Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών

«Κατανεμημένα Συστήματα, Ασφάλεια και Αναδυόμενες Τεχνολογίες Πληροφορίας»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Επιθέσεις τύπου Ransomware και η ανίχνευση των επιτιθέμενων μέσα από την αλυσίδα του Blockchain** **Ransomware attacks and the process of tracking the attackers within the Blockchain**
Ονοματεπώνυμο Φοιτητή	Αλκαίος - Δημήτριος Αναγνωστόπουλος
Πατρώνυμο	Αθανάσιος
Αριθμός Μητρώου	ΜΠΚΣΑ/ 18003
Επιβλέπων	Κωνσταντίνος Πατσάκης, Αναπληρωτής Καθηγητής

Ημερομηνία Παράδοσης Ιούλιος 2021

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Κωνσταντίνος Πατσάκης	Ευθύμιος Αλέπης	Ευάγγελος Σακκόπουλος
Αναπληρωτής Καθηγητής	Αναπληρωτής Καθηγητής	Επίκουρος Καθηγητής

Η παρούσα μεταπτυχιακή διατριβή είναι αφιερωμένη στην μητέρα μου

ΕΥΧΑΡΙΣΤΙΕΣ

Μέσω της παρούσας μεταπτυχιακής διατριβής, θέλω να ευχαριστήσω τον επιβλέποντα καθηγητή μου Κωνσταντίνο Πατσάκη, ο οποίος μου έδωσε την ευκαιρία να ασχοληθώ με το συγκεκριμένο αντικείμενο, ενώ υπήρξε υποστηρικτικός και καθοδηγητικός καθ'όλη τη διάρκεια συγγραφής της.

Παράλληλα, θα ήθελα να ευχαριστήσω τον φίλο και συνεργάτη μου Αχιλλέα Παπαγεωργίου υπ. Διδάκτορα του Πανεπιστημίου Πειραιώς, ο οποίος συνέβαλε στον εμπλουτισμό και την ενίσχυση των ερευνητικών και συγγραφικών μου δεξιοτήτων.

Τέλος, θα ήθελα να ευχαριστήσω την οικογένειά μου, η οποία συνεχίζει να με στηρίζει ανά τα έτη, παρά τις όποιες δυσκολίες που έχουν εμφανιστεί.

ABSTRACT

In this postgraduate dissertation, the mode of action of a ransomware attack, the method of payment of the attacker to decrypt the affected files on the victim's computer and the creation of a methodology for detecting the attacker were studied.

In the second phase of this project, a Web Application was created using the programming and markup languages PHP, JavaScript, HTML5 & CSS3 and the technology of creating RESTful APIs. This application aims to detect transactions and the "electronic wallet" of the attacker inside the Blockchain. The reason for creating and, consequently, using this particular web application is to properly integrate the Blockchain API with a more user-friendly interface to display all of these transactions involving the potential attacker.

Keywords: Malware, Malware campaigns, Ransomware attack, Blockchain, Wallet Track.

ΠΕΡΙΛΗΨΗ

Στην παρούσα μεταπτυχιακή διατριβή, μελετήθηκε ο τρόπος δράσης μιας επίθεσης τύπου ransomware, ο τρόπος πληρωμής του επιτιθέμενου για την αποκρυπτογράφηση των επηρεαζόμενων αρχείων στη συσκευή του θύματος αλλά και η δημιουργία μεθοδολογίας για την ανίχνευση του επιτιθέμενου.

Εν συνεχεία, δημιουργήθηκε ένα Web Application με τη χρήση των γλωσσών προγραμματισμού και σήμανσης PHP, JavaScript, HTML5 & CSS3, καθώς και την τεχνολογία των RESTful APIs, το οποίο αποσκοπεί στην ανίχνευση των συναλλαγών και του “ηλεκτρονικού πορτοφολιού” του επιτιθέμενου εντός του Blockchain. Ο λόγος δημιουργίας και κατ’ επέκταση, χρήσης του συγκεκριμένου web application είναι η ορθή ενσωμάτωση του Blockchain API με ένα πιο φιλικό περιβάλλον απεικόνισης όλων αυτών των συναλλαγών που αφορούν τον επιτιθέμενο.

Λέξεις κλειδιά: Malware, Malware campaigns, Ransomware attack, Blockchain, Wallet Track.

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΡΟΛΟΓΟΣ

Η παρούσα μεταπτυχιακή διατριβή, είναι αποτέλεσμα μελέτης, της θεωρίας γύρω από τα Malware Campaigns και κυρίως τις επιθέσεις τύπου Ransomware, παραθέτοντας πληροφορίες για τη φύση τους, τον τρόπο που αλληλεπιδρούν με τον απλό χρήστη αλλά και τον τρόπο που διαμοιράζουν τις πληρωμές των θυμάτων σε κρυπτονομίσματα, μέσα από την αλυσίδα του Blockchain.

Οι τεχνολογίες οι οποίες αναλύονται έχουν να κάνουν με την αρχιτεκτονική και τον τρόπο λειτουργίας του ίδιου του Blockchain, ενώ παράλληλα αναλύεται ο τρόπος με τον οποίο ένας αναλυτής ασφάλειας, μπορεί να εντοπίσει κατά προσέγγιση, τον ίδιο τον επιτιθέμενο. Η έρευνα αλλά και η συγκέντρωση στοιχείων γύρω από τον επιτιθέμενο, είναι διαδικασίες οι οποίες αναπτύχθηκαν παράλληλα, αφού κατά την περίοδο συγγραφής και ανάλυσης η κατηγορία επίθεσης Ransomware εξελίσσεται ολοένα και περισσότερο, ενώ την ίδια χρονική στιγμή το μέγεθος της αλυσίδας του Blockchain αυξάνεται εκθετικά ως προς τη μονάδα μέτρησης του χρόνου.

Πιο συγκεκριμένα, η διατριβή αυτή χωρίζεται σε τρεις φάσεις. Η πρώτη φάση της συλλογής πληροφοριών, αφορά οποιαδήποτε πληροφορία γύρω από τα Malware Campaigns και τον τρόπο που δρουν ανά τα έτη, ενώ εστιάζει στον τύπο επίθεσης Ransomware. Από τη στιγμή εμφάνισής του έως και σήμερα έχει αλλάξει σε μεγάλο ποσοστό, αν και η ιδέα πίσω από τον τρόπο που διενεργείται των Ransomware παραμένει η ίδια. Η κρυπτογράφηση δεδομένων του θύματος και η συλλογή λύτρων με τρόπο ανωνυμοποιημένο από την πλευρά του επιτιθέμενου, παραμένουν οι πρωταρχικοί στόχοι μιας Ransomware επίθεσης.

Κατά τη δεύτερη φάση της διατριβής, πραγματοποιήθηκε ανάλυση μέσα στην αλυσίδα του Blockchain, με εστίαση στο κρυπτονόμισμα Bitcoin, αλλά και στον τρόπο με τον οποίο “ταξιδεύει” η πρώτη συναλλαγή από το θύμα προς τον επιτιθέμενο, έως ότου ο δεύτερος συλλέξει τα χρήματα και προβεί σε εξαργύρωσή τους. Παρατίθενται πληροφορίες για το πως λειτουργεί η αλυσίδα του Blockchain, τι σημαίνει block και τι ανωνυμοποιημένες συναλλαγές με την έγκριση της πλειοψηφίας των μελών της αλυσίδας, αλλά και ποιοι περιορισμοί δημιουργούνται όταν ένας αναλυτής προσπαθεί να ενώσει τα παραπάνω κομμάτια.

Στην τρίτη και τελευταία φάση, αναπτύχθηκε μια ηλεκτρονική εφαρμογή, η οποία δέχεται ως είσοδο, πληροφορίες για μια διεύθυνση του Blockchain και επιστρέφει τα αποτελέσματα που έχει συλλέξει, με αντικειμενοστραφή τρόπο στην οθόνη του χρήστη. Παράλληλα, ο χρήστης έχει τη δυνατότητα αποθήκευσης ορισμένων κρίσιμων, για αυτόν, πληροφοριών. Αυτή η εφαρμογή, σε αντίθεση με παρεμφερείς έρευνες γύρω από την αναζήτηση του επιτιθέμενου, διαθέτει τους λιγότερο δυνατούς πόρους που υφίστανται για την ορθή λειτουργία της. Αυτό σημαίνει, πως ο αναλυτής θα πρέπει να αντιμετωπίσει συγκεκριμένους περιορισμούς, τους οποίους μπορεί να ξεπεράσει μόνο εφόσον η αρχιτεκτονική και ο τρόπος λειτουργίας της εφαρμογής, μεταβούν σε ένα πλάνο που εκμεταλλεύεται περισσότερες πηγές υπολογιστικής ισχύος και υπηρεσίες τρίτων μερών με οικονομικό κόστος.

ΕΙΣΑΓΩΓΗ

Είναι γνωστό, πως ο κόσμος του διαδικτύου κατακλύζεται σε καθημερινή βάση από πληθώρα ηλεκτρονικών επιθέσεων που ως κύριο σκοπό έχουν την αποκόμιση χρηματικών ποσών - και όχι μόνο - από τα θύματά τους.

Οι επιθέσεις αυτές μπορούν να γίνουν με τη χρήση πολλών μέσων και απευθύνονται είτε σε ένα θύμα, είτε σε ομάδες θυμάτων. Πολλές φορές βέβαια, αυτή η ομάδα θυμάτων μπορεί να αποτελείται από μικρές επιχειρήσεις/εταιρείες, πολυεθνικές ή/και μεγάλες κοινότητες ατόμων.

Παράλληλα, η αποκόμιση χρηματικών ποσών, γίνεται κατά κύριο λόγο με τρόπο ασφαλή για τους επιτιθέμενους όπως για παράδειγμα η συναλλαγή με τη χρήση κρυπτονομισμάτων, όπως το Bitcoin, μέσα στην αλυσίδα του Blockchain. Με αυτόν τον τρόπο διασφαλίζεται η ανωνυμότητά τους, ενώ ο βαθμός δυσκολίας για τον εντοπισμό τους από τις αρμόδιες αρχές, αυξάνεται ραγδαία.

Την ίδια χρονική στιγμή, η πρόληψη του προσωπικού σε θέματα ασφάλειας παραμένει σε χαμηλά επίπεδα, τα ίδια τα θύματα πραγματοποιούν στην πλειοψηφία τους τις πληρωμές προς τους επιτιθέμενους ενώ από τον τομέα της Ασφάλειας πληροφοριακών συστημάτων εκλείπει ένας τρόπος αντιμετώπισης του δεδομένου προβλήματος. Αυτοί είναι και οι λόγοι που τα Malware Campaigns εξελίσσονται ολοένα και περισσότερο ώς προς τη λήψη αγαθών από τα θύματά τους, αλλά και προς την τεχνολογική τους εξέλιξη.

ΚΕΦΑΛΑΙΟ 1ο: Τι είναι τα Malware Campaigns;

Ο τρόπος διάδοσης μιας επίθεσης από έναν επιτιθέμενο ή μια οικογένεια επιτιθέμενων σε ένα σύνολο ανθρώπων, ονομάζεται Malware Campaign.

1.1. Περιγραφή των Malware Campaigns

Τα Malware Campaigns, αποτελούν έναν ιδιαιτέρως διαδεδομένο τρόπο επίθεσης καθώς μπορούν να στοχεύσουν ταυτόχρονα πολλές ομάδες ανθρώπων. Ο τρόπος με τον οποίο λειτουργούν είναι με τη μαζική αποστολή κακόβουλου λογισμικού σε άτομα της ομάδας, αναμένοντας μόνο ένα από αυτά τα άτομα να εκτελέσει τον κακόβουλο κώδικα εν αγνοία του [1].

Επί παραδείγματι, ο τρόπος επίτευξης μιας τέτοιας επίθεσης θα μπορούσε να είναι η ενοικίαση πολλών φυσικών πόρων (ηλεκτρονικοί υπολογιστές από εταιρεία φιλοξενίας λογισμικού), οι οποίοι επικοινωνούν με έναν κεντρικό διακομιστή για να λάβουν το κακόβουλο λογισμικό και με τη σειρά τους να το δρομολογήσουν προς τα θύματα του επιτιθέμενου με τη χρήση ηλεκτρονικού ταχυδρομείου.

Εάν στο παραπάνω παράδειγμα προστεθούν πραγματικοί αριθμοί κατά προσέγγιση, τότε υπολογίζεται ότι με μέσο όρο την αποστολή 100 ηλεκτρονικών μηνυμάτων ανά ημέρα και όριο παραληπτών 100 χρήστες ανά μήνυμα (τα ποσά διαφέρουν σύμφωνα με τον εκάστοτε πάροχο), μόνο δέκα φυσικά μηχανήματα αρκούν για την αποστολή 100.000 μηνυμάτων σε τυχαίους χρήστες.

Συμπερασματικά, ο σκοπός του επιτιθέμενου είναι να εκτελεστεί το κακόβουλο λογισμικό από έναν από αυτούς ώστε να μολυνθεί και το υπόλοιπο του συνόλου στο οποίο ανήκει. Βέβαια, ακόμα και η μόλυνση ενός πολύ χαμηλού ποσοστού του παραπάνω συνόλου, μπορεί να χαρακτηρίσει την επίθεση ως άκρως επικίνδυνη.

1.2. Τύποι επιθέσεων

Οι τύποι των επιθέσεων με τη χρήση ενός Malware Campaign μπορούν να διαφέρουν ώς προς το κακόβουλο λογισμικό που θα χρησιμοποιηθεί ή τον τρόπο μετάδοσής του προς το πιθανό θύμα, αλλά η αρχιτεκτονική αυτής της επίθεσης παραμένει κοινή ανάμεσα στις οικογένειες των Malware Campaigns και αντικατοπτρίζει τη μαζική μόλυνση ενός δικτύου, εκμεταλλευόμενη τις ευπάθειες αυτού [2].

Κάποιοι από τους τρόπους με τους οποίους μπορούν να μεταδοθούν αυτές οι επιθέσεις είναι με τη χρήση [3]:

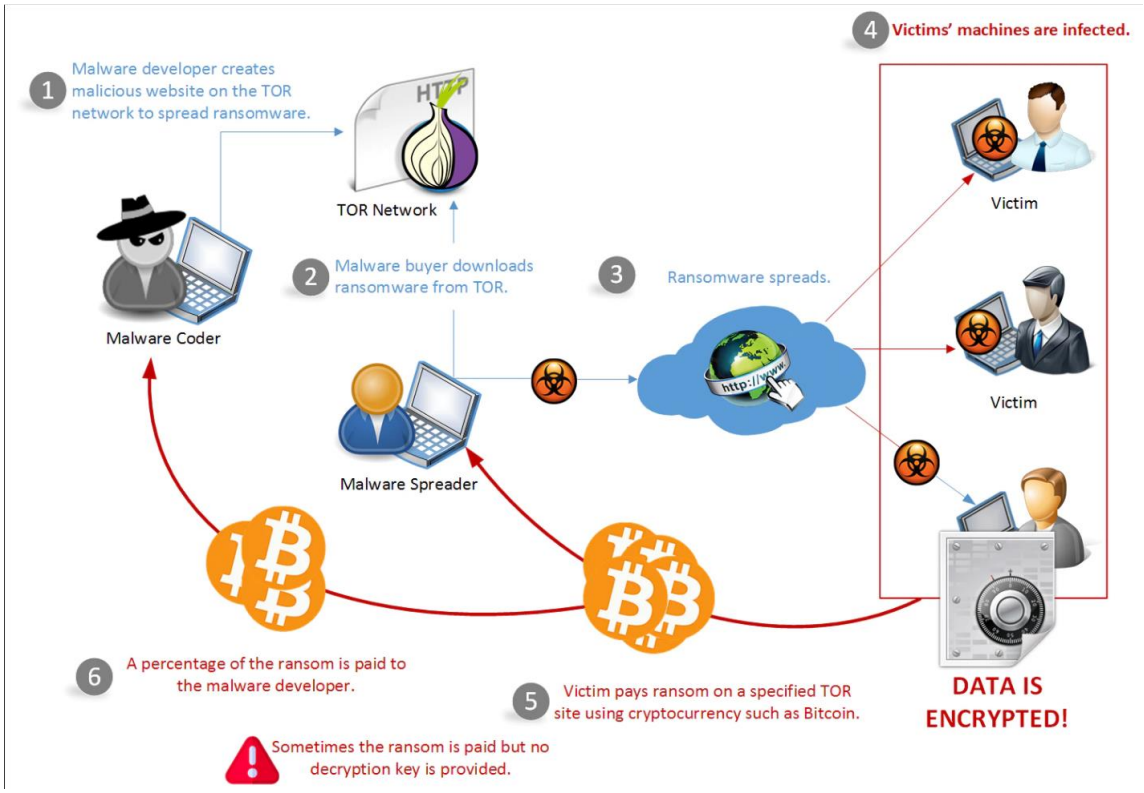
1. Phishing Emails: Πληθώρα από ηλεκτρονικά μηνύματα που αποστέλλονται σε μια ομάδα ατόμων και περιέχουν συνδέσμους προς έναν ιστότοπο για τη λήψη του κακόβουλου λογισμικού ή συνημμένα αρχεία, συνήθως συμπιεσμένα αρχεία τύπου .tar.bz2, .tar.gz, .zip, κ.α. Μόλις το θύμα επισκεφτεί την ιστοσελίδα ή αποσυμπιέσει το συνημμένο του μηνύματος και διαβάσει τα αρχεία, εκτελείται το κακόβουλο λογισμικό.

2. Μέσα αποθήκευσης πληροφοριών: Η χρήση μιας συσκευής αποθήκευσης όπως USB stick, οπτικά μέσα (CD/DVD), σκληροί δίσκοι, κ.α. είναι μια διαδεδομένη μέθοδος αποθήκευσης κακόβουλου λογισμικού. Ο επιτιθέμενος αποθηκεύει στην εκάστοτε συσκευή το κακόβουλο λογισμικό και έπειτα την απορρίπτει σε ένα εμφανές, για το

θύμα, σημείο. Το θύμα με τη σειρά του χρησιμοποιεί τη συσκευή και μολύνει τον προσωπικό του Η/Υ και κατ' επέκταση το δίκτυο στο οποίο ανήκει.

3. Cross-site Scripting: Ο όρος Cross-site Scripting ή XSS, αφορά τη χρήση κακόβουλου λογισμικού, ανεπτυγμένου συνήθως με γλώσσες λογισμικού όπως οι HTML και JavaScript. Ο επιτιθέμενος σε αυτή την περίπτωση, εκμεταλλεύεται ευπάθειες ενός ιστοτόπου με μεγάλη επισκεψιμότητα, όπως η εισαγωγή δεδομένων στον ιστότοπο χωρίς τη χρήση των απαραίτητων φίλτρων, και εκτελεί το κακόβουλο λογισμικό. Αυτό με τη σειρά του μπορεί να εκτελείται κάθε φορά που κάποιος απλός επισκέπτης εισέρχεται σε μία από τις μολυσμένες ιστοσελίδες του ιστοτόπου, με αποτέλεσμα να λαμβάνει το κακόβουλο λογισμικό και να μολύνεται και εκείνος.

4. Εκτελέσιμα αρχεία: Η χρήση εκτελέσιμων αρχείων στα Malware Campaigns δεν είναι απαραίτητο να γίνει μέσω κάποιου τρίτου μέρους. Ο επιτιθέμενος έχει τη δυνατότητα, εφόσον εκμεταλλευτεί κάποιο backdoor του δικτύου, να εγκαταστήσει είτε στον προσωπικό υπολογιστή του θύματος, είτε στο ίδιο το δίκτυο, εκτελέσιμα αρχεία ή συντομεύσεις τα οποία μόλις το θύμα εκτελέσει θα εκκινήσουν το κακόβουλο λογισμικό. Τις περισσότερες φορές, τα αρχεία αυτά είναι τύπου .exe, συνεπώς εκτελούνται αμέσως ή είναι τύπου .LNK (συντομεύσεις ενός εκτελέσιμου αρχείου) & Symbolic Links (θέσεις στο δίκτυο που παραπέμπουν σε μια κρυφή θέση με το εκτελέσιμο αρχείο).



Εικ: 1.1: Διάδοση ενός Ransomware
(Πηγή: **https://www.mcafee.com/blogs/mcafee-labs/free-ransomware-available-dark-web/**)

Στον παρακάτω πίνακα, παρατίθενται οι πιο διαδεδομένοι τύποι κακόβουλου λογισμικού που μπορούν να χρησιμοποιηθούν για την εκτέλεση ενός Malware Campaign [1] ή που συμβάλλουν στην προετοιμασία που χρειάζεται ένας επιτιθέμενος ώστε να εκτελεστεί το Malware Campaign:

Οικογένεια κακόβουλου λογισμικού	**Περιγραφή**	**Πραγματικά παραδείγματα**
Ransomware	Κρυπτογραφεί τα δεδομένα του θύματος και αποκλείει την πρόσβαση σε αυτά έως ότου πληρωθούν τα ζητούμενα λύτρα στον επιτιθέμενο	RYUK
Fileless Malware	Πραγματοποιεί αλλαγές σε πηγαία αρχεία του λειτουργικού συστήματος του θύματος	Astaroth
Spyware	Συλλέγει πληροφορίες για τον χρήστη, συνήθως για τον τρόπο χρήσης του προσωπικού του Η/Υ, εν αγνοία του	DarkHotel
Adware	Παραθέτει στον χρήστη μη αποδεκτό διαφημιστικό περιεχόμενο	Fireball
Trojans	Μέρος κακόβουλου λογισμικού που προσποιείται τη δομή ενός επιτρεπόμενου από το σύστημα, λογισμικού	Emotet
Worms	Μεταφέρεται εντός του δικτύου αναπαράγοντας εκ νέου τον εαυτό του	Stuxnet
Rootkits	Επιτρέπει στον επιτιθέμενο το χειρισμό της συσκευής του θύματος, εξ αποστάσεως	Zacinlo
Keyloggers	Καταγράφει με σειριακό τρόπο την πληκτρολόγηση του θύματος στη συσκευή του	Olympic Vision
Bots	Πυροδοτεί μια σειρά από πολλαπλές επιθέσεις στο θύμα την ίδια χρονική στιγμή	Echobot
Mobile Malware	Μολύνει κινητές συσκευές όπως smartphones και tablets	Triada

Πίνακας 1.1: Γνωστοί τύποι malware και πραγματικά παραδείγματα

1.3. Κοινό που στοχεύουν

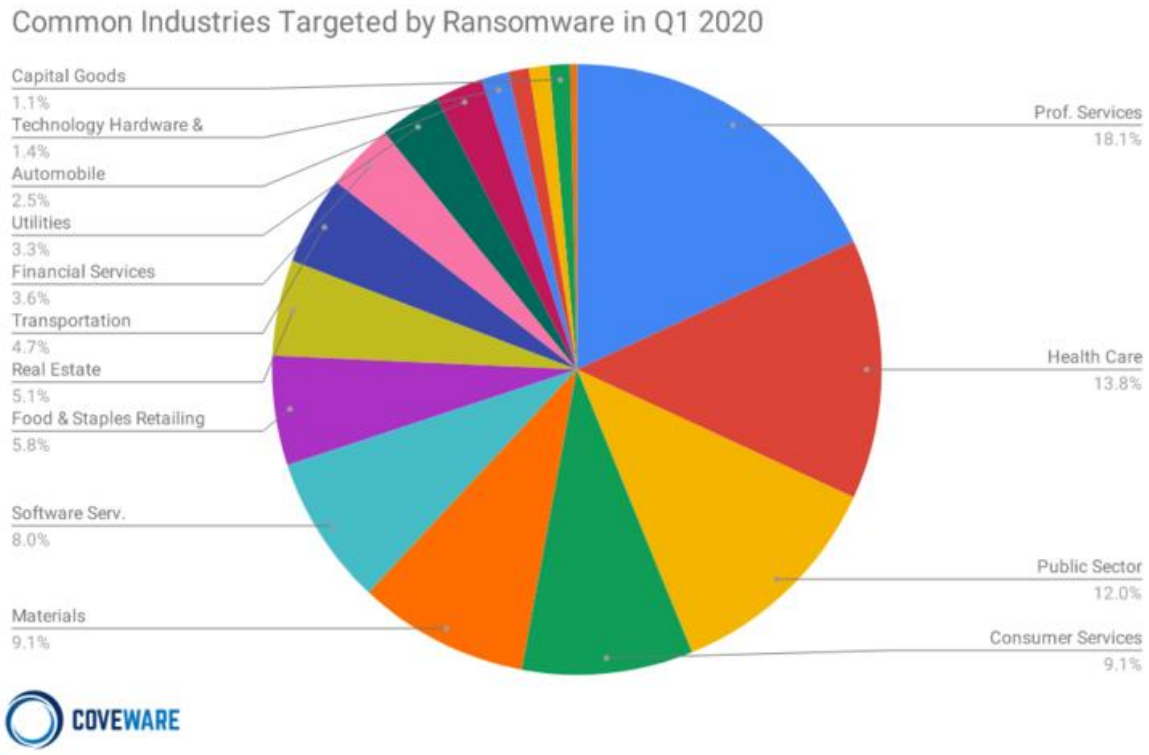
Όπως αναφέρθηκε και στην εισαγωγή του παρόντος κεφαλαίου, το κοινό στο οποίο στοχεύει ένα Malware Campaign διαφοροποιείται ποσοτικά και ποιοτικά. Από τη στιγμή που ένα Malware Campaign εκτελείται, θα πρέπει σε δεδομένο χρονικό διάστημα από τη στιγμή της επίθεσης να μολύνει όσο το δυνατόν περισσότερους χρήστες στο διαδίκτυο.

Η επιλογή μεταξύ ποσοτικής ή ποιοτικής επίθεσης (ή και των δύο), έχει να κάνει με τις δυνατότητες του κακόβουλου λογισμικού που θα χρησιμοποιηθεί, όπως και με τις ευπάθειες του στοχευμένου συστήματος, που είναι εκμεταλλεύσιμες εκείνη τη χρονική στιγμή αλλά δεν είναι ακόμη γνωστές στο ευρύ κοινό (zero day vulnerabilities). Φυσικά, δεν αποκλείονται ευπάθειες οι

οποίες είναι ήδη γνωστές στο στοχευμένο σύστημα, αλλά ο εκάστοτε οργανισμός δεν έχει προβεί στην εφαρμογή μιας αναβάθμισης που επιλύει το πρόβλημα.

Στην περίπτωση της ποσοτικής επίθεσης, τα Malware Campaigns στοχεύουν σε όσο το δυνατόν περισσότερους χρήστες ενός συνόλου. Αυτό το σύνολο θα μπορούσε να είναι οι χρήστες μιας ηλεκτρονικής πλατφόρμας με πληθώρα χρηστών όπως ένας ιστότοπος (π.χ. Facebook, Instagram, E-bay), οι χρήστες ενός γνωστού λογισμικού διεπικοινωνίας (π.χ. Zoom, Skype) ή οι χρήστες που οι ηλεκτρονικές τους διευθύνσεις έχουν διαρρεύσει από οποιοδήποτε ηλεκτρονικό μέσο και ο επιτιθέμενος έχει δημιουργήσει αντίστοιχες λίστες προώθησης, του κακόβουλου λογισμικού. Σε αυτήν την περίπτωση, ο επιτιθέμενος θα ζητήσει ένα ποσό X σε λύτρα, ώστε να επαναφέρει τη συσκευή του θύματος στην αρχική του κατάσταση, το οποίο συνήθως είναι αντικειμενικά προσιτό. Με αυτόν τον τρόπο, ο επιτιθέμενος αποσκοπεί στην απολαβή λύτρων από ένα μεγάλο ποσοστό του συνόλου.

Αντίθετα, στην περίπτωση της ποιοτικής επίθεσης, ο επιτιθέμενος μπορεί να στοχεύσει σε ιδιωτικά δίκτυα εταιρειών, τραπεζών ή κρατικών οργανισμών, όπου το στοχευμένο σύνολο είναι σαφώς μικρότερο από εκείνο μιας ποσοτικής επίθεσης, αλλά το κόστος της φθοράς που θα προκληθεί είναι εκθετικά μεγαλύτερο και προφανώς περισσότερο επωφελές, από πλευράς λύτρων.



Εικ. 1.2: Στόχοι μιας Ransomware επίθεσης κατά το 1ο τετράμηνο του 2020
(Πηγή: **https://www.coveware.com/blog/q1-2020-ransomware-marketplace-report**)

ΚΕΦΑΛΑΙΟ 2ο: Η χρήση Ransomware στα Malware Campaigns

Μία από τις πιο διαδεδομένες επιθέσεις ενός Malware Campaign είναι αυτή με τη χρήση Ransomware. Τα ransomwares κρυπτογραφούν κατά κύριο λόγο την πρόσβαση στα αρχεία του θύματος και ο επιτιθέμενος ζητάει λύτρα ώστε να την αποκρυπτογραφήσει (συνήθως σε μορφή κρυπτονομίσματος).

Οι επιθέσεις με τη χρήση ransomware, θεωρούνται αυτές με το μεγαλύτερο ποσοστό ζημίας για το θύμα, καθώς εάν δεν πληρωθούν τα λύτρα που ζητά ο επιτιθέμενος, τότε όλα τα αρχεία του θύματος κρυπτογραφούνται και μπορούν να θεωρηθούν κατεστραμμένα.

Αντίστοιχα, εάν το θύμα πληρώσει τον επιτιθέμενο και εκείνος με τη σειρά του αποκρυπτογραφήσει την πρόσβαση προς τα αρχεία του θύματος, η ζημία θα είναι οικονομική και στις περισσότερες περιπτώσεις καταστρεπτική για το θύμα. Ιδιαίτερα εάν το σύνολο που αποτελεί το στόχο του Ransomware Campaign είναι κάποιος οργανισμός, τράπεζα ή εταιρεία.

Σε αυτή την περίπτωση, το θύμα είναι πολύ δύσκολο να ανακάμψει μετά από μια τόσο μεγάλη οικονομική καταστροφή, ακόμα και στις περιπτώσεις που έχει προβλεφθεί και δημιουργηθεί κάποιο σχέδιο επιχειρησιακής συνέχειας (Business Continuity Plan).

2.1. Τι είναι το Ransomware

Το Ransomware είναι ένα υποσύνολο από κακόβουλα λογισμικά ή μέρη πηγαίου κώδικα, τα οποία στοχεύουν αρχικά στον αποκλεισμό της πρόσβασης του θύματος από τη συσκευή του και στη συνέχεια στην κρυπτογράφηση μιας συγκεκριμένης θέσης αρχείων. Σε κάποιες περιπτώσεις, η κρυπτογράφηση δρα σε ολόκληρο το αποθηκευτικό μέσο της συσκευής. Το κίνητρο αυτής της επίθεσης είναι η απόσπαση χρημάτων από το θύμα [4].

Με αυτόν τον τρόπο, η διαθεσιμότητα των αρχείων του θύματος καταργείται. Σε αρκετές περιπτώσεις βέβαια, διακυβεύεται και η ακεραιότητα των αρχείων, αφού ο επιτιθέμενος μπορεί είτε εκ προθέσεως είτε εξ αμελείας, να παραμετροποιήσει κάποια από τα αρχεία που έχουν κρυπτογραφηθεί, ενώ η εμπιστευτικότητα τους αναιρείται καθώς οι περιπτώσεις διατήρησης αντιγράφων από τους επιτιθέμενους πληθαίνουν.

Για την επαναφορά της πρόσβασης ή και την αποκρυπτογράφηση των παραπάνω αρχείων, ο επιτιθέμενος θα απαιτήσει να πληρωθούν λύτρα, τις περισσότερες φορές στη μορφή κρυπτονομισμάτων όπως τα Bitcoin (BTC), Monero, Ether, κ.α., ώστε να διασφαλίσει την ανωνυμότητα της ταυτότητάς του και να μην μπορεί να αναγνωριστεί από το θύμα ή τις αρμόδιες αρχές.

2.2. Τρόπος λειτουργίας ενός Ransomware Campaign

Η εκτέλεση ενός Ransomware Campaign περιέχει κάποια συγκεκριμένα βήματα για την επίτευξή της, αλλά για τη δημιουργία της χρειάζεται να μελετηθεί ένα μεγάλο φάσμα από πληροφορίες σχετικές με το θύμα, τις τεχνολογίες που θα χρησιμοποιηθούν, τον τρόπο μετάδοσης του malware αλλά και τη συλλογή των λύτρων.

Τα περισσότερα ransomware εκμεταλλεύονται ευπάθειες του συστήματος στη συσκευή ενός χρήστη, ή του δικτύου στο οποίο βρίσκεται ή ακόμη και την έλλειψη ενημέρωσης του ίδιου για σχετικές επιθέσεις.

Όπως προαναφερθηκε στο 1ο Κεφάλαιο, οι τρόποι μετάδοσης του ransomware ποικίλουν. Παραδείγματα αποτελούν η εκτέλεση ενός συνημμένου σε ένα ηλεκτρονικό μήνυμα, η λήψη αρχείων από το εσωτερικό chat ενός μέσου κοινωνικής δικτύωσης, το πάτημα ενός συνδέσμου σε ένα pop-up μήνυμα ενός ιστοτόπου ή σε μια ανεπιθύμητη διαφήμιση, κ.α.

Από τη στιγμή που το σύνολο του κακόβουλου λογισμικού που εμπεριέχεται στο αρχείο που θα ανοίξει ο χρήστης, εκτελεστεί, θα ξεκινήσει μια αλληλουχία προσπαθειών για τον αποκλεισμό της πρόσβασης από τη συσκευή του, ενώ παράλληλα θα κρυπτογραφηθούν συγκεκριμένες θέσεις αρχείων ή και ολόκληρα τμήματα μονάδων αποθήκευσης [5].

Εικ. 2.1: Οι φάσεις μιας επίθεσης τύπου Ransomware
(Πηγή: **https://www.carbonblack.com/2016/09/19/how-ransomware-works/**)

Ο τρόπος κρυπτογράφησης των αρχείων γίνεται συνήθως με ασύμμετρη κρυπτογράφηση, χρησιμοποιώντας αλγόριθμους όπως ο RSA (Rivest–Shamir–Adleman) [8]. Σε αυτού του είδους την κρυπτογράφηση απαιτείται η χρήση δύο κλειδιών, ενός δημόσιου και ενός ιδιωτικού. Με τη χρήση του δημόσιου κλειδιού κρυπτογραφούνται τα δεδομένα και με τη χρήση του ιδιωτικού κλειδιού αποκρυπτογραφούνται. Στην περίπτωση βέβαια ενός ransomware, οι αρχές δημιουργίας και ο τρόπος παραγωγής αυτών των κλειδιών είναι ο λόγος για τον οποίο είναι σχεδόν αδύνατο να αποκρυπτογραφηθούν τα δεδομένα ενός χρήστη χωρίς τη χρήση του κλειδιού αποκρυπτογράφησης.

Για την παραγωγή αυτού του ζεύγους κλειδιών με βάση τον ορισμό του RSA αλγορίθμου απαιτούνται τα παρακάτω βήματα [6][7][8]:

1. Η επιλογή δύο τυχαίων μεγάλων πρώτων αριθμών A και B, όπου A ≠ B
2. Ο υπολογισμός του $X = A \cdot B$
3. Ο υπολογισμός της συνάρτησης του Euler, $\varphi(X) = (A - 1) \cdot (B - 1)$
4. Η επιλογή ενός αριθμού e > 1, ώστε $e^{\varphi(X)} \equiv 1 \pmod{X}$
5. Ο υπολογισμός ενός αριθμού d έτσι ώστε $d \equiv e^{-1} \pmod{\varphi(X)}$

Το ζευγάρι των κλειδιών που θα δημιουργηθεί αντιστοιχεί στα:

- Κλειδί κρυπτογράφησης (X, e)
- Κλειδί αποκρυπτογράφησης (X, d)

Με αυτό τον τρόπο, και με τη χρήση δύο πρώτων αριθμών που έχουν προκύψει μέσω πιθανολογικών αλγορίθμων, είναι σχεδόν ακατόρθωτο για ένα υπολογιστικό σύστημα να προβλέψει το κλειδί αποκρυπτογράφησης που απαιτείται για την επαναφορά της πρόσβασης και των αρχείων στον χρήστη.

Τέλος, το σημαντικότερο σημείο της συγκεκριμένης επίθεσης, είναι η μεταφορά του ransomware και στο υπόλοιπο δίκτυο στο οποίο είναι συνδεδεμένη η συσκευή του 1ου θύματος. Σε περιπτώσεις όπου η επίθεση διενεργείται σε κάποιο ιδιωτικό δίκτυο, εφόσον μολυνθεί η πρώτη συσκευή το ransomware μεταφέρεται και στα υπόλοιπα θύματα, με τη δυνατότητα κρυπτογράφησης πληθώρας διακριτών συσκευών, λειτουργικών συστημάτων και θέσεων αρχείων.

2.3. Εκμεταλλεύσιμες ευπάθειες του θύματος

Οι ευπάθειες τις οποίες εκμεταλλεύεται ένας επιτιθέμενος κατά την εκτέλεση ενός Ransomware Campaign διαχωρίζονται σε αυτές που αφορούν το ίδιο το θύμα και τη συσκευή του, ή τον τρόπο χρήσης αυτής, αλλά και σε αυτές που επηρεάζουν έμμεσα ή άμεσα το δίκτυο στο οποίο φιλοξενείται η συσκευή του θύματος.

Οι κατηγορίες αυτές διακρίνονται ενδεικτικά σε:

1. Έλλειψη μέτρων ασφαλείας σε επίπεδο λογισμικού όπως, η χρήση προγραμμάτων αντιμετώπισης κακόβουλου λογισμικού, η χρήση συστημάτων εύρεσης και αντιμετώπισης επιθέσεων π.χ. Firewall, Antivirus, Intrusion Detection/Prevention System, κ.α.
2. Λανθασμένη διαμόρφωση ενός λογισμικού στη συσκευή του θύματος ή στο δίκτυο που ανήκει, π.χ. ανεπαρκής διαμόρφωση κανόνων ενός Firewall ή Anti-malware προγράμματος
3. Μη συχνή ενημέρωση του λογισμικού που χρησιμοποιείται εντός του δικτύου ή στη συσκευή του χρήστη
4. Ανεπαρκής ενημέρωση του χρήστη σχετικά με γνωστές κακόβουλες επιθέσεις αλλά και τρόπων προτροπής τους

Συνήθως οι εκμεταλλεύσιμες ευπάθειες, κυρίως όσον αφορά τις πιο γνωστές οικογένειες Ransomware, δεν είναι αναγνωρίσιμες από το ευρύ κοινό παρά μόνο μετά την επίθεση. Φυσικά, είναι σημαντικό να ακολουθούνται όλες οι βασικές αρχές της ασφάλειας (στο επίπεδο που είναι δυνατόν), καθώς πολλές από τις ευπάθειες που ανακαλύπτονται οφείλονται

σε παλαιότερες εκδόσεις λογισμικού ή σε λάθη διαμόρφωσης λογισμικού που βρίσκουν οι επιτιθέμενοι εντός του δικτύου των χρηστών.

2.4. Γνωστές οικογένειες ransomware ανά τα έτη

2.4.1 AIDS Trojan (1989)

Τα Ransomware campaigns αποτελούν μια μέθοδο επίθεσης η οποία πρωτοεμφανίστηκε το 1989 με το όνομα AIDS Trojan [9] και επηρέασε τον τομέα της υγείας στο συνέδριο για τον ιό του AIDS του Παγκόσμιου Οργανισμού της Υγείας. Ο τρόπος με τον οποίο ο Joseph L. Popp δημιούργησε αυτό το Ransomware Campaign, ήταν γράφοντας σε 20.000 δισκέτες ένα κακόβουλο λογισμικό και μοιράζοντάς το στους παρευρισκόμενους του συνεδρίου.

Η επίθεση είχε ως σκοπό την εγκατάσταση του κακόβουλου λογισμικού στους Η/Υ των θυμάτων οι οποίοι μετά από 90 επανεκκινήσεις το πυροδότησαν. Το λογισμικό με τη σειρά του κρυπτογραφούσε αρχεία και θέσεις αρχείων και εκτύπωνε στα θύματα του ένα μήνυμα που τους παρέπεμπε στην αποστολή χρηματικού ποσού σε συγκεκριμένη διεύθυνση ώστε να επαναφερθεί η κατάσταση του Η/Υ τους [10].

2.4.2 Archievus (2005)

Χρειάστηκε να περάσουν δεκαέξι χρόνια από την καμπάνια του AIDS Trojan, έως ότου να εμφανιστεί μια νέα γενιά από Ransomwares. Το ransomware Archievus [11] μεταδιδόταν μέσω κακόβουλων συνδέσμων από ιστοσελίδες και ανεπιθύμητη ηλεκτρονική αλληλογραφία, χωρίς να διαφαίνεται η μεθοδολογία μετάδοσής του.

Το Archievus επηρέαζε ως επί το πλείστον το λειτουργικό σύστημα Windows, ενώ ανάγκαζε τα θύματά του να επισκεφτούν συγκεκριμένη ιστοσελίδα για την αγορά 30ψήφιου κωδικού ώστε να επαναφερθεί η κατάσταση της συσκευής τους στο φυσιολογικό.

2.4.3 GPCoder (2005)

Την ίδια περίοδο με το Archievus, εμφανίστηκε άλλο ένα ransomware με τη μορφή Trojan, το GPCoder [12]. Στόχευε στον φάκελο “Έγγραφα” ή “My Documents” του λειτουργικού συστήματος Windows, καθώς η πλειοψηφία των ανθρώπων αποθήκευαν πολύτιμες, για αυτούς, πληροφορίες σε αυτή τη διαδρομή. Το θύμα συνέχιζε να έχει πρόσβαση στο υπόλοιπο λειτουργικό σύστημα.

Η σημαντική αλλαγή που έφερε στο προσκήνιο το GPCoder, ήταν η χρήση αλγορίθμου RSA 1024-bit για ασφαλή κρυπτογράφηση των δεδομένων. Συνεπώς το θύμα, ήταν αναγκασμένο να πληρώσει τον επιτιθέμενο, μέσω ενός μηνύματος που εμφανιζόταν στην αρχική οθόνη της συσκευής, και έδινε αναλυτικές οδηγίες για τον τρόπο πληρωμής των λύτρων [13].

2.4.4 Vundo (2009)

Το Vundo ή αλλιώς Virtumonde ή Virtumondo [14] αποτελεί ένα trojan που δημιουργήθηκε για τα Microsoft Windows, το οποίο ήταν υπεύθυνο για την δημιουργία αναδυόμενων παραθύρων τη στιγμή της περιήγησης του χρήστη στη συσκευή του. Πολλές φορές, το περιεχόμενο των συγκεκριμένων παραθύρων αφορούσε στη στοχευμένη διαφήμιση προγραμμάτων τύπου Spyware ενώ σε άλλες περιπτώσεις οδηγούσε στην μείωση της απόδοσης της συσκευής. Ακόμη, έχουν υπάρξει περιπτώσεις όπου το Vundo θεωρήθηκε το μέσο για την μετάδοση επιθέσεων τύπου Denial of Service (DoS) προς τους ιστοτόπους Facebook και Google.

2.4.5 Trojan WinLock (2011)

Το WinLock αποτελεί ένα ιδιαίτερο ransomware καθώς διοχέτευε το κακόβουλο λογισμικό του κυρίως μέσω ειδησεογραφικών ιστοσελίδων. Ο πυρήνας του WinLock στόχευε στο λειτουργικό σύστημα Windows από όπου γινόταν ο αποκλεισμός συγκεκριμένων λειτουργιών του χρήστη, καθιστώντας αδύνατη τη χρήση του Η/Υ και προβάλλοντας στην οθόνη του πορνογραφικό υλικό [15].

Για να επαναφέρει το σύστημα σε λειτουργικό επίπεδο, έπρεπε ο χρήστης να εισάγει έναν κωδικό, καθώς η οθόνη του κλείδωνε λόγω του κακόβουλου κώδικα, τον οποίο μπορούσε να παραλάβει στέλνοντας ένα SMS στον επιτιθέμενο, με κόστος 300 έως 1000 ρούβλια. Η κύρια εμφάνιση του συγκεκριμένου “ransomware”, ήταν στη Ρωσία.

2.4.6 Reveton & ‘Police’ Ransomware (2012)

Τα Ransomware Campaigns, έχουν επιθετικό χαρακτήρα αποκλείοντας την πρόσβαση και κρυπτογραφόντας θέσεις αρχείων του θύματος, με κίνητρο οικονομικές απολαβές.

Φυσικά, υπάρχουν οι χρήστες που δεν θα πληρώσουν τον επιτιθέμενο και θα προσπαθήσουν να αποκρυπτογραφήσουν μόνοι τους τα αρχεία που έχουν μολυνθεί, ή θα αντικαταστήσουν τη συσκευή τους.

Για το λόγο αυτό έκαναν την εμφάνισή τους Ransomwares, που λειτουργούσαν με την ίδια μεθοδολογία μετάδοσης, κρυπτογράφησης και αποκρυπτογράφησης, αλλά προσποιούνταν ότι η ανάκληση της πρόσβασης του θύματος από τη συσκευή του έχει γίνει από Αρμόδιες Αρχές όπως Νομικές ή Αστυνομικές υπηρεσίες. Με αφορμή την “ανίχνευση” παράνομων ενεργειών από την μεριά του θύματος, ο επιτιθέμενος ανάγκάζε το θύμα να πληρώσει ένα πρόστιμο ώστε να μην υπάρξουν νομικές κυρώσεις.

Το πιο γνωστό ransomware τέτοιου τύπου, ήταν το Reveton [16] - με κύρια τοποθεσία τις Η.Π.Α. - προσποιούμενο την κρατική υπηρεσία Federal Bureau of Investigation (F.B.I.) και ζητώντας την πληρωμή προστίμου ύψους $200,00 από το θύμα. Η πληρωμή γινόταν με τη χρήση προπληρωμένων καρτών [17].

2.4.7 CryptoLocker (2013)

Από τον Σεπτέμβριο του 2013 έως και τις αρχές Μαΐου του 2014, το Ransomware CryptoLocker [18] εκτελούνταν σε μεγάλο πλήθος συσκευών με λειτουργικό σύστημα Microsoft Windows. Η επίθεση μόλυνε τις συσκευές με ένα trojan το οποίο όταν ενεργοποιούνταν κρυπτογραφούσε

συγκεκριμένους τύπους αρχείων, σε τοπικές θέσεις ή σε θέσεις του δικτύου, με τη χρήση ασύμμετρης κρυπτογραφίας τύπου RSA. Τα δεδομένα κρυπτογραφούνταν με τη χρήση του δημοσίου κλειδιού ενώ το ιδιωτικό κλειδί βρισκόταν σε ιδιωτικούς servers που ήλεγχε το CryptoLocker.

Το συνάλλαγμα για την πληρωμή ήταν το κρυπτονόμισμα Bitcoin ή προπληρωμένες κάρτες. Βέβαια, είναι σημαντικό να αναφερθεί η άκρως επιθετική μορφή του CryptoLocker καθώς έθετε προθεσμία πληρωμής, με την απειλή να καταστραφεί το ιδιωτικό κλειδί μετά το πέρας της. Σε άλλες περιπτώσεις, το ποσό των λύτρων ανέβαινε ανεξέλεγκτα, ενώ δεν υπήρξε ποτέ εγγύηση πως τα στοιχεία του θύματος θα αποκρυπτογραφηθούν.

2.4.8 CryptoWall (2014) - CryptoWall Evolution (2016)

Αποτελώντας κλώνους του CryptoLocker, τα CryptoWall και CryptoWall Evolution [4], παρέμειναν υψηλά στις θέσεις χρημάτων που έχει αποκομίσει ένα Ransomware, καθώς επί δύο χρόνια κατέκλυσαν με τις επιθέσεις του.

Ο τρόπος λειτουργίας τους είναι η διάδοση ηλεκτρονικών μηνυμάτων με συνημμένα κακόβουλα αρχεία ή η διάδοση τους μέσα από ηλεκτρονικές διαφημίσεις, εκμεταλλευόμενα ευπάθειες της γλώσσας προγραμματισμού Java. Όπως και οι υπόλοιπες οικογένειες ransomware, αποσκοπούσαν στην κρυπτογράφηση συγκεκριμένων και σημαντικών αρχείων ή θέσεων αρχείων στις συσκευές του θύματος. Αντίστοιχα, και στην περίπτωση του CryptoWall η αποκρυπτογράφηση γινόταν μετά την πληρωμή των λύτρων, ενώ εάν το θύμα δεν πλήρωνε εντός προθεσμίας είτε θα καταστρεφόταν το ιδιωτικό κλειδί αποκρυπτογράφησης, είτε το ποσό των λύτρων ανέβαινε κατά ένα μεγάλο ποσοστό. Συνολικά το CryptoWall, κατάφερε να αποκομίσει από τα θύματά του $18 εκατομμύρια δολάρια [19].

2.4.9 Locky (2016)

Το Ransomware Locky [20], υπήρξε μία από τις πιο επικίνδυνες οικογένειες Ransomware καθώς μόλυνε πληθώρα χρηστών. Αποτέλεσε τεράστια απειλή για τα θύματά του, αφού κρατούσε αντίγραφο των αρχείων τους όπου αν η πληρωμή δεν γινόταν από την πλευρά του θύματος, τότε τα αρχεία αυτά δημοσιοποιούνταν στη μαύρη αγορά του Web. Αυτό συντέλεσε στην πληρωμή τρίτων για την ανάκτηση των δεδομένων του θύματος, κάτι που απέβει μοιραίο, καθώς πολλοί από αυτούς χρησιμοποιούσαν backdoors για να επιτεθούν εκ νέου στο θύμα.

Ο τρόπος που ενεργούσε το Locky ήταν κρυπτογραφώντας αρχεία και θέσεις αρχείων, σε συσκευές με λειτουργικό σύστημα Windows. Το μέσο μετάδοσης ήταν και πάλι η μαζική αποστολή ηλεκτρονικών μηνυμάτων που περιήχαν αρχεία κειμένου (π.χ. Word, Excel, κ.α.). Ο λόγος χρήσης των συγκεκριμένων αρχείων και όχι ενός συμπιεσμένου αρχείου, όπως συνηθιζόταν από άλλες οικογένειες ransomware, ήταν η χρήση κακόβουλων μακροεντολών γραμμένων στις γλώσσες προγραμματισμού JavaScript, Visual Basic, Rhino JS, κ.α., οι οποίες ήταν μη ανιχνεύσιμες από προεγκατεστημένα λογισμικά ασφάλειας όπως ο Windows Defender.

Συμπληρωματικά, οι συνήθεις επεκτάσεις των αρχείων που κρυπτογραφούσε το Locky ήταν της μορφής .aesir, .asasin, .diablo6, .locky, .loptr, .odin, .osiris, κ.α.

2.4.10 WannaCry (2017)

Όταν κάποιος αναλογίζεται ποια ήταν τα ισχυρότερα ransomware που υπήρξαν, σίγουρα θα σκεφτεί την οικογένεια WannaCry [21]. Υπήρξε ένα από τα χειρότερα malware campaigns στην ιστορία του ransomware, κυρίως ως προς τις επιπτώσεις που επέφερε στα θύματά του.

Η αρχιτεκτονική του WannaCry δε διέφερε από αυτή των μέχρι τότε εμφανιζόμενων ransomware, καθώς και αυτό με τη σειρά του κρυπτογραφεί τα δεδομένα του θύματος και του παρέχει το κλειδί αποκρυπτογράφησης εφόσον γίνει η πληρωμή των λύτρων στο wallet του επιτιθέμενου. Για να μολύνει έναν Η/Υ και κατ'επέκταση να εξαπλωθεί σε ένα δίκτυο, χρησιμοποιούσε την ευπάθεια του λειτουργικού συστήματος Windows, EternalBlue [22].

Η διαφορά του με τις υπόλοιπες οικογένειες ransomware, ήταν τα θύματα στα οποία στόχευε, αφού επρόκειτο για νοσοκομεία, μεγάλες πολυεθνικές, πανεπιστήμια και κυβερνητικούς οργανισμούς παγκοσμίως, επιτυγχάνοντας έτσι την κρυπτογράφηση δεδομένων για περισσότερα από 2 εκατομμύρια θύματα.

2.4.11 Petya (2016)

Η οικογένεια ransomware Petya [23], μόλυνε τα θύματά της και στη συνέχεια ζητούσε από αυτά το σταθερό ποσό των $300 σε Bitcoin, για την πληρωμή των λύτρων. Το κακόβουλο λογισμικό είχε μεγάλο ρυθμό εξάπλωσης εντός του οργανισμού, από τη στιγμή που ένας Η/Υ το εκτελούσε, καθώς χρησιμοποιούσε είτε την ευπάθεια του λειτουργικού συστήματος Windows, EternalBlue, είτε δύο διαχειριστικές υπηρεσίες του.

Σκοπός του κακόβουλου λογισμικού, ήταν η δοκιμή εκμετάλλευσης της πρώτης ευπάθειας, ενώ στην περίπτωση που αποτύγχανε εκκινούσε η απόπειρα εκμετάλλευσης της δεύτερης. Μια ειδοποιός διαφορά μεταξύ του Petya και ransomwares όπως το WannaCry, ήταν η τροφοδότηση του κακόβουλου λογισμικού η οποία δεν γινόταν από κάποια πηγή εκτός του δικτύου που είχε μολύνει, σε αντίθεση με άλλες οικογένειες, με αποτέλεσμα να μειωθεί η εξάπλωσή του μέσω του διαδικτύου αλλά και η οποιαδήποτε νέα επίθεση από αυτό.

2.4.12 NotPetya (2019)

Όπως και η οικογένεια Petya, έτσι και το ransomware NotPetya [23] είναι η εξελιγμένη μορφή του πρώτου. Παρόλο που και τα δύο ransomware είναι εξίσου καταστροφικά, έχουν κάποια διακριτά σημεία αναφοράς όπως η χρήση διαφορετικού κλειδιού για την κρυπτογράφηση των αρχείων, ο τρόπος επανεκκίνησης του συστήματος μετά την επίθεση ή τα σημειώματα που εκτυπώνονταν στην οθόνη του χρήστη με τις πληροφορίες για την πληρωμή των λύτρων.

2.4.13 LeakerLocker (2017)

Η περίπτωση του ransomware LeakerLocker [24], διαφοροποιείται κατά κάποιο τρόπο σε σχέση με τις υπόλοιπες οικογένειες καθώς πρόκειται για ένα campaign που στοχεύει σε κινητές συσκευές και δεν κρυπτογραφεί τα αρχεία του θύματος. Αυτό το ransomware, απειλεί το θύμα πως σε περίπτωση που δε γίνει πληρωμή των λύτρων, οι προσωπικές πληροφορίες του θα δημοσιευτούν.

Ο τρόπος με τον οποίο ισχυριζόταν πως γίνεται αυτό, ήταν κρατώντας ένα μη εξουσιοδοτημένο αντίγραφο ασφαλείας των ευαίσθητων πληροφοριών από τη συσκευή, οι οποίες δημοσιεύονταν σε μια τυχαία επαφή του θύματος εκτός και αν είχε προηγηθεί η πληρωμή των λύτρων.

2.4.14 Ryuk (2018)

Η οικογένεια Ryuk [25] υπήρξε μία από τις πρώτες που ενσωμάτωσε τη δυνατότητα ανίχνευσης θέσεων και δίσκων εντός ενός δικτύου και εν συνεχεία κρυπτογράφησής τους. Παράλληλα, μπορούσε να διαγράψει τα shadow copies από τον τελικό στόχο με αποτέλεσμα οι επιτιθέμενοι να απενεργοποιούν τη λειτουργικότητα επαναφοράς συστήματος που διέθεταν τα Windows λειτουργικά συστήματα. Οι επιπτώσεις από την εν λόγω επίθεση ήταν καταστροφικές αφού ο χρήστης μπορούσε να επαναφέρει το σύστημά του μόνο με τη χρήση εξωτερικού αντιγράφου ασφαλείας.

Ο τρόπος διάδοσης του κακόβουλου λογισμικού γινόταν με τη χρήση ανεπιθύμητων μηνυμάτων ηλεκτρονικού ταχυδρομείου (όπως και η πλειοψηφία των ransomware επιθέσεων) με τη διαφορά πως ο αποστολέας του μηνύματος ήταν μια spoofed ηλεκτρονική διεύθυνση, δηλαδή προσομοίωνε το όνομα μιας διεύθυνσης που δεν κινεί υποψίες.

Όπως και σε άλλου είδους campaigns, το κακόβουλο λογισμικό βρισκόταν εντός κάποιου αρχείου κειμένου με τη μορφή macro, και εκτελούνταν μόλις το θύμα άνοιγε το έγγραφο. Το macro αυτό, προσπαθούσε μέσω Powershell να κατεβάσει στον Η/Υ του θύματος το Trojan Emotet [26].

2.4.15 GandCrab (2018)

Το ransomware GandCrab [27] θεωρείται πως αποτελεί τη μητρική οικογένεια άλλων ransomware οικογενειών όπως το Sodinokibi. Κατέχει την πρώτη θέση σε επιθέσεις ransomware ανά τον κόσμο με ποσοστό 40%, ενώ ο τρόπος λειτουργίας του ήταν να εντοπίζει θέσεις δικτύου του μολυσμένου Η/Υ, όπως και κοινά αρχεία μεταξύ χρηστών ώστε να τα κρυπτογραφήσει.

Έχουν υπάρξει διάφορες εκδόσεις του συγκεκριμένου ransomware, με κάθε μία από αυτές να χρησιμοποιεί διαφορετικές καταλήξεις στα κρυπτογραφημένα αρχεία, όπως φαίνεται παρακάτω:

- Η έκδοση 1 χρησιμοποιεί την κατάληξη .gdcb
- Οι εκδόσεις 2 & 3 χρησιμοποιούν την κατάληξη .crab
- Η έκδοση 4 χρησιμοποιεί την κατάληξη .krab
- Η έκδοση 5 χρησιμοποιεί μια κατάληξη παραγόμενη από πέντε τυχαία γράμματα

Η διάδοση του κακόβουλου λογισμικού γινόταν μέσω ανεπιθύμητων ηλεκτρονικών μηνυμάτων, μέσω επιθέσεων τύπου Social Engineering ή μέσω ιστοσελίδων που παρείχαν στο κοινό λογισμικά - συνήθως απαιτούσαν άδεια ή κλειδί χρήσης - με ενσωματωμένο το κλειδί για την ενεργοποίησή τους.

2.4.16 PureLocker (2019)

Υπάρχουν περιπτώσεις malware campaigns, όπου η οικογένεια πίσω από το εκάστοτε campaign παραμένει άγνωστη προς τους αναλυτές. Μια τέτοια περίπτωση είναι και το ransomware PureLocker [28] το οποίο παρέμενε μη ανιχνεύσιμο προς το ευρύ κοινό έως ότου αναλυτές κυβερνοάμυνας των εταιρειών Intezer και IBM X-Force, του έδωσαν το όνομα του. Λόγω της γλώσσας προγραμματισμού PureBasic με την οποία ήταν γραμμένος ο πηγαίος κώδικάς του, το ransomware πήρε το όνομα PureLocker.

Η χρήση της PureBasic δεν συνηθίζεται για την κατασκευή ενός ransomware αλλά υπάρχουν περιπτώσεις όπως η συγκεκριμένη, όπου είναι δύσκολο να δημιουργηθούν έμπιστα εργαλεία για τον εντοπισμό του κακόβουλου λογισμικού. Παράλληλα, η PureBasic είναι εύκολο να διαδοθεί μεταξύ διακριτών λειτουργικών συστημάτων όπως τα Windows, Linux και Mac OS, με αποτέλεσμα την ευρεία μόλυνση διαφορετικών συσκευών και δικτύων.

Η επίθεση του PureLocker, στόχευε στη δέσμευση servers, θέτοντάς τους εκτός του λειτουργικού τους πλάνου για την εκάστοτε εταιρεία, ενώ προχωρούσε στην αποδέσμευσή του μετά την πληρωμή των λύτρων.

2.4.17 Zeppelin (2019)

Το ransomware Zeppelin [29] αποτελεί ένα από τα νεότερα μέλη της οικογένειας ransomware VegaLocker, η οποία αποτελείται και από άλλα ransomware όπως τα Jamper, Storm ή Buran, κ.α. [30].

Το Zeppelin, στόχευε κυρίως σε μεγάλες εταιρείες της Ευρώπης και των Η.Π.Α, ενώ κατατάσσεται στις περιπτώσεις χρήσης ενός Ransomware-as-a-Service (RaaS) [31][32], όπου οι δημιουργοί του κατασκευάζουν το ransomware και στη συνέχεια το πουλούν ή το ενοικιάζουν στους επιτιθέμενους, κρατώντας ένα μικρό ποσοστό από τα κέρδη μιας επιτυχημένης επίθεσης.

Ο τρόπος λειτουργίας του Zeppelin, είναι η εγκατάστασή του εντός ενός προσωρινού φακέλου με όνομα .zeppelin και ο διαμοιρασμός του εντός του λειτουργικού συστήματος. Μετά τη φάση του διαμοιρασμού, ξεκινά η φάση κρυπτογράφησης αρχείων όπως οι συστημικές θέσεις του λειτουργικού συστήματος Windows, οι εφαρμογές διαδικτύου όπως τα προγράμματα περιήγησης, αρχεία τα οποία εκτελούνται κατά την εκκίνηση του συστήματος καθώς και αρχεία που ανήκουν στο προφίλ χρήστη που διαθέτει το θύμα.

Πολλές φορές, μέσα στο μήνυμα με τις οδηγίες για την πληρωμή των λύτρων και την αποκρυπτογράφηση των αρχείων του θύματος, δίνεται και η δυνατότητα αποκρυπτογράφησης ενός μόνο αρχείου ως απόδειξη της μεθόδου αποκρυπτογράφησης, ώστε να ωθήσει το θύμα στην πληρωμή των λύτρων.

2.4.18 REvil (2019)

Το ransomware REvil [33], όπως και το Zeppelin, υπόκειται στο πλαίσιο των Ransomware-as-a-Service επιθέσεων. Ο τρόπος λειτουργίας του είναι μέσω συγκεκριμένων δυνατοτήτων που δίνει στον επιτιθέμενο, οι οποίες δέχονται μεταβλητές παραμετροποίησης που επηρεάζουν το ποσοστό προσαρμογής του στον εκάστοτε στόχο. Οι δυνατότητες αυτές είναι:

- Η εκμετάλλευση ευπάθειας που διαθέτουν τα λειτουργικά συστήματα Windows στην οποία το service Win32k του λειτουργικού, αποτυγχάνει στη διαχείριση αντικειμένων εντός της μνήμης του συστήματος, με αποτέλεσμα ο επιτιθέμενος να αναβαθμίζει τον εαυτό του σε διαχειριστή (Win32k Elevation of Privilege Vulnerability) όπως φαίνεται και στο CVE-2018-8453 [34]
- Ο τερματισμός διεργασιών που είναι χαρακτηρισμένες ως blacklisted, πριν τη φάση της κρυπτογράφησης ώστε να αποφευχθούν σφάλματα λόγω έλλειψης συστημικών πόρων
- Η εκκαθάριση του περιεχομένου των blacklisted διαδρομών
- Η κρυπτογράφηση αρχείων και φακέλων τόσο στην τοπική μνήμη του συστήματος, όσο και στις κοινές διαδρομές εντός του δικτύου
- Η απομάκρυνση των βασικών στοιχείων του χρήστη από το σύστημα

2.4.19 RobbinHood (2019)

Σε αντίθεση με την πλειοψηφία των ransomware campaigns, το RobbinHood [35] δεν διαδιδόταν με τη χρήση ανεπιθύμητων ηλεκτρονικών μηνυμάτων αλλά χρησιμοποιούσε άλλες μεθόδους, όπως trojans που δίνουν πρόσβαση στους επιτιθέμενους ή παραποιημένες εφαρμογές απομακρυσμένης πρόσβασης που χρησιμοποιούσε το θύμα.

Κατά την εκτέλεσή του, η εντολή `cmd.exe /c net use * /DELETE /Y` αποσυνέδεε όλες τις θέσεις δικτύου του Η/Υ, γεγονός που οδηγεί στο συμπέρασμα πως κάθε Η/Υ αποτελούσε ένα ξεχωριστό στόχο, ενώ οποιαδήποτε κοινή θέση μεταξύ δύο μηχανημάτων στο εσωτερικό δίκτυο, δεν κρυπτογραφούνταν με την ίδια μέθοδο.

Η παραπάνω συμπεριφορά εξηγείται από τη φύση του συγκεκριμένου ransomware, που χρησιμοποιούσε τη διαδρομή C:\Windows\Temp\pub.key για να αντλήσει το δημόσιο RSA κλειδί κρυπτογράφησης, ενώ αν δεν υπήρχε εκεί, η διαδικασία σταματούσε έως ότου παραχθεί ένα νέο RSA κλειδί..

Στη συνέχεια, τερμάτιζε συγκεκριμένες υπηρεσίες του λειτουργικού συστήματος Windows που συνδέονταν με τη χρήση antivirus, βάσεων δεδομένων, mail servers, κ.α. Ο λόγος τερματισμού αυτών των υπηρεσιών οφειλόταν στην προτροπή τους για μη επεξεργασία ενός αρχείου, όσο αυτό είναι ανοιχτό μέσω του προγράμματος. Έτσι, αν οι παραπάνω υπηρεσίες δεν έκλειναν τότε η φάση της κρυπτογράφησης δεν θα ολοκληρωνόταν. Παράλληλα, κατά τη φάση προετοιμασίας της κρυπτογράφησης, το RobinHood διέγραφε τα Shadow Copies του συστήματος και όλα τα event logs, ενώ απενεργοποιούσε την αυτόματη επιδιόρθωση που παρέχει το λειτουργικό σύστημα.

Στη φάση της κρυπτογράφησης του RobbinHood, χρησιμοποιείται ένα κλειδί τύπου AES για την κρυπτογράφηση του αρχείου, ενώ το δημόσιο RSA κλειδί που προαναφέρθηκε χρησιμοποιείται για την κρυπτογράφηση του AES κλειδιού και του ονόματος του αρχείου, θέτοντας έτσι ένα διπλό επίπεδο κρυπτογράφησης στο σύστημα. Τα ονόματα των αρχείων μετά το πέρας της κρυπτογράφησης είναι της μορφής _[τυχαίο αλφαριθμητικό].enc_robbinhood, π.χ. `_SCLRib2kxt7Ku8YTB9L.enc_robbinhood`.

2.4.20 Sodinokibi (2020)

Μέσα σε πολύ μικρό χρονικό διάστημα, το ransomware Sodinokibi [36], κατάφερε να γίνει το 4ο πιο διαδεδομένο ransomware στο διαδίκτυο. Ανήκει και αυτό στην κατηγορία RaaS, το οποίο

στοχεύει σε λειτουργικά συστήματα Windows, ενώ ανακαλύφθηκε για πρώτη φορά αφότου εκμεταλλεύθηκε ευπάθειες του Oracle WebLogic Server [37].

Η μέθοδοι για την εξάπλωση και εκτέλεση του Sodinokibi θυμίζουν κατά πολύ αυτές που χρησιμοποιούσε η οικογένεια ransomware GandCrab, οι οποίες παρατίθενται στην υποενότητα 2.4.15. Μετά την εκτέλεσή του, το Sodinokibi κρυπτογραφεί τα αρχεία του θύματος χρησιμοποιώντας διακριτές επεκτάσεις σε κάθε ένα από αυτά όπως οι .jpeg, .jpg, .tif, .raw, .bmp, .png, .max, .3dm, .db, .accdb, .mdb, .dxf, .dwg, .cs, .cpp, .asp, .php, .java, .gif, κ.α.

Μόλις η φάση της κρυπτογράφησης ολοκληρωθεί, η εικόνα παρασκηνίου του θύματος στην επιφάνεια εργασίας αλλάζει σε αυτή ενός σημειώματος. Οι πληροφορίες που απεικονίζονται πλέον στο θύμα, αφορούν το ποσό σε Bitcoin που πρέπει να πληρωθεί ως λύτρα ώστε να αποκρυπτογραφηθούν τα δεδομένα του, καθώς και τον τρόπο με τον οποίο θα πραγματοποιήσει την πληρωμή. Το ποσό αυτό διαφοροποιείται αναλόγως την επίθεση αλλά το εύρος του είναι μεταξύ 0.32 και 0.41 BTC [38].

2.4.21 Avaddon (2021)

Το ransomware Avaddon [39] έκανε την εμφάνισή του τον Ιούνιο του 2020 αλλά παραμένει ενεργό, αφού μέχρι και τα τέλη Ιανουαρίου του 2021 έχουν βγει στο προσκήνιο διαφορετικές εκδόσεις του. Ανήκει και αυτό στο πλαίσιο των RaaS, ενώ συμμετείχε σε πληθώρα κυβερνοπεριστατικών για τα έτη 2020 &ι 2021 και ανέδειξε ένα τρόπο κατηγοριοποίησης των θυμάτων μεταξύ αυτών που πληρώνουν τα λύτρα και αυτών που δεν πληρώνουν και στιγματίζονται με τον όρο “name and shame” [32]. Μέχρι τις αρχές Φεβρουαρίου του 2021, το Avaddon υπέκλεψε και δημοσίευσε πάνω από 574GB δεδομένων μέσα από 23 εταιρείες.

Ο τρόπος διάδοσής του είναι χρησιμοποιώντας τον τύπο επίθεσης DDoS [56] για να αποστείλει μαζικά ανεπιθύμητα ηλεκτρονικά μηνύματα στο δίκτυο των θυμάτων. Για την αποκρυπτογράφηση των δεδομένων τους, τα θύματα είτε πρέπει να πληρώσουν το ζητούμενο ποσό σε Bitcoin, είτε να χρησιμοποιήσουν κάποιο από τα decryptor εργαλεία που δημοσιεύτηκαν άμεσα στο ευρύ κοινό, αλλά πλέον μπορεί να έχουν καταργηθεί, σύμφωνα με την τρέχουσα έκδοση του ransomware.

ΚΕΦΑΛΑΙΟ 3ο: Πρώτες ενέργειες μετά την επίθεση

Με το πέρας του χρόνου, ολοένα και περισσότερα Ransomware Campaigns δρουν εναντίον εταιρειών, κυβερνητικών ή μη οργανισμών, κ.λπ. Πέρα από αλλαγές σε πηγαία τμήματα της επίθεσης, όπως ο τρόπος εκτέλεσης του κακόβουλου λογισμικού ή ο αλγόριθμος κρυπτογράφησης, η αρχιτεκτονική αυτών των επιθέσεων δεν διαφοροποιείται ανά τα έτη. Το χαρακτηριστικό όμως, που με ακρίβεια κατηγοριοποιεί αυτά τα campaigns, είναι τα έσοδα που λαμβάνει κάθε επιτιθέμενος.

Σύμφωνα με αναφορά του CyberEdge Group, που δημοσιεύτηκε τον Μάρτιο του 2020, το 62% των οργανισμών μέσα από 17 χώρες ανά τον κόσμο, δέχτηκαν επιθέσεις μέσω Ransomware Campaign, ενώ το 58% εξ αυτών, πλήρωσαν τα λύτρα στους επιτιθέμενους. Αυτά τα ποσοστά τείνουν να μεγαλώνουν ραγδαία, αφού συγκριτικά με παρόμοια αναφορά του 2018, από το 55% των οργανισμών που δέχτηκε επίθεση τύπου ransomware, μόνο το 39% προχώρησε σε πληρωμή των λύτρων [40].

Εικ. 3.1: Δημογραφική αναφορά της της CyberEdge Group για το 2020
(Πηγή: **https://cyber-edge.com/cdr/#infographic**)

3.1. Πληρωμή επιτιθέμενου

Η πληρωμή των λύτρων, θα μπορούσε κάλλιστα να αποτελεί σενάριο αστυνομικής ταινίας. Με τη βοήθεια των κατάλληλων εργαλείων και των αρμόδιων αρχών φαντάζεται κανείς πως θα μπορούσε να αποφευχθεί η πληρωμή. Δυστυχώς όμως, ο τρόπος κρυπτογράφησης των δεδομένων είναι καθοριστικός παράγοντας για την πληρωμή τους από έναν οργανισμό, αφού το ρίσκο απώλειας των δεδομένων τους μπορεί να είναι καταστρεπτικό τόσο για τον οργανισμό όσο και τα τρίτους φορείς που ενεργούν υπέρ ή μέσω αυτού.

Για τη διασφάλιση της ανωνυμότητας του επιτιθέμενου η διαδικασία των πληρωμών γίνεται με ηλεκτρονικό τρόπο και στην πλειοψηφία των περιπτώσεων με τη χρήση κρυπτονομίσματος. Πιο συγκεκριμένα, ο επιτιθέμενος έχει τη δυνατότητα δημιουργώντας ένα ψηφιακό πορτοφόλι στην αλυσίδα του Blockchain, να κρατήσει ανώνυμη την ταυτότητά του ενώ παράλληλα να παρέχει δημοσίως στην εν λόγω αλυσίδα, όλη την πληροφορία των συναλλαγών.

Από την μεριά του το εκάστοτε θύμα, θα λάβει είτε με κάποια ειδοποίηση, είτε με ένα μήνυμα στην επιφάνεια εργασίας της συσκευής του (διαφέρει ανάλογα με την οικογένεια του Ransomware) τις παρακάτω πληροφορίες:

- μια ή πολλές διευθύσεις της μορφής **`1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2`** που αφορά τη διεύθυνση αποστολής των χρημάτων
- το ποσό που θα πρέπει να κατατεθεί στη μορφή του κρυπτονομίσματος, π.χ. 1.5 BTC (Bitcoin)
- οδηγίες για τη δημιουργία λογαριασμού στο Blockchain ώστε να προβεί στην κατάθεση των κρυπτονομισμάτων

Φυσικά, για τη δημιουργία ενός λογαριασμού, το θύμα θα πρέπει χρησιμοποιώντας έναν browser, να περιηγηθεί στον ιστότοπο https://www.blockchain.com/. Σε αυτό το σημείο, χρησιμοποιώντας τον περιηγητή Tor [57] και συνήθως συνδυαστικά με κάποια επέκταση του όπως το Onion [58] (εκτελείται στον παραπάνω περιηγητή), η χρήση του διαδικτύου από το θύμα επιτρέπεται μόνο προς τον ιστότοπο του Blockchain και προς σημεία επικοινωνίας με τον επιτιθέμενο. Η χρήση του Tor γίνεται ώστε να μην αποκαλυφθεί το σημείο δράσης του επιτιθέμενου, αφού ο εν λόγω περιηγητής κρυπτογραφεί κάθε επικοινωνία προς το διαδίκτυο, ενώ παράλληλα δρομολογεί όλες τις εξερχόμενες επικοινωνίες σε τυχαίους κόμβους προτού καταλήξουν στον προορισμό τους, ώστε να αποφευχθεί κάθε είδους παρέμβαση τρίτων μεταξύ θύματος και επιτιθέμενου.

3.2. Τρόπος λειτουργίας του Blockchain

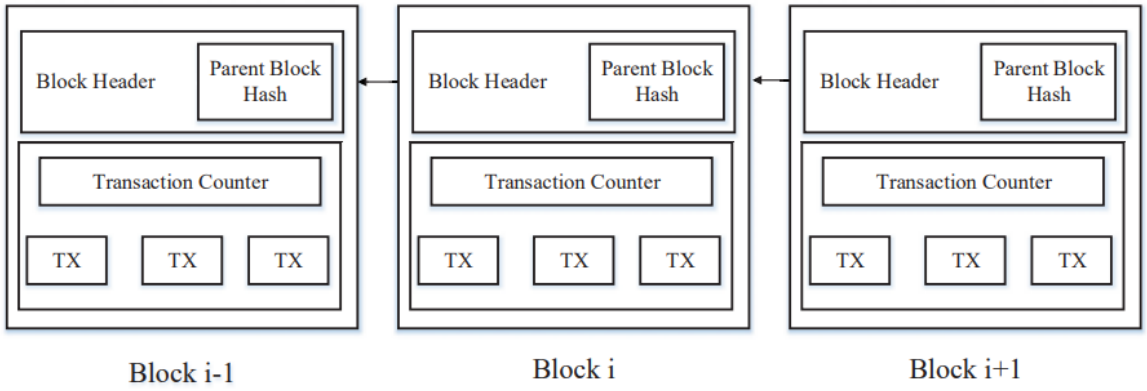
3.2.1. Τι είναι το Blockchain

Το Blockchain μπορεί να χαρακτηριστεί ως ένα οικονομικό βιβλίο καταγραφής κινήσεων μεταξύ των χρηστών του. Οι συναλλαγές που γίνονται στο Blockchain αποτελούν τους συνδετικούς κρίκους(blocks) μιας αλυσίδας όπου κάθε κρίκος εξαρτάται από τον προηγούμενο και από τους κανόνες που έχουν τεθεί και συμφωνηθεί μεταξύ των χρηστών του. Αυτά τα blocks περιέχουν μία ή πολλές συναλλαγές, ανάλογα με το επιτρεπόμενο μέγεθος που μπορεί να έχει το εκάστοτε block [41].

Η καινοτομία του Blockchain ήταν η δημιουργία ενός οικονομικού δικτύου το οποίο θα έχει αποκεντροποιημένη σύσταση. Συγκεκριμένα, ας θεωρηθεί ως κεντρικοποιημένο οικονομικό σύστημα το παράδειγμα ενός υποκαταστήματος τράπεζας. Το κεφάλαιο του υποκαταστήματος, οι εσωτερικές και εξωτερικές συναλλαγές του αλλά και τα χρήματα των πελατών του φυλάσσονται εντός της τράπεζας. Στην περίπτωση που πρέπει να πραγματοποιηθεί μια συναλλαγή μεταξύ δύο πελατών, θα πρέπει τότε το εξουσιοδοτημένο προσωπικό του υποκαταστήματος να ελέγξει και να εγκρίνει τη συναλλαγή, καθώς και να την εκτελέσει.

Σε αντίθετη περίπτωση με το παραπάνω παράδειγμα, ένα αποκεντροποιημένο οικονομικό σύστημα είναι η περίπτωση του Blockchain. Σε αυτό το σύστημα τα χρήματα του κάθε χρήστη βρίσκονται στο προσωπικό του wallet ενώ για να πραγματοποιηθεί μια συναλλαγή θα πρέπει να ελεγχθεί η εγκυρότητα των χρηστών από όλους τους χρήστες του Blockchain και εφόσον η συναλλαγή αυτή πληροί τα κριτήρια και τους κανονισμούς του συστήματος, θα πραγματοποιηθεί.

Συμπληρωματικά, όλες οι συναλλαγές που πραγματοποιούνται στο Blockchain, είναι εμφανείς από όλους τους χρήστες του, ενώ κάθε ένας από αυτούς έχει στη διάθεσή του ένα ακριβές αντίγραφο αυτής της αλυσίδας συναλλαγών.



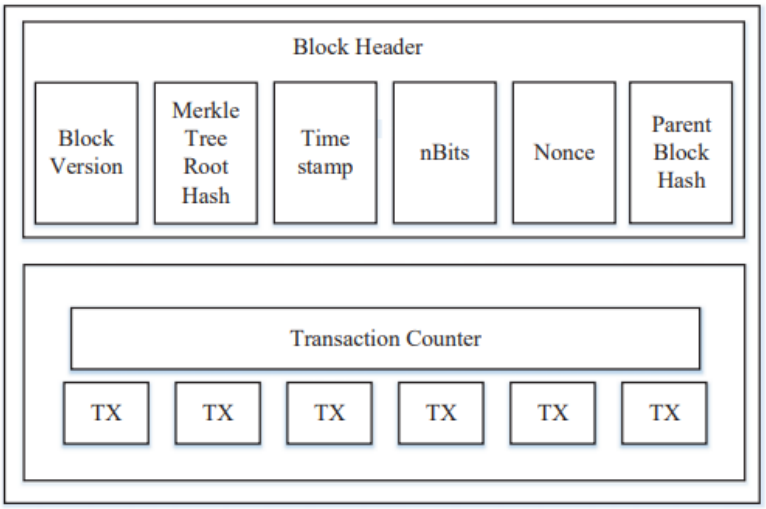
Εικ. 3.2: Αρχιτεκτονική του Blockchain
(Πηγή: https://ieeexplore.ieee.org/abstract/document/8029379)

Όπως αναφέρεται και στο παραπάνω παράδειγμα, οι πληροφορίες των χρηστών αλλά και των συναλλαγών του Blockchain είναι δημόσιες προς τους υπόλοιπους χρήστες. Για να διατηρηθεί λοιπόν οι ανωνυμότητα τους αλλά και για την ασφάλεια τόσο των χρηστών όσο και του ίδιου του αρχείου συναλλαγών, χρησιμοποιείται ασύμμετρη κρυπτογράφηση και κατανεμημένοι αλγόριθμοι συναίνεσης.

Με τη χρήση της ασύμμετρης κρυπτογράφησης στις πληροφορίες των συναλλαγών μπορεί πέρα από την ανωνυμοποίηση των δεδομένων να μειωθεί και το μέγεθος των αρχείων που δημιουργούνται και αποθηκεύονται στην αλυσίδα του Blockchain, κατά την εκτέλεση μιας συναλλαγής. Μετατρέποντας τα δεδομένα μιας συναλλαγής σε ανωνυμοποιημένα δεδομένα με τη χρήση συναρτήσεων κατακερματισμού, το μέγεθος της αλυσίδας μειώνεται εκθετικά.

3.2.2. Η δομή ενός block

Τα blocks ή συνδετικοί κρίκοι της αλυσίδας του Blockchain, αποτελούνται από την κεφαλίδα και το κύριο μέρος.



Εικ. 3.3: Δομή ενός block
(Πηγή: https://ieeexplore.ieee.org/abstract/document/8029379)

Η κεφαλίδα του block αποτελείται από τα εξής τμήματα [42]:

- Την έκδοση του block, η οποία περιέχει τους κανόνες του Blockchain και με τους οποίους πρέπει να είναι συμβατό το ίδιο το block, ώστε να θεωρηθεί έγκυρο και να καταγραφεί στο Blockchain
- Την κατακερματισμένη τιμή της αρχικής τιμής του block, η οποία θα πρέπει να είναι η ίδια με όλα τα προηγούμενα blocks της αλυσίδας και παράγεται με τη χρήση της δομής δεδομένων Merkle tree. Το παραγόμενο hash, χρησιμοποιείται από το Blockchain ώστε να δώσει περιληπτική δομή στο εκάστοτε block για όλα τα transactions εντός αυτού, όπως και ένα ψηφιακό αποτύπωμα που καθορίζει αν μια συναλλαγή ανήκει σε αυτό το block [43]
- Την τρέχουσα χρονική τιμή υπολογισμένη σε δευτερόλεπτα από την 1η Ιανουαρίου του 1970 (Unix epoch)
- Τον αριθμό του ορίου σε bits για την τιμή κατακερματισμού του συγκεκριμένου block
- Ένα πεδίο τεσσάρων byte (nonce) το οποίο αυξάνεται για κάθε έναν υπολογισμό τιμών κατακερματισμού που προκύπτει στο block
- Την τιμή 256-bit κατακερματισμού του γονικού block που δημιουργήθηκε πριν από το τρέχων block με τη χρήση του SHA256 αλγορίθμου

Το κύριο μέρος ενός block αποτελείται από έναν μετρητή συναλλαγών και από τις ίδιες τις συναλλαγές που μπορεί να αποθηκεύσει αυτό το block. Ο μέγιστος αριθμός συναλλαγών που μπορούν να αποθηκευτούν σε ένα block εξαρτάται από το μέγεθός του ίδιου του block αλλά και από το μέγεθος της κάθε συναλλαγής [44].

Πέρα από τις ανωνυμοποιημένες πληροφορίες που υπάρχουν στην κεφαλίδα και το κύριο μέρος του εκάστοτε συνδετικού κρίκου, το Blockchain χρησιμοποιεί ασύμμετρη κρυπτογράφηση για να εγκρίνει και να αυθεντικοποιήσει κάθε συναλλαγή.

Όπως και σε προηγούμενη αναφορά έτσι και εδώ, το κάθε block υπογράφεται ψηφιακά με το ιδιωτικό κλειδί του χρήστη (το οποίο δεν πρέπει να γνωστοποιείται σε κανέναν) και κρυπτογραφείται.

Για την αποκρυπτογράφηση του block από τους υπόλοιπους χρήστες, χρησιμοποιείται το δημόσιο κλειδί του χρήστη το οποίο είναι γνωστό σε όλο το δίκτυο του Blockchain. Μέσω αυτής της διαδικασίας κάθε χρήστης μπορεί να επαληθεύσει την εγκυρότητα του περιεχομένου ενός block και να διακρίνει αν τα δεδομένα του έχουν παραποιηθεί ή όχι. Ένας συνήθης αλγόριθμος που χρησιμοποιείται από τα blockchains για την ψηφιακή υπογραφή ενός block είναι ο αλγόριθμος ψηφιακής υπογραφής ελλειπτικής καμπύλης (Elliptic Curve Digital Signature Algorithm - ECDSA) [45].

3.2.3. Παράγοντες “κλειδιά” στην αλυσίδα του Blockchain

Χάρη σε κάποιους βασικούς παράγοντες “κλειδιά” του Blockchain, οι χρήστες και η αλυσίδα του μπορούν να διατηρούν τα δεδομένα των συναλλαγών τους ασφαλή ενώ παράλληλα να διατηρείται σε χαμηλά επίπεδα το κόστος δημιουργίας νέων συναλλαγών που προστίθενται σε αυτό, όπως και σε υψηλά επίπεδα η αποδοτικότητα του ως προς την αποθήκευση και τη μεταβίβαση της πληροφορίας. Κάποιοι από τους βασικούς παράγοντες “κλειδιά” του Blockchain είναι:

Αποκεντροποιημένη δομή: Δεν απαιτείται κάποιο τρίτο μέρος (όπως στην περίπτωση της τράπεζας) ώστε να εγκρίνει και να εκτελέσει τις συναλλαγές. Οι κατανεμημένοι αλγόριθμοι του Blockchain εφαρμόζουν το πρόβλημα της συναίνεσης, δηλαδή **α)** κάθε συναλλαγή έχει μια αρχική τιμή η οποία μετά από επεξεργασία με τον αλγόριθμο κατακερματισμού μετατρέπεται σε ένα τυχαίο αλφαριθμητικό, **β)** αυτό το αλφαριθμητικό θα πρέπει να είναι ίδιο για όλες τις συναλλαγές της αλυσίδας του Blockchain παρ’όλο που οι αρχικές τους τιμές είναι διαφορετικές και **γ)** θα πρέπει η αρχική τιμή της συναλλαγής να πληροί τους κανόνες που έχουν οριστεί από το ίδιο το Blockchain. Με αυτόν τον τρόπο διατηρείται η συνοχή των δεδομένων μεταξύ των συναλλαγών του.

Διατήρηση της δομής: Για την διατήρηση δομής της αλυσίδας, θα πρέπει όλες οι συναλλαγές του Blockchain να μπορούν να εγκριθούν ή όχι, άμεσα. Είναι σχεδόν αδύνατο να διαγράψει κάποιος ή να μεταβεί σε κάποια προηγούμενη έκδοση του Blockchain από τη στιγμή που μια συναλλαγή καταγραφεί σε αυτό. Παράλληλα, εάν κάποιο από τα blocks της αλυσίδας περιέχει μη έγκυρες συναλλαγές, τότε είναι εύκολο να ανακαλυφθεί και να απορριφθεί.

Ανωνυμοποίηση των δεδομένων: Κάθε χρήστης εντός του Blockchain μπορεί να αλληλεπιδράσει με τους υπόλοιπους χρήστες, χρησιμοποιώντας μια διεύθυνση αντί για τα προσωπικά του δεδομένα. Όπως αναφέρθηκε και στην υποενότητα 3.1. η μορφή της διεύθυνσης είναι ένα hash ώστε να διατηρείται η ανωνυμότητα του χρήστη ώς προς το Blockchain. Βέβαια, υπάρχουν περιπτώσεις όπου στοιχεία για τον χρήστη πίσω από την πιθανή διεύθυνση **`1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2`** μπορούν να αποκαλυφθούν αφού οποιαδήποτε πληροφορία εντός του Blockchain είναι δημόσια από τους άλλους χρήστες. Συνεπώς, στοιχεία όπως η διεύθυνση IP του που μπορεί να συνδέεται με κάποια συναλλαγή, μπορούν να οδηγήσουν στην εύρεση του χρήστη, χρησιμοποιώντας πάντα τα κατάλληλα εργαλεία.

Έλεγχος των συναλλαγών: Το Blockchain διατηρεί δεδομένα στη δομή του όπως το υπόλοιπο του χρήστη. Από τη στιγμή που ένας χρήστης προβεί στην εκτέλεση μιας συναλλαγής, τότε το Blockchain μπορεί να ελέγξει εύκολα και άμεσα την κατάστασή της, να την χαρακτηρίσει ως έγκυρη ή άκυρη και να την καταγράψει. Επί παραδείγματι, αν έχει αφαιρεθεί το ποσό της συναλλαγής από το σύνολο των κρυπτονομισμάτων στο ηλεκτρονικό πορτοφόλι του χρήστη και το υπόλοιπό του είναι θετικό, ενώ ταυτόχρονα συνάδει με το συνολικό υπόλοιπο του Blockchain, τότε η συναλλαγή καταγράφεται και χαρακτηρίζεται ως έγκυρη. Σε αντίθετη περίπτωση, η συναλλαγή καταγράφεται αλλά δεν εκτελείται και χαρακτηρίζεται ως άκυρη.

3.3. Ανάκτηση Δεδομένων

Είναι σαφές το γεγονός πως αν ένας οργανισμός αξιολογήσει την απώλεια των δεδομένων του ως κρίσιμη για τη βιωσιμότητά του, θα προβεί σε πληρωμή των λύτρων για να τα ανακτήσει. Φυσικά, υπάρχουν και οι περιπτώσεις όπου τα θύματα ενήργησαν διαφορετικά και προσπάθησαν να ανακτήσουν τα δεδομένα τους με τη χρήση εργαλείων.

Στην περίπτωση χρήσης εργαλείων, υπάρχουν λύσεις που αφορούν κάθε μία οικογένεια Ransomware και σε κάποιες περιπτώσεις μπορεί να φανούν κρίσιμα για την ανάκτηση των δεδομένων του θύματος. Συνήθως, αυτές οι λύσεις προκύπτουν εφόσον έχει επέλθει το σημείο μηδέν της επίθεσης, ενώ τις περισσότερες φορές μπορεί να περάσει κάποιο μεγάλο χρονικό διάστημα προτού βρεθεί λύση. Παράδειγμα εύρεσης τέτοιων εργαλείων αποτελεί και η διαδικτυακή εφαρμογή “No more ransom!” στην οποία μπορεί κανείς να αποκτήσει λογισμικό για την αφαίρεση συγκεκριμένων Ransomware Families [46].

Εικ. 3.4: Χρήση εργαλείου για την ανάκτηση των δεδομένων και την απομάκρυνση του Ransomware WannaCry
(Πηγή: **https://www.nomoreransom.org/en/decryption-tools.html**)

Βέβαια, υπάρχει πληθώρα περιπτώσεων όπου κάποια Ransomware Campaigns ακόμα και μετά την πληρωμή των λύτρων δεν αποκρυπτογράφησαν τα δεδομένα του θύματος ή διατήρησαν κάποιο backdoor στη συσκευή του για μελλοντική επίθεση.

Αξιολογώντας λοιπόν, τον τρόπο λειτουργίας του Blockchain και κατανοώντας το μέγεθος του φάσματος στο οποίο συνυπάρχουν ανώνυμοι χρήστες και ανώνυμες συναλλαγές, η επαναφορά της πρόσβασης στα δεδομένα ενός χρήστη από τον επιτιθέμενο μπορεί να μην γίνει. Μια πιθανή εξήγηση πίσω από αυτή τη συμπεριφορά, ενδέχεται να είναι λόγω περιορισμένης έως μηδενικής ιχνηλασιμότητας του επιτιθέμενου στο Blockchain ή λόγω ηθικών

ιδεών του επιτιθέμενου οι οποίοι δεν θεωρείται σκόπιμο να αξιολογηθούν και να αναλυθούν στην παρούσα μεταπτυχιακή διατριβή.

Ολοκληρώνοντας, θα μπορούσε να συμπεράνει κάποιος, ότι η ανάγκη για την εύρεση του επιτιθέμενου πριν από τη χρήση κάποιου εργαλείου ή από την πληρωμή των λύτρων είναι καθοριστικός παράγοντας για τη μείωση των επιθέσεων αλλά και για την ανάκτηση των δεδομένων του θύματος χωρίς καταστροφικές, για τον εκάστοτε οργανισμό, συνέπειες.

ΚΕΦΑΛΑΙΟ 4ο: Το ηλεκτρονικό “πορτοφόλι” του επιτιθέμενου, ο διαμοιρασμός των κρυπτονομισμάτων & η νομιμοποίηση των εσόδων

Κατά την πληρωμή του ζητούμενου ποσού, από τον επιτιθέμενο, για την ανάκτηση των δεδομένων του θύματος, είναι σημαντικό να αναφερθεί πως η διεύθυνση πληρωμής δεν είναι η τελική διεύθυνση από την οποία ο επιτιθέμενος θα εισπράξει τα λύτρα. Αυτό συμβαίνει γιατί όπως αναλύθηκε και σε προηγούμενο κεφάλαιο αυτής της μεταπτυχιακής διατριβής, υπάρχουν τρόποι ώστε να αποκαλυφθούν κάποια στοιχεία του ανθρώπου πίσω από τη διεύθυνση του Blockchain και εν συνεχεία με τις κατάλληλες διαδικασίες, ο ίδιος ο επιτιθέμενος.

Συνεπώς, κάθε επιτιθέμενος μπορεί να διακινήσει το ποσό των κρυπτονομισμάτων που μόλις έλαβε σε πληθώρα από άλλες διευθύνσεις εντός του Blockchain, μεταφέροντας είτε το ακριβές ποσό είτε διαμοιράζοντάς το σε μικρότερα ποσά. Το σύνολο αυτών των συναλλαγών θα καταλήξει κάποια στιγμή σε ένα συγκεντρωτικό ηλεκτρονικό πορτοφόλι (accumulative wallet) από το οποίο ο επιτιθέμενος θα εξαργυρώσει το ποσό της επίθεσης.

4.1. Διανομή και διαμοιρασμός κρυπτονομίσματος

Κάθε Blockchain μπορεί να αποτελείται από συναλλαγές του ίδιου κρυπτονομίσματος στο ίδιο blockchain ή από συναλλαγές μεταξύ διαφορετικών blockchains και διαφορετικών κρυπτονομισμάτων. Αυτή η διαδικασία περιγράφει τη διανομή και το διαμοιρασμό των κρυπτονομισμάτων εντός του Blockchain.

Το πλήθος των διαφορετικών κρυπτονομισμάτων που υπάρχουν τη χρονική στιγμή δημιουργίας αυτής της διατριβής, ανέρχεται σε 6.044 [59] διαφορετικά κρυπτονομίσματα ενώ παράλληλα αν όλα τα διαθέσιμα κρυπτονομίσματα μετατραπούν σε φυσικό συνάλλαγμα τότε το συνολικό ποσό που προκύπτει αγγίζει τα $1.286.883.393.332,00 (USD) (κατά την 21η Ιουλίου 2021) [60].

Είναι λοιπόν φυσιολογικό, η εύρεση ενός επιτιθέμενου μέσα σε αυτό το δαίδαλο από κρυπτογραφημένες συναλλαγές, να αποτελεί μια εξαιρετικά δύσκολη, χρονοβόρα και τις περισσότερες φορές ανώφελη διαδικασία. Φυσικά, μόλις ελάχιστα από αυτά τα διαθέσιμα κρυπτονομίσματα, χρησιμοποιούνται σε συναλλαγές που προκύπτουν μεταξύ των Ransomware Campaigns και των θυμάτων, αφού για κάθε επιτιθέμενο ο βασικός παράγοντας για μια επιτυχημένη πληρωμή είναι ένα ευρέως διαδεδομένο δίκτυο κρυπτονομισμάτων. Με αυτόν τον τρόπο, ο επιτιθέμενος διασφαλίζει την ανάγκη του για αύξηση των λύτρων, την ευκολία πληρωμής τους από το θύμα μέσω του δικτύου του εκάστοτε blockchain, αλλά και την εξαργύρωση του accumulative wallet μέσω άλλων ηλεκτρονικών μέσων ή με φυσικούς τρόπους.

Στον παρακάτω πίνακα εμφανίζονται κάποια από τα πιο διαδεδομένα κρυπτονομίσματα ανά τον κόσμο τα οποία χρησιμοποιούνται κατά κόρον για τις συναλλαγές των χρηστών αλλά και για τις πληρωμές επιτιθέμενων, ως αποτέλεσμα δράσης ενός Malware Campaign:

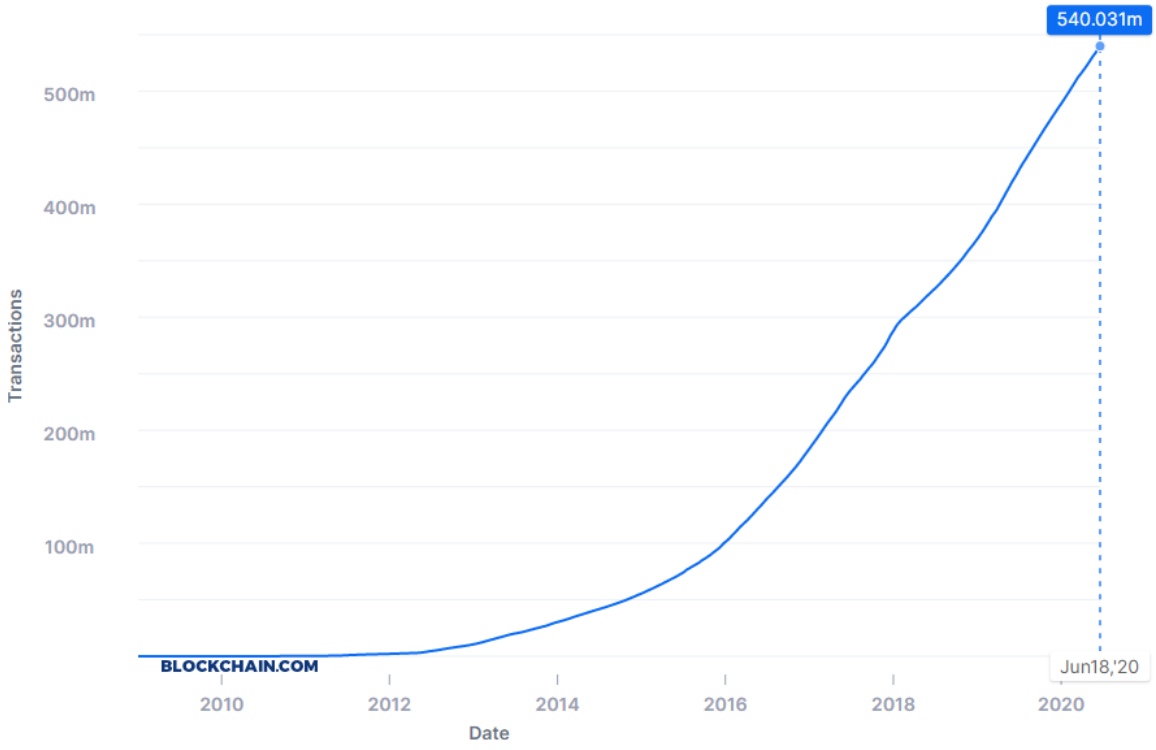
#	Κρυπτονόμισμα	Τιμή μονάδας (2020-06-21)	Τιμή μονάδας (2021-03-21)	Αξία συνολικής αγοράς (2020-06-21)	Αξία συνολικής αγοράς (2021-03-21)
1.	Bitcoin	$9.357,54 / BTC	$57.395,61 / BTC	$172.277.870.173	$1.070.568.715.165
2.	Ethereum	$231,10 / ETH	$1.791,80 / ETH	$25.753.898.818	$206.260.103.107
3.	Tether	$1,00 / USDT	$0,9999 / USDT	$9.220.600.325	$39.513.961.399
4.	XRP	$0,187625 / XRP	$0,5055 / XRP	$8.303.861.764	$22.854.563.577
5.	Bitcoin Cash	$232,54 / BCH	$526,70 / BCH	$4.288.305.235	$9.841.791.603
6.	Bitcoin SV	$173,69 / BSV	$204,50 / BSV	$3.202.740.895	$3.820.779.753
7.	Litecoin	$43,31 / LTC	$197,28 / LTC	$2.809.393.809	$13.156.644.959
8.	Binance Coin	$16,06 / BNB	$263,51 / BNB	$2.497.990.307	$40.701.475.539
9.	EOS	$2,53 / EOS	$4,21 / EOS	$2.359.095.869	$3.999.911.036
10.	Crypto.com Coin	$0,119722 / CRO	$0,2214 / CRO	$2.087.481.682	$5.592.865.096
11.	Cardano	$0,079564 / ADA	$1,21 / ADA	$2.062.854.609	$38.562.280.377
12.	Tezos	$2,61 / XTZ	$4,19 / XTZ	$1.916.055.931	$3.199.581.373
13.	Chainlink	$4,16 / LINK	$29,69 / LINK	$1.456.938.945	$12.323.234.646
14.	Stellar	$0,069770 / XLM	$0,4017 / XLM	$1.419.265.496	$9.098.490.880
15.	UNUS SED LEO	$2,13 / LEO	$1,18 / LEO	$1.174.459.773	$2.132.741.985
16.	Monero	$64,71 / XMR	$235,58 / XMR	$1.139.246.188	$4.199.617.349
17.	TRON	$0,015947 / TRX	$0,06156 / TRX	$1.063.369.355	$4.371.477.404
18.	Compound	$357,02 / COMP	$409,63 / COMP	$914.427.632	$1.915.222.496
19.	Huobi Token	$4,10 / HT	$13,94 / HT	$901.758.321	$2.548.775.439
20.	USD Coin	$1,00 / USDC	$0,9995 / USDC	$734.065.890	$9.886.119.913

Πίνακας 4.1: Αξία μονάδας, αξία συνόλου και συνολικής αγοράς των 20 πρώτων στη συνολική κατάταξη κρυπτονομισμάτων κατά την 21η Ιουνίου 2020, και η διαφοροποίησή τους εννέα μήνες μετά κατά την 21η Μαρτίου 2021 (η σειρά κατάταξης ενδέχεται να έχει αλλάξει)
(Πηγή: **https://coinmarketcap.com/**)

4.2. Δημόσια πληροφορία συναλλαγών στο Blockchain

Κάθε πληροφορία στην αλυσίδα του Blockchain είναι δημόσια προς τους χρήστες του. Με τη σειρά του κάθε χρήστης, έχει τη δυνατότητα να παρακολουθήσει όλες τις συναλλαγές που έχουν καταγραφεί στο Blockchain από την ημέρα 0 (ημέρα έναρξης της αλυσίδας) έως και την τρέχουσα χρονική στιγμή.

Αυτό και μόνο, θα μπορούσε να είναι η λύση στο ερώτημα “Μπορούμε να εντοπίσουμε μια οικογένεια Ransomware μέσα στην αλυσίδα του Blockchain;”. Σε αυτό το σημείο όμως, η πολυπλοκότητα παραγωγής των blocks αλλά και ο τεράστιος όγκος του, καθιστούν σχεδόν αδύνατη την καταγραφή της πορείας ενός χρηματικού ποσού από το πορτοφόλι Α στο πορτοφόλι Β.



Εικ. 4.1: Προσέγγιση συνόλου συναλλαγών στο Blockchain έως τις 18 Ιουνίου 2020
(Πηγή: **https://www.blockchain.com/**)

Με το συνολικό αριθμό συναλλαγών στο Blockchain.com να αγγίζει περίπου τα 540 εκατομμύρια και τον συνολικό αριθμό μοναδικών wallets να είναι περίπου ίσο με 51 εκατομμύρια θα έπρεπε να αναλυθούν 11 εκατομμύρια συναλλαγές ώς προς την σχέση τους μεταξύ 2 χρηστών. Πιο συγκεκριμένα, έστω ότι ο χρήστης **X** με διεύθυνση **`16ggYu4eHZ5mqTcZ2RCQEbPZWBQ2aN3oDs`** του Blockchain.com θέλει να αποστείλει 0.2BTC στον χρήστη **Y** με διεύθυνση **`16ggYu4eHZ5mqTcZ2RCQEbPZWBQ2aN3oDs`**.

Εάν θεωρήσουμε ως χρήστη **X** το θύμα ενός Ransomware Campaign και χρήστη Y την οικογένεια του Ransomware τότε τα πιθανά σενάρια σύμφωνα με τα οποία θα μπορούσε να εκτελεστεί αυτή η συναλλαγή είναι τα εξής:

Σενάριο 1ο: Ο χρήστης **X** μπορεί να αποστείλει μέσω του Transaction **e70af92fs17c7a1425c37e48c5931ae19cc333515388b168791967f070346bch** το ποσό των 0.5 BTC στον χρήστη **Y**. Σε αυτή την περίπτωση δε μένει παρά να αναλυθεί μόνο μία συναλλαγή και από τα στοιχεία που μας οδηγούν στον επιτιθέμενο, να εντοπιστεί η θέση του με τα κατάλληλα εργαλεία.

Σενάριο 2ο: Ο χρήστης **X** μπορεί να αποστείλει μέσω του Transaction **e70af92fs17c7a1425c37e48c5931ae19cc333515388b168791967f070346bch** το ποσό των 0.5 BTC στον χρήστη **A**. Με τη σειρά του, ο χρήστης **A** θα αποστείλει το ίδιο ποσό στον χρήστη **B** και αυτός με τη σειρά του στον χρήστη **Y.** Σε αυτή την περίπτωση η ανάλυση της αρχικής συναλλαγής θα μας οδηγήσει σε δύο ενδιάμεσες συναλλαγές προτού φτάσει το τελικό ποσό στον επιτιθέμενο. Όπως και στο 1ο Σενάριο, θα μπορούσε να θεωρηθεί λογική η ανάλυση 2 περαιτέρω συναλλαγών ώστε να πραγματοποιηθεί ο εντοπισμός του επιτιθέμενου. Στην πραγματικότητα όμως ένα τέτοιο σενάριο δεν θα αντικατοπτρίζεται από 2 ενδιάμεσες συναλλαγές, αλλά από δεκάδες, εκατοντάδες ή χιλιάδες συναλλαγών. Ακόμα και τότε, ο χρόνος εκτέλεσης της ανάλυσης θα αυξηθεί αλλά η διεύθυνση του τελικού wallet θα εξακριβωθεί.

Σενάριο 3ο: Με την πολυπλοκότητα καταγραφής αυτής της συνέχειας συναλλαγών να ανεβαίνει κατακόρυφα, μπορεί να προστεθεί άλλος ένας κρίσιμος παράγοντας που καθιστά σχεδόν αδύνατη την εύρεση του επιτιθέμενου. Ο χρήστης **X** θα αποστείλει στον χρήστη **A** 0.12 BTC και στον χρήστη **B** 0.48 BTC. Εκείνοι με τη σειρά τους θα αποστείλουν σε περισσότερους χρήστες το ποσό που έλαβαν διαμοιρασμένο. Έστω ότι το πλήθος των wallets που έχουν συγκεντρωτικά το αρχικό ποσό των 0.5 BTC, είναι 100. Σε αυτήν την περίπτωση και τα 100 wallets θα αποστείλουν σε διακριτές χρονικές στιγμές τα ποσά τους στον επιτιθέμενο. Θεωρείται πλέον βέβαιο πως η πολυπλοκότητα εύρεσής του, μέσω της διαδοχικής ανάλυσης των συναλλαγών του Blockchain, έχει μεγαλώσει εκθετικά.

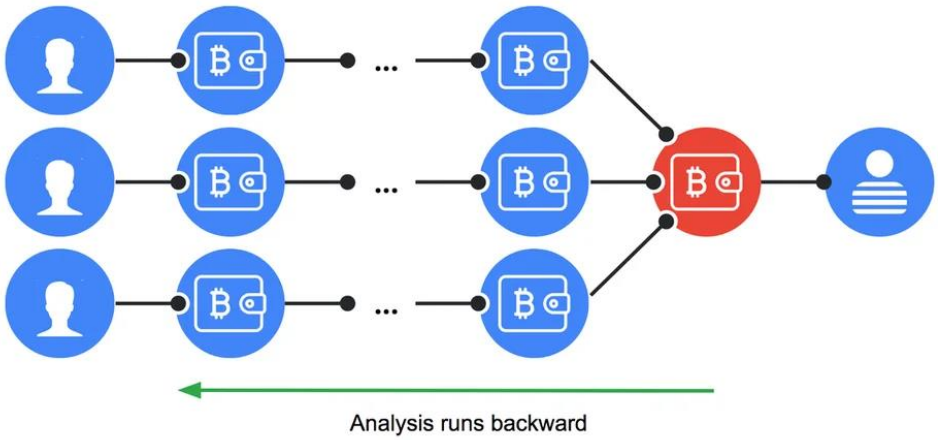
Σενάριο 4ο: Θα μπορούσε κάποιος να πει πως με τη χρήση του κατάλληλου λογισμικού ανάλυσης δεδομένων, η εύρεση του επιτιθέμενου στο 3ο σενάριο μπορεί να επιτευχθεί. Εάν όμως προσθέσουμε μία ακόμη μεταβλητή στον αλγόριθμο εύρεσης, η οποία αφορά τις συναλλαγές μεταξύ διαφορετικών blockchains, τότε το ποσοστό επιτυχίας εύρεσης ενός επιτιθέμενου μπορεί να αγγίξει το μηδέν. Σε αυτή την περίπτωση, ο Χρήστης **Y** αποστέλλει το ζητούμενο ποσό στον χρήστη **A**. Ο τελευταίος ακολουθεί ακριβώς τη διαδικασία διαμοιρασμού του ποσού που περιγράφηκε στο 3ο σενάριο και κάποια στιγμή, ένα πλήθος αυτών των συναλλαγών μετατρέπεται σε συνάλλαγμα. Εάν για παράδειγμα ο ενδιάμεσος χρήστης **Z** πραγματοποιήσει μια συναλλαγή μεταξύ ενός wallet στο Blockchain.com και ενός wallet του blockchain του Monero, τότε η διαδοχική σειρά συναλλαγών στο Blockchain.com έχει σταματήσει. Πλέον, ξεκινάει μια παρεμφερής διαδοχική σειρά από συναλλαγές στο blockchain του Monero όπου κάποια στιγμή μπορεί είτε να εξαργυρωθεί απευθείας εκεί, είτε να επιστρέψει στην αλυσίδα του Blockchain.com και να προστεθεί στο τελικό wallet του επιτιθέμενου.

Αποδεικνύεται λοιπόν, ότι όσο οι επιτιθέμενοι μιας οικογένειας Ransomware εκμεταλλεύονται την πολυπλοκότητα των blockchains είναι αδύνατο να εντοπιστούν ακολουθώντας ένα μοντέλο σειριακής ανάλυσης των συναλλαγών τους.

4.3. Συσσώρευση συναλλαγών στο wallet του επιτιθέμενου

Σκοπός κάθε οικογένειας Ransomware είναι να αποκομίσει όσο το δυνατόν περισσότερα χρήματα από τους οργανισμούς που στοχεύει. Χρησιμοποιώντας μεθόδους που αναλύθηκαν στην προηγούμενη ενότητα, οι επιτιθέμενοι μπορεί να έχουν στην κατοχή τους ένα ή περισσότερα “τελικά πορτοφόλια” (accumulative wallets), τα οποία έπειτα θα εξαργυρώσουν με ηλεκτρονικό ή φυσικό τρόπο.

Αναλύοντας τη διαδρομή των συναλλαγών από το accumulative wallet προς τις διευθύνσεις των θυμάτων, μπορούν να παραχθούν αποδεικτικά στοιχεία για το πλήθος των επιτυχημένων πληρωμών από ένα Ransomware Family αλλά και ο τόπος δράσης του.



Εικ. 4.2: Ανάλυση από το **accumulative** wallet προς τις διευθύνσεις των θυμάτων
(Πηγή: **https://elie.net/blog/security/how-to-trace-ransomware-payments-end-to-end/**)

Η συσσώρευση των συναλλαγών σε ένα ή πολλά τελικά wallets είναι ο βασικός τρόπος συσσώρευσης των χρημάτων από ένα Ransomware Campaign. Παράλληλα, ο εντοπισμός ενός accumulative wallet μπορεί να βοηθήσει στον εντοπισμό ενός επιτιθέμενου αφού όλες οι συναλλαγές καταλήγουν εκεί.

4.4. Τρόπος εξαργύρωσης (bitcoin.de, cex.io, κ.α.)

Η εξαργύρωση των εσόδων που έχουν συσσωρευτεί στο τελικό wallet της οικογένειας του Ransomware, είναι μια διαδικασία που λόγω της φύσης των κρυπτονομισμάτων απαιτεί σωστό σχεδιασμό.

Γενικά, η εξαργύρωση κρυπτονομισμάτων μπορεί να επιτευχθεί με διάφορους τρόπους. Οι περισσότεροι σχετίζονται με το συνάλλαγμα του κρυπτονομίσματος σε φυσικό νόμισμα, άλλοι αφορούν την κατάθεση σε λογαριασμούς τραπέζης ενώ υπάρχουν και οι τρόποι φυσικής εξαργύρωσης σε μετρητά ή άλλα υλικά αγαθά (ηλεκτρονικές αγορές).

Τα περισσότερα τρίτα μέρη που εξυπηρετούν τους ανωτέρω σκοπούς για την εξαργύρωση των κρυπτονομισμάτων, παρέχουν τις υπηρεσίες τους για συγκεκριμένα κρυπτονομίσματα και όχι για όλο το φάσμα των διακριτών κρυπτονομισμάτων που είναι ενεργά αυτή τη στιγμή. Συνεπώς, οι οικογένειες των Ransomware θα πρέπει να περιορίζονται σε συγκεκριμένα κρυπτονομίσματα ώστε να βρίσκουν διαθέσιμο συνάλλαγμα, κάτι που μειώνει τα σημεία ελέγχου κατά την απόπειρα εύρεσής τους.

Κάποιες παράμετροι που πρέπει να έχει υπόψη του ο επιτιθέμενος πριν την εξαργύρωση είναι:

- Οι ευκολότεροι τρόποι εξαργύρωσης είναι και οι ακριβότεροι, ως προς την προμήθεια που θα αφαιρεθεί από το τελικό συνάλλαγμα. Παράλληλα, οι φθηνότεροι τρόποι έχουν άλλους περιορισμούς όπως το μέσο συναλλαγής ή ο χρόνος αναμονής έως ότου ολοκληρωθεί η συναλλαγή.
- Η κατάθεση των χρημάτων μετά τη συναλλαγή μπορεί να γίνει είτε σε κάποιο φυσικό τραπεζικό λογαριασμό είτε σε τρίτες υπηρεσίες όπως το Paypal. Στην πρώτη περίπτωση βέβαια, είναι παρακινδυνευμένο από την μεριά του επιτιθέμενου να ζητήσει την κατάθεση του συναλλάγματος σε λογαριασμό του αφού αυξάνει τις πιθανότητες εντοπισμού του.
- Θα πρέπει να επιλεχθεί ο τρόπος συναλλάγματος που εξυπηρετεί τον σκοπό της εξαργύρωσης όσον αφορά τη χρονική περίοδο από τη στιγμή έναρξης του αιτήματος έως την τελική στιγμή της ανάληψής του.
- Θα πρέπει να επιλεχθεί εάν το συνάλλαγμα θα δοθεί σε φυσικό νόμισμα ή σε κάποιο άλλο κρυπτονόμισμα. Και στις δύο περιπτώσεις διαφαίνονται περιορισμοί όπως τα διακριτά νομίσματα και κρυπτονομίσματα, αφού όλες οι τρίτες υπηρεσίες ανταλλαγής συναλλάγματος συνεργάζονται με συγκεκριμένα συναλλάγματα.

Το επόμενο βήμα είναι η επιλογή του τρόπου εξαργύρωσης. Αυτοί διακρίνονται σε:

- Υπηρεσίες εξαργύρωσης από τρίτα μέρη μέσα από τα οποία επιτρέπεται η κατάθεση του συναλλάγματος σε τραπεζικό λογαριασμό του επιτιθέμενου. Αυτή η διαδικασία διαρκεί συνήθως 1 έως 5 ημέρες.
- Εξαργύρωση απευθείας σε άλλους χρήστες του Blockchain ή αλλιώς Peer-2-Peer(P2P) [47]. Ο επιτιθέμενος έχει τη δυνατότητα να βρει κάποιον άλλο ενδιαφερόμενο χρήστη του Blockchain που επιθυμεί την αγορά κρυπτονομίσματος και να ζητήσει την κατάθεση χρημάτων σε τραπεζικό λογαριασμό, τη μεταφορά χρημάτων με τη μέθοδο του εμβάσματος ή ακόμα και τη φυσική συναλλαγή μεταξύ των δύο χρηστών.

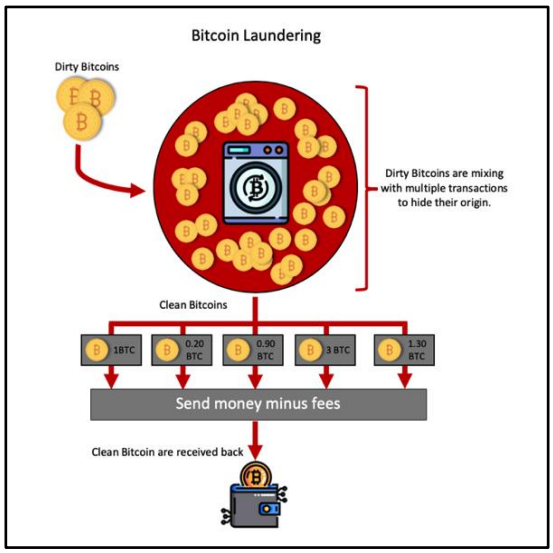
Επειδή στην περίπτωση ανίχνευσης των συγκεκριμένων κρυπτονομισμάτων, η οποιαδήποτε συναλλαγή θεωρείται παράνομη, πολλές φορές οι επιτιθέμενοι πριν από την επιλογή του τρόπου εξαργύρωσης χρησιμοποιούν μεθόδους νομιμοποίησης των κρυπτονομισμάτων (cryptocurrency laundering). Με αυτό τον τρόπο καταφέρνουν να νομιμοποιούν τα έσοδα του Ransomware Campaign.

4.5. Νομιμοποίηση εσόδων από παράνομες δραστηριότητες

Η νομιμοποίηση των εσόδων από ένα Ransomware Campaign αλλά και γενικά από οποιοδήποτε Malware Campaign, είναι μια διαδικασία που δεν παραλείπεται από τους επιτιθέμενους.

Υπάρχουν πολλές μέθοδοι για την νομιμοποίηση των εσόδων ενός επιτιθέμενου αφού δεν είναι απαραίτητο να υπάρχουν φυσικά συναλλάγματα από το εκάστοτε κρυπτονόμισμα στο εκάστοτε φυσικό νόμισμα. Η συναλλαγή κρυπτονομισμάτων μπορεί να γίνει με πολλούς τρόπους όπως με την τυχαιοπαιγνία, τη χρήση τρίτων μερών/υπηρεσιών συναλλάγματος, την εξ επαφής συναλλαγή (P2P) ή τον διαμοιρασμό του συνολικού ποσού σε τρίτους και την εκ νέου απόδοσή του στον επιτιθέμενο.

Ο τελευταίος είναι ένας από τους πιο συνήθεις τρόπους νομιμοποίησης. Οι υπηρεσίες που εκτελούν τη διαδικασία του money laundering διαμοιράζουν τα κρυπτονομίσματα του χρήστη σε τρίτους και του αποδίδουν εκ νέου τα νομιμοποιημένα πλέον έσοδα. Αυτές οι υπηρεσίες χαρακτηρίζονται και ως Mixers [48].

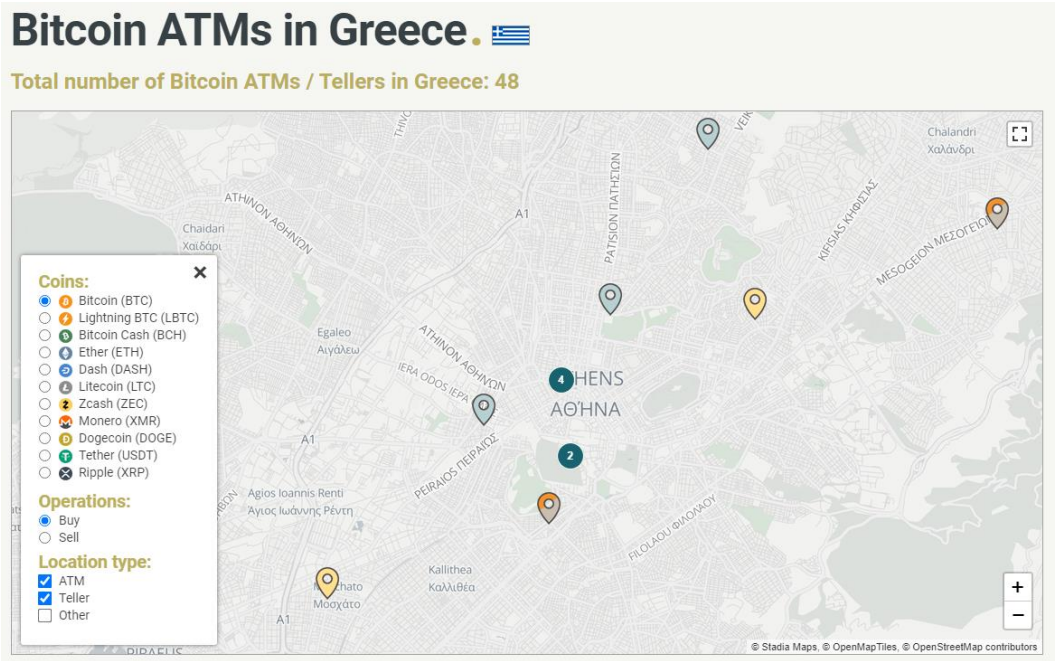


Εικ. 4.3: Χρήση Mixer για τη νομιμοποίηση κρυπτονομίσματος
(Πηγή: **https://www.cyberscoop.com/bestmixer-bitcoin-laundering-mcafee-europol/**)

Οι Mixers δέχονται ένα συγκεκριμένο ποσό από τον επιτιθέμενο και αυξάνουν την τυχαιότητα ανίχνευσής του διαμοιράζοντάς στο σε πολλά μικρότερα μέρη. Τα νέα μέρη του συνολικού ποσού αποστέλλονται με τη μορφή συναλλαγών σε διαφορετικές διευθύνσεις και επιστρέφουν στη συνέχεια στον Mixer. Εφόσον το συνολικό ποσό συγχωνευθεί εκ νέου, τότε ο Mixer κρατάει ένα ποσοστό ως φόρο παροχής υπηρεσιών και έπειτα διαμοιράζει το νέο

υπόλοιπο που πρέπει να επιστραφεί, σε wallets του επιτιθέμενου, τα οποία χαρακτηρίζονται ως Collectors.

Επιπροσθέτως, υπάρχουν πολλά φυσικά ATM για την αγορά και πώληση κρυπτονομισμάτων, στα οποία μπορεί ο επιτιθέμενος να εξαργυρώσει σε φυσικό νόμισμα το σύνολο ή μέρος του συνόλου που διαθέτει στο wallet του.



Εικ. 4.4: Διαθέσιμα ATM για αγορά/πώληση bitcoin στην Ελλάδα
(Πηγή: https://coinatmradar.com/country/83/bitcoin-atm-greece/)

ΚΕΦΑΛΑΙΟ 5ο: Εύρεση επιτιθέμενου αναλύοντας τις οικογένειες Ransomware και το Blockchain

Η εύρεση του επιτιθέμενου μετά από μια επιτυχημένη επίθεση με τη χρήση Ransomware δεν είναι πάντοτε εφικτή, αφού οι οικογένειες Ransomware κρύβουν τα ίχνη τους σε όλες τις φάσεις της επίθεσης. Πιο συγκεκριμένα, από τη μεταφορά του ransomware μέσω ενός ηλεκτρονικού μηνύματος έως την εκτέλεση του κακόβουλου κώδικα, είθισται να μην υπάρχουν τρωτά σημεία για την εύρεση του επιτιθέμενου. Παράλληλα, από τη στιγμή που ο επιτιθέμενος κρυπτογραφεί όλη την επικοινωνία μεταξύ προσβεβλημένης συσκευής και του ιδίου, οι πιθανότητες εύρεσής του μειώνονται κατακόρυφα.

Εφόσον συνδυαστούν κάποιες βασικές πληροφορίες όπως η πρωταρχική διεύθυνση που έπρεπε το θύμα να καταθέσει τα λύτρα, μαζί με τα εκτελέσιμα αρχεία(binaries) από διακριτές οικογένειες Ransomware, τότε με μεθοδολογίες ταυτοποίησης πολλών θυμάτων με τα binaries από συγκεκριμένη οικογένεια Ransomware, συνδυαστικά με τις πρωταρχικές διευθύνσεις πληρωμών, μπορεί να οδηγήσουν στον εντοπισμό του επιτιθέμενου.

5.1. Συλλογή αρχικών διευθύνσεων των ransomware

Είναι σύνηθες για μια οικογένεια Ransomware, να δίνει στο θύμα μια διεύθυνση κατάθεσης των λύτρων οι οποία έχει επαναχρησιμοποιηθεί. Η ίδια η οικογένεια δεν γνωρίζει τα στοιχεία του θύματος καθώς το Ransomware Campaign μπορεί να εκτελεστεί ταυτόχρονα σε πολλά θύματα.

Το παραπάνω γεγονός οδηγεί στο συμπέρασμα ότι μπορεί να γίνει η συλλογή των αρχικών διευθύνσεων που έχει χρησιμοποιήσει μια οικογένεια Ransomware από θύματα που έχουν αναφέρει το συμβάν ή από αποθήκες δεδομένων που διατηρούν ιστορικό αυτών των διευθύνσεων.

Ένας άλλος τρόπος για τη συλλογή των διευθύνσεων, είναι η εκτέλεση των binaries που εκκινούν την κρυπτογράφηση της συσκευής του θύματος, σε ελεγμένο περιβάλλον όπως Virtual Machines, Εργαστήρια Η/Υ σε ιδιωτικό δίκτυο, φυσικές ή εικονικές συσκευές που λειτουργούν σε περιβάλλον sandbox, κ.α. Κατά την εκτέλεση των binaries η συσκευή θα κλειδώσει και θα αποτυπώσει στην οθόνη του χρήστη τη διεύθυνση που πρέπει να καταθέσει το χρηματικό ποσό. Στην περίπτωση της εκτέλεσης σε headless mode μέσα από κάποιο sandbox, τότε αποθηκεύεται η μνήμη του Virtual Machine και εξάγεται από αυτή η διεύθυνση του Blockchain.

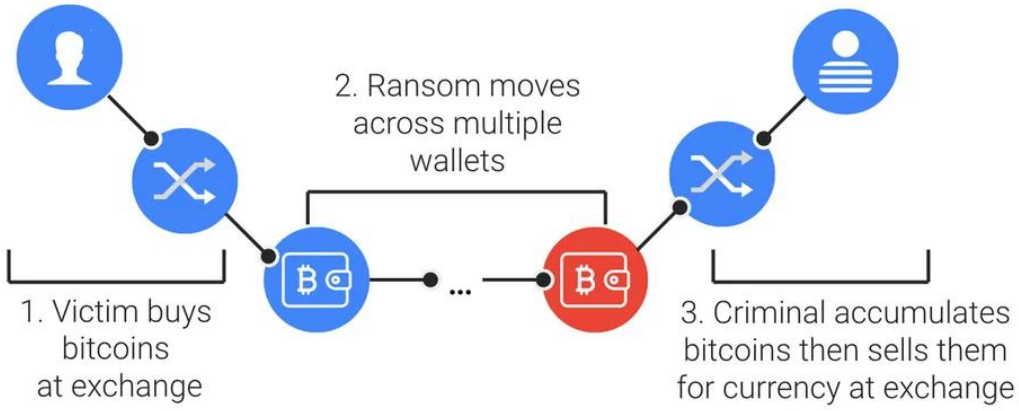
Μετά την ολοκλήρωση της φάσης συγκέντρωσης αυτών των πρωταρχικών διευθύνσεων, ταυτοποιώντας τα binaries που έχουν χρησιμοποιηθεί με υπηρεσίες όπως το VirusTotal - που ελέγχουν τον πηγαίο κώδικα ενός αρχείου και τον ταυτοποιούν με γνωστά malware - με τις οικογένειες των Ransomware, μπορεί να γίνει η κατηγοριοποίηση των διευθύνσεων ανά οικογένεια.

5.2. Δημιουργία εικονικών θυμάτων και πληρωμή επιτιθέμενου

Εφόσον έχει δημιουργηθεί μια αποθήκη με πρωταρχικές διευθύνσεις από οικογένειες Ransomware, σειρά έχει η δημιουργία εικονικών θυμάτων με σκοπό τις διαδοχικές πληρωμές στους πραγματικούς επιτιθέμενους.

Διατηρώντας τα εικονικά θύματα που χρησιμοποιήθηκαν για την ανάκτηση των πρωταρχικών διευθύνσεων, μπορεί να ξεκινήσει μια σειρά μικρο-πληρωμών προς αυτές, της τάξης του 0.0001 BTC. Διατηρώντας ένα αρχείο καταγραφών με τις πληρωμές ανά οικογένεια Ransomware μπορεί να ξεκινήσει η φάση παρακολούθησης των πληρωμών και κατά πως αυτές μεταφέρονται από τη μια διεύθυνση στην επόμενη. Παράλληλα, παρακολουθώντας τις ημερομηνίες που ένα binary από μια οικογένεια Ransomware, αναφέρεται σε αποθήκες δεδομένων όπως το VirusTotal, μπορεί να παραχθεί η ταύτιση μεταξύ διεύθυνσης και οικογένειας, αλλά και η περίοδος που το συγκεκριμένο Ransomware είναι ή ήταν ενεργό.

Μέσα από τη μέθοδο της παρακολούθησης του παραπάνω συστήματος, μπορούν να προκύψουν πρότυπα (patterns) από ποσά πληρωμών, ανάλογα με την κάθε οικογένεια. Συνεπώς η παρακολούθηση των συναλλαγών εντός του Blockchain τις περιόδους που το κάθε Ransomware φαίνεται ενεργό, μπορεί να δώσει στοιχεία για τον τρόπο με τον οποίο η κάθε οικογένεια διαμοιράζει τα ποσά που έχει λάβει. Από αυτές τις συναλλαγές, προκύπτει και εάν η οικογένεια του Ransomware μεταφέρει απλώς το ποσό από τα λύτρα σε ένα τελικό πορτοφόλι ή εάν το διασπά και το διαμοιράζει σε πληθώρα από άλλα πορτοφόλια έως ότου καταλήξουν στο τελικό πορτοφόλι της οικογένειας.



Εικ. 5.1: Προσομοίωση πληρωμής λύτρων, μεταφοράς στην αλυσίδα και εξαργύρωσης από τον επιτιθέμενο
(Πηγή: https://elie.net/blog/security/how-to-trace-ransomware-payments-end-to-end/)

Ενσωματώνοντας μεθόδους όπως η ομαδοποίηση (clustering) και η μηχανική μάθηση στην παραπάνω μεθοδολογία, μπορούν να προκύψουν τουλάχιστον τα διπλάσια δείγματα από αρχεία binaries που ανήκουν στις οικογένειες του Ransomware, άρα και περισσότερες διευθύνσεις που μπορούν να ομαδοποιηθούν για να ανιχνευτεί το τελικό wallet των επιτιθέμενων. Εν συνεχεία, αν οι μικρές καταθέσεις που έχουν γίνει από τα εικονικά θύματα καταγραφούν, είναι δυνατό να ανιχνευθεί κατά προσέγγιση το τελικό πορτοφόλι ενός επιτιθέμενου.

Όσο περισσότερο επαναλαμβάνεται αυτή η διαδικασία, τόσο περισσότερες είναι οι πιθανότητες να προκύψει το ίδιο τελικό πορτοφόλι από κάθε επαναληπτική πληρωμή των - διακριτών σε κάθε επανάληψη - εικονικών θυμάτων [49].

5.3. Ανίχνευση IP διευθύνσεων από τα εκτελέσιμα αρχεία

Μια παράλληλη ενέργεια που μπορεί να εκτελεστεί κατά τη διάρκεια της φάσης ανίχνευσης ενός accumulative wallet της οικογένειας Ransomware, είναι η προσπάθεια ανάκτησης στοιχείων του επιτιθέμενου μέσα από το ίδιο το binary.

Το binary αρχείο εκτελείται σε μια συσκευή χωρίς πρόσβαση στο διαδίκτυο. Κατα την εκτέλεση του πηγαίου κώδικα που φιλοξενεί το malware για την κρυπτογράφηση των αρχείων, εκτελούνται κάποιες εντολές επικοινωνίας προς συγκεκριμένες διευθύνσεις IP με συγκεκριμένα ports. Εάν αυτό το πείραμα επαναληφθεί κάποιες φορές, μπορεί να εντοπιστεί ένα υποδίκτυο διευθύνσεων IP με τις οποίες προσπαθεί να επικοινωνήσει η κλειδωμένη συσκευή.

Για την ανάκτηση των δεδομένων επικοινωνίας από τον κλειδωμένο και κρυπτογραφημένο Η/Υ χρησιμοποιούνται τεχνικές reversed engineering [50] με τη χρήση εργαλείων όπως το TCPDump, όπου παρέχεται η δυνατότητα καταγραφής όλων των πακέτων που προσπάθησαν να αποσταλούν προς το διαδίκτυο και συγκεκριμένα προς τις διευθύνσεις που επιχειρήθηκε η επικοινωνία. Συμπληρωματικά, ενεργοποιώντας την συστημική καταγραφή της συσκευής σε αρχεία logs πριν την εκτέλεση του binary, μπορούν να καταγραφούν όλα τα αρχεία τα οποία έχει επηρεάσει το Ransomware και να δημιουργηθεί ένα πρότυπο στο οποίο θα διαφαίνεται τόσο ο τρόπος και το σημείο επικοινωνίας της οικογένειας, όσο και η μέθοδος για τα σημεία που θα ενεργήσει η κρυπτογράφηση των αρχείων.

Από τα αποτελέσματα που θα δώσει το TCPDump, αντλείται το σύνολο των διευθύνσεων με τις περισσότερες απόπειρες επικοινωνίας, ενώ από αυτές μπορούν να εντοπιστούν οι πάροχοι από τους οποίους σε επόμενη φάση, είναι εφικτό να αναλυθεί το φυσικό τους μηχάνημα κατόπιν αιτήματος.

```
tcpdump: listening on eth0, link-type EN10MB (Ethernet), 23:11:10.370321 IP
(tos 0x20, ttl  48, id 34859, offset 0, flags [none], length: 84)
69.254.213.43 > 72.21.34.42: icmp 64: echo request seq 0
      0x0000:  4520 0054 882b 0000 3001 7cf5 45fe d52b  E..T.+..0.|.E..+
      0x0010:  4815 222a 0800 3530 272a 0000 25ff d744  H."..50'..%..D
      0x0020:  ae5e 0500 0809 0a0b 0c0d 0e0f 1011 1213  .^..............
      0x0030:  1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  .............!"#
      0x0040:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
      0x0050:  3435 3637                                4567
1 packets captured
1 packets received by filter
0 packets dropped by kernel
```

Εικ. 5.2: Παρακολούθηση επικοινωνίας μεταξύ δύο διευθύνσεων IP και εντοπισμός του πακέτου που στάλθηκε
(Πηγή: **https://infosecaddicts.com/tcpdump/**)

Για να θεωρηθεί επιτυχημένη η παραπάνω διαδικασία, θα πρέπει να ξεκινήσει μια επικοινωνία με τον πάροχο που προκύπτει από τις έως τότε αναλύσεις, ώστε προβεί ο εκάστοτε

αναλυτής στην ενοικίαση του φυσικού μηχανήματος (είναι απαραίτητο πάροχος να παρέχει υπηρεσίες ενοικίασης ή υποενοικίασης φυσικών μηχανημάτων).

ΚΕΦΑΛΑΙΟ 6ο: Εύρεση επιτιθέμενου με τη χρήση ενός Blockchain API

Ίσως το σημαντικότερο ερώτημα γύρω από το Blockchain, εφόσον αυτό χρησιμοποιείται για την πληρωμή λύτρων σε οικογένειες Ransomware είναι το εξής. Πως μπορούν να βρεθούν τα φυσικά πρόσωπα πίσω από μια τέτοιου είδους επίθεση ώστε να αποδοθεί δικαιοσύνη;

Η απάντηση στο παραπάνω ερώτημα έχει ταλαιπωρήσει ένα μεγάλο πλήθος επιστημόνων και επαγγελματιών στο χώρο της ασφάλειας πληροφοριακών συστημάτων, καθώς είναι τόσο δαιδαλώδης η πορεία των κρυπτονομισμάτων εντός της αλυσίδας του Blockchain, που φαντάζει σχεδόν αδύνατο να βρεθεί ένα συγκεντρωτικό wallet με τους επιτιθέμενους να διαφαίνονται πίσω από αυτό.

6.1. Υπάρχον μοντέλο ανίχνευσης επιτιθέμενου & περιορισμοί

Σύμφωνα με τη μέχρι τώρα βιβλιογραφική ανασκόπηση που πραγματοποιήθηκε στην παρούσα μεταπτυχιακή διατριβή, μόνο ένα μοντέλο ανίχνευσης των επιτιθέμενων εντός του Blockchain εντοπίστηκε να έχει προταθεί. Είναι αυτό που περιγράφεται στο 5ο κεφάλαιο και αποτελεί έργο των Elie Bursztein, Luca Invernizzi και Kylie McRoberts [49]. Το αποτέλεσμα του μοντέλου τους, καταλήγει σε συγκεκριμένες διευθύνσεις IP μέσα από την εκτενή ανάλυση που πραγματοποιείται κατά τη διάρκεια των εργαστηριακών τους μελετών, και αφορούν γνωστές οικογένειες ransomware.

Το συγκεκριμένο μοντέλο, επιφέρει ένα ποσοστό επιτυχίας για την εύρεση του επιτιθέμενου της τάξης του 90%[to be changed], το οποίο όμως, απαρτίζεται από βασικούς περιορισμούς. Πιο συγκεκριμένα, οι περιορισμοί του μοντέλου ανίχνευσης των Elie Bursztein, Luca Invernizzi και Kylie McRoberts [49], είναι:

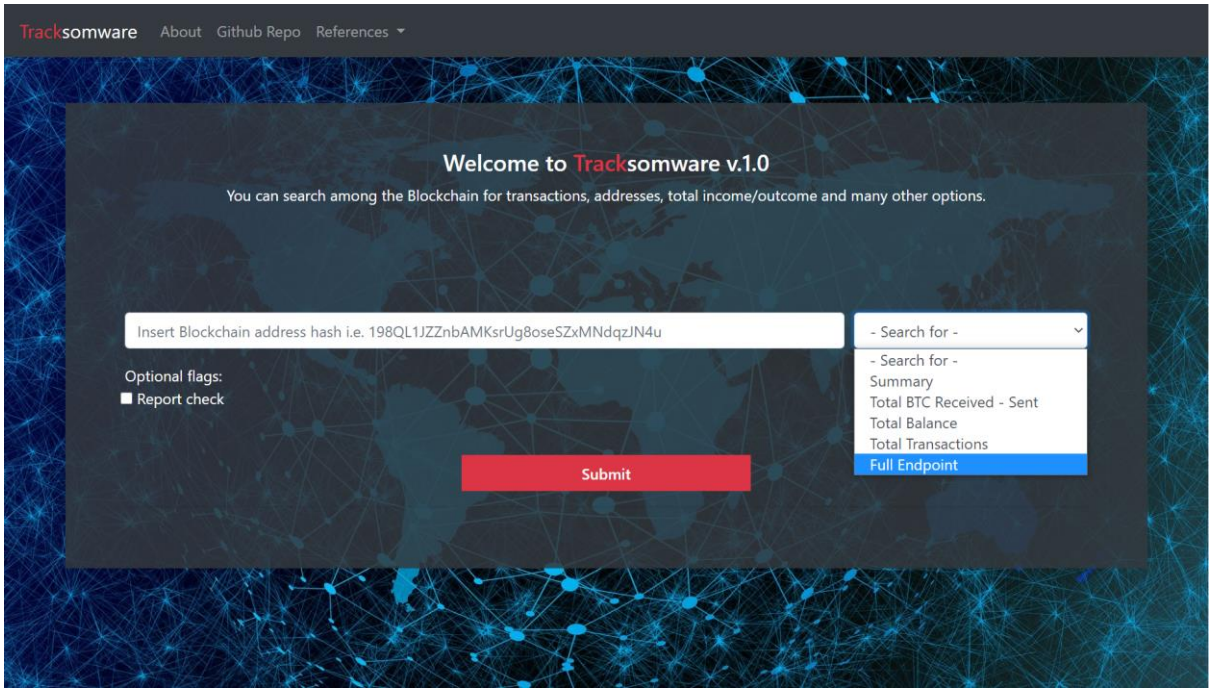
1. Χρήση πληθώρας από binary αρχεία επιθέσεων που είχαν ήδη πραγματοποιηθεί σε μεγάλο διάστημα πριν την έναρξη της ανάλυσής τους
2. Τα binaries που αναλύθηκαν την ίδια χρονική στιγμή, προέκυπταν από πολλές οικογένειες ransomware
3. Η υπολογιστική ισχύς που είχαν στη διάθεσή τους, βοήθησε στην ταυτόχρονη ανάλυση τόσο των binaries, όσο και της εκτέλεσής τους σε μεγάλο όγκο από εικονικές μηχανές, ώστε:
    a. τα αποτελέσματά τους να προκύψουν από ένα πιο ρεαλιστικό μοντέλο
    b. να γίνει αποκλεισμός των διευθύνσεων από mixers εντός της αλυσίδας συναλλαγών
4. Ο χρόνος απόκρισης από τη στιγμή της επίθεσης έως τα πρώτα έγκυρα αποτελέσματα, άγγιξε περίπου τα δύο χρόνια

Φαίνεται λοιπόν, πως ένα τέτοιο έργο, αν και αποτελεσματικό, δημιουργεί ένα κενό μεταξύ των επιστημονικών ομάδων στον τομέα της ασφάλειας και του προβλήματος, αφού η υπολογιστική ισχύς, η χρονική περίοδος και οι οικονομικοί πόροι για μια παρεμφερή μελέτη, είναι δυσεύρετοι για την πλειονότητα αυτών των μελετητών.

6.2. Δημιουργία ηλεκτρονικής εφαρμογής

Με αφορμή τους περιοριστικούς παράγοντες που περιγράφηκαν παραπάνω, δημιουργήθηκε μια ηλεκτρονική εφαρμογή, η οποία συνδυάζει πληροφορίες που παρέχουν τρίτα μέρη για το Blockchain με εγγενή στοιχεία του ίδιου, και σχηματίζει ένα αποτέλεσμα κατανόησης της διαδρομής που ακολουθούν τα κρυπτονομίσματα από την αρχική κατάθεση έως το acumulative wallet.

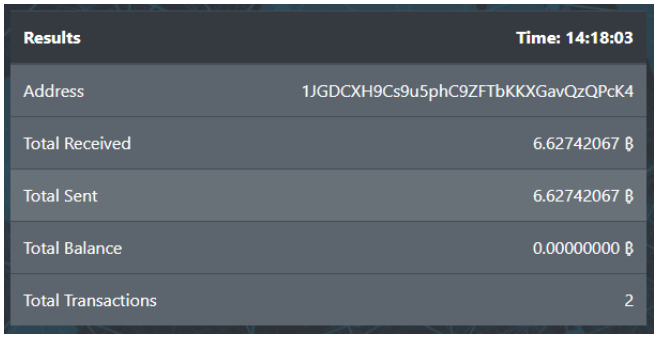
Λαμβάνοντας υπόψη το γεγονός πως για την ορθή λειτουργία της απαιτείται μηδενικό κόστος, αλλά και τους περιορισμούς που προκύπτουν λόγω αυτού, καταλήγει σε κάποια συμπεράσματα τα οποία μπορούν να αποτελέσουν ενεργό κομμάτι της έρευνας γύρω από έναν επιτιθέμενο σε δεδομένη χρονική στιγμή.



Εικ. 6.1: Η ηλεκτρονική πλατφόρμα “Tracksomware”
(Πηγή: Tracksomware Web Application)

Σκοπός της εφαρμογής, είναι μέσα από μια σειρά από ερωτήσεις προς το RESTful API του Blockchain, να επιστρέψει δεδομένα για ένα ή πολλά transactions, που συμπεριλαμβάνονται στο εκάστοτε block του address που εισήγαγε ο αναλυτής (όπως φαίνεται και στην παραπάνω εικόνα). Οι επιλογές του αναλυτή πέρα από την εισαγωγή ενός address, είναι να επιλέξει τι επιθυμεί να μάθει για αυτό. Πιο συγκεκριμένα, διατίθενται:

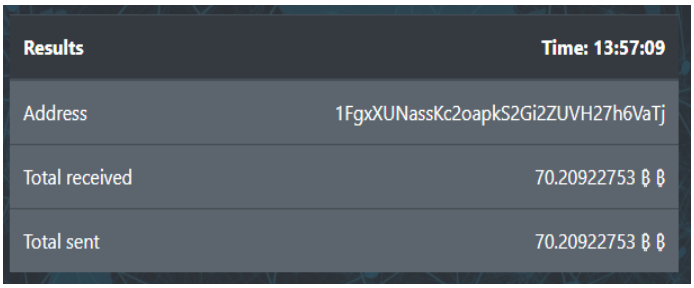
Summary: Αφορά μια περιληπτική εικόνα της κατάστασης του δεδομένου address με στοιχεία όπως το σύνολο των Bitcoins που διαθέτει, τα συνολικά transactions από και προς αυτό, καθώς και το πλήθος σε Bitcoins που έχει στείλει ή λάβει.



Results	Time: 14:18:03
Address	1JGDCXH9Cs9u5phC9ZFTbKKXGavQzQPcK4
Total Received	6.62742067 ฿
Total Sent	6.62742067 ฿
Total Balance	0.00000000 ฿
Total Transactions	2

Εικ. 6.2: Αποτελέσματα επιλογής “Summary”
(Πηγή: Tracksomware Web Application)

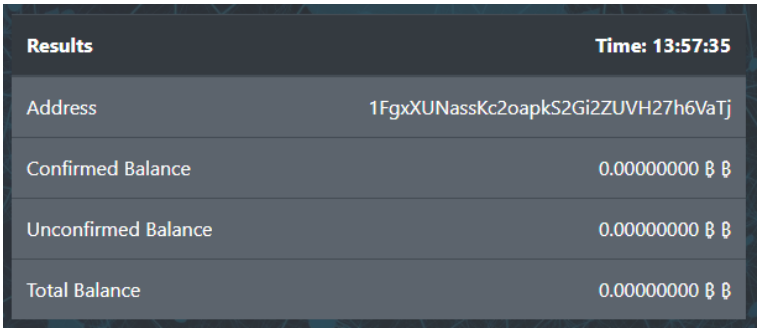
Total BTC Received - Sent: Το σύνολο σε Bitcoins που έχει λάβει ή στείλει το συγκεκριμένο address.



Results	Time: 13:57:09
Address	1FgxXUNassKc2oapkS2Gi2ZUVH27h6VaTj
Total received	70.20922753 ฿ ฿
Total sent	70.20922753 ฿ ฿

Εικ. 6.3: Αποτελέσματα επιλογής “Total BTC Received - Sent”
(Πηγή: Tracksomware Web Application)

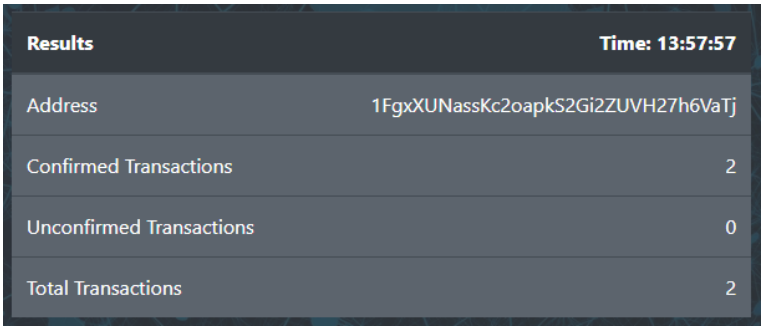
Total Balance: Το σύνολο σε Bitcoins που διαθέτει τη χρονική στιγμή της ερώτησης το συγκεκριμένο address.



Results	Time: 13:57:35
Address	1FgxXUNassKc2oapkS2Gi2ZUVH27h6VaTj
Confirmed Balance	0.00000000 ฿ ฿
Unconfirmed Balance	0.00000000 ฿ ฿
Total Balance	0.00000000 ฿ ฿

Εικ. 6.4: Αποτελέσματα επιλογής “Total Balance”
(Πηγή: Tracksomware Web Application)

Total Transactions:Τις εγκεκριμένες και μη συναλλαγές που έχουν πραγματοποιηθεί στο συγκεκριμένο address.



Εικ. 6.5: Αποτελέσματα επιλογής “Total Transactions”
(Πηγή: Tracksomware Web Application)

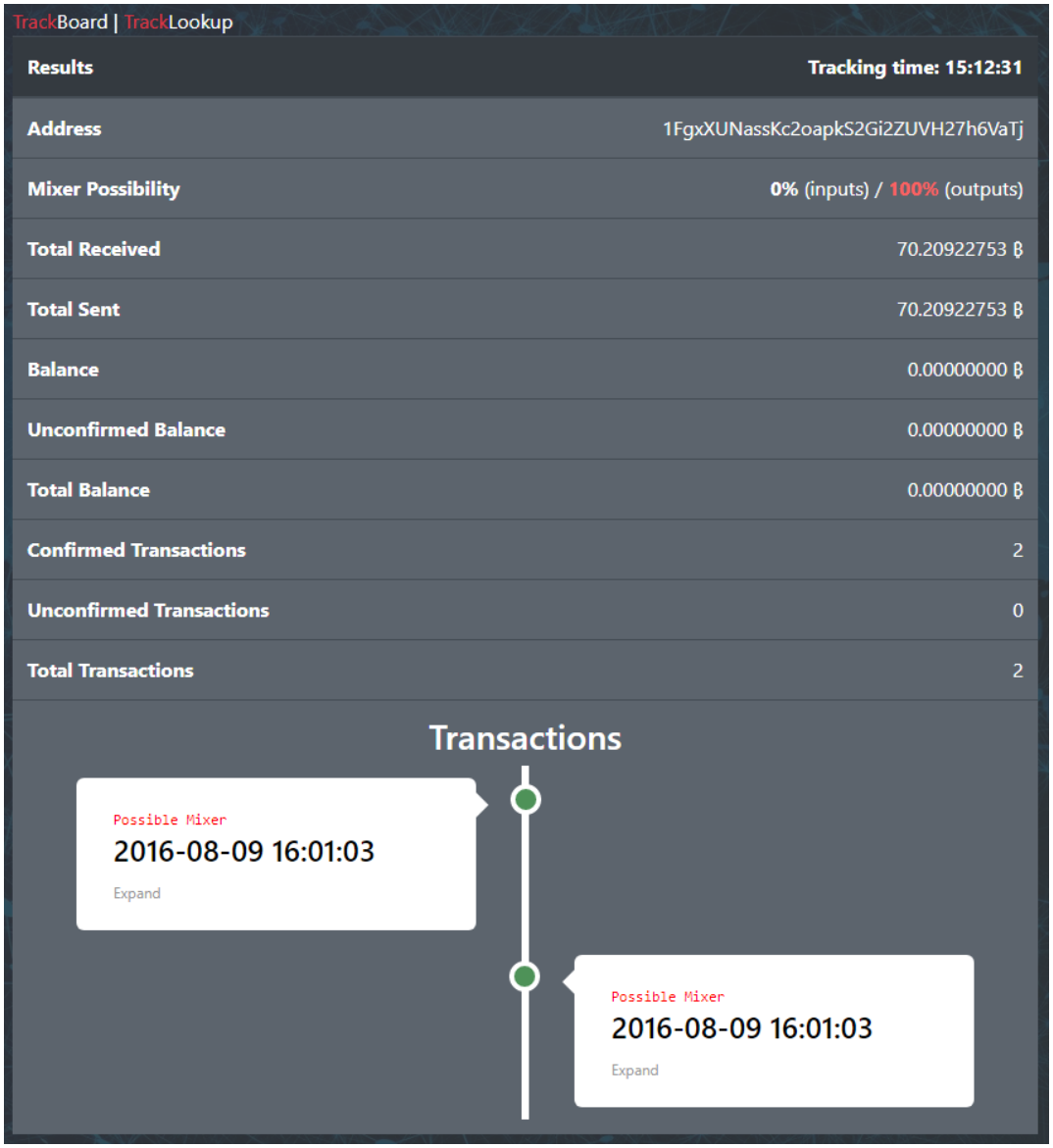
Full Endpoint: Όλες τις πληροφορίες που εμπεριέχονται στο συγκεκριμένο address με εις βάθος ανάλυση και πληροφόρηση προς τον αναλυτή.

6.2.1 Ανάλυση “Full Endpoint”

Η “**Full Endpoint**” επιλογή αποτελεί τον τρόπο με τον οποίο η εφαρμογή μπορεί να αναζητήσει δεδομένα μέσα από το Blockchain και συγκεκριμένα από την ιστορικότητα ενός δεδομένου address.

Αντλεί τα δεδομένα της μέσα από το Blockcypher API και εφόσον πραγματοποιηθεί η φάση της επεξεργασίας των δεδομένων, για την καλύτερη κατανόησή τους από τον αναλυτή, τα επιστρέφει στην οθόνη του. Παράλληλα, μετατρέπει το συνάλλαγμα από Satoshis σε Bitcoins και δημιουργεί ένα χρονολόγιο από transactions περιλαμβάνοντας όλες τις πληροφορίες τους σε κατηγοριοποιημένη μορφή.

Εφόσον το συγκεκριμένο address ξεπερνάει ένα δεδομένο κατώφλι συναλλαγών, τότε θεωρείται πως αποτελεί μέρος του δικτύου συναλλαγών με Mixers, χωρίς να αποκλείεται η περίπτωση όπου το ίδιο είναι ένας Mixer. Με τη σήμανση “**Mixer Possibility**”, ο αναλυτής μπορεί απευθείας να αναγνωρίσει αν το address ανήκει στην παραπάνω περίπτωση, ενώ μπορεί είτε να διακόψει την ανάλυσή του είτε να τη στοχεύσει προς ένα block συναλλαγών το οποίο περιλαμβάνει τιμές σε BTC που τείνουν προς το μοτίβο συναλλαγής από μια επίθεση.



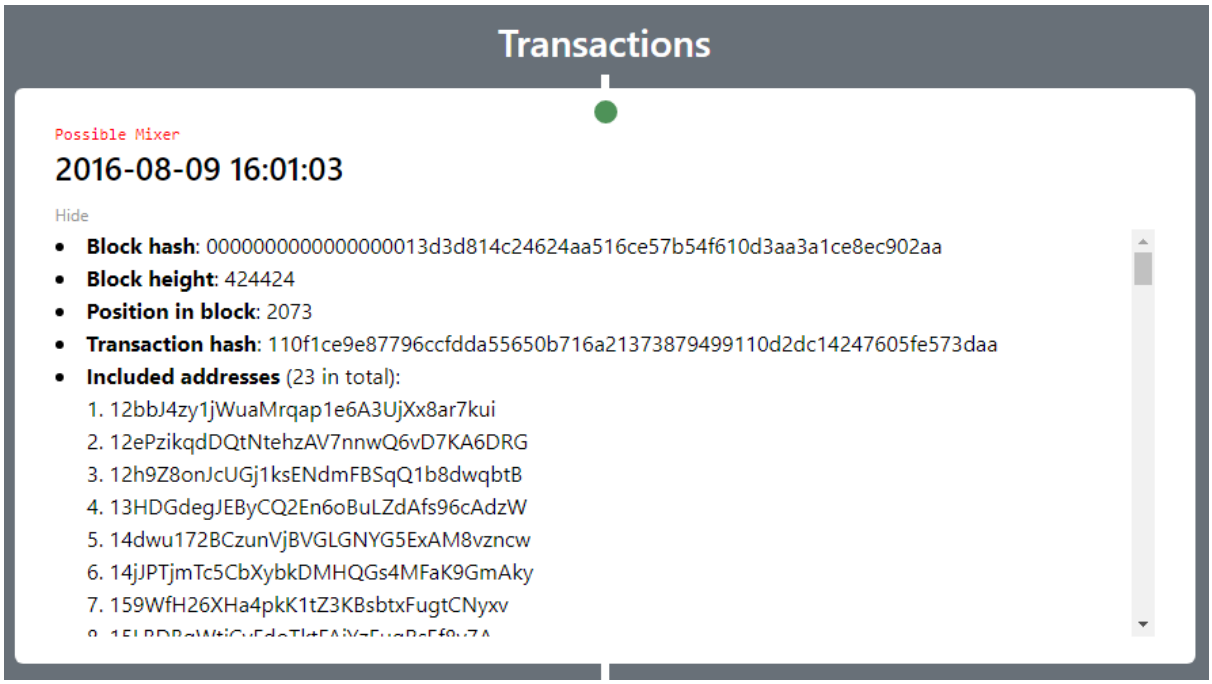
Εικ. 6.6: Αποτελέσματα επιλογής “Total Balance”
(Πηγή: Tracksomware Web Application)

6.2.2 Ανάλυση συναλλαγών

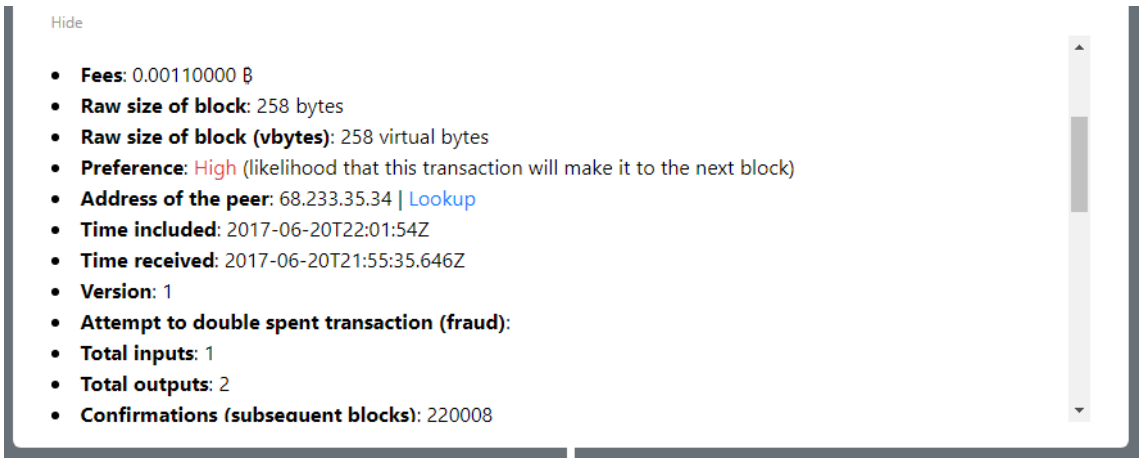
Πατώντας την επιλογή “*Expand*”, ο αναλυτής μπορεί να δει αναλυτικά όλες τις πληροφορίες που περιέχονται στο transaction της συγκεκριμένης ημερομηνίας. Παράλληλα, του δίνεται η δυνατότητα να αποθηκεύσει συγκεκριμένα στοιχεία για το συγκεκριμένο transaction, να κάνει μια εις βάθος ανάλυση για τη IP διεύθυνση του Peer που έστειλε το αίτημα (εφόσον αυτή έχει αποθηκευτεί στο Blockchain) και να αποθηκεύσει πληροφορίες για αυτή, καθώς και να επαναλάβει τη διαδικασία του “Full Endpoint” χρησιμοποιώντας μια διεύθυνση που έχει βρει κατά τη διάρκεια προβολής των δεδομένων. Η ανάλυση της διεύθυνσης IP του Peer, αναλύεται παρακάτω στην υποενότητα 6.2.3.

Ένα σημαντικό στοιχείο της συγκεκριμένης ανάλυσης, είναι η τιμή που επιστρέφεται στο πεδίο “**Attempt to double spent transaction**”. Το πεδίο αυτό αφορά τις περιπτώσεις όπου για

το συγκεκριμένο transaction έχουν γίνει δύο απόπειρες για την εκτέλεσή του, ενώ μόνο η 1η έχει εγκριθεί από το Blockchain και από τον λογαριασμό που πραγματοποιεί την κατάθεση. Αυτές οι συναλλαγές ονομάζονται “Double Spend” και αποτελούν προϊόν απάτης προς το ίδιο το Blockchain καθώς δεν πληρούν τους κανόνες που ορίζονται από αυτό, ώστε να θεωρούνται έγκυρες.



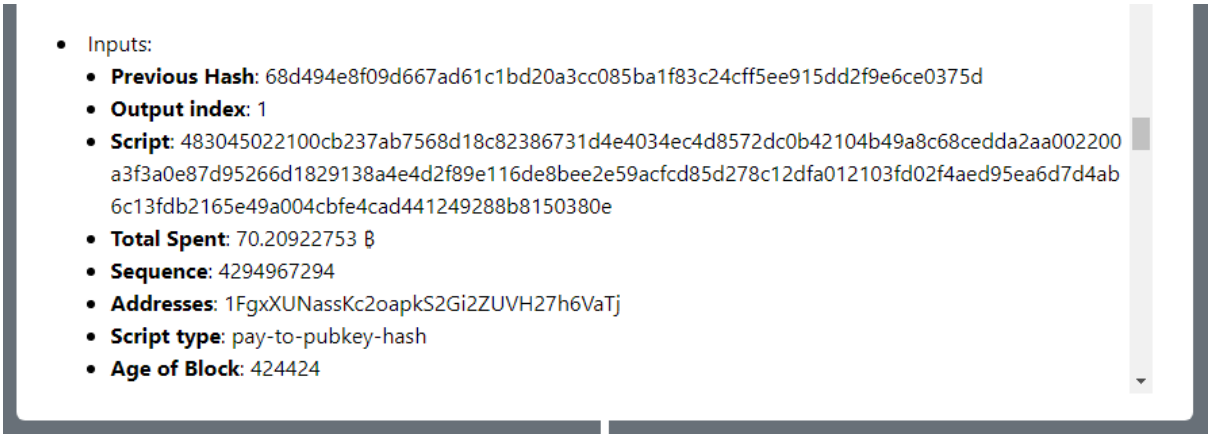
Εικ. 6.7: Αποτελέσματα επιλογής “Full Endpoint” - Μέρος Α
(Πηγή: Tracksomware Web Application)



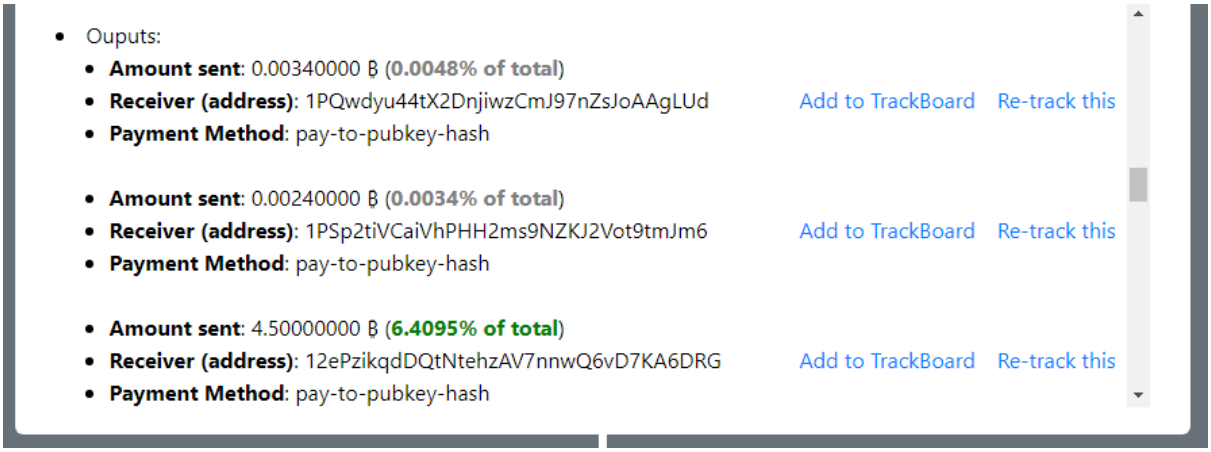
Εικ. 6.8: Αποτελέσματα επιλογής “Full Endpoint”, Μέρος Β - Δυνατότητα IP Lookup
(Πηγή: Tracksomware Web Application)

Όπως φαίνεται και στις εικόνες 6.7 - 6.10, ο αναλυτής έχει στη διάθεσή του πληθώρα δεδομένων που αφορούν το δεδομένο address όπως το hash του block, το hash της συναλλαγής, όλες τις διευθύνσεις που συμπεριλαμβάνονται σε αυτό το block (συνήθως πρόκειται για άλλα θύματα, mixers ή collector addresses του επιτιθέμενου), τη διεύθυνση του Peer που έχει δεχτεί αυτή τη συναλλαγή, το input του επιτιθέμενου, δηλαδή πόσα bitcoins έχουν

διαμοιραστεί αλλά και με ποιον τρόπο (pay-to-pubkey-hash), φυσικά τα outputs τα οποία αναλύουν διακριτά κάθε μία συναλλαγή προς αυτό το address, κ.α.



Εικ. 6.9: Αποτελέσματα επιλογής “Full Endpoint”, Μέρος Γ
(Πηγή: Tracksomware Web Application)



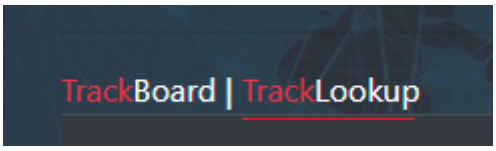
Εικ. 6.10: Αποτελέσματα επιλογής “Full Endpoint”, Μέρος Δ - Δυνατότητα καταγραφής συναλλαγής ή εκ νέου αναζήτησης με τη διεύθυνση του παραλήπτη
(Πηγή: Tracksomware Web Application)

6.2.3 Ανάλυση διεύθυνσης - IP Address (TrackLookup)

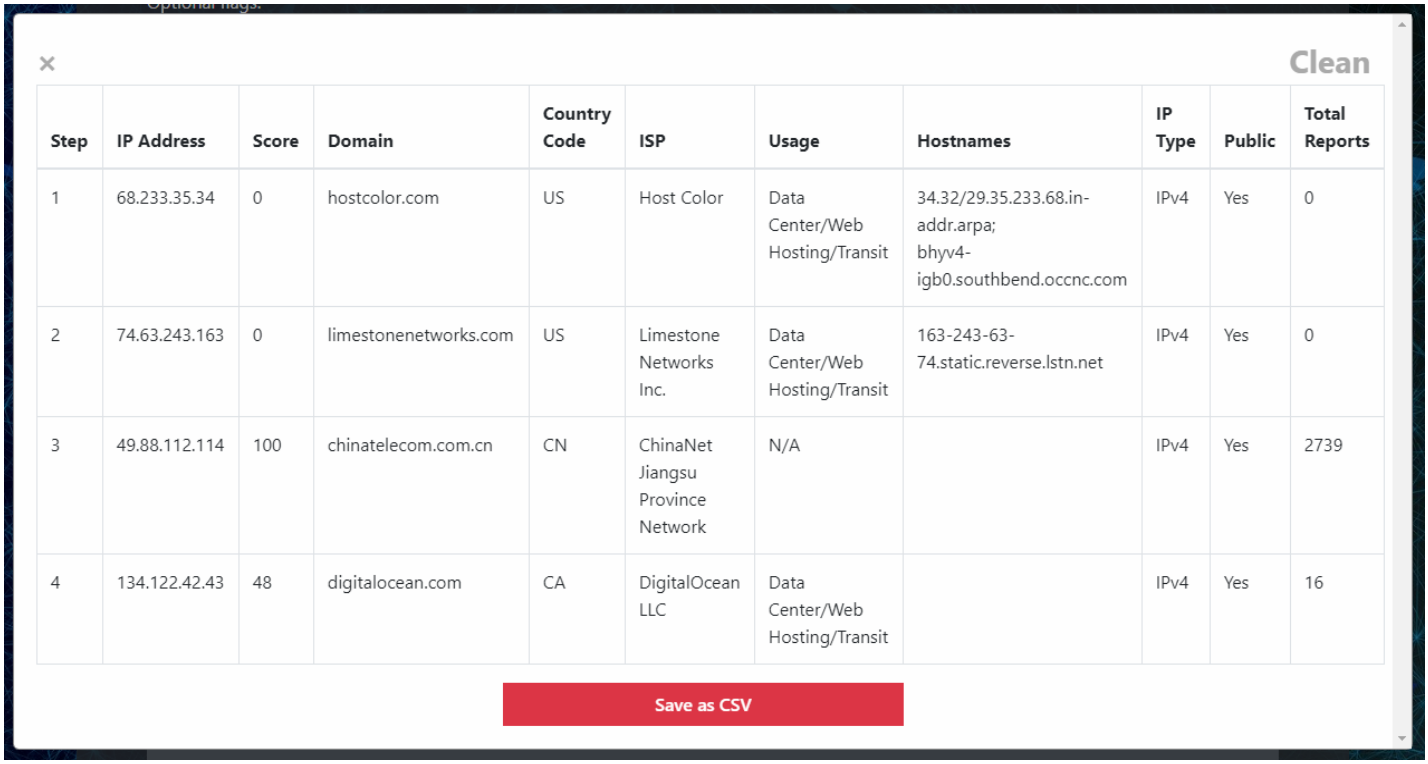
Πιο συγκεκριμένα, στην εικόνα 6.8, και εφόσον πρόκειται για συναλλαγή P2P, δίνεται στον αναλυτή η διεύθυνση IP του χρήστη που έλαβε το εν λόγω ποσό και παράλληλα η δυνατότητα να την αναλύσει μέσα από το API της υπηρεσίας AbuseIPDB.

Η υπηρεσία αυτή παρέχει δεδομένα τα οποία έχουν αναφερθεί από απλούς χρήστες, webmasters, IT administrators ή και παρόχους υπηρεσιών διαδικτύου και παραθέτουν τη βαθμολογία της διεύθυνσης ως προς την κατάχρηση που ασκεί, ένα χαρακτηρισμό π.χ. Spam, Ransomware, Blackmailing, κ.λπ., καθώς και πληροφορίες για τη δεδομένη διεύθυνση IP.

Τα αποτελέσματα που επιστρέφονται αποθηκεύονται αυτόματα στον πίνακα “*TrackLookup*” από όπου ο αναλυτής μπορεί να ανατρέξει σε αυτά ακόμα και μετά από πολλές χρήσεις της υπηρεσίας ή/και να τα αποθηκεύσει τοπικά σε μορφή CSV.



Εικ. 6.11: Πρόσβαση στον πίνακα “**TrackLookup**” πατώντας στον ομώνυμο σύνδεσμο
(Πηγή: Tracksomware Web Application)



Clean

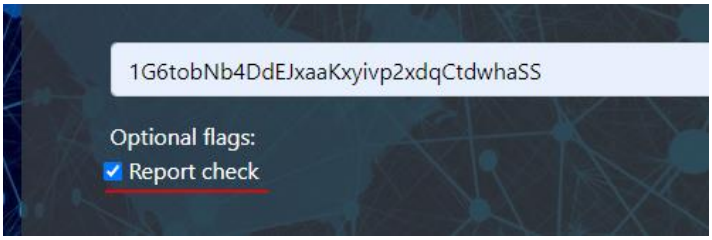
Step	IP Address	Score	Domain	Country Code	ISP	Usage	Hostnames	IP Type	Public	Total Reports
1	68.233.35.34	0	hostcolor.com	US	Host Color	Data Center/Web Hosting/Transit	34.32/29.35.233.68.in-addr.arpa; bhyv4-igb0.southbend.occnc.com	IPv4	Yes	0
2	74.63.243.163	0	limestonenetworks.com	US	Limestone Networks Inc.	Data Center/Web Hosting/Transit	163-243-63-74.static.reverse.lstn.net	IPv4	Yes	0
3	49.88.112.114	100	chinatelecom.com.cn	CN	ChinaNet Jiangsu Province Network	N/A		IPv4	Yes	2739
4	134.122.42.43	48	digitalocean.com	CA	DigitalOcean LLC	Data Center/Web Hosting/Transit		IPv4	Yes	16

Εικ. 6.12: Αποτελέσματα χρήσης του “Report check” για τη δεδομένη διεύθυνση
(Πηγή: Tracksomware Web Application)

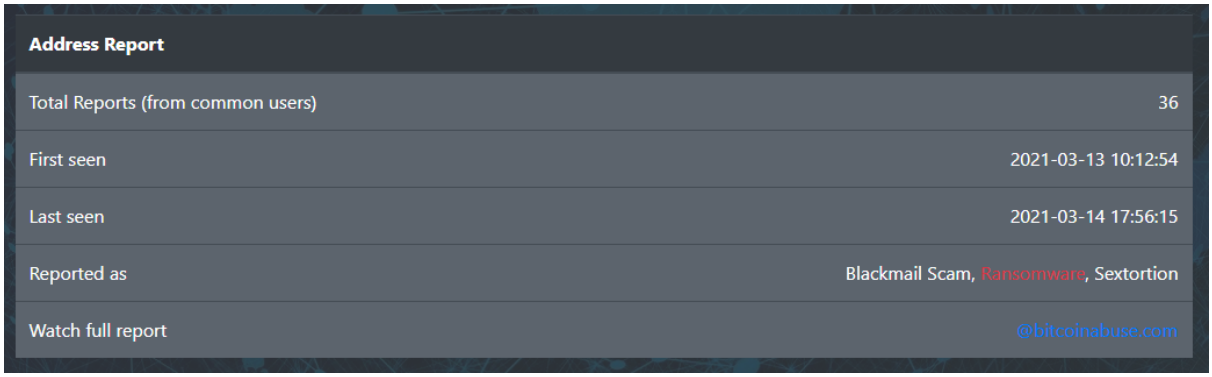
6.2.4 Ανάλυση διεύθυνσης - Έλεγχος αναφορών

Μία ακόμα λειτουργικότητα της εφαρμογής “Tracksomware”, είναι η ενεργοποίηση της ρύθμισης “Report check” κατά τη φάση της αρχικής ανάλυσης. Αυτή η ρύθμιση μπορεί να ενεργοποιηθεί συνδυαστικά με οποιαδήποτε από τις επιλογές ανάλυσης και επιστρέφει στον αναλυτή περιληπτικά δεδομένα για το αν η δεδομένη διεύθυνση έχει αναφερθεί στο παρελθόν στη βάση δεδομένων της υπηρεσίας BitcoinAbuse.

Εφόσον βρεθούν δεδομένα για τη διεύθυνση, τότε στο κάτω μέρος της οθόνης του αναλυτή θα δημιουργηθεί ένας πίνακας που περιέχει τις συνολικές αναφορές από απλούς χρήστες, την ημερομηνία εμφάνισής της με βάση την αρχική αλλά και την πιο πρόσφατη αναφορά, την κατηγορία ή τις κατηγορίες επίθεσης στις οποίες ανήκει, καθώς και ένα σύνδεσμο ώστε ο αναλυτής να ανατρέξει στη συνολική αναφορά που παρέχεται μέσα από την υπηρεσία BitcoinAbuse, εφόσον το κρίνει απαραίτητο.



Εικ. 6.13: Δυνατότητα εμφάνισης αναφοράς για τη συγκεκριμένη διεύθυνση του Blockchain
(Πηγή: Tracksomware Web Application)



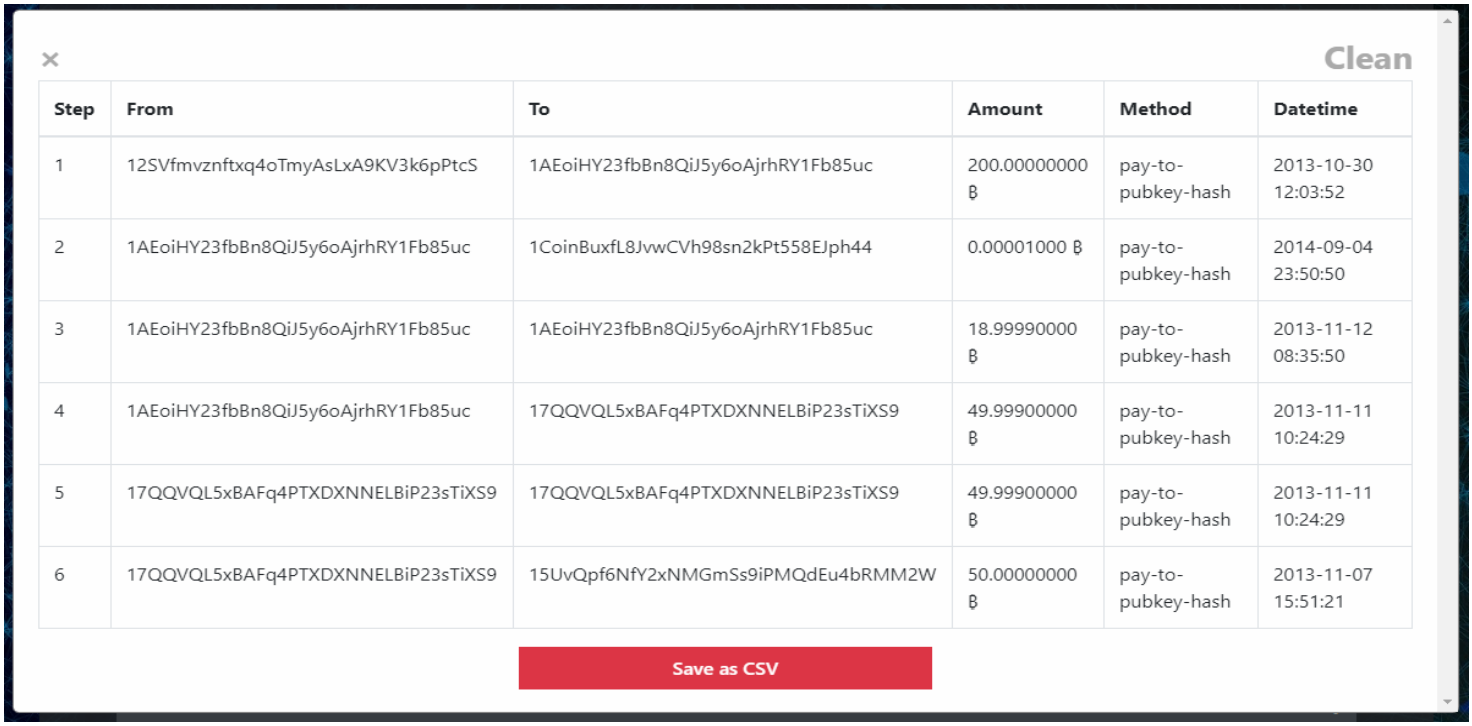
Εικ. 6.14: Αποτελέσματα χρήσης του “Report check” για τη δεδομένη διεύθυνση
(Πηγή: Tracksomware Web Application)

6.2.5 Ανάλυση διεύθυνσης - Έλεγχος Output

Το σημείο αναφοράς της συγκεκριμένης εφαρμογής, είναι η δυνατότητα επαναληπτικής ανάλυσης που διαθέτει ο αναλυτής, εφόσον εντοπίσει μια ύποπτη συναλλαγή μέσα στη δεδομένη διεύθυνση.

Για παράδειγμα, αν εκτελεστεί ανάλυση για τη διεύθυνση της οικογένειας ransomware Cryptolocker **`12SVfmvznftxq4oTmyAsLxA9KV3k6pPtcS`** μπορεί να φανεί αναδρομικά, ότι πρόκειται για μια collector address ή αλλιώς διεύθυνση συλλέκτη. Αυτή η διεύθυνση συλλέγει μεγάλα ποσά από πολλαπλές διευθύνσεις, τα ανακατευθύνει στον εαυτό της και σε άλλους collectors έως ότου καταλήξουν στο τελικό πορτοφόλι της οικογένειας. Κάθε address που αποτελεί μέρος μιας καμπάνιας ransomware, μπορεί να χαρακτηριστεί ως θύμα, συλλέκτης, mixer ή τελικό πορτοφόλι.

Συνεπώς, θα πρέπει να επαναληφθεί η διαδικασία της αναδρομικής ανάλυσης και στις υπόλοιπες διευθύνσεις που έχει συλλέξει ο αναλυτής κατά την πρώτη φάση. Είναι σημαντικό να αναφερθεί, πως λόγω μεμονωμένων πόρων η ανάλυση παραμένει μια χειροκίνητη και όχι αυτοματοποιημένη διαδικασία, κάτι που περιγράφεται στους περιορισμούς της εφαρμογής στην ενότητα 6.4 του παρόντος κεφαλαίου, αλλά και στη μελλοντική της εξέλιξη στο 8ο κεφάλαιο.



×

Clean

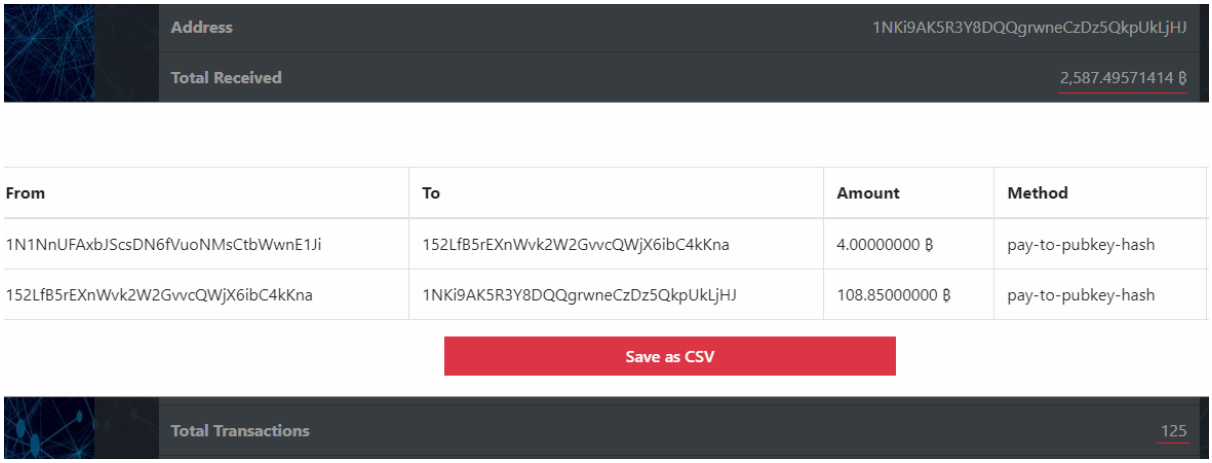
Step	From	To	Amount	Method	Datetime
1	12SVfmvznftxq4oTmyAsLxA9KV3k6pPtcS	1AEoiHY23fbBn8QiJ5y6oAjrhRY1Fb85uc	200.00000000 ฿	pay-to-pubkey-hash	2013-10-30 12:03:52
2	1AEoiHY23fbBn8QiJ5y6oAjrhRY1Fb85uc	1CoinBuxfL8JvwCVh98sn2kPt558EJph44	0.00001000 ฿	pay-to-pubkey-hash	2014-09-04 23:50:50
3	1AEoiHY23fbBn8QiJ5y6oAjrhRY1Fb85uc	1AEoiHY23fbBn8QiJ5y6oAjrhRY1Fb85uc	18.99990000 ฿	pay-to-pubkey-hash	2013-11-12 08:35:50
4	1AEoiHY23fbBn8QiJ5y6oAjrhRY1Fb85uc	17QQVQL5xBAFq4PTXDXNNELBiP23sTiXS9	49.99900000 ฿	pay-to-pubkey-hash	2013-11-11 10:24:29
5	17QQVQL5xBAFq4PTXDXNNELBiP23sTiXS9	17QQVQL5xBAFq4PTXDXNNELBiP23sTiXS9	49.99900000 ฿	pay-to-pubkey-hash	2013-11-11 10:24:29
6	17QQVQL5xBAFq4PTXDXNNELBiP23sTiXS9	15UvQpf6NfY2xNMGmSs9iPMQdEu4bRMM2W	50.00000000 ฿	pay-to-pubkey-hash	2013-11-07 15:51:21

Save as CSV

Εικ. 6.15: Αποτελέσματα χρήσης της “Re-track this” επιλογής μετά από επιλογή δεδομένων προς ανάλυση και αποθήκευση στο “TrackBoard”
(Πηγή: Tracksomware Web Application)

Ως δεύτερο παράδειγμα, ο αναλυτής εισάγει τη διεύθυνση ενός θύματος (εφόσον είναι κοινοποιημένη σε εκείνον/η) **`152LfB5rEXnWvk2W2GvvcQWjX6ibC4kKna`** και προσπαθεί να ακολουθήσει όλα τα βήματα προς το τελικό πορτοφόλι, αποκλείοντας στην πορεία πιθανούς mixers, και αποθηκεύοντας πιθανές διευθύνσεις IP. Η συγκεκριμένη διεύθυνση ανήκει σε θύμα του ransomware Locky και έστειλε 4.0 BTC στον 1ο collector του campaign. Αυτός με τη σειρά του διαμοιράζει σε mixers και λοιπούς collectors το ποσό των 2.587,49 BTC το οποίο έχει συλλεχθεί από το σύνολο των θυμάτων για το συγκεκριμένο campaign.

Για άλλη μια φορά, εφόσον συνεχιστεί η εις βάθος ανάλυση όπως στο προηγούμενο παράδειγμα, μπορεί να γίνει συλλογή πολλαπλών διευθύνσεων IP καθώς και στοιχείων για τα ίχνη του επιτιθέμενου, τα οποία συνδυαστικά με binaries από το κάθε θύμα μπορούν να ταυτοποιήσουν την οικογένεια ransomware.



Εικ. 6.16: Αποτελέσματα χρήσης της “Re-track this” για την καταγραφή collector εισάγοντας τη διεύθυνση του θύματος
(Πηγή: Tracksomware Web Application)

6.2.6 Ανάλυση διεύθυνσης - Επεξήγηση αποτελεσμάτων

Στον παρακάτω πίνακα παρατίθενται όλες οι επεξηγήσεις σχετικά με τα ονόματα κλειδιά που επιστρέφει μια αναζήτηση μέσω της πλατφόρμας Tracksomware. Θα πρέπει να επισημανθεί, πως τα κλειδιά τα οποία μεταφράζονται και επεξηγούνται αφορούν τη δεδομένη χρονική στιγμή που συντάσσεται η παρούσα μεταπτυχιακή διατριβή, και όχι την αντικειμενική εικόνα που μπορεί να έχουν ανά πάσα ώρα και στιγμή, καθώς κάποιο από αυτά ενδέχεται να αλλάξει.

Πηγαίο όνομα	**Μετάφραση**	**Περιγραφή**
`address`	Address	Η δεδομένη διεύθυνση προς ανάλυση.
`total_received`	Total Received	Το σύνολο σε satoshi που έχει λάβει η διεύθυνση.
`total_sent`	Total Sent	Το σύνολο σε satoshi που έχει στείλει η διεύθυνση.
`balance`	Balance	Η διαφορά σε satoshi μεταξύ των outputs και inputs της συγκεκριμένης διεύθυνσης για συναλλαγές που έχουν εγκριθεί τουλάχιστον 1 φορά στο Blockchain (confirmations > 0).
`unconfirmed_balance`	Unconfirmed Balance	Το σύνολο σε satoshi των μη εγκεκριμένων συναλλαγών (συναλλαγές που δεν έχουν μεταβεί σε κάποιο block). Η τιμή τους μπορεί να είναι αρνητική εφόσον η διεύθυνση στέλνει αποκλειστικά σε άλλες διευθύνσεις και δεν λαμβάνει satoshi.
`final_balance`	Total Balance	Το σύνολο σε satoshi όλων των συναλλαγών της διεύθυνσης (εγκεκριμένες και μη εγκεκριμένες συναλλαγές).

n_tx	Confirmed Transactions	Ο αριθμός των εγκεκριμένων συναλλαγών της διεύθυνσης.
unconfirmed_n_tx	Unconfirmed Transactions	Ο αριθμός των μη εγκεκριμένων συναλλαγών της διεύθυνσης.
final_n_tx	Total Transactions	Το σύνολο των συναλλαγών της διεύθυνσης (εγκεκριμένες και μη εγκεκριμένες συναλλαγές).
has_more	Has More	Η διεύθυνση διαθέτει πάνω από 50 συναλλαγές άρα θα πρέπει να πραγματοποιηθεί επιπλέον request προς το API.
prev_hash	Previous Hash	Το hash της συναλλαγής της οποία το output είναι το input της δεδομένης διεύθυνσης.
output_index	Output Hash	Ο αύξων αριθμός των outputs μιας συναλλαγής.
script	Script	Η κωδικοποίηση του script της συναλλαγής σε δεκαεξαδική μορφοποίηση.
script_type	Script type	Ο τύπος του script που έχει χρησιμοποιηθεί για την πραγματοποίηση της συναλλαγής
output_value	Total Spent	Το σύνολο σε satoshi που περιλαμβάνονται στην αποστολή κρυπτονομισμάτων.
sequence	Sequence	Ο αριθμός ακολουθίας 4 byte που σχετίζεται με συναλλαγές που έχουν “κλειδωθεί” λόγω επιβαρύνσεων.
addresses	Addresses	Ο πίνακας των διευθύνσεων που συμμετέχουν στη συναλλαγή.
age	Age of block	Ο αριθμός των εγκρίσεων που έχει λάβει η συναλλαγή από τη στιγμή που δημιουργήθηκε στο Blockchain.
value	Amount sent	Το σύνολο σε satoshi που έχει σταλεί μέσω της συγκεκριμένης συναλλαγής.
spent_by	Spent By	Το unique hash της συναλλαγής (αφορά μόνο εγκεκριμένες συναλλαγές).
block_hash	Block hash	Το unique hash του block στο οποίο συμπεριλαμβάνεται η συναλλαγή (αφορά μόνο εγκεκριμένες συναλλαγές).
block_height	Block height	Το ύψος του block το οποίο συμπεριλαμβάνει τη συναλλαγή (αφορά μόνο εγκεκριμένες συναλλαγές). Αντιπροσωπεύει τη χρονική στιγμή καταγραφής της.
block_index	Position in block	Ο αύξων αριθμός που προβάλει τη θέση της

		συναλλαγής το συγκεκριμένο block (αφορά μόνο εγκεκριμένες συναλλαγές).
hash	Transaction hash	Το unique hash της συναλλαγής (αφορά μόνο εγκεκριμένες συναλλαγές).
fees	Fees	Το σύνολο των φόρων που έχουν παρακρατηθεί, σε satoshi.
size	Raw size of block	Το μέγεθος της συναλλαγής σε bytes.
vsize	Raw size of block (vbytes)	Το μέγεθος της συναλλαγής σε virtual bytes.
preference	Preference	Η πιθανότητα της συναλλαγής ώστε να συμπεριληφθεί στο επόμενο block. Αντιπροσωπεύει κυρίως το αν οι miners θα την συμπεριλάβουν στις συναλλαγές τους. Παίρνει τις τιμές high, medium και low.
relayed_by	Address of the peer	Η διεύθυνση του Peer που έστειλε τη συναλλαγή.
confirmed	Time included	Η χρονική στιγμή κατά την οποία η συναλλαγή συμπεριλήφθηκε στο block (αφορά μόνο εγκεκριμένες συναλλαγές).
received	Time received	Η χρονική στιγμή κατά την οποία η συναλλαγή λήφθηκε από τους servers του BlockCypher.
ver	Version	Ο αριθμός έκδοσης της συναλλαγής. Ο αριθμός 1 συνήθως αφορά συναλλαγές του Blockchain (bitcoin συναλλαγές).
double_spend	Attempt to double spent transaction (fraud)	Προσπάθεια επανεκτέλεσης της συναλλαγής 2 φορές κατά την ίδια χρονική στιγμή. Αφορά περιπτώσεις όπου η συναλλαγή είναι προϊόν απάτης από αυτόν που την έχει εκτελέσει. Για την τιμή True το double_spend έχει επιτευχθεί, ενώ για false έχει απορριφθεί.
vin_sz	Total inputs	Το σύνολο των inputs της συναλλαγής.
vout_sz	Total outputs	Το σύνολο των outputs της συναλλαγής.
confirmations	Confirmations (subsequent blocks)	Ο αριθμός εγκρίσεων που έχει λάβει η συναλλαγή από γειτονικά blocks. (εάν πρόκειται για μη εγκεκριμένη συναλλαγή η επιστρεφόμενη τιμή είναι 0)
confidence	Likelihood for double spent	Η πιθανότητα για την εκτέλεση του “Attempt to double spent transaction”
lock_time	Time transaction locked	Η χρονική στιγμή κατά την οποία η συναλλαγή θεωρείται έγκυρη. Εάν η επιστρεφόμενη τιμή είναι μικρότερη από 500

		εκατομμύρια τότε αφορά το ύψος του block. Εάν είναι μεγαλύτερη, τότε αφορά τη Unix epoch time.

Πίνακας 6.1: Αντιστοίχιση κλειδιών του Blockcypher API με την εφαρμογή Tracksomware και περιγραφή τους
(Πηγές: **https://www.blockcypher.com/dev/bitcoin/**, **https://blockcypher.github.io/documentation/**)

6.3. Αρχιτεκτονική της εφαρμογής

Ο σκελετός της παρούσας υλοποίησης, βασίζεται στην ανάλυση του Blockchain με τη χρήση ελαχίστων πόρων. Οι πόροι αυτοί το καθιστούν ένα εργαλείο το οποίο μπορεί να εκμεταλλευτεί πηγές όπως το API του Blockchain και να αναλύσει εις βάθος, με χειροκίνητο τρόπο την κάθε συνδιαλλαγή σε αυτό για μια δεδομένη διεύθυνση.

Ο πυρήνας της εφαρμογής είναι γραμμένος στη γλώσσα προγραμματισμού PHP και χρησιμοποιεί κατά προσέγγιση το μοντέλο Model-View-Controller (MVC), ώστε να επεξεργαστεί και να παράξει δυναμικά δεδομένα μέσα από πληθώρα επαναλήψεων προς τρίτα μέρη όπως τα API των Blockcypher, AbuseIPDB και BitcoinAbuse, χωρίς να καταχραστεί το εκάστοτε δωρεάν πλάνο που αυτά παρέχουν.

Η αποστολή του κάθε request προς τον server γίνεται με τρόπο ασύγχρονο χρησιμοποιώντας τη μέθοδο AJAX (Asynchronous JavaScript and XML) και συγκεκριμένα για λόγους ευχρηστίας τη βιβλιοθήκη της jQuery (βιβλιοθήκη για τη γλώσσα προγραμματισμού JavaScript), ώστε να είναι εφικτό πολλαπλά requests να επιστρέψουν, με την ελάχιστη κατανάλωση υπολογιστικής ισχύος, τα δεδομένα στην οθόνη του αναλυτή.

Παράλληλα, η επεξεργασία των δεδομένων στην πλευρά του server αφορά τη μετάφραση συγκεκριμένων κλειδιών από το αντικείμενο που επιστρέφει το Blockchain, τη μετατροπή των Satoshis σε Bitcoins με τη χρήση αλγορίθμου, την εκμετάλλευση πολλαπλών iterations ώστε να παραχθεί ένα human readable αποτέλεσμα, έχοντας πάντα ως γνώμονα την καλύτερη επίδοση για το σύνολο του συστήματος (χρόνος απόκρισης, εκτύπωση αποτελεσμάτων, κ.α.).

Παρακάτω, παρατίθενται σημεία του πηγαίου κώδικα που αντιπροσωπεύουν όλα όσα αναφέρθηκαν σε αυτή την ενότητα:

```
class IpChecker
{
    function check($ipAddress)
    {
        $token = '5e68bXXXXXXXXXXXXXXXXXXXXX6a620c';

        $curl = curl_init();

        curl_setopt_array($curl, array(
```

```
        CURLOPT_URL => 'https://api.abuseipdb.com/api/v2/check?ipAddress=' .
$ipAddress,
        CURLOPT_RETURNTRANSFER => true,
        CURLOPT_ENCODING => '',
        CURLOPT_MAXREDIRS => 10,
        CURLOPT_TIMEOUT => 0,
        CURLOPT_FOLLOWLOCATION => true,
        CURLOPT_HTTP_VERSION => CURL_HTTP_VERSION_1_1,
        CURLOPT_CUSTOMREQUEST => 'GET',
        CURLOPT_HTTPHEADER => array(
            'Key: ' . $token,
            'Accept: application/json',
        ),
        ));
        $response = curl_exec($curl);

        curl_close($curl);

        return $response;
    }
}
```

Εικ. 6.17: Συνάρτηση για την επικοινωνία με το API της υπηρεσίας AbuseIPDB
(Πηγή: Tracksomware Web Application)

```
// Convert satoshi units to bitcoin
public function satoshiToBtc($value, $flag = false)
{
    if($flag)
    {
        return number_format(($value * pow(10,-8)),8);
    }
    else
    {
        return number_format(($value * pow(10,-8)),8) . ' ฿';
    }
}
```

Εικ. 6.18: Συνάρτηση για τη μετατροπή από Satoshi σε Bitcoin
(Πηγή: Tracksomware Web Application)

```
if(isset($_POST['hash']) && $_POST['hash'] !== null)
{
   $address = htmlspecialchars(strip_tags($_POST['hash']), ENT_QUOTES);
   $type = (int) htmlspecialchars(strip_tags($_POST['type']), ENT_QUOTES);
   $report = (int) htmlspecialchars(strip_tags($_POST['report']),
ENT_QUOTES);

   //Get totals from single address (i.e. 198QL1JZZnbAMKsrUg8oseSZxMNdqzJN4u)
   if($type == 4)
   {
      $fullAddress = $api->getFullAddress($address, array("limit" => 50,
"omitWalletAddresses" => true));
      echo $blockchain->addressWithTxInfo($fullAddress, $report);
    }
    else
    {
      $balanceObj = $api->getBalance($address);
      echo $blockchain->addressInfo($balanceObj, $type, $report);
    }
}
elseif(isset($_POST['ipCheck']) && is_numeric($_POST['ipCheck']) == 1)
{
    $ipAddress = htmlspecialchars(strip_tags($_POST['ip']), ENT_QUOTES);
    echo $ipChecker->check($ipAddress);
}
else
{ die(); }
```

Εικ. 6.19: Επαλήθευση τιμών μετά από ασύγχρονο request και επιλογή τύπου αναζήτησης
(Πηγή: Tracksomware Web Application)

```
$.ajax({
         url: url,
         method:"POST",
         data:{
             hash: hash,
             type: type,
             report: report
         },
         success:function(data)
         {
```

```
            $("#btc-results-loader").addClass('d-none');
            $("#btc-results-container").removeClass('d-none');
            document.getElementById('btc-results').innerHTML = data;
        }
    });
```

Εικ. 6.20: Ασύγχρονο αίτημα προς το server με hash και τύπο αναζήτησης
(Πηγή: Tracksomware Web Application)

6.4. Ενσωμάτωση του Blockchain API στην πλατφόρμα

Η ενσωμάτωση του Blockchain API έγινε με τη χρήση ενός middleware και για την ακρίβεια με τη χρήση του τρίτου μέρους Blockcypher, όπως έχει προαναφερθεί και σε προηγούμενα κεφάλαια της παρούσας μεταπτυχιακής διατριβής. Ο λόγος για τον οποίο έχει γίνει αυτό, είναι γιατί από το 2018 το Blockchain.com δεν παράγει άλλα κλειδιά προς την development κοινότητα.

Από τους ίδιους τους δημιουργούς του Blockchain.com δεν υπάρχει κάποια εξήγηση, συνεπώς το πρόβλημα ανάλυσης του Blockchain έπρεπε να γίνει είτε τοπικά με ανανέωση της αλυσίδας ανά τακτά χρονικά διαστήματα, ή με την εκμετάλλευση μιας τρίτης υπηρεσίας η οποία εκμεταλλεύεται ήδη ένα κλειδί για το RESTful API του Blockchain και λειτουργεί ως middleware, προσφέροντας παράλληλα και δικές της υπηρεσίες ανάλυσης, κυρίως για τη δημιουργία Wallet, για την αποστολή κρυπτονομίσματος και για την λήψη πληροφοριών για το address ενός χρήστη.

Από τεχνικής πλευράς, όπως φαίνεται και στην εικόνα 6.17, όλα τα request προς το API του Blockchain έχουν γίνει με τις μεθόδους GET και POST, με υλοποίηση στη γλώσσα προγραμματισμού PHP, αφού όλη διαδικασία επικοινωνίας γίνεται στην πλευρά του server.

6.5. Δυναμική ανάλυση και περιορισμοί χρήσης

Κατά τη φάση υλοποίησης της εφαρμογής “Tracksomware” εμφανίστηκαν ανάγκες προς υλοποίηση, με βάση τα ερωτήματα που θα έκανε ένας αναλυτής στην αλυσίδα του Blockchain. Ενώ αρκετές λειτουργικότητες του λογισμικού καλύπτουν τις ανάγκες ενος αναλυτή, υπάρχουν και άλλες οι οποίες λόγω βασικών περιορισμών δεν δύναται να υλοποιηθούν, τουλάχιστον στην 1η έκδοσή του.

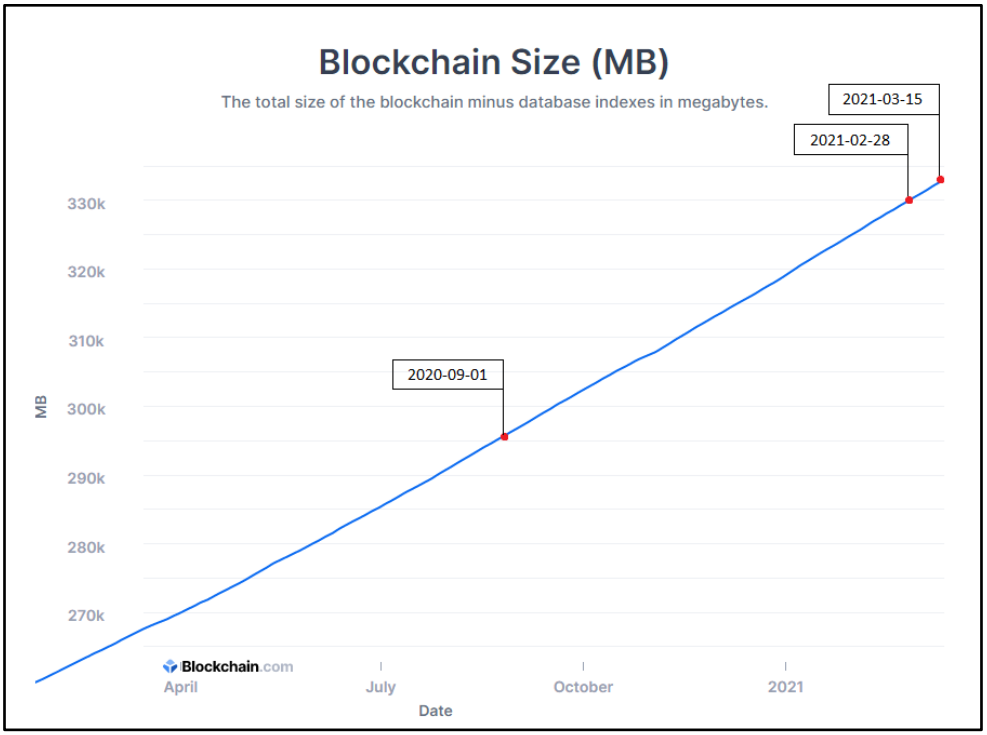
Οι ανάγκες καθώς και οι περιορισμοί που κρύβονται πίσω από αυτές παρατίθενται παρακάτω αναλυτικά.

6.5.1 Στιγμιαία ανανέωση της αλυσίδας του Blockchain

Κάθε δευτερόλεπτο που περνάει, η αλυσίδα του blockchain μεγαλώνει ολοένα και περισσότερο, με την προσθήκη χιλιάδων συναλλαγών. Είναι λογικό λοιπόν να υποθέσει κάποιος, πως για να

ανατρέξει σε όλη την αλυσίδα με την ίδια χρονική απόκριση θα πρέπει αποθηκεύσει όλο το Blockchain τοπικά και εν συνεχεία να ενημερώνει αυτή την “αποθήκη δεδομένων” με τις νέες συναλλαγές που πραγματοποιούνται.

Δυστυχώς, η αποθήκευση της συνολικής αλυσίδας σε τοπικό μέσο και machine readable format, απαιτεί τη χρήση δίσκου ή workstation με μέγεθος > **326.6GB** (το μέγεθος αφορά τη χρονική στιγμή συγγραφής της παρούσας μεταπτυχιακής διατριβής) καθώς μεγαλώνει εκθετικά προς το χρόνο. Ενδεικτικά, κατά τη χρονική περίοδο Σεπτέμβριος 2020 - Φεβρουάριος 2021, η αύξηση της αλυσίδας ήταν **~35GB**.



Εικ. 6.21: Συνολικό μέγεθος της αλυσίδας του Blockchain και σύγκριση περιόδου Σεπτέμβριος 2020 - Φεβρουάριος 2021
(Πηγή: **https://www.blockchain.com/charts/blocks-size**)

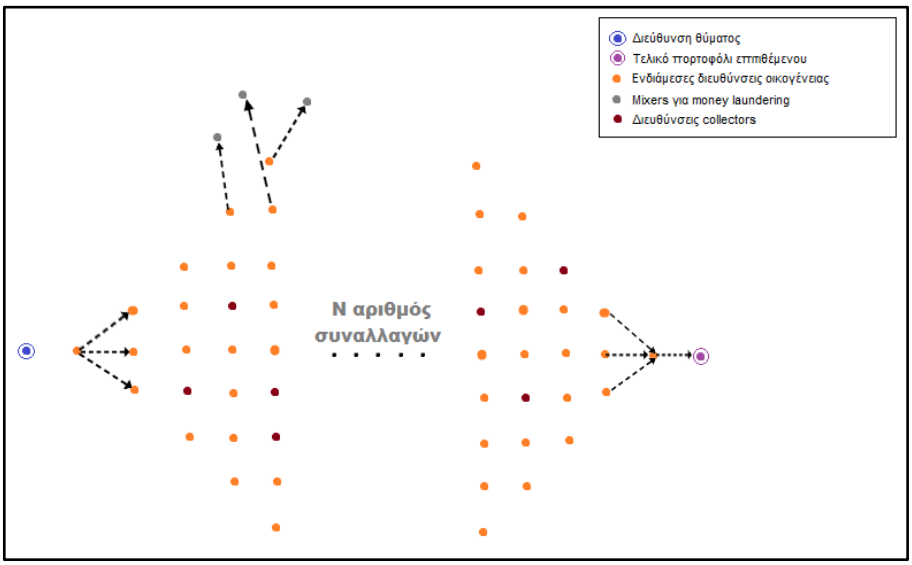
Αυτός ο περιορισμός, μπορεί να επιλυθεί με τη χρήση του Blockchain API το οποίο εξέδωσε τα τελευταία λειτουργικά κλειδιά εντός του έτους 2018. Από τότε μέχρι και σήμερα, παρόλο που η διαδικασία λήψης κλειδιού παραμένει ενεργή, το κλειδί δεν παράγετα. Αυτό το λειτουργικό πρόβλημα δημιουργεί έναν εσωτερικό περιορισμό, ο οποίος αναγκάζει τον εκάστοτε αναλυτή, να προβεί στη χρήση υπηρεσιών ενός τρίτου μέρους, όπως το Blockcypher, το οποίο με τη σειρά του είτε διατηρεί και ανανεώνει τοπικά την αλυσίδα του Blockchain, είτε εκμεταλλεύεται ένα από τα ενεργά κλειδιά του πρωτότυπου API που παράχθηκε πριν το 2018.

Σε αυτήν την περίπτωση, ο αναλυτής είναι αναγκασμένος να περιοριστεί στις τιμές που καθορίζει το τρίτο μέρος για την απόκτηση και χρήση ενός κλειδιού, ενώ αν επιλέξει να ακολουθήσει ένα δωρεάν πακέτο, θα συναντήσει πληθώρα περιορισμών όπως το όριο από requests που μπορεί να εκτελέσει ανα προκαθορισμένη χρονική στιγμή (δευτερόλεπτο, λεπτό, ώρα, ημέρα), όπως και το σύνολο των αποτελεσμάτων που θα του επιστραφούν, π.χ. έως 50 transactions ανά address.

Ως συμπέρασμα, η έλλειψη οικονομικών πόρων για την αποθήκευση της αλυσίδας ή για τη διατήρηση ενός υψηλού πακέτου αναζητήσεων από ένα τρίτο μέρος, οδηγούν στη χειροκίνητη και όχι δυναμική φύση λειτουργίας της εφαρμογής.

6.5.2 Αδυναμία δημιουργίας αυτοματοποιημένης δενδρικής αναζήτησης

Μία από τις βασικές λειτουργικότητες του Tracksomware, είναι η δυνατότητα που δίνει στον αναλυτή να εκτελέσει μια εκ νέου αναζήτηση για μια από τις διευθύνσεις που εντόπισε στα αποτελέσματα των Outputs. Εκμεταλλεύοντας αυτή τη λειτουργικότητα, ο αναλυτής μπορεί να προχωρήσει σε εις βάθος ανάλυση μιας ακολουθίας συναλλαγών, να συλλέξει και αποθηκεύσει δεδομένα αλλά και να εξάγει τα δικά του συμπεράσματα σύμφωνα με το Input ή το μονοπάτι που έχει επιλέξει. Τι συμβαίνει όμως εάν πρέπει να αναζητήσει χιλιάδες συναλλαγές μέσα από μία ακολουθία;



Εικ. 6.22: Αναπαράσταση δενδρικής αναζήτησης εντός του Blockchain

Η υποδομή της εφαρμογής, διαθέτει τη δυνατότητα επέκτασής της ώστε μετά το πρώτο input του χρήστη (π.χ. address θύματος) να εκτελέσει πολλαπλές αναζητήσεις για κάθε ένα από τα Inputs & Outputs που θα παραχθούν, δημιουργώντας έτσι μια δενδρική αναζήτηση, όπως φαίνεται και στην εικόνα 6.22, η οποία θα καταλήξει στο τελικό πορτοφόλι από το οποίο έγινε η εξαργύρωση ή/και η μεταπήδηση σε άλλο κρυπτονόμισμα.

Για να υλοποιηθεί όμως αυτή η λειτουργικότητα, η έλλειψη υπολογιστικής ισχύος για την αναπαραγωγή όλων αυτών των αναζητήσεων σε συνδυασμό με τον περιορισμό που αναφέρθηκε στην ενότητα 6.4.1 με βάση το κόστος ενός API, οδηγούν στον αποκλεισμό της. Πρόκειται λοιπόν, για μια σχέση κόστους και εξοπλισμού η οποία δεν δύναται να συγκριθεί με μελετητές όπως αυτή των Elie Bursztein, Luca Invernizzi, Kylie McRoberts και άλλοι, που δρουν με εργαστηριακούς πόρους από το Πανεπιστήμιο του Πρίνστον (Princeton University), το Πανεπιστήμιο της Νέας Υόρκης (New York University), το Πανεπιστήμιο της Καλιφόρνια, Σαν Ντιέγκο (University of California, San Diego), την Google Inc. και την Chainalysis Inc. [49]

6.5.3 Αδυναμία αναζήτησης με δεδομένη χρονική στιγμή

Είναι λογικο κατά την αναζήτηση στοιχείων εντός της αλυσίδας, να προκύψει η ανάγκη για αναζήτηση με βάση μια συγκεκριμένη ημερομηνία και όχι απαραίτητα με βάση μια διεύθυνση του Blockchain. Για παράδειγμα, θα μπορούσε ο αναλυτής να αναζητήσει όλα τα transactions που έχουν πραγματοποιηθεί σε μια δεδομένη χρονική στιγμή εφόσον γνωρίζει ότι σε εκείνη την περίοδο έχει πραγματοποιηθεί ένα ransomware campaign.

Εκ φύσεώς του το Blockchain, δεν χρησιμοποιεί το χρόνο ως timestamp για μια ενέργεια που συμβαίνει εντός του, αλλά το ύψος. Μπορεί μια συναλλαγή που ανήκει σε ένα block να έχει αποθηκευμένη την ημερομηνία που πραγματοποιήθηκε, αλλά η αμέσως επόμενη συναλλαγή μπορεί να έχει ελαφρώς διαφορετική ημερομηνία. Γι'αυτόν τον λόγο, το Blockchain καταγράφει το ύψος ενός block ως σημείο αναφοράς του στην κλίμακα του χρόνου.

Για να μπορέσει λοιπόν η εφαρμογή να αναζητήσει δεδομένα με βάση μια ημερομηνία, θα πρέπει από το σημείο γέννησης του Blockchain, όπου height = 0, να χαρτογραφίσει κάθε ύψος της αλυσίδας με τις ημερομηνίες που εμπεριέχονται στα transactions αυτού του block. Αυτό σημαίνει πως θα υπάρχει απόκλιση αναλόγως με τη χρονική στιγμή που αναζητά ο αναλυτής όπως επίσης και περιορισμοί στην αναζήτηση με βάση το εύρος χρονικών στιγμών.

Ως αποτέλεσμα, η συγκεκριμένη λειτουργικότητα δεν μπορεί να επιστρέψει προσεγγιστικά δεδομένα, παρά μόνο εάν γίνει παράλληλη χαρτογράφηση όλων των transactions με βάση την ημερομηνία τους, κάτι που επαναφέρει τους περιορισμούς της εφαρμογής σε αυτούς των ενοτήτων 6.5.1 και 6.5.2.

6.5.4 Αδυναμία αναζήτησης με δεδομένη τιμή φυσικού συναλλάγματος

Άλλη μία παράμετρος που έχει εξεταστεί ως προς την λεπτομερή αναζήτηση εντός της αλυσίδας του Blockchain, είναι η χρήση ενός πεδίου στο οποίο αντί για το address ενός επιτιθέμενου, ο αναλυτής θα έχει τη δυνατότητα να αναζητήσει για addresses, wallets ή transactions με βάση την τιμή των λύτρων σε φυσικό νόμισμα. Για να τεθεί σε λειτουργία η συγκεκριμένη αναζήτηση, θα πρέπει συνδυαστικά να θεωρηθεί λειτουργική και η παράμετρος αναζήτησης με βάση το χρόνο.

Εάν για παράδειγμα ο αναλυτής θέλει να αναζητήσει για όλες τις συναλλαγές που κατατέθηκαν σε wallets στο διάστημα 1η έως 15η Ιανουαρίου του 2020 και το ποσό που κατατέθηκε είναι τα 300 €, θα πρέπει με τη βοήθεια ενός Currency API να υπολογιστεί η αναλογία μεταξύ Ευρώ και Δολαρίου και στη συνέχεια η αναλογία μεταξύ Δολαρίου και Bitcoin.

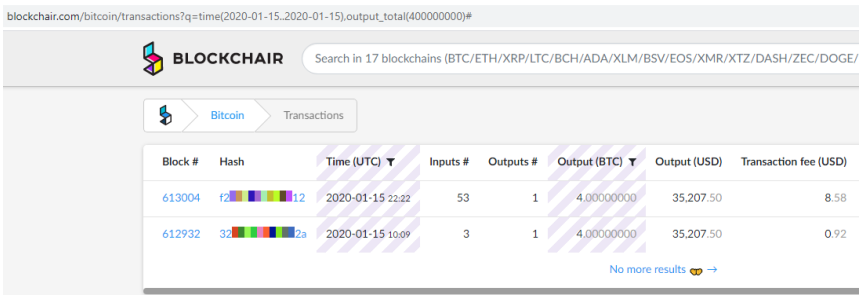
Παρόλο που η χρήση ενός τέτοιου API είναι δυνατή, τα δεδομένα που επιστρέφονται έχουν μεγάλη απόκλιση από τις πραγματικές συναλλαγές. Αυτό συμβαίνει για τους παρακάτω λόγους:

1. Τα currency APIs επιστρέφουν την τιμή του συναλλάγματος για τη δεδομένη ημέρα αλλά για συγκεκριμένη χρονική στιγμή και όχι σε ανάλυση εντός 24ώρου.
2. Η συναλλαγή εκτελείται με ακρίβεια microtime (χρησιμοποιείται το Unix epoch), συνεπώς μια μη προσεγγιστική τιμή δεν θα επιστρέψει σωστά δεδομένα
3. Ακόμα και στην περίπτωση που το currency API επιστρέψει την ίδια ημερομηνία και ώρα με αυτή μιας συναλλαγής, η δεδομένη τιμή σε ευρώ θα πολλαπλασιαστεί με την

τιμή του συναλλάγματος, η οποία έχει ακρίβεια τριών ή τεσσάρων δεκαδικών ψηφίων και στη συνέχεια θα πρέπει να υπολογιστεί η τιμή των Bitcoins σε Satoshis όπου υπάρχει ακρίβεια 8 δεκαδικών ψηφίων. Ακόμα και σε αυτή την περίπτωση, η πιθανότητα να πετύχει κάποιος την ακριβή τιμή της συναλλαγής είναι πολύ χαμηλή.

Η απόδειξη για τη μη εγκυρότητα των τιμών είναι απλή:

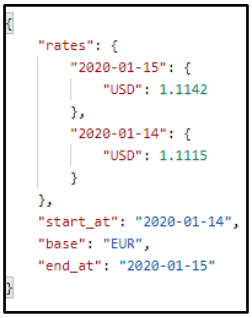
Έστω ότι ο αναλυτής θέλει να βρει συναλλαγές που να θυμίζουν πληρωμές σε οικογένειες ransomware για την ημερομηνία **2020-01-15** όπως φαίνεται και στην παρακάτω εικόνα:



Εικ. 6.23: Αποτελέσματα αναζήτησης με βάση την ημερομηνία και το ποσό των 4BTC
(Πηγή: **https://blockchair.com/bitcoin/transactions**)

Στο συγκεκριμένο παράδειγμα, το ζητούμενο είναι το ποσό που πρέπει να εισάγει ο αναλυτής ώστε να προσεγγίσει τις παραπάνω συναλλαγές εντός του Blockchain. Για να εντοπίσει αυτή την πληρωμή των 4BTC θα πρέπει να αντιστραφεί η διαδικασία και να γίνει ως εξής:

Πρώτο βήμα είναι ο υπολογισμός συναλλάγματος μεταξύ EUR και USD ο οποίος προκύπτει από ένα request στο δωρεάν API του https://api.exchangeratesapi.io. Το αποτέλεσμα φαίνεται στην εικόνα 6.24:

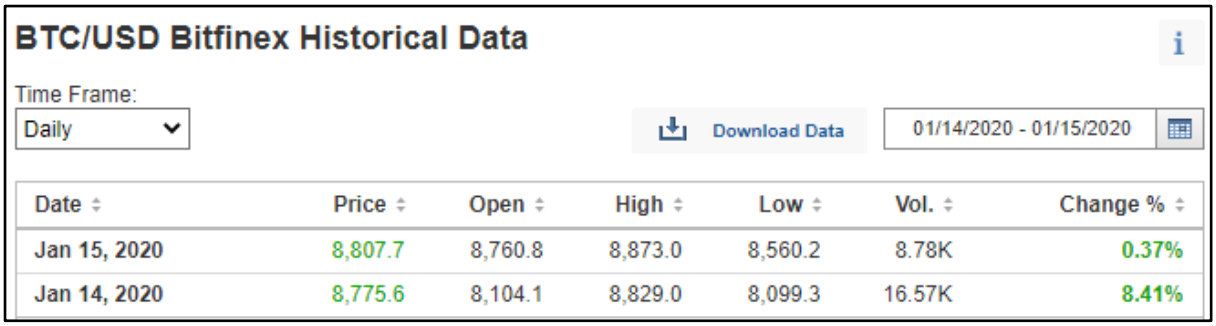


Εικ. 6.24: Αναλογία συναλλάγματος μεταξύ EUR/USD σύμφωνα με τον ιστότοπο **exchangerates**
(Πηγή: **https://exchangeratesapi.io/**)

Εάν ο αναλυτής εισάγει μια στρογγυλοποιημένη τιμή όπως **30.000,00 €** τότε η μετατροπή θα γίνει ως εξής (όπου L, το αποτέλεσμα της μετατροπής):

$$L = 1.1142 \times 30000 = 33.426{,}00 \text{ USD}$$

Στη συνέχεια θα πρέπει να εντοπιστεί η αναλογία BTC/USD για την παραπάνω ημερομηνία η οποία είναι **1 BTC = 8.807.70 USD** και φαίνεται στην εικόνα 6.25.



BTC/USD Bitfinex Historical Data

Time Frame: Daily | Download Data | 01/14/2020 - 01/15/2020

Date	Price	Open	High	Low	Vol.	Change %
Jan 15, 2020	8,807.7	8,760.8	8,873.0	8,560.2	8.78K	0.37%
Jan 14, 2020	8,775.6	8,104.1	8,829.0	8,099.3	16.57K	8.41%

Εικ. 6.25: Αναλογία BTC/USD για τις ημέρες 14 & 15 Ιανουαρίου 2020
(Πηγή: **https://www.investing.com/crypto/bitcoin/btc-usd-historical-data**)

Για να βρεθεί στο τελικό βήμα το input του αναλυτή θα πρέπει να πραγματοποιηθεί η ακόλουθη πράξη (όπου J, το πραγματικό input του χρήστη):

J = 33.426 / 8.807,70 = 3.795088388569092952757246500221 4 BTC

Όπως φαίνεται και στον υπολογισμό για το input του χρήστη, δεν υπάρχει προσέγγιση με το πραγματικό αποτέλεσμα. Για να είχε θετική έκβαση η παραπάνω αναζήτηση θα έπρεπε ο χρήστης να εισάγει το ποσό των **Z = 4BTC x 8.807,70 = 35.230,80 USD** ή αλλιώς **~31.619,82 EUR**.

Φυσικά, είναι άξιο αναφοράς, πως ακόμα και η μετατροπή συναλλάγματος από Ευρώ σε Δολάριο και Δολάριο σε Bitcoins για παρελθοντικούς χρόνους παραμένει προσεγγιστική, καθώς η ίδια η τιμή του συναλλάγματος προκύπτει από το κλείσιμο του χρηματιστηρίου. Αυτό σημαίνει πως σε ένα ακριβές, ως προς το χρόνο, σενάριο η τιμή του συναλλάγματος που θα υπολογιστεί μέσω ενός εξωγενούς service μπορεί να έχει απόκλιση από την πραγματική τιμή, σύμφωνα πάντα με την ακριβή τιμή συναλλάγματος κατά τη χρονική στιγμή της συναλλαγής.

ΚΕΦΑΛΑΙΟ 7ο: Αντιμετώπιση επίθεσης

Βασική προϋπόθεση για την ορθή και ασφαλή λειτουργία ενός οργανισμού, είναι η λήψη των κατάλληλων μέτρων για την αποφυγή οποιουδήποτε κινδύνου. Είναι άκρως σημαντικό, να ενσωματώνονται όλα τα πιθανά αντίμετρα ενός κινδύνου από την αρχή της δημιουργίας του οργανισμού (Security by default & by design) [51], αλλά και να γίνονται τακτικοί έλεγχοι, σύμφωνα πάντα με το εκάστοτε πλάνο που διατηρεί ο οργανισμός, ώστε να ελέγχεται και να επιβεβαιώνεται η ορθή χρήση αυτών των αντίμετρων.

7.1. Υπολογισμός κινδύνου για τη βιωσιμότητα του εκάστοτε οργανισμού

Ένας τρόπος για τη μέτρηση του κινδύνου σε συνολικό ή τμηματικό επίπεδο στον οργανισμό, είναι η κατανομή του σε τμήματα και κατ'επέκταση η κατανομή των τμημάτων σε αγαθά, τα οποία με βάσει τις παροχές τους βαθμολογούνται ως προς την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα τους σε επίπεδο ασφάλειας.

Ο τρόπος κατανομής και βαθμολόγησης αυτών των αγαθών ονομάζεται "Μελέτη Ανάλυσης και Διαχείρισης Επικινδυνότητας" και προκύπτει από μεθοδολογίες που έχουν ορίσει παγκόσμιοι φορείς, ώστε να πληροί ο οργανισμός τα κριτήρια που ορίζει ένα πρότυπο ασφάλειας, σύμφωνα με τις ανάγκες του. Συμπληρωματικά, η κάθε δεδομένη μεθοδολογία μπορεί να τροποποιηθεί (δημιουργία υβριδικής μεθοδολογίας) ώστε να εφάπτεται αποκλειστικά στο συγκεκριμένο οργανισμό, ή να δημιουργηθεί εξ ολοκλήρου για αυτόν.

Κάποιες από τις γνωστές μεθοδολογίες για τη μελέτη ανάλυσης και διαχείρισης επικινδυνότητας αποτελούν οι CRAMM [52] από τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA), PRAM [53][54] από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST), κ.α.

Η συγκεκριμένη μελέτη θα πρέπει να αποτελείται από τα εξής βήματα:

- Περιγραφή της μεθοδολογίας
- Περιγραφή του Οργανισμού που εφάπτεται η παραπάνω μεθοδολογία
- Απαιτήσεις ασφάλειας - νομικές απαιτήσεις
- Χαρτογράφηση αγαθών
- Αποτίμηση επιπτώσεων
- Αποτίμηση απειλών
- Αποτίμηση αδυναμιών
- Αποτίμηση κινδύνων
- Προτεινόμενα μέτρα προστασίας
- Σχέδιο υλοποίησης μέτρων προστασίας

Αποτέλεσμα της παραπάνω ανάλυσης είναι η βαθμολόγηση όλων των αγαθών ενός οργανισμού, η οποία αποκαλύπτει τα κενά ασφάλειας αλλά και την προτεραιότητα που πρέπει να δοθεί σε αυτά από τον οργανισμό. Εφόσον τα συγκεκριμένα κενά ασφαλείας μπορούν να καλυφθούν από τον ίδιο τον οργανισμό, τότε μπορεί να θεωρηθεί πως ο πιθανός κίνδυνος έχει ελαχιστοποιηθεί. Στις περιπτώσεις επίθεσης από Ransomware Campaigns συνήθεις ευπάθειες

βρίσκονται εντός του εσωτερικού δικτύου ενός οργανισμού όπως για παράδειγμα η μη χρήση ενός τείχους προστασίας, η ανεξέλεγκτη εγκατάσταση προγραμμάτων από τους χρήστες του οργανισμού, η ανεπαρκής ενημέρωση των χρηστών για τους πιθανούς τρόπους μόλυνσής τους όπως Phishing emails, εκτέλεση συνημμένων, κ.α.

7.2. Γνωστοποίηση επίθεσης

Η χρονική στιγμή σύμφωνα με την οποία αναγνωρίζεται μια επίθεση, αποτελεί το σημείο μηδέν για τον οργανισμό όσον αφορά την αντιμετώπισή της. Θα πρέπει λοιπόν, να γνωστοποιηθεί η επίθεση στο αρμόδιο τμήμα του οργανισμού ώστε να ληφθούν έγκαιρα τα κατάλληλα μέτρα.

Στις περιπτώσεις ειδικά των Ransomware Campaigns, όπου η πιθανότητα μόλυνσης ενός ολόκληρου εσωτερικού δικτύου από έναν και μόνο χρήστη είναι υψηλές, η γνωστοποίηση του κινδύνου είναι ένας κρίσιμος παράγοντας για την αποφυγή όσο το δυνατόν περισσότερων καταστροφών.

Από τη στιγμή της γνωστοποίησης, θα πρέπει ο οργανισμός να πράξει αναλόγως και να προσπαθήσει να απομονώσει τον κίνδυνο ή/και να τον εξαλείψει. Για να επιτευχθεί αυτό χρειάζεται η γνωστοποίηση να επεκταθεί και στις αρμόδιες αρχές όπως το τμήμα Δίωξης Ηλεκτρονικού Εγκλήματος ή σε οποιονδήποτε άλλο αρμόδιο φορέα που ορίζεται από τον εκάστοτε κρατικό μηχανισμό και νομοθεσία.

Φυσικά, δεν πρέπει η επίθεση να διαδίδεται στον οποιονδήποτε τρίτο, παρά μόνο σε όσους επηρεάζονται άμεσα από αυτή. Αυτό συμβαίνει καθώς πρέπει να αποφεύγεται ο πανικός αλλά και η πιθανότητα ενημέρωσης του επιτιθέμενου έμμεσα. Μετά το πέρας του κινδύνου και την εξάλειψη αυτού, μπορεί ο οργανισμός να ανακοινώσει το συμβάν εφόσον αυτό κρίνεται αναγκαίο από τη διοίκηση και τη νομική του υπηρεσία.

7.3. Προσπάθεια εξάλειψης ευπαθειών

Οι ευπάθειες που προκύπτουν εντός των συστημάτων ενός οργανισμού μετά τη “Μελέτη Ανάλυσης και Διαχείρισης Επικινδυνότητας”, όπως αναφέρθηκε και στην υποενότητα 7.1., θα πρέπει να εξαλειφθούν.

Για να επιτευχθεί η εξάλειψη μιας ευπάθειας θα πρέπει ο οργανισμός να επενδύσει είτε σε υλικοτεχνικό εξοπλισμό όπου θα ενισχύσει τα επίπεδα ασφάλειας των πληροφοριακών συστημάτων του, είτε σε ανθρώπινο δυναμικό όπου θα προσλάβει άτομα ικανά για την κατάλληλη ρύθμιση της λειτουργίας των συστημάτων του από μη ασφαλή σε ασφαλή.

Η εξάλειψη των ευπαθειών, είναι μια διαδικασία που δεν επηρεάζει μόνο τη χρονική στιγμή αναγνώρισής της. Αντιθέτως, επηρεάζει τον οργανισμό σε βάθος χρόνου καθώς πέρα από την εξάλειψη μιας ευπάθειας για τη δεδομένη χρονική στιγμή, θα πρέπει να ελέγχεται τακτικά από τον οργανισμό η μη επανεμφάνισή της ή τουλάχιστον η αποδοχή του ρίσκου από αυτή την ευπάθεια όσο παραμένει σε χαμηλά, για τον οργανισμό, επίπεδα. Για το λόγο αυτό, κάθε οργανισμός θα πρέπει να ορίζει κάποιες πολιτικές ανά κατηγορία πληροφοριακών

συστημάτων, οι οποίες θα πρέπει να τηρούνται ώστε να εξασφαλίζεται η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα των πληροφοριών εντός του οργανισμού.

Ενδεικτικά παραδείγματα πολιτικών ασφαλείας είναι τα παρακάτω:

Πολιτικές Ασφαλείας	**Περιγραφή**
Πολιτική Κρυπτογράφησης	Θα πρέπει όλες οι επικοινωνίες του οργανισμού καθώς και τα δεδομένα που μεταφέρονται μέσω αυτών να κρυπτογραφούνται τόσο κατά τη μετάδοση όσο και κατά την αποθήκευση και διατήρησή τους. Η μέθοδος κρυπτογράφησης θα πρέπει να γίνεται με τη χρήση ενός αλγορίθμου υψηλής πολυπλοκότητας για την αποφυγή αποκρυπτογράφησης των επικοινωνιών με τη χρήση εργαλείων.
Πολιτική Ελέγχου	Θα πρέπει σε τακτικά διαστήματα, ο οργανισμός να επανεκτελεί την μελέτη ανάλυσης και διαχείρισης επικινδυνότητας ώστε να εντοπίζονται άμεσα πιθανές ευπάθειες.
Πολιτική Δικτύου DMZ	Θα πρέπει ομάδες χρηστών ή επισκέπτες του οργανισμού να έχουν πρόσβαση σε σημεία του δικτύου και όχι σε ολόκληρο το δίκτυο για την αποφυγή διαρροής πληροφοριών σε μη εξουσιοδοτημένους χρήστες. Ένας από τους τρόπους επίτευξης του συγκεκριμένου πλάνου είναι η χρήση ενός DMZ δικτύου (Demilitarized Zone Network), το οποίο απομονώνει τους χρήστες του σε συγκεκριμένα επίπεδα πρόσβασης εντός του συνολικού δικτύου.
Πολιτική Λογαριασμών Ηλεκτρονικού Ταχυδρομείου	Θα πρέπει η πρόσβαση στους ηλεκτρονικούς λογαριασμούς των χρηστών να γίνεται με τον τρόπο που έχει ορίσει το τμήμα πληροφορικής του οργανισμού. Για την χρήση προγραμμάτων ανάγνωσης, αποθήκευσης και αποστολής ηλεκτρονικών μηνυμάτων θα πρέπει να χρησιμοποιούνται μόνο έμπιστα, κατά τον οργανισμό, λογισμικά.
Πολιτική Φύλαξης Δεδομένων	Θα πρέπει όλα τα δεδομένα που συλλέγει ο οργανισμός να φυλάσσονται και να παραμένουν στις υποδομές του για ορισμένο χρονικό διάστημα. Το χρονικό διάστημα αυτό, ορίζεται είτε από τις ανάγκες του οργανισμού είτε από την εκάστοτε ισχύουσα νομοθεσία.
Πολιτική Κωδικών Πρόσβασης	Θα πρέπει οι κωδικοί πρόσβασης των χρηστών ενός οργανισμού να πληρούν τα πρότυπα που έχει ορίσει ο οργανισμός. Για παράδειγμα, το μήκος ενός κωδικού πρόσβασης θα πρέπει να είναι 10 χαρακτήρες ενώ θα πρέπει να αποτελείται τουλάχιστον από 1 κεφαλαίο χαρακτήρα του αλφάβητου, 1 μικρό χαρακτήρα του αλφάβητου, 1 αριθμό και 1 σύμβολο. Συμπληρωματικά, ο κωδικός πρόσβασης ενός χρήστη θα πρέπει να αλλάζει κάθε δύο μήνες ενώ δεν θα υπάρχει η δυνατότητα χρήσης των τελευταίων 3 κωδικών που έχουν ήδη χρησιμοποιηθεί.
Πολιτική Αντιγράφων Ασφαλείας	Θα πρέπει ο οργανισμός να διατηρεί μηχανισμούς δημιουργίας αντιγράφων ασφαλείας ώστε να διασφαλίσει την

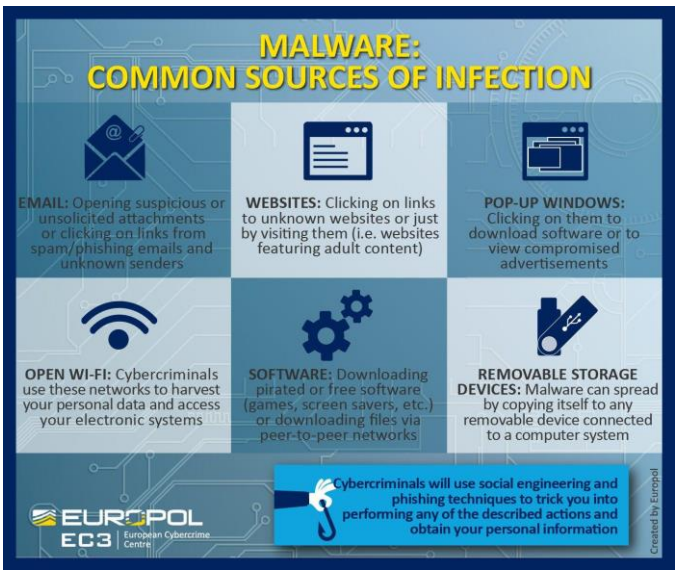
	πληροφορία που αποθηκεύεται σε θέσεις δικτύου, βάσεις δεδομένων, κλπ. Ο τρόπος δημιουργίας των αντιγράφων μπορεί να γίνεται με τη μεθοδολογία Grandfather - Father - Son [55]
Πολιτική Απομακρυσμένης Πρόσβασης	Θα πρέπει η διασύνδεση στα συστήματα και το δίκτυο του οργανισμού απομακρυσμένα, να γίνεται με τη χρήση μόνο έμπιστων, κατά τον οργανισμό, προγραμμάτων και μόνο από συσκευές που έχει χορηγήσει ο οργανισμός στον εκάστοτε χρήστη. Οποιαδήποτε άλλη προσπάθεια απομακρυσμένης πρόσβασης θα πρέπει να καταγράφεται και να αποκλείεται.

Πίνακας 7.1: Παραδείγματα πολιτικών ασφαλείας

7.4. Ενημέρωση προσωπικού

Αρκετές από τις φορές όπου ένα Malware Campaign επιτυγχάνει το στόχο του, οφείλονται στην μη επαρκή ενημέρωση ενός χρήστη (user security awareness) για τον τρόπο λειτουργίας και συμπεριφοράς στο εκάστοτε δίκτυο.

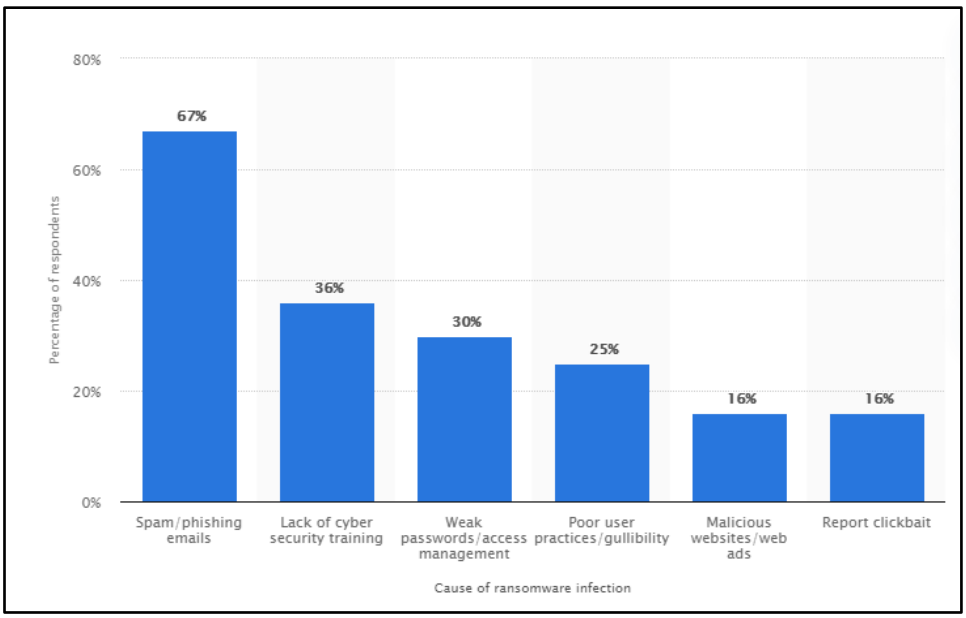
Δεν είναι λίγες οι φορές όπου υπάλληλος ενός οργανισμού έχει ανοίξει κάποιο ηλεκτρονικό μήνυμα με κακόβουλο περιεχόμενο ή έχει εισάγει στην εταιρική του συσκευή κάποιο μέσο αποθήκευσης που βρήκε στο δρόμο, όπως ένα USB stick, και άθελά του έχει μεταφέρει το κακόβουλο λογισμικό εντός ολόκληρου του δικτύου ή σε μέρος αυτού.



Εικ. 7.1: Γνωστοί τρόποι διάδοσης ενός Malware
(Πηγή: **https://twitter.com/europol/status/717375303161679872?lang=en**)

Ειδικά στις περιπτώσεις των Ransomware Campaigns, οι παραπάνω τρόποι μόλυνσης του οργανισμού είναι και αυτοί που ευθύνονται στην πληρώρα των περιπτώσεων. Όπως φαίνεται και παρακάτω στην εικόνα 7.2, ως μέσα για τους πιο γνωστούς τρόπους διάδοσης ενός Ransomware είναι τα Phishing Emails, η ελλιπής ενημέρωση των χρηστών για θέματα

ασφάλειας, η χρήση αδύναμων κωδικών πρόσβασης, η έλλειψη διαχείρισης της πρόσβασης των χρηστών σε επίπεδα, και η ανεπαρκής εκπαίδευση των χρηστών ως προς την αναγνώριση ενός πιθανού malware.



Εικ. 7.2: Πηγές μόλυνσης ενός Ransomware με βάση στατιστικές μελέτες του 2019 (Πηγή: **https://www.statista.com/statistics/700965/leading-cause-of-ransomware-infection/**)

7.5. Επιχειρησιακή συνέχεια και σχέδιο αποκατάστασης λειτουργίας

Όταν ένας οργανισμός μολυνθεί από οποιοδήποτε Malware Campaign, ή πιο συγκεκριμένα από ένα Ransomware Campaign, θα πρέπει πέρα από τα πρώτα βήματα εξάλειψης του κινδύνου, να έχει υπολογίσει την πιθανότητα επερχόμενης καταστροφής του. Η καταστροφή του οργανισμού από μια τέτοια επίθεση μπορεί να είναι είτε σε υψηλά ή χαμηλά ποσοστά ενώ συνυπολογίζεται σε αυτά και το τμήμα ή τα τμήματα που έχουν δεχτεί την επίθεση.

Οι απώλειες του οργανισμού μετά από μια τέτοια καταστροφή κατηγοριοποιούνται σε οικονομικές, υλικοτεχνικές, απώλειες δεδομένων, απώλειες προσωπικού, κ.α. Συνεπώς θα πρέπει να έχει οριστεί έγκαιρα, ένα σχέδιο επιχειρησιακής συνέχειας (Business Continuity Plan) για τον οργανισμό, το οποίο ορίζει εάν συνολικά ο οργανισμός ή τμήματα αυτού θα σταματήσουν να λειτουργούν ή θα υπολειτουργούν, και για ποιο χρονικό διάστημα από τη χρονική στιγμή μηδέν της επίθεσης.

Στις πρώτες φάσεις του BCP έχουν οριστεί τα εξής:

- Maximum tolerable period of disruption (MTPD): Η μέγιστη ανεκτή περίοδος διακοπής της υπηρεσίας (π.χ. 24 ώρες)
- Recovery Point Objective (RPO): Το χρονικό σημείο κατά το οποίο θα μπορέσει να γίνει επαναφορά των υπηρεσιών από ένα ασφαλές αντίγραφο ασφαλείας (π.χ. 10 ώρες)

- Recovery Time Objective: Το χρονικό περιθώριο ώστε να εφαρμοστεί το RPO και να επανέλθουν όλες οι κρίσιμες υποδομές σε επίπεδα λειτουργίας

Φυσικά απομένει και μια περίοδος που στο σύνολό της μαζί με το RTO δεν θα πρέπει να ξεπερνούν το MTPD και είναι αυτή που ορίζει το διάστημα που χρειάζεται ώστε να επιστρέψει σε φυσιολογική κατάσταση ο οργανισμός.

Σε συνέχεια των παραπάνω, θα πρέπει ο οργανισμός να έχει δημιουργήσει συμβάσεις μεταξύ τρίτων μερών, τα οποία θα μπορούν να τον υποστηρίξουν στην περίπτωση μιας καταστροφής. Για παράδειγμα, εάν μετά το Ransomware Campaign έχουν καταστραφεί οι servers ενός τμήματος, θα πρέπει ένα συμφωνητικό (Service Level Agreement) μεταξύ του οργανισμού και ενός παρόχου μηχανημάτων server να είναι αυτό που θα διασφαλίσει την άμεση αποκατάσταση των μηχανημάτων που καταστράφηκαν.

Τέλος, θα πρέπει να οριστούν ασκήσεις ανά δύο ή τρεις μήνες όπου η ομάδα που ορίστηκε για την υλοποίηση του BCP θα πρέπει να το εφαρμόσει δοκιμαστικά και να προτείνει βελτιώσεις και αλλαγές που θα κρίνουν την επίτευξή του σε περίπτωση πραγματικού περιστατικού.

ΚΕΦΑΛΑΙΟ 8ο: Συμπεράσματα & μελλοντικές προοπτικές

Στην παρούσα μεταπτυχιακή διατριβή παρουσιάστηκαν τα malware campaigns τύπου Ransomware, η επικινδυνότητα αυτών, καθώς και ο τρόπος με τον οποίο λειτουργεί το κύκλωμα αυτής της επίθεσης χρησιμοποιώντας blockchains όπως αυτό του Bitcoin.

Παράλληλα, παρατέθηκαν ήδη γνωστοί τρόποι ανίχνευσης ενός επιτιθέμενου μέσα από την αλυσίδα συναλλαγών του Blockchain, καθώς και το εργαλείο αναζήτησης αυτού, Tracksomware, το οποίο στοχεύει στην ενίσχυση της αναζήτησης παράνομων συναλλαγών από έναν αναλυτή που διενεργεί μεθόδους forensics στο Blockchain.

Οι περιορισμοί της εύρεσης ενός τελικού wallet που ανήκει σε μια οικογένεια Ransomware, είναι αρκετοί αλλά προσπελάσιμοι. Με τη σωστή κατανομή υλικών και οικονομικών πόρων τόσο ο ευρύτερος τομέας αναζήτησής του όσο και το εργαλείο Tracksomware, μπορούν να αποφέρουν ακριβέστερα αποτελέσματα.

Ως μελλοντική εξέλιξη της παρούσας έρευνας γύρω από τις επιθέσεις τύπου Ransomware, αλλά και του τεχνικού παραρτήματος που παρατέθηκε, μπορεί να εφαρμοστεί στην υπάρχουσα υλοποίηση η μέθοδος της ανεστραμμένης πυραμίδας, η οποία αφορά τη δυνατότητα καταγραφής όλων αυτών των συνδεδεμένων συναλλαγών αυτοματοποιημένα, χωρίς να πρέπει ο αναλυτής να θέσει ένα ανώτατο κατώφλι στον αριθμό των επαναλήψεων που θα εκτελεστούν από τη μία συναλλαγή στην άλλη.

Η παρούσα υλοποίηση αντλεί και αναλύει δεδομένα από την αλυσίδα του Blockchain (συναλλαγές σε bitcoins). Άλλος ένας τομέας επέκτασής της, είναι η δυνατότητα που παρέχει για την ανάλυση διακριτών αλυσίδων όπου πραγματοποιούνται συναλλαγές με διαφορετικά κρυπτονομίσματα (Ether, Monero, κ.λπ) ή συνδυαστικές συναλλαγές π.χ. Bitcoin σε Ether. Προσθέτοντας αυτήν την επέκταση, θα μπορεί η μέθοδος ανεστραμμένης πυραμίδας να εκτελεστεί σε πολλαπλές αλυσίδες και να συνεχιστεί η ανάλυση στις περιπτώσεις όπου μια συναλλαγή του επιτιθέμενου “φεύγει” από το Blockchain και μεταπηδά σε μια διαφορετική αλυσίδα.

Με αυτόν τον τρόπο, τόσο σε επίπεδο καταγραφής, όσο και σε επίπεδο ανίχνευσης μιας τελικής διεύθυνσης, τα στοιχεία που μπορούν να παραχθούν θα είναι καταλυτικά για την μετάβαση στο επόμενο επίπεδο που είναι η ανίχνευση της ηλεκτρονικής ή και φυσικής παρουσίας του επιτιθέμενου.

Ολοκληρώνοντας, μέσα από την εκτενή έρευνα που πραγματοποιήθηκε σε πληθώρα από οικογένειες Ransomware, δημιουργήθηκε μια αποθήκη πληροφοριών η οποία περιλαμβάνει γενικά χαρακτηριστικά, τρόπους επίθεσης αλλά και τρόπους αντιμετώπισης των γνωστότερων ή και μη, οικογενειών.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] K.Baker, "The 11 Most Common Types of Malware," Crowdstrike, 2021 [Online], Available: https://www.crowdstrike.com/cybersecurity-101/malware/types-of-malware/.

[2] A.Hardikar. “Malware 101 - Viruses”. SANS. Information Security Reading Room, SANS Institute. 2021.

[3] University of Delaware. “How Is Malware Distributed?” Secure UD News, University of Delaware, 18 May 2015, sites.udel.edu/infosecnews/2015/05/18/how-is-malware-distributed/. Accessed 21 Mar. 2021.

[4] Richardson, Ronny, and Max M. North. "Ransomware: Evolution, mitigation and prevention." International Management Review 13.1 (2017): 10.

[5] Johnson, Ben. “How Ransomware Works.” VMware Carbon Black, 19 Sept. 2016, www.carbonblack.com/blog/how-ransomware-works/. Accessed 21 Mar. 2021.

[6] “Prime number” Wikipedia. 24 Feb. 2021, en.wikipedia.org/wiki/Prime_number. Accessed 20 Mar. 2021.

[7] “Euler's totient function” Wikipedia. 26 Feb. 2021, en.wikipedia.org/wiki/Euler%27s_totient_function. Accessed 21 Mar. 2021.

[8] “RSA (cryptosystem)” Wikipedia. 21 Mar. 2021, en.wikipedia.org/wiki/RSA_(cryptosystem). Accessed 21 Mar. 2021.

[9] Lessing, Marlese. “Case Study: AIDS Trojan Ransomware.” Edited by Ashley Wiesner, Sdxcentral, 3 June 2020, www.sdxcentral.com/security/definitions/case-study-aids-trojan-ransomware/. Accessed 18 Mar. 2021.

[10] Gazet, Alexandre. “Comparative Analysis of Various Ransomware Virii.” Journal in Computer Virology, vol. 6, no. 1, 2008, pp. 77–90., doi:10.1007/s11416-008-0092-2.

[11] Lessing, Marlese. “Case Study: Archievus Ransomware.” Edited by Ashley Wiesner, Sdxcentral, 11 June 2020, www.sdxcentral.com/security/definitions/case-study-archievus-ransomware/. Accessed 18 Mar. 2021.

[12] “PGPCoder.” Wikipedia, 28 Apr. 2020, en.wikipedia.org/wiki/PGPCoder. Accessed 18 Mar. 2021.

[13] Nazarov, Denis, and Olga Emelyanova. “Blackmailer: the Story of Gpcode.” SECURELIST, Kaspersky, 26 June 2006, securelist.com/blackmailer-the-story-of-gpcode/36089/. Accessed 18 Mar. 2021.

[14] “Vundo.” Wikipedia, 21 Jan. 2021, en.wikipedia.org/wiki/Vundo. Accessed 18 Mar. 2021.

[15] McMillan, Robert. “Alleged Ransomware Gang Investigated by Moscow Police.” PCWorld, IDG News Service, 31 Aug. 2010, www.pcworld.com/article/204577/article.html. Accessed 18 Mar. 2021.

[16] Hampton, Nikolai, and Zubair A. Baig. "Ransomware: Emergence of the cyber-extortion menace." (2015).

[17] Lessing, Marlese. “Case Study: Reveton Ransomware.” Edited by Ashley Wiesner, Sdxcentral, 18 June 2020, www.sdxcentral.com/security/definitions/case-study-reveton-ransomware/. Accessed 18 Mar. 2021.

[18] Cannell, Joshua. “Cryptolocker Ransomware: What You Need to Know.” Malwarebytes Labs, 21 Feb. 2018, blog.malwarebytes.com/101/2013/10/cryptolocker-ransomware-what-you-need-to-know/. Accessed 18 Mar. 2021.

[19] “Ransomware.” Wikipedia, 17 Mar. 2021, en.wikipedia.org/wiki/Ransomware#CryptoWall. Accessed 18 Mar. 2021.

[20] Tan Seng, Francis, and Duc Nguyen. “The New .LNK between Spam and Locky Infection.” Microsoft Security, 27 Aug. 2019, www.microsoft.com/security/blog/2016/10/19/the-new-lnk-between-spam-and-locky-infection/. Accessed 18 Mar. 2021.

[21] Mohurle, Savita, and Manisha Patil. "A brief study of wannacry threat: Ransomware attack 2017." International Journal of Advanced Research in Computer Science 8.5 (2017): 1938-1940.

[22] “EternalBlue” Wikipedia, 16 Mar. 2021, en.wikipedia.org/wiki/EternalBlue. Accessed 20 Mar. 2021.

[23] Solon, Olivia, and Alex Hern. “'Petya' Ransomware Attack: What Is It and How Can It Be Stopped?” The Guardian, Guardian News and Media, 28 June 2017, www.theguardian.com/technology/2017/jun/27/petya-ransomware-cyber-attack-who-what-why-how. Accessed 18 Mar. 2021.

[24] Ruiz, Fernando, and ZePeng Chen. “LeakerLocker: Mobile Ransomware Acts Without Encryption.” McAfee Blogs, 23 Aug. 2017, www.mcafee.com/blogs/other-blogs/mcafee-labs/leakerlocker-mobile-ransomware-acts-without-encryption/. Accessed 18 Mar. 2021.

[25] “What Is Ryuk Ransomware?” Malwarebytes, Dec. 2019, www.malwarebytes.com/ryuk-ransomware/. Accessed 18 Mar. 2021.

[26] Patsakis, Constantinos, and Anargyros Chrysanthou. "Analysing the fall 2020 Emotet campaign." arXiv preprint arXiv:2011.06479 (2020).

[27] Malwarebytes Labs. “Ransom.GandCrab.” Malwarebytes Labs, 25 Sept. 2020, blog.malwarebytes.com/detections/ransom-gandcrab/. Accessed 21 Mar. 2021.

[28] Palmer, Danny. “This Unusual New Ransomware Is Going after Servers.” ZDNet, ZDNet, 12 Nov. 2019, www.zdnet.com/article/this-unusual-new-ransomware-is-going-after-servers/. Accessed 18 Mar. 2021.

[29] “What Is Zeppelin Ransomware? Steps to Prepare, Respond, and Prevent Infection.” Core Security, 2020, www.coresecurity.com/core-labs/articles/what-zeppelin-ransomware-steps-prepare-respond-and-prevent-infection. Accessed 18 Mar. 2021.

[30] Mundo, Alexandre. “Buran Ransomware; the Evolution of VegaLocker.” *McAfee Blogs*, McAfee, 5 Nov. 2019, www.mcafee.com/blogs/other-blogs/mcafee-labs/buran-ransomware-the-evolution-of-vegalocker/. Accessed 21 Mar. 2021.

[31] Kost, Edward. “What Is Ransomware as a Service (RaaS)? The Dangerous Threat to World Security: UpGuard.” UpGuard, 5 Mar. 2021, www.upguard.com/blog/what-is-ransomware-as-a-service. Accessed 21 Mar. 2021.

[32] Intel 471. “Ransomware-as-a-Service: The Pandemic within a Pandemic.” *Intel 471*, 10 Dec. 2020, intel471.com/blog/ransomware-as-a-service-2020-ryuk-maze-revil-egregor-doppelpaymer/. Accessed 21 Mar. 2021.

[33] Research Team, Counter Threat Unit. “REvil/Sodinokibi Ransomware.” Secureworks, 24 Sept. 2019, www.secureworks.com/research/revil-sodinokibi-ransomware. Accessed 18 Mar. 2021.

[34] “CVE-2018-8453” Cve.mitre.org, 2018, cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8453. Accessed 18 Mar. 2021.

[35] Abrams, Lawrence. “A Closer Look at the RobbinHood Ransomware.” BleepingComputer, 28 May 2019, www.bleepingcomputer.com/news/security/a-closer-look-at-the-robbinhood-ransomware/. Accessed 18 Mar. 2021.

[36] Belding, Greg. “Malware Spotlight: Sodinokibi.” Infosec, 9 Apr. 2020, resources.infosecinstitute.com/topic/malware-spotlight-sodinokibi/. Accessed 18 Mar. 2021.

[37] Oracle. Oracle WebLogic Server, Oracle, 19 Apr. 2018, www.oracle.com/middleware/technologies/weblogic.html. Accessed 18 Mar. 2021.

[38] Research Team, Counter Threat Unit. “REvil/Sodinokibi Ransomware.” Secureworks, 24 Sept. 2019, www.secureworks.com/research/revil-sodinokibi-ransomware. Accessed 18 Mar. 2021.

[39] Yuste, Javier, and Sergio Pastrana. "Avaddon ransomware: an in-depth analysis and decryption of infected systems." arXiv preprint arXiv:2102.04796 (2021).

[40] CYBEREDGE Group. (2020, Mar.) 2020 CYBERTHREAT DEFENSE REPORT [Online]. Available: https://cyber-edge.com/cdr/#about-this-report.

[41] Casino, Fran, Thomas K. Dasaklis, and Constantinos Patsakis. "A systematic literature review of blockchain-based applications: current status, classification and open issues." Telematics and informatics 36 (2019): 55-81.

[42] Zheng, Zibin, et al. "An overview of blockchain technology: Architecture, consensus, and future trends." 2017 IEEE international congress on big data (BigData congress). IEEE, 2017.

[43] Politou, Eugenia, et al. "Blockchain mutability: Challenges and proposed solutions." IEEE Transactions on Emerging Topics in Computing (2019). IEEE, 2019.

[44] Zheng, Zibin, et al. "An overview of blockchain technology: Architecture, consensus, and future trends." *2017 IEEE international congress on big data (BigData congress)*. IEEE, 2017.
[45] “Elliptic Curve Digital Signature Algorithm” Wikipedia, 6 Jan. 2021 en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm. Accessed 21 Mar. 2021.

[46] No More Ransom. “Decryption Tools.” DECRYPTION TOOLS, No More Ransom, www.nomoreransom.org/en/decryption-tools.html. Accessed 21 Mar. 2021.

[47] Nakamoto, Satoshi. Bitcoin: A peer-to-peer electronic cash system. Manubot, 2019. Accessed 09 Jul. 2021.

[48] Moser, Malte. "Anonymity of bitcoin transactions.", https://allquantor.at/blockchainbib/, 2013, https://allquantor.at/blockchainbib/pdf/moser2013anonymity.pdf. Accessed 09 Jul. 2021.

[49] Huang, Danny Yuxing, et al. "Tracking ransomware end-to-end." 2018 IEEE Symposium on Security and Privacy (SP). IEEE, 2018.

[50] Wang, Zhi, et al. "ReFormat: Automatic reverse engineering of encrypted messages." European Symposium on Research in Computer Security. Springer, Berlin, Heidelberg, 2009.

[51] Ross, Ron, Michael McEvilley, and Janet Oren. Systems security engineering: Considerations for a multidisciplinary approach in the engineering of trustworthy secure systems. No. NIST Special Publication (SP) 800-160 (Withdrawn). National Institute of Standards and Technology, 2016.

[52] ENISA. “Cramm.” ENISA, ENISA, 6 July 2016, www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_cramm.html. Accessed 19 Jul. 2021.

[53] NIST. “Resources.” NIST, 8 Apr. 2020, www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources. Accessed 19 Jul. 2021.

[54] Boeckl, Kaitlin R., and Naomi B. Lefkovitz. "NIST privacy framework: A tool for improving privacy through enterprise risk management, version 1.0." (2020).

[55] “Backup rotation scheme” Wikipedia, 14 Jun. 2021 en.wikipedia.org/wiki/Backup_rotation_scheme. Accessed 19 Jul. 2021.

[56] Douligeris, Christos, and Aikaterini Mitrokotsa. "DDoS attacks and defense mechanisms: classification and state-of-the-art." Computer networks 44.5 (2004): 643-666.

[57] The Tor Project. “Tor Browser User Manual.” Tor Browser User Manual | Tor Project | Tor Browser Manual, The Tor Project, 2021, tb-manual.torproject.org/. Accessed 21 Jul. 2021.

[58] The Tor Project. “ONION SERVICES.” ONION SERVICES | Tor Project | Tor Browser Manual, The Tor Project, 2021, tb-manual.torproject.org/onion-services/. Accessed 21 Jul. 2021.

[59] de Best, Raynor. “Number of Cryptocurrencies Worldwide from 2013 to July 2021.” Statista, Statista Inc., 22 July 2021, www.statista.com/statistics/863917/number-crypto-coins-tokens/#statisticContainer. Accessed 22 Jul. 2021.

[60] CoinMarketCap. “Global Cryptocurrency Market Charts.” CoinMarketCap, CoinMarketCap, 21 July 2021, coinmarketcap.com/charts/. Accessed 22 Jul. 2021.

ΕΥΡΕΤΗΡΙΟ ΕΙΚΟΝΩΝ & ΠΙΝΑΚΩΝ

Μέρος Α' - Εικόνες:

Μέρος Β' - Πίνακες: