψιμα στη βάση μαθηματικής μοντελοποίησης υψηλής ακρίβειας. Ως εκ τούτου, για τη διαχείριση όλων αυτών των κινδύνων, απαιτείται ένα ισχυρό πλαίσιο διαχείρισης κινδύνων για την πρόβλεψη των πιο σημαντικών κινδύνων και τη σωστή διαχείριση τους.

2.3 Ασφάλεια δικτύου

Η ασφάλεια δικτύου αφορά την προστασία του δικτύου υπολογιστών του οργανισμού έναντι μη εξουσιοδοτημένης εισβολής καθώς και κακόβουλων εισβολέων. Η διασφάλιση της ασφάλειας του δικτύου απαιτεί συχνά συμβιβασμούς με τη διατήρηση της λειτουργικότητας των χρηστών, για παράδειγμα τα στοιχεία ελέγχου πρόσβασης μπορεί να είναι απαραίτητα αλλά οι περισσότεροι έλεγχοι ταυτότητας των χρηστών μειώνουν την παραγωγικότητα.

Η ασφάλεια δικτύου χρησιμοποιείται για την προστασία των συσκευών δικτύωσης όπως οι μεταγωγείς και δρομολογητές, της διατήρησης της σύνδεσης διαφορετικών δικτύων καθώς και του περιεχομένου που σχετίζεται με το δίκτυο, και συνήθως βασίζεται σε επίπεδα ασφάλειας και αποτελείται από περισσότερα από ένα στοιχεία λογισμικού και υλικού που περιλαμβάνονται στο δίκτυο για την παρακολούθηση της ασφάλειας του δικτύου και των συσκευών του. Όλα τα στοιχεία συνεργάζονται για να αυξήσουν τη συνολική ασφάλεια και απόδοση του δικτύου υπολογιστών.

Η τμηματοποίηση δικτύου επιτρέπει την κατάτμηση σε πολλαπλά τμήματα με περιορισμένη πρόσβαση μεταξύ τους, έτσι ώστε να μετριάζεται ο κίνδυνος από επιθέσεις όπως οι παραλλαγές ransomware *προσγείωση και επέκταση* (*land and expand*). Ένα σωστά διαμορφωμένο τείχος προστασίας (firewall) είναι ένα κρίσιμο μέρος της περιμετρικής ασφάλειας, επίσης οι αλλαγές στο τείχος προστασίας πρέπει να αξιολογούνται για ευπάθειες ασφαλείας.

Επίσης πρέπει να αποφεύγεται η χρήση κοινότυπων κωδικών πρόσβασης στον εξοπλισμό δικτύου και οι κωδικοί πρόσβασης πρέπει να αλλάζουν περιοδικά καθώς και μετά τον τερματισμό απασχόλησης μελών του προσωπικού υποστήριξης. Όλες οι συσκευές τελικού χρήστη του δικτύου υπολογιστών θα πρέπει να είναι διαμορφωμένες και κρυπτογραφημένες με ασφάλεια, με υποστηριζόμενα λειτουργικά συστήματα και με άμεση εφαρμογή των ενημερώσεων συστήματος και εφαρμογών μόλις αυτές γίνονται διαθέσιμες.

2.4 Κινητές συσκευές

Ένα στοιχείο ευπάθειας προκύπτει από την έλλειψη πολιτικών ασφάλειας για την προστασία της πρόσβασης σε ευαίσθητα δεδομένα από μη ασφαλείς κινητές συσκευές, όπως φορητούς υπολογιστές και smartphone, που χρησιμοποιούν οι εργαζόμενοι και αποκτούν εύκολη πρόσβαση στο δίκτυο. Επιπλέον, οι περισσότερες εταιρείες παρέχουν στους επισκέπτες πελάτες ή τους προμηθευτές τους πρόσβαση σε Wi-Fi. Κατά συνέπεια, το μεγαλύτερο μέρος του εγκλήματος στον κυβερνοχώρο προέρχεται από κινητές συσκευές, καθώς πάνω από το 60% της διαδικτυακής απάτης επιτυγχάνεται μέσω πλατφορμών για κινητές συσκευές και το 80% της απάτης για κινητά πραγματοποιείται μέσω εφαρμογών για κινητά αντί για προγράμματα περιήγησης ιστού για κινητά (F-Secure Labs, 2013).

Με περιορισμένη γνώση και επισφαλή συμπεριφορά, οι χρήστες θα μπορούσαν να χρησιμοποιήσουν εν αγνοία τους μολυσμένο υλικό, να υποστούν πειρατεία συσκευής ή ακόμα και να καταλήξουν να χάσουν τις συσκευές τους. Οι πιο συνηθισμένοι κίνδυνοι που σχετίζονται με τη χρήση κινητών συσκευών έχουν ποικίλες επιπτώσεις στην ασφάλεια του κυβερνοχώρου όπου και χρησιμοποιούνται. Το πρόβλημα επίσης μεγεθύνεται από την έλλειψη ετοιμότητας, καθώς στο 67% των οργανισμών οι υπεύθυνοι κυβερνοασφάλειας ομολόγησαν ότι είναι λιγότερο σίγουροι για την ασφάλεια των κινητών συσκευών σε σύγκριση με άλλες συσκευές στο δίκτυό τους (CSEC, 2017).

2.5 Διαχείριση ταυτότητας και πρόσβασης

Η ευθύνη διασφάλισης της Εμπιστευτικότητας, Ακεραιότητας και Διαθεσιμότητας (Confidentiality, Integrity, Availability, CIA) των οργανωτικών και προσωπικών συστημάτων υπολογιστών ανήκει σε ανθρώπους (Teoh et al., 2018). Ο έλεγχος της φυσικής πρόσβασης στην περίμετρο του οικοπέδου, στο κτίριο και στις περιοχές που περιέχουν ευαίσθητα δεδομένα αποτελούν ανησυχία υψηλής ασφάλειας σε διάφορους οργανισμούς. Με παρόμοιο τρόπο, ο στόχος οποιασδήποτε λύσης κυβερνοασφάλειας είναι να ελέγξει ποιος και τι έχει πρόσβαση στις εφαρμογές και τα δεδομένα του οργανισμού και αυτό βρίσκεται στον πυρήνα της Διαχείρισης Ταυτότητας και Πρόσβασης (Identity and Access Management, IAM).

Η χρηματοδότηση έργων διαχείρισης ταυτότητας και πρόσβασης δεν ανήκει σχεδόν ποτέ στις προτεραιότητες μιας επιχείρησης, επειδή τα έργα αυτά δεν αυξάνουν άμεσα ούτε την κερδοφορία ούτε τη λειτουργικότητα. Ωστόσο, η διαχείριση ταυτότητας και πρόσβασης αντιμετωπίζει την κρίσιμη απαίτηση της εξασφάλισης κατάλληλης πρόσβασης σε πόρους σε όλο και πιο ετερογενή τεχνολογικά περιβάλλοντα. Η διαχείριση ταυτότητας σύμφωνα με τους Wu et al. (2005) θα πρέπει να περιλαμβάνει ταυτοποίηση και έλεγχο ταυτότητας ατόμων και συσκευών, φυσικό και λογικό έλεγχο στοιχείων, επιθέσεις ελέγχου πρόσβασης και μέτρα μετριασμού καθώς και την Ταυτότητα ως Υπηρεσία (Identity as a Service, IaaS).

Εκτός από τον περιορισμό της πρόσβασης στους εργαζόμενους της εταιρείας, είναι επίσης σημαντικό να διασφαλιστεί ότι μόνο εξουσιοδοτημένα άτομα έχουν πρόσβαση στο δίκτυο και στα δεδομένα, όπως επίσης και να διασφαλιστεί ότι μόνο εξουσιοδοτημένα άτομα έχουν φυσική πρόσβαση σε αυτούς τους χώρους. Η διαχείριση πρόσβασης ταυτότητας (Identity and Access Management, IAM), ο έλεγχος πρόσβασης βάσει κανόνων (Rules-based Access Control, RAC), ο έλεγχος πρόσβασης βάσει ρόλων (Roles-Based Access Control, RBAC) (CSEC, 2017) και οι μέθοδοι δημιουργίας ταυτότητας συμβάλλουν στην αύξηση της ασφάλειας με τον έλεγχο πρόσβασης ανάλογα με τον τύπο αναγνωριστικού χρήστη που εκδίδεται σε ένα εξουσιοδοτημένο άτομο.

Το IAM διασφαλίζει ότι μόνο τα πιστοποιημένα άτομα μπορούν να έχουν πρόσβαση σε ένα δίκτυο και ελέγχει και περιορίζει τις πληροφορίες που μπορούν να έχουν πρόσβαση αυτά τα άτομα. Ουσιαστικά τα μέτρα IAM επιτρέπουν την πρόσβαση των κατάλληλων ανθρώπων, στους κατάλληλους πόρους, στις κατάλληλες χρονικές στιγμές και για τους κατάλληλους λόγους. Τα στοιχεία ελέγχου πρόσβασης, όπως τα διακριτικά αναγνώρισης φωτογραφίας, οι άδειες περιορισμένης πρόσβασης για πρόσβαση σημάτων, οι κάμερες ασφαλείας, η πολιτική που απαιτεί check-in επισκέπτη, είναι όλα σημαντικά παραδείγματα ελέγχων φυσικής πρόσβασης που θα πρέπει κάθε επιχείρηση να εξετάσει ως προς την εφαρμογή τους.

Οι έλεγχοι όπως τα δικαιώματα περιορισμένης πρόσβασης για την πρόσβαση του τελικού χρήστη στο δίκτυο, οι περιοδικοί έλεγχοι των αδειών πρόσβασης και η άμεση κατάργηση της πρόσβασης λόγω αλλαγής ρόλου ή τερματισμού της ιδιότητας εργαζομένου είναι ιδιαίτερα σημαντικά στοιχεία για ένα ολοκληρωμένο σχέδιο ασφάλειας. Η διαχείριση ταυτότητας ως υπηρεσία (π.χ. ταυτότητα Cloud) αναδεικνύει ζητήματα όπως το ότι το σύστημα είναι εκτός ελέγχου του χρήστη χωρίς τρόπο αυτός να γνωρίζει τι έχει συμβεί με τις πληροφορίες στο σύστημα, σχετικά με τον έλεγχο πρόσβασης, με τη διασφάλιση συμμόρφωσης και την ευελιξία για γρήγορη ανάκληση αδειών.

2.6 Ασφάλεια εφαρμογών

Η ασφάλεια λογισμικού και εφαρμογών εστιάζει στην ανάπτυξη και χρήση λογισμικού που αξιόπιστα διατηρεί τις ιδιότητες ασφαλείας των πληροφοριών και των συστημάτων που προστατεύει (CSEC, 2017). Η ασφάλεια ενός συστήματος και των δεδομένων που αυτό αποθηκεύει και διαχειρίζεται, εξαρτάται σε μεγάλο βαθμό από την ασφάλεια του λογισμικού του. Η ασφάλεια του λογισμικού και των εφαρμογών εξαρτάται από το πόσο καλά ταιριάζουν οι απαιτήσεις με τις ανάγκες που πρέπει να καλύψει το λογισμικό, το πόσο καλά έχει σχεδιαστεί, εφαρμοστεί, δοκιμαστεί, αναπτυχθεί και συντηρηθεί το λογισμικό. Ορισμένες εφαρμογές είναι πιο επιρρεπείς σε απειλές από άλλες. Η τεκμηρίωση είναι ζωτικής σημασίας για να κατανοήσει ο καθένας αυτούς τους λόγους και να αντιμετωπιστούν ζητήματα κατά τη δημιουργία, την ανάπτυξη, τη χρήση και την απόσυρση του λογισμικού.

Οι γνώσεις για την ασφάλεια λογισμικού και εφαρμογών αποτελούνται από θεμελιώδεις αρχές και πρακτικές και αντιμετωπίζουν τα ζητήματα ασφάλειας. Έχει καταστεί ζωτικής σημασίας η αντιμετώπιση βασικών αρχών για την αποφυγή ελαττωμάτων στον σχεδιασμό ασφάλειας λογισμικού (Arce et al., 2014). Οι θεμελιώδεις αρχές σχεδιασμού περιλαμβάνουν τα λιγότερα προνόμια, τον ανοιχτό σχεδιασμό και την αφαίρεση, ενώ οι απαιτήσεις ασφάλειας και ο ρόλος τους στο σχεδιασμό θα πρέπει να προσδιορίζονται με σαφήνεια. Τα ζητήματα υλοποίησης, καθώς και η ρύθμιση παραμέτρων και η ενημέρωση κώδικα θα πρέπει να υποβάλλονται σε ενδελεχή δοκιμή, τόσο στατικά όσο και δυναμικά. Επιπλέον, η προοπτική εξέλιξης θα πρέπει να λαμβάνεται υπόψη με ακρίβεια, ειδικά στην ανάπτυξη, τη δοκιμή και την αποκάλυψη ευπάθειας.

2.7 Ασφάλεια στο cloud

Η μετακίνηση της επιχείρησης σε υπηρεσίες υπολογιστικού νέφους (cloud computing) δημιουργεί νέες προκλήσεις ασφαλείας (Spector, 2008), καθώς από τη μία πλευρά αυτό μπορεί να διευκολύνει την ασφάλεια για τις εταιρείες που αναθέτουν τα δεδομένα τους σε μια υπηρεσία cloud όπου το κόστος της ασφάλειας βαρύνει τον προμηθευτή, αλλά από την άλλη συγκεντρώνει τις υπηρεσίες cloud ως εξαιρετικά ελκυστικούς στόχους για επίθεση.

Το κύριο ζήτημα με το cloud computing είναι ότι το στοιχείο της εμπλοκής κάποιου τρίτου μέρους (ο πάροχος των υπηρεσιών cloud), ευθύνεται για μεγάλο μέρος της απροθυμίας να

υιοθετηθούν υπηρεσίες cloud στο παρελθόν, καθώς υπήρχε η ανησυχία ότι τα δεδομένα θα ήταν λιγότερο ασφαλή λόγω της εμπλοκής του τρίτου μέρους καθώς και της απώλειας φυσικής πρόσβασης στον διακομιστή που φιλοξενεί τα δεδομένα επειδή πλέον δεν βρίσκεται στο κτίριο του οργανισμού,.

Στην πραγματικότητα, τα κέντρα δεδομένων απασχολούν άτομα που έχουν πολύ πιο εξειδικευμένες γνώσεις όσον αφορά τα μέτρα ασφάλειας για την προστασία διακομιστών και δεδομένων (Kuerbis & Badiei, 2017). Οι μεγάλοι οργανισμοί πολλών δισεκατομμυρίων μπορούν να αντέξουν οικονομικά να αφιερώσουν εξειδικευμένους πόρους στην εργασία της ασφάλειας διακομιστή, αλλά ακόμη και η πιο αφοσιωμένη εσωτερική ομάδα δεν θα είναι σε θέση να ανταποκρίνεται στο επίπεδο γνώσεων και δεξιοτήτων των μεγάλων παρόχων υπολογιστικού νέφους.

Η ασφάλεια των δεδομένων cloud δεν αφορά μόνο την κρυπτογράφηση, αλλά και την εξουσιοδότηση πρόσβασης όταν τα δεδομένα βρίσκονται φυσικά σε μια εξωτερική δικαιοδοσία ενός τρίτου μέρους (Spector, 2008). Το λογισμικό ασφάλειας cloud είναι ένα κρίσιμο στοιχείο μιας ολοκληρωμένης στρατηγικής κυβερνοασφάλειας. Ανεξάρτητα από το εάν ένας διακομιστής είναι εντός ή εκτός της εγκατάστασης του οργανισμού, η ασφάλεια στον κυβερνοχώρο και σε επίπεδο cloud απαιτεί λογισμικό εσωτερικής εγκατάστασης που βασίζεται σε σύννεφο που βρίσκεται μεταξύ των χρηστών υπηρεσιών και των εφαρμογών cloud.

Αυτό το λογισμικό παρακολουθεί όλες τις δραστηριότητες των χρηστών, προειδοποιεί τους διαχειριστές για δυνητικά επικίνδυνες ενέργειες, επιβάλλει τη συμμόρφωση με την πολιτική ασφάλειας και αποτρέπει αυτόματα το κακόβουλο λογισμικό. Οι πάροχοι cloud δημιουργούν συνεχώς νέα εργαλεία ασφάλειας για να βοηθήσουν τους εταιρικούς χρήστες να προστατεύουν καλύτερα τα δεδομένα τους. Επιπλέον, οι πάροχοι υπηρεσιών cloud πραγματοποιούν πολύ πιο διεξοδικούς ελέγχους ιστορικού σε υπαλλήλους που έχουν φυσική πρόσβαση σε διακομιστές.

Το Διαδίκτυο μπορεί να μην έχει σύνορα, αλλά τα ίδια τα δεδομένα εξακολουθούν να βρίσκονται εντός των παραδοσιακών ορίων του πραγματικού κόσμου και με τη σειρά τους μπορεί να δεσμεύονται από τους νόμους ενός ξένου κράτους. Ανεξάρτητα από την αξιοπιστία των ισχυόντων νόμων ενός ξένου κράτους, δεν υπάρχει καμία εγγύηση ότι δεν θα αλλάξουν και τα δεδομένα που προστατεύονταν προηγουμένως θα μπορούσαν να προσπελαστούν από κυβερνητικές υπηρεσίες ή να μοιραστούν με τρίτους χωρίς συναίνεση.

Ενώ οι πάροχοι υπηρεσιών cloud όπως το Amazon Web Services (AWS), το Microsoft Azure και το Google Cloud Platform (GCP) συνεχίζουν να επεκτείνουν τις υπηρεσίες ασφαλείας για να προστατεύσουν τις εξελισσόμενες πλατφόρμες cloud τους, είναι τελικά ευθύνη των πελατών να προστατεύουν τα δεδομένα τους σε αυτά τα περιβάλλοντα cloud (Kuerbis & Badiei, 2017).

Διάφορες αναφορές ασφαλείας των τελευταίων ετών (Abomhara & Køien, 2015; Kuerbis & Badiei, 2017) τονίζουν ότι οι ομάδες ασφάλειας cloud πρέπει να επαναξιολογήσουν τη στάση και τις στρατηγικές ασφαλείας τους και να αντιμετωπίσουν τις ελλείψεις των παλαιών εργαλείων ασφαλείας για να προστατεύσουν τα εξελισσόμενα περιβάλλοντα στα πληροφοριακά συστήματα τους. Η ασφάλεια στο cloud θα μπορούσε ενδεχομένως να παραμείνει μια σημαντική ανησυχία καθώς η ουσία παραμένει: Η μετάβαση στο cloud δεν αποτελεί αυτόματα τη λύση σε ότι αφορά την ασφάλεια στον κυβερνοχώρο.

2.8 Ασφάλεια βάσεων δεδομένων

Η ασφάλεια των βάσεων δεδομένων καλύπτει και επιβάλλει την ασφάλεια σε όλες τις πτυχές και τα στοιχεία της βάσης δεδομένων και πρέπει να σχεδιάζεται, υλοποιείται και διατηρείται από έναν διαχειριστή βάσεων δεδομένων ή άλλον επαγγελματία ασφάλειας πληροφοριών. Τα μέτρα ασφάλειας των δεδομένων επικεντρώνονται στην ασφάλεια των ίδιων των δεδομένων σε αντίθεση με τα μέτρα ασφάλειας πρόσβασης που εστιάζουν στην ασφάλεια δικτύων, διακομιστών ή εφαρμογών.

Τα μέτρα για την κυβερνοασφάλεια της βάσης δεδομένων περιλαμβάνουν τον περιορισμό της μη εξουσιοδοτημένης πρόσβασης σε δεδομένα, αλλά και τη φυσική ασφάλεια του διακομιστή και του εφεδρικού εξοπλισμού σε περίπτωση καταστροφής ή αστοχίας. Ορισμένα βασικά στοιχεία αυτού του τομέα της κυβερνοασφάλειας περιλαμβάνουν την εφαρμογή ισχυρού και πολυπαραγοντικού ελέγχου ταυτότητας για τον καλύτερο έλεγχο του ποιος έχει πρόσβαση

στα δεδομένα, καθώς και τον έλεγχο και τη χαρτογράφηση γνωστών τρωτών σημείων. Θα πρέπει επίσης να διεξάγονται δοκιμές φόρτωσης και ακραίων καταστάσεων για να διασφαλιστεί ότι μια βάση δεδομένων δεν θα σταματήσει να λειτουργεί κατά τη διάρκεια επιθέσεων Κατανεμημένης Άρνησης Υπηρεσίας (Distributed Denial of Service, DDoS) ή υπερφόρτωσης.

Οι οργανισμοί θα πρέπει πάντα να στοχεύουν στα ελάχιστα απαιτούμενα προνόμια, που σημαίνει ότι οι τελικοί χρήστες και οι διαχειριστές θα πρέπει να έχουν τον ελάχιστο αριθμό προνομίων που απαιτούνται για να κάνουν τη δουλειά τους και μόνο τις στιγμές που χρειάζονται πρόσβαση. Είναι συχνό το φαινόμενο κάποιοι χρήστες να συγκεντρώνουν προνόμια καθώς μετακινούνται σε ρόλους μέσα στον οργανισμό, η επένδυση σε ισχυρά προϊόντα διαχείρισης πρόσβασης μπορεί να βοηθήσει στην αποφυγή πολύ μεγαλύτερου κόστους που ίσως προκύψει από συμβάντα ασφαλείας και παραβιάσεις δεδομένων που προκαλούνται από τη συγκέντρωση προνομίων.

2.9 Ασφάλεια Internet of Things

Οι προκλήσεις και οι απειλές για την ασφάλεια στο IoT πρέπει να αναγνωρίζονται για να ληφθούν προστατευτικά μέτρα. Ο γενικός στόχος πρέπει να είναι ο εντοπισμός των πολύτιμων στοιχείων και η τεκμηρίωση πιθανών απειλών, επιθέσεων και τρωτών σημείων που αντιμετωπίζει το IoT. Με πολλές προκλήσεις ασφαλείας που έχουν εντοπιστεί, όπως η εμπιστευτικότητα, το απόρρητο και η εμπιστοσύνη των οντοτήτων, ήταν σαφές ότι οι προκλήσεις ασφάλειας και απορρήτου πρέπει να αντιμετωπιστούν. Επιπλέον, η έρευνα θα πρέπει να δώσει επιπλέον έμφαση στις κυβερνοαπειλές που περιλαμβάνουν παράγοντες, κίνητρα και ικανότητες που τροφοδοτούνται από τα μοναδικά χαρακτηριστικά του Κυβερνοχώρου.

Είναι σημαντικό για τα επερχόμενα πρότυπα να αντιμετωπίσουν τις ελλείψεις των υφιστάμενων μηχανισμών ασφάλειας IoT (Abomhara & Køien, 2015). Ως μελλοντική εργασία, ο στόχος είναι η βαθύτερη κατανόηση των απειλών που αντιμετωπίζει η υποδομή IoT καθώς και ο εντοπισμός των απειλών κατά του IoT. Οι ορισμοί των κατάλληλων μηχανισμών ασφαλείας για τον έλεγχο πρόσβασης, τον έλεγχο ταυτότητας, τη διαχείριση ταυτότητας και ένα ευέλικτο πλαίσιο διαχείρισης εμπιστοσύνης θα πρέπει να λαμβάνονται υπόψη από την αρχή της ανάπτυξης του προϊόντος. Τα κύρια ζητήματα στην ασφάλεια του IoT θα πρέπει να αντιμετωπιστούν διεξοδικά, παρέχοντας καλύτερη κατανόηση των απειλών και των ιδιοτήτων τους που προέρχονται από διάφορους εισβολείς, όπως κακόβουλους χρήστες ή ανταγωνιστικές οργανώσεις.

2.10 Ευαισθητοποίηση για την ασφάλεια στον κυβερνοχώρο

Στην κυβερνοασφάλεια είναι δύσκολη η ανίχνευση της προσπάθειας του εισβολέα εξαιτίας της χαμηλότερης εκπαίδευσης και ευαισθητοποίησης. Ο πιο αδύναμος κρίκος στην αλυσίδα κυβερνοασφάλειας μιας εταιρείας είναι συνήθως οι άνθρωποι της και κυρίως λόγω έλλειψης επαρκούς γνώσης και ευαισθητοποίησης, συχνά οι ίδιοι οι εργαζόμενοι ανοίγουν τις πύλες στους επιτιθέμενους.

Η ευαισθητοποίηση σχετικά με την ασφάλεια για τις αναδυόμενες τεχνολογίες είναι κρίσιμης σημασίας για την πρόληψη των επιθέσεων στον κυβερνοχώρο. Λίγες μόνο χώρες διαθέτουν ορισμένες κατάλληλες πολιτικές και σύστημα εκπαίδευσης και ευαισθητοποίησης. Επομένως, για να περιοριστούν τέτοιου είδους κακόβουλες δραστηριότητες, η κοινωνία μας πρέπει να επινοήσει ένα κατάλληλο σύνολο πολιτικών.

Μια κατάλληλη στρατηγική άμυνας στον κυβερνοχώρο θα πρέπει να αναθέτει την ευθύνη για τον συντονισμό των εκστρατειών ευαισθητοποίησης για την ασφάλεια στον κυβερνοχώρο και των δραστηριοτήτων σε εθνικό επίπεδο σε μια αρμόδια αρχή για να διασφαλίσει την επιτυχία της εκστρατείας ενημέρωσης. Η ευαισθητοποίηση για την ασφάλεια στον κυβερνοχώρο προωθεί θεμελιώδη κατανόηση σχετικά με τις απειλές και τους κινδύνους και τις κατάλληλες επιλογές αντίδρασης, ενημερώνει τους πολίτες για τις βέλτιστες πρακτικές και τα προληπτικά μέτρα όταν έρχονται αντιμέτωποι με κινδύνους στον κυβερνοχώρο.

Η δημόσια αρχή θα πρέπει να συνεργάζεται με τους σχετικούς ενδιαφερομένους για την ανάπτυξη και εφαρμογή προγραμμάτων ευαισθητοποίησης για την ασφάλεια στον κυβερνοχώρο που εστιάζουν στη διάδοση πληροφοριών σχετικά με κινδύνους και απειλές στον κυβερνοχώρο, καθώς και για βέλτιστες πρακτικές για την αντιμετώπισή τους. Τα κράτη θα πρέπει να προωθούν

την ευαισθητοποίηση για τις απειλές που σχετίζονται με τον κυβερνοχώρο μεταξύ του κοινού, των εταιρειών και των κρατικών οργανισμών.

Ένα πρόγραμμα ευαισθητοποίησης για την ασφάλεια στον κυβερνοχώρο θα μπορούσε να περιλαμβάνει εκστρατείες ευαισθητοποίησης που απευθύνονται είτε στο ευρύ κοινό, είτε στα παιδιά είτε σε στελέχη σε δημόσιο και ιδιωτικό τομέα προωθώντας επιμορφωτικά προγράμματα. Η εκπαίδευση των τελικών χρηστών αφορά την εκπαίδευση των εργαζομένων αλλά και τον έλεγχο και τη δοκιμή ότι ακολουθούν τις συμβουλές που τους δίνονται και θα βοηθήσει στην πρόληψη του κινδύνου ανθρώπινου λάθους.

3 Αντιμετώπιση Κινδύνων Ασφάλειας Εφαρμογών Απομακρυσμένης Σύνδεσης

Υπάρχουν διάφοροι έλεγχοι ασφαλείας για την αντιμετώπιση τρωτών σημείων στην απομακρυσμένη πρόσβαση. Οι έλεγχοι ασφαλείας όπως για παράδειγμα το antivirus, βασίζονται σε υπογραφές όπου η γνώση της παραλλαγής κακόβουλου λογισμικού είναι απαραίτητη για τον αποτελεσματικό εντοπισμό του.

Οι προσεγγίσεις που βασίζονται σε ευεργετικές μεθόδους, είναι επιρρεπείς σε υψηλό ποσοστό ψευδών θετικών αποτελεσμάτων και χρειάζονται πολύ χρόνο για να αναλυθεί η επισκεψιμότητα για κακόβουλο λογισμικό και άλλους κινδύνους ασφάλειας δικτύων. Με τα χρόνια, έχουν αναπτυχθεί και εφαρμοστεί αρκετές προσεγγίσεις για τη διασφάλιση της ασφάλειας στα δίκτυα, ένας σημαντικός αριθμός επικεντρώνεται στην ασφάλεια της απομακρυσμένης πρόσβασης. Οι παρακάτω είναι παραδοσιακές προσεγγίσεις στην ασφάλεια απομακρυσμένης πρόσβασης.

3.1 Έλεγχος Πρόσβασης Δικτύου (Network Access Control, NAC)

Ο Έλεγχος Πρόσβασης Δικτύου (NAC) είναι μια εφαρμογή για τον προσδιορισμό της υγείας και της κατάστασης των συσκευών που ζητούν πρόσβαση σε πόρους δικτύου. Επιβάλλει την πολιτική ασφάλειας, αποτρέπει την πρόσβαση από μη εξουσιοδοτημένες συσκευές ελέγχοντας διάφορες προκαθορισμένες καταστάσεις, όπως εγκατάσταση και ενημερώσεις για προγράμματα προστασίας από ιούς, ενημερώσεις κώδικα, διεύθυνση IP, διεύθυνση MAC (Media Access Control, ελέγχου πρόσβασης μέσων) ή ακόμη και πολιτική κωδικού πρόσβασης (Ciampa, 2012).

Οποιαδήποτε συσκευή δεν πληροί τις απαιτήσεις ασφάλειας δικτύου, τίθεται σε καραντίνα ώστε να αποτραπεί η σύνδεση απομακρυσμένων συσκευών που ενδέχεται να τεθούν σε κίνδυνο. Η εξέταση της συσκευής ταξινομεί τις συσκευές ως ασφαλείς ή μη, επιτρέποντας μόνο την ασφαλή πρόσβαση στο δίκτυο. Οι πολιτικές ασφάλειας πληροφοριών χρησιμοποιούνται για να καθοριστεί εάν μια συσκευή πληροί τις προκαθορισμένες απαιτήσεις. Το NAC διασφαλίζει τη συμμόρφωση με τις πολιτικές ασφαλείας του οργανισμού για κάθε απομακρυσμένη συσκευή και επιτρέπει ή αρνείται την πρόσβαση στο δίκτυο με:

- Ταυτοποίηση και έλεγχο ταυτότητας.
- Επιβολή πολιτικής ασφάλειας δικτύου.
- Διαλογή συσκευών, η ασφαλής απομακρυσμένη συσκευή έχει πρόσβαση σε δεδομένα ή εάν δεν είναι ασφαλής τίθεται σε καραντίνα.
- Η απομακρυσμένη συσκευή έχει πρόσβαση σε δεδομένα και πόρους αφού συμμορφωθεί με τις πολιτικές ασφαλείας.
- Η απομακρυσμένη συσκευή αποσυνδέεται εάν δεν συμμορφώνεται.
- Συνεχής έλεγχος στο δίκτυο και κάθε προσπάθεια σύνδεσης.

Ωστόσο, ο διακομιστής NAC μπορεί να κλειδώσει οποιαδήποτε συσκευή δεν θεωρείται ασφαλής από τον οργανισμό, όπως οι μη διαχειριζόμενες συσκευές. Το κλείδωμα σημαίνει ότι η διαθεσιμότητα είναι περιορισμένη, για παράδειγμα, εάν ο υπάλληλος συνδέεται χωρίς συσκευή που έχει εκδοθεί από τον οργανισμό, δεν θα υπάρχουν μέσα πρόσβασης στα δεδομένα και πόρους που μπορεί να χρειάζονται, γεγονός που μπορεί να καταλήξει να εμποδίζει την επιχείρηση ή τις βασικές λειτουργίες.

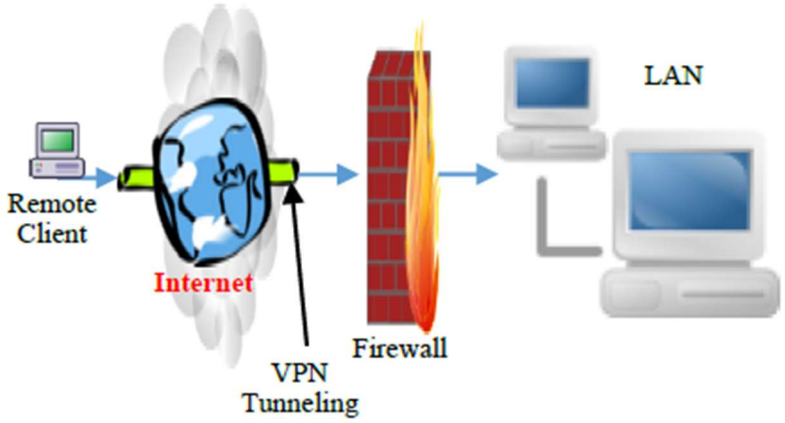
Επιπλέον, ακόμη και για μια συσκευή που θα μπορούσε να θεωρηθεί ασφαλής, μόλις δημιουργηθεί μια συνεδρία, δεν θα υπήρχε κανένας τρόπος αξιολόγησης της νομιμότητας όπως κρυπτογραφημένης κίνησης στη σήραγγα.

3.2 Εικονικό Ιδιωτικό Δίκτυο (VPN)

Ένα VPN συνδέει με ασφάλεια έναν απομακρυσμένο χρήστη ή συσκευή σε ένα εσωτερικό ή ιδιωτικό δίκτυο (Harmening, 2017). Χρησιμοποιεί το Διαδίκτυο ή οποιοδήποτε άλλο μη ασφαλές δίκτυο για τη μετάδοση δεδομένων εγκαθιστώντας μια σήραγγα και τους μηχανισμούς ασφαλείας για την αποτροπή πρόσβασης και υποκλοπής δεδομένων από μη εξουσιοδοτημένους χρήστες. Η σήραγγα παρέχει κρυπτογράφηση και ακεραιότητα δεδομένων.

Ο απομακρυσμένος χρήστης ή η συσκευή που είναι συνδεδεμένη σε ένα εικονικό ιδιωτικό δίκτυο ενεργεί ως τοπικός χρήστης συνδεδεμένος στο τοπικό δίκτυο. Ένα VPN διευκολύνει την ασφαλή πρόσβαση σε δεδομένα από διαφορετικές γεωγραφικές τοποθεσίες με χρήση του Διαδικτύου και την πρόσβαση σε ιστότοπους ή εφαρμογές που έχουν αποκλειστεί στην τοποθεσία του απομακρυσμένου χρήστη.

Τα VPN μπορούν να ταξινομηθούν ανάλογα με το περιβάλλον εφαρμογής τους όπου τα περιβάλλοντα περιλαμβάνουν τοπικό δίκτυο (LAN), απομακρυσμένη πρόσβαση και χρήση εκτός δικτύου. Το (Σχήμα 6) παρακάτω δείχνει ένα συμβατικό VPN απομακρυσμένης πρόσβασης που συνδέει απομακρυσμένες συσκευές στο εσωτερικό δίκτυο.

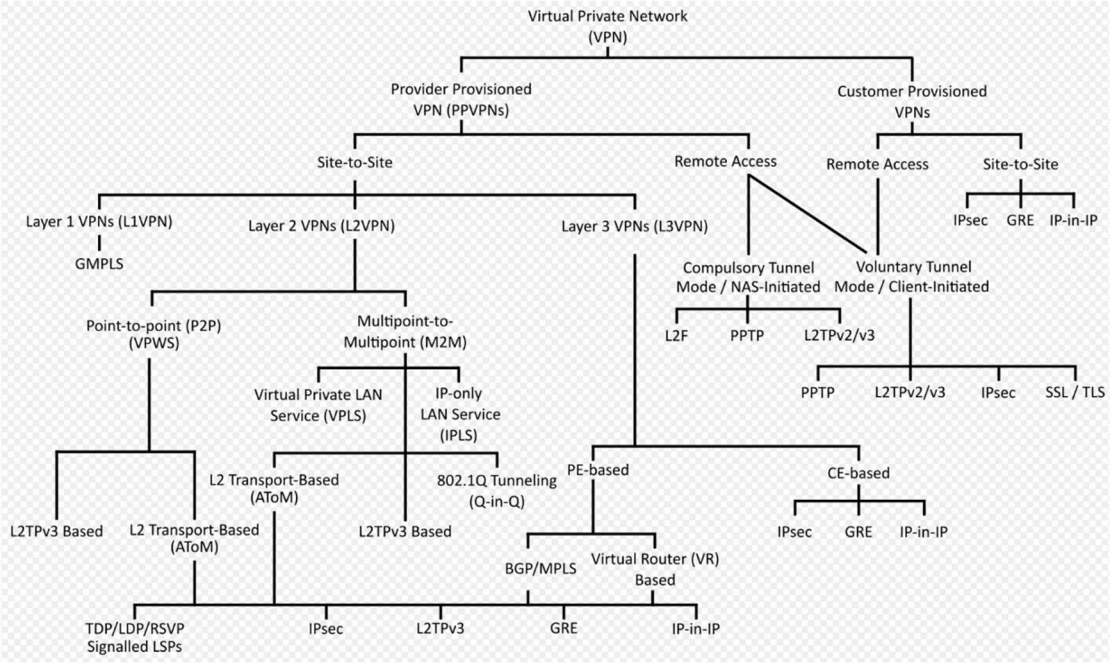


Σχήμα 6. Ένα VPN απομακρυσμένης πρόσβασης.

Το tunneling μπορεί να είναι εθελοντικό ή υποχρεωτικό, εθελοντικό είναι όταν δημιουργείται μια σύνδεση κατόπιν αιτήματος από την απομακρυσμένη συσκευή ή χρήστη. Ο πάροχος υπηρεσιών ρυθμίζει και διαχειρίζεται το υποχρεωτικό tunneling και τη σύνδεση διακομιστή VPN. Τα πρωτόκολλα VPN περιλαμβάνουν πρωτόκολλο σήραγγας από σημείο σε σημείο (point-to-point tunneling protocol, PPTP), πρωτόκολλο σήραγγας επιπέδου δύο (layer two tunneling protocol, L2TP) και ασφάλεια πρωτοκόλλου διαδικτύου (internet protocol security, Ipsec).

Το IPsec λειτουργεί είτε σε λειτουργία σήραγγας όπου κρυπτογραφείται ολόκληρο το πακέτο IP είτε σε κατάσταση μεταφοράς όπου τα δεδομένα και το πακέτο IP είναι κρυπτογραφημένα και η κεφαλίδα του πακέτου παραμένει μη κρυπτογραφημένη. Ο συγκεντρωτής VPN είναι όπως μηχανισμός διακομιστή για την επικύρωση και την εξουσιοδότηση αιτημάτων σύνδεσης VPN.

Οι απομακρυσμένες συσκευές συνδέονται με τον συγκεντρωτή VPN. Ωστόσο, ένα VPN εισάγει και μερικές απρόβλεπτες προκλήσεις για την ασφάλεια του εσωτερικού δικτύου, με τις σημαντικότερες να είναι κακόβουλο λογισμικό, botnet και DdoS. Εάν μολυνθεί μια απομακρυσμένη συσκευή, η παραβιασμένη κίνηση θα μεταδοθεί χωρίς τους περιμετρικούς ελέγχους ασφαλείας, όπως το τείχος προστασίας ή το Σύστημα Ανίχνευσης Εισβολής (Intrusion Detection System, IDS) να προκαλούν συναγερμό, καθώς δεν είναι σε θέση να αναλύσουν την κρυπτογραφημένη κίνηση. Επομένως, το βασικό πλεονέκτημα και η ισχύς του VPN χρησιμοποιούνται για την αποφυγή μηχανισμών ανίχνευσης.



Σχήμα 7. Κατηγορίες/Πρωτόκολλα VPN

Πιο αναλυτικά, όπως θα δείτε και στο παραπάνω σχεδιάγραμμα, ένα Virtual Private Network (VPN) χωρίζεται σε δύο βασικές κατηγορίες. Η πρώτη κατηγορία είναι VPN συνδέσεις από τον Πάροχο (Provider Provisioned VPN, PPVPN) και η δεύτερη κατηγορία είναι VPN του Πελάτη (Customer Provisioned VPN). Από τις δύο παραπάνω κατηγορίες θα επικεντρωθούμε στις υποκατηγορίες της απομακρυσμένης σύνδεσης και τα πρωτόκολλα που χρησιμοποιούν.

Η κατηγορία VPN του Πελάτη (Customer Provisioned VPN), είναι όταν ο χρήστης δημιουργεί και διαχειρίζεται τις συνδέσεις VPN μόνος του. Τα Tunnel που δημιουργούνται είναι μεταξύ τoy χρήστη και του route που βοηθάει στην σύνδεση του τερματικού προς το Internet (Customer Edge, CE). Η συγκεκριμένη κατηγορία, εμφανίζει δύο υποκατηγορίες, τα Site-to-Site VPN (S2S VPN) και την απομακρυσμένη πρόσβαση (Remote Access). Για τις ανάγκες τις διατριβής, η κατηγορία που υπόκεινται η διατριβή και θα αναλύσουμε είναι του Remote Access. Όπως θα δείτε και στο παραπάνω (Σχήμα 7) δημιουργείται μια «αυθόρμητη δίοδος» (Voluntary Tunnel) από τον χρήστη και συμπεριλαμβάνει τα παρακάτω πρωτόκολλα:

a) *Point-to-Point Tunneling Protocol (PPTP):* Πρόκειται για το πρωτόκολλο το οποίο είναι μια παλαιά μέθοδος για την υλοποίηση εικονικών ιδιωτικών δικτύων VPN. Για το συγκεκριμένο πρωτόκολλο αναφέρονται αρκετά ζητήματα ασφαλείας. Το PPTP χρησιμοποιεί το πρωτόκολλο TCP και μια γενικού τύπου δίοδο για την ενθυλάκωση των πακέτων Point-2-Point Protocol (PPP). Πολλές σύγχρονες μέθοδοι VPN χρησιμοποιούν πρωτόκολλο UDP για την ίδια λειτουργία. Η προδιαγραφές για το Point-2-Point Protocol (PPTP) δεν περιέχουν χαρακτηριστικά κρυπτογράφησης ή ελέγχου ταυτότητας και βασίζεται στη μεταφορά δεδομένων από σημείο σε σημείο για την υλοποίηση οποιονδήποτε λειτουργιών ασφαλείας. Το πρωτόκολλο PPTP που χρησιμοποιείται από τα προϊόντα της Microsoft, εφαρμόζει διάφορα επίπεδα ελέγχου ταυτότητας και κρυπτογράφησης ως τυπικές δυνατότητες του PPTP των Windows. Η βέλτιστη χρήση αυτού του πρωτοκόλλου θα ήταν να παρέχει επίπεδα ασφάλειας και επίπεδα απομακρυσμένης πρόσβασης συγκρίσιμα με άλλα προϊόντα VPN.
b) *Layer 2 Tunneling Protocol (L2TP):* Στη δικτύωση των υπολογιστών, το Layer 2 Tunneling Protocol (L2TP) είναι ένα πρωτόκολλο που χρησιμοποιείται για την υποστήριξη εικονικών ιδιωτικών δικτύων (VPN) ως μέρος της παροχής υπηρεσιών από τους Παρόχους (Internet Service Provider, ISP). Χρησιμοποιεί κρυπτογράφηση με σκοπό να αποκρύψει μόνο τα δικά του μηνύματα ελέγχου και δεν παρέχει καμία κρυπτογράφηση ή εμπιστευτικότητα του περιεχομένου του. Αντίθετα το πρωτόκολλο, παρέχει μια σήραγγα για το Επίπεδο 2 (το οποίο μπορεί να είναι κρυπτογραφημένο) και η ίδια η σήραγγα

μπορεί να περάσει πάνω από ένα πρωτόκολλο κρυπτογράφησης επιπέδου 3 όπως το Internet Protocol Security (IPsec).

c) *Internet Protocol Security (IPsec):* Το IPsec protocol, είναι μια ομάδα πρωτοκόλλων που χρησιμοποιούνται για τη δημιουργία κρυπτογραφημένων συνδέσεων μεταξύ συσκευών. Βοηθά στη διατήρηση ασφαλών δεδομένων που αποστέλλονται μέσω δημόσιων δικτύων. Το IPsec πρωτόκολλο, χρησιμοποιείται συχνά για τη ρύθμιση των VPN και λειτουργεί κρυπτογραφώντας τα πακέτα IP σε συνδυασμό με τον έλεγχο ταυτότητας της πηγής από την οποία προέρχονται τα πακέτα.
d) *Secure Sockets Layer (SSL):* Το SSL πρωτόκολλο, είναι ένα πρωτόκολλο ασφαλείας Διαδικτύου που βασίζεται στην κρυπτογράφηση. Αναπτύχθηκε για πρώτη φορά από τη Netscape το 1995 με σκοπό τη διασφάλιση του απορρήτου, του ελέγχου ταυτότητας και της ακεραιότητας των δεδομένων στις επικοινωνίες του Διαδικτύου. Το SSL είναι ο προκάτοχος της σύγχρονης κρυπτογράφησης TLS που χρησιμοποιείται σήμερα και
e) *Transport Layer Security (TLS):* Το TLS είναι ένα πρωτόκολλο που χρησιμοποιεί κρυπτογράφηση και παρέχει ασφάλεια από άκρο σε άκρο (End-2-End, E2E) των δεδομένων που αποστέλλονται μεταξύ εφαρμογών. Χρησιμοποιείται ευρέως από τους χρήστες για την ασφαλή περιήγηση στο διαδίκτυο και συγκεκριμένα εμφανίζεται στο εικονίδιο του λουκέτου των εκάστοτε προγραμμάτων περιήγησης ιστού και εμφανίζεται όταν δημιουργείται μια ασφαλής λειτουργία σύνδεσης. Επιπροσθέτως, μπορεί να χρησιμοποιηθεί και σε άλλες εφαρμογές όπως e-mail, μεταφορές αρχείων, βίντεο/τηλεδιάσκεψη, ανταλλαγή άμεσων μηνυμάτων και φωνή μέσω IP, καθώς και υπηρεσίες Διαδικτύου όπως DNS και NTP.

Έπειτα την παραπάνω ανάλυση, ερχόμαστε στην δεύτερη κατηγορία των VPN, που είναι οι συνδέσεις VPN από τον Πάροχο (Provider Provisioned VPN, PPVNP). Τα Εικονικά Ιδιωτικά Δίκτυα από τον Πάροχο (PPVPN) είναι VPN σε εταιρικό επίπεδο που χρησιμοποιούνται κυρίως από επιχειρήσεις για να επιτρέπουν στο προσωπικό ασφαλή απομακρυσμένη πρόσβαση στο εταιρικό τους δίκτυο. Τα PPVPN χρησιμοποιούνται επίσης για την ασφαλή σύνδεση φυσικών τοποθεσιών και δικτύων μεταξύ τους μέσα από το Διαδίκτυο. Όπως και στην κατηγορία VPN από τον Πελάτη (Customer Provisioned VPN), έτσι και στο VPN που παρέχεται από τον Πάροχο, υπάρχουν κατηγορίες/πρωτόκολλα οι οποίες βοηθούν στο να γίνει πιο ασφαλή η σύνδεση σε απομακρυσμένη επιφάνεια. Σε αντίθεση με την κατηγορία VPN από τον Πελάτη, το VPN από τον Πάροχο, περιέχει και «αυθόρμητες διόδους» (voluntary tunnels) και «αναγκαστικές» δίοδοι (compulsory ή mandatory tunnels). Συνεπώς, πέραν του ότι χρησιμοποιεί όλα τα πρωτόκολλα για την υποκατηγορία «αυθόρμητες διόδους» (voluntary tunnels) που αναφέρθηκαν παραπάνω, χρησιμοποιεί και τα παρακάτω πρωτόκολλα:

a) *Layer Two Forwarding (L2F):* Το Layer Two Forwarding (L2F) είναι ένα πρωτόκολλο σήραγγας που δημιουργήθηκε από την Cisco και χρησιμοποιεί εικονικά δίκτυα μέσω τηλεφώνου για ασφαλή μεταφορά πακέτων δεδομένων. Η λειτουργικότητα του L2F είναι παρόμοια με το Πρωτόκολλο Σήραγγας Σημείου προς Σημείο (PPTP) που αναφερθήκαμε πιο πανω, το οποίο αναπτύχθηκε από το Φόρουμ PPTP υπό την ηγεσία της Microsoft. Το L2F δημιουργεί συνδέσεις δικτύου και χρήστη από σημείο σε σημείο (P2PP) και επιτρέπει σε πρωτόκολλα υψηλού επιπέδου να δημιουργούν σήραγγες μέσα στο επίπεδο σύνδεσης. Σε αυτό το επίπεδο συμπεριλαμβάνονται και πλαίσια ελέγχου σύνδεσης δεδομένων υψηλού επιπέδου (High-Level Data Link Control, HDLC) ή πλαίσιο Πρωτοκόλλου Διαδικτύου Σειριακής Γραμμής (Serial Line Internet Protocol, SLIP). Αυτές οι σήραγγες χωρίζουν τα σημεία διακομιστή και τερματικού με σκοπό την πρόσβαση στο δίκτυο.

Επιπλέον, στην κατηγορία «αναγκαστικές» δίοδοι (compulsory ή mandatory tunnels) χρησιμοποιούνται και τα πρωτόκολλα Point-to-Point (PPTP) καθώς επίσης και Layer 2 Tunneling Protocol (L2TP).

Με τα παραπάνω πρωτόκολλα, ολοκληρώνεται η ανάλυση των πρωτοκόλλων που χρησιμοποιούνται από clients και Παρόχους με σκοπό να γίνεται πιο ασφαλής η σύνδεση μεταξύ τερματικών.

Τέλος, τα πρωτόκολλα/στρατηγικές που χρησιμοποιούνται αρκετά από εταιρίες και οργανισμούς και αναφέρονται ως πιο ασφαλή για απομακρυσμένες συνδέσεις είναι τα παρακάτω:

1) Δημιουργία VPN σύνδεσης στο δίκτυο του οργανισμού και έπειτα σύνδεση με το αντίστοιχο τερματικό
2) IPsec VPN που χρησιμοποιεί ένα γκρουπ από πρωτόκολλα δικτύου στα οποία κρυπτογραφείται η σύνδεση
3) SSL VPN που χρησιμοποιεί αυθεντικοποίηση και κρυπτογράφηση των δεδομένων έτσι ώστε οι χρήστες να μπορούν μέσω διαδικτύου να έχουν πρόσβαση σε δεδομένα και εταιρικές εφαρμογές
4) Κοινή χρήση επιφάνειας εργασίας όπου μπορεί κάποιος χρήστης σε ζωντανό χρόνο να μοιραστεί την επιφάνεια εργασίας και σε συνδυασμό του χρήστη που είναι συνδεδεμένος στο τερματικό και του απομακρυσμένου χρήστη να γίνει διαμοιρασμός της ίδιας επιφάνειας εργασίας
5) SSH remote access που είναι δικτυακό πρωτόκολλο και επιτρέπει στους χρήστες να συνδέονται χωρίς την χρήση κωδικού μέσα από ασφαλή σύνδεση σε τερματικά γραμμής εντολών (Command Line Interface, CLI)
6) Χρήση NAC όπου παρέχει πρόσβαση σε εταιρικό δίκτυο και χρησιμοποιεί συνδυασμό αυθεντικοποίησης, ασφάλεια τερματικού και πολιτικές ασφάλειας του δικτύου. Το NAC μπορεί να αποτρέψει επιθέσεις προτού φτάσουν στο δίκτυο της εταιρίας.
7) Single Sign-on (SSO) όπου χρησιμοποιεί την αυθεντικοποίηση του χρήστη και παρέχει πρόσβαση σε αρκετές εφαρμογές και δεδομένα της εταιρίας με την χρήση μόνο μιας μεθόδου ταυτοποίησης.
8) Zero Trust network access (ZTNA) είναι σύστημα το οποίο ενεργοποιεί ασφαλή πρόσβαση σε εφαρμογές στο δίκτυο μέσω αυθεντικοποίησης. Το συγκεκριμένο μοντέλο είναι ασφαλής διότι δεν αποδέχεται τους χρήστες αυτόματα και παρέχει μόνο τις σωστές προσβάσεις με βάση τους ρόλους που έχει ο χρήστη, τα λιγότερα προνόμια και παρέχει πρόσβαση σε περιοδικό χρόνο.
9) Context-base remote access είναι στρατηγική η οποία περιέχει ένα γκρουπ από προσβάσεις σε αρκετά επίπεδα ανάλογα τον κίνδυνο. Παρέχει ευελιξία στον έλεγχο ταυτότητας πολλών παραγόντων (Multi-factor authentication, MFA). Δημιουργεί ένα προφίλ αξιολόγησης κινδύνου στις προσβάσεις του χρήστη αναλύοντας την συμπεριφορά και το πλαίσιο των χρηστών, όπως την συσκευή σύνδεσης, ζώνη σύνδεσης ή και ακόμα το δίκτυο από το οποίο συνδέονται.
10) Privileged access management (PAM) είναι ένα σύνολο από στρατηγικές κυβερνοασφάλειας οι οποίες ασφαλίζουν, διαχειρίζονται και ελέγχουν τα πλεονεκτήματα χρηστών σε ένα IT δίκτυο. Το συγκεκριμένο σύνολο, ελέγχει τους χρήστες, τους λογαριασμούς, τις εφαρμογές, τα συστήματα και τις διεργασίες που υφίσταται σε ένα δίκτυο.

3.3 Ασφάλεια δικτύου με εφαρμογές Τρίτων

Αρκετές εταιρίες που διαχειρίζονται πληροφορίες, επιλέγουν συστήματα και εφαρμογές οι οποίες θα βοηθήσουν τον οργανισμό να διαχειριστεί και να ελέγξει την απομακρυσμένη πρόσβαση των χρηστών με ασφάλεια. Τέτοιες εφαρμογές, χρησιμοποιούν πρωτόκολλα σύνδεσης όπως αναφέραμε σε προηγούμενη ενότητα και μας επιτρέπουν να συνδεθούμε εύκολα, γρήγορα και κυρίως με ασφάλεια σε απομακρυσμένα συστήματα.

Παρακάτω θα κάνουμε μια αναφορά σε τέτοιες εφαρμογές και λογισμικά από εταιρίες που κατέχουν μεγάλο κομμάτι στον χώρο της τεχνολογίας και έχουν αναπτύξει αρκετά τους τρόπους ασφάλειας:

1) *Endpoint detection and response (EDR):* Πρόκειται για ένα εργαλείο το οποίο ως κύριες λειτουργίες έχει:
    a. Τον έλεγχο και την συλλογή πληροφοριών από τερματικά τα οποία μπορεί να αποτελούν απειλή
    b. Ανάλυση δεδομένων με σκοπό να γίνει η αναγνώριση του πρότυπου απειλής
    c. Αυτόματη ανταπόκριση σε απειλές οι οποίες εντοπίζονται και προχωράει στην αφαίρεση ή τον περιορισμό τους και ταυτόχρονα ειδοποιεί το προσωπικό ασφαλείας/διαχειριστή
    d. Forensic & security ανάλυση με εργαλεία τα οποία διαθέτει με σκοπό να γίνει η κατανόηση και εύρεση των ύποπτων δραστηριοτήτων.

Αν και το EDR αποτελεί ένα πολύ εξελιγμένο σύστημα ανάλυσης, ελέγχου και περιορισμού ύποπτης δραστηριότητας, παρά τα προβλήματα που έχουν αναφερθεί (Karantzas G., Patsakis C., 2021). Οι δοκιμές που έγιναν στο παραπάνω άρθρο χωρίζουν τους τύπους επιθέσεων σε 4 vectors με την χρήση αρχείων .DLL, .CPL, .HTA και EXE-DLL εκτελέσιμων.

Παρόλο που το EDR είναι ένα εξελιγμένο εργαλείο, πέραν του ότι σε κάποιες από τις παραπάνω επιθέσεις ανταποκρίθηκε και μπλόκαρε τα αντίστοιχα αρχεία-ενέργειες, υπήρξαν περιπτώσεις στις οποίες είτε το alert χαρακτηρίστηκε ως χαμηλού κινδύνου είτε δεν ανιχνεύτηκε καθόλου.

2) *Check Point:* Πρόκειται για μια εταιρία η οποία δραστηριοποιείται στον τομέα ασφάλειας δικτύων και χρηστών. Πιο συγκεκριμένα, παρέχει υπηρεσία ασφάλειας δικτύου στην οποία μπορεί να προστατέψει από επιθέσεις Gen VI και αντίστοιχα να κλείσει κενά ασφάλειας, να ανταλλάξει δεδομένα επιθέσεων για την διατήρηση ασφάλειας του περιβάλλοντος και όλα αυτά μέσα από ένα φιλικό προς τον διαχειριστή περιβάλλον. Επιπρόσθετα, έχει δημιουργήσει και αντίστοιχη εφαρμογή VPN tunnel, η οποία είναι διαθέσιμη για κινητές συσκευές και laptop. Χρησιμοποιεί τα πρωτόκολλα IPsec/TCP με αλγόριθμους κρυπτογράφησης 3DES και SHA1 για την πιο ασφαλή και κρυπτογραφημένη μετάδοση δεδομένων.

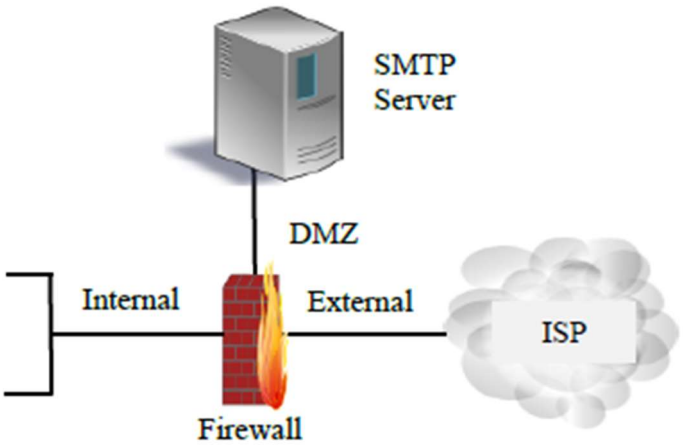
Συμπερασματικά, όπως έχει αποδειχθεί, κανέναν εργαλείο δεν μπορεί να προστατέψει στο ακέραιο την πληροφοριακή υποδομή μιας εταιρίας. Θα πρέπει να υπάρξει συνδυασμός εργαλείων τα οποία θα προστατεύουν και την πλευρά του δικτύου και την πλευρά των χρηστών-τερματικών. Με την αναφορά των παραπάνω εργαλείων και του θέματος της διατριβής, θα μπορούσαμε ως πρόταση προστασίας από κακόβουλα λογισμικά καθώς και κακόβουλες ενέργειες απομακρυσμένα, να ορίσουμε έναν συνδυασμό της Check Point για την προστασία στην πλευρά του δικτύου και το εργαλείο EDR με σκοπό την αναγνώριση εγκατεστημένων λογισμικών απομακρυσμένης πρόσβασης και αποτροπής αυτών με σχετική ενημέρωση των διαχειριστών και αντίστοιχα μπλοκαρίσματος της εγκατάστασης ή Isolation του μηχανήματος κατά την αναγνώριση τέτοιων ενεργειών.

3.4 Αποστρατιωτικοποιημένη Ζώνη (DMZ)

Η αποστρατιωτικοποιημένη ζώνη (demilitarized zone, DMZ) είναι ένα μέσο ενίσχυσης της ασφάλειας δικτύου που διαχωρίζει το εσωτερικό δίκτυο του οργανισμού από το δίκτυο πρόσβασής του (Fung, 2004). Είναι ένα στοιχείο απομακρυσμένης πρόσβασης που εάν ρυθμιστεί σωστά, μπορεί να εντοπίσει και να αποτρέψει κακόβουλες δραστηριότητες που διαπράττονται στο εσωτερικό δίκτυο.

Οι διακομιστές μεσολάβησης σε ένα DMZ περιορίζουν περαιτέρω την πρόσβαση σε πόρους του οργανισμού από απομακρυσμένους χρήστες και συσκευές. Το (Σχήμα 8) παρακάτω, δείχνει έναν διακομιστή μεσολάβησης Simple Mail Transfer Protocol (SMTP) σε ένα DMZ. Η διάταξη είναι μόνο μια από τους πολλούς τρόπους ρύθμισης του DMZ. Το firewall σε ένα DMZ παρέχει βασικές λειτουργίες ασφαλείας, όπως έλεγχος υπηρεσιών και έλεγχος ταυτότητας.

Σε ένα DMZ, η κυκλοφορία τερματίζεται σε μια απομονωμένη περιοχή του δικτύου, αποτρέποντας έτσι το κακόβουλο λογισμικό και άλλη κακόβουλη κίνηση να φτάσει στο εσωτερικό δίκτυο. Ωστόσο οι πόροι σε ένα DMZ, για παράδειγμα, οι διακομιστές μεσολάβησης, θα εκτεθούν σε παραβιασμένη κίνηση, καθώς το τείχος προστασίας δεν είναι σε θέση να ελέγξει την κρυπτογραφημένη κίνηση.



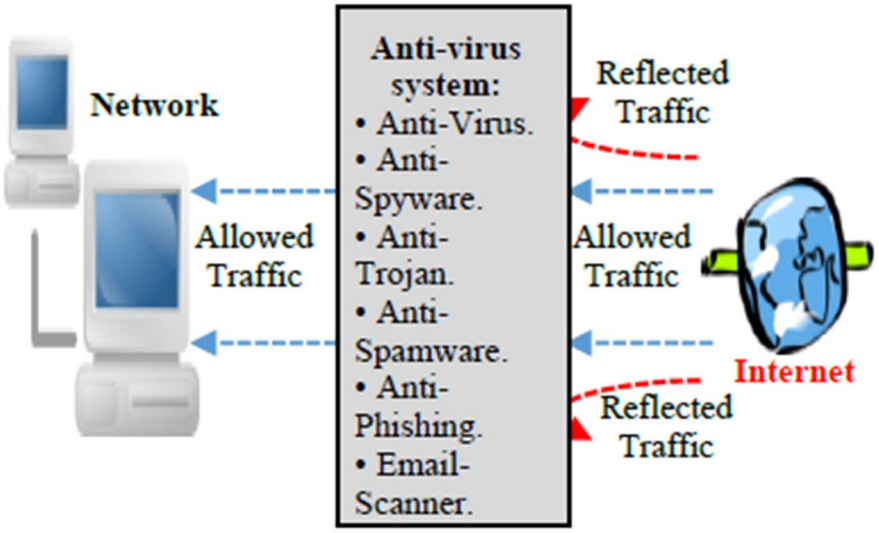
Σχήμα 8. Ένα παράδειγμα DMZ.

3.5 Sheep-dip Δικτύου

Το Network sheep dip στις πληροφορίες και την ασφάλεια δικτύου, είναι η διαδικασία ελέγχου των μέσων και της κυκλοφορίας για κακόβουλο λογισμικό πριν επιτραπούν στο εσωτερικό δίκτυο (Dong, 2007). Τα δεδομένα και τα μηνύματα που εισέρχονται στο δίκτυο από μια απομακρυσμένη συσκευή πρέπει να αναλυθούν για κακόβουλο λογισμικό και ένα sheep dip δικτύου έχει τις δυνατότητες εκτέλεσης ελέγχων για τη θύρα, το δίκτυο, το χρήστη, την άδεια ομάδας, τη διαδικασία, τη συσκευή, το αρχείο, το μητρώο και τον πυρήνα.

Ένα sheep dip θα έχει ελέγχους για λογισμικό αρχείων, δικτύου και προστασίας από ιούς. Οι έλεγχοι sheep dip δικτύου θα ανιχνεύουν και θα αναλύουν κακόβουλα δεδομένα και κώδικα για ιούς, σκουλήκια και Trojans. Το (Σχήμα 9) παρακάτω δείχνει μια υλοποίηση ενός sheep dip δικτύου, το οποίο περιλαμβάνει antivirus, anti-spyware, anti-trojan, anti-spam ware, anti-phishing και έναν σαρωτή ηλεκτρονικού ταχυδρομείου. Ένα sheep-dip δικτύου σαρώνει την αποκρυπτογραφημένη κίνηση από την πρόσβαση ή το δημόσιο δίκτυο προτού επιτραπεί η κυκλοφορία στο εσωτερικό δίκτυο, κάτι που είναι ζωτικής σημασίας για την αποτροπή κακόβουλης κυκλοφορίας.

Ωστόσο, το sheep-dip είναι μια παραδοσιακή προσέγγιση βασισμένη σε υπογραφές και ευρετικές και ως εκ τούτου είναι επιρρεπές στις προκλήσεις των επιθέσεων zero-day, ψευδώς θετικών σε συνδυασμό με μακρά ανάλυση και χρόνο σάρωσης.



Σχήμα 9. Ένα sheep-dip δικτύου.

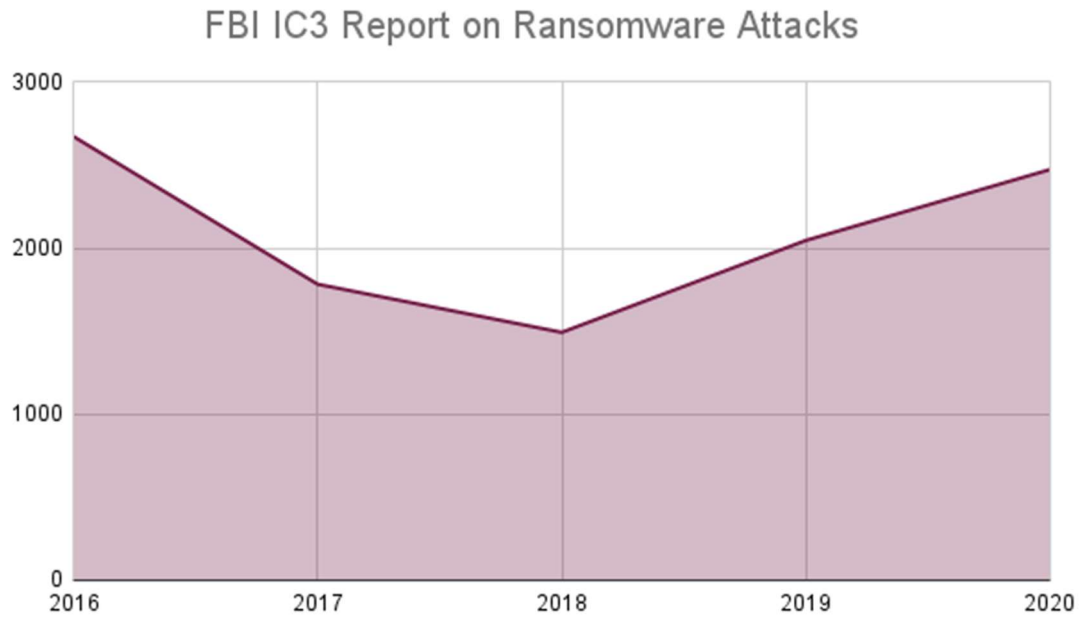
Αυτές οι συμβατικές προσεγγίσεις για την ασφάλεια απομακρυσμένης πρόσβασης έχουν παραβιαστεί επανειλημμένα από επιθέσεις εισβολέων και σε ορισμένες περιπτώσεις, χρησιμοποιούν τις πολύ βασικές τεχνολογίες και τα πλεονεκτήματά τους για να παρακάμψουν για παράδειγμα την αποτυχία των περιμετρικών ελέγχων να ανιχνεύσουν κακόβουλο λογισμικό σε κρυπτογραφημένη κυκλοφορία.

Οι δικτυακές απειλές παραμονεύουν, με τους επιτιθέμενους να υιοθετούν γρήγορα νέες προσεγγίσεις και τεχνικές αποφυγής ανίχνευσης, επομένως οι προληπτικές και δυναμικές προσεγγίσεις είναι απαραίτητες για την αντιμετώπιση της διαρκώς μεταβαλλόμενης δικτυακής απειλής απομακρυσμένης πρόσβασης.

4 Στατιστικά Στοιχεία Επιθέσεων

Η αύξηση της απομακρυσμένης εργασίας σήμαινε ότι οι περισσότεροι οργανισμοί παρουσίαζαν μεγαλύτερη επιφάνεια επίθεσης. Αυτή η ευπάθεια οδήγησε σε σημαντική αύξηση των κυβερνοεπιθέσεων συνολικά, αλλά σε ακόμη μεγαλύτερο άλμα στις επιθέσεις ransomware, οι οποίες αυξήθηκαν κατά 150% το 2020. Το FBI Internet Crime Complaint Center (IC3) παρακολουθεί τις επιθέσεις ransomware που αναφέρθηκαν στο IC3 τουλάχιστον από το 2016.

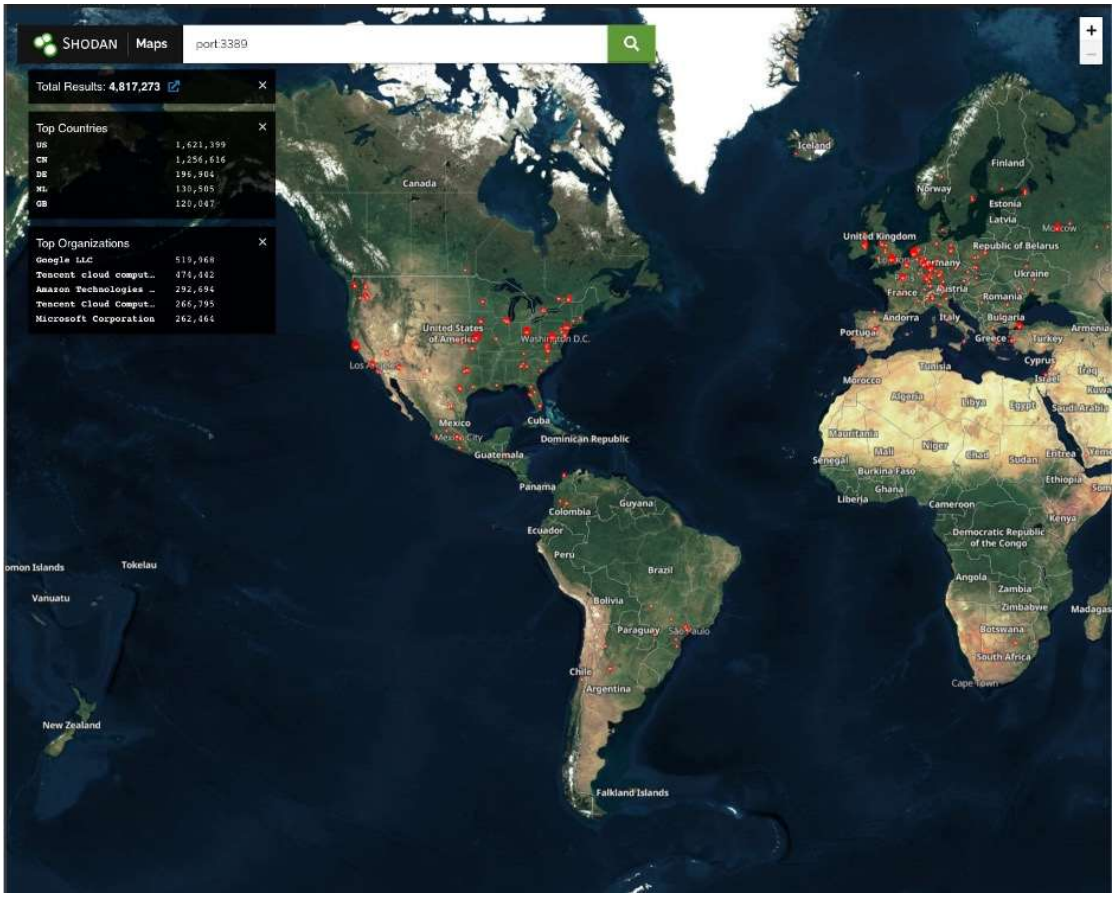
Το γράφημα στο (Σχήμα 10), δείχνει την αύξηση επιθέσεων ransomware τα τελευταία χρόνια μετά τη μετάβαση από μια κυρίως αυτοματοποιημένη μορφή κακόβουλου λογισμικού το 2016 και τις αρχές του 2017 για τις χειροκίνητες επιθέσεις στον κυβερνοχώρο από το 2018 και μετά, ενώ είναι αξιοσημείωτη η σταθερή αύξηση από το 2018.



Σχήμα 10. Αναφορές επιθέσεων ransomware του FBI Internet Crime Complaint Center (IC3) από το 2016-2020.

Αξίζει να σημειωθεί ότι δεν ήταν μόνο ο COVID-19 που προκάλεσε την αύξηση των επιθέσεων ransomware το 2020. Η ανάπτυξη του RaaS και οι συνεχείς τίτλοι σχετικά με τα λύτρα πολλών εκατομμυρίων δολαρίων που καταβάλλονται προσέλκυαν ήδη περισσότερους κυβερνοεγκληματίες στο ransomware πριν από την εμφάνιση της πανδημίας. Ωστόσο, η αυξημένη επιφάνεια επίθεσης που αντικατόπτριζε τους τύπους συστημάτων στα οποία ήθελαν να επιτεθούν τα ransomware έκανε την ανάπτυξη πολύ πιο εύκολη.

Ανάλογα με το ποιες ομάδες ransomware είναι ενεργές και ποιος κάνει την αναφορά, οι επιθέσεις είτε τύπου phishing είτε μέσω πρωτοκόλλου απομακρυσμένης επιφάνειας εργασίας (Remote Desktop Protocol, RDP) είναι οι πιο συχνά χρησιμοποιούμενες επιθέσεις αρχικής πρόσβασης για ransomware. Δυστυχώς, η ευκολία εύρεσης εκτεθειμένων συστημάτων RDP σε συνδυασμό με την άφθονη τεκμηρίωση σχετικά με τον τρόπο απόκτησης πρόσβασης σε εκτεθειμένα συστήματα RDP που δημοσιεύονται σε υπόγειες αγορές, σημαίνει ότι εξακολουθούν να αποτελούν έναν επικερδή φορέα αρχικής πρόσβασης για ομάδες ransomware.



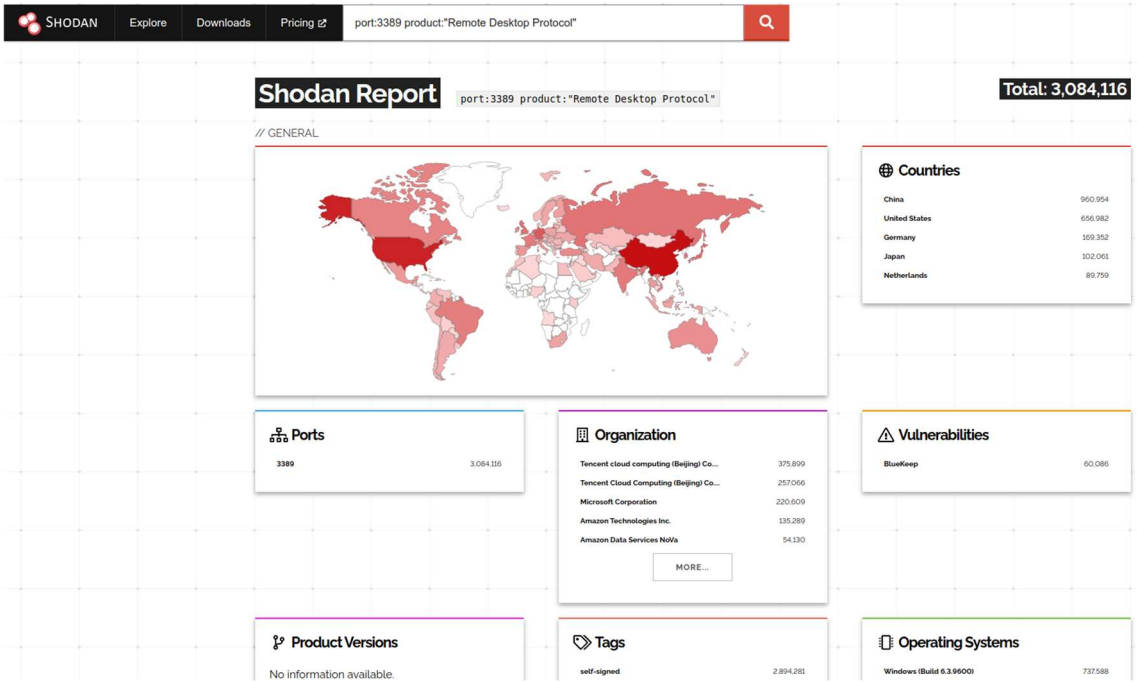
Σχήμα 11. Διακομιστές με υπηρεσία RDP (θύρα 3389) εκτεθειμένη στο Διαδίκτυο.

Το (Σχήμα 11) δείχνει έναν χάρτη διακομιστών που είναι εκτεθειμένοι στο Διαδίκτυο με ανοιχτή τη θύρα 3389, δηλαδή την προεπιλεγμένη θύρα για το RDP. Οι πληροφορίες προέρχονται από μια έρευνα που πραγματοποιήθηκε από την εταιρεία σάρωσης Shodan[3]. Δείχνει 4,8 εκατομμύρια συστήματα δυνητικά ευάλωτα σε επιθέσεις δοκιμής διαπιστευτηρίων ή επαναχρησιμοποίησης διαπιστευτηρίων. Αυτή η έρευνα πραγματοποιήθηκε στα τέλη Αυγούστου του 2021, και είναι αντιπροσωπευτική των ευρημάτων των τελευταίων ετών.

Η συγκεκριμένη προβολή δεν λαμβάνει υπόψη τα συστήματα οργανισμών που εκτελούν RDP σε θύρα διαφορετική από την 3389. Είναι όλα τα συστήματα δυνητικά ευάλωτα σε επίθεση επαναχρησιμοποίησης διαπιστευτηρίων ή γεμίσματος διαπιστευτηρίων; Όχι, δεν τρέχουν όλοι καν το RDP, αλλά εκατομμύρια από αυτά είναι και τα περισσότερα από αυτά κινδυνεύουν.

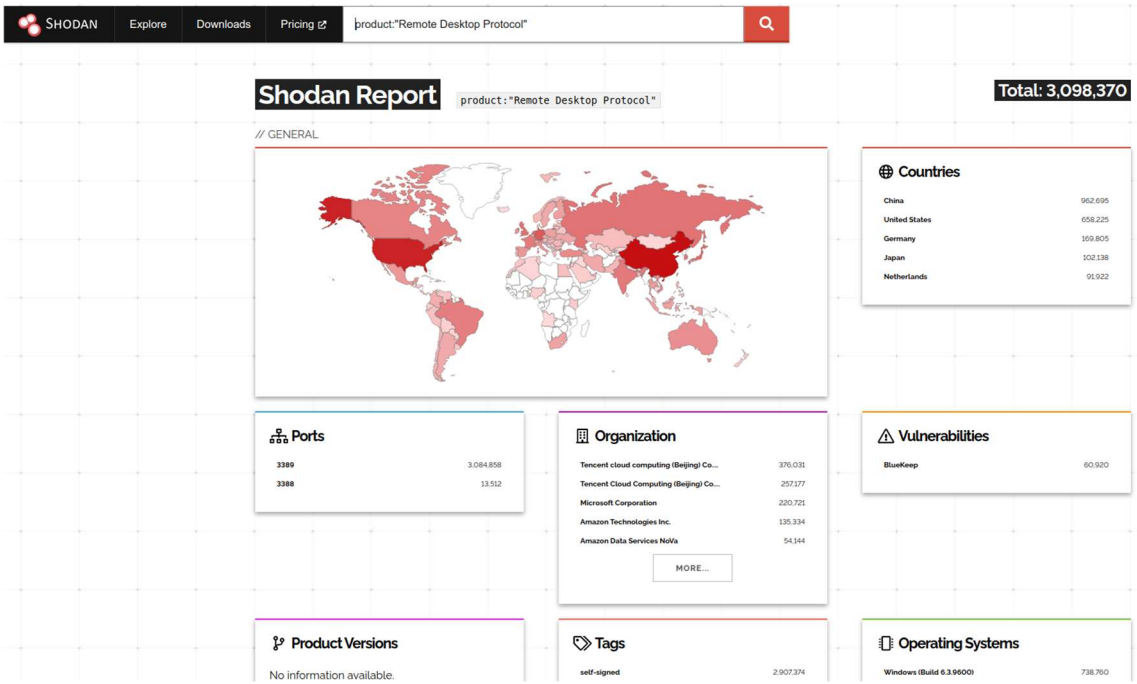
Ενδεικτικά, το Shodan αυτή τη στιγμή αναφέρει πλέον των 3 εκατομμύρια υπολογιστών προσβάσιμων από την πόρτα 3389 και να χρησιμοποιούν το RDP ενώ λίγες χιλιάδες ακόμα φαίνεται να χρησιμοποιούν την πόρτα 3388.

[3] https://www.shodan.io/



Σχήμα 12. Στατιστικά χρήσης πόρτας 3389

Όπως εμφανίζεται και στο παραπάνω (Σχήμα 12), στατιστικά στην 1η θέση ανέρχεται η Κίνα με σχεδόν 1 εκατομμύριο συστήματα τα οποία είναι ευάλωτα σε επιθέσεις δοκιμής διαπιστευτηρίων ή επαναχρησιμοποίησης διαπιστευτηρίων. Ακολουθούν οι Ηνωμένες Πολιτείες της Αμερική με περισσότερο από μισό εκατομμύριο και την τρίτη θέση κατέχει από τις χώρες της Ευρωπαϊκής Ηπείρου η Γερμανία με περίπου 170 χιλιάδες συστήματα εκτεθειμένα.



Σχήμα 13. Στατιστικά χρήσης πρωτόκολλου RDP πόρτες 3389 και 3388

Στο (Σχήμα 13) παρουσιάζονται στατιστικά στοιχεία από το πρωτόκολλο απομακρυσμένης σύνδεσης για συστήματα τα οποία είναι εκτεθειμένα και χρησιμοποιούν πέραν της πόρτα 3389 και την πόρτα 3388.

5 Βιβλιογραφική ανασκόπηση μελετών από δοκιμές διείσδυσης σε RDP

5.1 Πλαίσιο Αξιολόγησης Ασφάλειας Πληροφοριακών Συστημάτων

Το “Πλαίσιο Αξιολόγησης Ασφάλειας Πληροφοριακών Συστημάτων (Information System Security Assessment Framework, ISSAF)” είναι ένα πλαίσιο δοκιμών διείσδυσης ανοιχτού κώδικα, αξιολογημένο από ομότιμους (peer-reviewed) που δημιουργήθηκε από την Ομάδα Ασφάλειας Ανοικτών Πληροφοριακών Συστημάτων (Open Information Systems Security Group, OISSG). Το ISSAF περιγράφεται ως πλαίσιο, ενσωματώνει πολλαπλές μεθοδολογίες και φαίνεται να είναι ένα λεπτομερές και περιεκτικό πλαίσιο που καλύπτει μια ποικιλία τομέων όπου ο καθένας επιτρέπεται να έχει τη δική του μεθοδολογία. Οι τομείς περιλαμβάνουν αλλά δεν περιορίζονται σε: δοκιμή ασφαλείας κωδικού πρόσβασης, ασφάλεια μεταγωγέα και δρομολογητή, ασφάλεια τείχους προστασίας, αξιολογήσεις συστημάτων ανίχνευσης εισβολής, ασφάλεια VPN, ασφάλεια εφαρμογών ιστού και ασφάλεια των Windows.

Αν και δεν αναφέρονται όλοι οι τομείς εδώ, η ISSAF προσπαθεί να καλύψει όλους τους πιθανούς τομείς μιας δοκιμής διείσδυσης από τη σύλληψη έως την ολοκλήρωση. Η μεθοδολογία δοκιμών διείσδυσης του πλαισίου χωρίζεται σε τρεις κύριες φάσεις: σχεδιασμός και προετοιμασία, αξιολόγηση, αναφορά και εκκαθάριση. Ένα πλεονέκτημα του ISSAF είναι ότι εμφανίζεται η διακριτή σχέση μεταξύ των εργασιών και των σχετικών εργαλείων για κάθε εργασία, επιπλέον παρέχονται στιγμιότυπα οθόνης των αναμενόμενων εξόδων, μαζί με επεξηγήσεις για το *πώς* και το *γιατί* εκτελείται κάθε εργασία.

Το ISSAF είναι μεγάλο σε σύγκριση με άλλα πλαίσια, αλλά υποθέτει ότι είναι ευκολότερο για τους οργανισμούς να διαγράψουν υλικό παρά να το αναπτύξουν από την αρχή (OISSG, 2005).

5.2 Εγχειρίδιο Μεθοδολογίας Δοκιμών Ασφαλείας Ανοικτού Κώδικα

Το “Εγχειρίδιο Μεθοδολογίας Δοκιμών Ασφαλείας Ανοικτού Κώδικα (Open Source Security Testing Methodology Manual - OSSTMM)” είναι μια μεθοδολογία δοκιμών ασφαλείας ανοιχτού κώδικα που εισήχθη το 2000 από το Ινστιτούτο Ασφάλειας και Ανοιχτών Μεθοδολογιών (ISECOM). Το OSSTMM αναπτύχθηκε με αξιολόγηση από ομότιμους και επωφελείται από την άδεια χρήσης ανοιχτού κώδικα, ωστόσο, η πρόσβαση από την έκδοση 4 απαιτεί χρηματική συνδρομή.

Το OSSTMM στην έκδοση 3, ορίζεται ως μια μεθοδολογία που ενσωματώνει ενότητες και κανάλια (ISECOM, 2000). Το OSSTMM ταξινομεί μια περιοχή ενδιαφέροντος τομέα ως κανάλι. Το OSSTMM αποτελείται από πέντε κανάλια: ανθρώπινο, φυσικό, ασύρματο, τηλεπικοινωνίες και ασφάλεια δικτύου δεδομένων. Σε αυτά τα κανάλια, η μεθοδολογία περιλαμβάνει τρέχοντα περιβάλλοντα και συγκεκριμένα, υπολογιστικό νέφος και εικονικοποίηση.

Σε αντίθεση με την ISSAF, η OSSTMM δεν συνιστά ποια εργαλεία πρέπει να χρησιμοποιηθούν, αλλά προτείνει βέλτιστες πρακτικές που πρέπει να ακολουθηθούν. Το OSSTMM αναφέρεται σε κάθε επαναλαμβανόμενη φάση ως ενότητα και υποθέτει ότι ένας επαγγελματίας ασφαλείας διαθέτει επαρκή γνώση των εργαλείων και των τεχνικών που απαιτούνται για την εκτέλεση κάθε ενότητας. Το OSSTMM παρέχει επαρκείς κατευθυντήριες γραμμές συνοδευόμενες από πρότυπα αναφοράς. Περιλαμβάνει επίσης μετρήσεις εμπιστοσύνης που επιτρέπουν την εκτίμηση κινδύνου για άλλους παράγοντες που δεν μπορούν να ελεγχθούν. Αυτό σημαίνει ότι το cloud, οι συμβάσεις και οι υπηρεσίες προμηθευτών, τα προϊόντα, ακόμη και οι προσλήψεις εργαζομένων μπορούν να μετρηθούν για τον κίνδυνο και την επιφάνεια επίθεσης, κάτι που θα μπορούσε να θεωρηθεί βελτίωση σε σύγκριση με την ISSAF.

Η επιφάνεια επίθεσης μπορεί να μετρηθεί και να υποδειχθούν τα μέρη όπου ένας επιτιθέμενος μπορεί να επιτεθεί και ποιοι τύποι επιθέσεων θα ήταν πιθανώς επιτυχημένοι. Συνοπτικά, το OSSTMM είναι μια μεθοδολογία ελέγχου που έχει σχεδιαστεί για να είναι συνεπής

και επαναλαμβανόμενη σε επιχειρησιακό επίπεδο παρέχοντας ακριβή μέτρα ασφάλειας μέσω ελέγχου ασφαλείας.

Τόσο το OSTMM όσο και το ISSAF παρέχουν καθοδήγηση, αλλά το τελευταίο προτείνει εργαλεία ή μεθόδους για τη συμπλήρωση ενοτήτων. Το OSTMM είναι ένας πολύτιμος ελεγκτικός πόρος που μπορεί να χρησιμοποιηθεί για την ικανοποίηση κανονιστικών απαιτήσεων για εταιρικά περιουσιακά στοιχεία, υπό τον όρο ότι οι ελεγκτές ασφαλείας έχουν επαρκείς δεξιότητες για να ολοκληρώσουν κάθε ενότητα.

Το NIST 800-115 είναι ένας τεχνικός οδηγός για δοκιμές και αξιολόγηση ασφάλειας πληροφοριών και διατηρείται από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (National Institute of Standards and Technology, NIST) για ομοσπονδιακούς κρατικούς φορείς στις ΗΠΑ. Είναι δωρεάν για χρήση στον ιδιωτικό τομέα και δεν υπόκειται σε πνευματικά δικαιώματα αν και είναι επιθυμητή η απόδοση τους (NIST, 2008). Το NIST-800-115 παρέχει οδηγίες για τον σχεδιασμό και τη διεξαγωγή δοκιμών ασφάλειας πληροφοριών. Συγκριτικά, δεν είναι τόσο λεπτομερές όσο το OSSTMM και το ISSAF. Το NIST προσφέρει δομημένη τεκμηρίωση σχετικά με τον τρόπο εφαρμογής μιας μεθοδολογίας με επαναλαμβανόμενες διαδικασίες για 23 αξιολογήσεις ασφαλείας που απευθύνονται κυρίως σε οργανισμούς. Το NIST 800-115 εξηγεί λεπτομερώς τις τεχνικές σχεδιασμού και εκτέλεσης με έμφαση στον εντοπισμό τρωτών σημείων.

Παρόμοια με το OSSTMM, το NIST 800-115 δεν συνιστά συγκεκριμένα εργαλεία, αλλά παρουσιάζει ένα παράρτημα προτεινόμενων εργαλείων που χρησιμοποιούνται στον τομέα της ασφάλειας στον κυβερνοχώρο για συγκεκριμένες εργασίες. Το NIST 800-115 υποθέτει ότι ο επαγγελματίας ασφαλείας διαθέτει τις γνώσεις και τις δεξιότητες που απαιτούνται για τη διεξαγωγή δοκιμών διείσδυσης.

Ο Οδηγός NIST 800-115 σχεδιάστηκε με στόχο να παρέχει στους οργανισμούς ένα μέσο ανάπτυξης μιας μεθοδολογίας που μπορεί να προσαρμοστεί για αξιολογήσεις ασφαλείας, ενισχύοντας έτσι επαναλαμβανόμενες διαδικασίες, τεχνικές σχεδιασμού, εκτέλεσης για οργανισμούς.

Συνοπτικά, το NIST 800-115 είναι ένας χρήσιμος οδηγός που μπορεί να εφαρμοστεί ως στρατηγική ασφάλειας για οργανισμούς. Η τεκμηρίωση βοηθά τους οργανισμούς στην ανάπτυξη μιας μεθοδολογίας δοκιμών ασφάλειας πληροφοριών, πώς να σχεδιάζουν και να εκτελούν με ακρίβεια μια αξιολόγηση και πώς να διεξάγουν αναφορές ανάλυσης.

5.3 Ανοιχτό Εγχείρημα Ασφάλειας Εφαρμογών Ιστού

Το “Ανοιχτό Εγχείρημα Ασφάλειας Εφαρμογών Ιστού (Open Web Application Security Project, OWASP)” είναι ένας μη κερδοσκοπικός οργανισμός που επικεντρώνεται στη βελτίωση της ασφάλειας του λογισμικού. Το OWASP παρέχει πολυάριθμα εργαλεία, οδηγούς και μεθοδολογίες δοκιμών για την ασφάλεια στον κυβερνοχώρο υπό την άδεια ανοιχτού κώδικα. Ένας από τους πολλούς οδηγούς ασφαλείας που διατίθενται είναι ο οδηγός δοκιμής OWASP (OTG), ο οποίος μπορεί να ληφθεί από τον ιστότοπο του OWASP.

Το OTG ενσωματώνει ένα πλαίσιο δοκιμών για την ανάπτυξη λογισμικού, μεθοδολογία δοκιμών ασφάλειας εφαρμογών Ιστού για εφαρμογές web δοκιμής διείσδυσης και έναν οδηγό αναφοράς. Το OTG περιγράφει λεπτομερώς τις εργασίες και τις τεχνικές κατάλληλες για διάφορες φάσεις του κύκλου ζωής ανάπτυξης λογισμικού που επικεντρώνονται στην ανάπτυξη λογισμικού με γνώμονα την ασφάλεια σε αντίθεση με τον εντοπισμό τρωτών σημείων μετά την ανάπτυξη. Ο Οδηγός δοκιμής OWASP χωρίζεται σε τρεις κύριες ενότητες, συγκεκριμένα, το πλαίσιο δοκιμών OWASP για την ανάπτυξη εφαρμογών Ιστού, τη μεθοδολογία δοκιμής εφαρμογών Ιστού και την αναφορά.

Η μεθοδολογία Εφαρμογών Ιστού μπορεί να χρησιμοποιηθεί ανεξάρτητα ή σε συνδυασμό με το πλαίσιο δοκιμών. Η μεθοδολογία OWASP για εφαρμογές Ιστού συγκεντρώνει εργαλεία και τεχνικές που χρησιμοποιούνται για κάθε φάση μιας δοκιμής διείσδυσης, ωστόσο, δεν παρέχει λεπτομέρειες για κάθε εργαλείο, αλλά προϋποθέτει γνώση εργαλείων και τεχνικών.

Τα συνιστώμενα εργαλεία για κάθε φάση περιγράφονται αναλυτικά. Επιπλέον, προσφέρονται σύνδεσμοι ιστού με σχετικές πληροφορίες εργαλείων και τεχνικών για να βοηθήσουν με τυχόν κενά γνώσης που μπορεί να υπάρχουν. Το κοινό-στόχος είναι επαγγελματίες ασφάλειας στον κυβερνοχώρο μεσαίου έως προχωρημένου επιπέδου με έντονη εστίαση στις τεχνολογίες διαδικτυακών εφαρμογών.

6 Βιβλιογραφική ανασκόπηση Λογισμικού Ransomware

6.1 Κακόβουλο Λογισμικό Ransomware

Το ransomware είναι κακόβουλο λογισμικό που μπορεί να κλειδώσει μια συσκευή ή να κρυπτογραφήσει τα περιεχόμενά της, προκειμένου να ζητήσει χρήματα ως λύτρα από τον ιδιοκτήτη της. Στην εποχή μας τα ransomware έχουν εξελιχθεί σε σημαντική απειλή για τους χρήστες υπολογιστών και έξυπνων συσκευών. Το ransomware μπορεί να αναφέρεται ως scareware, δηλαδή ως κακόβουλο λογισμικό που έχει σχεδιαστεί βασικά για να τρομάζει τους χρήστες και να τους αναγκάζει είτε να αγοράσουν γρήγορα το λογισμικό που χρησιμοποιείται για την προστασία των προσωπικών δεδομένων του χρήστη είτε για να αποτρέψουν μη αναστρέψιμες ζημιές.

Ένα ransomware κρυπτογραφεί τα δεδομένα των μολυσμένων συστημάτων και ζητά από τον χρήστη να πληρώσει λύτρα συνήθως κάποιο κρυπτονόμισμα όπως το bitcoin (Nakamoto, 2008) για να ανακτήσει την πλήρη πρόσβαση στο σύστημα που έχει προσβληθεί. Πολλά θύματα πληρώνουν λύτρα για να επαναφέρουν σημαντικά δεδομένα για τα οποία δεν έχουν αντίγραφο ασφαλείας. Ένα χαρακτηριστικό παράδειγμα είναι η έκδοση 3 του CryptoWall (Sgandurra et al., 2016), η οποία προκάλεσε ζημιά περίπου 325 εκατομμυρίων δολαρίων μόνο στις ΗΠΑ κατά την περίοδο από τον Νοέμβριο του 2015 έως τον Ιούνιο του 2016. Η έκδοση 4 του CryptoWall έφτασε τα 7,1 εκατομμύρια δολάρια παγκοσμίως (Cyber Threat Alliance, 2015).

Αυτοί οι τύποι ransomware συνήθως περνούν από τρεις φάσεις: 1) εύρεση στόχου για θυματοποίηση. 2) αποτροπή πρόσβασης σε τοπικές πληροφορίες. και στη συνέχεια 3) εμφανίζοντας κάποιο τρομακτικό μήνυμα και προσπαθώντας να εκβιάσουν την καταβολή λύτρων. Σύμφωνα με τους (Sgandurra et al. (2016), υπάρχουν δύο βασικοί τύποι ransomware που είναι διαθέσιμοι σήμερα, (α) Locker ransomware και, (β) Crypto ransomware. Το πρώτο έχει σχεδιαστεί για να κλειδώνει τον υπολογιστή του θύματος και τελικά να εμποδίζει τον χρήστη να τον χρησιμοποιήσει. Το δεύτερο που είναι πιο συνηθισμένο, κρυπτογραφεί προσωπικά αρχεία για να τα κάνει απρόσιτα στο θύμα του.

Τα κακόβουλα λογισμικά για Windows είναι σύνηθες ότι εκβιάζουν απαιτώντας λύτρα, για παράδειγμα, το λογισμικό για υπολογιστές Trojan Kenzero (Aurangzeb et al., 2017) όχι μόνο κλέβει το ιστορικό του προγράμματος περιήγησης του χρήστη αλλά επίσης το δημοσιεύει δημόσια στο Διαδίκτυο μαζί με το όνομα του ατόμου, απαιτώντας συνήθως 1500 γιεν για να καταργηθεί το ιστορικό του προγράμματος περιήγησης του θύματος (Felt et al., 2011). Σε ότι αφορά την κατάσταση σε κινητές συσκευές, χρησιμοποιούνται λογισμικά εκφοβισμού και απαίτησης λύτρων, αλλά δεν έχει υπάρξει ακόμη κάποιο κακόβουλο λογισμικό για κινητά που να απειλεί σοβαρά ή να ντροπιάζει δημόσια τον χρήστη για απόσπαση λύτρων.

Υπήρχε ένα κακόβουλο λογισμικό για κινητά, ένα ολλανδικής κατασκευής σκουλήκι (worm) το οποίο κλείδωνε τις οθόνες iPhone και αργότερα απαιτούσε λύτρα πέντε ευρώ (5,00€) για να ξεκλειδώσει την οθόνη του μολυσμένου τηλεφώνου (Clucley, 2009). Τα smartphone συνήθως δεν προσφέρουν κανένα τεχνικό πλεονέκτημα σε σύγκριση με τους επιτραπέζιους υπολογιστές όπου οι εγκληματίες συνεχίζουν να αναζητούν λύτρα από τους χρήστες.

Μπορεί να υπάρχουν διαφορές συμπεριφοράς μεταξύ των χρηστών που καθιστούν μια πλατφόρμα πιο πολύτιμο στόχο λύτρων από την άλλη. Τα θύματα συνήθως επηρεάζονται από απειλές που μπορούν να ταξινομηθούν σε τρεις κατηγορίες:

- **Κακόβουλο λογισμικό:** Το κακόβουλο λογισμικό είναι ένα κακόβουλο κομμάτι κώδικα που αναλαμβάνει τον έλεγχο μιας συσκευής ή ενός συστήματος με σκοπό είτε να κλέψει δεδομένα είτε να τα καταστρέψει και μερικές φορές απλώς να ενοχλήσει τον χρήστη. Αυτός ο τύπος απειλής περιλαμβάνει συνήθως Trojans, worms, botnets και ιούς (Felt et al., 2011).
- **Personal Spyware:** Προσπαθεί να συλλέξει προσωπικές πληροφορίες, όπως γεωγραφική τοποθεσία ή ιστορικό μηνυμάτων κειμένου για μια συγκεκριμένη χρονική περίοδο. Με το προσωπικό λογισμικό κατασκοπείας, ο εισβολέας εγκαθιστά το λογισμικό χωρίς τη γνώση του χρήστη και έχει φυσική πρόσβαση στη συσκευή.

- Το κακόβουλο λογισμικό που μπορεί να χρησιμοποιηθεί ως εργαλείο εκβιασμού αναφέρεται ως ransomware. Το ransomware είναι κακόβουλο λογισμικό που μολύνει κρυφά τη συσκευή του θύματος και ξαφνικά απαιτεί πληρωμή λύτρων για να επαναφέρει τα κρυπτογραφημένα δεδομένα.

6.2 Μοτίβα Επιθέσεων

Υπάρχει ένα γενικό μοτίβο επίθεσης το οποίο είναι παρόμοιο για όλα τα ransomware, και διαφοροποιείται αν ο στόχος είναι υπολογιστής με Windows ή αν είναι κινητή συσκευή με Android. Στην περίπτωση των μολυσμένων συσκευών Android ένα ransomware προσπαθεί πρώτα να αποκτήσει ένα διαχειριστικό προνόμιο απλά ζητώντας το ή χρησιμοποιώντας κάποιες τακτικές κοινωνικής μηχανικής. Ένας άλλος τρόπος για να αποκτήσει το προνόμιο διαχειριστή είναι να ζητήσει από τον χρήστη να εγκαταστήσει ενημερώσεις κώδικα λογισμικού ή να κάνει κλικ σε κάποια ψεύτικα αναδυόμενα παράθυρα ενημέρωσης ή ενημερώσεις προστασίας από ιούς.

Γενικά ένα άλλο βήμα που χρησιμοποιεί το ransomware είναι να ζητήσει δικαιώματα σε επίπεδο εφαρμογής, τα οποία απαιτούνται για την εκτέλεση των απαραίτητων εργασιών. Μια εφαρμογή που ζητά περιττές άδειες σε σχέση με τη φύση της εργασίας της εκτελεί σχεδόν πάντα κακόβουλη δραστηριότητα. Σχεδόν όλοι οι τύποι κακόβουλων προγραμμάτων έχουν κάποιου είδους κανάλι κερκόπορτας ανοιχτό για τον εισβολέα να αποκτήσει πρόσβαση στο μολυσμένο σύστημα.

Οι backdoored πελάτες αναφέρονται ως ζόμπι, όπου ένα μηχάνημα ή ένα δίκτυο zombie είναι συστήματα που μπορούν να ελέγξουν οι χάκερ και να τα κάνουν για παράδειγμα, να ενωθούν με άλλα ζόμπι για να ξεκινήσουν επιθέσεις κατανεμημένης άρνησης υπηρεσίας (Distributed denial of service, DDoS) (Luo et al., 2017). Ένα μηχάνημα ή ένα δίκτυο zombie που συχνά ονομάζεται και botnet. Οι επιτιθέμενοι χρησιμοποιώντας αυτά τα ζόμπι, τα εκμεταλλεύονται για να κερδίσουν χρήματα χρησιμοποιώντας διάφορα μέσα και πάντοτε αποκρύβοντας τη δική τους ταυτότητα. Επιπλέον, ένας εισβολέας ransomware μπορεί σχετικά εύκολα να κλέψει κωδικούς πρόσβασης και τραπεζικά στοιχεία.

Εάν ένας εισβολέας ransomware αποκτήσει με επιτυχία πρόσβαση και δικαιώματα διαχειριστή στη συσκευή του θύματος, θα αρχίσει να συλλέγει πληροφορίες και να στέλνει τις πληροφορίες που συλλέγει στον διακομιστή εντολών και ελέγχου (command and control, C&C). Τα C&C χρησιμοποιούνται για τη συλλογή κλεμμένων πληροφοριών από διαφορετικά ζόμπι που διαδίδονται σε όλο το δίκτυο. Τα ζόμπι συνήθως συνδέουν C&C χρησιμοποιώντας κρυπτογραφημένο μηχανισμό Transport Layer Security για την ασφαλή αποστολή των κλεμμένων πληροφοριών (Zavarsky & Lindskog, 2016).

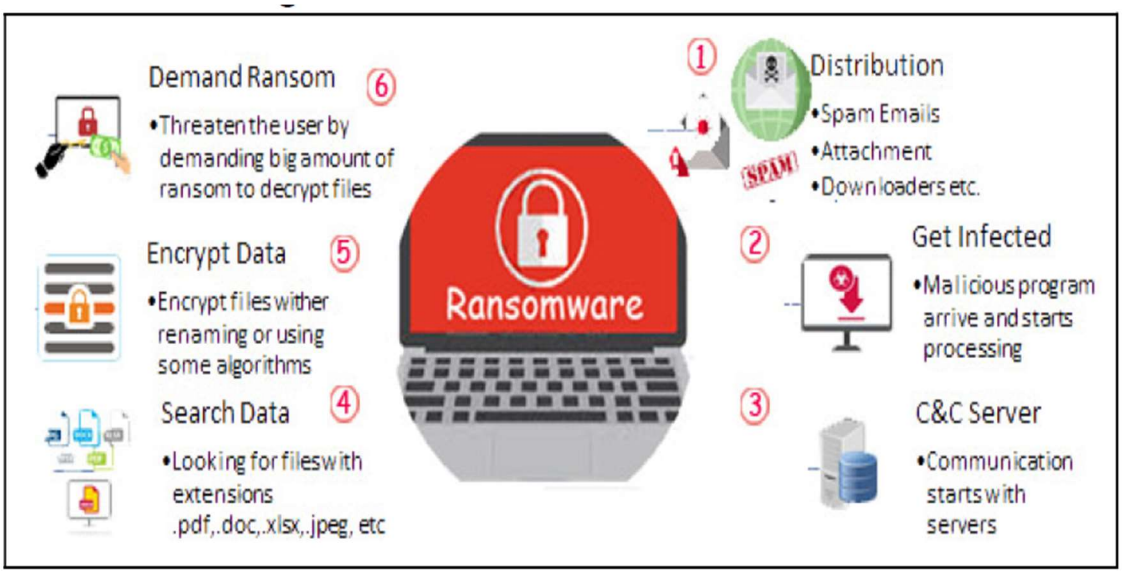
Για παράδειγμα, το ransomware crypto αποκτά ένα ιδιωτικό κλειδί από C&C για να κρυπτογραφήσει τα αρχεία της συσκευής Android του θύματος. Μετά από αυτήν την κρυπτογράφηση εμφανίζει απειλητικά μηνύματα που ζητούν από το θύμα να πληρώσει τα λύτρα. Το ransomware Locker (Zavarsky & Lindskog, 2016) λειτουργεί διαφορετικά σε σύγκριση με το crypto, τελικά επαναφέρει το PIN της συσκευής και ζητά την πληρωμή λύτρων.

Στην πλατφόρμα των Windows, αρκετοί μηχανισμοί επίθεσης είναι κοινοί μεταξύ των επιτιθέμενων ransomware. Ένα ransomware επιτίθεται στον υπολογιστή του θύματος μέσω οποιουδήποτε κακόβουλου ιστότοπου, συνημμένου ηλεκτρονικού ταχυδρομείου ή οποιουδήποτε κακόβουλου συνδέσμου ιστού ή με διάφορους άλλους τρόπους. Μόλις το σύστημα μολυνθεί, έρχεται σε επαφή με τον διακομιστή C&C ακριβώς όπως μια συνηθισμένη εφαρμογή Android. Αρχίζει να κλέβει τις πληροφορίες του θύματος και τις μεταδίδει στον εισβολέα. Ο εισβολέας αποκτά επίσης ένα συμμετρικό κλειδί που δημιουργείται τυχαία από τον διακομιστή C&C. Μετά από αυτό, ξεκινά την κρυπτογράφηση αρχείων και φακέλων χρησιμοποιώντας ασύμμετρη κρυπτογράφηση RSA, όπου το κλειδί που χρησιμοποιείται για την κρυπτογράφηση δεν μπορεί να χρησιμοποιηθεί για την αποκρυπτογράφηση των δεδομένων. Ο αλγόριθμος RSA χρησιμοποιεί δύο διαφορετικά κλειδιά, ένα δημόσιο κλειδί για την κρυπτογράφηση δεδομένων και ένα ιδιωτικό κλειδί για την αποκρυπτογράφηση (Barbulescu et al., 2016). Παράλληλα, το κακόβουλο λογισμικό διαγράφει όλα τα σημεία επαναφοράς, τους φακέλους αντιγράφων ασφαλείας και τα σκιώδη αντίγραφα τόμου.

Λαμβάνοντας υπόψη το ransomware Locker (Zavarsky & Lindskog, 2016), εκτελούνται τα ίδια βήματα εκτός του ότι δεν εκτελεί κρυπτογράφηση σε δεδομένα. Μετά την απόκτηση

δικαιωμάτων διαχειριστή, κλειδώνει την πρόσβαση του χρήστη στο σύστημα και αλλάζει την ταπετσαρία της επιφάνειας εργασίας ή μερικές φορές εμφανίζει ένα παράθυρο, το οποίο ειδοποιεί για την επίθεση ransomware και δείχνει τα βήματα που πρέπει να ακολουθήσει ο χρήστης για να ανακτήσει την πρόσβαση στο σύστημα.

Το (Σχήμα 14) δείχνει τις λεπτομέρειες και τη δομή της επίθεσης ransomware που ακολουθεί 6 διαφορετικά στάδια.



Σχήμα 14. Δομή μιας επίθεσης Ransomware.

6.3 Human-Operated-Ransomware

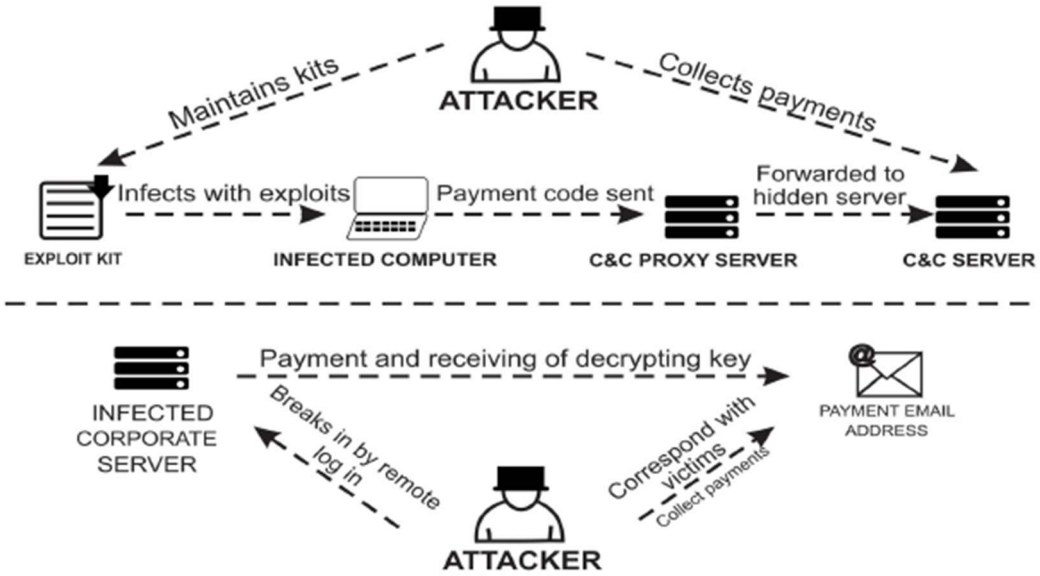
Το Ransomware είναι κακόβουλο λογισμικό που παραβιάζει δεδομένα ή συστήματα και εμποδίζει τους νόμιμους κατόχους τέτοιων δεδομένων ή συστημάτων να έχουν πρόσβαση σε αυτά. Το Ransomware μπορεί να κρυπτογραφήσει δεδομένα ή να κλειδώσει το σύστημα χρησιμοποιώντας διαδικασίες, εργαλεία και τεχνικές που καθιστούν την αποκατάσταση ή την αποκρυπτογράφηση εξαιρετικά δύσκολη ή αδύνατη ακόμα για εξειδικευμένους τεχνικούς πληροφορικής. Μπορεί επίσης να κλέψει ευαίσθητα δεδομένα από τους υπολογιστές και τα δίκτυα των θυμάτων.

Το Ransomware στοχεύει προσωπικούς υπολογιστές, επιχειρηματικά συστήματα (συμπεριλαμβανομένων των δεδομένων και των εφαρμογών τους) και συστήματα βιομηχανικού ελέγχου. Επιτίθεται επίσης σε αισθητήρες που χρησιμοποιούν τεχνολογία Διαδικτύου των Πραγμάτων (Internet of Things, IoT) (Celdran et al., 2022). Μια επίθεση ransomware χρησιμοποιεί κρυπτογράφηση ιδιωτικού κλειδιού για να αρνηθεί σε έναν νόμιμο χρήστη την πρόσβαση στο σύστημά του ή στα δεδομένα του μέχρι να πληρώσει κάποιο ποσό χρημάτων ως λύτρα, συνήθως η καταβολή των λύτρων γίνεται σε bitcoin (Richardson & North, 2017).

Οι επιθέσεις ransomware μπορεί επίσης να περιλαμβάνουν εξαγωγή και κλοπή δεδομένων, κατά την οποία οι εισβολείς αντιγράφουν ευαίσθητα αρχεία από παραβιασμένες συσκευές με απειλή να τα αποκαλύψουν δημόσια στο διαδίκτυο εάν ο κάτοχος δεν καταβάλει λύτρα. Το κακόβουλο λογισμικό εξαπλώνεται μέσω συνημμένων email, κακόβουλων διαφημίσεων και κάνοντας κλικ σε έναν σύνδεσμο προς έναν κακόβουλο ιστότοπο. Εντοπίζει τις μονάδες δίσκου στο σύστημα ή το δίκτυο του θύματος και κρυπτογραφεί τα αρχεία σε κάθε μονάδα δίσκου για να αρνηθεί την πρόσβαση των νόμιμων κατόχων σε τέτοια αρχεία (Morhurle & Patil, 2017).

Ο εισβολέας παρέχει επίσης ένα αρχείο, (ή αρχεία) που περιέχει οδηγίες για την πληρωμή των λύτρων. Το κλειδί αποκρυπτογράφησης διατίθεται στο θύμα μόλις ο εισβολέας επιβεβαιώσει την πληρωμή των λύτρων. Τα αρχεία που έχουν μολυνθεί ή κρυπτογραφηθεί από ransomware συνήθως περιέχουν επεκτάσεις όπως .aaa, .micro, .encrypted, .ttt, .xyz, .zzz, .locky, .crypt, .cryptolocker, .vault ή .petya. Η επέκταση κάθε αρχείου καθορίζει τον τύπο του ransomware που μόλυνε το αρχείο.

Παραδείγματα ransomware είναι τα Reveton, CryptoLocker, CryptoLocker.F και TorrentLocker, CryptoWall, CryptoTear, Fusob και WannaCry (Andronio et al., 2015). Το ransomware μπορεί να ομαδοποιηθεί σε (1) crypto ransomware, (2) locker ransomware και (3) scareware (Andronio et al., 2015). Το (Σχήμα 15) απεικονίζει τις λειτουργίες των ransomware locker και κρυπτογράφησης (crypto) (F-Secure Labs, 2013).



Σχήμα 15. Διάγραμμα ροής κρυπτογράφησης ransomware έναντι αστυνομικών ransomware.

Το Crypto είναι το πιο κοινό ransomware που επιτίθεται σε συστήματα υπολογιστών και δίκτυα. Αυτή η κατηγορία ransomware χρησιμοποιεί συμμετρικό ή/και ασύμμετρο κρυπτογραφικό αλγόριθμο για την κρυπτογράφηση αρχείων και δεδομένων. Το ransomware Crypto καθιστά τα κρυπτογραφημένα δεδομένα απρόσιτα ακόμα και αν το κακόβουλο λογισμικό αφαιρεθεί από μια μολυσμένη συσκευή ή ένα παραβιασμένο μέσο αποθήκευσης εισαχθεί σε άλλη συσκευή. Η μολυσμένη συσκευή μπορεί ακόμα να λειτουργήσει και θα μπορούσε να χρησιμοποιηθεί για την πληρωμή των λύτρων, επειδή το κακόβουλο λογισμικό δεν επηρεάζει συνήθως κρίσιμα αρχεία συστήματος (Savage et al., 2015).

Το ransomware Locker, από την άλλη πλευρά, κλειδώνει έναν υπολογιστή ή οποιαδήποτε άλλη συσκευή και εμποδίζει τον ιδιοκτήτη να το χρησιμοποιήσει (Savage et al., 2015). Το ransomware Locker επηρεάζει μόνο τη συσκευή, χωρίς να καθιστά απρόσιτα τα αποθηκευμένα δεδομένα. Επίσης, δεν υπάρχει καμία αλλαγή στα δεδομένα μετά την αφαίρεση του κακόβουλου λογισμικού. Τα δεδομένα μπορούν συχνά να ανακτηθούν με την εισαγωγή της μολυσμένης συσκευής αποθήκευσης, όπως ένας σκληρός δίσκος, σε άλλο σύστημα. Αυτό καθιστά το Locker μη κατάλληλο για την εκβίαση χρημάτων από θύματα επίθεσης.

Σε αντίθεση το scareware εκμεταλλεύεται τα θύματά του εμφανίζοντας μια προειδοποίηση στις οθόνες του υπολογιστή τους ότι τα συστήματα έχουν μολυνθεί και με τον ισχυρισμό ότι ένα ψεύτικο antivirus που διαφημίζεται από τον εισβολέα θα μπορούσε να χρησιμοποιηθεί για την αφαίρεση του ransomware (Brewer, 2016). Η επανειλημμένη εμφάνιση της ειδοποίησης scareware ωθεί πολλούς ανυποψίαστους χρήστες να αγοράσουν και να εγκαταστήσουν το ψεύτικο antivirus. Άλλες κατηγορίες ransomware περιλαμβάνουν αυτά που λειτουργούν από ανθρώπους (Microsoft Ignite, 2022) και ransomware χωρίς αρχεία (Crowdstrike, 2022a).

Οι εγκληματίες του κυβερνοχώρου χρησιμοποιούν ransomware που χειρίζονται από ανθρώπους για να διεισδύσουν σε δίκτυα ή υποδομές cloud, να εκτελούν κλιμάκωση προνομίων και να εξαπολύσουν επιθέσεις κατά κρίσιμων δεδομένων. Είναι μια ενεργή επίθεση που στοχεύει έναν ολόκληρο οργανισμό αντί για ένα ενιαίο σύστημα. Οι επιτιθέμενοι συνήθως χρησιμοποιούν

λανθασμένες διαμορφώσεις ασφαλείας για να διεισδύσουν σε μια ολόκληρη υποδομή πληροφοριακών συστημάτων, να εκτελέσουν έμμεσες κινήσεις και να εκμεταλλευτούν τρωτά σημεία. Αυτό έχει ως αποτέλεσμα μη εξουσιοδοτημένη πρόσβαση σε διαπιστευτήρια προνομιούχων χρηστών με απώτερο στόχο την έναρξη επιθέσεων ransomware κατά πληροφοριακών υποδομών που υποστηρίζουν κρίσιμες επιχειρηματικές λειτουργίες.

Το ransomware χωρίς αρχεία, από την άλλη πλευρά, χρησιμοποιεί εγγενή και νόμιμα εργαλεία συστήματος για την εκτόξευση επιθέσεων (Crowdstrike, 2022b). Είναι δύσκολο να εντοπιστούν επειδή η επίθεση δεν απαιτεί την εγκατάσταση οποιουδήποτε κώδικα στο σύστημα του θύματος. Ως εκ τούτου, τα εργαλεία anti-ransomware δεν βρίσκουν κανένα ύποπτο αρχείο για παρακολούθηση κατά τη διάρκεια μιας επίθεσης. Το ransomware που λειτουργεί από τον άνθρωπο και το ransomware χωρίς αρχεία μπορούν να χρησιμοποιηθούν για την πραγματοποίηση κρυπτογράφησης αρχείων, κλειδώματος ή διαρροής δεδομένων, ανάλογα με το κίνητρο του κακόβουλου εισβολέα.

Το Ransomware αποτελεί σοβαρή απειλή για αρχεία και συσκευές που χρησιμοποιούνται από επιχειρήσεις και ιδιώτες. Εμποδίζει τα θύματα να έχουν πρόσβαση σε μολυσμένα αρχεία ή σε παραβιασμένες συσκευές μέχρι να πληρώσουν λύτρα συνήθως με τη μορφή bitcoin. Σε πολλές περιπτώσεις, οι χάκερ δεν παρέχουν το κλειδί αποκρυπτογράφησης ακόμη και αφού το θύμα πληρώσει λύτρα. Σε άλλες περιπτώσεις, μια προσπάθεια αποκρυπτογράφησης αρχείων χρησιμοποιώντας το κλειδί που παρέχεται από έναν εισβολέα προκαλεί περαιτέρω βλάβη στα αρχεία που είναι αποθηκευμένα στο σύστημα.

Τεχνολογικές καινοτομίες όπως κιτ ανάπτυξης ransomware, ransomware-as-a-service και bitcoins διευκολύνουν τη διαρκή αύξηση των επιθέσεων ransomware εναντίον προσωπικών υπολογιστών, δικτύων και φορητών συσκευών (Zetter, 2015). Οι επιχειρήσεις και τα άτομα υφίστανται απώλειες ύψους εκατοντάδων εκατομμυρίων δολαρίων ετησίως λόγω επιθέσεων ransomware (Fitzpatrick et al., 2016).

Το τεράστιο χρηματικό ποσό που βγάζουν οι χάκερ από επιθέσεις ransomware τροφοδοτεί τη συχνή ανάπτυξη νέων εκδόσεων του κακόβουλου λογισμικού. Στην πραγματικότητα, πολλαπλές εκδόσεις ransomware εμφανίζονται κάθε χρόνο από το 2013. Η εξέλιξη διαφορετικών παραλλαγών ransomware που δεν μπορούν να εντοπιστούν από τα συμβατικά συστήματα προστασίας από ιούς και άλλα συστήματα ανίχνευσης εισβολών, καθώς και οι τεράστιες απώλειες που προκαλούν οι επιθέσεις ransomware σε άτομα και επιχειρήσεις, τονίζουν την ανάγκη για καινοτόμες, αποτελεσματικές και αξιόπιστες τεχνικές για τον αποτελεσματικό εντοπισμό, την πρόληψη και τον μετριασμό των επιθέσεων ransomware.

7. Πρακτικό μέρος powershell script

Σε αυτό το μέρος της διατριβής, θα γίνει αναφορά στο ποιος είναι ο στόχος του powershell script, στη μεθοδολογία που ακολουθήθηκε, τους περιορισμούς που εμφανίστηκαν κατά την συγγραφή του κώδικα, καθώς επίσης και στις προτάσεις βελτίωσης και σύνδεσης του συγκεκριμένου script με εφαρμογές και ανάπτυξη αυτού.

7.1 Μεθοδολογία δημιουργίας κώδικα και Στόχος

Η μεθοδολογία που ακολουθήθηκε για την συγγραφή του κώδικα χωρίζεται σε δύο μέρη. Στο πρώτο μέρος, γίνεται η ανάλυση της εφαρμογών που επιλέχθηκαν και πως μπορούμε να αποκομίσουμε σημαντικές πληροφορίες για την λειτουργία της εφαρμογής μέσα από τα αρχεία καταγραφής της (Log Files).

Σε αρκετές εφαρμογές, για την καλύτερη λειτουργία του, στους φακέλους εγκατάστασης αυτών υπάρχουν και αρχεία που διαθέτουν κατάληξη .txt, .log, .trace και χρησιμοποιούνται για την αποθήκευση ευαίσθητων δεδομένων και πληροφοριών των απομακρυσμένων συνδέσεων. Αυτό τις περισσότερες φορές γίνεται για λόγους καταγραφής των διαδικασιών της εφαρμογής, με σκοπό αργότερα να χρησιμοποιηθούν από την εταιρία που έχει την ιδιοκτησία της εφαρμογής είτε για λόγους καταγραφής ενεργειών των χρηστών είτε για λόγους διόρθωσης σφαλμάτων που μπορεί να έχουν αναφερθεί από τους χρήστες.

Με την δημιουργία του συγκεκριμένου script προσπαθούμε στο πρώτο μέρος των ελέγχων να αναλύσουμε και να αποκρυπτογραφήσουμε τις πληροφορίες που υπάρχουν μέσα στα προαναφερθέντα αρχεία, έτσι ώστε να γίνει η εξαγωγή και παρουσίαση δεδομένων του τύπου:

a) Ποιος χρήστης συνδέθηκε
b) Από ποιο μηχάνημα συνδέθηκε
c) Τι όνομα χρήστη (ID) διαθέτει από την εκάστοτε εφαρμογή
d) Τι λογισμικό χρησιμοποιεί το συγκεκριμένο μηχάνημα
e) Τι ώρα πραγματοποιήθηκε η σύνδεση
f) Από ποια διεύθυνση IP συνδέθηκε
g) Τι αρχεία και φακέλους επηρέασε
h) Τι αρχεία μετέφερε από τον υπολογιστή του
i) Τι αρχεία επηρεάστηκαν κατά την σύνδεση
j) Πότε αποσυνδέθηκε ο χρήστης

Οι περισσότερες από τις παραπάνω πληροφορίες παρέχονται από την εκάστοτε εφαρμογή, όμως σε κάποιες από αυτές τις περιπτώσεις οι παραπάνω πληροφορίες δεν είναι όλες διαθέσιμες και σε αυτό έρχεται το δεύτερο μέρος ελέγχων του powershell scrip, το οποίο με την βοήθεια του Event Viewer των Windows, μας βοηθάει στην εξαγωγή πιο αναλυτικών δεδομένων τα οποία με την βοήθεια του κώδικα μπορούμε να αναγνωρίσουμε και να εξάγουμε. Κάποια παραδείγματα πληροφοριών είναι τα παρακάτω:

a) Πότε συνδέθηκε ο χρήστης απομακρυσμένα
b) Πότε αποσυνδέθηκε από την απομακρυσμένη σύνδεση
c) Ποια αρχεία και φακέλους επηρεάστηκαν και πώς
d) Ποιες εφαρμογές εγκαταστάθηκαν
e) Τι αρχεία τοποθετήθηκαν και σε ποια σημεία του Η/Υ
f) Ποιες εφαρμογές ενεργοποιήθηκαν κατά την απομακρυσμένη σύνδεση
g) Ποιες εφαρμογές απενεργοποιήθηκαν κατά την απομακρυσμένη σύνδεση

Για να μπορεί να γίνει η εξαγωγή των παραπάνω δεδομένων σε μια απομακρυσμένη επιφάνεια εργασίας, υπάρχουν κάποιες προ απαιτούμενες επιλογές οι οποίες θα πρέπει να έχουν ενεργοποιηθεί πριν την χρήστη του script για την ορθότερη εξαγωγή. Οι επιλογές που πρέπει να είναι ενεργές, υπόκεινται στην κατηγορία των πολιτικών του λογισμικού (Group Policies). Οι πολιτικές, είναι μια ιεραρχική υποδομή που επιτρέπει σε έναν διαχειριστή συστήματος, που είναι

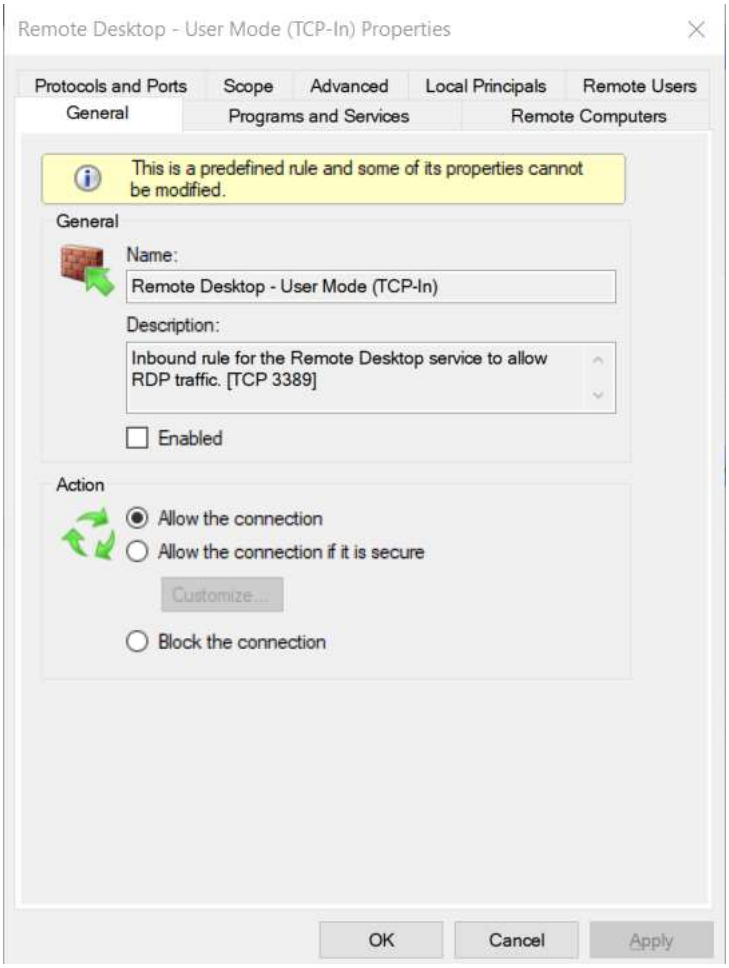
υπεύθυνος για την υπηρεσία καταλόγου Active Directory μιας υποδομής, να υλοποιεί συγκεκριμένες διαμορφώσεις σε χρήστες και υπολογιστές.

Οι πολιτικές, είναι κατά κύριο λόγο ένα εργαλείο ασφαλείας και μπορεί να χρησιμοποιηθεί για την εφαρμογή ρυθμίσεων ασφαλείας. Συνεπώς, Εφαρμόζοντας τις αντίστοιχες πολιτικές στο εκάστοτε μηχάνημα, μπορεί να επιτευχθεί η εξαγωγή των παραπάνω δεδομένων μέσα από το δημιουργημένο powershell script. Οι πολιτικές οι οποίες θα πρέπει να έχουν ενεργοποιηθεί υπόκεινται στην κατηγορία *Computer Configuration→Windows Settings→Security Settings→Local Policies→Audit Policy.*

Για τις ανάγκες του συγκεκριμένου script και έπειτα από ενδελεχή προσωπική μελέτη των πολιτικών και γνώση πάνω στις πολιτικές που αποκτήθηκαν από το επάγγελμά μου, οι επιλογές που ενεργοποιήθηκαν είναι οι παρακάτω:

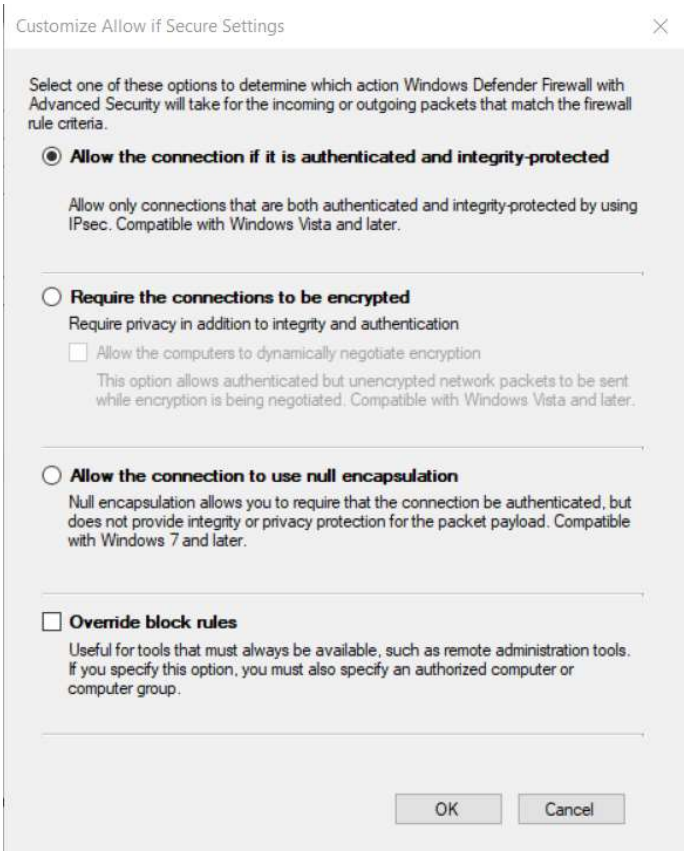
i. *Audit account Logon events:* Είναι πολιτική η οποία δημιουργεί εγγραφές οι οποίες αναφέρουν ποιοι λογαριασμοί χρηστών/διαχειριστών αυθεντικοποιήθηκαν στο συγκεκριμένο σύστημα. Για τις ανάγκες των αποτελεσμάτων, η τιμές που ορίστηκαν είναι Επιτυχίας (Success) και Αποτυχίας (Failure) έτσι ώστε να μπορούμε να εξάγουμε και αποτυχημένες προσπάθειες σύνδεσης στο συγκεκριμένο τερματικό
ii. *Audit Logon events:* Η παρούσα πολιτική, δημιουργεί αποτελέσματα τα οποία μας δείχνουν ποιοι χρήστες συνδέθηκαν, αποσυνδέθηκαν, συνδέθηκαν με ειδικά δικαιώματα, κλειδώθηκαν κ.α. Για να μπορούμε να εξάγουμε πληροφορίες από την συγκεκριμένη πολιτική, ορίσαμε τις τιμές Επιτυχίας (Success) και Αποτυχίας (Failure).
iii. *Audit Object Access:* Η συγκεκριμένη πολιτική, δημιουργεί εγγραφές οι οποίες αναφέρουν ποια αντικείμενα του τερματικού, έγιναν προσπάθειες οποιαδήποτε αλλαγής (διαγραφή, μετονομασία, αντιγραφή, επικόλληση, άνοιγμα αρχείου, προβολή κ.α.). Για να μπορούμε να αντλήσουμε πληροφορίες, δεδομένου του όγκου των πληροφοριών που δημιουργούσε η συγκεκριμένη κατηγορία, ορίσαμε την τιμή Επιτυχίας (Success).
iv. *Audit process tracking:* Σε αυτή την πολιτική, οι εγγραφές που δημιουργούνται είναι για όσες διεργασίες ενεργοποιήθηκαν, απενεργοποιήθηκαν, τροποποιήθηκαν. Για την ορθή εξαγωγή των δεδομένων, ορίσαμε την τιμή Επιτυχίας (Success).

Ένα πρόσθετο στάδιο που θα πρέπει να ενεργοποιηθεί για το Remote Desktop Connection των Windows θα είναι να επιτραπεί η εισερχόμενη κίνηση για απομακρυσμένο έλεγχο. Για να ενεργοποιηθεί το παραπάνω θα πρέπει στην απομακρυσμένη επιφάνεια εργασίας, να πλοηγηθούμε στον πίνακα ελέγχου και από εκεί στο «Τοίχος προστασίας» των Windows. Στην νέα κατηγορία που θα ανοίξει, στο αριστερό μενού επιλέγουμε τις «Ρυθμίσεις για προχωρημένους». Στο νέο παράθυρο που θα εμφανιστεί, επιλέγουμε την «Εισερχόμενους κανόνες» (Inbound Rules). Από εκεί, θα πρέπει να βρούμε τον κανόνα ο οποίος έχει όνομα “Remote Desktop – User Mode (TCP-in)” και να επιλέξουμε το “Allow” όπως φαίνεται και στο παρακάτω (Σχήμα 16).



Σχήμα 16. Κανόνας Τοίχους προστασίας για RDP σύνεση

Όπως είναι εμφανές και στο παραπάνω (Σχήμα 16), έχουμε επιτρέψει οποιαδήποτε εισερχόμενη κίνηση στην πόρτα TCP 3389 που είναι η κλασσική πόρτα του Windows Remote Desktop connection. Δεδομένου ότι δεν υπόκεινται σε αρκετή ασφάλεια η συγκεκριμένη υλοποίηση, ως επιπρόσθετο μέσο ασφάλειας, θα μπορούσαμε να επιλέξουμε να επιτρέπονται εισερχόμενες κινήσεις οι οποίες περιέχουν ασφαλείς ρυθμίσεις.



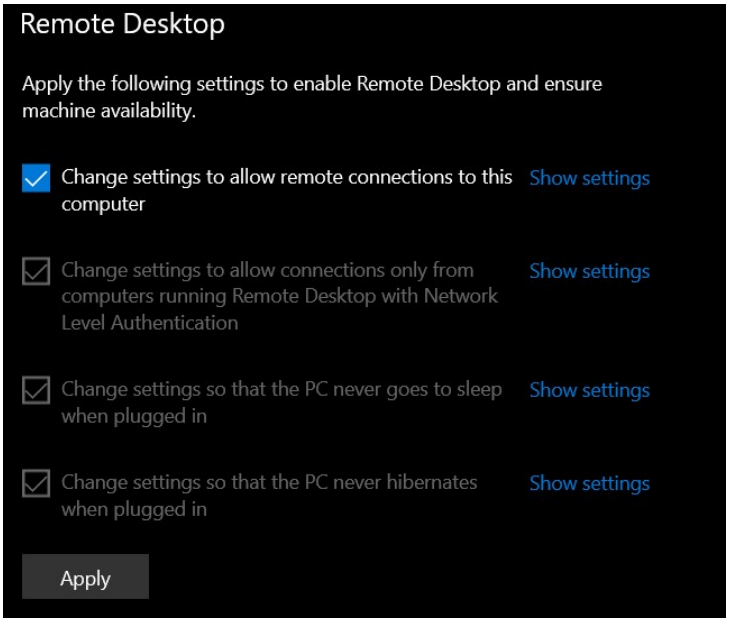
Σχήμα 17. Πρόσθετες επιλογές Ασφάλειας Remote Desktop connection

Πιο αναλυτικά, αν στο παραπάνω (Σχήμα 17), επιλέξουμε το “Allow the connection if it is secure”, θα μας εμφανίσει ένα επιπλέον κουμπί το οποίο μας δίνει την δυνατότητα να προσθέσουμε έξτρα μέτρα ασφάλειας στην απομακρυσμένη σύνδεση. Μόλις επιλέξουμε το κουμπί “Customize…”, στο νέο παράθυρο που θα εμφανιστεί βλέπε (Σχήμα 17) μπορούμε να διαλέξουμε τις παρακάτω επιλογές:

1) *Allow the connection if it is authenticated and integrity-protected:* Επιτρέπουμε την εισερχόμενη κίνηση η οποία έχει αυθεντικοποιηθεί αλλά όχι απαραίτητα να είναι κρυπτογραφημένη. Δεδομένου ότι η εισερχόμενη κίνηση είναι ήδη κρυπτογραφημένη μέσω του RDP, η απαίτηση κρυπτογράφησης στο επίπεδο μεταφοράς δεδομένων είναι απλώς επιπλέον επιβάρυνση.
2) *Require the connection to be encrypted:* Η συγκεκριμένη επιλογή, απαιτεί η σύνδεση να είναι κρυπτογραφημένη, πέραν της αυθεντικοποίησης. Επιπρόσθετα, δίνεται η επιλογή να γίνεται μεταφορά πακέτων απομακρυσμένης σύνδεσης έως ότου γίνει η διαπραγμάτευση της κρυπτογράφησης.
3) *Allow the connection to use null encapsulation:* Η συγκεκριμένη επιλογή απαιτεί η αντίστοιχη κυκλοφορία δικτύου να χρησιμοποιεί έλεγχο ταυτότητας IPsec, αλλά δεν απαιτεί ούτε ακεραιότητα ούτε κρυπτογράφηση σύνδεσης. Η επιλογή αυτή, προτείνεται να ενεργοποιήσετε εάν διαθέτουμε εξοπλισμό δικτύου ή λογισμικό που δεν είναι συμβατό με τα πρωτόκολλα ακεραιότητας ESP (Encapsulating Security Payload) ούτε με το AH (Authentication Header).

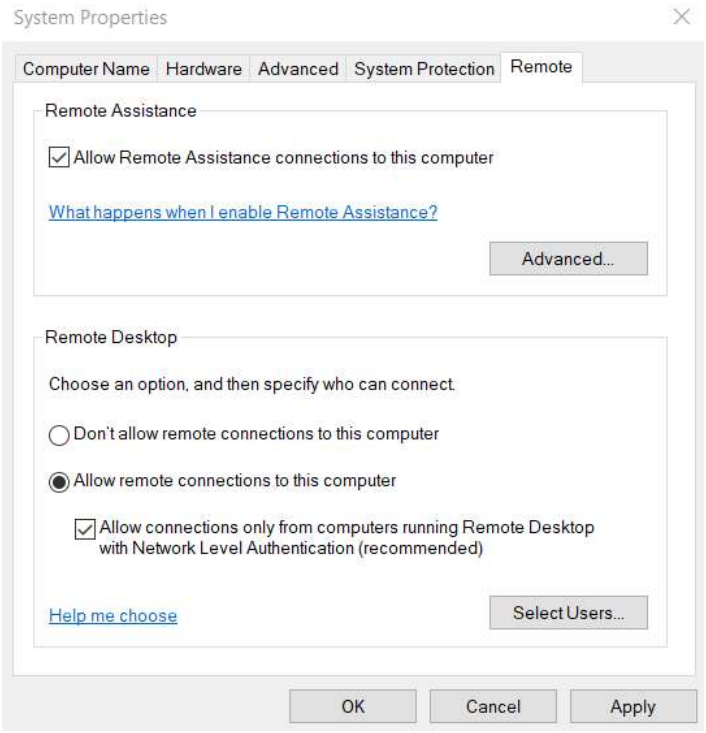
Αφού επιλεχθεί μια από τις παραπάνω επιλογές, υπάρχει ακόμα μια επιπλέον επιλογή η “Override block rules”. Η συγκεκριμένη επιλογή μας δίνει την δυνατότητα, σε περίπτωση που υπάρχει εφαρμογή που χρησιμοποιεί την πόρτα 3389, να επιτρέπει την κίνηση χωρίς να υφίσταται κάποιος συγκεκριμένος κανόνας εισερχόμενης κίνησης. Για να ενεργοποιηθεί ορθά αυτή η επιλογή, θα πρέπει να οριστεί κάποιο άλλο απομακρυσμένο μηχάνημα ή group από μηχανήματα, τα οποία θα έχουν διαχειριστική πρόσβαση πάνω στην απομακρυσμένη επιφάνεια.

Αφού ολοκληρώσουμε τις δικτυακές επιλογές με βάση τις παραπάνω αναφορές, θα πρέπει αντίστοιχα να δοθούν και τα δικαιώματα στους χρήστες οι οποίοι θα μπορούν να συνδέονται απομακρυσμένα. Αυτό μπορεί να επιτευχθεί αν πλοηγηθούμε από την «Έναρξη των Windows», στις «Ρυθμίσεις» (Settings) του μηχανήματος. Στο νέο παράθυρο, επιλέγουμε την κατηγορία «Ασφάλεια και Ενημερώσεις» (Update & Security) και στο νέο παράθυρο που θα εμφανιστεί, στο μενού αριστερά επιλέγουμε «Για προγραμματιστές» (For Developers). Σε αυτό το σημείο να αναφερθεί, ότι για να μπορέσουμε να ενεργοποιήσουμε την απομακρυσμένη σύνδεση, θα πρέπει να διαθέτουμε άδεια για Windows 10 Pro ή Windows 10 Enterprise, για να ξεκλειδωθεί η επιλογή ενεργοποίησης απομακρυσμένης επιφάνειας.



Σχήμα 18. Επιλογές ενεργοποίησης απομακρυσμένης σύνδεσης

Για την ενεργοποίησή της, θα πρέπει να επιλέξουμε να επιτρέπεται η απομακρυσμένη σύνδεση όπως παρουσιάζεται στο παραπάνω (Σχήμα 18) και έπειτα επιλέγοντας την «Εμφάνιση επιλογών» (Show Settings), στο παράθυρο που θα εμφανιστεί να επιλέξουμε να επιτρέπονται απομακρυσμένες συνδέσεις όπως φαίνεται στο παρακάτω (Σχήμα 19).



Σχήμα 19. Επιλογές συστήματος για απομακρυσμένη σύνδεση

Ως επιπρόσθετες επιλογές, για την ενεργοποίηση της απομακρυσμένης επιφάνειας εργασίας, μας δίνεται η δυνατότητα να επιτρέψουμε συνδέσεις που διαθέτουν NLA (Network Level Authentication). Αυτό σημαίνει ότι μπορούν να συνδεθούν χρήστες οι οποίοι έχουν περάσει το στάδιο αυθεντικοποίησης πριν την σύνδεση. Τέλος, δίνεται η δυνατότητα να επιλέξουμε και χρήστες ή γκρουπ χρηστών οι οποίοι θα έχουν μόνο απομακρυσμένη πρόσβαση στον υπολογιστή.

Με τις παραπάνω επιλογές και ρυθμίσεις, κλείνουμε τον κύκλο προαπαιτούμενων ρυθμίσεων έτσι ώστε να μπορούμε με ασφάλεια να ενεργοποιήσουμε την απομακρυσμένη πρόσβαση. Στις επόμενες παραγράφους θα αναλύσουμε πως μπορεί να γίνει καλύτερη διαχείριση των παραπάνω επιλογών και ρυθμίσεων με εργαλεία και εφαρμογές από γνωστές εταιρίες του χώρου της ασφάλειας.

Κλείνοντας αυτή την ενότητα, θα πρέπει να αναφέρουμε ότι ο στόχος της δημιουργίας του παραπάνω κώδικα σε powershell script είναι να αντλήσει όσα περισσότερα δεδομένα μπορούμε με την βοήθεια και των εφαρμογών και των Εγγραφών (Event Log των windows). Η άντληση αυτών των δεδομένων έχει ως στόχο να βοηθήσει έναν αναλυτή να διαλευκάνει με ποιον τρόπο συνδέθηκε κάποιος κακόβουλος χρήστης και τι ενέργειες ακολούθησε έτσι ώστε να υπάρχει μια πιο ξεκάθαρη εικόνα της ασφάλειας του συστήματος είτε ακόμα και της διόρθωσης ενός μολυσμένου με κακόβουλο λογισμικό μηχανήματος. Τα δεδομένα που θέλουμε να αντλήσουμε δεν βοηθούν μόνο στην αναγνώριση των κακόβουλων ενεργειών που ακολουθήθηκαν, αλλά και στο να γίνει ανίχνευση (Trace) ποιος ή τί αποτελεί την πηγή (Source) αυτών των ενεργειών.

7.2 Περιορισμοί και αντιμετώπιση

Κατά την δημιουργία του συγκεκριμένου κώδικα, υπήρξαν περιορισμοί και τροχοπέδη τα οποία με συγκεκριμένες αλλαγές στις επιλογές του μηχανήματος ή του κώδικα μπόρεσαν να αντιμετωπιστούν. Παρακάτω, παρουσιάζονται οι περιορισμοί που ανιχνεύτηκαν κατά την συγγραφή του συγκεκριμένου script, ποιοι επιλύθηκαν, ποιοι παραμένουν και ποιοι δεν είναι δυνατόν να αντιμετωπιστούν.

Περίπτωση 1η: Απεγκατάσταση της εφαρμογής απομακρυσμένης διαχείρισης

Παράκαμψη-Επίλυση: Δεδομένου ότι το πρώτο μέρος του script βασίζεται στα δεδομένα τα οποία αντλούνται από τα αρχεία καταγραφής των εφαρμογών (log files, txt files, trace files), παρατηρήθηκε ότι και με την απεγκατάσταση των εφαρμογών τα αρχεία καταγραφής συνέχιζαν να παραμένουν στις αντίστοιχες τοποθεσίες του υπολογιστή. Συνεπώς, ορίζοντας μια μεταβλητή στο script η οποία περιέχει τις αντίστοιχες διαδρομές (Paths) των log/trace αρχείων, μπορούμε με έναν απλό έλεγχο με την χρήση της εντολής AN (IF) να ελέγξουμε αν τα συγκεκριμένα αρχεία υπάρχουν και περιέχουν δεδομένα. Η παραπάνω παράκαμψη-λύση, χρησιμοποιείται μόνο για της εφαρμογές που διαθέτουν αρχεία καταγραφής και δεν είναι εφαρμόσιμη στο Remote Desktop Connection των Windows, διότι το Windows RDP καταγράφεται στα Event Logs των Windows.

Περίπτωση 2η: Διαγραφή αρχείων καταγραφής

Παράκαμψη-Επίλυση: Στην συγκεκριμένη περίπτωση γίνεται παράκαμψη από τον κώδικα διότι χωρίς τα αρχεία καταγραφής στις εφαρμογές (εξαιρείται το Windows RDP) δεν είναι εφικτό να γίνει έλεγχος ποιος χρήστης συνδέθηκε, πότε συνδέθηκε κ.α. Η παράκαμψη η οποία υλοποιήθηκε είναι ότι, ο κώδικας θα ανιχνεύσει αν δεν υπάρχουν αρχεία καταγραφής για την εκάστοτε εφαρμογή και θα προχωρήσει στον έλεγχο των αρχείων που τοποθετήθηκαν σήμερα, των αρχείων που διαγράφηκαν/τροποποιήθηκαν σήμερα, εφαρμογές οι οποίες εγκαταστάθηκαν, εφαρμογές οι οποίες απεγκαταστάθηκαν καθώς και ποιες διεργασίες ανοίχτηκαν και ποιες διεργασίες έκλεισαν. Η παραπάνω παράκαμψη επιτυγχάνεται με τον έλεγχο στον κώδικα, ότι AN η μεταβλητή που έχουμε εκχωρήσει την διαδρομή του αρχείου είναι κενή. Τότε εκχωρούμε σε μια 2η δυαδική μεταβλητή (Boolean) αληθή (true) ή ψευδή (false) τιμή ούτος ώστε στους επόμενου ελέγχους AN (IF) του κώδικα που γίνεται για τα δεδομένα της εφαρμογής, να μας αναφέρεται ότι η αντίστοιχη εφαρμογή έχει διαγραφεί. Έπειτα από την αναφορά της διαγραφής των αρχείων καταγραφής της εφαρμογής και δεδομένου ότι πλέον δεν υπάρχει χρονικό περιθώριο για να μπορούμε να εμφανίσουμε κινήσεις που έγιναν κατά την διείσδυση στο σύστημα (Intrusion), το script θα εμφανίσει όλα τα events που δημιουργήθηκαν την σημερινή ημέρα που έγινε αντιληπτή η κακόβουλη ενέργεια. Το παραπάνω, δεν υπόκεινται στο Windows Remote Desktop connection, διότι τα connections καταγράφονται στον Event viewer των Windows.

Περίπτωση 3η: Τροποποίηση αρχείων καταγραφής (διαγραφή, κρυπτογράφηση, καθαρισμός δεδομένων)

Παράκαμψη-Επίλυση: Σε περίπτωση που τα αρχεία καταγραφής διαγραφούν, είτε κρυπτογραφηθούν (στην περίπτωση crypto ransomware), είτε τροποποιηθούν εσωτερικά, δεν θα γίνει η άντληση των πληροφοριών ποιος χρήστης συνδέθηκε, πότε συνδέθηκε κ.α. και θα ισχύσει η εξαγωγή δεδομένων όπως αναφέρεται στην περίπτωση 2. Συνεπώς, η μεταβλητή η οποία έχουμε εκχωρήσει το συγκεκριμένο αρχείο καταγραφής, ελέγχεται με την λειτουργία AN και αντιλαμβάνεται αν το αρχείο που έχει εισαχθεί στην μεταβλητή υπάρχει και αν είναι διάφορο (Not equal) με το κενό. Έπειτα, ενημερώνει τον χρήστη ότι το αρχείο έχει διαγραφεί/μετονομαστεί και εκχωρεί στην σχετική δυαδική μεταβλητή αληθή ή ψευδή τιμή με σκοπό στον αμέσως επόμενο έλεγχο για την εξαγωγή των δεδομένων από τα αρχεία καταγραφής, να μην ξεκινήσει την άντληση των πληροφοριών και να προχωρήσει στο 2ο σκέλος του script για τον έλεγχο των Events. Σε περίπτωση που τα αρχεία καταγραφής έχουν κρυπτογραφηθεί, οι εξαγωγή πληροφοριών δεν μπορεί να ολοκληρωθεί. Η παραπάνω λύση, δεν υπόκεινται στο Windows Remote Desktop Connection, διότι όλες οι πληροφορίες αντλούνται από το Event Viewer των Windows.

Περίπτωση 4η: Αφαίρεση μερικών εγγραφών από το Event Viewer των Windows

Παράκαμψη-Επίλυση: Στην συγκεκριμένη περίπτωση, αν κάποιες εγγραφές διαγραφούν από το Windows Event Viewer, το script θα ελέγξει ποιες εγγραφές αφαιρέθηκαν και αντίστοιχα θα ενημερώσει τον αναλυτή. Ο κώδικας θα συνεχίσει να εξάγει οποιαδήποτε πληροφορία είναι εφικτή από τα αρχεία καταγραφής των εφαρμογών και έπειτα θα προχωρήσει στην εξαγωγή όσων καταγραφών είναι διαθέσιμες από το Event Viewer των Windows. Αυτό επιτυγχάνεται διότι γίνεται έλεγχος των events στο Event Viewer των Windows με το ID (1102). Πριν ξεκινήσει οποιοσδήποτε έλεγχος αναφέρεται σε μια από τις 3 εφαρμογές που πραγματευόμαστε, γίνεται έλεγχος με το AN το παραπάνω Event ID, έχει εμφανιστεί σήμερα εντός 24ων ωρών και μας το παρουσιάζει. Έπειτα, ελέγχονται οι εφαρμογές με σκοπό να αντλήσουμε την πληροφορία του πότε έγινε είσοδος κάποιου χρήστη απομακρυσμένα και πότε έγινε η αντίστοιχη έξοδος από το σύστημα και

με την χρήση της AN, ελέγχουμε αν το παραπάνω event ID εμφανίστηκε εντός των συγκεκριμένων χρονικών ορίων. Στην περίπτωση που δεν έχουν αφαιρεθεί τα events για την σύνδεση με το Windows RDP connection, αντλούμε τις πληροφορίες εισόδου και εξόδου του χρήστη με απομακρυσμένη σύνδεση και ελέγχουμε εκ νέου με την AN το παραπάνω event ID, εμφανίστηκε στα συγκεκριμένα χρονικά περιθώρια και αναφέρουμε στον χρήστη πότε έγινε.

Περίπτωση 5η: Αφαίρεση όλων των εγγραφών από το Event Viewer των Windows

Παράκαμψη-Επίλυση: Στην περίπτωση όπου διαγραφούν όλες οι εγγραφές από το Windows Event Viewer, ο κώδικας θα το αναγνωρίσει και αντίστοιχα θα ενημερώσει ότι δεν είναι δυνατόν να εξάγει τις πληροφορίες για το ποιες εφαρμογές εγκαταστάθηκαν, ποιες εφαρμογές απεγκαταστάθηκαν, ποια αρχεία τροποποιήθηκαν/διαγράφηκαν, ποια αρχεία άνοιξαν, ποιες εφαρμογές ξεκίνησαν και ποιες εφαρμογές έκλεισαν. Θα συνεχίσει να εμφανίσει οποιοδήποτε δεδομένο από τα αρχεία καταγραφής της εκάστοτε εφαρμογής καθώς και πιθανές αλλαγές σε κλειδιά του μητρώου των Windows (Registry). Όπως προαναφέρθηκε, γίνεται εξαγωγή των events από τον Event Viewer των Windows και εμφανίζουμε το πότε έγινε η διαγραφή των events. Από εκεί και πέρα, εξάγουμε ξανά με την βοήθεια των αρχείων καταγραφής, τα χρονικά όρια σύνδεση και αποσύνδεσης απομακρυσμένα και ελέγχουμε την χρήση της AN, έχει γίνει διαγραφή των events στα συγκεκριμένα όρια. Ως επόμενο βήμα, εξάγουμε ότι δεδομένα από εφαρμογές που ανοίχτηκαν, αρχεία που τροποποιήθηκαν, εφαρμογές που εγκαταστάθηκαν με την βοήθεια του ελέγχου της AN για το χρονικό περιθώριο 24ων ωρών. Στην περίπτωση του Windows Remote Desktop Connection, ελέγχουμε οποιοδήποτε event για απομακρυσμένη σύνδεση έχει καταγραφεί με την χρήση της AN και σε περίπτωση που δεν υπάρχει κάποιο event ID (1149), εκμεταλλευόμαστε το μήνυμα σφάλματος της powershell ότι δεν βρέθηκε κανένα event απομακρυσμένης σύνδεσης. Ο ίδιος έλεγχος, γίνεται ακριβώς και για τις αποσυνδέσεις από το σύστημα όπου και πάλι, εκμεταλλευόμαστε το μήνυμα σφάλματος της powershell και αναγράφεται στο χρήστη ότι δεν υπάρχει κανένα event με το συγκεκριμένο ID (24). Δυστυχώς, στο 2ο σκέλος για έλεγχο αρχείων και διεργασιών, γίνεται μόνο η εξαγωγή δεδομένων από διεργασίες που εκκινήθησαν και έκλεισαν και από αρχεία που τροποποιήθηκαν με οποιοδήποτε τρόπο εντός 24ων ωρών.

Περίπτωση 6η: Αφαίρεση όλων των εγγραφών από το Event Viewer των Windows και Απεγκατάσταση των εφαρμογών

Παράκαμψη-Επίλυση: Σε περίπτωση που διαγραφούν όλες οι εγγραφές και απεγκατασταθούν οι εφαρμογές, παρατηρήθηκε ότι ορισμένα αρχεία καταγραφής παραμένουν, συνεπώς γίνεται έλεγχος και εξαγωγή δεδομένων από τα αρχεία καταγραφής και έπειτα η εφαρμογή ενημερώνει ότι δεν υπάρχουν εγγραφές στο Event Viewer των Windows. Με την χρήση της AN, γίνεται έλεγχος αν τα αρχεία καταγραφών υφίστανται και περιέχουν δεδομένα και ξεκινάει η άντληση οποιασδήποτε πληροφορίας και καταγραφή αυτών των πληροφοριών στους σχετικούς πίνακες (Arrays). Από εκεί, με την χρήση της AN, ελέγχουμε εκ νέου αν η διαγραφή των events έχει γίνει εντός των χρονικών ορίων που έγινε η απομακρυσμένη σύνδεση και έπειτα ενημερώνουμε τον χρήστη με το σχετικό μήνυμα. Το script θα συνεχίσει να ελέγξει τις αλλαγές που έχουν γίνει σε αρχεία και εφαρμογές εντός των τελευταίων 24ων ωρών. Στην περίπτωση του RDP connection, γίνεται έλεγχος με την AN έτσι ώστε να ανιχνεύσουμε οποιοδήποτε στοιχείο remote connection μπορεί να βρεθεί. Αν δεν βρεθεί κάποιο στοιχείο εκμεταλλευόμαστε το σφάλμα της powershell και εμφανίζεται στον χρήστη ότι δεν υπάρχουν δεδομένα σύνδεσης με το ID (1149) ή δεδομένα αποσύνδεση με το ID (24).

Περίπτωση 7η: Αφαίρεση όλων των εγγραφών από το Event Viewer των Windows και Απεγκατάσταση των εφαρμογών και διαγραφή/κρυπτογράφηση/τροποποίηση των αρχείων καταγραφής

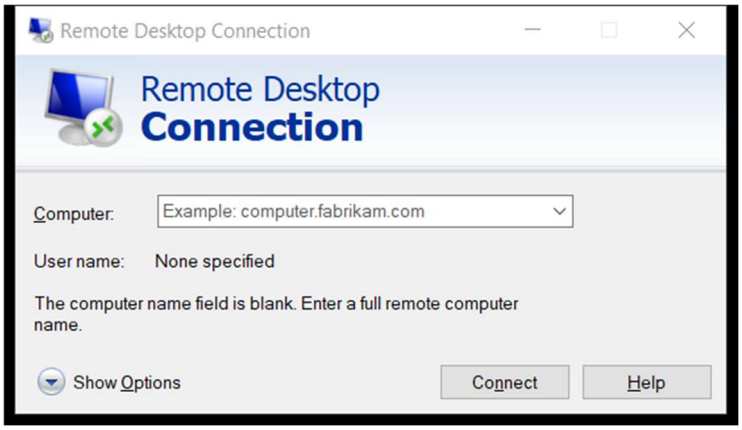
Παράκαμψη-Επίλυση: Στην τελευταία περίπτωση που θα εξετάσουμε, είναι να αφαιρεθούν και οι εφαρμογές απομακρυσμένης πρόσβασης και τα αρχεία καταγραφής (Log Files – Trace files) αλλά και να διαγραφούν τα events του Event Viewer των Windows. Ο κώδικας δεν θα φέρει πληροφορίες όπως ποιος χρήστης συνδέθηκε, από ποια εφαρμογή, με ποια διεύθυνση κ.ο.κ και θα προσπαθήσει να αντλήσει όσα δεδομένα μπορεί από τον Windows Event Viewer μεταξύ 24ων ωρών από την ενεργοποίηση του powershell script.

8. Παρουσίαση εφαρμογής/Powershell Script

Όπως αναφέρθηκε και στις προηγούμενες ενότητες, το πρακτικό μέρος της διατριβής αποτελείται από ένα powershell script το οποίο αναγνωρίζει συγκεκριμένες εφαρμογές και με την βοήθεια των log file ή trace file, αντλεί πληροφορίες αναφορικά με τις συνδέσεις που έγιναν στο απομακρυσμένο μηχάνημα και εμφανίζει πληροφορίες σχετικά με όσες ενέργειες έγιναν κατά την σύνδεση.

Οι εφαρμογές οι οποίες ανιχνεύονται από το powershell script είναι:

a) *Windows Remote Desktop Connection:* Πρόκειται για την προ εγκατεστημένη εφαρμογή των Windows, η οποία επιτρέπει σε χρήστες την απομακρυσμένη σύνδεση σε επιφάνεια εργασίας με την χρήση ονόματος χρήστη και κωδικού. Η διαδικασία αυθεντικοποίησης (authentication) γίνεται από την απομακρυσμένη επιφάνεια εργασίας (σε τοπικό επίπεδο), είτε σε επίπεδο Τομέα (Domain). Μόλις ολοκληρωθεί η αυθεντικοποίηση (authentication), ο χρήστης συνδέεται στην απομακρυσμένη επιφάνεια εργασίας και το περιβάλλον που παρουσιάζεται είναι ακριβώς ενός υπολογιστή μετά την σύνδεση στα Windows. Η άντληση δεδομένων για τις απομακρυσμένες συνδέσεις που πραγματοποιήθηκαν γίνονται με την βοήθεια των Event με ID 1149 που έχουν δημιουργηθεί αντίστοιχα στον Event Viewer της απομακρυσμένης επιφάνειας.



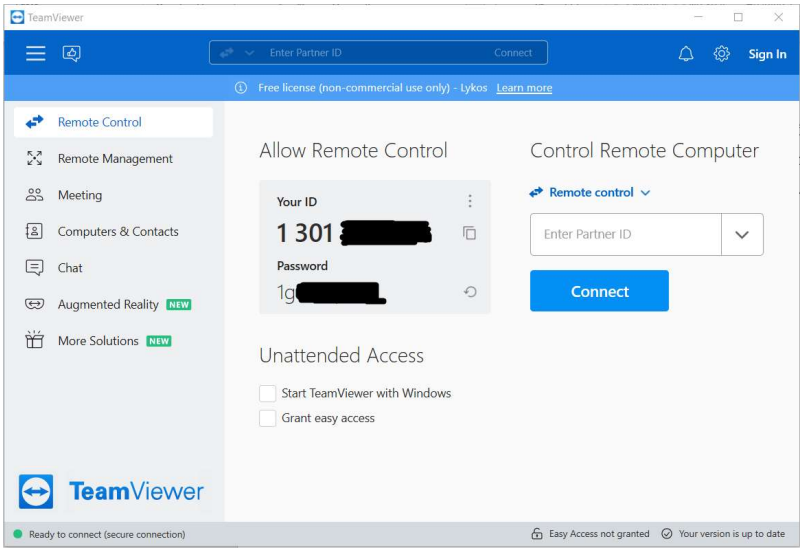
Σχήμα 20. Windows Remote Desktop Connection

b) *Teamviewer:* Πρόκειται για εφαρμογή απομακρυσμένης σύνδεσης της Teamviewer στην οποία οι χρήστες κατεβάζουν μέσα από την επίσημη σελίδα της Teamviewer (https://www.teamviewer.com/) την εφαρμογή και πραγματοποιούν την εγκατάσταση στο τερματικό τους. Για να μπορούν να συνδεθούν σε οποιοδήποτε απομακρυσμένο τερματικό, θα πρέπει και το απομακρυσμένο τερματικό να διαθέτει εγκατεστημένη την εφαρμογή της Teamviewer. Από εκεί και πέρα, το τερματικό που χρειάζεται να συνδεθούμε απομακρυσμένα, θα πρέπει να μας παρέχει το μοναδικό ID που δίνεται από τον κεντρικό διακομιστή (Server) της Teamviewer καθώς επίσης και το μοναδικό κωδικό (Password) με σκοπό να γίνει η απομακρυσμένη σύνδεση μεταξύ των τερματικών. Για την άντληση δεδομένων για τις απομακρυσμένες συνδέσεις, γίνεται η χρήση των Log/txt files της εφαρμογής που εμφανίζονται στις παρακάτω διευθύνσεις αρχείων:

C:\Program Files\TeamViewer\TeamViewer15_Logfile.log

C:\Program Files\TeamViewer\Connections_incoming.txt

C:\Users*User*\AppData\Roaming\TeamViewer\TeamViewer15_Logfile.log

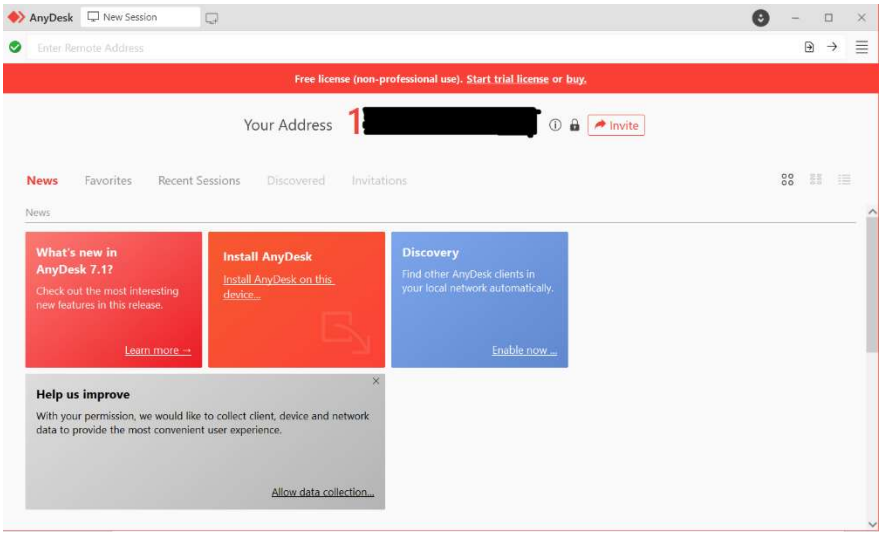


Σχήμα 21. Teamviewer Remote connection interface

c) *Anydesk:* Η τελευταία εφαρμογή που γίνεται έλεγχος είναι το Anydesk της ομώνυμης εταιρίας (https://anydesk.com/). Ο χρήστης, όπως αναφέρθηκε και με τη εφαρμογή της Teamviewer, πρέπει μέσα από την επίσημη σελίδα της Anydesk, να κατεβάσει την εφαρμογή στο τερματικό του, να την εγκαταστήσει και αντίστοιχα να πραγματοποιήσει την εγκατάσταση και στο απομακρυσμένο τερματικό. Για να πραγματοποιηθεί η σύνδεση, ο χρήστης πρέπει να εισάγει το μοναδικό ID που παρέχεται από τον διακομιστή της εφαρμογής στην απομακρυσμένη επιφάνεια εργασίας, να πατήσει να συνδεθεί και έπειτα η απομακρυσμένη πλευρά, να αποδεχθεί το αίτημα σύνδεσης. Από εκεί και πέρα, ολοκληρώνεται η σύνδεση στην απομακρυσμένη επιφάνεια. Για την άντληση δεδομένων για τις απομακρυσμένες συνδέσεις, γίνεται η χρήση των Trace files της εφαρμογής που εμφανίζονται στις παρακάτω διευθύνσεις αρχείων:

C:\Users*User*\AppData\Roaming\AnyDesk\ad.trace

C:\ProgramData\AnyDesk\ad_svc.trace

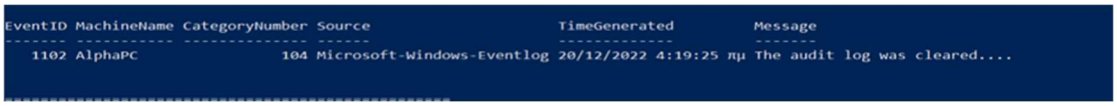


Σχήμα 22. Anydesk Remote connection interface

8.1 Παρουσίαση Αποτελεσμάτων Powershell Script

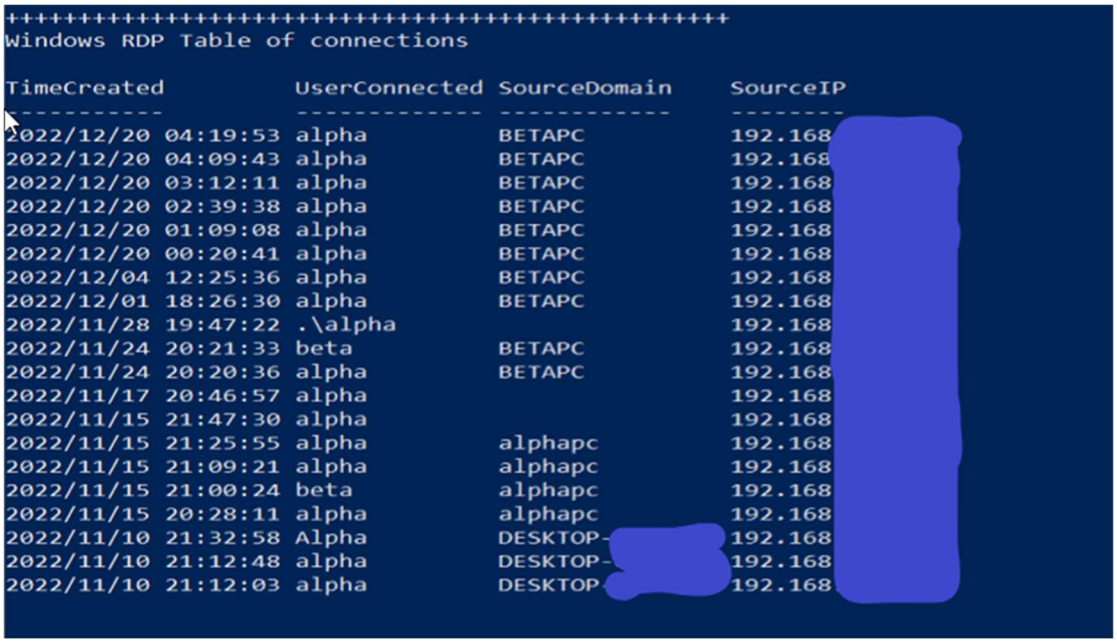
Όπως αναφέραμε και στα προηγούμενα μέρη της διατριβής, τα δεδομένα αντλούνται σε δύο διαφορετικές φάσεις και αντίστοιχα παρουσιάζονται κατά την υλοποίηση του κώδικα ο οποίος έχει γραφεί σε γλώσσα Powershell και έχει αποθηκευτεί με την μορφή Script. Παρακάτω θα δοθούν ορισμένα παραδείγματα από το ποιες πληροφορίες παρουσιάζονται και το πως εξάγονται σε αντίστοιχα αρχεία Json.

Στα παρακάτω παραδείγματα εμφανίζονται δεδομένα που αντλήθηκαν από το powershell script για κάθε μια από τις εφαρμογές που ελέγχουμε.



Σχήμα 23. Έλεγχος διαγραφής Event Logs

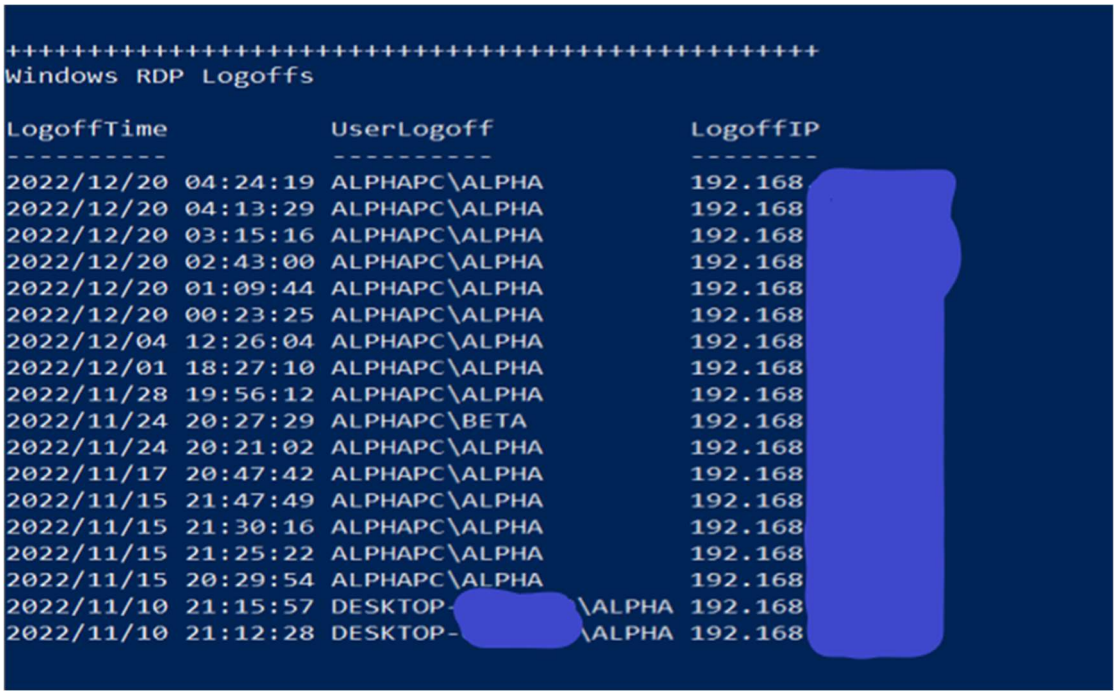
Στο (Σχήμα 23), εμφανίζεται ο αρχικός έλεγχος που γίνεται με την εντολή Get-EventLog στην κατηγορία του Security. Αφού εκχωρήσουμε σε μεταβλητή τα events των τελευταίων 24ων ωρών, ελέγχουμε με συνθήκη IF(), αν μέσα στα events που εκχωρήθηκαν στην μεταβλητή υπάρχουν events με ID 1102. Σε περίπτωση που υπάρχουν τέτοιου είδους events, αναφέρουμε στον χρήστη ότι τις τελευταίες 24 ώρες έχουν διαγραφεί event logs και αντίστοιχα εμφανίζουμε με την εντολή write-host ως πίνακα, την τελευταία φορά που έγινε τέτοιου είδους διαγραφή.



Σχήμα 24. Επιτυχείς συνδέσεις με Remote Desktop Connection

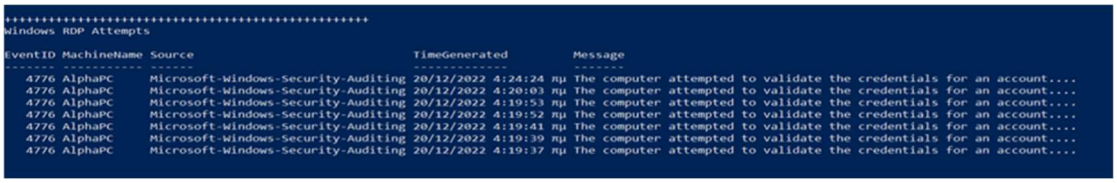
Στο παραπάνω (Σχήμα 24) γίνεται εκχώρηση σε μεταβλητή με την χρήση της εντολής Get-WinEvent, για όσα events έχουν δημιουργηθεί με ID (1149) στο event log path “Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational”. Έπειτα, τα δεδομένα της μεταβλητής ελέγχονται με τη IF, για να γίνει έλεγχος σε περίπτωση που έχουν αφαιρεθεί τα events με το συγκεκριμένο ID. Σε περίπτωση που δεν έχουν διαγραφεί τα events, γίνεται ανάγνωση από το script των event με την χρήση xml μορφοποίησης και τα δεδομένα παρουσιάζονται στην οθόνη

του τερματικού και εκχωρούνται σε αντίστοιχο πίνακα με σκοπό να είναι προσβάσιμα για ελέγχους σε επόμενα βήματα.



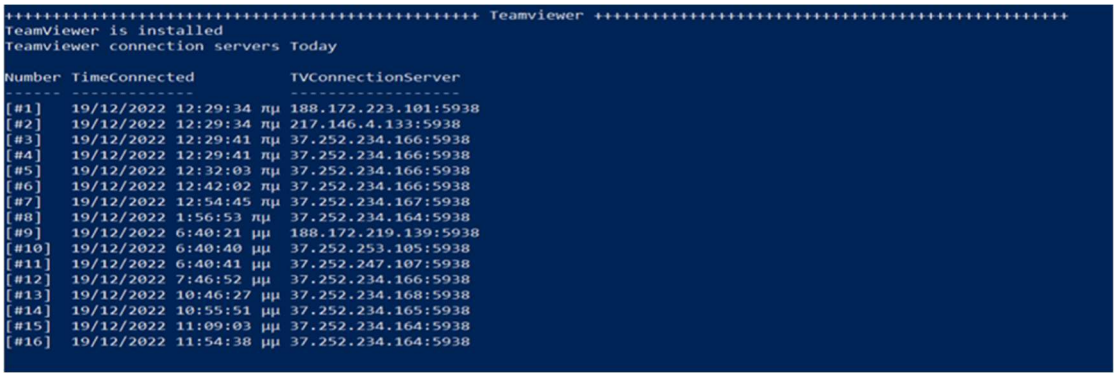
Σχήμα 25. Αποσυνδέσεις χρηστών με την εφαρμογή Windows RDP

Στο (Σχήμα 25), εμφανίζονται όλες οι αποσυνδέσεις που έχουν γίνει από χρήστες που συνδέθηκαν απομακρυσμένα στο τερματικό. Αυτή η πληροφορία, αντλείτε πάλι με την χρήση της Get-WinEvent με βάση το ID (24) στο event log path “Microsoft-Windows-TerminalServices-LocalSessionManager/Operational”. Τα δεδομένα που εξάγονται, παρουσιάζονται στην οθόνη του τερματικού και εκχωρούνται σε πίνακα για μελλοντική χρήστη στα επόμενα βήματα.



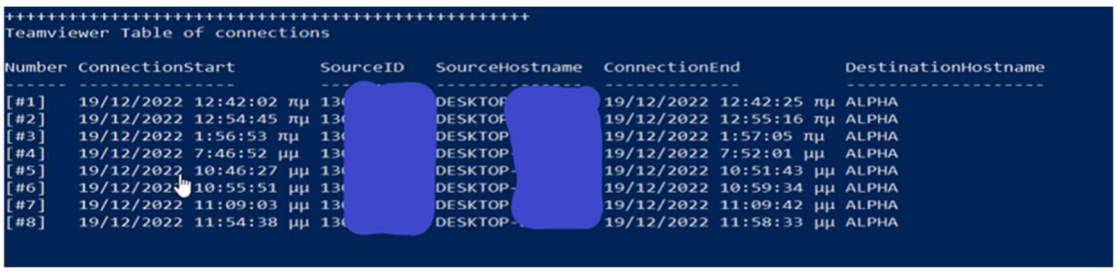
Σχήμα 26. Απόπειρες απομακρυσμένης σύνδεσης με το Remote Desktop Connection

Το παραπάνω (Σχήμα 26), παρουσιάζει πόσες προσπάθειες απομακρυσμένης σύνδεσης έγιναν στο τερματικό καθώς επίσης και ποιες ώρες έχουν πραγματοποιηθεί. Τα συγκεκριμένα δεδομένα εξάγονται με την χρήση της εντολής Get-EventLog για το ID (4776). Τα αποτελέσματα της εντολής εισάγονται σε πίνακα και παρουσιάζονται στην οθόνη του τερματικού.



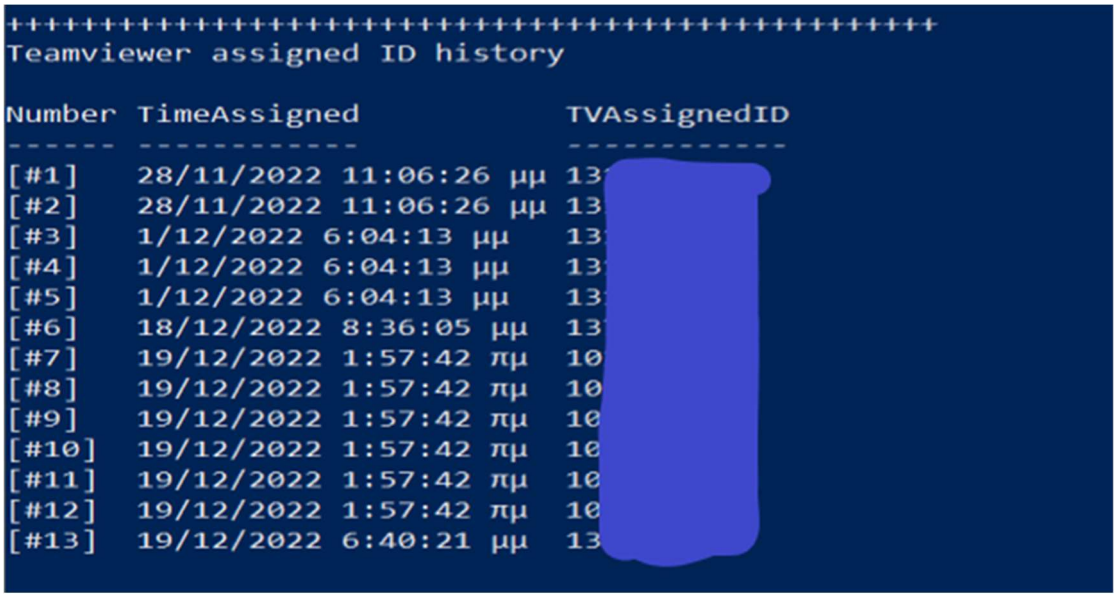
Σχήμα 27. Σύνδεση της εφαρμογής Teamviewer στους κεντρικούς server

Στο (Σχήμα 27), στο αρχείο που υπάρχει στον φάκελο “C:\Program Files\TeamViewer\TeamViewer15_Logfile.log” καταγράφονται δεδομένα στα οποία μπορούμε να αντλήσουμε αρκετές πληροφορίες. Μια από τις πληροφορίες είναι η σύνδεση που κάνει η εφαρμογή Teamviewer, με τον διαθέσιμο server για να γίνει η ανάθεση του Teamviewer ID στο τερματικό και αντίστοιχα να δηλωθεί η σύνδεση του τερματικού στο δίκτυο της Teamviewer. Προγραμματιστικά, εισάγουμε το .Log file σε μια μεταβλητή πίνακα και κάνοντας προσπέλαση ως αναγνώσιμο αρχείο, αναζητούμε την φράση “Connecting to endpoint”. Μόλις βρεθεί στην αναζήτηση η συγκεκριμένη φράση, ελέγχουμε την συγκεκριμένη εγγραφή και αναζητούμε την διεύθυνση IP που εμφανίζεται και την εκχωρούμε σε νέο πίνακα μαζί με την ημερομηνία της εγγραφής που βρίσκεται στην αρχή της γραμμής.



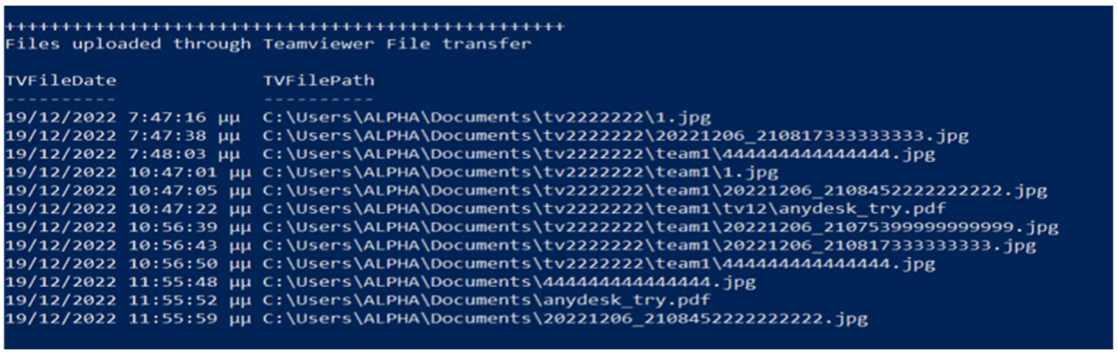
Σχήμα 28. Συνδέσεις της τελευταίας ημέρας στο Teamviewer

Στην εικόνα που παρουσιάζεται παραπάνω, αναφέρονται οι συνδέσεις που έχουν γίνει εντός της τελευταίας ημέρας. Οι συγκεκριμένες πληροφορίες αντλούνται από το αρχείο txt που βρίσκεται στο path “C:\Program Files\TeamViewer\Connections_incoming.txt”. Εισάγουμε το αρχείο σε μεταβλητή και από εκεί χωρίζουμε το txt αρχείο σε γραμμές με βάση τις συνδέσεις που έχουν γραφεί. Από εκεί χωρίζουμε την εκάστοτε γραμμή σε επιμέρους κομμάτια με την χρήση της function Split() και αναγράφουμε σε νέο πίνακα το κάθε στοιχείο που εμφανίζεται στο αρχείο txt.



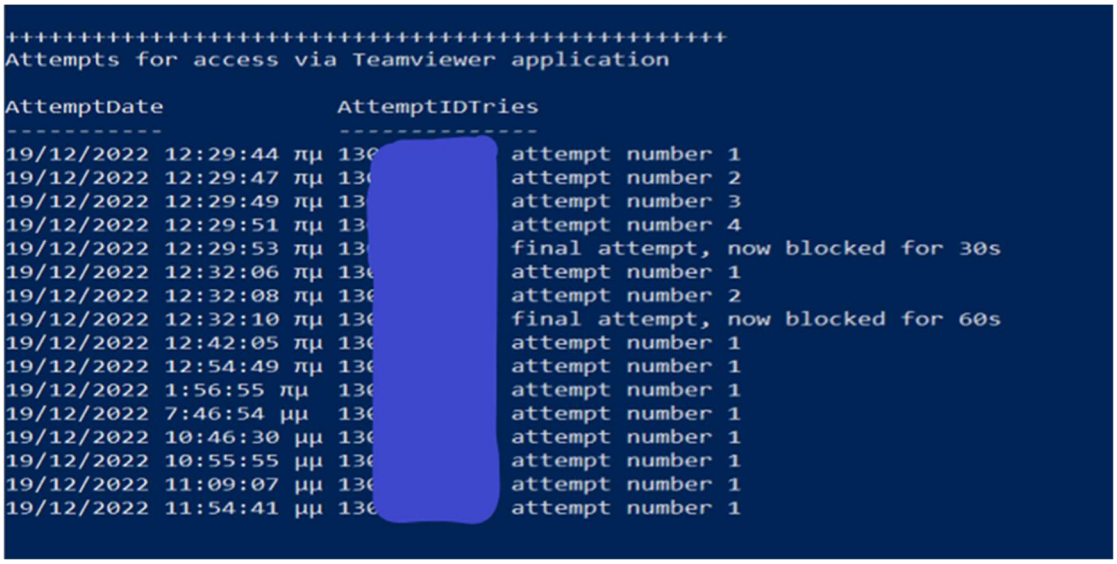
Σχήμα 29. Teamviewer IDs assigned

Στο παραπάνω (Σχήμα 29) εμφανίζονται ιστορικά όλα τα IDs που έχουν γίνει από τον server της Teamviewer assign στον client του τερματικού. Τα παραπάνω δεδομένα τα εξάγουμε από το αρχείο “C:\Program Files\TeamViewer\TeamViewer15_Logfile.log”. Έχουμε εισάγει το αρχείο σε προηγούμενο βήμα σε μεταβλητή και με την χρήση της foreach επανάληψης, ελέγχουμε κάθε γραμμή του αρχείο για να βρούμε την φράση “SenderID:”. Από εκεί κάνουμε εξαγωγή του συγκεκριμένου κομματιού της γραμμής με την function substring() και ελέγχουμε αντίστοιχα με την IF() αν η ημερομηνία της γραμμής είναι σημερινή. Από εκεί σε έναν νέο πίνακα εισάγουμε τα πεδία της ώρας/ημερομηνίας καθώς επίσης και το ID το οποίο ανιχνεύσαμε.



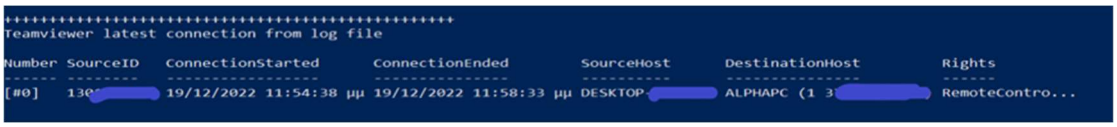
Σχήμα 30. Μεταφορά αρχείων μέσα από την εφαρμογή Teamviewer

Στο (Σχήμα 30), γίνεται έλεγχος εκ νέου του αρχείου με την foreach() “C:\Program Files\TeamViewer\TeamViewer15_Logfile.log” με σκοπό να βρεθεί φράση “Write file”. Εφόσον βρεθεί η φράση, ελέγχουμε με την IF αν η ημερομηνία της συγκεκριμένης εγγραφής είναι σημερινή και σε έναν νέο πίνακα, εισάγουμε την ημερομηνία και το path όπου τοποθετήθηκαν τα αρχεία που μεταφέρθηκαν.



Σχήμα 31. Προσπάθειες σύνδεσης στο τερματικό μέσω Teamviewer

Το (Σχήμα 31), εμφανίζει τι προσπάθειες που έγιναν προς το απομακρυσμένο τερματικό με σκοπό την σύνδεση σε αυτό. Εμφανίζει επίσης και το Teamviewer ID του χρήστη που προσπαθεί να συνδεθεί. Οι συγκεκριμένες πληροφορίες εμφανίζονται στο αρχείο “C:\Program Files\TeamViewer\TeamViewer15_Logfile.log” όπου στην μεταβλητή που έχουμε εισάγει το αρχείο, κάνουμε μια προσπέλαση με την function foreach() και αναζητούμε όσες γραμμές του αρχείο περιέχουν την φράση “AuthenticationBlocker::Allocate: allocate ok for DyngateID”. Σε μελέτη των log που έγινε, ο AuhtentificationBlocker αποτελεί worker της εφαρμογής που μπλοκάρει εισερχόμενες μη αυθεντικοποιημένες συνδέσεις. Από τις γραμμές που περιέχουν αυτή την φράση, ελέγχουμε με την If() αν οι προσπάθειες έχουν γίνει εντός ημέρας και σε έναν νέο πίνακα, εισάγουμε την ημερομηνία και το λεκτικό των προσπαθειών μαζί με την αντίστοιχη προσπάθεια που εμφανίζεται μέσα στο αρχείο.



Σχήμα 32. Τελευταία επιτυχημένη σύνδεση στο Teamviewer

Στο (Σχήμα 32), εμφανίζεται η τελευταία επιτυχημένη σύνδεση στο απομακρυσμένο τερματικό. Πρόκειται για μια παραλλαγή του πίνακα στο (Σχήμα 28). Οι βασικότερες διαφορές που υπάρχουν σε αυτές τις παραδοχές είναι ότι οι πληροφορίες που αντλούνται και παρουσιάζονται γίνονται από διαφορετικά αρχεία, κάτι που θα μπορούσε να θεωρηθεί και δικλίδα ασφαλείας σε περίπτωση που ένα από τα δύο αρχεία τροποποιηθεί από κακόβουλη προσπάθεια. Το παραπάνω (Σχήμα 32), αποτελείται από σύνδεση 5 διαφορετικών πινάκων. Οι πίνακες που συνδέονται περιέχουν τις διαφορετικές πληροφορίες αλλά ως υλοποίηση χρησιμοποιούν το ίδιο ακριβώς μοτίβο με την χρήση της foreach() function αναζητώντας διαφορετικό λεκτικό σε κάθε γραμμή. Συνεπώς, από τον κάθε πίνακα παίρνουμε τις παρακάτω πληροφορίες

a) $tableTVID → Γίνεται αναζήτηση των γραμμών με το λεκτικό “client hello received from” → Εξάγουμε σε έναν νέο πίνακα Το Teamviewer ID το οποίο δεχόμαστε επιτυχή σύνδεση καθώς και την ημερομηνία/ώρα η οποία αναγράφεται στην αρχή τις εκάστοτε εγγραφής.
b) $TVConnectionShut → Γίνεται αναζήτηση των γραμμών με λεκτικό “JitterBuffer was permanently shut!” → Στην συγκεκριμένη γραμμή εξάγουμε την ημερομηνία/ώρα όπου καταγράφηκε όταν έκλεισε οριστικά η απομακρυσμένη σύνδεση.
c) $tableTVhostnames → Γίνεται αναζήτηση των γραμμών με λεκτικό “ type=6 name=” → Από προσωπική επαφή με τα αρχεία καταγραφής της εφαρμογής Teamviewer, παρατηρήθηκε ότι όσες γραμμές εμφάνιζαν το παραπάνω λεκτικό ακολουθούνταν από το HostName του μηχανήματος που ήθελες να συνδεθεί στο απομακρυσμένο τερματικό.

d) $TVdestinationHost → Γίνεται αναζήτηση των γραμμών με λεκτικό " *). Our participant id is" → Από προσωπική επαφή με τα αρχεία καταγραφής της εφαρμογής Teamviewer, παρατηρήθηκε ότι μετά το παραπάνω λεκτικό ακολουθούσε το Teamviewer ID του απομακρυσμένοι τερματικού.
e) $tableTVrights → Γίνεται αναζήτηση των γραμμών με λεκτικό "ConnectionAccessControl» → Από προσωπική επαφή με τα αρχεία καταγραφή της εφαρμογής, παρατηρήθηκε ότι ακολουθούσαν με συγκεκριμένη μορφοποίηση και τρόπο γραφής τα Access rights του χρήστη που προσπαθούσε να συνδεθεί στο απομακρυσμένο τερματικό.

Αντλώντας την τελευταία εγγραφή από κάθε πίνακα από τα συγκεκριμένα πεδία, δημιουργούμε έναν νέο πίνακα ο οποίος εμφανίζει τις πληροφορίες που αναγράφονται στο (Σχήμα 32).

Σχήμα 33. Τελευταία επιτυχημένη σύνδεση με Anydesk

Το παραπάνω (Σχήμα 33), εμφανίζει την τελευταία επιτυχημένη σύνδεση στο απομακρυσμένο τερματικό με την εφαρμογή του Anydesk. Η συγκεκριμένη εγγραφή αποτελεί συνδυασμό 6 διαφορετικών πινάκων από πληροφορίες που αντλήθηκαν από αρχεία .trace δύο διαφορετικών τοποθεσιών "C:\Users*User*\AppData\Roaming\AnyDesk\ad.trace" και "C:\ProgramData\AnyDesk\ad_svc.trace"

Η μέθοδος εξαγωγής των δεδομένων από τα παραπάνω αρχεία και η καταχώρηση αυτών σε διαφορετικούς πίνακες γίνεται ακριβώς με τον ίδιο τρόπο. Για αρχή, εκχωρούμε και τα δύο παραπάνω αρχεία σε δύο διαφορετικές μεταβλητές και ελέγχουμε με την IF() αν τα αρχεία υπάρχουν και είναι προσπελάσιμα. Έπειτα με την χρήση της Foreach() function, γίνεται προσπέλαση του κάθε αρχείο και αντίστοιχα αναζήτηση συγκεκριμένων λεκτικών με σκοπό την αναζήτηση πληροφοριών στις γραμμές όπου εμφανίζονται τα λεκτικά που αναζητούμε.

Πιο αναλυτικά, οι πίνακες του οποίους εξάγουμε ως πρώτο στάδιο προτού γίνει η ένωση όλων αναφέρονται παρακάτω:

a) $TableADIncoming → Γίνεται αναζήτηση στο αρχείο ad.trace με το λεκτικό " Incoming session request" → Από την συγκεκριμένη γραμμή που εμφανίζεται το παραπάνω λεκτικό, εξάγουμε την ημερομηνία/ώρα όπου έγινε η καταγραφή της εισερχόμενης σύνδεσης και το Anydesk ID του χρήστη που θέλει να συνδεθεί στο απομακρυσμένο τερματικό.
b) $TableADIPAdd → Γίνεται αναζήτηση στο αρχείο ad_svc.trace με το λεκτικό "Logged in from" → Από τις γραμμές που θα εμφανίσει, αντλούμε την πληροφορία της διεύθυνσης IP του χρήστη που προσπαθεί να συνδεθεί στην απομακρυσμένη επιφάνεια εργασίας.
c) $TableADRights → Γίνεται αναζήτηση στο αρχείο ad.trace με το λεκτικό " Remote caps" → Από τις γραμμές που θα εμφανιστούν, εξάγουμε τα δικαιώματα που επιτρέπει το Anydesk και θα έχει ο χρήστης που θα συνδεθεί απομακρυσμένα μέσα από την εφαρμογή. Πρόκειται για δικαιώματα τα οποία δίνει η εφαρμογή ξεχωριστά από τον χρήστη που είναι ήδη συνδεδεμένος στο τερματικό και μπορεί είτε να περιέχει δικαιώματα γραφής, δικαιώματα administrator, δικαιώματα χρήσης ήχου και μικροφώνου, δικαιώματα αποσύνδεσης τοπικού χρήστη κ.ο.κ.
d) $TableADVersion → Γίνεται αναζήτηση στο αρχείο ad.trace με το λεκτικό "Remote version" → Εξάγουμε την πληροφορία για την έκδοση λογισμικού Anydesk, που χρησιμοποιεί ο χρήστης που θα συνδεθεί απομακρυσμένα.
e) $TableADSourceOS → Γίνεται αναζήτηση στο αρχείο ad.trace με το λεκτικό "Remote OS" → Από την συγκεκριμένη εγγραφή, εμφανίζεται το λειτουργικό σύστημα που χρησιμοποιεί ο χρήστης που συνδέεται απομακρυσμένα.
f) $TableADSessionEnd → Γίνεται αναζήτηση στο αρχείο ad.trace με το λεκτικό "Session stopped." → Εξάγουμε την ημερομηνία/ώρα που αναγράφεται στην αρχή της γραμμή καθώς θα χρησιμοποιηθεί για επόμενα βήματα.

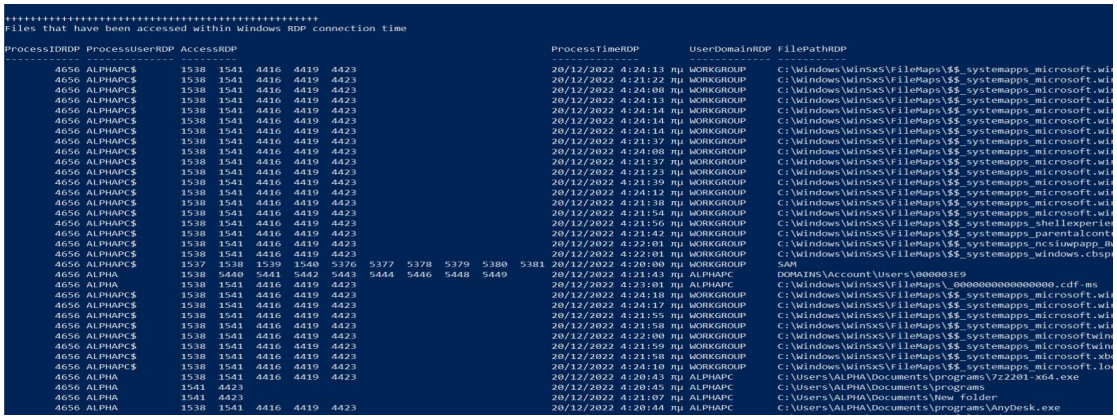
Μόλις έχουν γίνει εξαγωγή στα δεδομένα από τα παραπάνω ευρήματα σε πίνακες, χρησιμοποιούμε τον πίνακα $TableADIncoming με σκοπό να μετρήσουμε τις εγγραφές που έχουν

καταχωρηθεί στο σύνολο και να βγάλουμε ένα count το οποίο θα πρέπει να είναι ίδιο σε κάθε ένα από τους παραπάνω 6 πίνακες με σκοπό τα δεδομένα που θα συμπτύξουμε να αντικατοπτρίζουν τις σωστές εγγραφές. Δημιουργούμε έναν νέο πίνακα και με την χρήση της function For(), για κάθε i που θα είναι μικρότερο ή ίσο του ποσού των εγγραφών του πίνακα $TableADIncoming, στον νέο πίνακα θα αναγράφεται στις εκάστοτε στήλες η κάθε εγγραφή από τους 6 παραπάνω πίνακες. Μόλις ολοκληρωθεί η παραπάνω σύμπτυξη, γίνεται και παρουσίαση των δεδομένων όπως φαίνεται στο (Σχήμα 33).

Σχήμα 34. Προσπάθεια προσπέλασης αρχείων μέσω Anydesk

Στο (Σχήμα 34), αναφέρονται οι προσπάθειες που έγιναν για πρόσβαση σε φακέλους όπου ο απομακρυσμένος χρήστης δεν διαθέτει τα κατάλληλα δικαιώματα. Η εφαρμογή Anydesk, διαθέτει File Transfer System. Το συγκεκριμένο σύστημα μεταφοράς αρχείων μπορεί να λειτουργήσει χωρίς να εμφανίζεται οπτικά στο τερματικό οποιαδήποτε αλλαγή ή μεταφορά αρχείων γίνεται στο background. Αυτό μπορεί να χρησιμοποιηθεί για αρκετές κακόβουλες ενέργειες όπως τοποθέτηση worms ή ακόμη και υποκλοπή ευαίσθητων αρχείων χωρίς την γνώση και έγκριση του χρήστη. Δεδομένου των παραπάνω, πραγματοποιούμε έλεγχο μέσα από το αρχείο ad.trace αναζητώντας με την χρήση της foreach() σε κάθε γραμμή του αρχείου με το λεκτικό “app.dir_sentinel”. Οι γραμμές οι οποίες περιέχουν το προηγούμενο λεκτικό, αναφέρουν επακριβώς το path το οποίο έγινε προσπάθεια access όπως και την ημερομηνία/ώρα στην αρχή της γραμμής.

Με το (Σχήμα 34) ολοκληρώνεται το πρώτο μέρος από το powershell script, το οποίο ελέγχει ποιες εφαρμογές έχουν εγκατασταθεί και αντίστοιχα αντλούμε στοιχεία από τα log ή τα trace files καθώς και από τον event viewer για την περίπτωση του windows Remote Desktop Connection. Τα στοιχεία και οι πίνακες που έχουμε κρατήσει από το 1ο μέρος, θα μας βοηθήσουν στο να κάνουμε πιο συγκεκριμένα τα αποτελέσματα και να μπορέσουμε να αναγνωρίσουμε και να κάνουμε trace πότε, από ποιον και με ποια μέσα κατάφερε να κάνει infect ένα μηχάνημα απομακρυσμένα με την χρήση RDP πρωτοκόλλου.



Σχήμα 35. Αρχεία τα οποία έγιναν προσπέλαση

Ξεκινώντας το 2ο μέρος του script, αυτό που κάνουμε είναι να ελέγξουμε μέσα στον Event viewer των windows, και με την χρήση της function Get-WinEvent() ελέγχουμε για όσα events δημιουργήθηκα με ID (4656). Το ID (4656) πρόκειται για event των windows το οποίο αναφέρεται ως αίτημα του συστήματος για προσπέλαση αντικειμένου “A handle to an object was requested”. Συνεπώς, κρατάμε σε μια μεταβλητή όλες τις πληροφορίες που αντλήθηκαν από τα συγκεκριμένα events και δεδομένου του όγκου event που πιθανόν να υπάρχουν, ορίζουμε να πάρουμε τα events τα οποία έγιναν μέσα στο χρονικό περιθώριο σύνδεσης και αποσύνδεσης από την απομακρυσμένη επιφάνεια. Αυτό γίνεται διότι ορίζουμε κατά την Get-WinEvent() Starttime και

EndTime με βάση τις μεταβλητές χρόνου που έχουμε κρατήσει στους πίνακες των συνδέσεων. Από το συγκεκριμένο event αντλούμε τις πληροφορίες από ποιον χρήστη έγινε η προσπέλαση, τα access rights που έχει ο χρήστης πάνω στο συγκεκριμένο αρχείο την στιγμή την οποία έγιναν προσπέλαση σε ποιο Domain ανήκει ο χρήστης που έκανε την προσπέλαση καθώς και το path ή το αρχείο που έγινε προσπέλαση. Αυτά όλα τα δεδομένα, αποθηκεύονται σε μεταβλητή πίνακα και παρουσιάζονται αντίστοιχα στην οθόνη του τερματικού.

```
++++++++++++++++++++++++++++++++++++++++++++++++++
Deleted/Changed files/folders with Window process of deletion

DeletedTimeRDP         ProcessHostRDP  ProcessIDRDP LocalProcessUserRDP DeletedFilesPathRDP
--------------         --------------  ------------ -------------------- -------------------
20/12/2022 4:20:00 μμ DESKTOP-[redacted] alpha        ALPHAPC$             ALPHAPC
20/12/2022 4:21:01 μμ DESKTOP-[redacted] alpha        ALPHA                C:\Users\ALPHA\Documents\anydesk_try.pdf
20/12/2022 4:21:06 μμ DESKTOP-[redacted] alpha        ALPHA                C:\Users\ALPHA\Documents\New folder
20/12/2022 4:20:59 μμ DESKTOP-[redacted] alpha        ALPHA                C:\Users\ALPHA\Documents\TableOfProcessesStart.json
20/12/2022 4:23:58 μμ DESKTOP-[redacted] alpha        ALPHA                C:\Users\ALPHA\Documents\ViberDownloads
20/12/2022 4:20:00 μμ DESKTOP-[redacted] alpha        ALPHAPC$             DOMAINS\Account\Users\000003E9
20/12/2022 4:20:00 μμ DESKTOP-[redacted] alpha        ALPHAPC$             SAM
```

Σχήμα 36. Αρχεία τα οποία τροποποιήθηκαν/διαγράφηκαν

Συνεχίζοντας τους ελέγχους μέσα από το Event Viewer, προχωράμε στο (Σχήμα 36) στο οποίο ανιχνεύουμε αρχεία τα οποία έχουν γίνει διαγραφή/τροποποίηση. Για λόγους βελτιστοποίησης της ταχύτητας του script, από προσωπικούς ελέγχους και εμπειρία στα events του Event viewer, παρατηρήθηκε ότι από τα δεδομένα του πίνακα στο (Σχήμα 35) όσα αρχεία είχαν τροποποιηθεί/διαγραφεί, διέθεταν συγκεκριμένο Access Right με ID (1537). Οπότε, για καλύτερη ταχύτητα του script, από το να ελέγξουμε εκ νέου τα event logs, τρέχουμε την στήλη του προηγούμενου πίνακα με την λειτουργία foreach() και με τον έλεγχο της IF() ανιχνεύουμε ποιες εγγραφές διαθέτουν Access right ίσο με το (1537). Έτσι λοιπόν, σε μια νέα μεταβλητή πίνακα, καταχωρούμε την ημερομηνία, το hostname του υπολογιστή του χρήστη που συνδέθηκε απομακρυσμένα, τον local χρήστη που είναι συνδεδεμένος την δεδομένη στιγμή (στην περίπτωση του Remote desktop connection, πρόκειται για τον χρήστη που συνδέθηκε απομακρυσμένα), το domain που ανήκει ο χρήστης που έχει συνδεθεί και τα αρχεία μαζί με το path τους που έγιναν τροποποίηση/διαγραφή.

Στις περιπτώσεις του Teamviewer και του Anydesk που διαθέτουν δικό τους file transfer system, έχει το μειονέκτημα ότι σε περίπτωση που τα αρχεία trace ή log διαγραφούν ή τροποποιηθούν δεν γίνεται να αντληθεί καμία επιπλέον πληροφορία και συνεπώς δεν έχουμε ξεκάθαρη εικόνα για το ποια αρχεία έχουν πειραχτεί. Ο παραπάνω τρόπος ανίχνευσης αρχείων μέσα από τα Event logs που τροποποιήθηκαν/διαγράφηκαν, θεωρείτε από προσωπική εμπειρία ο καλύτερος διότι αντλούμε δεδομένα τα οποία μπορεί να μην έχουν καταγραφεί σε οποιοδήποτε log file ή trace file. Στο συγκεκριμένο script, εμφανίζονται και οι εγγραφές από τα log/trace files των εφαρμογών για τις περιπτώσεις όπου έχουν διαγραφεί τα αρχεία των events ούτος ώστε να έχουμε έστω μια μικρή πληροφορία για τα αρχεία που έχουν τροποποιηθεί.

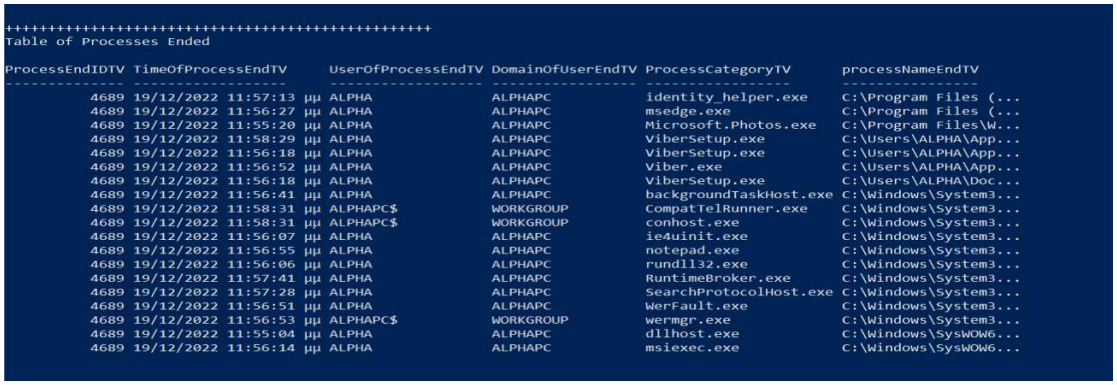
```
++++++++++++++++++++++++++++++++++++++++++++++++++
Table of Processes started

ProcessStartIDTV TimeOfProcessTV          UserOfProcessTV DomainOfUserTV ProcessCategoryTV      ProcessNameTV
---------------- ----------------         --------------- -------------- ------------------      -------------
            4688 19/12/2022 11:57:01 μμ ALPHA           ALPHAPC        msedge.exe              C:\Program Files (x86)...
            4688 19/12/2022 11:57:03 μμ ALPHA           ALPHAPC        msedge.exe              C:\Program Files (x86)...
            4688 19/12/2022 11:54:38 μμ ALPHAPC$        WORKGROUP      TeamViewer_Service.exe C:\Program Files\TeamV...
            4688 19/12/2022 11:55:22 μμ ALPHAPC$        WORKGROUP      svchost.exe             C:\Program Files\Windo...
            4688 19/12/2022 11:57:08 μμ ALPHA           ALPHAPC        ViberSetup.exe          C:\Users\ALPHA\AppData...
            4688 19/12/2022 11:55:00 μμ ALPHA           ALPHAPC        ViberSetup.exe          C:\Users\ALPHA\AppData...
            4688 19/12/2022 11:56:48 μμ ALPHA           ALPHAPC        Viber.exe               C:\Users\ALPHA\AppData...
            4688 19/12/2022 11:54:59 μμ ALPHA           ALPHAPC        explorer.exe            C:\Users\ALPHA\Documen...
            4688 19/12/2022 11:54:46 μμ LOCAL SERVICE   NT AUTHORITY   svchost.exe             C:\Windows\System32\au...
            4688 19/12/2022 11:56:59 μμ ALPHAPC$        WORKGROUP      svchost.exe             C:\Windows\System32\ba...
            4688 19/12/2022 11:58:31 μμ ALPHAPC$        WORKGROUP      svchost.exe             C:\Windows\System32\Co...
            4688 19/12/2022 11:55:37 μμ ALPHAPC$        WORKGROUP      CompatTelRunner.exe     C:\Windows\System32\co...
            4688 19/12/2022 11:56:07 μμ ALPHAPC$        WORKGROUP      msiexec.exe             C:\Windows\System32\ie...
            4688 19/12/2022 11:55:10 μμ ALPHAPC$        WORKGROUP      services.exe            C:\Windows\System32\ms...
            4688 19/12/2022 11:56:42 μμ ALPHA           ALPHAPC        explorer.exe            C:\Windows\System32\no...
            4688 19/12/2022 11:56:06 μμ ALPHA           ALPHAPC        ie4uinit.exe            C:\Windows\System32\ru...
            4688 19/12/2022 11:57:00 μμ ALPHAPC$        WORKGROUP      svchost.exe             C:\Windows\System32\Ru...
            4688 19/12/2022 11:55:44 μμ ALPHAPC$        WORKGROUP      SearchIndexer.exe       C:\Windows\System32\Se...
            4688 19/12/2022 11:54:59 μμ ALPHAPC$        WORKGROUP      svchost.exe             C:\Windows\System32\sm...
            4688 19/12/2022 11:55:11 μμ ALPHAPC$        WORKGROUP      services.exe            C:\Windows\System32\sv...
            4688 19/12/2022 11:56:48 μμ ALPHAPC$        WORKGROUP      svchost.exe             C:\Windows\System32\We...
            4688 19/12/2022 11:56:51 μμ ALPHAPC$        WORKGROUP      svchost.exe             C:\Windows\System32\We...
            4688 19/12/2022 11:54:58 μμ ALPHAPC$        WORKGROUP      svchost.exe             C:\Windows\SysWOW64\dl...
            4688 19/12/2022 11:55:13 μμ ALPHAPC$        WORKGROUP      msiexec.exe             C:\Windows\SysWOW64\ms...
```

Σχήμα 37. Διεργασίες οι οποίες άρχισαν κατά το Remote connection

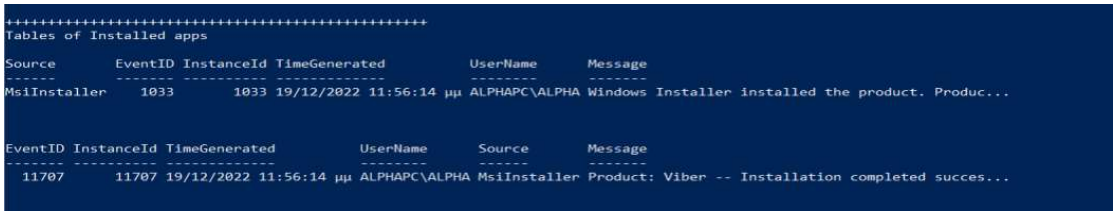
Σε συνέχεια των ελέγχων του Event viewer, ανιχνεύουμε ποιες διεργασίες έχουν ξεκινήσει κατά το διάστημα που υπήρχε απομακρυσμένη σύνδεση στον υπολογιστή. Αυτό επιτυγχάνεται

με την χρήση της function Foreach() όπου ανιχνεύουμε τα events που δημιουργήθηκαν με ID (4688) χρησιμοποιώντας ως starttime και endtime τα χρονικά όρια από την τελευταία απομακρυσμένη σύνδεση. Από το συγκεκριμένο ID, εξάγουμε σε έναν νέο πίνακα ο οποίος αναγράφει το ID ελέγχουμε, το timestamp του ID, τον χρήστη με τον οποίο ξεκίνησε η εφαρμογή, το Domain του χρήστη που ξεκίνησε η εφαρμογή, την κατηγορία που υπάγεται η συγκεκριμένη εφαρμογή καθώς και το path του αντίστοιχου process. Με την χρήση της Write-host, εμφανίζουμε τα δεδομένα στην οθόνη.



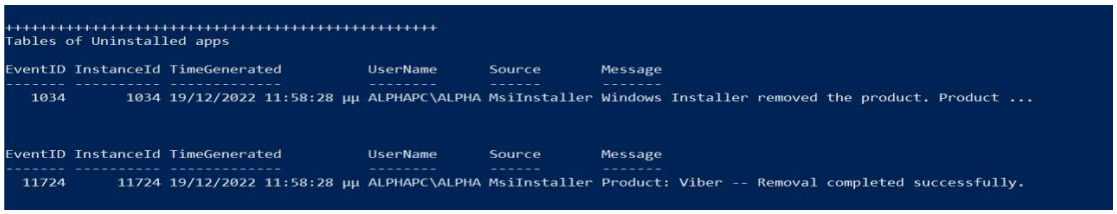
Σχήμα 38. Διεργασίες που έκλεισαν κατά το Remote connection

Στο (Σχήμα 38), χρησιμοποιούμε ακριβώς την ίδια διαδικασία που έγινε για το (Σχήμα 37) αλλά εξάγουμε όσα events έχουν ID (4689). Από τον συγκεκριμένο πίνακα μπορούμε να αντλήσουμε πληροφορίες όπως το timestamp της διαδικασίας που έκλεισε, από ποιον χρήστη έκλεισε η διαδικασία, το Domain του χρήστη που έκλεισε την διαδικασία, την κατηγορία της διαδικασίας που τερματίστηκε καθώς και το path από την διαδικασία. Αυτά τα δεδομένα εκχωρούνται σε μια μεταβλητή πίνακα και παρουσιάζονται στην οθόνη του τερματικού.



Σχήμα 39. Εφαρμογές οι οποίες εγκαταστάθηκαν κατά την διάρκεια του remote connection

Όπως φαίνεται στο παραπάνω (Σχήμα 39), με την βοήθεια της function Get-EventLog() στην κατηγορία των Application logs του Event viewer, αναζητούμε με το ID (1033) και το ID (11707) για εφαρμογές που έγιναν εγκατάσταση εντός των χρονικών ορίων της απομακρυσμένης σύνδεσης. Τα σημαντικότερα δεδομένα που αντλούμε από αυτά τα events είναι η ώρα που έγιναν εγκατάσταση, με ποιου χρήστη τα δικαιώματα έγιναν εγκατάσταση και στο αντίστοιχο μήνυμα του event, εμφανίζονται πληροφορίες όπως η έκδοση της εφαρμογής, το όνομα της εφαρμογής κ.α. Τα δεδομένα αυτά, καταχωρούνται σε δύο διαφορετικούς πίνακες και παρουσιάζονται στην οθόνη του υπολογιστή.



Σχήμα 40. Εφαρμογές που απεγκαταστήθηκαν κατά την διάρκεια του remote connection

Όπως και στο παραπάνω (Σχήμα 40), έτσι και στο (Σχήμα 39) με την χρήση της function Get-EventLog() στην κατηγορία των Application logs του Event viewer, αναζητούμε με το ID (1034) και το ID (11724) για εφαρμογές που έγιναν απεγκατάσταση εντός των χρονικών ορίων της απομακρυσμένης σύνδεσης. Τα δεδομένα που αντλούμε από τα συγκεκριμένα events είναι η ώρα που έγιναν απεγκατάσταση οι εφαρμογές, με ποιου χρήστη τα δικαιώματα έγιναν απεγκατάσταση και στο αντίστοιχο μήνυμα του event, εμφανίζονται πληροφορίες όπως η έκδοση της εφαρμογής, το όνομα της εφαρμογής κ.α. Τα δεδομένα αυτά, καταχωρούνται σε δύο διαφορετικούς πίνακες και παρουσιάζονται στην οθόνη του υπολογιστή.

Με τις παραπάνω κατηγορίες/τρόπους εξαγωγής των δεδομένων ολοκληρώνεται η άντληση οποιασδήποτε πληροφορίας που μπορούμε να βρεθεί μέσα από τα log file, τα trace files και τα windows events. Να σημειωθεί επίσης, ότι για όλους τους παραπάνω πίνακες, αφού γίνει η παρουσίαση των δεδομένων στην οθόνη του τερματικού, χρησιμοποιούνται οι function ConvertTo-Json() και Out-File() οι οποίες κάνουν μετατροπή των πινάκων σε συγκεκριμένη μορφή και εξάγουν τα παραπάνω δεδομένα σε αρχείο τύπου Json (JavaScript Object Notation).


```
[
    {
        "DomainOfUser":  "ALPHAPC",
        "ProcessName":  "C:\\Program Files (x86)\\Microsoft\\Edge\\Application\\107.0.1418.62\\identity_helper.exe",
        "UserOfProcess":  "ALPHA",
        "ProcessStartID":  4688,
        "TimeOfProcess":  "\/Date(1671372509177)\/",
        "ProcessCategory":  "msedge.exe"
    },
    {
        "DomainOfUser":  "ALPHAPC",
        "ProcessName":  "C:\\Program Files (x86)\\Microsoft\\Edge\\Application\\msedge.exe",
        "UserOfProcess":  "ALPHA",
        "ProcessStartID":  4688,
        "TimeOfProcess":  "\/Date(1671372508027)\/",
        "ProcessCategory":  "msedge.exe"
    },
    {
        "DomainOfUser":  "ALPHAPC",
        "ProcessName":  "C:\\Users\\ALPHA\\AppData\\Local\\Package Cache\\{e9fe7c4d-6a26-48aa-82a7-4a314a54b30e}\\ViberSetup.exe",
        "UserOfProcess":  "ALPHA",
        "ProcessStartID":  4688,
        "TimeOfProcess":  "\/Date(1671372552162)\/",
        "ProcessCategory":  "explorer.exe"
    },
    {
        "DomainOfUser":  "ALPHAPC",
        "ProcessName":  "C:\\Users\\ALPHA\\AppData\\Local\\Temp\\{240E8B24-B353-463C-959E-FF04B55933F2}\\.cr\\ViberSetup.exe",
        "UserOfProcess":  "ALPHA",
        "ProcessStartID":  4688,
        "TimeOfProcess":  "\/Date(1671372492560)\/",
        "ProcessCategory":  "ViberSetup.exe"
    },
    {
        "DomainOfUser":  "ALPHAPC",
        "ProcessName":  "C:\\Users\\ALPHA\\AppData\\Local\\Viber\\Viber.exe",
        "UserOfProcess":  "ALPHA",
        "ProcessStartID":  4688,
        "TimeOfProcess":  "\/Date(1671372535824)\/",
        "ProcessCategory":  "ViberSetup.exe"
    },
```


Σχήμα 41. Αρχείο τύπου Json για τις διεργασίες που εκκινήθησαν


```
[
    {
        "ProcessTime":  "\/Date(1671372511707)\/",
        "FilePath":  "\\Device\\HarddiskVolume3\\Windows\\System32\\lsass.exe",
        "Access":  "4484  4490  4492",
        "Accessdel1":  "4484  4490  4492",
        "UserDomain":  "ALPHAPC",
        "ProcessUser":  "ALPHA",
        "Accessdel":  "4484",
        "ProcessID":  4656
    },
    {
        "ProcessTime":  "\/Date(1671372508342)\/",
        "FilePath":  "ALPHAPC",
        "Access":  "1538  5392  5394  5399  5400  5401",
        "Accessdel1":  "1538  5392  5394  5399  5400  5401",
        "UserDomain":  "ALPHAPC",
        "ProcessUser":  "ALPHA",
        "Accessdel":  "1538",
        "ProcessID":  4656
    },
    {
        "ProcessTime":  "\/Date(1671372488737)\/",
        "FilePath":  "C:\\$Recycle.Bin\\S-1-5-21-3161196374-1550691159-2676119750-1001\\$RNTI2CE.jpg",
        "Access":  "1538  1539  4423",
        "Accessdel1":  "1538  1539  4423",
        "UserDomain":  "ALPHAPC",
        "ProcessUser":  "ALPHA",
        "Accessdel":  "1538",
        "ProcessID":  4656
    },
    {
        "ProcessTime":  "\/Date(1671372487961)\/",
        "FilePath":  "C:\\Users\\ALPHA\\Documents",
        "Access":  "1538  4423",
        "Accessdel1":  "1538  4423",
        "UserDomain":  "ALPHAPC",
        "ProcessUser":  "ALPHA",
        "Accessdel":  "1538",
        "ProcessID":  4656
    },
```


Σχήμα 42. Αρχείο τύπου Json για τα αρχεία που έγινε προσπέλαση

Σχήμα 43. Αρχείο τύπου Json για τις εφαρμογές που έγιναν απεγκατάσταση

Τα συγκεκριμένα αρχεία περιέχουν όλες τις πληροφορίες από την άντληση δεδομένων με κωδικοποίηση αρχείου json, το οποίο σε μετέπειτα χρόνο μπορεί είτε όπως φαίνεται στα παραπάνω (Σχήμα 41, Σχήμα 42, Σχήμα 43) να αναγνωστεί από τον χρήστη/διαχειριστή για ανάλυση συμβάντος, είτε να φορτωθεί σε διαφορετικό script/εφαρμογή και να γίνει πιο συγκεκριμένη ανάλυση και εξαγωγή δεδομένων. Αυτό αποτελεί μια πρόταση για σύνδεση του script, που δημιουργήθηκε στην εκπόνηση αυτής της διατριβής, με άλλες εφαρμογές στις οποίες θα αναφερθούμε αναλυτικά στην επόμενη ενότητα.

9. Προσθήκη νέων λογισμικών και σύνδεση με άλλες εφαρμογές

Με βάση όσα αναφέρθηκαν στις προηγούμενες ενότητες, για να γίνει ένταξη νέου λογισμικού στο script, θα πρέπει να ελεγχθεί αν κατά την εγκατάσταση ή την λειτουργία αυτού δημιουργούνται αρχεία τα οποία παρέχουν events και καταγραφές για συνδέσεις ή ενέργειες που έγιναν κατά την σύνδεση. Από εκεί και πέρα, το script παρέχει ήδη το δεύτερο μέρος αναφορικά με τον έλεγχο των διεργασιών, αλλαγών σε αρχεία και φακέλους, εγκαταστάσεις και απεγκαταστάσεις. Συνεπώς, θα πρέπει να γίνει η αντίστοιχη μελέτη πάνω στην εφαρμογή, να συνταχθεί το πρώτο μέρος του κώδικα και να συμπεριληφθεί σε ξεχωριστή ενότητα μέσα στο powershell script.

Σε τεχνικούς όρους, αν θεωρήσουμε ότι το νέο λογισμικό που θέλουμε να εισάγουμε περιέχει log files ή δημιουργεί ένα είδος log file το οποίο καταχωρεί λειτουργίες για τις διεργασίες που τρέχουν κατά την χρήση της εφαρμογής τότε σε μια νέα μεταβλητή, θα εκχωρήσουμε το αρχείο από το path που δημιουργείται. Με την χρήση της function IF() θα αναγνωρίσουμε αν το αρχείο υπάρχει και περιέχει δεδομένα. Από εκεί, θα ελέγχουμε με την μέθοδο Foreach() αν υπάρχουν σε γραμμές αναφορές όπως π.χ. “Session Started”, “Connection established” κ.ο.κ με σκοπό να αντλήσουμε πληροφορίες όπως το timestamp της σύνδεσης, πληροφορίες για το ποιος χρήστης συνδέθηκε και πιο συγκεκριμένα αν αναφέρεται κάποια IP address, machine hostname, username και επίσης κύριο δεδομένο το πότε έγινε η αποσύνδεση από το απομακρυσμένο σύστημα. Επιπρόσθετα, θα μπορούσαμε να εξάγουμε και πληροφορίες για το ποια δικαιώματα δίνονται από την εφαρμογή στο χρήστη για τις λειτουργίες της απομακρυσμένης επιφάνειας. Αυτά τα δεδομένα, θα καταχωρηθούν σε έναν πίνακα, τον οποίο θα μπορούσαμε να εξάγουμε και σαν αρχείο Json.

Έχοντας τα παραπάνω δεδομένα, θα προχωρούσαμε στο 2ο μέρος του script όποτε θα ανατρέχαμε τον πίνακα της με τα στοιχεία που έχουμε αποθηκεύσει από την εφαρμογή και χρησιμοποιώντας το timestamp του Start time και του End time, θα καλούσαμε την function Get-EventLog() με συγκεκριμένα όρια με σκοπό να αντλήσουμε τα events που δημιουργήθηκαν εντός των συγκεκριμένων ορίων απομακρυσμένης σύνδεσης. Θα ελέγχαμε το ID (4656) για να ανιχνεύσουμε ποια αρχεία έγιναν προσπέλαση και τροποποιήθηκαν, με το ID (4663) θα ελέγχαμε ποια αρχεία έχουν γίνει αναγνωστεί, με τα ID (4688) και (4689) θα ελέγχαμε ποιες εφαρμογές εκκινήθησαν και ποιες τερματίστηκαν αντίστοιχα και τέλος με τα ID (1033),(11707) και (1034),(11724) θα ελέγξουμε ποιες εφαρμογές εγκαταστάθηκαν και ποιες απεγκαταστάθηκαν. Με τα παραπάνω δεδομένα, θα έχουμε μια ολοκληρωμένη εικόνα του τι συνέβη κατά την διάρκεια της απομακρυσμένης σύνδεσης και αντίστοιχα τα δεδομένα θα τα εξάγουμε σε Json files, με σκοπό την καλύτερη ανάλυσή τους είτε από χρήστη είτε από κάποια 3η εφαρμογή.

Το συγκεκριμένο powershell script, θα μπορούσε φυσικά να συνδεθεί με εφαρμογές όπως για παράδειγμα το log2timeline Plaso[4]. Η εφαρμογή log2timeline Plaso, δημιουργεί ένα πιο συγκεκριμένο εύρος event που θα μπορούσε να χρησιμοποιηθεί για την άντληση δεδομένων στο powershell script. Συνεπώς το Json script, θα μπορούσε να δίνει τις επιλογές των event ID που έχουν δημιουργηθεί κατά την απομακρυσμένη σύνδεση, το log2timeline θα πραγματοποιεί τον targeted έλεγχο και θα κάνει export τα αποτελέσματα. Τα δεδομένα που έχουν γίνει export από το log2timeline Plaso, θα διαβάζονται από το powershell script και θα γίνονται present κατά το runtime του script και τέλος export στο αντίστοιχο Json export που περιέχει το script.

Σε πιο τεχνικούς όρος, για να μπορέσουμε να χρησιμοποιήσουμε το log2timeline, θα πρέπει αρχικά να έχουμε φτιάξει ένα image του υπάρχον δίσκου του μηχανήματος που θέλουμε να ανιχνεύσουμε και να το εξάγουμε σε έναν δίσκο ή σημείο σε διαφορετικό δίσκο. Τη ενέργεια αυτή την κάνουμε διότι είναι πιο ασφαλής και θα έχουμε καλύτερα αποτελέσματα σε ένα infected machine από άποψης του ότι μπορεί να μην επιτραπούν οι παρακάτω εντολές λόγω κακόβουλου λογισμικού. Αυτό μπορεί να γίνει με την χρήση του Disk2vhd που προτείνεται από την Microsoft. Στα εκτελέσιμα που θα κατεβούν, ανοίγουμε το αντίστοιχο .exe αρχείο με βάση την έκδοση των windows που διαθέτουμε και διαλέγουμε την επιλογή VHDX (τύπος δίσκου που μπορεί να αναγνωριστεί από το log2timeline) και επιλέγουμε Create. Μόλις δημιουργηθεί το αρχείο VHDX. Αφού δημιουργηθεί το αρχείο, με την χρήση του script θα μπορούμε να ανιχνεύσουμε ποιες

[4]https://github.com/log2timeline/plaso

εφαρμογές έχουν εγκατασταθεί με τους σχετικούς ελέγχουν IF() στα αρχεία εγκατάστασης και στις διαδρομές αυτών.

Έπειτα, αφού έχουμε δημιουργήσει τους αντίστοιχους πίνακες-μεταβλητές για τα χρονικά περιθώρια σύνδεσης-αποσύνδεσης και έχουμε δημιουργήσει τα Json files, μπορούμε να μετακινηθούμε σε ένα 2ο μηχάνημα το οποίο μπορούμε να χρησιμοποιήσουμε για forensic analysis του VHDX. Θα ξεκινούσαμε εκ νέου το PowerShell script όπου θα χρησιμοποιούμε τις εντολές ConvertFrom-Json(), θα διαβάζαμε τα αρχεία Json που είχαμε κρατήσει μαζί με τον VHDX δίσκο για να διαβάσουμε τις ώρες σύνδεσης-αποσύνδεσης και έπειτα θα καλούσαμε την log2timeline Plaso.

Ως προαπαιτούμενο, είναι να έχει γίνει η εγκατάσταση της Python, μέσα από το windows store, να έχουμε εγκαταστήσει τα plaso-tools έτσι ώστε να μπορέσει να αναγνωρίσει τις παρακάτω εντολές. Η εντολή που θα δημιουργούσε το .dump file από όλο τον VHDX δίσκο θα ήταν “log2timeline.py forensics.dump win10_diskfile.vhdx”. Στο επόμενο βήμα της εντολή θα επιλέγαμε όλα τα partitions και μετά θα επιλέγαμε όλα τα Volume Shadows (VSS). Θα περιμέναμε έως ότου ολοκληρώσει η ανάλυση και έχουμε διαθέσιμο το .dump file. Η PowerShell εξ’ ορισμού αναμένει την ολοκλήρωση της προηγούμενης εντολής πριν προχωρήσει στην επόμενη.

Έπειτα, μόλις ολοκληρωθεί η δημιουργία του dump file και με βάση τις οδηγίες της log2timeline Plaso, θα χρησιμοποιούσαμε την παρακάτω εντολή σε συνδυασμό με τα πεδία των πινάκων που έχουμε καταχωρήσει στο PowerShell script μας για τις ώρες εισόδου-εξόδου από την απομακρυσμένη σύνδεση. Έτσι, η εντολή στο script θα καταγραφόταν ως εξής: «psort.py -z EET -o Json -w timeline.json forensics.dump “date > $application_table[-1].starttime AND date < $application_table[-1].endtime». Από εκεί και πέρα θα μπορούσαμε είτε να φορτώσουμε τα δεδομένα του Json με την εντολή ConvertFrom-Json() στο PowerShell script μας και είτε να τα παρουσιάσουμε με την μορφή πίνακα είτε να προχωρήσουμε σε ελέγχους πιο συγκεκριμένους, όπως να αναγνωρίσουμε από τα δεδομένα του Json file.

Επιπλέον έλεγχοι που θα μπορούσαμε να κάνουμε είναι είτε να δούμε ποια αρχεία της registry έχουν τροποποιηθεί, να εξάγουμε συγκεκριμένα δεδομένα για εφαρμογές, να ελέγξουμε συγκεκριμένα προγράμματα που μας χρειάζονται κ.α. Το παραπάνω αποτελεί μια ιδέα εξέλιξης-σύνδεσης του PowersShell script που έχουμε δημιουργήσει.

Επιπλέον, θα μπορούσαμε να κάνουμε σύνδεση του PowerShell Script με το Case Ontology. Η Cyber-investigation Analysis Standard Expression (CASE) είναι μια κοινότητα η οποία συμπεριλαμβάνει contributors από όλο κόσμο που τοποθετούν δεδομένα από forensic analysis. Θα μπορούσαμε μέσα από το PowerShell Script μας, τα Json αρχεία που εξάγουμε να τα τοποθετούμε την κοινότητα Case. Επιπρόσθετα θα μπορούσαμε να δεχόμαστε αρχεία Json από το CASE και να τα εισάγουμε μέσα στο Script. Από εκεί και πέρα, χρησιμοποιώντας συγκεκριμένες συνθήκες με την χρήση της IF() να ελέγχουμε αν τα δεδομένα που έχουμε εξάγει στην ανάλυσή μας συνάδουν με αντίστοιχα στοιχεία των αρχείων που θα έχουμε δεχτεί, ανάλογα την κατηγορία ανάλυσης-προβλήματος που θέλουμε να ελέγξουμε.

Συμπεράσματα

Στην συγκεκριμένη μεταπτυχιακή διατριβή έγινε ανάλυση των προβλημάτων ασφάλειας της απομακρυσμένης σύνδεσης. Δεδομένου του ότι μετά από την πανδημία COVID-19 δημιουργήθηκαν οι ανάγκες απομακρυσμένης σύνδεσης των χρηστών στις εταιρίες για την συνέχεια της λειτουργικότητας, αυτό «άνοιξε» τις πόρτες σε αρκετούς επιτήδειους με σκοπό το κέρδος. Εκμεταλλευόμενοι τις υπάρχουσες «τρύπες» και ελλείψεις στην ασφάλεια δικτύων και εφαρμογών, οι hackers αποσκοπούν στο να επιτεθούν με την χρήση διάφορων μέσων στην υποδομή πληροφοριών μιας εταιρίας. Απώτερος σκοπό, όπως έχει αναλυθεί και στην διατριβή, είναι το κέρδος. Αυτό μπορεί να μεταφράζεται είτε σε ευαίσθητες πληροφορίες, είτε σε κρυπτονομίσματα, είτε σε χρηματικά ποσά.

Στην ανάλυση που έγινε, αναφέρουμε ποια προβλήματα αντιμετωπίζουν οι εταιρίες και πως μπορεί κάποιος εισέλθει μέσω της απομακρυσμένης σύνδεσης στα συστήματα μιας εταιρίας. Με το human-operated-ransomware οι επιτήδειοι προσπαθούν να αποκτήσουν πρόσβαση διαχειριστή μέσα σε έναν οργανισμό και από εκεί να προχωρήσουν στις κακόβουλες ενέργειες κατά της εταιρίας. Αυτό όπως αναφέρθηκε εκτενέστερα μπορεί να αποτραπεί αλλά όπως είδαμε και στις αναλύσεις δεν μπορεί να αποφευχθεί.

Στις αναλύσεις και τις αναφορές που έγιναν, αναγνωρίζουμε ότι κανένα λογισμικό ή πρωτόκολλο δεν μπορεί να μας προστατέψει στο 100% παρά μόνο ο συνδυασμός λογισμικών για την προστασία δικτύων, εφαρμογών και χρηστών από σχετικές επιθέσεις είτε ransomware, είτε phishing κ.ο.κ.

Στην συνέχεια έγινε ανάλυση του πρακτικού κομματιού στο οποίο ανιχνεύουμε συγκεκριμένα τις εφαρμογές Teamviewer, Anydesk και Windows Remote Desktop πότε έγινε σύνδεση, από ποιον χρήστη έγινε σύνδεση και τι ενέργειες ακολουθήθηκαν στο σύνολο της σύνδεσης. Τα αποτελέσματα αυτού του PowerShell script που δημιουργήθηκε, εξάγει τα αποτελέσματα σε αρχεία τύπου JSON τα οποία όπως αναφέραμε και μπορούν να συνδεθούν με άλλες εφαρμογές και να διαμοιραστούν σε κοινότητα με σκοπό την εύρεση της πηγής των κακόβουλων ενεργειών.

Από τα συμπεράσματα που καταγράψαμε στο σύνολο αυτής της διατριβής, μπορούμε να αναφέρουμε ότι δεν είναι εφικτό πάντα να γίνει το αντίστοιχο trace στο source αυτών των ενεργειών, δεδομένου του ότι αρκετές πληροφορίες και στοιχεία μπορούν να κρυπτογραφηθούν και να μην καταστούν εμφανή προς ανάγνωση. Όπως και εμείς σαν χρήστες σκοπεύουμε στην προστασία των δεδομένων μας και της «ηλεκτρονικής ταυτότητάς» μας, έτσι και οι hackers που αποσκοπούν σε κακόβουλες ενέργειες και απόκτηση χρημάτων αμοιβών, προσπαθούν να αποκρύψουν με τους ίδιους τρόπους την ταυτότητά τους και τα ηλεκτρονικά ίχνη τους. Αυτό μας φέρνει στην δύσκολη θέση του ότι όσο και να προστατεύουμε ένα σύστημα δεδομένων, σε περίπτωση που γίνουμε αποδέκτες μιας κακόβουλης ενέργειας, δεν είναι πάντα εφικτό να αναστρέψουμε την κατάσταση ή έστω να μάθουμε ποιος βρίσκεται πίσω από τις ενέργειες.

Βιβλιογραφία

Abomhara, M., & Køien, G. M. (2015). Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security and Mobility*, 65-88.

Alshalan, A., Pisharody, S., & Huang, D. (2015). A survey of mobile VPN technologies. *IEEE Communications Surveys & Tutorials*, *18*(2), 1177-1196.

Amin, S. M., & Wollenberg, B. F. (2005). Toward a smart grid: power delivery for the 21st century. *IEEE power and energy magazine*, *3*(5), 34-41.

Andronio, N. (2015). *Heldroid: Fast and efficient linguistic-based ransomware detection* (Doctoral dissertation, University of Illinois at Chicago).

Andronio, N., Zanero, S., & Maggi, F. (2015, November). Heldroid: Dissecting and detecting mobile ransomware. In *international symposium on recent advances in intrusion detection* (pp. 382-404). Springer, Cham.

Arce, I., Clark-Fisher, K., Daswani, N., DelGrosso, J., Dhillon, D., Kern, C., ... & West, J. (2014). Avoiding the top 10 software security design flaws. *IEEE Computer Society Center for Secure Design (CSD), Tech. Rep*.

Aurangzeb, S., Aleem, M., Iqbal, M. A., & Islam, M. A. (2017). Ransomware: a survey and trends. *Journal of Information Assurance & Security*, *6*(2), 48-58.

Avani P. and Ankita G. (2017). A Survey of VPN Performance Evaluation. International *Journal on Recent and Innovation Trends in Computing and Communication*, *5*(5), 409–413.

Bakni M. & Andersson, L. (March 2005) RFC 4026, Provider Provisioned Virtual Private Network (VPN) Terminology, Interner Society, p. 7 DOI: 10.17487/RFC4026.Lewis, Mark (April 2006) Comparing, Designing, and Deploying VPNs, Cisco Press, p. 10 ISBN: 1587051796., CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=84112082

Barbulescu, M., Stratulat, A., Traista-Popescu, V., & Simion, E. (2016, June). Rsa weak public keys available on the internet. In *International Conference for Information Technology and Communications* (pp. 92-102). Springer, Cham.

Brewer, R. (2016). Ransomware attacks: detection, prevention and cure. *Network security*, *2016*(9), 5-9.

Celdrán, A. H., Sánchez, P. M. S., Castillo, M. A., Bovet, G., Pérez, G. M., & Stiller, B. (2022). Intelligent and behavioral-based detection of malware in IoT spectrum sensors. *International Journal of Information Security*, 1-21.

Chen, J. C., & Li, B. (2015). *Evolution of exploit kits: Exploring past trends and current improvements (Research Paper). Irving, Texas: Trend Micro. Online*. https://www. trendmicro. com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-evolution-of-exploit-kits. pdf.

Choi, K. S., Scott, T. M., & LeClair, D. P. (2016). Ransomware against police: diagnosis of risk factors via application of cyber-routine activities theory. *International Journal of Forensic Science & Pathology*.

Chowdhury, N., & Gkioulos, V. (2021). Cyber security training for critical infrastructure protection: A literature review. *Computer Science Review*, *40*, 100361.

Ciampa, M. (2012). *Security+ guide to network security fundamentals*. Cengage Learning.

Clucley, G. (2009). Hacked iPhones held hostage for 5 Euros. *Naked Security*.

Crowdstrike (2022a). How ransomware works. https://www.crowdstrike.com /resources/infographics/how-fileless-ransomware-works/

Crowdstrike (2022b). Fileless Malware Explained. https://www.crowdstrike. com/cybersecurity-101/malware/fileless-malware/

CSEC (2017). Joint Task Force, Cybersecurity Curricula 2017, Version 1.0 Report, CSEC2017.

Cyber Threat Alliance, (2015). Lucrative ransomware attacks: Analysis of the cryptowall version 3 threat. *Cryptowall version 3 Threat report*.

Dong, J. (Ed.). (2007). *Network dictionary*. Javvin Technologies Inc..

Dwyer, C., & Kanguri, A. (2017). Malvertising-a rising threat to the online ecosystem. *Journal of Information Systems Applied Research*, *10*(3), 29.

Elhady, A. M., El-Bakry, H. M., & Abou Elfetouh, A. (2019). Comprehensive risk identification model for SCADA systems. *Security and Communication Networks*, *2019*.

Felt, A. P., Finifter, M., Chin, E., Hanna, S., & Wagner, D. (2011, October). A survey of mobile malware in the wild. In *Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices* (pp. 3-14).

Fitzpatrick, D. & Griffin, D. (2016). Cyber-extortion losses skyrocket, says FBI. http:// money.cnn.com/2016/04/15/technology/ransomwarecyber-security.

F-Secure Labs (2013). Threat Report H1, Helsinki, Finland. https://www.antivirus.si/docs/Novice/F-Secure_Threat_Report_H1_2013.pdf

Fung, K. T. (2004). *Network security technologies*. Auerbach Publications.

Hampton, N., & Baig, Z. A. (2015). Ransomware: Emergence of the cyber-extortion menace. *Proceedings of 13th Australian Information Security Management Conference.*

Harmening, J. T. (2017). Virtual private networks. In *Computer and Information Security Handbook* (pp. 843-856). Morgan Kaufmann.

ISECOM (2000). Open Source Security Testing Methodology: ISECOM. http://www. isecom.org

Jarvis, K. (2013). Cryptolocker ransomware. *Viitattu*, *20*, 2014.

Karantzas, G.; Patsakis, C. An Empirical Assessment of Endpoint Detection and Response Systems against Advanced Persistent Threats Attack Vectors. *J. Cybersecur. Priv.* 2021, *1*, 387-421. https://doi.org/10.3390/jcp1030021

Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., & Kirda, E. (2015, July). Cutting the gordian knot: A look under the hood of ransomware attacks. In *International conference on detection of intrusions and malware, and vulnerability assessment* (pp. 3-24). Springer, Cham.

Kuerbis, B., & Badiei, F. (2017). Mapping the cybersecurity institutional landscape. *Digital Policy, Regulation and Governance*.

Luo, H., Chen, Z., Li, J., & Vasilakos, A. V. (2017). Preventing distributed denial-of-service flooding attacks with dynamic path identifiers. *IEEE Transactions on Information Forensics and Security*, *12*(8), 1801-1815.

ManageEngine. Secure Remote Access: A complete guide https://www.manageengine.com/privileged-session-management/what-is-secure-remote-access.html

McAfee Labs. (2017). Threat Predictions Ransomware Infographic. *McAfee Labs Threats Predictions 2017 report.*

Mercaldo, F., Nardone, V., Santone, A., & Visaggio, C. A. (2016, June). Ransomware steals your phone. formal methods rescue it. In *International Conference on Formal Techniques for Distributed Objects, Components, and Systems* (pp. 212-221). Springer, Cham.

Microsoft Ignite (2022). What is ransomware? https://docs.microsoft.com/enus /security/compass/human-operated-ransomware

Mohurle, S., & Patil, M. (2017). A brief study of wannacry threat: Ransomware attack 2017. *International Journal of Advanced Research in Computer Science*, *8*(5), 1938-1940.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, 21260.

Νικολάου Σ. Σχεδιασμός Εικονικών Δικτύων. https://openclass.teiwm.gr/modules/document/file.php/INFORMATIC105/VPN.pdf IETF (1999) RFC 2661. Layer Two Tunneling Protocol "L2TP"

Narayan, S., Brooking, K., & de Vere, S. (2009, April). Network performance analysis of vpn protocols: An empirical comparison on different operating systems. In *2009 International Conference on Networks Security, Wireless Communications and Trusted Computing* (Vol. 1, pp. 645-648). IEEE.

NIST. (2008). Technical Guide to Information Security Testing and Assessment NIST 800-115: NIST. http://csrc.nist.gov/publications

O'Brien, D. (2016). Dridex: Tidal waves of spam pushing dangerous financial trojan. *Symantec Corporation*.

O'Gorman, G., & McDonald, G. (2012). *Ransomware: A growing menace*. Arizona, AZ, USA: Symantec Corporation.

OISSG (2005). Information Systems Security Assessment Framework OISSG. http: //sourceforge.net/projects/isstf/

Rajamohan, P. (2014). An Overview of Remote Access Vpns: Architecture and Efficient Installation. *Ipasj International Journal of Information Technology (Iijit)*.

Richardson, R., & North, M. M. (2017). Ransomware: Evolution, mitigation and prevention. *International Management Review*, *13*(1), 10.

Safa, H. H., Souran, D. M., Ghasempour, M., & Khazaee, A. (2016). Cyber security of smart grid and scada systems, threats and risks. CIRED 2016, Helsinki, DOI: 10.1049/cp.2016.0692, 2016.

Savage, K., Coogan P, & Lau, H. (2015). The evolution of ransomware. Secur. Response, Symantec. https://its.fsu.edu/sites/g/files/imported/storage/images /information-security-and-privacy-office/theevolution-of-ransomware.pdf

Shaikh M. A. (June 2020). Provider Provisioned VPN (PPVPN). https://www.linkedin.com/pulse/provider-provisioned-vpn-ppvpn-abdul-majid-shaikh

Scarfone, K., Hoffman, P., & Souppaya, M. (2009). Guide to enterprise telework and remote access security. *NIST Special Publication*, *800*, 46.

Sgandurra, D., Muñoz-González, L., Mohsen, R., & Lupu, E. C. (2016). Automated dynamic analysis of ransomware: Benefits, limitations and use for detection. *arXiv preprint arXiv:1609.03020*.

Sobh, T. S., & Aly, Y. (2011). Effective and extensive virtual private network. *Journal of Information Security*, *2*(01), 39.

Souppaya, M., & Scarfone, K. (2016). Guide to enterprise telework, remote access, and bring your own device (BYOD) security. *NIST Special Publication*, *800*, 46.

Spector, P. (2008). *Data manipulation with R* (Vol. 1). New York, NY: Springer.

Symantec. (2016). An ISTR Special Report: Ransomware and Businesses 2016.

Tagliaferri L. (2016). An Introduction to JSON. https://www.digitalocean.com/community/tutorials/an-introduction-to-json

Ten, C. W., Manimaran, G., & Liu, C. C. (2010). Cybersecurity for critical infrastructures: Attack and defense modeling. *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, *40*(4), 853-865.

Teoh, T. T., Nguwi, Y. Y., Elovici, Y., Ng, W. L., & Thiang, S. Y. (2018). Analyst intuition inspired neural network based cyber security anomaly detection. *International Journal of Innovative Computing, Information and Control*, *14*(1), 379-386.

Trend Micro. (2016). Ransomware. *Trend Micro Incorporated Labs report*.

Ullah, I., Khan, N., & Aboalsamh, H. A. (2013, April). Survey on botnet: Its architecture, detection, prevention and mitigation. In *2013 10th IEEE International Conference on Networking, Sensing and Control (ICNSC)* (pp. 660-665). IEEE.

Wu, F. F., Moslehi, K., & Bose, A. (2005). Power system control centers: Past, present, and future. *Proceedings of the IEEE*, *93*(11), 1890-1908.

Yorkdale, G. (2015). Criminals Continue to Defraud and Extort Fund s from Victims Using CryptoWall Ransomware Schemes. *Federal Bureau o f Investigation*.

Zavarsky, P., & Lindskog, D. (2016). Experimental analysis of ransomware on windows and android platforms: Evolution and characterization. *Procedia Computer Science*, *94*, 465-472.

Zetter, K. (2015). Hacker lexicon: A guide to ransomware, the scary hack that's on the rise. https://www.wired.com/2015/09/hacker-lexicon-guideransomware-scary- hack-thats-rise/