



ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΑΔΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

**Ανάκτηση δεδομένων και οπτική αναπαράσταση συσχετίσεων
μεταξύ οντοτήτων που συμμετείχαν σε μια εγκληματική ενέργεια**

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

των

Μουζάκη Ευστάθιου και Φωτίου Δημήτριου

Επιβλέπουσα : **Δρ. Κωσταντία Μπαρμπάτσαλου**

Μέλη εξεταστικής επιτροπής: **Γεώργιος Καμπουράκης , Μαρία Καρύδα**

Σάμος, Μάρτιος 2021

Η σελίδα αυτή είναι σκόπιμα λευκή.

Πρόλογος και ευχαριστίες

Θα θέλαμε να ευχαριστήσουμε από καρδιάς τους καθηγητές μας κ. Καμπουράκη, κα.Καρύδα και κα. Μπαρμπάτσαλου, για την εξαιρετική συνεργασία που είχαμε στα πλαίσια της παρούσας διπλωματικής εργασίας. Οι συμβουλές της κας. Μπαρμπάτσαλου ήταν παραπάνω από πολύτιμες και βοήθησαν τα μέγιστα στην ολοκλήρωση αυτής της εργασίας.

Τέλος θα θέλαμε να ευχαριστήσουμε τις οικογένειες μας για την στήριξή τους καθ' όλη την διάρκεια του μεταπτυχιακού .

© 2021

των

ΜΟΥΖΑΚΗ ΕΥΣΤΑΘΙΟΥ ΚΑΙ ΦΩΤΙΟΥ ΔΗΜΗΤΡΙΟΥ

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

Η σελίδα αυτή είναι σκόπιμα κενή.

Πίνακας περιεχομένων

1	Εισαγωγή.....	17
1.1	Εξέλιξη του Ψηφιακού Εγκλήματος και Σημαντικότητα της Ψηφιακής Εγκληματολογίας	17
1.2	Αντικείμενο της Μεταδιπλωματικής Εργασίας	18
1.3	Σκοπός της εργασίας και επιμέρους στόχοι	18
2	Διερεύνηση Και Απόδοση Βασικών Ορισμών	19
2.1	Ηλεκτρονική επίθεση.....	19
2.2	Ηλεκτρονικό Έγκλημα.....	20
2.3	Ψηφιακά Αποδεικτικά Στοιχεία.....	21
2.4	Ψηφιακή Εγκληματολογία	23
2.5	Ασφάλεια στον Κυβερνοχώρο.....	24
3	Ιστορική Αναδρομή Στο Ηλεκτρονικό Έγκλημα.....	25
3.1	Η εξέλιξη του Ηλεκτρονικού Εγκλήματος και της Ψηφιακής Εγκληματολογίας	25
3.2	Διεθνές και Ευρωπαϊκό Νομοθετικό πλαίσιο	26
4	Μελλοντικές Τάσεις Στο Ηλεκτρονικό Έγκλημα	29
4.1	Το μέλλον του Ηλεκτρονικού Εγκλήματος.....	29
4.2	Ερευνητικές Τάσεις	30
5	Σταδιοποίηση Των Διαδικασιών Στην Ψηφιακή Εγκληματολογία.....	33
5.1	Προσδιορισμός των ψηφιακών πειστηρίων	41
5.2	Συλλογή των ψηφιακών πειστηρίων.....	41
5.3	Διατήρηση των ψηφιακών πειστηρίων	41
5.4	Εξέταση και Ανάλυση των ψηφιακών πειστηρίων.....	42
5.4.1	Επαλήθευση του συμβάντος	42
5.4.2	Περιγραφή του συστήματος.....	42
5.4.3	Ανάλυση του χρονικού πλαισίου.....	42
5.4.4	Κατηγοριοποίηση δεδομένων	42
5.4.5	Εφαρμογή φίλτρων ή αναζήτηση με λέξεις κλειδιά κατά την αναζήτηση πληροφοριών	43
5.4.6	Ανάκτηση Δεδομένων	43
5.4.7	Συλλογή στοιχείων από RAM.....	43
5.4.8	Δημιουργία μιας απεικόνισης του δίσκου	43
5.4.9	Αποκάλυψη και ανάλυση των ψηφιακών αποδεικτικών στοιχείων.....	43

5.5	Παρουσίαση των ψηφιακών πειστηρίων.....	44
6	Εργαλεία Ανάλυσης Δεδομένων Στην Ψηφιακή Εγκληματολογία	47
6.1	FRED (FRED SR, FRED L)	47
6.2	Encase	48
6.3	FTK imager	48
6.4	Slauth Kit και Autopsy.....	48
6.5	Digital Forensics Framework	49
6.6	Open Computer Forensics Architecture (OCFA)	49
6.7	CAINE	49
6.8	X-way Forensics	49
6.9	SANS Investigative Forensics Toolkit.....	50
6.10	Registry Recon.....	50
6.11	LIBFORENSICS.....	50
6.12	Windows SCOPE	50
6.13	Belkasoft evidence centre	50
6.14	Foremost	51
6.15	MemGator	51
6.16	Galleta.....	51
6.17	Wireshark.....	52
6.18	Rifiuti.....	52
6.19	NMAP.....	52
6.20	The Coroner's toolkit	53
6.21	Oxygen Forensic Suite.....	53
6.22	Bulk Extractor	53
6.23	Xplico	53
6.24	Mandiant RedLine.....	54
6.25	XRY	54
6.26	P2 explorer.....	54
6.27	PlainSight.....	54
7	Τεχνητή Νοημοσύνη Ως Λύση Ασφάλειας.....	56
7.1	Δυνατότητες Τεχνητής Νοημοσύνης στην ψηφιακή εγκληματολογία	58
7.1.1	Ανίχνευση.....	58
7.1.2	Πρόγνωση.....	58
7.1.3	Ανταπόκριση στις απειλές στον κυβερνοχώρο	59
7.2	Επιθυμητά Χαρακτηριστικά της Τεχνητής Νοημοσύνης.....	59

7.3	Εφαρμογές τεχνητής νοημοσύνης	59
7.3.1	<i>Εφαρμογές τεχνητού νευρωνικού δικτύου (Artificial Neural Network Applications ANN).....</i>	60
7.3.2	<i>Ευφυείς Δρώντες (Intelligent agents)</i>	60
7.3.3	<i>Εφαρμογές τεχνητής ανοσοποίησης συστήματος (Artificial Immune System Applications)</i>	60
7.3.4	<i>Μοντέλα Ταυτοποίησης.....</i>	61
7.3.5	<i>Μοντέλα Αυθεντικοποίησης</i>	61
7.3.6	<i>Μοντέλα Απόδοσης.....</i>	61
7.3.7	<i>Μοντέλα Κακόβουλου Λογισμικού.....</i>	61
7.4	Προκλήσεις για τις εφαρμογές τεχνητής νοημοσύνης	62
7.5	Το μέλλον της Τεχνητής Νοημοσύνης.....	63
8	Παρουσίαση Του Κακόβουλου Λογισμικού TelegramRat.exe	65
8.1	Μεθοδολογία	65
8.2	Αποτελέσματα	70
9	Παρουσίαση Της Προσομοίωσης Της Επίθεσης Τύπου Ransomware.....	83
9.1	Μεθοδολογία και υλικό.....	84
9.2	Περιγραφή διαδικασίας και αποτελέσματα	85
10	Συζήτηση.....	83
11	Συμπεράσματα και Περιορισμοί	84
	Βιβλιογραφία.....	86

Λίστα Σχημάτων

Εικόνα 1 Ο κύκλος ζωής των ψηφιακών πειστηρίων Stoyanova M. Et al (2020).....	22
Εικόνα 2 Η ασφάλεια των πληροφοριών, των ΤΠΕ και η ασφάλεια στον κυβερνοχώρο Von Solms et al (2013).	24
Εικόνα 3 Η ψηφιακή εγκληματολογική διαδικασία χωρισμένη σε επτά φάσεις.....	44
Εικόνα 4 Αξιολόγηση κινδύνου κακόβουλου λογισμικού TelegramRat μέσω του VirusTotal	67
Εικόνα 5 Μεθοδολογία που ακολουθήθηκε ώστε να πραγματοποιηθεί η εικονική επίθεση τύπου ransomware..	84
Εικόνα 6 Δημιουργία νέου bot στο Telegram.	85
Εικόνα 7 Αυτόματη δημιουργία access token από το bot του Telegram	86
Εικόνα 8 Εισαγωγή παραμέτρων και δημιουργία του κακόβουλου λογισμικού TelegramRat.exe.....	87
Εικόνα 9. Email που στάλθηκε στο θύμα	88
Εικόνα 10 Εργαλείο Fiddler έλεγχος εισερχόμενων και εξερχόμενων δεδομένων στον υπολογιστή θύμα	89
Εικόνα 11 Εκτέλεση εντολής /EncryptFileSystem <password>	89
Εικόνα 12 Ανάλυση επικοινωνίας θύτη θύματος κατά την εκτέλεση της εντολής /EncryptFileSystem	90
Εικόνα 13 Ανάλυση επικοινωνίας θύτη θύματος κατά την επιτυχή εκτέλεση της εντολής /EncryptFileSystem	91
Εικόνα 15 Κρυπτογραφημένο αρχείο	91
Εικόνα 14 Αρχείο πριν την κρυπτογράφηση.....	91
Εικόνα 16 Εκτέλεση εντολής /DecryptFileSystem <password>	92
Εικόνα 17 Ανάλυση επικοινωνίας θύτη θύματος κατά την επιτυχή εκτέλεση της εντολής /DecryptFileSystem με σκοπό την αποκρυπτογράφηση του συστήματος.....	92
Εικόνα 18 Αποκρυπτογραφημένο αρχείο	93
Εικόνα 19 Δημιουργία memory dump	93
Εικόνα 20 Δημιουργία Case στο Autopsy.....	94
Εικόνα 21 Καρτέλα Details του Autopsy.....	94

Λίστα Πινάκων

Πίνακας 1 Οι πέντε φάσεις κατά Yusoff Y et al (2011)	40
Πίνακας 2 Ανάλυση της κλάσης “static void Main(string[] args)” που αναπτύσσεται στο αρχείο “Program.cs” του project TelegramRAT	71
Πίνακας 2 Ανάλυση της κλάσης “static void Main(string[] args)” που αναπτύσσεται στο αρχείο “Program.cs” του project TelegramRAT	74
Πίνακας 4 Ανάλυση της κλάσης “ internal static class utils ” που αναπτύσσεται στο αρχείο “ utils .cs ” του project TelegramRAT	76
Πίνακας 5 Ανάλυση της κλάσης “ internal class telegram” που αναπτύσσεται στο αρχείο	77
Πίνακας 6 Ανάλυση κλάσεων που αναπτύσσονται στο αρχείο “ SimpleJSON.cs ” του project TelegramRAT	78
Πίνακας 7 Ανάλυση της κλάσης “internal sealed class persistence” που αναπτύσσεται στο αρχείο “ persistence .cs ” του project TelegramRAT	81
Πίνακας 8 Ανάλυση των κλάσεων που αναπτύσσονται στον υποφάκελο stealer του project TelegramRAT ..	82
Πίνακας 9 Δεδομένα που ανακτήθηκαν από το Autopsy	83

Ακρωνύμια

AI	Artificial Intelligence
ARP cache	Address Resolution Protocol entries
CD	Compact Disc
DoS	Denial of Service
DVD	Digital Video Disc
GPS	Global Positioning System
IDPS	Intrusion Detection and Prevention Systems
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
IoT	Internet of Things
RAM	Random Access Memory
TB	Terabyte
TΠΕ	Τεχνολογία Πληροφοριών

Περίληψη

Η ψηφιακή εγκληματολογία είναι η επιστήμη στην οποία εφαρμόζονται μέθοδοι για τη συλλογή, την αποθήκευση, τη διατήρηση, την επικύρωση, την αναγνώριση, την ανάλυση, την ερμηνεία, την καταγραφή και την παρουσίαση των ψηφιακών αποδεικτικών στοιχείων από πολλαπλές ψηφιακές πηγές και έχει ως στόχο τη διερεύνηση και την αναπαράσταση εγκληματικών ενεργειών και επιθέσεων.

Η ψηφιακή εγκληματολογία στηρίζεται σε κατάλληλα τεχνολογικά εργαλεία, καθώς και σε ενδεδειγμένες διαδικασίες. Οι τεχνικές προκλήσεις περιλαμβάνουν την πολυπλοκότητα και την ετερογένεια των ψηφιακών πηγών που αφορούν κυρίως στις διαφορετικές πλατφόρμες, ποικίλες εφαρμογές και δρομολογητές καθώς και στον μεγάλο όγκο των διαθέσιμων δεδομένων.

Αναμένεται πως το μέλλον θα φέρει ραγδαία εξέλιξη σε τεχνολογικούς τομείς οι οποίοι με τη σειρά τους θα επηρεάσουν την ψηφιακή εγκληματολογία.

Με βάση τη βιβλιογραφική ανασκόπηση και με την υλοποίηση του τεχνικού μέρους που αφορούσε στην εκτέλεση της επίθεσης και στην εύρεση αποδεικτικών στοιχείων φαίνεται πως τα τεχνικά μέτρα που προορίζονται για την ασφάλεια στον κυβερνοχώρο καθώς και το εκπαιδευμένο προσωπικό είναι απαραίτητα στοιχεία για την αποφυγή επιθέσεων. Ακόμη, η χρήση εργαλείων τεχνητής νοημοσύνης κρίνεται αναγκαία καθώς βελτιώνει την ποιότητα της έρευνας των αναλυτών μειώνοντας σημαντικά το χρόνο εύρεσης νέων στοιχείων και βοηθούν στην ανάπτυξη πιο ισχυρών αντίμετρων.

Στην παρούσα εργασία παρουσιάζεται ένα κακόβουλο λογισμικό απομακρυσμένου ελέγχου υπολογιστών RAT το οποίο έχει γραφτεί με τη γλώσσα προγραμματισμού C# στο περιβάλλον ανάπτυξης της Microsoft Visual Studio και στο οποίο χρησιμοποιείται ως εντολέας το bot του Telegram. Όταν είναι ενεργοποιημένη η απομακρυσμένη πρόσβαση, οι εξουσιοδοτημένοι υπολογιστές και οι διακομιστές μπορούν να ελέγχουν όλα όσα συμβαίνουν στον υπολογιστή του χρήστη ανοίγοντας έγγραφα, εγκαθιστώντας λογισμικό και μετακινώντας τον κέρσorra της οθόνης σε πραγματικό χρόνο.

Στα πλαίσια της εργασίας πραγματοποιήθηκε μια προσομοίωση της επίθεσης τύπου ransomware και ακολούθησε ανάλυση των δεδομένων που συλλέχθηκαν και αφορούν στην επικοινωνία θύτη και θύματος με τη χρήση του εργαλείου Fiddler. Μετά από ανάλυση βρέθηκαν στοιχεία όπως ημερομηνίες και ενέργειες οι οποίες πραγματοποιήθηκαν από την εγκατάσταση του κακόβουλου λογισμικού και έπειτα.

Λέξεις Κλειδιά: TelegramRat, κακόβουλο λογισμικό, κυβερνοεπίθεση, ψηφιακή εγκληματολογία

Abstract

Digital Forensics is the science where methods related to the collection, storage, preservation, validation, recognition, analysis, interpretation, recording and presentation of digital evidence collected from various digital sources are applied with the aim of investigating and representing in the court criminal acts and cyber attacks.

Digital Forensics relies on the appropriate technological tools as well as validated processes. Technical challenges include the complexity of digital sources, the vast variety of different platforms, the heterogeneity of the applications and routers, as well as the large amount of available data.

Scholars report that the future will bring rapid developments in technological fields which in turn will affect digital criminology.

Based on literature and the technical part of this work, it is evident that technical measures as well as competent and skilled professionals are important factors in avoiding cyber attacks. Still, the use of artificial intelligence tools can play a vital role in the amelioration of the cyber forensics research by reducing the required time for data retrieval and by developing robust countermeasures.

This thesis presents a RAT remote control malware program written in the C # programming language in the Microsoft Visual Studio development environment that uses the Telegram bot as the client. When remote access is enabled, authorized computers and servers can control everything on the user's computer for example open documents, download software, and move the screen cursor.

As part of the work, a simulation of the ransomware attack was performed, followed by an analysis of the data collected regarding the perpetrator-victim communication using the Fiddler tool. Data such as dates and actions that were performed from the installation of the malware and beyond was retrieved.

Keywords: *TelegramRat, Malware Software, Cyber Attack, Digital Forensics*

1

Εισαγωγή

1.1 Εξέλιξη του Ψηφιακού Εγκλήματος και Σημαντικότητα της Ψηφιακής Εγκληματολογίας

Με την ταχεία εξέλιξη της τεχνολογίας, την έντονη παρουσία της σε κάθε πτυχή της καθημερινής, επαγγελματικής ακόμη και κοινωνικής έκφρασης, καθώς και την ευρεία διάδοση της γνώσης των υπολογιστών και της πληροφορικής αναμένεται ραγδαία αύξηση και των διαδικτυακών επιθέσεων και του ψηφιακού εγκλήματος. Το γεγονός αυτό επιβεβαιώνεται από τα ποσοστά του ψηφιακού εγκλήματος τα οποία αυξάνονται και μάλιστα αντιστρόφως ανάλογα από τα παραδοσιακά εγκλήματα στον φυσικό κόσμο (Tcherni et al. 2016) χωρίς ωστόσο να υπάρχουν επίσημες στατιστικές για τις περισσότερες μορφές εγκλήματος στον κυβερνοχώρο (Bossler A. et al, 2019).

Καθώς οι υπολογιστές γίνονται μικρότεροι, ταχύτεροι, οικονομικότεροι και πιο εύχρηστοι και το λογισμικό μπορεί πλέον να ενσωματώνεται οπουδήποτε όπως σε μέσα μετακίνησης, σε εργαλεία, σε οικιακές συσκευές και μηχανήματα, σε τηλεπικοινωνιακά συστήματα ακόμη και στο ανθρώπινο σώμα (Ryan D.J. et al. 2002), μια ψηφιακή επίθεση είναι πια αναμενόμενη αφήνοντας τα θύματα εκτεθειμένα σε καταστάσεις υποκλοπής, εκφοβισμού, διαρροής προσωπικών δεδομένων κτλ.

Υπό αυτές τις συνθήκες που αναφέρθηκαν καθίσταται εύλογο το συμπέρασμα για το πώς η έρευνα στο πεδίο της ψηφιακής εγκληματολογίας αναπτύσσεται ακολουθώντας τις εξελίξεις της τεχνολογίας.

1.2 Αντικείμενο της Μεταδιπλωματικής Εργασίας

Η παρούσα εργασία υλοποιείται στα πλαίσια του μεταπτυχιακού προγράμματος «Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων» και ασχολείται με την ανάκτηση δεδομένων και την οπτική αναπαράσταση συσχετίσεων μεταξύ οντοτήτων που συμμετείχαν σε μια εγκληματική ενέργεια. Η συνεισφορά της έρευνας που πραγματοποιήθηκε στα πλαίσια αυτής της εργασίας και αφορά στο πεδίο της Ψηφιακής εγκληματολογίας αναμένεται σημαντική καθώς θα πραγματοποιηθεί η εγκληματολογική εξέταση στο τερματικό ενός θύματος αφού προηγηθεί η επιτυχής εκτέλεση της επίθεσης μετά την εφαρμογή του *TelegramRat*, ενός προγράμματος που δύναται να καταλάβει ολόκληρο τον υπολογιστή του χρήστη.

1.3 Σκοπός της εργασίας και επιμέρους στόχοι

Επίκεντρο της παρούσας διπλωματικής εργασίας είναι η ερευνητική συνεισφορά στην επιστήμη της ψηφιακής εγκληματολογίας. Αναλυτικότερα, σκοπό της διπλωματικής εργασίας αποτελεί η διεξαγωγή εγκληματολογικής εξέτασης στο τερματικό ενός θύματος μετά την επιτυχή εκτέλεση της επίθεσης η οποία αναλύεται διεξοδικά σε επόμενα κεφάλαια. Για την εκπλήρωση του σκοπού της διπλωματικής εργασίας, χρειάζεται να επιτευχθούν συγκεκριμένοι θεωρητικοί στόχοι όπως είναι η βιβλιογραφική επισκόπηση που επικεντρώθηκε στην ανάλυση των εννοιών της ψηφιακής εγκληματολογίας, στην επισκόπηση των βασικών τεχνικών προκλήσεων και νομικών ζητημάτων που εμφανίζονται κατά την εγκληματολογική εξέταση και στην ανάλυση εργαλείων και διαδικασιών που εφαρμόζονται κατά την εγκληματολογική εξέταση. Επιμέρους τεχνικοί και ερευνητικοί στόχοι που πραγματοποιήθηκαν κατά την υλοποίηση της εργασίας είναι η εφαρμογή του *TelegramRat*.

2

Διερεύνηση Και Απόδοση Βασικών Ορισμών

Στο παρόν κεφάλαιο θα επιχειρηθεί η διερεύνηση και η απόδοση των ορισμών κάποιων βασικών εννοιών με τις οποίες ασχολείται η εργασία όπως: η ηλεκτρονική επίθεση, το ηλεκτρονικό έγκλημα, τα ψηφιακά αποδεικτικά στοιχεία, η ψηφιακή εγκληματολογία και η ασφάλεια στον κυβερνοχώρο.

2.1 Ηλεκτρονική επίθεση

Σύμφωνα με το πρότυπο ISO/IEC 27000, η ηλεκτρονική επίθεση περιγράφεται σαν «μια προσπάθεια καταστροφής, αποκάλυψης, μετατροπής, αδρανοποίησης, κλοπής ή μη εξουσιοδοτημένης πρόσβασης ή χρήσης δεδομένων, συστημάτων ή άλλων στοιχείων τα οποία επιφέρουν αξία σε έναν οργανισμό.» (ISO, 2018)

Η ηλεκτρονική επίθεση σχετίζεται στενά με το ηλεκτρονικό έγκλημα καθώς κατά την ηλεκτρονική επίθεση η οποία ορίζεται ως «μια εκούσια εκμετάλλευση των πληροφοριακών συστημάτων και δικτύων των τεχνολογικά εξαρτώμενων οργανισμών» (Marshall J.B. et al.nd). Κατά την ηλεκτρονική επίθεση χρησιμοποιούνται κακόβουλα προγράμματα ώστε να τροποποιηθεί το λογισμικό του υπολογιστή γεγονός που έχει ως απόρροια τη διακύβευση των δεδομένων γεγονός που συντελεί σε ηλεκτρονικά εγκλήματα όπως είναι η υποκλοπή πληροφοριών ή ταυτότητας (Marshall J.B. et al.nd)

Κατά τον Ajit A. Et al (2008) οι ηλεκτρονικές επιθέσεις αφορούν σε: τυχαία αποκάλυψη πληροφοριών, πρόσβαση σε δεδομένα από περιέργεια ή για προσωπικό συμφέρον, ηθελημένη

παραβίαση εμπιστευτικών πληροφοριών και μετάδοση σε τρίτους για κερδοσκοπία ή εκδίκηση, παραβίαση δεδομένων από εξωτερική απειλή με φυσική εισβολή και μη εξουσιοδοτημένη διείσδυση στο δίκτυο από hackers οι οποίοι εισέρχονται στο σύστημα του οργανισμού και αποκτούν πρόσβαση στις πληροφορίες ή καθιστούν το σύστημα ανενεργό (Ajit A. et al, 2008).

Πιο συγκεκριμένα, οι επιθέσεις οι οποίες διευκολύνονται από το διαδίκτυο είναι προγράμματα (ιοί, spyware, worms, Trojans) που μολύνουν τον υπολογιστή και μπορεί να εξαπλωθούν εύκολα μεταξύ των υπολογιστών. (Heaney J, online). Για παράδειγμα, το ransomware συνιστά έναν τύπο κακόβουλου λογισμικού που απειλεί να δημοσιεύσει σημαντικά δεδομένα ή να αποκλείσει την πρόσβαση του σε αυτά αν δεν καταβληθεί κάποιο χρηματικό ποσό. (Armstrong J. et al., 2017). Συχνή είναι επίσης η επίθεση κατά της άρνησης υπηρεσίας (DoS) κατά την οποία ένα δίκτυο υπερφορτώνεται με κίνηση, καθιστώντας το ανενεργό και άχρηστο στους χρήστες του, (Heaney J, online) καθώς και οι επιθέσεις ηλεκτρονικού ψαρέματος, η υποκλοπή ταυτότητας, η μαζική αποστολή ηλεκτρονικών μηνυμάτων ή συνδέσμων (spam) και η καταγραφή πληκτρολόγησης (key logging). (Μήτρου Λ., nd)

2.2 Ηλεκτρονικό Έγκλημα

Οι Gordon και Ford (2006) ταξινόμησαν το έγκλημα στον κυβερνοχώρο σε αδικήματα τύπου I και τύπου II όπου ο τύπος I αναφέρεται στο έγκλημα που έχει πιο τεχνικό χαρακτήρα (π.χ. hacking), ενώ το έγκλημα τύπου II βασίζεται περισσότερο στην ανθρώπινη επαφή παρά στην τεχνολογία (π.χ. διαδικτυακά τυχερά παιχνίδια).

Ο Grabosky (2007) διερευνώντας τη νομοθεσία και το δίκαιο προσπάθησε να κατατάξει τα ηλεκτρονικά εγκλήματα και κατέληξε σε τρεις γενικές κατηγορίες: στα εγκλήματα όπου ο υπολογιστής χρησιμοποιείται ως το μέσο εγκλήματος, στα εγκλήματα στα οποία ο υπολογιστής συνεπικουρεί στο αδίκημα και στα εγκλήματα όπου ο υπολογιστής είναι ο στόχος του εγκλήματος.

Ακόμη, οι McGuire και Dowling (2013) κατηγοριοποίησαν το ψηφιακό έγκλημα σε έγκλημα «ενεργοποιημένο στον κυβερνοχώρο» και έγκλημα «εξαρτώμενο από τον κυβερνοχώρο».

Στα ηλεκτρονικά εγκλήματα υπάγονται η διαδικτυακή απάτη ή κλοπή (π.χ. κλοπή ταυτότητας) η ψηφιακή πειρατεία, η διαδικτυακή πορνογραφία και η βία (π.χ. διαδικτυακή τρομοκρατία, διαδικτυακό bullying) (Holt et al. 2018). Ωστόσο, υπάρχουν ελάχιστες αξιόπιστες στατιστικές σχετικά με τον αριθμό των εγκλημάτων στον κυβερνοχώρο (Holt et al. 2016).

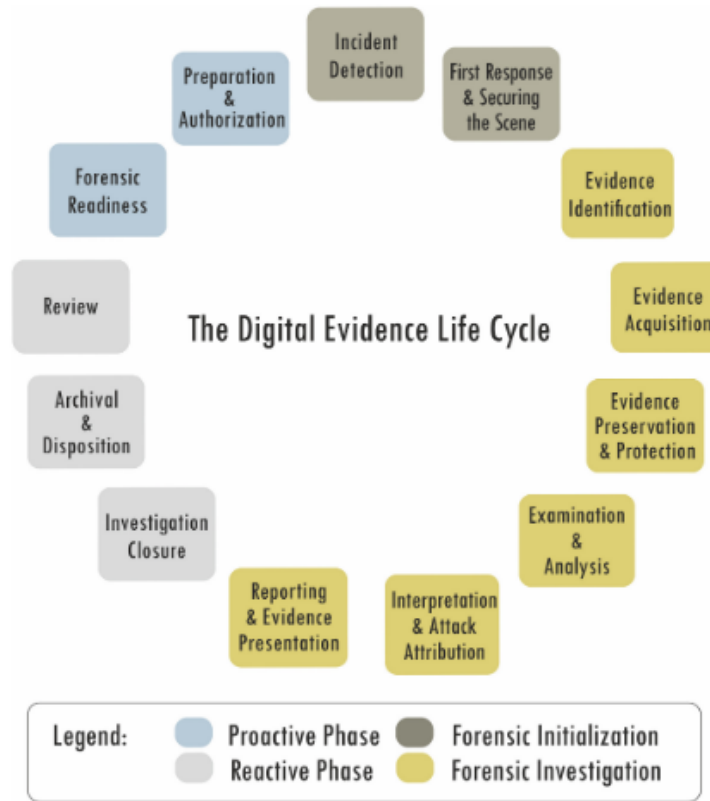
Συγκεντρωτικά, το έγκλημα στον κυβερνοχώρο ή ηλεκτρονικό έγκλημα ή ψηφιακό έγκλημα αναφέρεται σε εγκληματικές ενέργειες που υποστηρίζονται από την τεχνολογία και συγκεκριμένα από υπολογιστές ή άλλα ηλεκτρονικά μέσα. Το ηλεκτρονικό έγκλημα είναι άμεσο αποτέλεσμα της τεχνολογίας των υπολογιστών, της πληροφορικής και των δικτύων και δεν δύναται να υπάρχει χωρίς αυτήν. (Bossler A. et al, 2019)

2.3 Ψηφιακά Αποδεικτικά Στοιχεία

Στα ψηφιακά εγκλήματα οι δράστες αφήνουν ίχνη ή ψηφιακά αποτυπώματα. Σε αυτό το σημείο ξεκινάει ο ρόλος της Ψηφιακής Εγκληματολογίας, που ασχολείται κατά κύριο λόγο με την ανάκτηση χαμένων πληροφοριών, την ανάλυση ψηφιακών αποδεικτικών στοιχείων ακόμα και με την αναπαράσταση του ψηφιακού εγκλήματος. (Κασούμης Ν, 2014)

Τα ψηφιακά πειστήρια ή ψηφιακά αποδεικτικά στοιχεία παίζουν τον πιο σημαντικό ρόλο στην διαμόρφωση του αποτελέσματος σε μια έρευνα. Οι Carrier και Spafford (2004) όρισαν τα ψηφιακά αποδεικτικά στοιχεία σαν τις πληροφορίες που μπορούν να στηρίξουν ή να διαψεύσουν μια υπόθεση. Τέτοιου είδους πειστήρια μπορούν να συλλεχθούν από περιπτώσεις όπου εμπλέκονται ψηφιακές συσκευές που παρέχουν τα αντίστοιχα δεδομένα. Ο ερευνητής συλλέγοντας αυτά τα στοιχεία, μπορεί να δημιουργήσει το εγκληματολογικό προφίλ ενός ατόμου σε αρκετά μεγάλο βαθμό και να διατυπώσει συγκεκριμένα μοτίβα.

Τα ψηφιακά πειστήρια κατά τους Stoyanova M. Et al (2020) ακολουθούν έναν κύκλο ζωής ο οποίος παρουσιάζεται στην παρακάτω εικόνα και αναλύεται ως μέρος της ψηφιακής εγκληματολογικής διαδικασίας σε επόμενο κεφάλαιο.



Εικόνα 1 Ο κύκλος ζωής των ψηφιακών πειστηρίων Stoyanova M. Et al (2020)

Τα ψηφιακά αποδεικτικά στοιχεία είναι ιδιαίτερα ευπαθή και μπορούν να μορφοποιηθούν ή ακόμα και να καταστραφούν από οποιονδήποτε απρόσεκτο χειρισμό. Κρίνεται επιβεβλημένο να λαμβάνονται μέτρα ασφαλείας για να διατηρούν την αρχική τους κατάσταση. Οι ψηφιακές πηγές από όπου μπορεί να προκύψουν τα ψηφιακά πειστήρια είναι πολλές όπως για παράδειγμα οι υπολογιστές, τα κινητά τηλέφωνα, οι έξυπνες συσκευές κτλ. (Pradillo J.,2011).

Σε μια άλλη κατηγοριοποίηση των πηγών προχώρησε ο Henseler (2000): τα Ανοιχτά Υπολογιστικά Συστήματα (Open computer systems) δηλαδή οι κοινοί υπολογιστές που πλέον χρησιμοποιούνται ευρέως, τα Συστήματα Επικοινωνίας (Communication Systems) δηλαδή τα ασύρματα δίκτυα επικοινωνίας και το Διαδίκτυο και τα Ενσωματωμένα Υπολογιστικά Συστήματα (Embedded Computer Systems) όπως τα κινητά τηλέφωνα, οι έξυπνες κάρτες και οι συσκευές με GPS.

2.4 Ψηφιακή Εγκληματολογία

Κάποιοι από τους τομείς που ανήκουν στην Εγκληματολογία είναι η Δικανική Ανθρωπολογία, η Δικανική Οδοντιατρική, η Τοξικολογία, η Βαλλιστική και η Ψηφιακή Εγκληματολογία (Κασούμης Ν., 2014). Η Ψηφιακή Εγκληματολογία είναι η απόδοση στην Ελληνική γλώσσα των ορισμών Internet Forensics, Cyberforensics, Network Forensics και Computer-Forensics. Η ψηφιακή εγκληματολογία καταπιάνεται με τη συλλογή, διατήρηση, και ανάλυση των ψηφιακών αποδεικτικών στοιχείων ώστε να γίνουν αποδεκτά από το δικαστήριο. (Kenneally EK, 2005)

Ως Ψηφιακή Εγκληματολογία ορίζεται ένας κλάδος της παραδοσιακής επιστήμης της εγκληματολογίας που εφαρμόζει επιστημονικές μεθόδους στη συλλογή, αποθήκευση, διατήρηση, επικύρωση, αναγνώριση, ανάλυση, ερμηνεία, καταγραφή και παρουσίαση των ψηφιακών αποδεικτικών στοιχείων τα οποία προέρχονται από ψηφιακές πηγές και στοχεύουν στην διευκόλυνση, ανακατασκευή και αναπαράσταση εγκληματικών ενεργειών ή στην αποτροπή μη εξουσιοδοτημένων επικίνδυνων ενεργειών (Palmer, 2001).

Η Ψηφιακή Εγκληματολογία είναι μια πολυδιάστατη επιστήμη η οποία έχει αρκετούς κλάδους όπως είναι η εγκληματολογία δικτύων, η εγκληματολογία υπολογιστών, η εγκληματολογία βάσεων δεδομένων κ.λπ. (Κασούμης Ν., 2014), στηρίζεται κυρίως στην επιστήμη των υπολογιστών, στα μαθηματικά, στη φυσική και στη μηχανική (Ryan D.J. et al. 2002) και εφαρμόζεται στο νόμο. Ο σκοπός της είναι να χρησιμοποιηθεί σε ευθυγράμμιση με το ποινικό δίκαιο ώστε να διευκολύνει την εξέλιξη μιας υπόθεσης στο δικαστήριο. Οι ειδικοί που ασχολούνται με τον κλάδο μπορούν να προέρχονται από διάφορες ειδικότητες της ιατρικής, της πληροφορικής και της βιολογίας και να έχουν σχετική εξειδίκευση στην ταυτοποίηση, τη συλλογή, την ανάκτηση, την ανάλυση και την παρουσίαση ψηφιακών πειστηρίων (Κασούμης Ν., 2014).

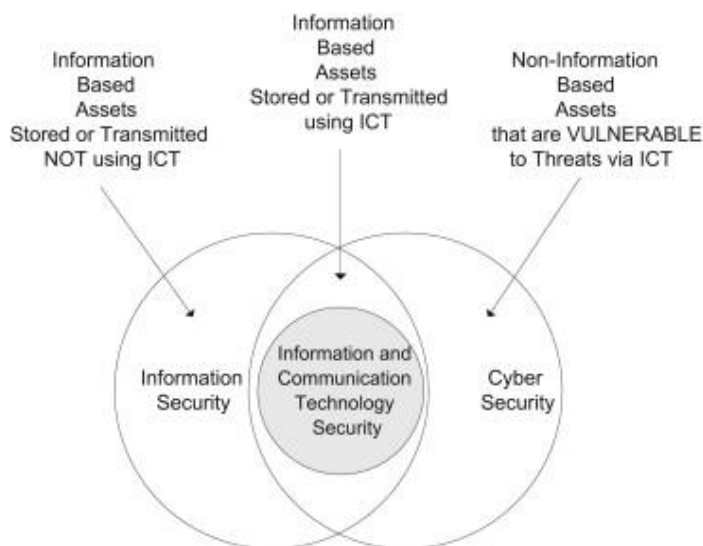
Ένας αναδυόμενος κλάδος της επιστήμης της Ψηφιακής Εγκληματολογίας ασχολείται με το διαδίκτυο των πραγμάτων IoT δημιουργώντας ένα σχετικά νέο πεδίο έρευνας. Ο σκοπός είναι ο εντοπισμός και η εξαγωγή ψηφιακών πειστηρίων με νόμιμο και ορθό τρόπο από ποικίλες πηγές όπως από αισθητήρες IoT, από το εσωτερικό δίκτυο για παράδειγμα από έναν δρομολογητή ή από το cloud. Ο επιστημονικός αυτός κλάδος μπορεί να διαιρεθεί σε τρεις επιμέρους κατηγορίες που αφορούν σε

επίπεδο συσκευής IoT, σε επίπεδο δικτύου και σε επίπεδο cloud. Σε αντίθεση με την παραδοσιακή Ψηφιακή Εγκληματολογία, όπου τα συνηθισμένα αντικείμενα της εξέτασης είναι υπολογιστές, smartphones, tablets, διακομιστές ή πύλες, στο IoT Forensics οι πηγές αποδεικτικών στοιχείων θα μπορούσαν να είναι πολύ πιο εκτεταμένες, συμπεριλαμβανομένων συστημάτων παρακολούθησης βρεφών ή ασθενών, συστημάτων ψυχαγωγίας σε μέσα μεταφοράς, φωτεινών σηματοδοτών και ακόμη και ιατρικών εμφυτευμάτων και συσκευών (Stoyanova M. Et al 2020).

2.5 Ασφάλεια στον Κυβερνοχώρο

Αν και είναι δύσκολο να διαχωριστεί η ασφάλεια των πληροφοριών και των συστημάτων από την ασφάλεια στον κυβερνοχώρο, οι von Solms et.al (2013) εντόπισαν τις διαφορές μεταξύ αυτών των δύο όρων. Η ασφάλεια των πληροφοριών ασχολείται με την προστασία των πληροφοριών αυτών καθαντών σε φυσική ή μη φυσική μορφή, ενώ η ασφάλεια στον κυβερνοχώρο αναφέρεται στην διασφάλιση τόσο πληροφοριακών όσο και μη πληροφοριακών στοιχείων μέσω της υποδομής υπολογιστών. Οι δυο όροι συναντώνται υποστηρίζοντας τον όρο της ασφάλειας των ΤΠΕ όπως φαίνεται στην Εικόνα 2.

Στο επόμενο κεφάλαιο θα γίνει μια σύντομη ιστορική αναδρομή στις πρώτες επιθέσεις της ασφάλειας των ηλεκτρονικών συστημάτων καθώς και τις τρώσεις στην ασφάλεια στον κυβερνοχώρο και θα αναπτυχθεί η ανάδυση του ηλεκτρονικού εγκλήματος.



Εικόνα 2 Η ασφάλεια των πληροφοριών, των ΤΠΕ και η ασφάλεια στον κυβερνοχώρο Von Solms et al (2013).

3

Ιστορική Αναδρομή Στο Ηλεκτρονικό Έγκλημα

3.1 Η εξέλιξη του Ηλεκτρονικού Εγκλήματος και της Ψηφιακής Εγκληματολογίας

Η πρώτη χρήση του όρου «κυβερνοχώρος» εμφανίστηκε πριν από επτά δεκαετίες κατά τους Ottis et al (2010) ενώ αργότερα το 1980 χρησιμοποιήθηκε στη λογοτεχνία από τον Gibson (1984) και από τότε διαδόθηκε ευρύτερα και συμπεριλήφθηκε στην έρευνα στον τομέα της πληροφορικής και των υπολογιστών.

Επικρατεί η θεώρηση πως την εμφάνιση των πρώτων υπολογιστών διαδέχτηκε το ηλεκτρονικό έγκλημα. Η ανάπτυξη του ηλεκτρονικού εγκλήματος τοποθετείται χρονικά τις δεκαετίες των 1940-1960 όταν σταδιακά το ευρύ κοινό άρχισε να κατανοεί τις δυνατότητες και τη χρησιμότητα των υπολογιστών θεωρώντας τους δε «περιστασιακά αναξιόπιστους», αλλά «συνήθως ασφαλείς» (Dunlop C. et al, 1991). Στο σημείο αυτό αξίζει να αναφερθεί πως παλαιότερες μελέτες ανέφεραν ότι το ηλεκτρονικό έγκλημα πρωτίστως κατευθύνθηκε σε τομείς του εμπορίου, του στρατού και της τραπεζικής στην αρχή του 1950.

Ωστόσο, η πρώτη τεκμηριωμένη κατάχρηση υπολογιστή, η οποία περιελάμβανε την αλλοίωση τραπεζικών αρχείων, συνέβη το 1958 (Li X.Z.,2017). Την περίοδο αυτή η κατασκευή, η εγκατάσταση

και η συντήρηση ενός υπολογιστή αποτελούσε μια κοστοβόρα και επίπονη διαδικασία. Ωστόσο, κατά τη διάρκεια αυτού του σταδίου, το ηλεκτρονικό έγκλημα εμφανίστηκε σποραδικά σε ένα περιορισμένο αριθμό υπολογιστών που χρησιμοποιούνταν

Στη φάση αυτή η νομοθεσία δεν είχε προβλέψει κάποιο αντίμετρο κατά του φαινομένου, αφήνοντας τους αρμόδιους θεσμούς και τις αρχές επιβολής του νόμου να το αντιμετωπίσουν εντός του τυπικού παραδοσιακού νομικού πλαισίου. Άλλωστε ο περιορισμένος αριθμός των υπολογιστών άφηνε περιθώρια χρήσης από τρίτους χωρίς το φαινόμενο να λαμβάνεται σοβαρά υπόψιν (Li X.Z.,2017).

Αργότερα, στη δεκαετία του 1980, περισσότεροι υπολογιστές ήταν ευρέως διαθέσιμοι και έτσι δεν μπορούσε να δικαιολογηθεί η ανάγκη να γίνεται χρήση υπολογιστών από τρίτους. Επομένως, η μη εξουσιοδοτημένη χρήση υπολογιστών θεωρήθηκε και επίσημα καταχρηστική και το φαινόμενο άρχισε να λαμβάνει και νομική υπόσταση. Παράλληλα το κόστος αγοράς και εγκατάστασης των συστημάτων άρχισε να μειώνεται, η γνώση γύρω από τους υπολογιστές άρχισε να διαχέεται και έτσι άρχισε να εμφανίζεται ένας ολοένα αυξανόμενος αριθμός χάκερ με διάφορα κίνητρα και παρουσιάστηκε μια αύξηση σε μεμονωμένα περιστατικά επιθέσεων (Li X.Z.,2017).

Σημαντικά γεγονότα που καθόρισαν την εξέλιξη της ψηφιακής εγκληματολογίας ήταν η δημιουργία της ομάδας Computer Analysis and Response Team (CART) του FBI το 1984 που ασχολήθηκε με τα ψηφιακά αποδεικτικά στοιχεία. Λίγα χρόνια μετά, το 1990 αναπτύχθηκαν τα πρώτα εργαλεία της ψηφιακής εγκληματολογίας, όπως το Encase και σηματοδοτήθηκε η εξέλιξη της επιστήμης αυτής. Στην δεκαετία του 2000-2010 το λειτουργικό σύστημα των Windows κατάφερε να γίνει το κύριο και κοινό λειτουργικό σύστημα διευκολύνοντας έτσι την ψηφιακή εγκληματολογία. Με την πρόοδο της τεχνολογίας άρχισαν παράλληλα να αναδύονται οι παράνομες δραστηριότητες καθώς και η διακίνηση ύποπτου υλικού ενώ σήμερα οι ψηφιακές συσκευές μπορούν να αποθηκεύουν τεράστιο όγκο δεδομένων από όπου δύναται κανείς να αποσπάσει στοιχεία. (Κασούμης Ν.,2014)

3.2 Διεθνές και Ευρωπαϊκό Νομοθετικό πλαίσιο

Όπως προαναφέρθηκε, όταν αναδύθηκε το ηλεκτρονικό έγκλημα στις δεκαετίες 1940-1960 δεν υπήρχε διαθέσιμος κάποιος νόμος ώστε να αντιμετωπίσει τέτοιες περιπτώσεις (Chen, 1990). Έτσι εφαρμόζονταν περιστασιακά οι παραδοσιακοί νόμοι για να καλύψουν το νομοθετικό κενό. Άλλωστε το

ηλεκτρονικό έγκλημα δεν είχε ακόμη διευκρινιστεί, πολλώ δε μάλλον καθοριστεί σε σαφή πλαίσια. Στις αρχές της δεκαετίας του 1970, οι περισσότερες ανεπτυγμένες χώρες εισήγαγαν νόμους που ποινικοποιούσαν το ψηφιακό έγκλημα και η νομοθεσία επεκτάθηκε το 1980 σε άλλες χώρες. Οι χώρες κατέβαλαν κάθε προσπάθεια για να προβλέψουν και να αντιμετωπίσουν νομικά το ψηφιακό έγκλημα, ωστόσο οι νόμοι ήταν συχνά αναποτελεσματικοί, (Dierks, 1993) καθώς ο αριθμός και η περιπλοκότητα των επιθέσεων αυξανόταν.

Η δυσκολία όμως δεν περιορίστηκε μόνο στη ραγδαία αύξηση των χακερς στην σταδιακή αύξηση της πολυπλοκότητας των επιθέσεων και των ενδεχόμενων κενών στη νομοθεσία. Κατά την παράλληλη ανάπτυξη και εξέλιξη της ψηφιακής εγκληματολογίας άρχισαν να υπάρχουν προβλήματα σχετικά με την ποιότητα και σχετικότητα των ψηφιακών αποδεικτικών στοιχείων. Όπως αναφέρεται από τους Goodison S.E. et al. (2015) για να είναι αποδεκτά στο δικαστήριο τα ψηφιακά αποδεικτικά στοιχεία, πρέπει να είναι συναφή, ουσιώδη και έγκυρα και η αποδεικτική τους αξία θα πρέπει να υπερβαίνει κάθε επίσημο ενδεχόμενο αποτέλεσμα.

Επειδή τα ψηφιακά αποδεικτικά στοιχεία μπορούν εύκολα να αναπαραχθούν και να τροποποιηθούν, συχνά χωρίς να αφήνουν ίχνη, παρουσιάζουν ειδικά προβλήματα που σχετίζονται με την ικανότητα να γίνονται αποδεκτά από το δικαστήριο. Για το λόγο αυτό, τα ψηφιακά αποδεικτικά στοιχεία οφείλουν να υποβάλλονται σε ειδικές δοκιμές. Τα στοιχεία γίνονται αποδεκτά μόνο εάν η επιστημονική κοινότητα και επιστήμονες με εξειδικευμένες γνώσεις και εμπειρογνώμονες αποδέχονταν γενικά τις επιστημονικές αρχές στις οποίες βασίστηκε η συλλογή, η αποθήκευση και η ανάλυσή τους (Ryan D.J. et al. 2002).

Έτσι προτάθηκαν διάφορες υποθέσεις που πρέπει να ληφθούν υπόψη. Αν οι θεωρίες και οι τεχνικές που χρησιμοποιούνται από τους εμπειρογνώμονες έχουν δοκιμαστεί, εάν υπάρχουν δημοσιεύσεις που έχουν υποβληθεί σε αξιολόγηση από ομότιμους, εάν οι τεχνικές που χρησιμοποιεί ο εμπειρογνώμονας έχουν γνωστό ποσοστό σφάλματος, εάν υπόκεινται σε γνωστά πρότυπα και εάν οι θεωρίες και οι τεχνικές που χρησιμοποιούνται απολαμβάνουν ευρεία αποδοχή. Ωστόσο αυτές οι υποθέσεις είναι ενδεικτικές και δεν αποτελούν από μόνες τους μια λίστα απαραίτητων στοιχείων που οφείλει να καλυφθεί.

Τα ψηφιακά πειστήρια οφείλουν τυπικά να πληρούν τις εξής προϋποθέσεις: πρέπει να είναι σχετικά, αναμφισβήτητα και πρέπει να ακολουθούν κάποια επιστημονική μέθοδο και να υποστηρίζονται από κατάλληλη επικύρωση. Ειδικότερα, οι υπολογιστές σήμερα έχουν τη δυνατότητα να αποθηκεύουν και να διαχειρίζονται τεράστιες ποσότητες δεδομένων και εκεί εστιάζει ένα ακόμη πρόβλημα το οποίο αφορά στον ορθό εντοπισμό των ψηφιακών στοιχείων μέσα στην πληθώρα πληροφοριών χωρίς να ανοιχτούν (Ryan D.J. et al. 2002).

Τα ψηφιακά πειστήρια θα πρέπει να «παγώνουν» (freeze) πριν το άνοιγμά τους ώστε να μην αλλοιωθούν τα δεδομένα και τελικά να μην ακυρώνεται η ακεραιότητα τους κατά το δικαστήριο. Για το λόγο αυτό προτάθηκαν κατευθυντήριες γραμμές όπως αυτές αναφέρθηκαν στη διεθνή διάσκεψη εγκλήματος το 1999: «Κατά την κατάσχεση ψηφιακών στοιχείων, δεν πρέπει να πραγματοποιηθεί οποιαδήποτε τροποποίηση τους. Ακόμη όταν είναι απαραίτητο ένα άτομο να έχει πρόσβαση σε αυθεντικά ψηφιακά αποδεικτικά στοιχεία τότε αυτό το άτομο πρέπει να έχει σχετική κατάρτιση στη διαχείριση των στοιχείων. Όλες οι δραστηριότητες που σχετίζονται με την κατάσχεση, την πρόσβαση, την αποθήκευση ή τη μεταφορά ψηφιακών αποδεικτικών στοιχείων πρέπει να είναι πλήρως τεκμηριωμένες, καταγεγραμμένες και διαθέσιμες για τυχόν έλεγχο. Ένα άτομο είναι υπεύθυνο για όλες τις ενέργειες που έχουν αναληφθεί σε σχέση με τα ψηφιακά στοιχεία όσο αυτά βρίσκονται στην κατοχή τους. Οποιοσδήποτε οργανισμός είναι υπεύθυνος για την κατάσχεση, την πρόσβαση, την αποθήκευση ή τη μεταφορά ψηφιακών αποδεικτικών στοιχείων είναι υπεύθυνος για τη συμμόρφωση σε αυτές τις οδηγίες και αναφέρεται στις αρμόδιες αρχές.» (Strydom L.,2001)

Στο σημείο αυτό είναι σημαντικό να αναφερθεί πως ζητήματα προσωπικών δεδομένων και απορρήτου θα πρέπει να λαμβάνονται υπόψη κατά τη διαδικασία της αναζήτησης, αποθήκευσης και παρουσίασης των ψηφιακών αποδεικτικών στοιχείων καθώς σύμφωνα με τον Mugisha D. (2019) το απόρρητο είναι σημαντικό για κάθε οργανισμό ή υποκείμενο. Σε πολλές περιπτώσεις μπορεί να απαιτείται ο εμπειρογνώμονας να μοιράζεται τα δεδομένα θέτοντας σε κίνδυνο το απόρρητο με σκοπό να προσεγγίσει την αλήθεια. Συνοπτικά σε Ευρωπαϊκό επίπεδο, το 2000 υιοθετήθηκε ο χάρτης θεμελιωδών δικαιωμάτων και στο άρθρο 8 κατοχυρώνεται η προστασία των προσωπικών δεδομένων. Επιπροσθέτως θεσπίστηκε και ο κανονισμός γενικής προστασίας δεδομένων ο οποίος επεκτείνει τα δικαιώματα των ατόμων όσον αφορά τη συλλογή και επεξεργασία των προσωπικών τους δεδομένων στην Ευρώπη από το 2018 και στην Ελλάδα. (GDPR,2016)

4

Μελλοντικές Τάσεις Στο Ηλεκτρονικό Έγκλημα

4.1 Το μέλλον του Ηλεκτρονικού Εγκλήματος

Διαθέσιμα στοιχεία δείχνουν ότι τα ποσοστά του ψηφιακού εγκλήματος αυξάνονται αντιστρόφως ανάλογα από τα παραδοσιακά εγκλήματα που εκτελούνται δια ζώσης (Tcherni et al. 2016). Μια σημαντική πρόκληση για τους μελετητές διαχρονικά είναι η έλλειψη επίσημων στατιστικών για τις περισσότερες μορφές εγκλήματος στον κυβερνοχώρο. Ακόμη και στις Ηνωμένες Πολιτείες δεν παρέχονται ολοκληρωμένες πληροφορίες σχετικά με το ηλεκτρονικό έγκλημα ή κατά πόσο εμπλέκεται μια οποιαδήποτε μορφή τεχνολογίας στην διάπραξη ενός εγκλήματος. (Bossler A. et al, 2019)

Η πεποίθηση είναι πως καθώς οι υπολογιστές γίνονται μικρότεροι, γρηγορότεροι και φθηνότεροι θα εγκιβωτίζονται σε όλο και πολυπλοκότερα συστήματα με τρόπους που δεν είναι πάντα προφανείς δίνοντας έτσι νέες διαστάσεις στην αναζήτηση, τη συλλογή, την αποθήκευση και την ανάλυση πληροφοριών. Συγκεκριμένα, το λογισμικό είναι δυνατό να ενσωματώνεται πλέον σε μέσα μετακίνησης, σε εργαλεία, σε οικιακές συσκευές και μηχανήματα, σε τηλεπικοινωνιακά συστήματα ακόμη και στο ανθρώπινο σώμα. Κατά συνέπεια, τα ψηφιακά αποδεικτικά στοιχεία μπορούν να προκύψουν σε απροσδόκητα μέρη από ποικίλες πηγές ανοίγοντας ίσως νέους δρόμους στην έρευνα για το ηλεκτρονικό έγκλημα, την ψηφιακή εγκληματολογία και οδηγώντας τις εξελίξεις στις νομοθετικές ρυθμίσεις. (Ryan D.J. et al. 2002).

4.2 Ερευνητικές Τάσεις

Στη σημερινή ψηφιακή εποχή, οι τεχνολογικές καινοτομίες έχουν διευκολύνει σημαντικά την καθημερινή ζωή και η τεχνολογία καθώς και η πληροφορία είναι πλέον πάντα παρούσες και διαθέσιμες. Την άνθηση της τεχνολογίας ακολούθησε και η ανάπτυξη του ψηφιακού εγκλήματος το οποίο έχει λάβει ανησυχητικές διαστάσεις παγκοσμίως. Κατά τους Sarre R. et al. (2018) η έρευνα που απαιτείται στο πεδίο αυτό οφείλει να συνεχιστεί. Για το σκοπό αυτό πρέπει να υιοθετηθεί μια διεπιστημονική προσέγγιση ώστε περισσότεροι ακαδημαϊκοί να συμβάλλουν στην πρόληψη του ψηφιακού εγκλήματος (Sarre R, et al. 2018).

Η ψηφιακή εγκληματολογία είναι ένας επιστημονικός τομέας όπου χρειάζεται να αναπτυχθούν και να αξιοποιηθούν κατάλληλα τεχνολογικά εργαλεία καθώς και διαδικασίες. Οι τεχνικές προκλήσεις περιλαμβάνουν την πολυπλοκότητα και την ετερογένεια στις ψηφιακές πηγές που αφορούν κυρίως στις διαφορετικές πλατφόρμες, ποικίλες εφαρμογές και δρομολογητές (Μήτρου Λ., nd). Επιπρόσθετα, η ανάκτηση ψηφιακών αποδεικτικών στοιχείων ειδικότερα μέσω του Διαδικτύου συχνά συνοδεύεται από προκλήσεις αναφορικά με τη διεξαγωγή αναλύσεων χρονοδιαγράμματος σε δεδομένα που συλλέγονται.

Επιπλέον, χρειάζονται ισχυρά, αξιόπιστα και έξυπνα συστήματα τα οποία είναι ικανά να αποθηκεύσουν και να αναλύσουν ένα μεγάλο όγκο δεδομένων. Μια άλλη πρόκληση που αφορά στον μεγάλο όγκο δεδομένων είναι η ορθή επιλογή και συσχέτιση των στοιχείων. Σήμερα, για τη διευκόλυνση της ανάλυσης, χρησιμοποιούνται συχνά τεχνικές εξόρυξης δεδομένων. Ένα ακόμα τεχνικό ζήτημα που καλούνται οι επιστήμονες να αντιμετωπίσουν είναι η συγχρονικότητα της συλλογής των δεδομένων με την παράλληλη λειτουργία των υπολογιστών. Σε αυτές τις περιπτώσεις, η διεξαγωγή μιας "ζωντανής" διαδικασίας αναζήτησης και ανάκτησης στοιχείων συνεπάγεται ακόμη μεγαλύτερες τεχνικές προκλήσεις (Sumathi S., et al.2006).

Ακόμη, ο μεγάλος όγκος δεδομένων σε συνδυασμό με τα εργαλεία εξόρυξης δεδομένων και κειμένου αυξάνουν τον κίνδυνο συλλογής δεδομένων για δευτερεύοντες και συχνά άσχετους ή

ακατάλληλους σκοπούς με αποτέλεσμα να ανακύπτουν ζητήματα προσωπικών δεδομένων και απορρήτου (Μήτρου Λ., nd).

Όπως αναφέρθηκε πρωτύτερα, η ψηφιακή εγκληματολογία αντιμετωπίζει προκλήσεις οι οποίες προέρχονται από την ταχύτατη εξέλιξη της τεχνολογίας, την αφθονία των διαθέσιμων πηγών και τον μεγάλο όγκο των δεδομένων, την διάδοση του ψηφιακού εγκλήματος και την έλλειψη καταρτισμένου και εξειδικευμένου προσωπικού στις νέες αναδυόμενες τεχνολογίες και στις νέες τάσεις του κυβερνοεγκλήματος. Πιο συγκεκριμένα οι Khatter K et al (2017) αναφέρουν πως τα σημαντικότερα προβλήματα αφορούν πέντε άξονες: την τεχνολογία cloud, την κρυπτογράφηση, την έλλειψη πόρων και κατάρτισης, τον αυξανόμενο όγκο πηγών και δεδομένων και την αύξηση των ψηφιακών εγκλημάτων. Οι ερευνητές καταδεικνύουν προβλήματα που προκύπτουν στην ψηφιακή εγκληματολογία που ασχολείται με την τεχνολογία cloud καθώς σε αντίθεση με το παραδοσιακό εγκληματολογικό σχήμα όπου τα δεδομένα αποθηκεύονται σε μια καθορισμένη συσκευή, τα δεδομένα στο cloud αποθηκεύονται σε διαφορετικούς κόμβους γεγονός το οποίο επιβαρύνει το έργο των ερευνητών. Σχετικά με την κρυπτογράφηση, οι ερευνητές παρουσιάζουν χαρακτηριστικά παραδείγματα που αναφέρονται στην διαφορετικότητα ευκολίας συλλογής και ανάλυσης από διαφορετικές συσκευές ανάλογα με το επίπεδο κρυπτογράφησης. Ακόμη, αναλογιζόμενοι την πληθώρα πηγών οι ερευνητές αναφέρουν ότι οι εξοπλισμοί για κινητά και IoT χρησιμοποιούν μια σειρά λειτουργικών συστημάτων, προδιαγραφών και ρυθμίσεις αρχείων, οι οποίες με τη σειρά τους αυξάνουν την πολυπλοκότητα των ερευνών. Τέλος, αναφερόμενοι στην έλλειψη πόρων και κατάρτισης οι ερευνητές προτείνουν τη διαμόρφωση βασικών προγραμμάτων εκπαίδευσης από τους αρμόδιους φορείς.

Κατά τους Stoyanova M. Et al (2020), το μέλλον θα φέρει σημαντική ανάπτυξη σε τεχνολογικούς τομείς οι οποίοι με τη σειρά τους θα επηρεάσουν την ψηφιακή εγκληματολογία. Ειδικότερα αναφέρεται πως η ψηφιακή εγκληματολογία μελλοντικά θα συμβαδίσει με την εξέλιξη του IoT το οποίο βρίσκει εφαρμογή σε πολλαπλούς τομείς της καθημερινότητας και της οικονομικής ζωής όπως στις αλυσίδες εφοδιασμού, στη μηχανική, στο εμπόριο ακόμα και στην υγεία. Ωστόσο, υπάρχουν ακόμη τεχνολογικοί περιορισμοί οι οποίοι θα πρέπει να αρθούν όπως η ποικιλομορφία των αρχείων, η μη πλήρης συμβατότητα των συστημάτων, καθώς και η πολυπλοκότητα των κρυπτογραφικών τεχνικών.

Ακόμη, οι νεότερες συσκευές IoT δεν υποστηρίζονται από τα υπάρχοντα εγκληματολογικά εργαλεία, καθιστώντας τη διαδικασία εξαγωγής δεδομένων ακόμη πιο δύσκολη. Μια άλλη παράμετρος η οποία καθυστερεί την εξέλιξη της ψηφιακής εγκληματολογίας είναι η ανωνυμία. Παρόλο που οι τεχνικές ανωνυμοποίησης είναι νόμιμα εργαλεία για την προστασία της ιδιωτικής ζωής, είναι γεγονός πως χρησιμοποιούνται συχνά από εγκληματίες για να ελαχιστοποιηθεί ο κίνδυνος εντοπισμού. Ένας ακόμη παράγοντας είναι η ποσότητα υλικού που προωθείται καθημερινά στο διαδίκτυο καθιστώντας δύσκολο των εντοπισμό ψηφιακών πειστηρίων μέσα σε έναν μεγάλο όγκο πληροφορίας καθώς ο αριθμός των διασυνδεδεμένων συσκευών που παράγουν πληροφορία αναμένεται να φτάσει τα 25 δισεκατομμύρια έως το 2021 (Stoyanova M. Et al 2020).

Στο μέλλον, το Διαδίκτυο των Πραγμάτων το οποίο θα περιγράφει το συγκεκριασμό και τη διασύνδεση δεδομένων, συσκευών, ανθρώπων και διαδικασιών θα καταστήσει δυσκολότερες τις διαδικασίες της ψηφιακής εγκληματολογίας γεγονός το οποίο θα εντείνει την ανάγκη για περισσότερο δυναμικές εγκληματολογικές πρακτικές. Οι εξελίξεις αυτές θα οδηγήσουν στη συνέργια τεχνικών και μεθόδων όπως οι αλγόριθμοι ανάλυσης μεγάλων δεδομένων (Big Data), η προγνωστική ανάλυση AI (predictive analytics), η προσαρμοστική συλλογή δεδομένων (adaptive data collection) κά. με διαδικασίες εστιασμένες στην ιδιωτικότητα (Stoyanova M. Et al 2020).

Εκ των ανωτέρω γίνεται αντιληπτό πως η ψηφιακή εγκληματολογία επεκτείνεται σε ένα ευρύ φάσμα ζητημάτων που πρέπει να αντιμετωπιστούν διεπιστημονικά και τα οποία καλύπτουν όχι μόνο τεχνικές αλλά κοινωνικές, διαδικαστικές και νομικές πτυχές (Μήτρου Λ., nd).

Στο επόμενο κεφάλαιο θα παρουσιαστεί η σταδιοποίηση των διαδικασιών που ακολουθούνται στην ψηφιακή εγκληματολογία και έχουν προκύψει από συνεχείς μελέτες. Στο εν λόγω κεφάλαιο προτείνονται βελτιστοποιημένες διαδικασίες κατά τη βιβλιογραφία οι οποίες αποτελούνται από φάσεις που έχουν οριστεί από τους επιστήμονες ερευνητές.

5

Σταδιοποίηση Των Διαδικασιών Στην Ψηφιακή Εγκληματολογική Έρευνα

Όπως αναφέρθηκε σε προηγούμενα κεφάλαια, η ψηφιακή εγκληματολογία είναι η επιστήμη που εφαρμόζει τεκμηριωμένες μεθόδους, διαδικασίες και εργαλεία και αφορά στη διερεύνηση επιθέσεων ή εγκλημάτων που πραγματοποιούνται εξ ολοκλήρου ή τελούνται με τη βοήθεια της ψηφιακής τεχνολογίας όπως είναι οι υπολογιστές, τα κινητά τηλέφωνα, οι αισθητήρες, διάφορες έξυπνες συσκευές που συνδέονται στο διαδίκτυο κ.λπ. Η διαδικασία της ψηφιακής εγκληματολογίας εκκινεί από την αρχική ειδοποίηση για την ύπαρξη ενός υπό διερεύνηση συμβάντος και ολοκληρώνεται με την σύνταξη και την πλήρη αναφορά των ευρημάτων. Η διαδικασία που ακολουθείται έχει μελετηθεί πολλάκις κατά το παρελθόν και ακόμη και σήμερα παρουσιάζονται νέες βελτιστοποιημένες διαδικασίες οι οποίες αποτελούνται από φάσεις που έχουν οριστεί από τους επιστήμονες ερευνητές.

Με την πρώτη εμφάνιση της ψηφιακής εγκληματολογίας ένα από τα πιο κρίσιμα ζητήματα που ανέκυψαν ήταν ο καθορισμός ενός μοντέλου διεργασιών ώστε να καθίσταται ολόκληρη η διερευνητική διαδικασία συνεπής και τυποποιημένη. Για το λόγο αυτό, ορίστηκαν ορισμένα γενικά μοντέλα τα περισσότερα εκ των οποίων ορίζουν μια ομάδα απαραίτητων βημάτων σε μια ολόκληρη διαδικασία διερεύνησης. Τα πρώτα μοντέλα βελτιώθηκαν με την πάροδο του χρόνου ενώ τα μεταγενέστερα συνεχίζουν να βελτιώνονται συμπεριλαμβάνοντας μερικά επιπλέον βήματα. (Du X et al, nd)

Παρουσιάζοντας συνοπτικά τη διαδικασία που ακολουθείται στην ψηφιακή εγκληματολογία θα πρέπει να αναφερθεί πρωτίστως πως τα ψηφιακά μέσα πριν από την εξέταση των εμπειρογνομόνων οφείλουν να κατασχεθούν με ορισμένες διαδικασίες οι οποίες θα έχουν εγκριθεί από τους αρμόδιους φορείς ενώ η κατάσχεση σε ποινικές υποθέσεις πραγματοποιείται από το προσωπικό επιβολής του νόμου το οποίο είναι καταρτισμένο και εκπαιδευμένο σε τεχνικά ζητήματα ώστε να διασφαλιστεί η προστασία των αποδεικτικών στοιχείων ακολουθώντας τις νομοθετικές διατάξεις. (Du X et al, nd)

Μόλις κατασχεθούν οι πηγές και τα επιμέρους στοιχεία, δημιουργείται ένα ακριβές αντίγραφο των υπό διερεύνηση μέσων χρησιμοποιώντας εργαλεία αναπαραγωγής σκληρού δίσκου ή εργαλεία απεικόνισης λογισμικού τα οποία θα αναπτυχθούν εκτενώς σε επόμενο κεφάλαιο. Αργότερα, η αρχική μονάδα επιστρέφεται σε ασφαλή χώρο αποθήκευσης για την αποφυγή παραβίασης ή αλλοίωσης.

Στη συνέχεια επιχειρείται η ανάκτηση των στοιχείων κατά την οποία χρησιμοποιούνται διάφορες μέθοδοι που συνήθως περιλαμβάνουν είτε κάποια μορφή αναζήτησης λέξεων-κλειδιών από το αρχείο εικόνας που αποκτήθηκε, είτε κάποιων σχετικών φράσεων για τον εντοπισμό αντιστοιχιών.

Σε επόμενο στάδιο, αναλύονται τα περιεχόμενα των αρχείων και του σκληρού δίσκου για να εντοπιστούν στοιχεία που είτε υποστηρίζουν είτε έρχονται σε αντίθεση με μια υπόθεση ή για να προσδιοριστούν σημάδια παραβίασης που αποσκοπούν στην απόκρυψη δεδομένων. Σε κρίσιμα σημεία καθ' όλη τη διάρκεια της ανάλυσης, τα μέσα επαληθεύονται ξανά για να διασφαλιστεί ότι τα αποδεικτικά στοιχεία είναι ακόμη στην αρχική τους κατάσταση. Κατά τη διάρκεια της ανάλυσης, ένας ερευνητής ανακτά συνήθως αποδεικτικό υλικό χρησιμοποιώντας διαφορετικές μεθοδολογίες και εργαλεία, και προχωρά σε ανάκτηση διαγραμμένου υλικού το οποίο εφόσον εντοπιστεί μπορεί να ανακατασκευαστεί. Ο τύπος των δεδομένων που ανακτώνται ποικίλλει ανάλογα με την έρευνα, και συνήθως πρόκειται για email, αρχεία καταγραφής συνομιλιών, εικόνες, ιστορικό διαδικτύου ή έγγραφα.

Μόλις αναλυθούν οι πληροφορίες γίνεται ανασυγκρότηση γεγονότων ώστε οι ερευνητές να καταλήξουν σε συμπεράσματα. Οι ερευνητές, ιδίως σε ποινικές υποθέσεις, πρέπει να διασφαλίσουν ότι

τα συμπεράσματα βασίζονται σε σχετικά με την υπόθεση, ορθά δεδομένα και στις δικές τους ειδικές γνώσεις.

Τέλος, όταν ολοκληρωθεί μια έρευνα, οι πληροφορίες αποτυπώνονται συχνά σε κατάλληλη μορφή ώστε να γίνουν κατανοητές και σε άτομα χωρίς ισχυρό τεχνικό υπόβαθρο. Οι αναφορές μπορεί επίσης να περιλαμβάνουν κάποιες πληροφορίες ελέγχου, ορισμένα πρωτόκολλα, τη μεθοδολογία που εφαρμόστηκε, τα εργαλεία που χρησιμοποιήθηκαν κλπ. Όταν ολοκληρωθούν, οι αναφορές διαβιβάζονται συνήθως σε όσους αναθέτουν την έρευνα ώστε να αποφασίσει εάν θα χρησιμοποιηθούν τα αποδεικτικά στοιχεία στο δικαστήριο.

Η εξέλιξη της ψηφιακής εγκληματολογικής έρευνας ακολουθεί συνήθως την πορεία που συνοπτικά παρουσιάστηκε και δε δύναται να διαφέρει σημαντικά από την αρχή έως το τέλος. Ωστόσο κάθε έρευνα διαφέρει ανάλογα με τις μεθόδους που εφαρμόζονται, τα εργαλεία που χρησιμοποιούνται και τις φάσεις που έχουν οριστεί κατά την ψηφιακή εγκληματολογική διαδικασία και ακολουθούνται από τους ερευνητές.

Μια τυπική μεθοδολογία στην έρευνα του πεδίου της ψηφιακής εγκληματολογίας αποτελείται από μια ακολουθία απαραίτητων ενεργειών. Σύμφωνα με τους Du X et al (nd) ένα μοντέλο διαδικασιών εάν είναι πολύ απλοϊκό ενδέχεται να μην παρέχει μεγάλη καθοδήγηση κατά την έρευνα ενώ ένα μοντέλο με περισσότερες φάσεις μπορεί να αποδειχθεί πιο χρήσιμο. Ακόμα κι αν είναι σχεδόν αδύνατο να σχεδιαστεί ένα τέλειο μοντέλο διεργασίας που να προσαρμόζεται σε οποιαδήποτε έρευνα, ένα ιδανικό πλαίσιο θα πρέπει να είναι γενικό, πράγμα που σημαίνει ότι θα μπορούσε να εφαρμοστεί σε όσο το δυνατόν περισσότερες περιπτώσεις. Επιπλέον, δεδομένου ότι οι τεχνικές εξελίσσονται τόσο γρήγορα, ένα καλά καθορισμένο μοντέλο θα πρέπει επίσης να έχει την ικανότητα να υιοθετεί νέες τεχνικές στη διαδικασία της έρευνας.

Αφού ορίστηκε σαφώς η γενική διαδικασία, οι ερευνητές άρχισαν να εργάζονται σε συγκεκριμένα θέματα. Για παράδειγμα: 1) τη βελτιστοποίηση ενός μοντέλου διεργασίας και ενός συγκεκριμένου βήματος της έρευνας, 2) την ενασχόληση μόνο με μια συγκεκριμένη κατηγορία περιπτώσεων, όπως τα εγκλήματα στον κυβερνοχώρο, τη χρήση των κινητών συσκευών στις εγκληματικές ενέργειες κ.λπ., 3) την ανάπτυξη των μοντέλων Triage (Hitchcock et al. 2016) τα οποία περιγράφουν συγκεκριμένα

μοντέλα διαδικασιών για περιπτώσεις ευαίσθητες στο χρόνο, όπως οι απαγωγές παιδιών, οι περιπτώσεις αγνοουμένων κ.λπ.

Πιο αναλυτικά, οι μελέτες στον τομέα της ψηφιακής εγκληματολογίας που μπορούν να αναζητηθούν κατά τη βιβλιογραφική επισκόπηση στις μηχανές αναζήτησης βρίθουν αναλύσεων που σχετίζονται με μοντέλα και αναπτύσσουν τις διάφορες φάσεις στις διαδικασίες που ακολουθούνται κατά την ψηφιακή εγκληματολογική έρευνα.

Οι Du X et al (nd) επιχείρησαν να παρουσιάσουν μια αξιολόγηση των μοντέλων διαδικασιών στην ψηφιακή εγκληματολογία. Σύμφωνα με τη μελέτη, προέκυψε ότι έχουν προταθεί πολυάριθμα μοντέλα διεργασιών με το κάθε ένα από αυτά προσπαθεί να βελτιώσει τη βασική μεθοδολογία ώστε να εξατομικευτεί σε μια συγκεκριμένη περίπτωση χρήσης παρόλο που κάθε ένα από τα υπό μελέτη μοντέλα ακολουθούν την ίδια φιλοσοφία προσέγγισης.

Σύμφωνα με τους Du X et al (nd) αρκετά μοντέλα επεξεργασίας έχουν προταθεί μέχρι σήμερα και μπορούν να κατηγοριοποιηθούν σε τρεις βασικούς τύπους:

- Γενικά μοντέλα που ορίζουν ολόκληρη τη διαδικασία της ψηφιακής εγκληματολογικής έρευνας. Αυτά τα μοντέλα προτάθηκαν από το 2000 έως το 2010. Μέχρι εκείνη τη στιγμή δεν υπήρχαν ξεκάθαρες οδηγίες σχετικά με το τι πρέπει να γίνει και τι βήματα πρέπει να ακολουθηθούν.
- Ένα συγκεκριμένο βήμα στη διαδικασία της έρευνας ή ένα συγκεκριμένο είδος της υπόθεσης.
- Καθορισμός νέων προβλημάτων ή / και διερεύνηση νέων μεθόδων ή εργαλείων για την αντιμετώπιση συγκεκριμένων ζητημάτων.

Συμπερασματικά, ο πρώτος τύπος εστιάζει σε ένα γενικό μοντέλο που καλύπτει ολόκληρη τη διαδικασία της έρευνας, ο δεύτερος τύπος βελτιώνει τα προηγούμενα μοντέλα καθώς προάγει τη συμβατότητα με περισσότερες καταστάσεις και ο τρίτος τύπος χρησιμοποιεί νέες μεθόδους, τεχνικές και / ή εργαλεία στη διερευνητική διαδικασία για την αντιμετώπιση νέων προβλημάτων που συναντώνται στις σύγχρονες έρευνες

Άλλες έρευνες καταγράφουν τα μοντέλα βάσει χρονολογικής σειράς καθώς και σε σύγκριση των φάσεων που ακολουθούνται από τους ερευνητές χωρίς ωστόσο να προχωρούν σε αξιολόγησή τους. Συγκεκριμένα οι Yusoff Y et al (2011) συμπεριέλαβαν στη μελέτη τους ενδεικτικά ένα μοντέλο κατά έτος χωρίς όμως τα μοντέλα που συμπεριέλαβαν να πρόκειται για τα βέλτιστα ή τα καλύτερα μοντέλα από τα υπόλοιπα που προτάθηκαν στην ίδια χρονική περίοδο καθώς στόχος ήταν να εντοπιστούν οι φάσεις στα μοντέλα έρευνας αντί να γίνει αξιολόγηση των μοντέλων αυτών.

Το πρώτο μοντέλο που παρουσιάστηκε στην μελέτη των Yusoff Y et al αφορούσε στο Computer Forensic Investigative Process από τον Pollitt, έργο το οποίο χρονολογήθηκε το 1984. Ο Pollitt (2007) πρότεινε μια μεθοδολογία τεσσάρων φάσεων για τη διερεύνηση των ψηφιακών αποδεικτικών στοιχείων έτσι ώστε τα αποτελέσματα να είναι επιστημονικά αξιόπιστα και νομικά αποδεκτά. Στην πρώτη φάση της συλλογής, τα ψηφιακά αποδεικτικά στοιχεία αποκτήθηκαν μετά από την κατάλληλη έγκριση από την αρμόδια αρχή. Ακολούθησε η δεύτερη φάση της αναγνώρισης με εργασίες για τον προσδιορισμό των ψηφιακών στοιχείων από το σύνολο των συλλεχθέντων στοιχείων και τη μετατροπή τους σε ερμηνεύσιμη μορφή. Η τρίτη φάση της αξιολόγησης περιλάμβανε την αξιολόγηση της σχετικότητας των ψηφιακών πειστηρίων με την υπό διερεύνηση υπόθεση. Στην τελική φάση, τα ψηφιακά αποδεικτικά στοιχεία παρουσιάζονται στο δικαστήριο.

Το 2001, προτάθηκε (Palmer G.,2001) μια διαδικασία έρευνας αποτελούμενη από 6 φάσεις. Το Ερευνητικό Μοντέλο DFRWS ξεκίνησε με μια φάση ταυτοποίησης, στην οποία πραγματοποιήθηκε ανίχνευση προφίλ, παρακολούθηση συστήματος, ανάλυση ελέγχου κ.λπ. και ακολουθήθηκε αμέσως από τη φάση διατήρησης, η οποία περιλαμβάνει τη δημιουργία μιας αποδεκτής αλυσίδας διατήρησης (chain of custody). Στην επόμενη φάση της Συλλογής συλλέγονται σχετικά δεδομένα με τεκμηριωμένες μεθόδους και εργαλεία που χρησιμοποιούν διάφορες τεχνικές ανάκτησης. Μετά από αυτή τη φάση ακολουθούν η φάση της έρευνας/εξέτασης και η φάση ανάλυσης με σκοπό την ανίχνευση και ανάλυση των αποδεικτικών στοιχείων. Η τελευταία φάση σε αυτό το μοντέλο είναι η παρουσίαση.

Το 2002 προτάθηκε ένα βελτιωμένο μοντέλο γνωστό ως Αφηρημένο μοντέλο ψηφιακής εγκληματολογίας (Abstract Digital Forensic Model) (Reith M et al 2002). Σε αυτό το μοντέλο, ο συγγραφέας εισήγαγε τρεις επιπλέον φάσεις, επεκτείνοντας έτσι τον αριθμό των φάσεων σε εννέα. Οι 3 σημαντικές φάσεις που εισήχθησαν σε αυτό το μοντέλο ήταν η προετοιμασία, η στρατηγική

προσέγγισης και η επιστροφή των αποδεικτικών στοιχείων. επιστροφής. Στη φάση Προετοιμασίας, πραγματοποιήθηκαν δραστηριότητες όπως προετοιμασία εργαλείων, προσδιορισμός τεχνικών και λήψη υποστήριξης από τη διαχείριση. Η φάση της στρατηγικής προσέγγισης εισήχθη με στόχο να μεγιστοποιήσει την δυνατότητα ανάκτησης αποδεικτικών στοιχείων και ταυτόχρονα να ελαχιστοποιήσει τυχόν αρνητικές επιπτώσεις στο θύμα και στους γύρω ανθρώπους. Η διαδικασία ολοκληρώνεται με την επιστροφή των αποδεικτικών ώστε να διασφαλιστεί ότι τα αποδεικτικά στοιχεία επιστρέφουν με ασφάλεια στον νόμιμο κάτοχο ή έχουν διατεθεί σωστά.

Η Ολοκληρωμένη διαδικασία ψηφιακής έρευνας (IDIP) προτάθηκε από την Carrier & Spafford το 2003, με σκοπό να συνδυάσει τις διάφορες διαθέσιμες διερευνητικές διαδικασίες σε ένα ολοκληρωμένο μοντέλο. Ο ερευνητής εισάγει την έννοια της ψηφιακής σκηνής εγκληματικότητας που αναφέρεται στο εικονικό περιβάλλον που δημιουργείται από το λογισμικό και το υλικό που υπάρχει ψηφιακή απόδειξη εγκλήματος ή συμβάντος. Η διαδικασία ξεκινάει με μια φάση που απαιτεί η φυσική και επιχειρησιακή υποδομή να είναι έτοιμη να υποστηρίξει οποιαδήποτε μελλοντική έρευνα. Σε αυτήν τη φάση ο εξοπλισμός πρέπει να είναι πάντα έτοιμος και το προσωπικό πρέπει να είναι ικανό να τον χρησιμοποιήσει αποτελεσματικά. Το σημείο αυτό χαρακτηρίζεται επίσης από 2 δευτερεύουσες φάσεις, δηλαδή την ετοιμότητα λειτουργίας και την ετοιμότητα υποδομής. Αμέσως μετά τη φάση ετοιμότητας, βρίσκεται η φάση ανάπτυξης, η οποία παρέχει έναν μηχανισμό για τον εντοπισμό και την επιβεβαίωση ενός συμβάντος. Δύο δευτερεύουσες φάσεις εισάγονται περαιτέρω, δηλαδή η Ανίχνευση/Ειδοποίηση και η Επιβεβαίωση/Εξουσιοδότηση. Οι επιμέρους φάσεις που παρουσιάζονται είναι η Διατήρηση, η Έρευνα, η Τεκμηρίωση, η Αναζήτηση, η Συλλογή, η Ανασυγκρότηση και η Παρουσίαση. Η τελευταία φάση είναι η φάση αναθεώρησης.

Το Βελτιωμένο μοντέλο διαδικασίας της ψηφιακής έρευνας (Enhanced Digital Investigation Process Model), επίσης γνωστό ως EDIP παρουσιάστηκε το 2004 (Baryamereeba V et al 2004). Ξεκινά με τη φάση της Ετοιμότητας και ακολουθεί η δεύτερη φάση, η φάση ανάπτυξης, που παρέχει έναν μηχανισμό εντοπισμού και επιβεβαίωσης του συμβάντος. Αποτελείται από 5 δευτερεύουσες φάσεις, δηλαδή τον Εντοπισμό/Ενημέρωση, την Έρευνα στο Φυσικό χώρο, την Έρευνα στον ψηφιακό χώρο, την Επιβεβαίωση και τέλος την Υποβολή. Μετά τη φάση αυτή ακολουθεί η φάση Traceback. Αυτό γίνεται για να δώσει τη δυνατότητα στον ερευνητή να εντοπίσει τις πραγματικές συσκευές / υπολογιστές που χρησιμοποιεί ο εγκληματίας για την εκτέλεση του εγκλήματος. Υποστηρίζεται από δύο δευτερεύουσες φάσεις, δηλαδή, την Έρευνα και την Εξουσιοδότηση Σκηνών Ψηφιακού

Εγκλήματος. Ακολουθεί η φάση Dynamite όπου σε αυτήν τη φάση, διεξάγονται έρευνες στην πρωτογενή σκηνή του εγκλήματος, με σκοπό τον εντοπισμό του δυνητικού ενόχου και αποτελείται από τέσσερις δευτερεύουσες φάσεις, συγκεκριμένα, την έρευνα σκηνής φυσικού εγκλήματος, την έρευνα ψηφιακής σκηνής εγκλήματος, την ανακατασκευή και την επικοινωνία. Στην υπο-φάση της ανακατασκευής, συλλέγονται κομμάτια πληροφοριών που συλλέγονται έτσι ώστε να δημιουργούνται πιθανά γεγονότα που θα μπορούσαν να είχαν συμβεί. Η υπο-φάση επικοινωνίας είναι παρόμοια με την προηγούμενη φάση υποβολής. Η διαδικασία έρευνας ολοκληρώνεται με τη φάση ετοιμότητας.

Το μοντέλο Διαδικασίας Διαλογής στην ψηφιακή εγκληματολογία (Computer Forensics Field Triage Process Model - CFFTPM) (Rogers M.K. et. al 2006) προτείνει μια προσέγγιση για την ταυτοποίηση, ανάλυση και ερμηνεία των ψηφιακών στοιχείων σε σχετικά σύντομο χρονικό διάστημα χωρίς την ανάγκη να επιστραφούν οι συσκευές ή τα μέσα στο εργαστήριο. Το CFFTPM αποτελείται από 6 πρωτογενείς φάσεις που στη συνέχεια χωρίζονται περαιτέρω σε άλλες έξι υπο-φάσεις. Ο σωστός προγραμματισμός, που αποτελεί την πρώτη φάση πριν από την έναρξη της έρευνας θεωρείται στο μοντέλο αυτό πως θα βελτιώσει το ποσοστό επιτυχίας. Μετά τη φάση του προγραμματισμού συναντάται η φάση Triage/Διαλογή. Σε αυτή τη φάση, τα στοιχεία προσδιορίζονται και κατατάσσονται ως προς τη σημασία ή την προτεραιότητα. Τα πιο σημαντικά και ασταθή αποδεικτικά στοιχεία πρέπει πρώτα να υποβληθούν σε επεξεργασία. Η φάση Προφίλ Χρήστη εστιάζει την προσοχή στην ανάλυση της δραστηριότητας και του προφίλ χρήστη με σκοπό τη συσχέτιση αποδεικτικών στοιχείων με τον ύποπτο. Η οικοδόμηση της υπόθεσης του εγκλήματος από τη χρονολογική προοπτική είναι ο κύριος στόχος της φάσης της Χρονικότητας. Στη φάση του Διαδικτύου, εκτελούνται οι εργασίες εξέτασης των υπηρεσιών που σχετίζονται με το Διαδίκτυο. Τέλος, στη φάση συγκεκριμένων περιστατικών, ο ερευνητής μπορεί να προσαρμόσει το επίκεντρο της εξέτασης στις ιδιαιτερότητες της υπόθεσης.

Το 2009, η Perumal, S. πρότεινε ένα ακόμη μοντέλο έρευνας το DFMMIP, που αποτελείται από επτά φάσεις. Μετά την ολοκλήρωση της πρώτης φάσης του σχεδιασμού, ακολουθεί η επόμενη φάση, της ταυτοποίησης και αργότερα της αναγνώρισης. Προτού αναλυθούν τα δεδομένα, πρέπει να μεταφερθούν με ασφάλεια στον τόπο έρευνας και να αποθηκευτούν σωστά. Αυτό γίνεται στη φάση μεταφοράς και αποθήκευσης. Μόλις τα δεδομένα είναι έτοιμα, ακολουθεί η φάση ανάλυσης όπου τα δεδομένα θα αναλυθούν και θα εξεταστούν χρησιμοποιώντας τα κατάλληλα εργαλεία και τεχνικές. Παρόμοια με τη φάση παρουσίασης στα προηγούμενα μοντέλα, οι ερευνητές θα πρέπει να δείξουν τα αποδεικτικά στοιχεία για να υποστηρίξουν την υπόθεση που παρουσιάστηκε. Αυτό γίνεται στη φάση

απόδειξης. Τέλος, εκτελείται η φάση αποθήκευσης των αρχείων, όπου τα σχετικά αποδεικτικά στοιχεία αποθηκεύονται κατάλληλα για μελλοντικές αναφορές και ίσως μπορούν επίσης να χρησιμοποιηθούν για εκπαιδευτικούς σκοπούς .

Κατά τη βιβλιογραφική ανασκόπηση και συγκρίνοντας τα μοντέλα που παρουσιάστηκαν στη μελέτη, προέκυψε ότι επτά μοντέλα από αυτά που μελετήθηκαν υιοθέτησαν τη φάση της παρουσίας και της ανάλυσης, έξι μοντέλα υιοθέτησαν τη φάση της ταυτοποίησης και της συλλογής, πέντε μοντέλα τη φάση της έρευνας και τέσσερα μοντέλα τις φάσεις της προετοιμασίας και της διατήρησης και τρία μοντέλα τη φάση του σχεδιασμού. Από τις συνολικές 46 φάσεις που εντοπίστηκαν από τους ερευνητές οι 38 υιοθετήθηκαν από λιγότερα από δυο μοντέλα. Συμπερασματικά οι Yusoff Y et al (2011) κατέληξαν σε πέντε φάσεις όπως φαίνεται στον παρακάτω πίνακα.

Generic Phases
1.Pre-Process
1.Acquisition & Preservation
3. Analysis
4. Presentation
5.Post-Process

Πίνακας 1 Οι πέντε φάσεις κατά Yusoff Y et al (2011)

Σύμφωνα με τους Harbawi et al. (2016), η ψηφιακή εγκληματολογία βασίζεται σε διαδικασίες πέντε επιπέδων ξεκινώντας από τον προσδιορισμό και τη συλλογή των ψηφιακών αποδεικτικών στοιχείων και συνεχίζοντας με τη διατήρηση, την έρευνα, την ανάλυση και τέλος την παρουσίαση των ψηφιακών πειστηρίων. Κατά το στάδιο της ανάλυσης οι Khatter K et al (2017) εντόπισαν επιπλέον διαδικασίες οι οποίες θα αναλυθούν περαιτέρω στο παρόν κεφάλαιο αφού παρουσιαστεί πρωτίστως η σταδιοποίηση των διαδικασιών που ακολουθούνται στην ψηφιακή εγκληματολογική έρευνα κατά Harbawi et al. (2016).

5.1 Προσδιορισμός των ψηφιακών πειστηρίων

Το πρώτο στάδιο αναφέρεται στον προσδιορισμό των ψηφιακών αποδεικτικών από ποικίλες πηγές όπως από υπολογιστές, εξωτερικούς σκληρούς δίσκους ή οποιαδήποτε άλλη ηλεκτρονική συσκευή. Οι διαδικασίες που ακολουθούνται για τον προσδιορισμό των ψηφιακών πειστηρίων διαφέρουν αν η ηλεκτρονική συσκευή είναι ενεργή ή απενεργοποιημένη.

5.2 Συλλογή των ψηφιακών πειστηρίων

Κατά το στάδιο αυτό, τα ψηφιακά αποδεικτικά στοιχεία συλλέγονται με τέτοιο τρόπο έτσι ώστε τα δεδομένα που προσδιορίστηκαν να παραμένουν ακέραια και ανέπαφα. Υπάρχουν δυο κύριες μέθοδοι συλλογής δεδομένων οι οποίες εξαρτώνται από τα χαρακτηριστικά και την ποιότητα των δεδομένων αυτών. Στην περίπτωση που είναι σημαντική η σειρά με την οποία συλλέχθηκαν ευμετάβλητα δεδομένα έχει προταθεί μια συγκεκριμένη σειρά καταγραφής δεδομένων ξεκινώντας από τις διαδικτυακές συνδέσεις, την ARP cache, τα login session, τα running processes δηλαδή τις διεργασίες που εκτελούνται στον υπολογιστή, τα open files (τα ανοιχτά αρχεία) και τα περιεχόμενα της μνήμης RAM. Σε ότι αφορά δεδομένα τα οποία δεν πρόκειται να μεταβληθούν άμεσα έχουν προταθεί τρεις διαδικασίες διαχείρισης και συλλογής τα οποία βασίζονται σε εργαλεία τα οποία θα αναπτυχθούν αναλυτικά στο επόμενο κεφάλαιο και συνοπτικά αναφέρονται ως μια συσκευή υλικού όπως το write blocker, το εργαλείο Helix και ένα σύστημα live απόκτησης δεδομένων.

5.3 Διατήρηση των ψηφιακών πειστηρίων

Τα ψηφιακά πειστήρια που συλλέχθηκαν κατά το προηγούμενο στάδιο πρέπει να διατηρούνται ακριβή, ακέραια και ανέπαφα ακόμα και μετά το πέρας της διαδικασίας της έρευνας ώστε να μπορεί να διασφαλιστεί η εγκυρότητα κατά την παρουσίασή τους. Αυτό επιτυγχάνεται μέσω της αλυσίδας διαφύλαξης (chain of custody) που διασφαλίζει ότι τα πρωτότυπα συλλεχθέντα στοιχεία παραμένουν προστατευμένα σε ασφαλή τοποθεσία και καθίστανται αναλλοίωτα από οποιεσδήποτε αλλαγές ενώ οι ειδικοί εργάζονται πάνω σε ειδικά αντίγραφα επί των πρωτοτύπων. Κατά την αλυσίδα διαφύλαξης καταγράφονται τα γεγονότα διακίνησης των ψηφιακών πειστηρίων μεταξύ των εμπειρογνομόνων που εργάζονται διαδοχικά και έχουν εξουσιοδοτημένη πρόσβαση στα στοιχεία.

5.4 Εξέταση και Ανάλυση των ψηφιακών πειστηρίων

Αναφέρεται ως το πιο σημαντικό και τρωτό στάδιο της διαδικασίας, καθώς οποιοδήποτε λάθος ή παράλειψη μπορεί να καταστήσει τα στοιχεία ακατάλληλα για παρουσίαση. Η εξέταση των ψηφιακών πειστηρίων επιβάλλει την ορθή κατηγοριοποίησή τους καθώς και τον κατάλληλο καθορισμό των εργαλείων που θα μπορούσαν να χρησιμοποιηθούν για την ανάλυση τους. Η εγκυρότητα και η αυθεντικότητα των ψηφιακών πειστηρίων θα εξαρτηθούν σε ένα μεγάλο βαθμό από τις διαδικασίες που ακολουθήθηκαν και σε αυτό το στάδιο και σχετίζονται άμεσα με τις ικανότητες και γνώσεις του ειδικού ερευνητή. Στο στάδιο αυτό περιγράφονται ορισμένα βήματα τα οποία ακολουθούνται κατά την ανάλυση των στοιχείων και τα οποία είναι τα παρακάτω:

5.4.1 Επαλήθευση του συμβάντος

Το περιστατικό επαληθεύεται και διερευνώνται συγκεκριμένα χαρακτηριστικά τα οποία θα βοηθήσουν στον καθορισμό της βέλτιστης μεθοδολογίας που θα εφαρμοστεί στο στάδιο της ανάλυσης.

5.4.2 Περιγραφή του συστήματος

Τα δεδομένα που σχετίζονται με το υπό διερεύνηση περιστατικό καταγράφονται και παράλληλα περιγράφεται το σύστημα που θα αναλυθεί, καθώς και τα λειτουργικά και τεχνικά χαρακτηριστικά του όπως η μορφή του δίσκου, η χωρητικότητα της μνήμης RAM και η θέση των ψηφιακών αποδεικτικών στοιχείων.

5.4.3 Ανάλυση του χρονικού πλαισίου

Οι πληροφορίες σχετικά με τη χρονικότητα και την υπόσταση των δεδομένων στη διάρκεια του χρόνου δηλαδή το πότε δημιουργήθηκαν, τροποποιήθηκαν και προσπελάστηκαν αναλύονται στο πλαίσιο της ανάλυσης χρονοδιαγράμματος με ειδικά εργαλεία και αναφέρονται ως αποδείξεις χρόνου MAC. Η συλλογή των δεδομένων γίνεται χρησιμοποιώντας διάφορα εργαλεία, εξάγονται και ταξινομούνται για ανάλυση με αποτέλεσμα τη δημιουργία ενός στιγμιότυπου της δραστηριότητας που γίνεται στο σύστημα, συμπεριλαμβανομένης της ημερομηνίας του, του τεχνικού αντικειμένου / μέσων που εμπλέκονται, της ενέργειας που εκτελείται και της πηγής.

5.4.4 Κατηγοριοποίηση δεδομένων

Ο ειδικός ερευνητής οφείλει να κατηγοριοποιήσει τα τον μεγάλο αριθμό πληροφοριών που προέρχονται από αρχεία ως χρήσιμα ή μη. Αυτό μπορεί να πραγματοποιηθεί με εργαλεία όπως το hfind από το Sleuth Kit. Οι πληροφορίες παρέχουν λεπτομέρειες σχετικά με το ποια αρχεία ανοίχθηκαν, πού

πλοηγήθηκε ο χρήστης, ποια αρχεία κατεβάστηκαν, καθώς και ποια προγράμματα και εφαρμογές εκτελέστηκαν.

5.4.5 Εφαρμογή φίλτρων ή αναζήτηση με λέξεις κλειδιά κατά την αναζήτηση πληροφοριών

Η μέθοδος αυτή είναι χρήσιμη όταν ο ερευνητής γνωρίζει τι αναζητά και περιλαμβάνει την εφαρμογή εργαλείων αναζήτησης χρησιμοποιώντας λέξεις κλειδιά, συμβολοσειρές ή ολόκληρες εκφράσεις.

5.4.6 Ανάκτηση Δεδομένων

Μερικά από τα διαθέσιμα εργαλεία, όπως το Sleuth Kit χρησιμεύουν στην ανάκτηση δεδομένων από ένα σύστημα αρχείων. Ακόμη, ψηφιακά πειστήρια μπορούν να προέρχονται από τη συλλογή αρχείων που εντοπίζονται από τις κεφαλίδες των αρχείων των ακατέργαστων εικόνων, μια διαδικασία που πραγματοποιείται με το εργαλείο Foremost.

5.4.7 Συλλογή στοιχείων από RAM

Η μνήμη περιέχει πληροφορίες, όπως κλειδιά κρυπτογράφησης, εικόνες που προβλήθηκαν πρόσφατα, πρόσφατες επικοινωνίες στα ψηφιακά κοινωνικά δίκτυα, μηνύματα ηλεκτρονικού ταχυδρομείου που αποστέλλονται και λαμβάνονται μέσω υπηρεσιών Web, ενεργό κακόβουλο λογισμικό κ.λπ.

5.4.8 Δημιουργία μιας απεικόνισης του δίσκου

Η δημιουργία μιας εικόνας του σκληρού δίσκου του υπόπτου είναι ένα υποχρεωτικό βήμα για οποιαδήποτε έρευνα. Ένας συνδυασμός υλικού και λογισμικού χρησιμοποιείται με σκοπό την απόκτηση εικόνων δίσκου υπερνικώντας όλα τα πιθανά ζητήματα. Το υλικό έχει σχεδιαστεί για την απόκτηση σκληρών δίσκων ακόμα και αν αυτή έχουν υποστεί κάποια αλλοίωση. Ακόμη, το υλικό υποστηρίζει την κλωνοποίηση και την απεικόνιση ενός αρχείου, δημιουργώντας έως και 3 αντίγραφα της συσκευής προέλευσης.

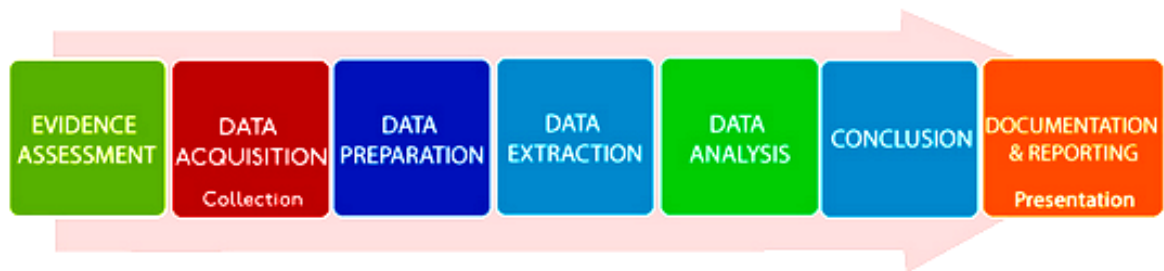
5.4.9 Αποκάλυψη και ανάλυση των ψηφιακών αποδεικτικών στοιχείων

Αυτό το βήμα μπορεί να περιλαμβάνει τη δημιουργία πολλαπλών εικόνων οι οποίες έχουν ανακτηθεί. Η ανάκτηση υπαρχόντων και διαγραμμένων αποδεικτικών στοιχείων συμβαίνει αυτόματα. Τα εργαλεία όπως το Belkasoft Live RAM capturer μπορούν γρήγορα να εξαγάγουν σημαντικές πληροφορίες. Είναι δυνατόν να εντοπιστούν ή να ανακτηθούν εάν διαγραφούν οι ακόλουθοι τύποι δεδομένων:

- Αρχεία Office.
- Ηλεκτρονικά μηνύματα
- Εικόνες
- Βίντεο
- Εφαρμογές για κινητά τηλέφωνα
- Κρυπτογραφημένα αρχεία
- Βάσεις δεδομένων SQLite

5.5 Παρουσίαση των ψηφιακών πειστηρίων

Αυτό είναι το τελευταίο στάδιο της διαδικασίας που περιλαμβάνει μια κατανοητή παρουσίαση μιας αναφοράς βασισμένης σε πρωτόκολλα, νομοθεσίες και στοιχεία σχετικά με τα χαρακτηριστικά των ψηφιακών πειστηρίων, τη σχετικότητά τους με την υπόθεση που υποστηρίζουν, την περιγραφή των ειδικών ερευνητών αναφορικά με τις μεθόδους που ακολουθήθηκαν για τη συλλογή, αποθήκευση και ανάλυσή τους καθώς και τα εργαλεία που επιλέχθηκαν να χρησιμοποιηθούν σε κάθε στάδιο.



Εικόνα 3 Η ψηφιακή εγκληματολογική διαδικασία χωρισμένη σε επτά φάσεις

Ενδεικτικά θα αναφερθεί ένα μοντέλο διαδικασιών με περισσότερες φάσεις όπως συνοψίζεται στην παραπάνω εικόνα και επικεντρώνεται σε επτά βασικούς άξονες και συγκεκριμένα στην αξιολόγηση των στοιχείων, την συλλογή, την προετοιμασία, την εξαγωγή, την ανάλυση των δεδομένων, την εξαγωγή συμπερασμάτων και τελικά την προετοιμασία της τελικής αναφοράς.

1. Αξιολόγηση αποδεικτικών στοιχείων

Για να προσδιοριστεί επιτυχώς το μέγεθος της έρευνας και τα βήματα που πρέπει να ακολουθηθούν θα πρέπει όλες οι πηγές πιθανών ψηφιακών αποδεικτικών στοιχείων να αξιολογούνται διεξοδικά σε σχέση

με το πεδίο εφαρμογής της υπόθεσης. Ωστόσο, ιδιαίτερη προσοχή θα πρέπει να δοθεί στις νομικές διαδικασίες εξουσιοδότησης της έρευνας ώστε το υλικό και το λογισμικό να καταχωρηθεί και διερευνηθεί από εξουσιοδοτημένους ερευνητές.

2. Συλλογή αποδεικτικών στοιχείων

Τα ψηφιακά αποδεικτικά στοιχεία είναι εύαλωτα και μπορούν εύκολα να τροποποιηθούν, ή να καταστραφούν από ακατάλληλο χειρισμό. Επομένως, απαιτείται ειδικός χειρισμός για τη διατήρησή τους ώστε να μην προκύψει ανακριβές συμπέρασμα από αλλοιωμένα ψηφιακά πειστήρια.

3. Προετοιμασία δεδομένων

Ακολουθεί η προετοιμασία των δεδομένων τα οποία πρέπει να ελεγχθούν για να διασφαλιστεί ότι αποτελούν αποδεκτά και σχετικά με την υπόθεση ψηφιακά πειστήρια.

4. Εξαγωγή δεδομένων

Στη διαδικασία εξαγωγής δεδομένων από ψηφιακές συσκευές υπάρχουν δύο διαφορετικοί τύποι εξαγωγής, οι φυσικοί και οι λογικοί. Στη φυσική εξαγωγή προσδιορίζονται και ανακτώνται δεδομένα σε ολόκληρη τη φυσική μονάδα δίσκου, ανεξάρτητα από το σύστημα αρχείων ενώ στη λογική εξαγωγή προσδιορίζονται και συλλέγονται αρχεία και δεδομένα με βάση τα εγκατεστημένα λειτουργικά συστήματα, τα συστήματα αρχείων ή / και τις εφαρμογές.

5. Ανάλυση δεδομένων

Οι ερευνητές εφαρμόζουν διαφορετικές αναλυτικές μεθόδους ώστε να ερμηνεύσουν τα δεδομένα με σκοπό να προσδιορίσουν τη σημασία τους στην υπόθεση.

6. Εξαγωγή συμπερασμάτων

Μεμονωμένα αποδεικτικά στοιχεία από μία πηγή θα είναι πιθανώς ανεπαρκή για να οδηγήσουν σε ένα οριστικό συμπέρασμα. Τα συμπεράσματα πρέπει να βασίζονται σε όλα τα στοιχεία της έρευνας, συμπεριλαμβανομένων των συσχετίσεων μεταξύ κάθε μέρους των αποδεικτικών στοιχείων.

7. Τελική αναφορά

Ο ερευνητής πρέπει να τεκμηριώσει πλήρως και με ακρίβεια κάθε βήμα του στην έρευνά του από την αρχή έως το τέλος και να αιτιολογήσει τις μεθόδους και το υλικό που εφάρμοσε ώστε να είναι δυνατή η αναπαραγωγή της έρευνας από άλλους ερευνητές οι οποίοι να μπορέσουν να καταλήξουν στα ίδια συμπεράσματα.

Για τις ανάγκες της παρούσας εργασίας θα εφαρμοστεί το μοντέλο των επτά διεργασιών καθώς δίνει μια ευρύτερη εικόνα των διαδικασιών που θα ακολουθηθούν και εφαρμόζεται καλύτερα στην περίπτωση μελέτης της διατριβής.

6

Εργαλεία Ανάλυσης Δεδομένων Στην Ψηφιακή Εγκληματολογία

Όπως αναφέρθηκε σε προηγούμενα κεφάλαια, η ψηφιακή εγκληματολογία είναι μια διαδικασία τεχνικής διερεύνησης ψηφιακών πειστηρίων. Πιο συγκεκριμένα η ψηφιακή εγκληματολογία αποτελείται από φάσεις διεργασίας με τα περισσότερα μοντέλα να προτείνουν τα στάδια καθορισμού της σκηνής, της διατήρησης των στοιχείων, της έρευνας και συλλογής των ψηφιακών πειστηρίων, της ανάλυσης και της παρουσίασης των ψηφιακών πειστηρίων (Kohn M. Et al 2013). Για τους σκοπούς αυτούς χρησιμοποιούνται ευρέως διαθέσιμα εργαλεία υλικού και λογισμικού ειδικότερα στα στάδια της συλλογής και της ανάλυσης των δεδομένων.

6.1 FRED (FRED SR, FRED L)

Υπάρχουν πολλά εργαλεία υλικού που θα μπορούσαν να χρησιμοποιηθούν από έναν ειδικό όπως είναι για παράδειγμα το FRED δηλαδή μια συσκευή που χρησιμοποιείται από τους περισσότερους ερευνητές και υπάρχει σε διάφορες εκδοχές όπως FRED SR, FRED L. κ.λπ. Τα συστήματα αυτά χρησιμοποιούνται για τη συλλογή και την ανάλυση των στοιχείων και είναι αρκετά εύχρηστα και απλά καθώς χρειάζεται να αφαιρεθεί ο σκληρός δίσκος από το ύποπτο σύστημα και να συνδεθεί στη συσκευή FRED ώστε να συλλεχθούν τα δεδομένα. Με τον τρόπο αυτό το FRED μπορεί να αποκτήσει δεδομένα απευθείας από τους σκληρούς δίσκους και τις συσκευές αποθήκευσης και δύναται να αποθηκεύσει εικόνες σε DVD, CD ή σκληρούς δίσκους έχοντας η συσκευή χωρητικότητα έως 1,6 TB.

Παλαιότερα και μέχρι σήμερα τα συστήματα FRED μπορούσαν να ανακτήσουν δεδομένα από δισκέτες, 100/2501750 MB κασέτες ZIP, CD-ROM, DVDROM, Compact Flash κá. (Prasanthi V.,2016)

6.2 Encase

Το Encase είναι μια εφαρμογή που βοηθά στην ανάκτηση στοιχείων από σκληρούς δίσκους και διευκολύνει την ανάλυση αρχείων. που προέρχονται από διάφορες συσκευές για παράδειγμα από κινητά τηλέφωνα, tablet κ.λπ.. Η εφαρμογή αυτή μπορεί να ξεκλειδώσει κρυπτογραφημένα αρχεία. Αυτό το εργαλείο μπορεί να συλλέξει γρήγορα γεγονότα από διάφορες συσκευές και να ανακαλύψει πιθανά ψηφιακά πειστήρια. Παράγει επιπλέον μια αναφορά βασισμένη εξ' ολοκλήρου στα ψηφιακά αποδεικτικά στοιχεία. (Prasanthi V.,2016)

6.3 FTK imager

Το FTK Imager είναι μια εργαλειοθήκη που μπορεί να χρησιμοποιηθεί στο πεδίο της ψηφιακής εγκληματολογίας για τη λήψη αποδεικτικών στοιχείων παρέχοντας τη δυνατότητα να δημιουργήσει αντίγραφα δεδομένων χωρίς να τροποποιήσει τα αρχικά στοιχεία. Αυτό το εργαλείο επιτρέπει να καθοριστούν ειδικά κριτήρια ώστε να μειωθεί η ποσότητα των μη σχετικών δεδομένων. Ακόμη προσφέρει καλή οπτικοποίηση των δεδομένων χρησιμοποιώντας ένα γράφημα. (Varol A et al, 2017) Το Forensic ToolKit (FTK) σαρώνει τον σκληρό δίσκο για οποιεσδήποτε πληροφορίες χρειάζεται ο ερευνητής. Το FTK Imager αποθηκεύει την εικόνα του σκληρού δίσκου σε ένα αρχείο ή σε τμήματα τα οποία μπορούν να ανακατασκευαστούν όποτε χρειάζεται. (Khatter K et al 2017)

6.4 Slauth Kit και Autopsy

Το Sleuth Kit είναι ένα εργαλείο που βασίζεται σε UNIX και Windows και επιτρέπει την εγκληματολογική ανάλυση των υπολογιστών. Έρχεται με πολυάριθμο εξοπλισμό που βοηθά στην ψηφιακή εγκληματολογία και συγκεκριμένα στην ανάλυση εικόνων δίσκου, εγγράφων κ.λπ. (Prasanthi V.,2016) Η εφαρμογή Autopsy είναι ένα εύχρηστο εργαλείο που χρησιμοποιείται ευρέως ώστε να διερευνηθεί τι συνέβη σε έναν υπολογιστή. Διαθέτει αναζήτηση λέξεων-κλειδιών για την πληρέστερη εύρεση αρχείων που αναφέρουν σχετικούς όρους, φιλτράρισμα με επισήμανση υπόπτων αρχείων,

ανάλυση χρονοδιαγράμματος, ανάλυση ιστορικού, σελιδοδεικτών και cookie από Firefox και Chrome και μπορεί να ανακτήσει διαγραμμένα αρχεία. (Rana N et al, 2017)

6.5 Digital Forensics Framework

Το Digital Forensics Framework είναι μια πλατφόρμα ανοιχτού κώδικα που μπορεί να χρησιμοποιηθεί και από μη ειδικούς. Εφαρμόζεται στην εικονική αλυσίδα διαφύλαξης (chain of custody), για να αποκτηθεί δικαίωμα εισόδου στις απομακρυσμένες ή τοπικές συσκευές, για να ανακτηθούν κρυμμένα και διαγραμμένα αρχεία, να πραγματοποιηθεί σύντομη αναζήτηση εγγράφων κ.ά. (Prasanthi V.,2016)

6.6 Open Computer Forensics Architecture (OCFA)

Το Open Computer Forensics Architecture (OCFA) είναι μια πλατφόρμα και χρησιμοποιεί τη βάση δεδομένων postgresQL για την αποθήκευση εγγραφών. Κατασκευάστηκε από την επιχείρηση της Εθνικής Αστυνομίας της Ολλανδίας για λόγους αυτοματοποίησης. (Prasanthi V.,2016)

6.7 CAINE

Το CAINE (ComputerAided Investigative Environment) είναι ένα εργαλείο ανοιχτού κώδικα που προσφέρει ένα περιβάλλον για να συνδυάζονται τα υπάρχοντα εργαλεία προγράμματος λογισμικού και οι λειτουργικές μονάδες με φιλικό προς τον χρήστη τρόπο. (Khatter K et al 2017)

6.8 X-way Forensics

Η X-way Forensics είναι μια πλατφόρμα για Windows. Έχει τη δυνατότητα ανάγνωσης συστημάτων gadget και εγγράφων μέσα από πολλά αρχεία φωτογραφιών. Μπορεί να γίνει αυτόματη ανίχνευση διαγραμμένου ή χαμένου τμήματος του σκληρού δίσκου. Ακόμη, πραγματοποιείται έλεγχος αρχείων καθώς εκτελούνται και διαδικασίες ανάκτησης. Παρέχει επίσης τη δυνατότητα αξιολόγησης της μνήμης RAM. Τέλος, εξάγει μεταδεδομένα από πολλούς τύπους αναφορών και έχει τη δυνατότητα εξαγωγής μηνυμάτων ηλεκτρονικού ταχυδρομείου. (Prasanthi V.,2016)

6.9 SANS Investigative Forensics Toolkit

Το SANS Investigative Forensics Toolkit ή το SIFT είναι μια συσκευή σε Ubuntu που συνοδεύει όλα τα απαραίτητα εργαλεία που χρησιμοποιούνται στην ψηφιακή εγκληματολογία και αποτελεί ένα εργαλείο ανοιχτού κώδικα. (Prasanthi V.,2016)

6.10 Registry Recon

Το Registry Recon είναι ένα δημοφιλές εργαλείο ανάλυσης μητρώου. Εξάγει πληροφορίες μητρώου και θα μπορούσε να ανοικοδομήσει μητρώα τόσο από τις σημερινές όσο και από τις προηγούμενες εγκαταστάσεις στον υπολογιστή. (Prasanthi V.,2016)

6.11 LIBFORENSICS

Το Libforensics χρησιμοποιείται για την ανάπτυξη εφαρμογών ψηφιακής εγκληματολογίας. Αναπτύχθηκε σε Python και μπορεί να εξάγει πληροφορίες από πολλές μορφές ψηφιακών αποδεικτικών στοιχείων. (Prasanthi V.,2016)

6.12 Windows SCOPE

Το Windows SCOPE χρησιμοποιείται για την ανάλυση ασταθούς μνήμης και στην αντίστροφη μηχανική των κακόβουλων προγραμμάτων. Προσφέρει τη δυνατότητα μελέτης του πυρήνα των Windows, των DLL, της μνήμης κλπ. (Prasanthi V.,2016)

6.13 Belkasoft evidence centre

Το Belkasoft evidence centre είναι ένα πρόγραμμα που χρησιμοποιείται για τον εντοπισμό, την αναζήτηση, την απόκτηση, την εξέταση και την αποθήκευση των αποδεικτικών στοιχείων που είναι αποθηκευμένα σε ψηφιακές πηγές όπως σε κινητές συσκευές και υπολογιστές. Συγκεκριμένα, η εργαλειοθήκη εξάγει τα ψηφιακά στοιχεία από σκληρούς δίσκους, Android backups και άλλα. Το εργαλείο ψάχνει σε κρυφές τοποθεσίες για κρυπτογραφημένες πληροφορίες με σκοπό τη λεπτομερή

διερεύνηση κατεστραμμένων ή διαγραμμένων αρχείων. Λειτουργεί σε διαφορετικά λειτουργικά συστήματα όπως Windows, Linux, Mac, και Blackberry. (Khatter K et al 2017)

6.14 Foremost

Το Foremost είναι ένα εργαλείο ψηφιακής εγκληματολογίας ανοιχτού κώδικα που έχει σχεδιαστεί για πλατφόρμες που βασίζονται σε Linux. Είναι δωρεάν και επιτρέπει την μερική ή ολική ανάκτηση αρχείων από μια εικόνα με βάση την εσωτερική δομή δεδομένων τους και τις κεφαλίδες και τα υποσέλιδά τους. Επιπλέον, το Foremost επιτρέπει στον ερευνητή να προσαρμόσει τον τύπο αρχείου που πρέπει να ανακτηθεί. Κυρίως μπορεί να ανακτήσει αρχεία και εικόνες που δημιουργούνται από το EnCase, το Safeback, ή εκείνες που υπάρχουν απευθείας στη μονάδα δίσκου. Κυρίως μπορεί να ανακτήσει αρχεία με διαφορετικές επεκτάσεις, όπως jpeg, png, gif, exe, bmp, avi, riff, wav, mpg, mov, pdf, wmv, doc, zip, ole, cpp, rar. (Khatter K et al 2017)

6.15 MemGator

Το MemGator είναι ένα εύχρηστο εργαλείο ανοιχτού κώδικα. Περιλαμβάνει όλες τις δυνατότητες του Memento aggregator και παρέχει επίσης η δυνατότητα για την προσαρμογή διαφορετικών επιλογών, συμπεριλαμβανομένων των αρχείων που συλλέγονται. Το MemGator χρησιμοποιείται για ανάλυση μνήμης εξάγοντας αυτόματα τα δεδομένα από αρχεία μνήμης και δημιουργεί μια τελική αναφορά. Το MemGator συνδυάζει διαφορετικά εργαλεία ανάλυσης μνήμης όπως το Volatility Framework, το AESKeyFinder, το PTFinder και το πρόγραμμα επεξεργασίας αρχείων Scalpel. Επιπλέον, μπορεί να εξάγει κλειδιά κρυπτογράφησης TrueCrypt από το δεδομένο αρχείο μνήμης. (Khatter K et al 2017)

6.16 Galleta

Η Galleta είναι ένα ανοιχτό λογισμικό και δωρεάν εργαλείο που εξετάζει και αναλύει το περιεχόμενο των αρχείων cookies του Internet Explorer που συνδέονται με το ιστορικό του προγράμματος περιήγησης και δίνουν μια εικόνα των ιστότοπων που επισκέφτηκε πρόσφατα ο χρήστης. Είναι δυνατό να αναλύει το περιεχόμενο των αρχείων cookies μετατρέποντας τα δεδομένα σε μορφή που μπορεί να εισαχθεί σε οποιοδήποτε πρόγραμμα υπολογιστικών φύλλων για περαιτέρω

εξέταση. Το Galleta έχει σχεδιαστεί για να λειτουργεί σε διάφορες πλατφόρμες και διαφορετικά λειτουργικά συστήματα. (Khatter K et al 2017)

6.17 Wireshark

Το Wireshark είναι ένα open source, δωρεάν εργαλείο που μπορεί να εκτελεστεί σε σχεδόν κάθε λειτουργικό σύστημα που περιλαμβάνει Microsoft Windows, Linux, Mac OS, Solaris και BSD. Το Wireshark χρησιμοποιείται για επικοινωνία και ανάπτυξη πρωτοκόλλου λογισμικού καθώς και ανάλυση και αντιμετώπιση προβλημάτων δικτύου επιτρέποντας στον χρήστη να εξετάσει το δίκτυο σε μικροσκοπικό επίπεδο. Τα δεδομένα που αποκτήθηκαν από τη σάρωση δικτύου μπορούν να εξεταστούν σε πραγματικό χρόνο ή μπορούν επίσης να αποθηκευτούν για μεταγενέστερη επανεξέταση. (Khatter K et al 2017)

6.18 Rifiuti

Το Rifiuti είναι ένα εργαλείο ανοιχτού κώδικα που κυκλοφόρησε με την ελεύθερη άδεια του FreeBSD, το οποίο έχει σχεδιαστεί για να εξαγάγει πληροφορίες από τα αρχεία του κάδου ανακύκλωσης στα Microsoft Windows. Λειτουργεί σε διαφορετικά λειτουργικά συστήματα όπως Linux, Mac κλπ. Το εργαλείο μπορεί να ανακτήσει τυχόν πρόσφατα διαγραμμένα αρχεία από τον κάδο ανακύκλωσης, επίσης μπορεί να εξαγάγει τη στιγμή που ένα συγκεκριμένο αρχείο διαγράφηκε, το μέγεθος του διαγραμμένου αρχείου και τον αρχικό αριθμό μονάδας δίσκου. (Khatter K et al 2017)

6.19 NMAP

Το NMAP, συντομογραφία του Network Mapper είναι ένα δωρεάν εργαλείο ανοιχτού κώδικα. Χρησιμοποιείται για τον έλεγχο ασφαλείας και για την αποκάλυψη υπηρεσιών και κεντρικών υπολογιστών σε ένα δίκτυο, δίνοντάς μας έτσι ένα «χάρτη» του δικτύου. Επίσης, πολλοί διαχειριστές και συστήματα δικτύου το χρησιμοποιούν για εργασίες ρουτίνας, όπως παρακολούθηση υπηρεσίας ή χρόνος λειτουργίας κεντρικού υπολογιστή. Αν και αρχικά είχε σχεδιαστεί για μεγάλα δίκτυα, λειτουργεί καλά και με έναν κεντρικό υπολογιστή. Το NMAP λειτουργεί σε σχεδόν όλα τα λειτουργικά συστήματα όπως Linux, Windows, Solaris, AmigaOS και Mac. Το NMAP μπορεί να προσαρμοστεί σε

οποιαδήποτε κατάσταση δικτύου όπως συμφόρηση και καθυστέρηση κατά τη διάρκεια της σάρωσης και είναι ευέλικτο, φορητό, ισχυρό και καλά τεκμηριωμένο. (Khatter K et al 2017)

6.20 *The Coroner's toolkit*

Το Coroner's Toolkit ή TCT είναι ένα εργαλείο το οποίο λειτουργεί σε πολλά λειτουργικά συστήματα που σχετίζονται με Unix και χρησιμοποιείται στην αξιολόγηση πόρων από κατεστραμμένους υπολογιστές. (Prasanthi V.,2016)

6.21 *Oxygen Forensic Suite*

Το εργαλείο αυτό χρησιμοποιείται στη συλλογή αποδεικτικών στοιχείων από ένα κινητό τηλέφωνο. Αυτή η συσκευή βοηθά στη συλλογή στατιστικών εργαλείων, επαφών, μηνυμάτων (μηνύματα ηλεκτρονικού ταχυδρομείου, SMS, MMS), στη λήψη διαγραμμένων μηνυμάτων, αρχείων καταγραφής ονομάτων και πληροφοριών ημερολογίου. (Prasanthi V.,2016)

6.22 *Bulk Extractor*

Το Bulk Extractor σαρώνει τα στιγμιότυπα δίσκων, αρχείων ή καταλόγου των εγγράφων για την εξαγωγή ωφέλιμων δεδομένων. Σε αυτήν τη διαδικασία, αγνοεί τη δομή του συστήματος εγγράφων, οπότε είναι πιο γρήγορη και έχει παρόμοιες ποικιλίες εργαλείου. (Prasanthi V.,2016)

6.23 *Xplico*

Το Xplico είναι μια συσκευή ανοικτού κώδικα. Χρησιμοποιείται σε μεγάλο βαθμό για την εξαγωγή χρήσιμων αρχείων από εφαρμογές που χρησιμοποιούν πρωτόκολλα δικτύου. (Prasanthi V.,2016)

6.24 Mandiant RedLine

Το Mandiant RedLine είναι ένα εργαλείο για την ανάλυση μνήμης και αρχείων. Συλλέγει πληροφορίες σχετικά με την τρέχουσα διαδικασία στον κεντρικό υπολογιστή και συλλέγει διαφορετικές πληροφορίες όπως στατιστικά μητρώου, στατιστικά δικτύου και ιστορικό δικτύου. (Prasanthi V.,2016)

6.25 XRY

Είναι ένα εργαλείο που συλλέγει αρχεία με σκοπό την ανάλυση στατιστικών στοιχείων από κινητές συσκευές. Αυτή η συσκευή διαθέτει ένα εργαλείο υλικού και λογισμικό. Το υλικό συνδέει τα κινητά τηλέφωνα με τον υπολογιστή και το πρόγραμμα λογισμικού εκτελεί την εξαγωγή και αξιολόγηση των στατιστικών εργαλείων. Τα αρχεία του έχουν σχεδιαστεί για να λαμβάνουν καλύτερα στατιστικά στοιχεία για την εγκληματολογική αξιολόγηση. Το σύγχρονο μοντέλο του εργαλείου μπορεί να ανακτήσει γεγονότα από κάθε είδους έξυπνα τηλέφωνα όπως Android, iPhone και BlackBerry. Συγκεντρώνει διαγραμμένα γεγονότα όπως στατιστικά στοιχεία κλήσεων, εικόνων, SMS και μηνυμάτων κειμένου. (Prasanthi V.,2016)

6.26 P2 explorer

Το P2 explorer είναι ένα εργαλείο ανάλυσης εικόνων με το οποίο οι ερευνητές μπορούν να αναγνωρίσουν στιγμιότυπα και να ανακαλύψουν το περιεχόμενο της φωτογραφίας καθώς και να εντοπίσουν διαγραμμένα γεγονότα της εικόνας. Υποστηρίζει τις περισσότερες μορφές εικόνων όπως PFR, FTK DD, Win Image fromLinux DD κ.ά (Prasanthi V.,2016)

6.27 PlainSight

Το PlainSight είναι μια ακόμη χρήσιμη συσκευή για την προβολή ιστορικών Διαδικτύου, τη συγκέντρωση στατιστικών στοιχείων, τον έλεγχο της χρήσης συσκευών USB, την προβολή τρεχόντων αρχείων κ.α. Για τη χρήση αυτού του εργαλείου, γίνεται εισαγωγή του CD και ακολουθούνται οι οδηγίες. (Prasanthi V.,2016)

Για της ανάγκες της διπλωματικής εργασίας έχει γίνει εφαρμογή της πλατφόρμας ψηφιακής εγκληματολογίας και γραφικής διεπαφής Autopsy, του εργαλείου προεπισκόπησης και απεικόνισης δεδομένων το οποίο δίνει τη δυνατότητα στους επαγγελματίες της ασφάλειας να αξιολογήσουν ηλεκτρονικά στοιχεία FTKimager, καθώς και του εργαλείου Fiddler που εφαρμόζεται στην ανάλυση της κίνησης στο δίκτυο. Το Fiddler είναι ένα εργαλείο διακομιστή μεσολάβησης εντοπισμού σφαλμάτων που χρησιμοποιείται για την καταγραφή και τροποποίηση της κίνησης HTTP και HTTPS μεταξύ ενός υπολογιστή και ενός διακομιστή ή μεταξύ διακομιστών.

7

Τεχνητή Νοημοσύνη Ως Λύση Ασφάλειας

Η τεχνητή νοημοσύνη χρησιμοποιείται ως λύση ασφάλειας και αφορά στην ανάπτυξη προγραμμάτων και συστημάτων ικανά να παρουσιάζουν χαρακτηριστικά που σχετίζονται με ανθρώπινες συμπεριφορές και θεωρούνται από τον άνθρωπο αντιπροσωπευτικά της νοημοσύνης δηλαδή δυνατότητα αναγνώρισης ομιλίας και εικόνας, αυξημένη δυνατότητα ανάλυσης δεδομένων, ικανότητα προσαρμογής σε ένα συγκεκριμένο περιβάλλον ή έξυπνης απόκρισης σε μια κατάσταση και ακόμα τη δυνατότητα πρόγνωσης. Στα πλαίσια αυτά εντάσσεται και η μηχανική εκμάθηση η οποία είναι η επιστήμη που ερευνά και αναπτύσσει υπολογιστές που είναι ικανοί να ενεργούν χωρίς να έχει προηγηθεί αυστηρός προγραμματισμός.

Η τεχνητή νοημοσύνη στην κυβερνοασφάλεια αποτελείται από ένα σύνολο δυνατοτήτων που επιτρέπει στους οργανισμούς να εντοπίζουν, να προβλέπουν και να ανταποκρίνονται σε κυβερνοαπειλές σε πραγματικό χρόνο χρησιμοποιώντας μηχανική και βαθιά μάθηση. (Carpemini,2019) Οι τεχνολογίες τεχνητής νοημοσύνης έχουν εφαρμοστεί εκτενώς σε λύσεις ασφάλειας στον κυβερνοχώρο, αλλά οι χάκερς τις αξιοποιούν επίσης για να αναπτύξουν έξυπνα προγράμματα κακόβουλου λογισμικού και να εκτελέσουν επιθέσεις. (Jeong D.,2020) Η τεχνητή νοημοσύνη εφαρμόζεται κυρίως στις παρακάτω κατηγορίες:

1. Μοντελοποίηση συμπεριφοράς χρήστη

Οι οργανισμοί χρησιμοποιούν τεχνητή νοημοσύνη για να μοντελοποιήσουν και να παρακολουθήσουν τη συμπεριφορά των χρηστών του συστήματος. Ο σκοπός της παρακολούθησης των αλληλεπιδράσεων μεταξύ ενός συστήματος και χρηστών είναι ο εντοπισμός επιθέσεων. Η τεχνητή νοημοσύνη «μαθαίνει» τις δραστηριότητες των χρηστών με την πάροδο του χρόνου, ώστε να εντοπίζει την ασυνήθιστη συμπεριφορά και να την κατηγοριοποιεί ως παρέκκλιση από την αναμενόμενη συμπεριφορά. Κάθε φορά που ένας διαφορετικός χρήστης χρησιμοποιεί τον λογαριασμό, τα συστήματα που λειτουργούν με τεχνολογία ΑΙ μπορούν να ανιχνεύσουν τα ασυνήθιστα μοτίβα δραστηριότητας και να ανταποκριθούν είτε κλειδώνοντας τον χρήστη είτε ειδοποιώντας τους διαχειριστές του συστήματος για την απρόσμενη συμπεριφορά.

2. Εφαρμογή τεχνητής νοημοσύνης σε προγράμματα προστασίας από ιούς

Τα εργαλεία προστασίας από ιούς με δυνατότητες ΑΙ εντοπίζουν ανωμαλίες δικτύου ή συστήματος αναγνωρίζοντας προγράμματα που παρουσιάζουν ασυνήθιστη συμπεριφορά. Τα προγράμματα κακόβουλου λογισμικού κωδικοποιούνται για την εκτέλεση λειτουργιών που διαφέρουν από τις τυπικές λειτουργίες του υπολογιστή. Τέτοια προγράμματα προστασίας από ιούς αξιοποιούν τις τακτικές μηχανικής εκμάθησης για να μάθουν πώς αλληλεπιδρούν προγράμματα με ένα λειτουργικό σύστημα. Ως εκ τούτου, κάθε φορά που εισάγονται προγράμματα κακόβουλου λογισμικού σε ένα δίκτυο, οι λύσεις προστασίας από ιούς μπορούν να τα εντοπίσουν αμέσως και να τους αποκλείσουν από την πρόσβαση σε πόρους συστημάτων.

3. Αυτόματη ανάλυση δικτύου και συστήματος

Η αυτοματοποιημένη ανάλυση δεδομένων συστήματος ή δικτύου διασφαλίζει συνεχή παρακολούθηση για την άμεση αναγνώριση των περιστατικών εισβολής. Στη σύγχρονη εποχή η χειροκίνητη ανάλυση είναι σχεδόν αδύνατη λόγω του τεράστιου όγκου δεδομένων που δημιουργούνται από τις καθημερινές πλέον δραστηριότητες των χρηστών στο διαδίκτυο. Στο πλαίσιο αυτό, η τεχνολογία ΑΙ χρησιμοποιείται για την ανίχνευση ανωμαλιών σε μεγάλους όγκους δεδομένων. Ως αποτέλεσμα, μπορούν να ανιχνεύσουν όλους τους τύπους εισβολής δικτύου ή συστήματος.

4. Σάρωση email

Οι εγκληματίες του κυβερνοχώρου προτιμούν την επικοινωνία μέσω ηλεκτρονικού ταχυδρομείου ως την κύρια τεχνική παράδοσης για κακόβουλους συνδέσμους και συνημμένα που χρησιμοποιούνται για τη διεξαγωγή επιθέσεων ηλεκτρονικού ψαρέματος. Οι τεχνολογίες ΑΙ και μηχανικής μάθησης είναι πολύ αποτελεσματικά στον εντοπισμό μηνυμάτων ηλεκτρονικού "ψαρέματος".

7.1 Δυνατότητες Τεχνητής Νοημοσύνης στην ψηφιακή εγκληματολογία

Σύμφωνα με αναφορά από το Ινστιτούτο ερευνών Cargemini που δημοσιεύτηκε το 2019 οι δυνατότητες της τεχνητής νοημοσύνης αφορούν στην ανίχνευση, στην πρόγνωση και στην ανταπόκριση στις απειλές στον κυβερνοχώρο οι οποίες αναλύονται παρακάτω.

7.1.1 Ανίχνευση

Η τεχνητή νοημοσύνη χρησιμοποιείται εκτενώς για τον εντοπισμό απειλών στον κυβερνοχώρο. Αυτό αντικατοπτρίζει τις μοναδικές δυνατότητες αυτών των τεχνολογιών: η μηχανική μάθηση ή η ανίχνευση με βαθιά μάθηση (Deep learning) επιτρέπει στους οργανισμούς να αναπτύσσουν συνεχώς παραμέτρους ανίχνευσης, χρησιμοποιώντας ανάλυση συμπεριφοράς για τον εντοπισμό ανωμαλιών δηλαδή ασυνήθιστων ακολουθιών από ενέργειες. Σύμφωνα με τον Khammas B. (2018), για την ανίχνευση κακόβουλου λογισμικού, υπάρχουν δύο τεχνικές: δυναμικής και στατικής ανάλυσης. Η δυναμική ανάλυση εστιάζει σε ενέργειες ή συμπεριφορές του κακόβουλου λογισμικού στο χρόνο εκτέλεσης πραγματοποιώντας την εκτέλεση του κακόβουλου λογισμικού σε απομονωμένο σύστημα ή εικονική μηχανή, λαμβάνοντας στιγμιότυπα και μελετώντας τη συμπεριφορά του. Στον αντίποδα, η στατική ανάλυση επικεντρώνεται σε μια πλήρη ανάλυση του κακόβουλου λογισμικού χωρίς να χρειάζεται αυτό να εκτελεστεί.

7.1.2 Πρόγνωση

Ένας μεγάλος αριθμός οργανισμών κάνουν εκτεταμένη χρήση της τεχνητής νοημοσύνης για την πρόβλεψη απειλών στον κυβερνοχώρο σαρώνοντας τεράστιες ποσότητες δεδομένων διαφόρων τύπων για να γίνουν προγνώσεις βάσει του τρόπου με τον οποίο έχει εκπαιδευτεί το σύστημα. Στη συνέχεια μπορούν να ληφθούν προληπτικά μέτρα για την αποφυγή επιθέσεων. Πρόσφατες προσπάθειες έχουν εστιάσει στην ενσωμάτωση μιας βιομηχανικής πλατφόρμας ασφάλειας στον κυβερνοχώρο που αξιοποιεί τη μηχανική εκμάθηση για τη μείωση των κινδύνων του βιομηχανικού διαδικτύου των πραγμάτων (IIoT) και του βιομηχανικού συστήματος ελέγχου (ICS). Σκοπός είναι να

χρησιμοποιηθεί η μη παρεμβατική πλατφόρμα επιχειρησιακής τεχνολογίας για να εντοπίσει κρίσιμες ευπάθειες και να παρακολουθεί συνεχώς τα δίκτυα για τυχόν καταστροφικές κυβερνοεπιθέσεις.

7.1.3 Ανταπόκριση στις απειλές στον κυβερνοχώρο

Σύμφωνα με την αναφορά (Cargemini, 2019), διαπιστώθηκε ότι λιγότερο από το 18% των οργανισμών κάνουν σημαντική χρήση της τεχνητής νοημοσύνης για την αντιμετώπιση των απειλών στον κυβερνοχώρο. Ωστόσο, μπορεί να χρησιμοποιηθεί για τη μείωση του χρόνου που απαιτείται για τη δημιουργία ενός εικονικού κώδικα για μια ανιχνευόμενη απειλή ή για την ανάπτυξη νέων μηχανισμών προστασίας για εξελισσόμενες τεχνολογίες. Ακόμη, από έρευνα που μελετήθηκε στην εν λόγω αναφορά διαπιστώθηκε ότι μια ομάδα ασφαλείας αποκάλυψε ότι οι επιτιθέμενοι χρησιμοποίησαν ρομπότ για να στοχεύσουν μια εταιρεία, αυξάνοντας τις επιθέσεις εξαγοράς λογαριασμών χρησιμοποιώντας μάλιστα κλεμμένα στοιχεία σύνδεσης και κωδικούς πρόσβασης. Για την καταπολέμηση των επιθέσεων, η εταιρία ανέπτυξε μια λύση που χαρακτήρισε ως «υπερασπιστή bot». Ο υπερασπιστής bot χρησιμοποιούσε μηχανική εκμάθηση για να εντοπίσει τη διαφορά μεταξύ φυσιολογικής και μη φυσιολογικής συμπεριφοράς, τερματίζοντας παράλληλα την ανώμαλη συμπεριφορά που προέκυψε.

7.2 Επιθυμητά Χαρακτηριστικά της Τεχνητής Νοημοσύνης

Μια εφαρμογή τεχνητής νοημοσύνης θα πρέπει να έχει ορισμένα χαρακτηριστικά για να μπορεί να παρέχει αποτελεσματική ασφάλεια έναντι σοβαρών επιθέσεων. Αυτά τα χαρακτηριστικά περιλαμβάνουν την ανίχνευση εισβολής σε πραγματικό χρόνο, ενώ δηλαδή η επίθεση βρίσκεται σε εξέλιξη ή αμέσως μετά, την ελαχιστοποίηση των ψευδώς θετικών συναγερμών, την μειωμένη ανθρώπινη παρέμβαση, τη δυνατότητα αυτοπαρακολούθησης για την ανίχνευση των προσπαθειών των εισβολέων να επέμβουν στο σύστημα, τη συμμόρφωση με τις πολιτικές ασφαλείας του συστήματος που παρακολουθείται και τέλος την προσαρμοστικότητα στις αλλαγές και τη συμπεριφορά των χρηστών με την πάροδο του χρόνου. (Dilek S et al. 2015)

7.3 Εφαρμογές τεχνητής νοημοσύνης

Τελευταία έχουν αναπτυχθεί πολλές μέθοδοι και εφαρμογές που προορίζονται για την ασφάλεια δεδομένων μέσω δικτύων όπως είναι το λογισμικό προστασίας από ιούς, το τείχος προστασίας, η

κρυπτογράφηση, τα ασφαλή πρωτόκολλα κ.λπ. Ωστόσο, οι χάκερς μπορούν πάντα να βρουν νέους τρόπους επίθεσης σε συστήματα. Ένα σύστημα ανίχνευσης και πρόληψης εισβολής (IDPS) αποτελεί ένα λογισμικό ή συσκευή υλικού τοποθετημένη μέσα στο δίκτυο, η οποία μπορεί να ανιχνεύσει πιθανές εισβολές και επίσης να προσπαθήσει να τις αποτρέψει. Τα IDPS παρέχουν τέσσερις ζωτικές λειτουργίες ασφαλείας: παρακολούθηση, ανίχνευση, ανάλυση και απόκριση σε μη εξουσιοδοτημένες δραστηριότητες. (Dilek S et al. 2015) Παρακάτω παρουσιάζονται εφαρμογές τεχνητής νοημοσύνης που στοχεύουν στο ηλεκτρονικό έγκλημα.

7.3.1 Εφαρμογές τεχνητού νευρωνικού δικτύου (Artificial Neural Network Applications ANN)

Οι εφαρμογές αυτές αποτελούν έναν υπολογιστικό μηχανισμό που προσομοιώνει δομικές και λειτουργικές πτυχές των νευρωνικών δικτύων που υπάρχουν στα βιολογικά νευρικά συστήματα. Είναι ιδανικά για καταστάσεις που απαιτούν πρόβλεψη, ταξινόμηση ή έλεγχο σε δυναμικά και σύνθετα περιβάλλοντα υπολογιστών. Τα προτερήματα της τεχνολογίας αυτής είναι η δυνατότητα παράλληλης επεξεργασίας πληροφοριών, η εκμάθηση μέσω παραδείγματος, ο χειρισμός σύνθετων μη γραμμικών λειτουργιών, η ανθεκτικότητα σε θόρυβο και ελλιπή δεδομένα και η ευελιξία με τα μοντέλα μάθησης. (Dilek S et al. 2015)

7.3.2 Ευφυείς Δρώντες (Intelligent agents)

Οι ευφυείς δρώντες είναι αυτόνομες δυνάμεις που δημιουργούνται από τον υπολογιστή και επικοινωνούν μεταξύ τους για να διαμοιράζονται δεδομένα και να συνεργάζονται μεταξύ τους, προκειμένου να σχεδιάζουν και να εφαρμόζουν κατάλληλες αποκρίσεις σε περίπτωση απροσδόκητων συμβάντων. Η κινητικότητα τους και η προσαρμοστικότητα τους στα περιβάλλοντα στα οποία αναπτύσσονται, καθώς και η συνεργατική τους φύση, καθιστούν αυτήν την τεχνολογία κατάλληλη για την καταπολέμηση των επιθέσεων στον κυβερνοχώρο. Συνοπτικά η τεχνολογία αυτή παρουσιάζει τα παρακάτω πλεονεκτήματα: ευχρηστία, ορθολογισμός στην επίτευξη των στόχων, προσαρμοστικότητα στο περιβάλλον και στις προτιμήσεις των χρηστών, συνεργασία - συνειδητοποίηση ότι ένας ανθρώπινος χρήστης μπορεί να κάνει λάθος και να παρέχει αβέβαιες πληροφορίες ή να παραλείπει άλλα σημαντικά γεγονότα και ως εκ τούτου δεν πρέπει να αποδέχονται οδηγίες χωρίς να προηγείται έλεγχος που να αφορά στις ασυνέπειες του χρήστη. (Dilek S et al. 2015)

7.3.3 Εφαρμογές τεχνητής ανοσοποίησης συστήματος (Artificial Immune System Applications)

Οι εφαρμογές αυτές, όπως και τα βιολογικά ανοσοποιητικά συστήματα στα οποία βασίζονται, χρησιμοποιούνται για τη διατήρηση της σταθερότητας σε ένα μεταβαλλόμενο περιβάλλον. Η

ανίχνευση εισβολής με βάση τις εφαρμογές τέτοιου είδους περιλαμβάνει την εξέλιξη των ‘ανοσοκυττάρων’, την παραγωγή αντισωμάτων και αναλόγως με τη μεταβολή της συγκέντρωσης αντισωμάτων αξιολογείται η βαρύτητα της επίθεσης. Ως εκ τούτου, οι εφαρμογές αυτές παίζουν σημαντικό ρόλο στην έρευνα για την ασφάλεια στον κυβερνοχώρο και παρουσιάζουν οφέλη όπως δυναμική δομή, παράλληλη και καταναεμημένη μάθηση χρησιμοποιώντας επικοινωνίες δικτύου δεδομένων σε εργασίες εντοπισμού και εξάλειψης καθώς και αυτο-προσαρμοστικότητα και αυτο-οργάνωση, πραγματοποιώντας ενημέρωση των σημείων εισβολής χωρίς ανθρώπινη παρέμβαση. Ακόμη οι τεχνολογίες αυτές έχουν τη δυνατότητα κατάργησης κακόβουλης δραστηριότητας με τα καλύτερα διαθέσιμα μέσα. Επιπρόσθετα, η πολυεπίπεδη δομή που υποστηρίζουν καθιστούν τους επιτιθέμενους ανίκανους να επιτύχουν με τις κακόβουλες δραστηριότητές τους παρακάμπτοντας μόνο ένα επίπεδο, καθώς πολλαπλά επίπεδα διαφορετικών δομών είναι υπεύθυνα για την παρακολούθηση ενός μόνο σημείου. (Dilek S et al. 2015)

7.3.4 Μοντέλα Ταυτοποίησης

Εάν το υπό έρευνα μοντέλο διαθέτει άγνωστες παραμέτρους και αρχιτεκτονική, τεχνικές όπως η αναστροφή και η εξαγωγή μοντέλων μπορεί να παρέχουν τα μέσα για την αναπαραγωγή της συγκεκριμένης συμπεριφοράς με σκοπό την περαιτέρω δοκιμή και ανάλυση. (Baggili I et al. 2020)

7.3.5 Μοντέλα Αυθεντικοποίησης

Ο στόχος είναι να επιτραπεί η επαλήθευση της αυθεντικοποίησης του υπό μελέτη μοντέλου με τη βοήθεια εξελιγμένων μοντέλων μηχανικής μάθησης. Για το σκοπό αυτό εφαρμόζονται τεχνικές κατακερματισμού σε επίπεδο λογισμικού. (Baggili I et al. 2020)

7.3.6 Μοντέλα Απόδοσης

Η καταγραφή των τιμών εσωτερικών μετρήσεων και μεταβλητών μπορεί να παρέχει μια λεπτομερή εικόνα για τις εσωτερικές λειτουργίες του μοντέλου. Επίσης, υψηλότερου επιπέδου μετρήσεις, όπως οι εκτιμήσεις αξίας κατάστασης και δράσης των ενισχυτικών μαθησιακών δρώντων καθώς και η κατανομή πολλαπλών τάξεων των ταξινομητών, μπορεί να παρέχουν μια χρήσιμη εικόνα σχετικά με την προέλευση των προβλημάτων του συστήματος. (Baggili I et al. 2020)

7.3.7 Μοντέλα Κακόβουλου Λογισμικού

Τα μοντέλα μηχανικής μάθησης μπορούν να μολυνθούν ή να έχουν εκπαιδευτεί σκόπιμα να ενεργήσουν κακόβουλα. Μια εφαρμογή ΑΙ πρέπει να μπορεί να εντοπίσει και να αποδείξει την ύπαρξη τέτοιου κακόβουλου λογισμικού και να παράσχει τα μέσα για τον προσδιορισμό της κακόβουλης

πρόθεσής τους. Σε τέτοιες περιπτώσεις είναι βοηθητικό να αναπαράγονται οι συνθήκες προσομοίωσης ή ενός ελεγχόμενου περιβάλλοντος για την παρατήρηση και την ανάλυση της συμπεριφοράς του υπό έρευνα μοντέλου. (Baggili I et al. 2020)

7.4 Προκλήσεις για τις εφαρμογές τεχνητής νοημοσύνης

Αν και τα συστήματα ανίχνευσης ανωμαλιών προσφέρουν την ευκαιρία να εντοπιστούν άγνωστες προηγούμενες επιθέσεις, υπάρχουν κάποιες σημαντικές προκλήσεις που πρέπει να αντιμετωπιστούν. Το κύριο ζήτημα είναι η δυσκολία καθορισμού μιας αποδεκτής συμπεριφοράς και μιας μη αναμενόμενης συμπεριφοράς που μπορεί να αποτελεί επίθεση στο σύστημα. Το γεγονός αυτό μπορεί να προκαλέσει ένα μεγάλο αριθμό ψευδών θετικών συναγερμών, οι οποίοι μπορεί να οφείλονται σε άτυπη συμπεριφορά που είναι στην πραγματικότητα φυσιολογική και εγκεκριμένη, καθώς η κανονική συμπεριφορά μπορεί εύκολα να αλλάξει. (Dilek S et al. 2015)

Ακόμη, οποιαδήποτε αλλαγή στα κανονικά πρότυπα του συστήματος και στις αναμενόμενες συμπεριφορές πρέπει απαραίτητα να οδηγήσει σε ενημέρωση της γνωσιακής βάσης του συστήματος προκειμένου το σύστημα ανίχνευσης ανωμαλιών να είναι σε θέση να διακρίνει εκ νέου τα κανονικά μοτίβα και να δημιουργεί ένα μοντέλο της φυσιολογικής συμπεριφοράς. Εάν το σύστημα ανίχνευσης και πρόληψης ταξινομήσει ανακριβώς μια νόμιμη δραστηριότητα ως κακόβουλη, το αποτέλεσμα θα είναι μια προσπάθεια αποτροπής ή τροποποίησης μιας έγκυρης δραστηριότητας η οποία θα έχει θεωρηθεί ως μη εγκεκριμένη. (Dilek S et al. 2015)

Η ορθή ανάλυση των δραστηριοτήτων απαιτεί ακριβή και έγκυρα τεχνολογικά εργαλεία. Ωστόσο, η έρευνα για την επεξήγηση των περίπλοκων συστημάτων τεχνητής νοημοσύνης συνεχίζεται. Καθώς η τεχνολογία και οι δυνατότητες της τεχνητής νοημοσύνης εξελίσσονται με την πάροδο του χρόνου, μπορεί να γίνει πιο δύσκολο ή ακόμη και αδύνατο να εξηγηθούν τα συστήματα AI. (Baggili I et al. 2020)

Ένα άλλο πρόβλημα περιλαμβάνει την απενεργοποίηση του συστήματος ανίχνευσης εισβολής, από τους χακερς σε περιπτώσεις που διαρρεύσει ο τρόπος λειτουργίας του συστήματος. Σε ετερογενή περιβάλλοντα υπάρχει επίσης ένα ζήτημα ενοποίησης πληροφοριών από διαφορετικούς ιστότοπους.

Τέλος, ζήτημα αποτελεί η διαμόρφωση συστημάτων ανίχνευσης εισβολής που θα συμμορφώνονται με τους νομικούς κανονισμούς, τις απαιτήσεις ασφαλείας ή / και τις συμφωνίες σε επίπεδο υπηρεσίας στον πραγματικό κόσμο. (Dilek S et al. 2015)

Τέλος, οι Baggili I et al (2020) αναφέρουν πως πρόκληση αποτελεί το γεγονός πως δεν υπάρχει επαρκής συνεργασία μεταξύ των επιστημόνων διαφορετικών κλάδων της ψηφιακής εγκληματολογίας και της τεχνητής νοημοσύνης πράγμα που παρακωλύει την πρόοδο της τεχνητής νοημοσύνης στην αποτροπή και διερεύνηση του ψηφιακού εγκλήματος.

7.5 Το μέλλον της Τεχνητής Νοημοσύνης

Λαμβάνοντας υπόψιν τους περιορισμούς που αφορούν στον ανθρώπινο παράγοντα καθώς και το γεγονός ότι παράγοντες όπως το κακόβουλο λογισμικό το οποίο βελτιώνεται συνεχώς, γίνεται εμφανές πως τα περιβάλλοντα δικτύου θα απαιτούν ολοένα και πιο έξυπνους δρώντες αισθητήρες στον κυβερνοχώρο που θα ανιχνεύουν, θα αξιολογούν και θα ανταποκρίνονται εγκαίρως σε κυβερνοεπιθέσεις. (Dilek S et al. 2015)

Ως εκ τούτου, οι εφαρμογές τεχνητής νοημοσύνης που προορίζονται για την άμυνα στον κυβερνοχώρο θα χρειαστούν σχεδιασμό και μελλοντική έρευνα. Σύμφωνα με τους Dilek S et al. 2015 ένας πολλά υποσχόμενος τομέας για την έρευνα είναι η εισαγωγή ιεραρχικής αρχιτεκτονικής γνώσης στο λογισμικό λήψης αποφάσεων. Η ταχεία αξιολόγηση της κατάστασης και η αναζήτηση ορθής λήψης αποφάσεων μπορούν να διασφαλιστούν μόνο με την αυτοματοποιημένη διαχείριση γνώσεων. Επιπλέον, πρέπει να γίνει πολλή περισσότερη έρευνα προτού κατασκευαστούν αξιόπιστα, ευέλικτα συστήματα έξυπνων δρώντων προς διαχείριση κατανεμημένων υποδομών. Το μέλλον της έρευνας θα πρέπει να στραφεί εν γένει στη διερεύνηση μιας θεωρίας για τον τρόπο λειτουργίας βοηθητικών ομάδων και του ρόλου τους στη λήψη αποφάσεων. Ακόμη, θα πρέπει να εξεταστούν από κοινού οι μη ελεγχόμενοι αλγόριθμοι μάθησης και κάποιες νέες τεχνικές για τη δημιουργία υβριδικών IDPS που θα βελτιώσουν την απόδοση της ανίχνευσης παραβιάσεων που χαρακτηρίζονται και γίνονται κατανοητές με βάση κάποια ανώμαλη συμπεριφορά. Επιπλέον, ο συνδυασμός όλων των ειδών τεχνολογιών τεχνητής νοημοσύνης θα αποτελέσει την κύρια τάση ανάπτυξης στον τομέα της τεχνολογίας κατά των ιών.

Παρόλο που η τεχνητή νοημοσύνη έχει χρησιμοποιηθεί ευρέως στον τομέα της ασφάλειας των υπολογιστών και της εγκληματολογίας, υπάρχουν ορισμένα ηθικά και νομικά προβλήματα που προκύπτουν καθώς η τεχνολογία επεκτείνεται γρήγορα. Μερικά από αυτά τα προβλήματα είναι ζητήματα απορρήτου ή ηθικά ζητήματα και άλλα νομικά θέματα. Ένα ευρύ φάσμα ηθικών και νομικών ζητημάτων έρχεται υπό το φως της πιθανής αυτονομίας αυτής της τεχνολογίας και ανακύπτουν ερωτήματα που αφορούν στον ενισχυμένο ρόλο της τεχνολογίας απέναντι στον άνθρωπο, το σύνολο των δυνατοτήτων της τεχνολογίας που μπορεί και θέλει ο άνθρωπος να αξιοποιήσει. (Dilek S et al. 2015)

Κατανοώντας το θεωρητικό υπόβαθρο στην ψηφιακή εγκληματολογία και αφού παρουσιάστηκαν τα σύγχρονα τεχνολογικά εργαλεία έρευνας και ανάλυσης στο εν λόγω πεδίο κρίνεται σκόπιμο να ακολουθήσει το ειδικό μέρος της εργασίας το οποίο έχει βασιστεί στην βιβλιογραφική ανασκόπηση και παρουσιάζει εκτενώς την εγκληματολογική εξέταση στο τερματικό ενός θύματος αφού προηγηθεί η επιτυχής εκτέλεση της επίθεσης μετά την εφαρμογή του *TelegramRat*, ενός προγράμματος που δύναται να καταλάβει ολόκληρο τον υπολογιστή του χρήστη.

8

Παρουσίαση Του Κακόβουλου Λογισμικού TelegramRat.exe

8.1 Μεθοδολογία

Στο ειδικό μέρος της παρούσας εργασία η οποία ασχολείται με την ανάκτηση δεδομένων και την οπτική αναπαράσταση συσχετίσεων μεταξύ οντοτήτων που συμμετείχαν σε μια εγκληματική ενέργεια παρουσιάζεται η επιτυχής εκτέλεση της επίθεσης στο τερματικό ενός θύματος μετά την εφαρμογή του *TelegramRat*, ενός προγράμματος που δύναται να καταλάβει ολόκληρο τον υπολογιστή του χρήστη.

Στην ενότητα αυτή θα αναλυθεί το κακόβουλο λογισμικό που χρησιμοποιήθηκε στην εικονική επίθεση που πραγματοποιήθηκε στα πλαίσια της διπλωματικής εργασίας. Το κακόβουλο λογισμικό έχει αναρτηθεί στο GitHub: <https://github.com/LimerBoy/ToxicEye> τον Απρίλιο του 2020 στην Ουκρανία. Είναι πρόγραμμα απομακρυσμένου ελέγχου υπολογιστών το οποίο έχει γραφτεί με τη γλώσσα προγραμματισμού C# στο περιβάλλον ανάπτυξης της Microsoft Visual Studio και στο οποίο χρησιμοποιείται ως εντολέας το bot του Telegram.

Όταν είναι ενεργοποιημένη η απομακρυσμένη πρόσβαση, οι εξουσιοδοτημένοι υπολογιστές και οι διακομιστές μπορούν να ελέγχουν όλα όσα συμβαίνουν στον υπολογιστή του χρήστη. Μπορούν να ανοίξουν έγγραφα, να κατεβάσουν λογισμικό, ακόμη και να μετακινήσουν τον κέρσορα της οθόνης σε πραγματικό χρόνο.

Το RAT είναι ένας τύπος κακόβουλου λογισμικού που μοιάζει πολύ με νόμιμα προγράμματα απομακρυσμένης πρόσβασης. Η κύρια διαφορά, φυσικά, είναι ότι τα RAT εγκαθίστανται σε έναν υπολογιστή χωρίς να το γνωρίζει ο χρήστης. Τα περισσότερα νόμιμα προγράμματα απομακρυσμένης πρόσβασης είναι κατασκευασμένα για τεχνική υποστήριξη και κοινή χρήση αρχείων, ενώ τα RAT δημιουργούνται με απώτερο σκοπό την κατασκοπεία, την πειρατεία ή την ολοκληρωτική καταστροφή υπολογιστών.

Όπως και τα περισσότερα κακόβουλα προγράμματα, το RAT κάνει piggyback σε αρχεία με νόμιμη εμφάνιση. Οι χάκερ μπορούν να επισυνάψουν ένα RAT σε ένα έγγραφο μέσω email ή σε ένα μεγάλο πακέτο λογισμικού, όπως σε ένα βιντεοπαιχνίδι. Οι διαφημίσεις και οι κακόβουλες ιστοσελίδες μπορούν επίσης να περιέχουν RAT. Τα περισσότερα προγράμματα περιήγησης αποτρέπουν τις αυτόματες λήψεις από ιστότοπους ή ειδοποιούν τον χρήστη όταν ένας ιστότοπος δεν είναι ασφαλής.

Σε αντίθεση με ορισμένα κακόβουλα προγράμματα και ιούς, ένα πρόγραμμα RAT είναι δύσκολο να γίνει αντιληπτό πότε έχει εγκατασταθεί. Σε γενικές γραμμές, ένα RAT δεν θα επιβραδύνει τον υπολογιστή του χρήστη και οι χάκερ θα είναι σε θέση να διαγράφουν τα αρχεία του υπολογιστή ή να διαχειρίζονται εξ ολοκλήρου τον κέρσορα στην οθόνη. Σε ορισμένες περιπτώσεις, οι συσκευές των χρηστών μολύνονται από RAT για χρόνια χωρίς να γίνει εμφανές.

Τα αποτελέσματα ανάλυσης κινδύνου αρχείων μέσω του [Virus Total](#) δείχνουν ότι 30 στις 70 μηχανές προστασίας γνωρίζουν το Malware RAT που χρησιμοποιήθηκε στην εικονική επίθεση που πραγματοποιήθηκε στα πλαίσια της διπλωματικής εργασίας.

30

70

?

Community Score

30 engines detected this file

7f2a8705b5520ed18e8bc14f6f2bfc259a8514db08858bdf3c03df30901c93d3

TelegramRAT.exe

110.50 KB

Size

2021-01-16 11:17:56 UTC

1 month ago

EXE

assembly

detect-debug-environment

direct-cpu-clock-access

peexe

runtime-modules

DETECTION	DETAILS	BEHAVIOR	COMMUNITY
Ad-Aware	Gen:Variant.Razy.692959	AhnLab-V3	Trojan.Win32.Ursu.C4090043
ALYac	Gen:Variant.Razy.692959	SecureAge APEX	Malicious
Arcabit	Trojan.Razy.DA92DF	Avast	Win32:TrojanX-gen [Trj]
AVG	Win32:TrojanX-gen [Trj]	Avira (no cloud)	HEUR/AGEN.1138822
BitDefender	Gen:Variant.Razy.692959	BitDefenderTheta	Gen:NN.Zemsi.F.34760.gmO@aaEOQqm
CAT-QuickHeal	Trojan.Yskbeex.MSIL.ZZ4	ClamAV	Win.Packed.Razy-9784041-0
Cybereason	Malicious.e560a9	Cynet	Malicious (score: 100)
DrWeb	Trojan.Download4.14061	Elastic	Malicious (high Confidence)
Emsisoft	Trojan.Generic (A)	eScan	Gen:Variant.Razy.692959
ESET-NOD32	A Variant Of MSIL/PSW.Discord.CV	F-Secure	Heuristic.HEUR/AGEN.1138822
FireEye	Generic.mg.680c872e560a9679	Fortinet	MSIL.Agent.RPTltr
GData	MSIL.Trojan.ClipBanker.F	Malwarebytes	Backdoor.TelegramRAT
MAX	Malware (ai Score=82)	Microsoft	Trojan:MSIL/AgentWrap.ABIMTB
Rising	Trojan.AntiVM1.CF63 (CLASSIC)	SentinelOne (Static ML)	Static AI - Malicious PE
ZoneAlarm by Check Point	HEUR:Trojan.MSIL.Shelpak.gen	Acronis	Undetected
AegisLab	Undetected	Alibaba	Undetected
Antiy-AVL	Undetected	Baidu	Undetected
Bkav Pro	Undetected	CMC	Undetected
Comodo	Undetected	CrowdStrike Falcon	Undetected
CyLance	Undetected	Cyren	Undetected
eGambit	Undetected	Gridinsoft	Undetected
Jiangmin	Undetected	K7AntiVirus	Undetected
K7GW	Undetected	Kaspersky	Undetected
Kingsoft	Undetected	MaxSecure	Undetected
McAfee	Undetected	McAfee-GW-Edition	Undetected
NANO-Antivirus	Undetected	Palo Alto Networks	Undetected
Panda	Undetected	Qihoo-360	Undetected
Sophos	Undetected	SUPERAntiSpyware	Undetected
Symantec	Undetected	TACHYON	Undetected
Tencent	Undetected	TotalDefense	Undetected
TrendMicro	Undetected	TrendMicro-HouseCall	Undetected
VBA32	Undetected	VIPRE	Undetected
ViRobot	Undetected	Webroot	Undetected
Yandex	Undetected	Zillya	Undetected
Zoner	Undetected	Avast-Mobile	Unable to process file type
BitDefenderFalx	Unable to process file type	Trapmine	Unable to process file type
Trustlook	Unable to process file type	Ikarus	—
Sangfor Engine Zero	—	Symantec Mobile Insight	—

Εικόνα 4 Αξιολόγηση κινδύνου κακόβουλου λογισμικού TelegramRat μέσω του VirusTotal

Οι μέθοδοι που έχουν αναπτυχτεί ώστε να επάγουν αντιδράσεις στον υπολογιστή θύμα του ξενιστή, μέσω του Telegram κατηγοριοποιούνται ως εξής :

(Network) Δίκτυο

- Τοποθεσία από BSSID
- Πληροφορίες συστήματος

(Main) Γενικές

- Λήψη στιγμιότυπου επιφάνειας εργασίας
- Λήψη στιγμιότυπου κάμερας Web
- Λήψη στιγμιότυπου ήχου
- Εκκίνηση υπολογιστή
 - Προσωρινή αναστολή λειτουργίας
 - Τερματισμός Λειτουργίας
 - Επανεκκίνηση
 - Αποσύνδεση
 - BSoD (Μπλε Οθόνη του Θανάτου)
- Διαχείριση εκκίνησης
 - Προσθήκη στο Autorun
 - Κατάργηση εγκατάστασης

(Files) Αρχεία

- Διαχείριση αρχείων
 - Τρέχων Φάκελος
 - Λίστα αρχείων
 - Διαγραφή αρχείου
 - Κατάργηση όλων των αρχείων
 - Ανέβασμα αρχείου
 - Λήψη αρχείου
 - Εκτέλεση αρχείου
 - Εκτέλεση αρχείου ως διαχειριστής
- Διαχειριστής διεργασιών
 - Λίστα διεργασιών

- Διαδικασία Τερματισμού
 - Τερματισμός όλων των διαδικασιών
 - Απενεργοποίηση της Διαχείρισης εργασιών

(Fun) Αλληλεπίδρασης

- Ανταλλαγή μηνυμάτων
- Εκφώνηση μηνύματος
- Άνοιγμα διεύθυνσης URL
- Ορισμός ταπετσαρίας

(Bomb) Πλημμύρισμα

- (ForkBomb) Πλημμύρισμα Μνήμης
- (ZipBomb) Πλημμύρισμα συμπιεσμένου αρχείου

(Stealer) Κλοπής

- Δεδομένα Wi-Fi
- FTP Client
- Discord Token
- Telegram Session
- Κλοπή στοιχείων πιστωτικής κάρτας
- Κλοπή σελιδοδεικτών
- Λήψη κωδικών πρόσβασης
- Λήψη Cookies
- Λήψη ιστορικού

(Other) Άλλα

- Επεξεργασία Clipboard
- Λήψη Keylogs
- Απομακρυσμένη πληκτρολόγηση
- Απομακρυσμένος έλεγχος οθόνης
- Απομακρυσμένος έλεγχος έντασης ήχου
- Περιστροφή οθόνης
- Αποτροπή εισαγωγής (Block Input)

- Απομακρυσμένος έλεγχος CD-ROM

(Scripting) Χρήση εντολών

- Απομακρυσμένη χρήση της γραμμής εντολών Shell (Remote Shell)
- Απομακρυσμένη χρήση της γραμμής εντολών cmd (Batch Scripting)

8.2 Αποτελέσματα

Η δομή του λογισμικού αναπτύσσεται σε ένα project με όνομα TelegramRAT. Πιο κάτω ακολουθεί περιγραφική αναφορά των μεθόδων και κλάσεων.

1. Στο αρχείο “Program.cs” αναπτύσσεται η main class “static void Main(string[] args)” το σημείο εισόδου στο πρόγραμμα που παρέχει τις προϋποθέσεις για την εκτέλεση του προγράμματός καλώντας τις αντίστοιχες μεθόδους.

Αρχείο	Περιγραφή	Μέθοδοι
Program.cs	Απόκρυψη κονσόλας	persistence.HideConsoleWindow();
	Έλεγχος σίγασης	persistence.CheckMutex();
	Έλεγχος ασφαλούς επικοινωνίας SSL	System.Net.ServicePointManager.SecurityProtocol = System.Net.SecurityProtocolType.Ssl3 System.Net.SecurityProtocolType.Tls System.Net.SecurityProtocolType.Tls11 System.Net.SecurityProtocolType.Tls12;
	Λήψη δικαιωμάτων διαχειριστή	persistence.elevatePrivileges();
	Καθυστέρηση πριν από την έναρξη	persistence.Sleep();
	Έλεγχος αν εκτελείτε VirtualBox, Sandbox ή Debugger	persistence.runAntiAnalysis();

Εγκατάσταση στο σύστημα & απόκρυψη φακέλου		persistence.installSelf();
Προσθήκη στην εκκίνηση		persistence.setAutorun();
Διαγραφή αρχείου μετά την πρώτη εκκίνηση		persistence.MeltFile();
Έλεγχος για σύνδεση στο δίκτυο		utils.isConnectedToInternet() ;
Έλεγχος για αποκλεισμένη διαδικασία		persistence.processCheckerThread.Start();
Έναρξη εκτός σύνδεσης keylogger		utils.keyloggerThread.Start();
Κλοπή κωδικών πρόσβασης και δεδομένων κατά την πρώτη εκκίνηση		AutoStealer.AutoStealerThread.Start();
Έναρξη ελέγχου διευθύνσεις πορτοφολιού κρυπτογράφησης.(Clipper)		Clipper.Run();
Διαδικασία προστασίας (BSOD)		persistence.protectProcess();
Αποστολή απόκρισης στο bot του telegram ότι "online"		telegram.sendConnection();
Αναμονή εντολών από το Telegram		telegram.waitCommandsThread.Start();
Τερματισμός ή όχι της Λειτουργίας σύμφωνα με τους ελέγχους που πραγματοποιήθηκαν		var shutdownForm = new persistence.MainForm();

Πίνακας 2 Ανάλυση της κλάσης “**static void Main(string[] args)**” που αναπτύσσεται στο αρχείο “**Program.cs**” του project **TelegramRAT**

2. Το αρχείο config.cs παρέχει την κλάση “ **internal sealed class config**” όπου αναπτύσσονται οι ρυθμίσεις και οι παράμετροι για την ορθή εκτέλεση του προγράμματος, με μεθόδους που παίρνουν τιμές **true/ false** ώστε να καλούνται ή όχι κατά την εκτέλεση του προγράμματος.

Αρχείο	Περιγραφή	Μέθοδοι
config.cs	Ρυθμίσεις που αφορούν την σύνδεση με το bot Telegram	<pre> public const string TelegramToken = "telegramToken"; public const string TelegramChatID = "telegramChatId"; public static int TelegramCommandCheckDelay = 1;</pre>
	Ρυθμίσεις που αφορούν την εγκατάσταση στο σύστημα.	<pre> public static bool AdminRightsRequired = true; public static bool AttributeHiddenEnabled = true; public static bool AttributeSystemEnabled = true; public static bool MeltFileAfterStart = true; public static string InstallPath = @"C:\rat.exe";</pre>
	Ρυθμίσεις που αφορούν την εκκίνηση	<pre> public static bool AutorunEnabled = true; public static string AutorunName = "Chrome Update";</pre>
	Ρυθμίσεις που αφορούν την προστασία της διαδικασίας	<pre> public static bool ProcessBSODProtectionEnabled = true;</pre>
	Ρυθμίσεις που αφορούν την απόκρυψη παράθυρου κονσόλας ή Debugger	<pre> public static bool HideConsoleWindow = true;</pre>
	Ρυθμίσεις που αφορούν την εκτέλεση του	<pre> public static bool</pre>

προγράμματος σε περίπτωση που εκτελείτε σε VirtualBox, VMWare, SandBoxie ή Debuggers.	PreventStartOnVirtualMachin e = true;
Ρυθμίσεις που αφορούν την καθυστέρηση εκτέλεσης σε δευτερόλεπτα.	public static int StartDelay = 0;
Ρυθμίσεις που αφορούν την μη εκτέλεση του προγράμματος σε περίπτωση που εκτελούνται εργαλεία ανάλυσης δικτυακής κίνησης	public static bool BlockNetworkActivityWhen ProcessStarted = true; public static string[] BlockNetworkActivityProces sList
Ρυθμίσεις που αφορούν την μορφή αρχείων που μπορούν να κρυπτογραφηθούν κατά την εκτέλεση του προγράμματος	public static string[] EncryptionFileTypes
Ρυθμίσεις που αφορούν τον όγκο αρχείων που μπορούν να μεταφερθούν κατά την εκτέλεση του προγράμματος	public static long GrabFileSize = 6291456;
Ρυθμίσεις που αφορούν τον τύπο αρχείων που μπορούν να μεταφερθούν κατά την εκτέλεση του προγράμματος	public static string[] GrabFileTypes
Ρυθμίσεις που αφορούν την κλοπή κωδικών πρόσβασης και δεδομένων κατά την πρώτη εκκίνηση	public static bool AutoStealerEnabled = false;
Ρυθμίσεις που αφορούν την αντικατάσταση διευθύνσεις πορτοφολιού bitcoin , ethereum και monero όταν ο χρήστης χρησιμοποιεί την αντιγραφή/ επικόλληση κατά εκτέλεση του προγράμματος (clipper).	public static bool ClipperEnabled = true; public static string bitcoin_address = "1dj5vetdbuqnmzjrhgeicwy wvc6pswu8"; public static string ethereum_address = "0x357c0541f19a7755afbf1c

		cd824ee06059404238"; public static string monero_address = "42pwy6xe4mptz3mlap7ab5j jd9nbt1mwjiqyvfx3fn8fo9cr w9ajuhe1itxepubqacmnisxyej bkfe7udgnyenceecjey9";
--	--	---

Πίνακας 3 Ανάλυση της κλάσης “**static void Main(string[] args)**” που αναπτύσσεται στο αρχείο “**Program.cs**” του project **TelegramRAT**

3. Το αρχείο `utils.cs` παρέχει την κλάση “ `internal static class utils` ” που αναπτύσσει μεθόδους που χρησιμοποιούνται για την άντληση πληροφοριών από τον υπολογιστή θύμα και υλοποιεί επιπρόσθετες λειτουργίες εκτέλεσης του προγράμματος.

Αρχείο	Περιγραφή	Μέθοδοι
utils .cs	Ορισμός ρόλου ως διαχειριστή	public static bool IsAdministrator()
	Αντιγραφή φακέλου	public static void CopyFolder(string sourceFolder, string destFolder)
	Ανάκτηση πληροφοριών ονόματος CPU	public static string GetCPUName()
	Ανάκτηση πληροφοριών ονόματος GPU	public static string GetGPUName()
	Ανάκτηση πληροφοριών μεγέθους RAM	public static int GetRamAmount()
	Αναγνώριση υλικού	public static string GetHWID()
	Ανάκτηση πληροφοριών σχετικά με την έκδοση των Windows	private static string GetWindowsVersionName()
	Ανάκτηση πληροφοριών σχετικά με την έκδοση Bit των Windows 32/64	private static string getBitVersion()

Ανάκτηση πληροφοριών σχετικά με την έκδοση του Συστήματος των Windows 7/8.1/10.	<code>public static string</code> GetSystemVersion()
Ανάκτηση λίστας με τα προγράμματα που έχουν εγκατασταθεί στον υπολογιστή θύμα .	<code>public static string</code> GetProgramsList()
Ανάκτηση της προκαθορισμένης πύλης δικτύου (Default Gateway)	<code>public static IPAddress</code> GetDefaultGateway()
Έλεγχος αν ο υπολογιστής θύμα είναι συνδεδεμένος στο διαδίκτυο και αν μπορεί να συνδεθεί με το api του Telegram	<code>public static void</code> isConnectedToInternet()
Έλεγχος αν ο υπολογιστής θύμα είναι συνδεδεμένος σε ασύρματο τοπικό δίκτυο υπολογιστών	<code>public static void</code> NetDiscover
Λήψη στιγμιότυπου επιφάνειας εργασίας	<code>public static void</code> desktopScreenshot()
Λήψη στιγμιότυπου κάμερας Web	<code>public static void</code> webcamScreenshot (string delay, string camera)
Εντολές Εκκίνησης/Τερματισμού του συστήματος	<code>public static void</code> recordMircophone(string time)
Διαγραφή καταγραφέα πληκτρολόγησης (Keylogger)	<code>public static void</code> startKeylogger() <code>private static IntPtr</code> SetHook(LowLevelKeyboard Proc proc) <code>private static string</code> KeyboardLayout(uint vkCode)
Ανάκτηση τίτλου παραθύρου που είναι ενεργό τη δεδομένη στιγμή.	<code>public static string</code> GetActiveWindowTitle()
Ελαχιστοποίηση όλων των παραθύρων.	<code>public static void</code>

		MinimizeAllWindows()
	Μεγιστοποίηση όλων των παραθύρων.	<code>public static void</code> MaximizeAllWindows()
	Δημιουργία Hash Function MD5	<code>public static string</code> MD5(<code>this string s</code>)
	Εκτέλεση λειτουργίας mp3	<code>public static void</code> PlayMusic(<code>string file</code>)
	Καταστροφή του ειδικού τομέα εκκίνησης (boot sector)	<code>public static void</code> DestroySystem()
	Κρυπτογράφηση των αρχείων	<code>public static void</code> EncryptFileSystem(<code>string key</code>) <code>private static byte[]</code> EncryptBytes(<code>byte[] clearBytes, string EncryptionKey</code>) <code>private static void</code> EncryptFile(<code>string inputFile, string password</code>)
	Αποκρυπτογράφηση των αρχείων	<code>public static void</code> DecryptFileSystem(<code>string key</code>) <code>private static byte[]</code> DecryptBytes(<code>byte[] cipherBytes, string EncryptionKey</code>) <code>private static void</code> DecryptFile(<code>string inputFile, string password</code>)
	Απομακρυσμένος έλεγχος έντασης ήχου	<code>public static void</code> AudioVolumeSet(<code>int volume</code>)
	Ανάκτηση έντασης ήχου	<code>public static double</code> AudioVolumeGet()

Πίνακας 4 Ανάλυση της κλάσης “ `internal static class utils` ” που αναπτύσσεται στο αρχείο “ `utils .cs` ” του project **TelegramRAT**

4. Το αρχείο telegram.cs παρέχει την κλάση “**internal class telegram**” που αναπτύσσει μεθόδους οι οποίες χρησιμοποιούνται για την επικοινωνία του Telegram με τον υπολογιστή θύμα ώστε ο επιτιθέμενος να προβεί σε αποστολή εντολών μέσω του bot του Telegram στο θύμα και πραγματοποιεί επιπρόσθετες λειτουργίες εκτέλεσης του προγράμματος που σχετίζονται με την διάδραση του επιτιθέμενου με το Telegram.

Αρχείο	Περιγραφή	Μέθοδοι
telegram .cs	Σε περίπτωση που ο υπολογιστής θύμα έχει αποτρέψει την επικοινωνία περίμενε για απόκριση	private static void waitForUnblock()
	Αναμονή για υποβολή εντολής	private static void waitCommands()
	Αποστολή αρχείου	public static void sendFile(string file, string type = " Document ")
	Αποστολή μηνύματος (text)	public static void sendText(string text, string chatID = config.TelegramChatID)
	Αποστολή Φωτογραφίας	public static void sendImage(string file)
	Αποστολή Ηχητικού μηνύματος	public static void sendLocation(float lat, float lon)
	Αποστολή στοιχείων τοποθεσίας	public static void DownloadFile(string file, string path = "")
	Λήψη αρχείων από το chat/url	public static void DownloadFile(string file, string path = "")
	Αποστολή αρχείου από τον επιτιθέμενο στο chat του Telegram	public static void UploadFile(string file, bool removeAfterUpload = false)
	Αναφορά σύνδεσης όταν το bot είναι σε σύνδεση με τον υπολογιστή θύμα	public static void sendConnection()

Πίνακας 5 Ανάλυση της κλάσης “**internal class telegram**” που αναπτύσσεται στο αρχείο “**telegram .cs**” του project TelegramRAT

5. Το αρχείο SimpleJSON.cs παρέχει στο πρόγραμμα την σωστή ανάλυση και δημιουργία JSON. Χρησιμοποιεί κλάσεις για διαφορετικούς τύπους JSON. Ο Αναλυτής (parser)/ δημιουργός (builder) κάνει διάκριση μεταξύ διαφορετικών τύπων τιμών, για τη σωστή διαχείριση των Node, Array, Object, String, Number, Bool και Null.

Αρχείο	Περιγραφή	Μέθοδοι
SimpleJSON .cs	Ανάλυση (parse)/ δημιουργία (build) Node	public abstract partial class JSONNode
	Ανάλυση (parse)/ δημιουργία (build) Array	public partial class JSONArray
	Ανάλυση (parse)/ δημιουργία (build) Object	public partial class JSONObject
	Ανάλυση (parse)/ δημιουργία (build) String	public partial class JSONString
	Ανάλυση (parse)/ δημιουργία (build) Bool	public partial class JSONBool
	Ανάλυση (parse)/ δημιουργία (build) Null	public partial class JSONNull
	Δημιουργία JSON	internal partial class JSONLazyCreator

Πίνακας 6 Ανάλυση κλάσεων που αναπτύσσονται στο αρχείο “ SimpleJSON.cs ” του project TelegramRAT

6. Το αρχείο persistence.cs παρέχει την κλάση “`internal sealed class persistence`” που αναπτύσσει μεθόδους για την οχύρωση των διεπαφών του προγράμματος κατά την εκτέλεση του ώστε να μην γίνεται αντιληπτό από το θύμα.

Αρχείο	Περιγραφή	Μέθοδοι / Κλάσεις
persistence .cs	Αποστολή μηνύματος στον επιτιθέμενο κατά τον τερματισμό λειτουργίας ή την Αποσύνδεση των Windows του θύματος ώστε ο επιτιθέμενος να προβεί σε ενέργειες προστασίας της εκτέλεσης του προγράμματος. • Να σταματήσει την εκτέλεση	public partial class MainForm

	τερματισμού λειτουργίας, • Να απενεργοποιήσει την προστασία εκτέλεσης του προγράμματος • Να τερματίσει την εκτέλεση του προγράμματος. Παράλληλα τρέχουν διεργασίες ώστε να μην γίνεται ορατό το πρόγραμμα στη γραμμή εργασιών ή το παράθυρο της κονσόλας κατά τον Τερματισμό λειτουργίας ή της Αποσύνδεση των Windows του θύματος, που να δείχνουν ότι η εκτέλεση του προγράμματος εμποδίζει την διαδικασία	
Συλλογή λίστας διαδικασιών που εκτελούνται από το πρόγραμμα	<code>private static List<string> GetProcessList()</code>	
Έλεγχος της διαδικασίας εκτέλεσης του προγράμματος και αποστολή μηνύματος στον επιτιθέμενο σε περίπτωση που κάτι εμποδίζει την διαδικασία.	<code>public static void processChecker()</code>	
Εκτελεί το πρόγραμμα σε λειτουργία εντοπισμού σφαλμάτων (Debug mode) ώστε να προστατέψει την διαδικασία εκτέλεσης του, σε πιθανές απειλές για το πρόγραμμα	<code>public static void protectProcess()</code>	
Απαλοιφή λειτουργίας εντοπισμού σφαλμάτων (Debug mode) του προγράμματος	<code>public static void unprotectProcess()</code>	
Απόκρυψη παράθυρου κονσόλας	<code>public static void HideConsoleWindow()</code>	
Έλεγχος αν το πρόγραμμα εκτελείτε σε VirtualBox	<code>public static bool inVirtualBox()</code>	
Έλεγχος αν το πρόγραμμα εκτελείτε σε SandBox	<code>public static bool inSandboxie()</code>	
Έλεγχος αν εκτελείτε Debugger κατά την εκτέλεση του προγράμματος	<code>public static bool inDebugger()</code>	
Έλεγχος αν εκτελείτε antivirus κατά την εκτέλεση του προγράμματος	<code>public static string DetectAntivirus()</code>	

Προγραμματισμός διαδικασίας μη εκτέλεσης του προγράμματος κατά την εκκίνηση του υπολογιστή του θύματος ή προσθήκη του προγράμματος στα προγράμματα που εκτελούνται κατά την εκκίνηση του υπολογιστή του θύματος	<pre>private static void TaskSchedulerCommand(string args) public static void setAutorun() public static void delAutorun()</pre>
Λήψη δικαιωμάτων διαχειριστή	<pre>public static void elevatePrivileges()</pre>
Εγκατάσταση του προγράμματος στον υπολογιστή του θύματος. Δημιουργία φακέλου, αντιγραφή, απόκρυψη χαρακτηριστικών και ρύθμισης συστήματος	<pre>public static void installSelf()</pre>
Απεγκατάσταση του προγράμματος από τον υπολογιστή του θύματος. Διαγραφή στοιχείων του προγράμματος όπως φάκελοι μονοπάτια και διαδικασίες εκτέλεσης.	<pre>public static void uninstallSelf()</pre>
Ενθυλάκωση μεθόδων Virtualbox/Sandbox/Debugger ώστε να γίνεται έλεγχος από το αρχείο config.cs που θέτει τις μεθόδους true ή false ώστε να καλούνται ή όχι κατά την εκτέλεση του προγράμματος	<pre>public static void runAntiAnalysis()</pre>
Έλεγχος αν το πρόγραμμα εκτελείτε ήδη	<pre>public static void CheckMutex()</pre>
Αναστολή λειτουργίας του προγράμματος .	<pre>public static void Sleep()</pre>
Διαγραφή αρχείων του προγράμματος μετά την πρώτη εκτέλεση	<pre>public static void MeltFile()</pre>
Αποτροπή αδράνειας του υπολογιστή του θύματος	<pre>public static void PreventSleep()</pre>

Πίνακας 7 Ανάλυση της κλάσης “**internal sealed class persistence**” που αναπτύσσεται στο αρχείο “ **persistence .cs** ” του project **TelegramRAT**

7. Τα αρχεία που βρίσκονται στον υποφάκελο stealer του προγράμματος παρέχουν στο πρόγραμμα κλάσεις που αναπτύσσουν μεθόδους ελέγχου και ενεργειών λήψης δεδομένων του προγράμματος από τον υπολογιστή του θύματος στον υπολογιστή του επιτιθεμένου.

Αρχείο	Περιγραφή	Κλάσεις
AutoStealer .cs	Ενθυλακώνονται και καλούνται οι κλάσεις που παρέχουν στο πρόγραμμα την λήψη δεδομένων από τον υπολογιστή του θύματος στον υπολογιστή του επιτιθεμένου, όπως : • στιγμιότυπο οθόνης • κωδικοί πρόσβασης , στοιχεία καρτών , σελιδοδείκτες, Cookies και ιστορικότητα περιήγησης από το πρόγραμμα περιήγησης (browser) • από εφαρμογές όπως File Zilla, Telegram, Discord και Steam • αρχεία που βρίσκονται στην επιφάνια εργασίας .	internal class AutoStealer
Bookmarks.cs	Παρέχει την κλάση για τον εντοπισμό και την λήψη των σελιδοδεικτών από το πρόγραμμα περιήγησης (browser)	internal class Bookmarks
Clipper.cs	Παρέχει τις κλάσεις ώστε να γίνεται αντικατάσταση της διεύθυνσης πορτοφολιού bitcoin , ethereum και monero κατά την διάρκεια που ο χρήστης χρησιμοποιεί την αντιγραφή/ επικόλληση εστιάζοντας στις λειτουργίες του Clipboard.	internal static class Clipper internal static class PatternRegex internal static class Clipboard internal static class NativeMethods public sealed class ClipboardNotification
Cookies.cs	Παρέχει την κλάση για τον εντοπισμό και την λήψη των Cookies από το πρόγραμμα	internal class Cookies

	περιήγησης (browser)	
CreditCards.cs	Παρέχει την κλάση για τον εντοπισμό και την λήψη των στοιχείων καρτών από το πρόγραμμα περιήγησης (browser)	internal class CreditCards
Crypt.cs	Παρέχει την κλάση που αποκρυπτογραφεί δεδομένα του Chrome	internal class Crypt
Discord.cs	Παρέχει την κλάση για τον εντοπισμό και την λήψη αρχείων που χρησιμοποιούνται για την παρακολούθηση των χρηστών που έχουν πρόσβαση σε βάσεις δεδομένων. (*.ldb files)	internal class DiscordGrabber
DPAPI.cs	Παρέχει την κλάση που αποκρυπτογραφεί οποιουδήποτε είδους δεδομένων που χρησιμοποιούν την μέθοδο DPAPI (Data Protection Application Programming Interface)	internal class DPAPI
FileZilla.cs	Παρέχει την κλάση για τον εντοπισμό και την λήψη αρχείων από το πρόγραμμα μεταφοράς αρχείων FILEZILLA	internal class FileZilla
GrabDesktop.cs	Παρέχει την κλάση για τον εντοπισμό και την λήψη αρχείων που βρίσκονται στην επιφάνια εργασίας.	internal class GrabDesktop
History.cs	Παρέχει την κλάση για τον εντοπισμό και την λήψη των δεδομένων ιστορικού περιήγησης από το πρόγραμμα περιήγησης (browser).	internal class History
Passwords.cs	Παρέχει την κλάση για τον εντοπισμό και την λήψη κωδικών πρόσβασης από το πρόγραμμα περιήγησης (browser).	internal class Passwords
SQLite.cs	Παρέχει την κλάση ώστε να γίνεται ανάγνωση και λήψη δεδομένων της βάσης δεδομένων του προγράμματος περιήγησης (browser).	internal class cSQLite
Steam.cs	Παρέχει την κλάση για τον εντοπισμό και την λήψη δεδομένων πρόσβασης της πλατφόρμας διαδικτυακών παιχνιδιών Steam.	class SteamGrabber
Telegram.cs	Παρέχει την κλάση για τον εντοπισμό και την λήψη δεδομένων της πλατφόρμας ανταλλαγής μηνυμάτων Telegram .	internal class TelegramGrabber

Πίνακας 8 Ανάλυση των κλάσεων που αναπτύσσονται στον υποφάκελο stealer του project TelegramRAT

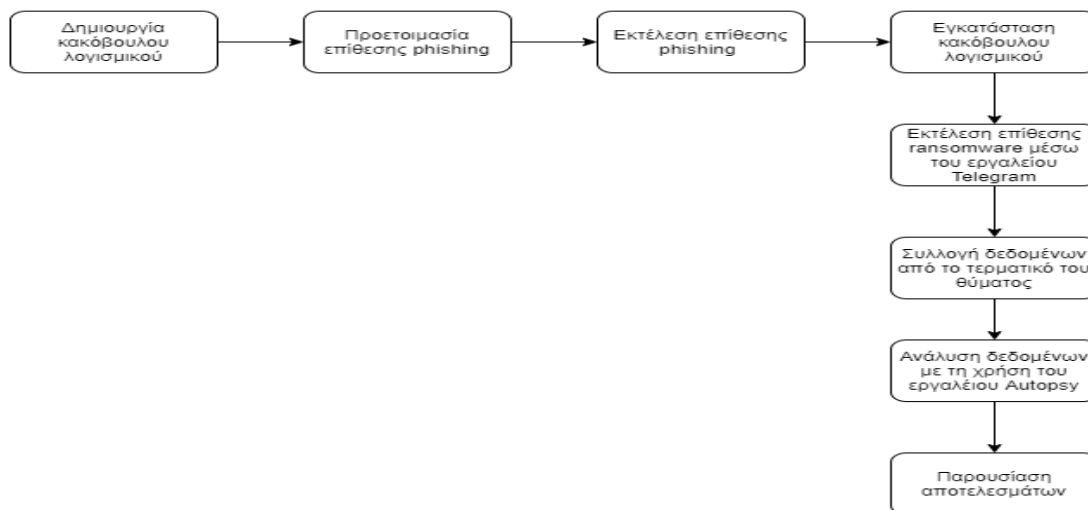
9

Παρουσίαση Της Προσομοίωσης Της Επίθεσης Τύπου Ransomware

Στο παρόν κεφάλαιο θα παρουσιαστεί η προσομοίωση της επίθεσης τύπου ransomware που πραγματοποιήθηκε. Βασικός σκοπός της επίθεσης ήταν η απόκτηση απομακρυσμένης (remote) διαχείρισης μέσω της εφαρμογής Telegram η οποία χρησιμοποιείται ευρέως καθώς είναι από τις πιο γνωστές εφαρμογές instant messaging.

9.1 Μεθοδολογία και υλικό

Η μεθοδολογία που ακολουθήθηκε στο στάδιο αυτό συνοψίζεται στο παρακάτω σχήμα (Εικόνα 5).



Εικόνα 5 Μεθοδολογία που ακολουθήθηκε ώστε να πραγματοποιηθεί η εικονική επίθεση τύπου ransomware

Για να επιτευχθεί η προσομοίωση της επίθεσης καθώς και της μετέπειτα ανάλυσης, στήθηκε το παρακάτω lab στο Hetzner cloud:

Attacker Machine:

- Windows 10
- Telegram
- Visual Studio 2019
- NextCloud
- Docker

Victim Machine:

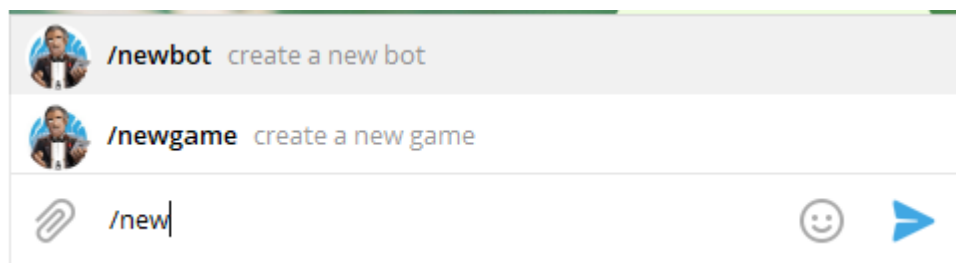
- Windows 10

Forensics Analysis tools

- FTK Imager
- Autopsy
- Fiddler

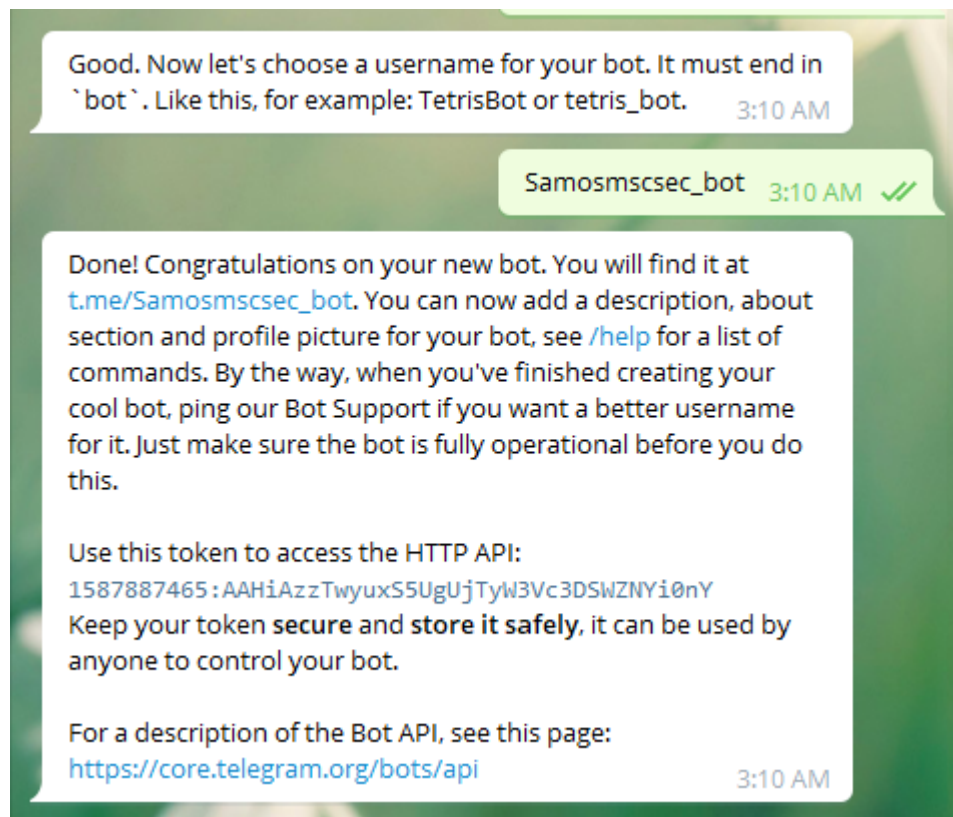
9.2 Περιγραφή διαδικασίας και αποτελέσματα

Στο πρώτο βήμα εκτελέστηκε η εντολή /newbot στο Telegram, δημιουργώντας ένα bot. Η επικοινωνία με το συγκεκριμένο bot πραγματοποιείται μέσω API calls όπως φαίνεται στην παρακάτω εικόνα (Εικόνα 6).

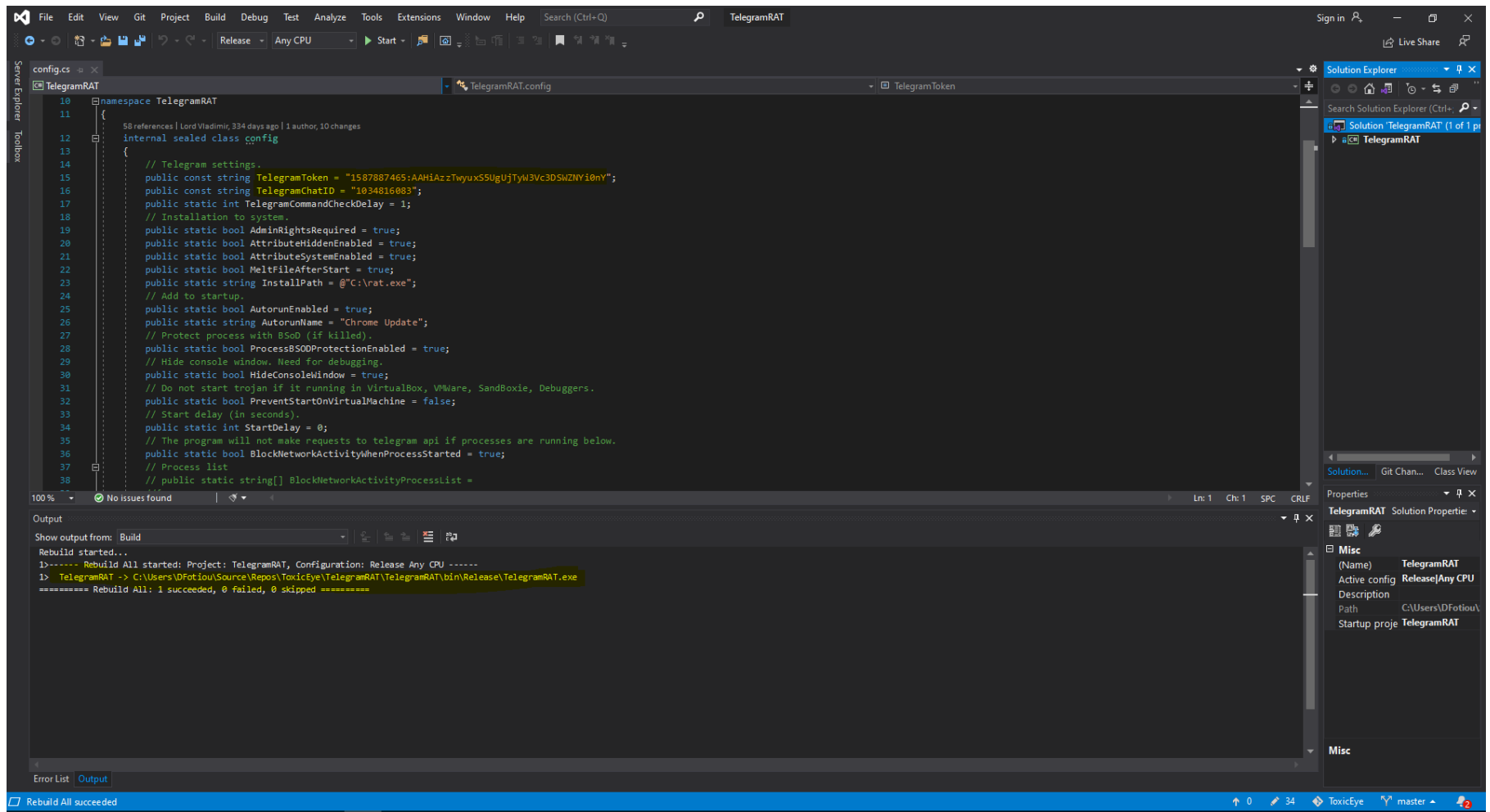


Εικόνα 6 Δημιουργία νέου bot στο Telegram.

Το access token δημιουργήθηκε αυτόματα μετά τη δημιουργία του bot (Εικόνα 7) και προστέθηκε στις παραμέτρους του κώδικα του κακόβουλου λογισμικού TelegramRat.exe (Εικόνα 8) ,το οποίο αναλύθηκε στο προηγούμενο κεφάλαιο, ώστε να επιτευχθεί η επικοινωνία.

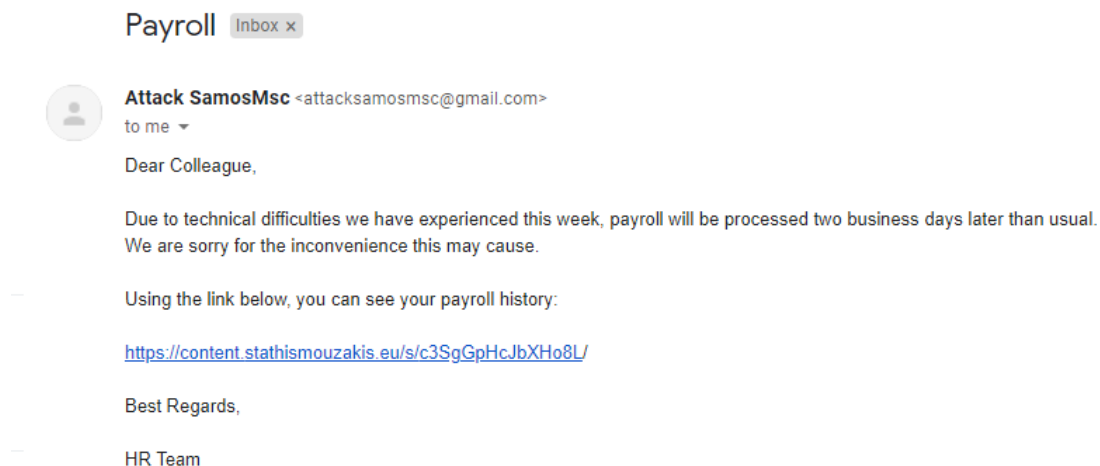


Εικόνα 7 Αυτόματη δημιουργία access token από το bot του Telegram



Εικόνα 8 Εισαγωγή παραμέτρων και δημιουργία του κακόβουλου λογισμικού TelegramRat.exe

Στη συνέχεια επετεύχθη η εγκατάσταση του κακόβουλου λογισμικού στον υπολογιστή του θύματος μέσω μιας επίθεσης ηλεκτρονικού ψαρέματος από μήνυμα ηλεκτρονικού ταχυδρομείου (Εικόνα 9) , πείθοντας το θύμα να ανοίξει ένα σύνδεσμο ώστε να δει το ιστορικό μισθοδοσίας στην εταιρεία στην οποία εργάζεται. Ο σύνδεσμος υλοποιήθηκε μέσω της εφαρμογής Nextcloud. Στην παρακάτω εικόνα φαίνεται το μήνυμα που στάλθηκε στο θύμα.



Εικόνα 9. Email που στάλθηκε στο θύμα

Μετά την επιτυχημένη επίθεση phishing, ο υπολογιστής του θύματος βρέθηκε κάτω από την απόλυτη διαχείριση του επιτιθέμενου με τη χρήση της εφαρμογής Telegram. Καταγράφοντας την κίνηση μεταξύ του διαδικτύου και του υπολογιστή-θύματος χρησιμοποιώντας το εργαλείο Fiddler έγινε εμφανές ότι η υπηρεσία που «τρέχει» στον υπολογιστή του θύματος, πραγματοποιεί κάθε ένα δευτερόλεπτο κλήση στο Telegram bot για να «ρωτήσει» αν υπάρχει κάποια εντολή προς εκτέλεση. (Εικόνα 10)

#	Result	Protocol	Host	URL	Body	Caching	Content-Type	Process	Comments	Custom
1	200	HTTPS	www.fiddler2.com	/UpdateCheck.aspx?i68et...	823	private	text/plain;...			
3	200	HTTP	Tunnel to	api.telegram.org:443	793			rat:3844		
4	200	HTTPS	api.telegram.org	/bot1587887465:AAH4zz...	23		application/...	rat:3844		
6	200	HTTPS	api.telegram.org	/bot1587887465:AAH4zz...	23		application/...	rat:3844		
7	200	HTTP	fiddler2.com	/content/GetArticles?client...	710	no-cac...	application/...	fiddler:...		
8	200	HTTP	fiddler2.com	/content/GetBanner?client...	132, 191	no-cac...	application/...	fiddler:...		
10	200	HTTPS	api.telegram.org	/bot1587887465:AAH4zz...	23		application/...	rat:3844		
12	200	HTTPS	api.telegram.org	/bot1587887465:AAH4zz...	23		application/...	rat:3844		
14	200	HTTPS	api.telegram.org	/bot1587887465:AAH4zz...	23		application/...	rat:3844		
16	200	HTTPS	api.telegram.org	/bot1587887465:AAH4zz...	23		application/...	rat:3844		
18	200	HTTPS	api.telegram.org	/bot1587887465:AAH4zz...	23		application/...	rat:3844		
20	200	HTTPS	api.telegram.org	/bot1587887465:AAH4zz...	23		application/...	rat:3844		
22	200	HTTPS	api.telegram.org	/bot1587887465:AAH4zz...	23		application/...	rat:3844		
24	200	HTTPS	api.telegram.org	/bot1587887465:AAH4zz...	23		application/...	rat:3844		
26	200	HTTPS	api.telegram.org	/bot1587887465:AAH4zz...	23		application/...	rat:3844		
28	200	HTTPS	api.telegram.org	/bot1587887465:AAH4zz...	23		application/...	rat:3844		
30	200	HTTPS	api.telegram.org	/bot1587887465:AAH4zz...	23		application/...	rat:3844		
32	200	HTTPS	api.telegram.org	/bot1587887465:AAH4zz...	23		application/...	rat:3844		
34	200	HTTPS	api.telegram.org	/bot1587887465:AAH4zz...	23		application/...	rat:3844		
36	200	HTTPS	api.telegram.org	/bot1587887465:AAH4zz...	23		application/...	rat:3844		

Get Started | Statistics | Inspectors | AutoResponder | Composer | Fiddler Orchestra Beta | FiddlerScript | Log | Filters | Timeline

Request Headers

Host: api.telegram.org

Transport

Host: api.telegram.org

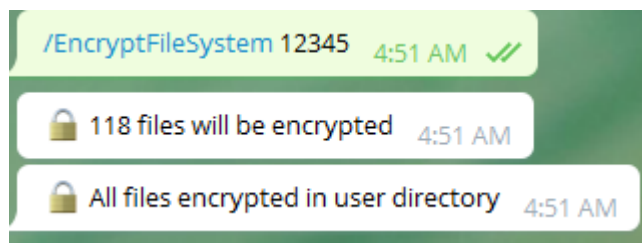
Transformer | Headers | Textview | Syntaxview | Imageview | Hexview | Webview | Auth | Caching | Cookies | Raw | JSON | XML

JSON

```
{
  "ok": true,
  "result": ...
}
```

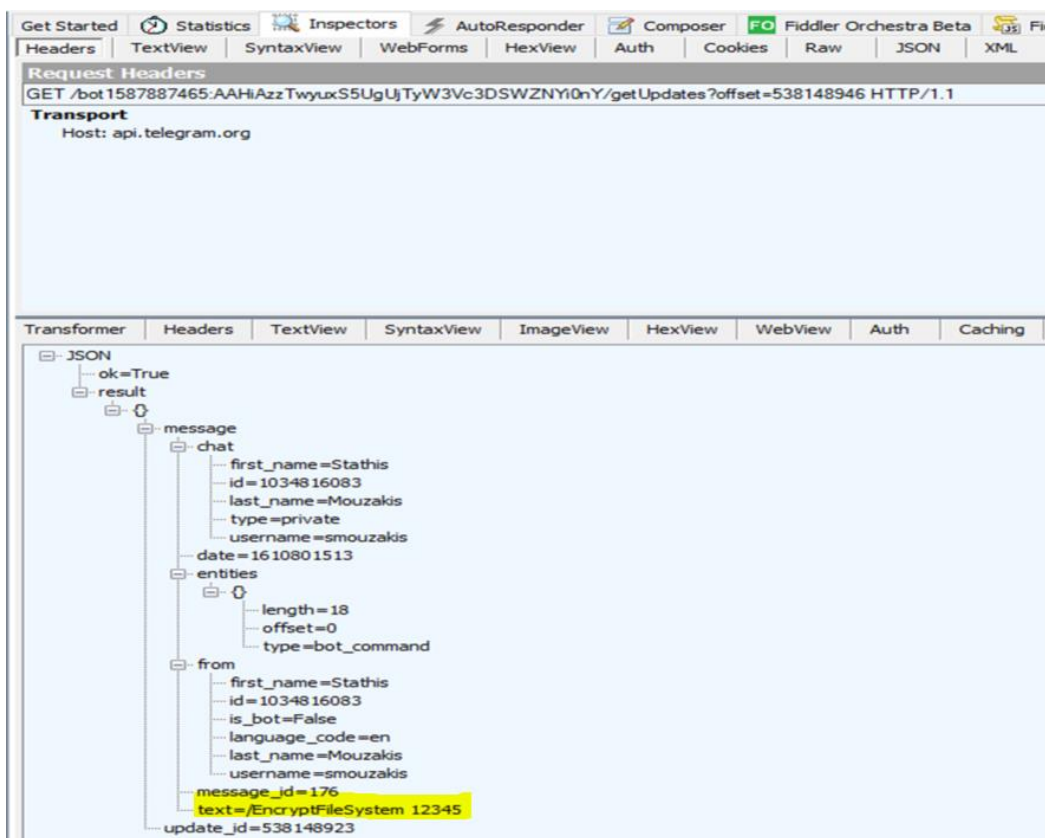
Εικόνα 10 Εργαλείο Fiddler έλεγχος εισερχόμενων και εξερχόμενων δεδομένων στον υπολογιστή θύμα

Σε συνέχεια της επίθεσης, έχοντας πλέον πρόσβαση στον υπολογιστή του θύματος, εκτελέστηκαν εντολές από το Telegram bot. Εκτελώντας την εντολή `/EncryptFileSystem`, με API call το Telegram bot ενημέρωσε την υπηρεσία που «τρέχει» στον υπολογιστή του θύματος να κρυπτογραφήσει τα δεδομένα. Όπως φαίνεται και στην Εικόνα 11, 118 αρχεία κρυπτογραφήθηκαν επιτυχώς.

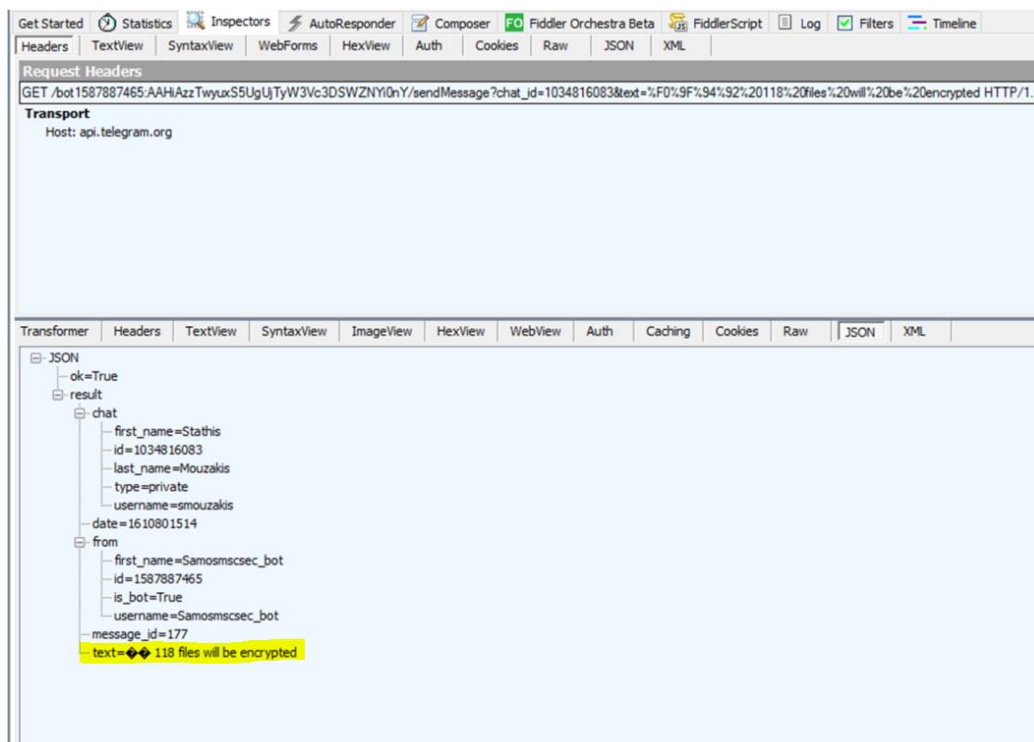


Εικόνα 11 Εκτέλεση εντολής `/EncryptFileSystem <password>`

Με τη χρήση του εργαλείου Fiddler πραγματοποιήθηκε η ανάλυση της επικοινωνίας θύτη και θύματος. Κατά την εκτέλεση της εντολής /EncryptFileSystem, στην Εικόνα 12, φαίνεται το API call και στην Εικόνα 13 γίνεται εμφανές ότι η εντολή εκτελέστηκε επιτυχώς, ενημερώνοντας το Telegram bot.

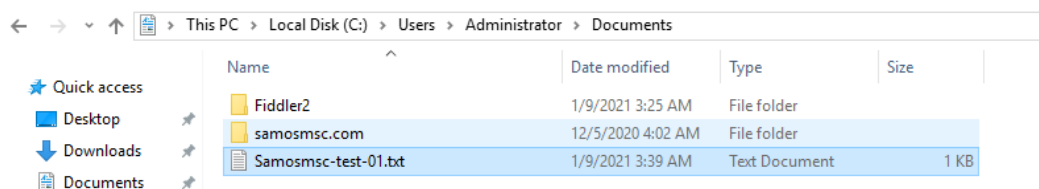


Εικόνα 12 Ανάλυση επικοινωνίας θύτη θύματος κατά την εκτέλεση της εντολής /EncryptFileSystem

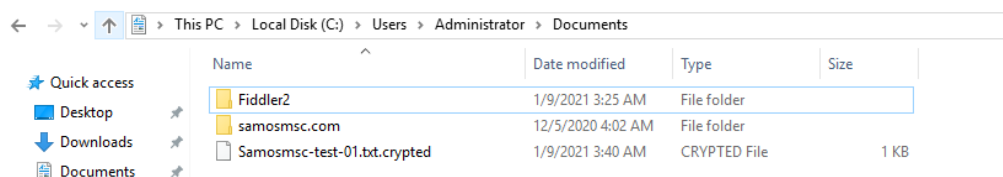


Εικόνα 13 Ανάλυση επικοινωνίας θύτη θύματος κατά την επιτυχή εκτέλεση της εντολής /EncryptFileSystem

Γενικότερα, σε σενάρια επιθέσεων Ransomware, σκοπός είναι να κρυπτογραφηθούν δεδομένα στο τερματικό του χρήστη, όπου το κλειδί αποκρυπτογράφησης βρίσκεται υπό την κατοχή του επιτιθέμενου. Συνήθως, ζητείται μια χρηματική αμοιβή ώστε ο επιτιθέμενος να αποκρυπτογραφήσει τα δεδομένα του θύματος, ή δίνοντας το κλειδί αποκρυπτογράφησης. Στον έλεγχο του συστήματος αρχείων (file system) διαπιστώθηκε ότι τα αρχεία στον υπολογιστή του θύματος έχουν κρυπτογραφηθεί και είναι αδύνατον να τα διαχειριστεί ο χρήστης. Στις Εικόνες 14 και 15 εμφανίζεται η εικόνα των αρχείων πριν και μετά την κρυπτογράφηση τους.

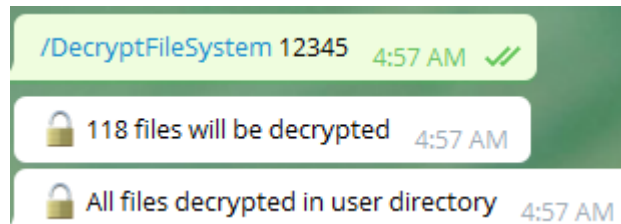


Εικόνα 14 Αρχείο πριν την κρυπτογράφηση

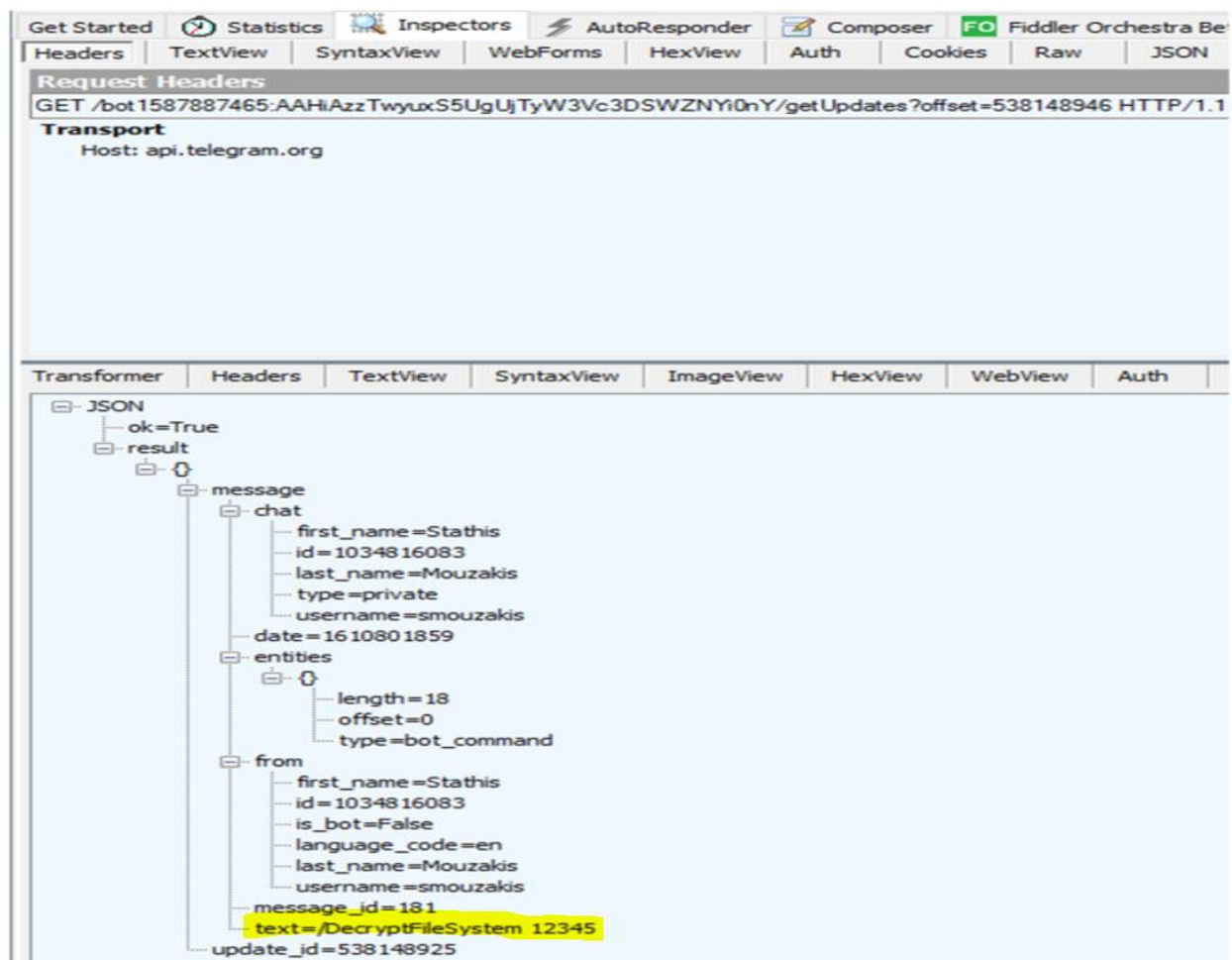


Εικόνα 15 Κρυπτογραφημένο αρχείο

Εκτελώντας την εντολή /DecryptFileSystem της Εικόνας 16 το Telegram bot ενημερώνει το service να προχωρήσει στην αποκρυπτογράφηση των αρχείων. Όπως φαίνεται στην Εικόνα 17, του εργαλείου Fiddler από την ανάλυση της επικοινωνίας η εντολή εκτελέστηκε επιτυχώς.

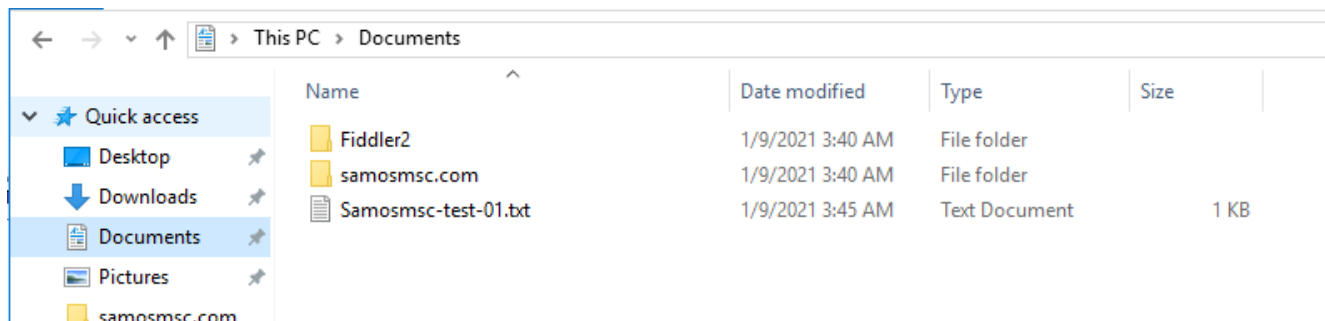


Εικόνα 16 Εκτέλεση εντολής /DecryptFileSystem <password>



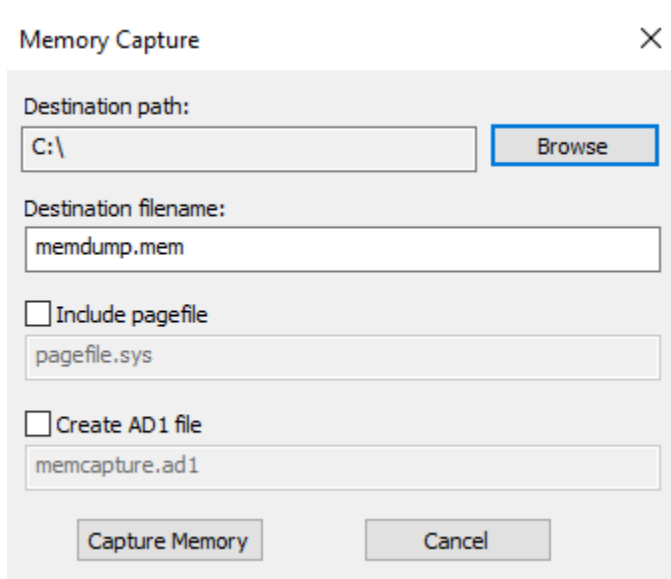
Εικόνα 17 Ανάλυση επικοινωνίας θύτη θύματος κατά την επιτυχή εκτέλεση της εντολής /DecryptFileSystem με σκοπό την αποκρυπτογράφηση του συστήματος

Στον έλεγχο του συστήματος αρχείων (file system) διαπιστώθηκε ότι τα αρχεία στον υπολογιστή του θύματος έχουν αποκρυπτογραφηθεί και είναι πλέον δυνατή η διαχείριση τους από το χρήστη. Στην Εικόνα 18 παρουσιάζεται η εικόνα των αρχείων μετά την αποκρυπτογράφηση τους.



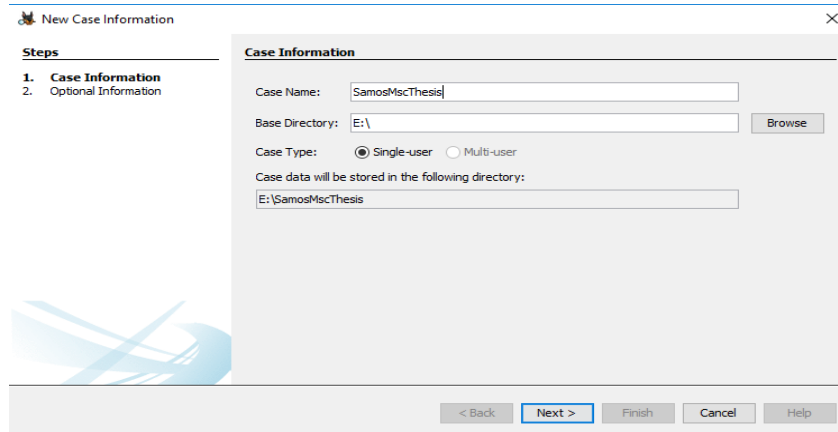
Εικόνα 18 Αποκρυπτογραφημένο αρχείο

Σε επόμενο στάδιο του Lab ανακτήθηκαν δεδομένα από τον υπολογιστή-θύμα ώστε να συσχετιστούν οι δυο οντότητες δηλαδή ο επιτιθέμενος και το θύμα. Τα εργαλεία που χρησιμοποιήθηκαν ήταν τα FTK Imager και Autopsy όπως αυτά παρουσιάστηκαν σε προηγούμενο κεφάλαιο. Με τη χρήση του εργαλείου FTK Imager, δημιουργήθηκε ένα memory dump (Εικόνα 19) από τον υπολογιστή του θύματος ώστε να ακολουθήσει η ανάλυση, η οποία πραγματοποιήθηκε με το εργαλείο Volatility το οποίο εγκαταστάθηκε ως plugin στο Autopsy.



Εικόνα 19 Δημιουργία memory dump

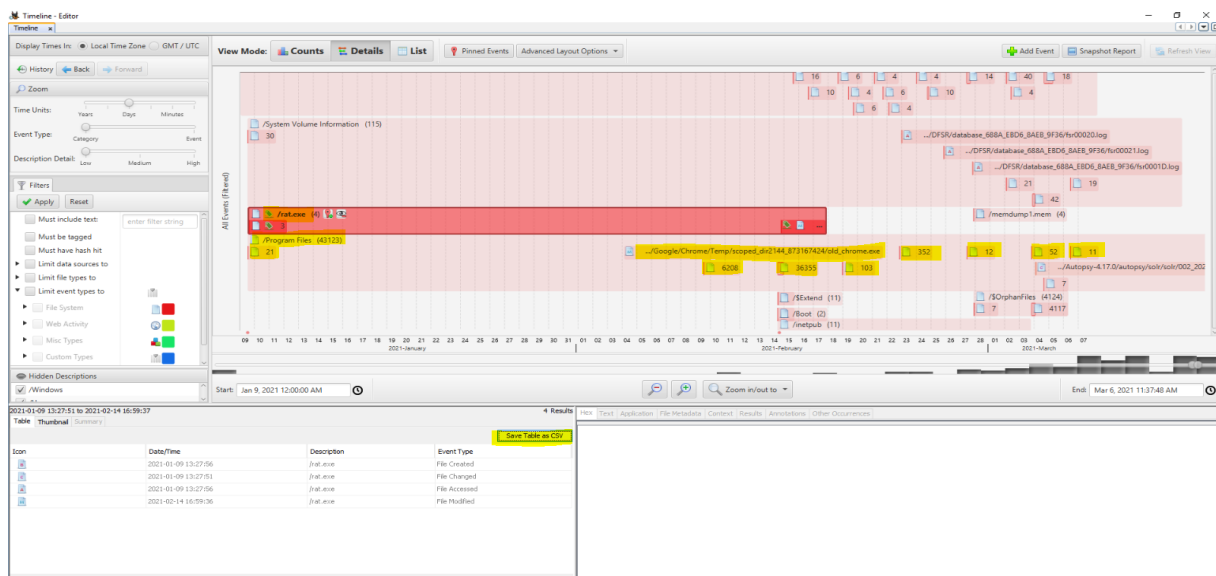
Στη συνέχεια αφού ανακτήθηκε το memory dump με το FTK Imager, δημιουργήθηκε ένα case στο Autopsy χρησιμοποιώντας το memory dump (Εικόνα 20) και πραγματοποιήθηκε η ανάλυση στο τερματικό του θύματος.



Εικόνα 20 Δημιουργία Case στο Autopsy

Μετά από ανάλυση βρέθηκαν στοιχεία όπως ημερομηνίες και ενέργειες οι οποίες πραγματοποιήθηκαν από την εγκατάσταση του κακόβουλου λογισμικού και έπειτα. Η γενική εικόνα των ενεργειών αυτών παρουσιάστηκε στην καρτέλα Details του Autopsy.

Το πρόγραμμα παρέχει στοιχεία για κάθε ενέργεια που πραγματοποιήθηκε μετά την εγκατάσταση του κακόβουλου λογισμικού σε αρχείο της μορφής csv (Εικόνα 21).



Εικόνα 21 Καρτέλα Details του Autopsy

Μέρος των δεδομένων που ανακτηθήκαν μέσω του Autopsy και αφορούν σε ενέργειες που έχουν πραγματοποιηθεί στον υπολογιστή- θύμα παρουσιάζονται και περιγράφονται στον Πινάκα 9.

Icon,"Date/Time","Description","Event Type"	Περιγραφή ενέργειας
true,"2021-01-09 13:27:56","/rat.exe","File Created"	Εγκατάσταση κακόβουλου λογισμικού στον υπολογιστή θύμα.
true,"2021-01-09 13:27:51","/rat.exe","File Changed"	
true,"2021-01-09 13:27:56","/rat.exe","File Accessed"	
true,"2021-02-14 16:59:36","/rat.exe","File Modified"	
true,"2021-01-09 13:29:49","/ProgramData/Microsoft/Windows/Start Menu/Programs/Google Chrome.lnk","File Created"	Παρεμβολή του κακόβουλου λογισμικού στο πρόγραμμα περιήγησης Google Chrome
true,"2021-01-09 13:29:49","/ProgramData/Microsoft/Windows/Start Menu/Programs/Google Chrome.lnk","File Accessed"	
true,"2021-02-14 13:30:13","/ProgramData/Microsoft/Crypto/RSA","File Accessed"	Κρυπτογράφηση αρχείων.
true,"2021-02-14 13:30:13","/ProgramData/Microsoft/Crypto/RSA","File Changed"	
true,"2021-02-14 13:30:13","/ProgramData/Microsoft/Crypto/RSA","File Modified"	
true,"2021-02-14 13:30:13","/ProgramData/Microsoft/Crypto/RSA/S-1-5-18","File Created"	
true,"2021-02-14 13:30:13","/ProgramData/Microsoft/Crypto/RSA/S-1-5-18","File Accessed"	
true,"2021-02-14 13:30:13","/ProgramData/Microsoft/Crypto/RSA/S-1-5-18","File Changed"	
true,"2021-02-14 13:30:13","/ProgramData/Microsoft/Crypto/RSA/S-1-5-18","File Modified"	
true,"2021-02-14 13:30:13","/ProgramData/Microsoft/Crypto/RSA/S-1-5-18/4eccd106f69e31c1b12304e5463bb71d_b6a7efe1-7f94-424c-b5bc-c98115ecf102","File Created"	
true,"2021-02-14 13:30:13","/ProgramData/Microsoft/Crypto/RSA/S-1-5-18/4eccd106f69e31c1b12304e5463bb71d_b6a7efe1-7f94-424c-b5bc-c98115ecf102","File Accessed"	
true,"2021-02-14 13:30:13","/ProgramData/Microsoft/Crypto/RSA/S-1-5-18/4eccd106f69e31c1b12304e5463bb71d_b6a7efe1-7f94-424c-b5bc-c98115ecf102","File Changed"	
true,"2021-02-14 13:30:13","/ProgramData/Microsoft/Crypto/RSA/S-1-5-18/4eccd106f69e31c1b12304e5463bb71d_b6a7efe1-7f94-424c-b5bc-c98115ecf102","File Modified"	

Πίνακας 9 Δεδομένα που ανακτήθηκαν από το Autopsy

10

Συζήτηση

Η παρούσα εργασία αποτελεί μια προσπάθεια να προσομοιωθεί μια πραγματική επίθεση τύπου Ransomware η οποία θεωρείται μια από τις πιο επικίνδυνες επιθέσεις στη σύγχρονη εποχή καθώς εκμεταλλεύεται αδυναμίες του χρήστη με σκοπό τον απόλυτο έλεγχο του υπολογιστή του και την εκτέλεση κακόβουλων ενεργειών.

Για να επιτευχθεί αυτό δημιουργήθηκε ένα lab χρησιμοποιώντας τα απαραίτητα εργαλεία τόσο για την εκτέλεση της επίθεσης όσο και για την εύρεση αποδεικτικών στοιχείων. Το Lab στήθηκε στο Hetzner cloud, ο υπολογιστής του επιτιθέμενου ήταν Windows 10 και χρησιμοποιήθηκε το περιβάλλον ανάπτυξης Visual Studio 2019 για τη δημιουργία του Malware, τον file server NextCloud ο οποίος έτρεξε ως container σε Docker για το Publishing του κακόβουλου αρχείου και στη συνέχεια χρησιμοποιήθηκε το Telegram σαν εντολέας.

Ο υπολογιστής του θύματος στήθηκε στο Hetzner cloud σε Windows 10. Τα εργαλεία ανάκτησης στοιχείων που χρησιμοποιήθηκαν ήταν τα FTK Imager και Autopsy για την ανάκτηση και ανάλυση αρχείων από τον υπολογιστή-θύμα και το εργαλείο Fiddler για την καταγραφή των API Calls μεταξύ του Telegram και του υπολογιστή-θύματος. Το σενάριο επίθεσης Ransomware επετεύχθη με αποτέλεσμα να κρυπτογραφηθούν δεδομένα στο τερματικό του θύματος όπως η ανάλυση και η εύρεση στοιχείων.

11

Συμπεράσματα και Περιορισμοί

Στην παρούσα εργασία παρουσιάστηκε μια προσομοίωση πραγματικής επίθεσης τύπου Ransomware με συλλογή στοιχείων. Μέρος της επίθεσης ήταν η εγκατάσταση του κακόβουλου λογισμικού στο τερματικό του θύματος. Έγινε προσπάθεια ώστε αυτό το σημείο να μην είναι εμφανές στο χρήστη χρησιμοποιώντας κώδικα σε JavaScript ο οποίος θα έκανε λήψη και θα εκτελούσε το κακόβουλο λογισμικό αυτόματα. Ωστόσο αυτό δεν κατέστη δυνατό καθώς λειτουργίες ασφαλείας του Chrome αδρανοποίησαν συγκεκριμένες λειτουργίες του εν λόγω κώδικα σε JavaScript. Συνεπώς η συμβολή του χρήστη στην επιτυχή εκτέλεση ήταν απαραίτητη και η διαδικασία λήψης του αρχείου πραγματοποιήθηκε με την χρήση Internet Explorer ο οποίος έχει σημαντικά λιγότερες δικλείδες ασφαλείας από τον Chrome.

Μεγάλη πρόκληση στην εκτέλεση της συγκεκριμένης επίθεσης ήταν η επιλογή του Antivirus που θα προστατεύει το τερματικό του χρήστη. Στην πρώτη φάση των δοκιμών μόνο το 10 % των προϊόντων ασφαλείας μπορούσε να ανιχνεύσει το κακόβουλο λογισμικό που χρησιμοποιήθηκε. Στη δεύτερη φάση των δοκιμών το ποσοστό αυξήθηκε στο 30% γεγονός πρόσθεσε δυσκολίες στην επίθεση.

Με βάση τη βιβλιογραφική ανασκόπηση αναφορικά με την ψηφιακή εγκληματολογία η οποία παρουσιάστηκε στο πρώτο μέρος της εργασίας καθώς και με την υλοποίηση του τεχνικού μέρους το οποίο ακολούθησε και αφορούσε στην εκτέλεση της επίθεσης και στην εύρεση αποδεικτικών στοιχείων συνάγεται το συμπέρασμα πως τα τεχνικά μέτρα που προορίζονται για

την ασφάλεια στον κυβερνοχώρο καθώς και το εκπαιδευμένο προσωπικό είναι απαραίτητα στοιχεία για την διαφύλαξη της ασφάλειας και την αποτροπή επιθέσεων. Είναι γνωστό από τα αναφερόμενα στην παρούσα εργασία ότι στη ψηφιακή εποχή υπάρχει μεγάλη αύξηση των ψηφιακών επιθέσεων και της πολυπλοκότητάς τους, συνεπώς η χρήση εργαλείων τεχνητής νοημοσύνης κρίνεται αναγκαία καθώς βελτιώνει την ποιότητα της έρευνας των αναλυτών μειώνοντας σημαντικά το χρόνο αναζήτησης και εύρεσης νέων στοιχείων και βοηθούν στην ανάπτυξη πιο ισχυρών αντίμετρων.

Βιβλιογραφία

Ελληνική Βιβλιογραφία

Κασούμης Ν.,(2014), Προσομοίωση σεναρίων ψηφιακής εγκληματολογίας στο διαδίκτυο των πραγμάτων με τον προσομοιωτή CUPCARBON. *Αποθετήριο Πανεπιστημίου Μακεδονίας*.
<https://dspace.lib.uom.gr/bitstream/2159/23017/4/KasoumisNikolaosMsc2018.pdf>

Μήτρου ,Λ.,(nd), Ειδικά θέματα δικαίου της πληροφορίας. *Αποθετήριο Πανεπιστημίου Αιγαίου*.

Ξενόγλωσση Βιβλιογραφία

Ajit A.,Johnson E.,(2008) Information security and privacy in healthcare .Current state of research
[online] <http://www.ists.dartmouth.edu/library/416.pdf>

Armstrong J, Bywater A, (2017), What healthcare organisations should know about the GDPR
[online] <https://www.whitepapers.em360tech.com/wp-content/uploads/GDPR-Implications-of-the-GDPR-in-Healthcare-042717-d1.pdf>

Baggili, I., Behzadan, V., (2020) Founding the Domain of AI Forensics. *Creative Commons License Attribution 4.0 International*.

Baryamereeba, V., and Tushabe, F., (2004), The Enhanced Digital Investigation Process Model. In *Proceeding of Digital Forensic Research Workshop*, Baltimore, MD.

Bossler, A., and Berenblum ,T. (2019), Introduction: new directions in cybercrime research. *Journal of Crime and Justice*, **42**:5, 495-499, DOI: 10.1080/0735648X.2019.1692426

Capgemini, (2019), Reinventing Cybersecurity with Artificial Intelligence: The new frontier in digital security.

Carrier, B., and Spafford, E.H., (2003), Getting Physical with the Digital Investigation Process. *International Journal of Digital Evidence*, **2**:2.

Carrier, B., and Spafford, E. H., (2004), An event-based digital forensic investigation framework. In *Digital forensic research workshop*, (pp. 11-13).

Chen, C. D., (1990), Computer Crime and the Computer Fraud and Abuse Act of 1986. *Computer Law Journal*, **10**:1, 71-86.

Dierks, M. P., (1993), Computer Network Abuse. *Harvard Journal of Law and Technology*, **6**, 307-342.

Dilek, S, Çakır , H, and Aydın M, (2015), Applications of Artificial intelligence techniques to combating cyber crimes : a review. *International Journal of Artificial Intelligence & Applications (IJAIA)*. **6**:1.

Du, X., Le-Khan, N., and Scanlon, N., (nd), Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service [online] <https://arxiv.org/ftp/arxiv/papers/1708/1708.01730.pdf>

Dunlop, C., and Kling, R., (1991), Introduction to Security and Reliability. In C. Dunlop & R. Kling (eds.), *Computerization and Controversy: Value Conflicts and Social Choices*, pp. 524-532, San Diego: Academic Press.

GDPR (2016), General Data Protection Regulation (EU) 2016/679 In *Official Journal of the European Union* <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>

Gibson, W., (1984). *Neuromancer T. Carr ed.*, New York: Ace Books.

Goodison S. E., Davis R. C., and. Jackson B. A. ,(2015), Digital Evidence and the U.S. Criminal Justice System. Identifying Technology and other needs to more effectively acquire and utilize digital evidence. *Rand Cooperation*.

Gordon, S., and Ford, R., (2006), On the definition and classification of cybercrime. *Journal of Computer Virology*, **2**, 13–20.

Grabosky, P., (2007), *Electronic crime*. New Jersey. Prentice Hall.

Heaney J Computer Security & Threat Prevention for Individuals & Organizations [online] <http://study.com/academy/lesson/computer-security-threat-prevention-for-individuals-organizations.html>

Harbawi, Malek, and Asaf, V., (2016), The role of digital forensics in combating cybercrimes. In *Digital Forensic and Security (ISDFS), 4th International Symposium IEEE*.

Henseler, J., (2000), Computer crime and computer forensics. In *The encyclopedia of forensic science*.

Hitchcock, B., Le-Khac, N.A. and Scanlon, M., (2016.), Tiered Forensic Methodology Model for Digital Field Triage by Non-Digital Evidence Specialists. *Digital Investigation*, **16**, 75–85.

Holt, T. J., and Bossler, A. M., (2016), *Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses. Crime Sciences Series*. New York: Routledge.

Holt, T. J., Bossler, A.M, and Seigfried-Spellar, K. C., (2018), *Cybercrime and Digital Forensics: An Introduction*. 2nd ed. New York: Routledge.

ISO (2018) ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary. [online] <https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en>

Jeong, D,(2020) Artificial Intelligence Security, Threat, Crime, and Forensics. Taxonomy and open issues. IEEE access. **8**, 184560 – 184574.

Kenneally, E.K., (2005), The Internet is the Computer: the role of forensics in bridging the digital and physical divide. *Digital Investigation*. **2**:1, 41-44.

Khammas, B.,(2018) Malware Detection using Sub-Signatures and Machine Learning Technique. In *Journal of Information Security Research*. **9**:3, 96-106.

Khatter., K.,Singh, S.,(2017), Taxonomy of Digital Forensics: Investigation Tools and Challenges. Online: <https://www.researchgate.net/publication/319930189>.

Li X.Z. ,(2017), Cyber Crime and Legal Countermeasures: A Historical Analysis, *International Journal of Criminal Justice Sciences*, **12**,196-207.

Marshal, J.B., and Saulawa M.A., Cyber attacks: the legal response. *International Journal of International Law* **1**:2.

Mughisa D., (2019), Digital Forensics : Digital evidence in judicial system. In *International Journal of Cyber Criminology 4(DF)*.

Ottis, R., and Lorents, P.,(2010). Cyberspace: Definition and Implication. In *Proceeding of the 5th International Conference Information Warfare and Security*. Ohio, USA: The Air Force Institute of Technology, pp. 267–269.

Palmer, G., (2001), A road map for digital forensic research. In *First Digital Forensic Research Workshop*, Utica, New York.

- Perumal, S., (2009), Digital Forensic Model Based on Malaysian Investigation Process. *International Journal of Computer Science and Network Security*, **9**, 38–44.
- Pollitt, M.M., (2007). An Ad Hoc Review of Digital Forensic Models. In *Proceedings of 2nd International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE 2007)*, pp. 43–54.
- Pradillo J.C.O., (2011), Fighting against Cybercrime in Europe: The Admissibility of Remote Searches in Spain, *European Journal of Crime, Criminal Law and Criminal Justice*, **19**, 363–395.
- Prasanthi, V.,B., (2016) Cyber Forensic Tools: A Review. *International Journal of Engineering Trends and Technology (IJETT)*, **41**:5.
- Rana N, Sansawal G, Khatter K, and Singh S., (2017), Taxonomy of Digital Forensics: Investigation tools and challenges. *Cornell University repository*.
- Reith, M., Carr, C., and Gunsh, G., (2002), An Examination of Digital Forensics Models. *International Journal of Digital Evidence*, **1**:3.
- Rogers, M. K., Goldman, J., Mislán, R., Wedge, T., and Debrota, S., (2006), Computer Forensic Field Triage Process Model, In *Conference on Digital Forensics, Security and Law*.
- Ryan, D.J., Shpantzer, G., (2002) Legal aspects of digital forensics In *Proceedings: Forensics Workshop*. <http://euro.ecom.cmu.edu/program/law/08-732/Evidence/RyanShpantzer.pdf>
- Sarre R., Lau L.Y. and Chang, L.Y.C, (2018), Responding to cybercrime: current trends. *Police Practice and Research An international Journal* **19**:6, 515-518.
- Stoyanov. M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., and Markakis E., (2020), A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues. *IEEE Communications surveys & Tutorials* **22**:2, 1191- 1221.
- Strydom L (2001), Computer Evidence. In *2nd World Conference on the Investigation of Crime, ICC Dec. 2001, Durban*.
- Sumathi, S., Sivanandam, S.N., (2006), Major and Privacy Issues in Data Mining and Knowledge Discovery. *Studies of Computational Intelligence* **29**, 271-291.

Tcherni, M., Davies A., Lopes G., and Lizotte A., (2016), The Dark Figure of Online Property Crime: Is Cyberspace Hiding a Crime Wave?, *Justice Quarterly* **33**: 890–911.
doi:10.1080/07418825.2014.994658.

Varol,A., Sonmez, Y., (2017) The importance of Web Activities for Computer Forensics. In *2nd International Conference on Computer Science and Engineering IEEE*.

Von Solms, R, Van Niekerk, J., (2013), From information security to cyber security. *Computers & Security* **38**, 97-102.

Yusoff, Y., Ismail, R.,and Hassan, Z., (2011) Common phases of computer forensics investigation models. *International Journal of Computer Science & Information Technology (IJCSIT)*, **3**:3, 17-31.