Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή

Στην Ασφάλεια Υπολογιστών και Δικτύων

Διερεύνηση του Σκοτεινού Διαδικτύου (Investigating Dark Web)

Κωνσταντίνος Παπιώτης

Επιβλέπων Καθηγητής

Ιωάννης Μαυρίδης

Δεκέμβριος 2017

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Διερεύνηση του Σκοτεινού Διαδικτύου (Investigating Dark Web)

Κωνσταντίνος Παπιώτης

Επιβλέπων Καθηγητής
Ιωάννης Μαυρίδης

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε
προς μερική εκπλήρωση των απαιτήσεων για απόκτηση

μεταπτυχιακού τίτλου σπουδών
στην Ασφάλεια Υπολογιστών και Δικτύων

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου

Δεκέμβριος 2017

Περίληψη

Ανασκόπηση Ο όρος Σκοτεινό Διαδίκτυο (Dark Web) αναφέρεται στη λειτουργία ενός ιστού, διαδικτυακά συνδεδεμένων, κόμβων στον οποίο οι χρήστες απολαμβάνουν ανωνυμία προκειμένου να έχουν πρόσβαση σε κρυφές υπηρεσίες αλλά και επικοινωνία με άλλους χρήστες χωρίς να φαίνεται η ταυτότητα τους (ανώνυμη επικοινωνία). Οι υπηρεσίες αυτές μπορούν να χρησιμοποιηθούν για θετικούς και για αρνητικούς σκοπούς. Η πρόσβαση σε ιστότοπους του Dark Web δεν μπορεί να επιτευχθεί με τις γνωστές μηχανές αναζήτησης, αλλά μόνο με την χρήση ειδικού λογισμικού. Στην παρούσα εργασία πραγματοποιείται εύρεση, καταγραφή, ανάλυση και αξιολόγηση των εργαλείων με τα οποία μπορεί να γίνει διερεύνηση του Dark Web.

Σκοπός της παρούσας εργασίας είναι η εύρεση των εργαλείων με τα οποία μπορεί να πραγματοποιηθεί διερεύνηση του Dark Web, καθώς και η καταγραφή, η ανάλυση και η αξιολόγησή τους. Επιπλέον, με τη χρήση αυτών των εργαλείων χαρτογραφούνται οι υπηρεσίες και οι δραστηριότητες εντός του Dark Web και δημιουργείται ένα ευρετήριο των ιστότοπων Dark Web.

Μεθοδολογία Πραγματοποιήθηκε ανασκόπηση επιλεγμένων δημοσιευμένων άρθρων από περιοδικά, πηγών από το (φανερό) διαδίκτυο, αλλά και δοκιμή των εργαλείων πρόσβασης στο Dark Web.

Η εργασία αποτελείται από έξι κεφάλαια στο πρώτο πραγματοποιείται η θεωρητική θεμελίωση του Dark Web, στο δεύτερο κεφάλαιο περιγράφεται η υλοποίηση των διάφορων δικτύων του Dark Web, στο τρίτο κεφάλαιο αναλύονται τα δίκτυα Friend to Friend, στο τέταρτο κεφάλαιο αναλύονται οι κακόβουλες και παράνομες χρήσεις του Dark Web, στο πέμπτο γίνεται περιγραφή των εργαλείων που χρησιμοποιήθηκαν και στο έκτο καταγράφονται τα συμπεράσματα.

Αποτελέσματα Η χρήση των εργαλείων του είχε ως αποτέλεσμα την ευρετηρίαση κρυφών υπηρεσιών. Έπιπλέον εξετάστηκε το επίπεδο της ασφάλειας και ανωνυμίας των κρυφών υπηρεσιών.

Συμπεράσματα Από την ανασκόπηση των πηγών, αλλά και με την χρήση εργαλείων διαπιστώθηκε η χρήση του Dark Web για κακόβουλους σκοπούς, ενώ η ανωνυμία εξαρτάται σε μεγάλο βαθμό από την ορθή διαχείριση και χρήση των κρυφών υπηρεσιών.

Λέξεις Κλειδιά Dark Web, Darknet, Deep Web, F2F Network, Tor, I2P, Freenet, Crawler, κρυφές υπηρεσίες

Summary

Review The Term Dark Web refers to the operation of a web-based, web-connected, node in which users enjoy anonymity in order to access hidden services and communicate with other users without showing their identity (anonymous communication). These services can be used for both positive and negative purposes. Access to Dark Web sites cannot be achieved with known search engines, but only with the use of special software. At the present work, finding, recording, analyzing and evaluating the tools with which Dark Web can be explored took place.

The purpose of this work is to find the tools for exploring the Dark Web, as well as recording, analyzing and evaluating them. In addition, using these tools, services and activities are mapped within the Dark Web and an Index of Dark Web sites is created.

Methodology Review of selected published articles from magazines, sources from the (obvious) internet, and testing of Dark Web access tools was made. Secondary analysis followed the collection and the recording of data. This work consists of five chapters, the first chapter describes the theoretical foundation of Dark Web, the second chapter describes the operation of the various Dark Web networks, the third chapter analyzes the Friend to Friend networks, while the fourth chapter analyzes the malicious and illegal uses of Dark Web, in the fifth chapter the used tools are described and in the sixth the conclusions are reported.

Results The use of the tools resulted in indexing of hidden services. Additionally, the level of security and anonymity of hidden services was examined.

Conclusions The review of the sources and the use of tools has revealed the use of Dark Web for malicious purposes, whereas anonymity largely depends on the proper management and use of hidden services.

Key Words Dark Web, Darknet, Deep Web, F2F Network, Tor, I2P, Freenet, Crawler, hidden services

Ευχαριστίες

Ευχαριστώ την οικογένειά μου για την αμέριστη υπομονή και συμπαράστασή τους.

Περιεχόμενα

Κεφάλαιο 1

Θεωρητική Θεμελίωση

1.1 Σκοπός Κεφαλαίου

Σκοπός του κεφαλαίου είναι να αναλυθούν θεωρητικά στοιχεία που αφορούν το Dark Web, να αποσαφηνιστούν οι έννοιες των Dark Web - Darknet και Deep Web καθώς παρατηρείται σύγχυση, να αναλυθούν οι μέθοδοι πρόσβασης στο Dark Web και η λειτουργία των συγκεκριμένων δικτύων.

1.1.1 Surface Web

Το διαδίκτυο είναι ένα τεράστιο δίκτυο επιμέρους δικτύων, το οποίο ενώνει εκατομμύρια μηχανές παγκοσμίως. Ως Surface Web – ιστός επιφανείας ή ορατός ιστός μπορεί να οριστεί οτιδήποτε εμφανίζεται σε μια συμβατική μηχανή αναζήτησης όπως είναι η Google, η Yahoo κλπ. Το Surface Web είναι το περιεχόμενο του διαδικτύου που μπορεί να βρεθεί μέσω τεχνικών link crawling. Οι τεχνικές αυτές αποσκοπούν στην εύρεση δεδομένων μέσω υπερσυνδέσμου, που βρίσκεται στην αρχική σελίδα ενός domain. Οι περισσότεροι χρήστες του διαδικτύου χρησιμοποιούν το Surface Web.

1.1.2 Deep Web

Ως Deep Web ορίζεται το τμήμα του World Wide Web, που είναι κρυμμένο από τις συμβατικές μηχανές αναζήτησης, δηλαδή το σύνολο των ιστοσελίδων που δεν ευρετηριάζονται από τις μηχανές αναζήτησης. Μεγάλο μέρος των πληροφοριών που υπάρχει στο παγκόσμιο διαδίκτυο δεν εμφανίζεται στις μηχανές αναζήτησης, όπως Google, Bing κλπ και αυτό συμβαίνει, συνήθως, διότι δεν είναι προσβάσιμες με υπερσυνδέσμους (hyperlinks). Ωστόσο, οι μηχανές αναζήτησης μπορούν να οδηγήσουν σε σελίδες που περιέχουν δεδομένα του Deep Web. Το σύνολο των δεδομένων του Deep Web μπορεί να είναι 500 φορές μεγαλύτερο από το Surface Web. Η πρόσβαση στα

περιεχόμενα του Deep Web απαιτεί τη συμπλήρωση και την υποβολή ερωτημάτων σε μορφή HTML, οι οποίες εμφανίζονται ως λίστα ή ως πίνακας [4, 27]. Οι πηγές του Deep Web αποθηκεύουν το περιεχόμενο τους σε βάσεις δεδομένων, που παράγουν μόνο δυναμικά αποτελέσματα, ως απάντηση σε ένα αίτημα. Το περιεχόμενο του Deep Web μπορεί να είναι:

α) Μη συνδεδεμένες σελίδες, δηλαδή να μην υπάρχει κάποιος υπερσύνδεσμος που να οδηγεί στην κάθε σελίδα.

β) Σελίδες που δεν έχουν html μορφή, αλλά οπτικοακουστικό περιεχόμενο, με αποτέλεσμα να μην υπάρχει η δυνατότητα δημιουργίας λέξεων κλειδιών.

γ) Περιεχόμενο βάσεων δεδομένων, στις οποίες οι crawlers δεν μπορούν να αλληλοεπιδράσουν με τις φόρμες αναζήτησης.

δ) Περιεχόμενο περιορισμένης πρόσβασης, το οποίο περιλαμβάνει σελίδες, οι οποίες απαιτούν την εγγραφή του χρήστη προκειμένου να είναι προσπελάσιμες.

ε) Περιεχόμενο το οποίο χρησιμοποιεί ειδικά προγράμματα, που αποτρέπουν την πρόσβαση των web crawlers ή η πρόσβαση σε αυτά γίνεται με τη χρήση CAPTCHAs.

στ) Δυναμικό περιεχόμενο, το οποίο περιλαμβάνει δεδομένα που δημιουργούνται δυναμικά ανάλογα με τις απαιτήσεις ενός χρήστη, δηλαδή δυναμικές σελίδες που είναι αποτέλεσμα ερωτημάτων (queries).

ζ) Αρχεία σε FTP διακομιστές.

1.1.3 Darknet

Ως Darknet μπορούμε να ορίσουμε τις μη αποδιδόμενες ή τις μη προσβάσιμες διευθύνσεις και πόρτες επικοινωνίας ενός δικτύου (δημόσιου ή ιδιωτικού). Αυτές οι μη αποδιδόμενες διευθύνσεις μπορούν να ρυθμιστούν κατάλληλα, ώστε να γίνουν αντικείμενο εκμετάλλευσης για κακόβουλους σκοπούς και να χρησιμοποιηθούν για διάφορα είδη κυβερνοεπιθέσεων, όπως Denial of Service Attack. [12]

1.1.4 Dark Web

Το Dark Web μπορεί να οριστεί ως ένα τμήμα του Deep Web, το οποίο σκοπίμως έχει αποκρυφθεί και δεν είναι προσβάσιμο μέσω συμβατικών λογισμικών πλοήγησης, όπως είναι τα Internet Explorer, Mozilla Firefox κλπ.. Ακόμη, μπορεί να είναι το μη ανιχνεύσιμο και μη προσβάσιμο διαδικτυακό περιεχόμενο, που δεν εμφανίζεται στον κυβερνοχώρο ή

στις μηχανές αναζήτησης. Επίσης, στο Dark Web περιλαμβάνονται κρυφές πλατφόρμες επικοινωνίας, όπως κοινωνικά δίκτυα και περιβάλλοντα διαμοιρασμού αρχείων [12].

Το σκοτεινό διαδίκτυο διαφέρει σε σχέση με το "επιφανειακό ή ορατό διαδίκτυο" με πολλούς τρόπους. Για παράδειγμα, τα domain names των κρυφών ιστότοπων έχουν την κατάληξη ".onion" ή ".i2p" ή κάποιο άλλο Top- Level domain name και είναι προσπελάσιμα μόνο μέσω τροποποιημένων προγραμμάτων περιήγησης (φυλλομετρητών) ή κάποιου ειδικού λογισμικού.[13] Στο λεξικό της Οξφόρδης (https://en.oxforddictionaries.com/definition/dark web) ως Dark Web ορίζεται «*το μέρος του διαδικτύου που είναι προσβάσιμο μόνο με ειδικό λογισμικό, το οποίο επιτρέπει τους χρήστες να παραμένουν ανώνυμοι ή μη ανιχνεύσιμοι*.» Επίσης, μπορούμε να ορίσουμε το περιεχόμενο του διαδικτύου που βρίσκεται σε Darknets ή σε επικαλυπτικά δίκτυα, τα οποία χρησιμοποιούν το δημόσιο διαδίκτυο και απαιτείται ειδικό λογισμικό ή διαμόρφωση ή εξουσιοδότηση προκειμένου να επιτευχθεί η πρόσβαση.

Τα Darknets αντιπροσωπεύουν μια κατηγορία δικτύων που παρέχουν ένα υπόστρωμα επικοινωνίας για αποκεντρωμένες κοινωνικές εφαρμογές. Το κοινό χαρακτηριστικό αυτών των δικτύων είναι ότι παρέχουν ασφαλή και ιδιωτική επικοινωνία στις διάφορες εφαρμογές τις οποίες προσφέρουν. Τα συγκεκριμένα δίκτυα παρέχουν ανωνυμία στον αποστολέα και τον δέκτη και υψηλές εγγυήσεις για την προστασία της ιδιωτικής ζωής τους, ωστόσο οι επιδόσεις αυτών των δικτύων είναι αρκετά χαμηλές.

Οι βασικές αρχές που εφαρμόζονται στα Darknets, προκειμένου να επιτευχθεί η ανωνυμία, αποτελούν την κύρια αιτία για τις χαμηλές επιδόσεις τους. Η πρώτη βασική αρχή είναι ότι οι συνδέσεις μεταξύ κόμβων επιτρέπονται μόνο εάν υπάρχει αμοιβαία εμπιστοσύνη μεταξύ τους, ώστε να αποφευχθεί η συμμετοχή μη αξιόπιστου και πιθανώς, κακόβουλου τρίτου μέρους. Η δεύτερη αρχή είναι η πηγή να επανεγγράφει όλα τα δεδομένα, με σκοπό να γίνει απόκρυψη της ταυτότητας του αποστολέα και της δρομολόγησης που ακολουθεί. Η τελευταία αρχή είναι ότι η επικοινωνία μεταξύ των στοιχείων των δικτύων γίνεται με τη χρήση κρυπτογράφησης, προκειμένου να επιτευχθεί εμπιστευτικότητα. [23]

Η πιο διάσημη και πλέον γνωστή μέθοδος προσπέλασης στο Dark Web είναι με τη χρήση του Tor browser (The onion routing), το οποίο είναι ένα δωρεάν open source λογισμικό. Με τον Tor browser μπορούμε να προσπελάσουμε το δίκτυο Tor, το οποίο είναι ευρέως γνωστό για την προστασία της ατομικής ελευθερίας, της ιδιωτικότητας και της δυνατότητας διεξαγωγής από τον χρήστη εμπιστευτικών εργασιών, χωρίς να καταγράφονται οι διαδικτυακές δραστηριότητές του, αλλά και για τις παράνομες δραστηριότητες, οι οποίες καθίστανται δυνατές λόγω της ανωνυμίας την οποία προσφέρει. Η μεγαλύτερη διαφορά του Dark Web από το Surface Web είναι η ανωνυμία την οποία προσφέρει το Dark Web, σε σχέση με το Surface Web, στο οποίο ένας ιστότοπος περιέχει πλήθος πληροφοριών, όπως η IP, η τοποθεσία, cookies, οι οποίες προσδιορίζουν την ταυτότητά του. [18]

1.1.5 Μηχανές αναζήτησης

Το Deep Web και το Dark Web ορίζονται με βάση τις μηχανές αναζήτησης. Μηχανή αναζήτησης είναι μια εφαρμογή που αναζητά δεδομένα στο διαδίκτυο, για συγκεκριμένη πληροφορία και παρέχει λίστα με τα δεδομένα τα οποία βρέθηκαν. Οι μηχανές αναζήτησης περιέχουν τρία στοιχεία:

α) Ένα spider ή crawler ή bot, το οποίο διατρέχει κάθε σελίδα ή αντιπροσωπευτικές σελίδες των διαδικτυακών τοποθεσιών, που πρόκειται να αναζητηθούν και να διαβαστούν. Για αυτή τη διαδικασία χρησιμοποιούνται σύνδεσμοι υπερκειμένου σε κάθε σελίδα, προκειμένου να ανακαλύψουν τις άλλες σελίδες του ιστότοπου.

β) Ένα κατάλογο, ο οποίος δημιουργεί ένα τεράστιο ευρετήριο με τις σελίδες που έχουν διαβαστεί από το spider.

γ) Το μηχανισμό αναζήτησης, που είναι ένα πρόγραμμα, που λαμβάνει το αίτημα της αναζήτησης, συγκρίνει με τις καταχωρήσεις στο ευρετήριο και επιστρέφει τα αποτελέσματα στον χρήστη.

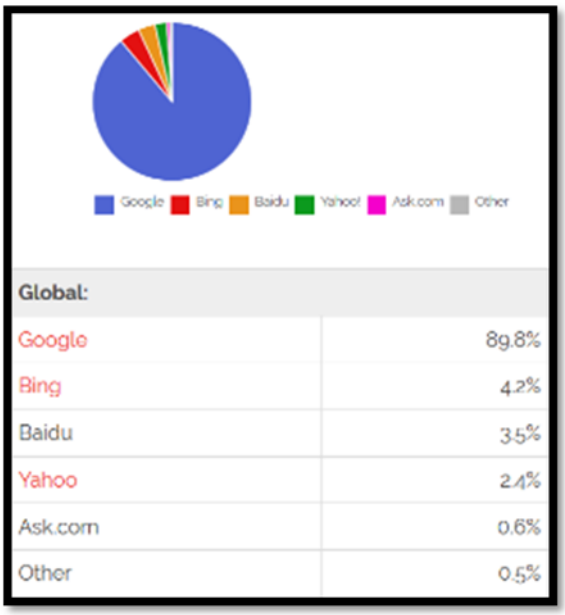
Οι Web Crawlers αποτελούνται από τέσσερα μέρη:

α) Το Scheduler, που πραγματοποιεί την εισαγωγή και την εξαγωγή των URLs στην ουρά και τον εντοπισμό των διπλότυπων URLs.

β) Το Downloader, που εξάγει τα URLs σε μορφή σελίδων και τις αποστέλλει στον Scheduler.

γ) Την ουρά, η οποία δέχεται από το Scheduler τα URLs.

δ) Τον χώρο αποθήκευσης, που αποθηκεύονται οι σελίδες από τον Downloader.



Global:	
Google	89.8%
Bing	4.2%
Baidu	3.5%
Yahoo	2.4%
Ask.com	0.6%
Other	0.5%

Εικόνα 1
Στην εικόνα φαίνονται οι πιο δημοφιλείς μηχανές αναζήτησης. (Πηγή: https://karmasnack.com/search-engine-market-share/)

1.2 Τρόποι προσπέλασης στο Dark Web

Σε αυτή την ενότητα θα αναλυθούν οι τρόποι προσπέλασης στο Dark Web, τα διάφορα ανώνυμα δίκτυα, τα οποία υπάρχουν, όπως τα Tor, I2P, καθώς και οι βασικοί τρόποι λειτουργίας τους.

1.2.1 Tor - The onion Routing

Το δίκτυο Tor είναι ένα δίκτυο επικάλυψης (εικονικό δίκτυο, το οποίο είναι δομημένο πάνω σε ένα υπάρχον δίκτυο), που αποτελείται από εθελοντικά λειτουργικούς διακομιστές και παρέχει την δυνατότητα της ανωνυμίας στο διαδίκτυο. Η σύνδεση στο δίκτυο Tor πραγματοποιείται με τον Tor browser. Ο Tor browser είναι ένα δωρεάν λογισμικό και αποτελεί μια τροποποιημένη έκδοση του Firefox ESR, που έχει ενσωματωμένες ρυθμίσεις και επεκτάσεις, προκειμένου να εκμεταλλεύεται το δίκτυο Tor. Οι χρήστες του δικτύου Tor, προκειμένου να ανταλλάξουν πληροφορίες, δεν πραγματοποιούν μια άμεση σύνδεση, αλλά συνδέονται μέσα από μια σειρά εικονικών tunnel. Το Tor αποτελεί ένα αποτελεσματικό εργαλείο κατά της λογοκρισίας, καθώς επιτρέπει στους χρήστες να προσπελάσουν προορισμούς και περιεχόμενα τα οποία έχουν αποκλειστεί από τον τοπικό πάροχο. Το Tor επιτρέπει στους χρήστες να δημοσιεύουν ιστοσελίδες, χωρίς να αποκαλύπτεται η ταυτότητα τους (Public IP, τοποθεσία).

Επιπλέον, με τη χρήση του Tor παρέχεται προστασία από την ανάλυση κυκλοφορίας (traffic analysis). Η ανάλυση κυκλοφορίας μπορεί να χρησιμοποιηθεί, προκειμένου να ερευνηθεί ποιος ανταλλάσσει δεδομένα με ποιον. Ένα τρίτο πρόσωπο, γνωρίζοντας την προέλευση και τον προορισμό των δεδομένων ενός προσώπου, μπορεί να παρακολουθήσει τη συμπεριφορά και τα ενδιαφέροντα του. Η ανάλυση κυκλοφορίας λειτουργεί με τον εξής τρόπο: τα πακέτα δεδομένων στο διαδίκτυο έχουν δύο μέρη, το ένα είναι το ωφέλιμο φορτίο δεδομένων και το δεύτερο μέρος μια κεφαλίδα που χρησιμοποιείται για τη δρομολόγηση του πακέτου. Το ωφέλιμο φορτίο περιέχει δεδομένα, που προέρχονται από το επίπεδο δικτύου. Ακόμη και από ένα κρυπτογραφημένο ωφέλιμο φορτίο, με την ανάλυση κίνησης, μπορούν να εξαχθούν συμπεράσματα και πληροφορίες. Αυτό συμβαίνει γιατί η ανάλυση κίνησης εστιάζει στην κεφαλίδα των πακέτων, η οποία δίνει πληροφορίες για τον προορισμό, την πηγή και το μέγεθος. Με την εξέταση της κεφαλίδας, οι μεσάζοντες μπορούν να δουν πληροφορίες σχετικά με τα δεδομένα, δημιουργώντας έτσι προβλήματα στην ιδιωτική ζωή ενός χρήστη.

Στο δίκτυο Tor τα πακέτα δεν κατευθύνονται απευθείας από την πηγή στον προορισμό, αλλά διανύουν μια τυχαία διαδρομή, μέσα από διάφορους αναμεταδότες (relays), καλύπτοντας έτσι τα ίχνη τους και αντιμετωπίζοντας με αυτό τον τρόπο την ανάλυση κίνησης. Δημιουργείται έτσι ένα μονοπάτι, στο οποίο είναι δύσκολο να αναλυθεί η πηγή ή η προέλευση των δεδομένων από ένα τρίτο πρόσωπο.

Προκειμένου να δημιουργηθεί ένα ιδιωτικό μονοπάτι δικτύου, το λογισμικό Tor δημιουργεί ένα κύκλωμα από κρυπτογραφημένες συνδέσεις μέσω των αναμεταδοτών του δικτύου. Το onion routing αναφέρεται στη στρωματοποιημένη φύση της υπηρεσίας κρυπτογράφησης, όπου τα αρχικά δεδομένα κρυπτογραφούνται και επανακρυπτογραφούνται πολλές φορές από τον κάθε διαδοχικό κόμβο από τον οποίο διέρχονται. Ο κάθε κόμβος αποκρυπτογραφεί ένα στρώμα κρυπτογράφησης, προτού μεταφέρει τα δεδομένα στον επόμενο και τελικά στον προορισμό τους, μέσω ενός κόμβου εξόδου. Αυτό έχει ως αποτέλεσμα να μειωθεί η πιθανότητα αποκρυπτογράφησης ή να γίνουν κατανοητά κατά τη μεταφορά τους τα αρχικώς απεσταλμένα δεδομένα.

Το κύκλωμα εκτείνεται κατά ένα κόμβο τη φορά, με κάθε αναμεταδότη να γνωρίζει μόνο σε ποιον αναμεταδότη θα στείλει τα δεδομένα και από ποιον θα λάβει. Ένας αναμεταδότης δεν γνωρίζει ποτέ την πλήρη διαδρομή που θα πραγματοποιήσει ένα πακέτο δεδομένων. Μόλις δημιουργηθεί ένα κύκλωμα στο δίκτυο Tor, μπορούν να μεταδοθούν πολλά είδη δεδομένων και εφαρμογές λογισμικού. Επειδή κάθε αναμεταδότης δεν επικοινωνεί με περισσότερους από δυο αναμεταδότες, δεν μπορεί να χρησιμοποιηθεί ωτακουστής. Επιπλέον, κανένας κακόβουλος αναμεταδότης δεν μπορεί να πραγματοποιήσει ανάλυση κίνησης και να εντοπίσει την πηγή και τον προορισμό της σύνδεσης. Το Tor λειτουργεί μόνο με συνδέσεις TCP και μπορεί να χρησιμοποιηθεί για οποιαδήποτε εφαρμογή με την υποστήριξη SOCKS. Για μεγαλύτερη αποτελεσματικότητα, το λογισμικό Tor χρησιμοποιεί το ίδιο κύκλωμα μέχρι 10 λεπτά, ενώ δημιουργείται ένα καινούριο κύκλωμα για μεταγενέστερες αιτήσεις.[57]

1.2.2 The invisible Internet Project (I2P)

Το I2P είναι ένα ανώνυμο επικαλυπτικό δίκτυο, στο οποίο διάφορες εφαρμογές μπορούν να χρησιμοποιηθούν ανώνυμα και με ασφάλεια, προκειμένου να ανταλλάξουν μηνύματα η μια με την άλλη. Οι εφαρμογές που υποστηρίζει το δίκτυο I2P είναι η προσπέλαση κρυφών υπηρεσιών- ιστοσελίδων, chatting, δημιουργία blog και μεταφορά αρχείων. Το δίκτυο I2P βασίζεται αυστηρά σε μηνύματα. Όλες οι επικοινωνίες από άκρο σε άκρο είναι κρυπτογραφημένες, ενώ ακόμη και τα τελικά σημεία χρησιμοποιούν κρυπτογράφηση.

Προκείμενου τα δεδομένα που αποστέλλονται να είναι ανώνυμα, η κάθε εφαρμογή πελάτη I2P έχει τον δικό της εικονικό router, ο οποίος δημιουργεί εισερχόμενες και εξερχόμενες σήραγγες (tunnel). Ουσιαστικά δημιουργείται μια ακολουθία μεταξύ ομότιμων χρηστών, που στέλνουν μηνύματα προς μια κατεύθυνση (από και προς τον πελάτη αντίστοιχα). Όταν ένας πελάτης θέλει να στείλει μήνυμα σε έναν άλλο πελάτη, τότε ο πελάτης- πομπός στέλνει το μήνυμα σε ένα από τα εξερχόμενα tunnel με στόχο ένα από τα εισερχόμενα tunnel του πελάτη-παραλήπτη, φθάνοντας έτσι στον προορισμό.

Την πρώτη φορά που ένας πελάτης θέλει να επικοινωνήσει με έναν άλλο πελάτη, αποστέλλει ένα ερώτημα σε έναν δομημένο πίνακα κατανεμημένου κατακερματισμού (Distributed Hash Table - DHT), που αποτελεί τη βάση δεδομένων του δικτύου. Η διαδικασία αυτή πραγματοποιείται, προκειμένου ο ένας πελάτης να εντοπίσει τα

εισερχόμενα tunnel του άλλου πελάτη με αποτελεσματικό τρόπο. Στη συνέχεια ανταλλάσσουν μεταξύ τους μηνύματα που περιλαμβάνουν δεδομένα. Στο δίκτυο I2P μπορούν να χρησιμοποιηθούν και εφαρμογές που χρησιμοποιούν το πρωτόκολλο UDP αλλά και TCP. [54]

1.3 Διαβαθμισμένα δίκτυα στο διαδίκτυο

Το Tor σχεδιάστηκε, υλοποιήθηκε και αναπτύχθηκε στα μέσα της δεκαετίας του 1990 από το Εργαστήριο Ερευνών του Πολεμικού Ναυτικού των ΗΠΑ, με στόχο την προστασία των κυβερνητικών επικοινωνιών. Παράλληλα, το Υπουργείο Άμυνας των ΗΠΑ ανέπτυσσε το Αμυντικό Δίκτυο Δεδομένων (Defense Data Network), το οποίο είναι ένα μεγάλης κλίμακας, ιδιωτικό διαδίκτυο, που παρείχε συνδεσιμότητα μεταξύ των στρατιωτικών εγκαταστάσεων των ΗΠΑ και στρατιωτικών βάσεων στο εξωτερικό. Το Αμυντικό Δίκτυο Δεδομένων περιλαμβάνει τα δίκτυα NIPRNET, SIPRNET και JWICS, τα οποία χρησιμοποιούνται ανάλογα με το βαθμό ασφαλείας των πληροφοριών που πρέπει να διακινηθούν.

Το JWICS (Joint Worldwide Intelligence Communications System) σύμφωνα με τον ορισμό του JP 1-02 (Joint Publication) Department of Defense Dictionary of Military and Associated Terms είναι: *«Το ευαίσθητο, διαχωρισμένο τμήμα πληροφοριών του Δικτύου Πληροφοριακών Συστημάτων Άμυνας. Ενσωματώνει προηγμένες τεχνολογίες δικτύωσης που επιτρέπουν την ανταλλαγή πληροφοριών, από σημείο σε σημείο ή σε πολλαπλά σημεία, που περιλαμβάνουν τηλεδιάσκεψη φωνής, κειμένου, γραφικών, δεδομένων και τηλεδιάσκεψης».* Την διαχείριση του JWICS έχει αναλάβει η Defense Intelligence Agency και υποστηρίζεται από το Υπουργείο Εθνικής Άμυνας. Στο συγκεκριμένο δίκτυο διαβιβάζονται πληροφορίες έως βαθμού ασφαλείας ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ.

Το SIPRnet (Secret Internet Protocol Router Network), σύμφωνα με τον ορισμό του JP 1-02 *«είναι ένα παγκόσμιο δίκτυο μεταγωγής πακέτου επιπέδου ΑΠΟΡΡΗΤΟ που χρησιμοποιεί δρομολογητές πρωτοκόλλου Internet υψηλής ταχύτητας και κυκλώματα του Δικτύου Πληροφοριακών Συστημάτων (Defense Information Systems Network) υψηλής χωρητικότητας»*. Αποτελεί το μεγαλύτερο δια -λειτουργικό δίκτυο διοίκησης και ελέγχου, υποστηρίζει το Σύστημα Παγκόσμιας Διοίκησης και Ελέγχου (Global Command and

Control System - GCCS), το Σύστημα Μηχανογραφικών Μηνυμάτων (Defense Message System - DMS), τον διακλαδικό σχεδιασμό και άλλες διαβαθμισμένες επιχειρησιακές εφαρμογές. Παρέχει ασφαλή, συνεχή και κοινή υπηρεσία δεδομένων μεταγωγής πακέτου, με ταχύτητες από 56 Kbps εώς και 1 Gbps. Στο συγκεκριμένο δίκτυο διαβιβάζονται πληροφορίες έως βαθμού ασφαλείας ΑΠΟΡΡΗΤΟ. Για την ασφάλεια του δικτύου χρησιμοποιείται Public Key Infrastructure (PKI).[24]

Στο δίκτυο SIPRnet, κατά την διάρκεια του Δεύτερου Πολέμου του Κόλπου (Operation Iraqi Freedom), αναπτύχθηκε από την 1η Μεραρχία Τεθωρακισμένων το forum CAVNET, που ανανεώνονταν σε πραγματικό χρόνο και χρησιμοποιούνταν μέχρι το επίπεδο Λόχου, για την ανταλλαγή απόψεων και γνώσεων, για πάνω από 30 κατηγορίες αποστολών. Το CAVNET δημιουργήθηκε με σκοπό την αξιοποίηση των φίλιων και εχθρικών στοιχείων που αφορούν τακτική, τεχνική και τις εφαρμοζόμενες διαδικασίες σε τακτικό επίπεδό, προκειμένου να εξασφαλισθεί πλεονέκτημα έναντι των εχθρικών δυνάμεων. Το γεγονός ότι στο SIPRnet έχουν πρόσβαση μέχρι και το επίπεδο της Υπομονάδας, βοήθησε στην ανάπτυξη του CAVNET σε τακτικό επίπεδο. Αυτό οδήγησε στην άμεση ανταλλαγή και ενσωμάτωση πληροφοριών, με αποτέλεσμα να επισπευσθεί η λήψη απόφασης και να αυξηθεί ο ρυθμός των επιχειρήσεων. Με την ανανέωση των πληροφοριών σε πραγματικό χρόνο, επιτυγχάνεται η «κοινή σχετική επιχειρησιακή εικόνα» όλων των φίλιων δυνάμεων και δίνεται αποφασιστικό πλεονέκτημα έναντι του εχθρού. [41] Τέλος, κάθε μήνα τα πιο σημαντικά συμβάντα και διαδικασίες προβάλλονταν σε ειδική ανάρτηση.

Το NIPRnet (Nonsecure Internet Protocol Router Network) είναι ένα αδιαβάθμητο ιδιωτικό δίκτυο, που χρησιμοποιείται για την ανταλλαγή αδιαβάθμητων αλλά ευαίσθητων (Sensitive but Unclassified - SBU) πληροφοριών. Αυτή η υπηρεσία προσφέρει και υποστηρίζει εφαρμογές του Υπουργείου Εθνικής Άμυνας των ΗΠΑ, όπως αποστολή email, δικτυακές υπηρεσίες και μεταφορά αρχείων, ενώ υπάρχει η δυνατότητα πρόσβασης στο δημόσιο διαδίκτυο. Το NIPRnet υποστηρίζει τις υπηρεσίες τηλεπικοινωνιακών δεδομένων SBU για εφαρμογές υποστήριξης μάχης, όπως το Joint Chiefs of Staff (JCS), το Military Departments (MILDEPS) και το Combatant Commands (COCOM). Η ταχύτητα των υπηρεσιών είναι από 56 Kbps εώς 2.4 Gbps.Τα τελευταία χρόνια, γίνεται προσπάθεια για αναβάθμιση του NIPRnet.

Σε εξέλιξη βρίσκεται το πρόγραμμα αναβάθμισης NIPRnet, που είναι μια προσπάθεια εξασφάλισης των πληροφοριών για την άμυνα του δικτύου υπολογιστών, με αρμόδια αρχή για την υλοποίηση του, την DISA(Defense Information Support Agency). Αποτελείται από διάφορα σχέδια, τα οποία έχουν ως στόχο να βελτιώσουν την άμυνα των αδιαβάθμιτων δικτύων του Υπουργείου Άμυνας των ΗΠΑ. Το πρόγραμμα φιλτραρίσματος δικτυακού περιεχομένου (Web Content Filter- WFC) σχετίζεται με το NIPRnet. Το WCF παρέχει διαχείριση κυκλοφορίας στο επίπεδο εφαρμογής, φιλτράρισμα των αιτήσεων των URLs και φιλτράρισμα κακόβουλου λογισμικού. Το πρόγραμμα WCF συμβάλει στην αντιμετώπιση κυβερνοεπιθέσεων μειώνοντας το πεδίο επίθεσης του δικτύου NIRPnet.

Επιπλέον, η Ομοσπονδιακή Πύλη του NIRPnet προσφέρει επιχειρηματικές δυνατότητες, που υποστηρίζουν επιπρόσθετες λειτουργίες, όπως ασφαλές Domain Name Service (DNS) για τα δίκτυα του Υπουργείου Άμυνας. Αυτό δημιουργεί ένας σαφές διαχωρισμό των μη διαβαθμισμένων δικτύων Ενόπλων Δυνάμεων και του υπόλοιπου διαδικτύου. Το δίκτυο NIRPnet χρησιμοποιείται για διακίνηση πληροφοριών μέχρι βαθμού ασφαλείας ΑΔΙΑΒΑΘΜΗΤΟ.[47]

Κεφάλαιο 2

Υλοποίηση Dark Web

2.1 Σκοπός Κεφαλαίου

Σκοπός του κεφαλαίου είναι η ανάλυση της αρχιτεκτονικής και των τρόπων υλοποίησης του Dark Web, αλλά και των υπηρεσιών που προσφέρουν.

2.2 Γενικά χαρακτηριστικά του δικτύου Tor

Το Onion Routing είναι ένα κατανεμημένο δίκτυο επικάλυψης, που σχεδιάστηκε για να προσφέρει ανώνυμες εφαρμογές (πλοήγηση στο διαδίκτυο, αποστολή άμεσων μηνυμάτων κλπ) βασισμένες στο πρωτόκολλο TCP. Προσφέρει ανώνυμες συνδέσεις, οι οποίες παρέχουν υψηλή προστασία από υποκλοπές και ανάλυση κίνησης (traffic analysis) και δυσκολεύουν ένα τρίτο μέρος να εντοπίσει πληροφορίες σχετικά με την σύνδεση.

Οι πελάτες Tor επιλέγουν ένα μονοπάτι και δημιουργούν ένα κύκλωμα, στο οποίο κάθε κόμβος (node - onion router) γνωρίζει μόνο τον επόμενο και τον προηγούμενο κόμβο. Τα δεδομένα που κινούνται στο μονοπάτι έχουν μια σταθερή σε μέγεθος μορφή στρωμάτων - κελιών δεδομένων, τα οποία ξετυλίγονται σε κάθε κόμβο με τη χρήση ενός συμμετρικού κλειδιού.

1. Σχεδιασμός του δικτύου Tor

Στο δίκτυο Tor, ο κάθε Onion Router λειτουργεί ως μια διαδικασία επιπέδου χρήστη, χωρίς να έχει κάποια ειδικά δικαιώματα. Κάθε Onion Router διατηρεί μια TLS σύνδεση με

τους άλλους Onion Routers. Κάθε χρήστης εκτελεί τοπικά ένα λογισμικό, το οποίο ονομάζεται Onion Proxy, που χρησιμοποιείται για την φόρτιση καταλόγων, για την εγκατάσταση κυκλωμάτων στο δίκτυο και για τον χειρισμό συνδέσεων των εφαρμογών του χρήστη. Οι Onion Proxies αποδέχονται τις TCP ροές και τις πολυπλέκουν στα κυκλώματα. Οι Onion Routers, από την άλλη μεριά του κυκλώματος, συνδέουν στους επιθυμητούς προορισμούς και αναμεταδίδουν τα δεδομένα.

Κάθε Onion Router διατηρεί ένα μακροχρόνιο κλειδί ταυτότητας και ένα βραχυχρόνιο κλειδί onion. Το κλειδί ταυτότητας χρησιμοποιείται για την υπογραφή των πιστοποιητικών TLS, για την υπογραφή του Router Descriptor και για την υπογραφή καταλόγων. Το κλειδί onion χρησιμοποιείται για την αποκρυπτογράφηση των αιτήσεων από τους χρήστες, για εγκατάσταση ενός κυκλώματος και για την διαπραγμάτευση προσωρινών κλειδιών. Το πρωτόκολλο TLS επίσης εγκαθιστά ένα βραχυπρόθεσμο κλειδί σύνδεσης, που χρησιμοποιείται για την επικοινωνία μεταξύ των Onion Routers. Τα βραχυπρόθεσμα κλειδιά εναλλάσσονται περιοδικά, προκειμένου να περιορίσουν την πιθανότητα επιτυχών επιθέσεων.[11]

2. Κελιά του Onion

Οι Onion Routers επικοινωνούν μεταξύ τους και με τις Onion Proxy των χρηστών, μέσω συνδέσεων TLS, με προσωρινά κλειδιά. Η χρήση του TLS εξασφαλίζει την εμπιστευτικότητα των δεδομένων και αποτρέπει την τροποποίηση των δεδομένων από έναν επιτιθέμενο.

Η κίνηση μεταφέρεται σε αυτές τις συνδέσεις μέσω κελιών με σταθερό μέγεθος. Κάθε κελί έχει μέγεθος 512 bytes και αποτελείται από την κεφαλίδα και το ωφέλιμο φορτίο. Η κεφαλίδα περιλαμβάνει ένα αναγνωριστικό κυκλώματος (circuit identifier), που καθορίζει για ποιο κύκλωμα αντιστοιχεί το κελί και μια εντολή που αφορά το ωφέλιμο φορτίο του κελιού. Με βάση την εντολή, τα κελιά μπορεί να είναι κελιά ελέγχου (control cells), τα οποία αφορούν τον κόμβο που τα λαμβάνει ή κελιά αναμετάδοσης, τα οποία φέρουν δεδομένα ροής από άκρο σε άκρο. Οι εντολές των κελιών ελέγχου είναι το padding, create ή created και destroy.

Τα κελιά αναμετάδοσης έχουν μια επιπρόσθετη κεφαλίδα, πρόκειται για την κεφαλίδα αναμετάδοσης, η οποία περιέχει ένα streamID, ένα checksum για έλεγχο ακεραιότητας από άκρο σε άκρο, το μήκος του ωφέλιμου φορτίου αναμετάδοσης και μια εντολή αναμετάδοσης. Η κεφαλίδα αλλά και το ωφέλιμο φορτίο του κελιού αναμετάδοσης κρυπτογραφούνται ή αποκρυπτογραφούνται, καθώς κινούνται στο κύκλωμα, με τον αλγόριθμο κρυπτογράφησης AES 128 bit σε counter mode, ώστε να δημιουργείται αλγόριθμος ροής.[11]

3. Τέλεια εμπιστευτικότητα

Το Tor χρησιμοποιεί μια τηλεσκοπική σχεδίαση στα μονοπάτια του δικτύου, όπου ο πελάτης που ξεκινάει την σύνδεση διαπραγματεύεται τα session κλειδιά σε κάθε διερχόμενο κόμβο. Το πλεονέκτημα είναι ότι δεν απαιτείται εντοπισμός της επαναλαμβανόμενης κίνησης και η διαδικασία δημιουργίας των κυκλωμάτων είναι πιο αξιόπιστη σε σχέση με την αρχική έκδοση του Tor, όπου ένας κακόβουλος κόμβος μπορούσε να καταγράψει την κίνηση, να εκθέσει – μολύνει τους κόμβους στους οποίους αποστέλλει τα δεδομένα και να τα αποκρυπτογραφήσει.[11]

4. Διαχωρισμός του πρωτοκόλλου από την ανωνυμία

Στον αρχικό σχεδιασμό του Tor απαιτούνταν ξεχωριστός Proxy εφαρμογής (Application Proxy) για κάθε εφαρμογή, κάτι το οποίο δεν ήταν πρακτικό και έτσι πολλές εφαρμογές δεν υποστηρίχτηκαν ποτέ. Το Tor υποστηρίζει την διεπαφή SOCKS proxy, επιτρέποντας έτσι την εκτέλεση προγραμμάτων βασισμένα σε πρωτόκολλο TCP, χωρίς περαιτέρω τροποποίηση. Η τρέχουσα έκδοση του Tor βασίζεται στις δυνατότητες φιλτραρίσματος των proxies επιπέδου εφαρμογής, που βελτιώνουν την ιδιωτικότητα, όπως για παράδειγμα το Privoxy. [11]

5. Μη ύπαρξη ανάμιξης, παραμόρφωσης ή διαμόρφωσης της κυκλοφορίας

Στην αρχική έκδοση του, το Tor πραγματοποιούσε διανομή και αναδιάταξη των πακέτων όταν έφθαναν στον προορισμό τους, υποθέτοντας ότι υπάρχει παραμόρφωση των δεδομένων μεταξύ των Onion Routers, ενώ και σε μεταγενέστερες εκδόσεις προστίθεντο δεδομένα μεταξύ των onion proxies και των onion routers. Ωστόσο, στην τελευταία

έκδοση του Tor, για οικονομικούς και πρακτικούς λόγους αυτή η διαδικασία δεν συνεχίστηκε. [11]

6. Πολλαπλές ροές TCP από ένα κύκλωμα

Αρχικά το Onion Routing δημιουργούσε ξεχωριστό κύκλωμα για κάθε αίτηση, από το επίπεδο της εφαρμογής, ωστόσο, αυτό απαιτούσε πολλαπλές διεργασίες δημόσιου κλειδιού για κάθε αίτηση, ενώ ο μεγάλος αριθμός των κυκλωμάτων μπορούσε να θέσει σε κίνδυνο την ανωνυμία. Το Tor πολυπλέκει πολλαπλές TCP συνδέσεις σε ένα κύκλωμα, προκειμένου να βελτιώσει την ανωνυμία και την αποδοτικότητα του. Για την αποφυγή καθυστερήσεων, οι χρήστες κατασκευάζουν κυκλώματα προληπτικά. Ενώ, για να περιοριστεί η δυνατότητα σύνδεσης μεταξύ των ροών, οι Onion Proxy, δημιουργούν περιοδικά κυκλώματα εφόσον τα προηγούμενα έχουν χρησιμοποιηθεί, ενώ λήγουν τα χρησιμοποιημένα κυκλώματα που δεν έχουν ανοιχτές ροές. Οι Onion Proxy ανανεώνουν τα κυκλώματα κάθε ένα λεπτό, έτσι ακόμα και για βαριά χρήση ο χρόνος για την δημιουργία κυκλωμάτων είναι αμελητέος. [11]

7. Έλεγχος συμφόρησης

Οι τυπικές προσεγγίσεις εξισορρόπησης του φορτίου και ελέγχου κίνησης σε δίκτυα επικάλυψης, περιλαμβάνουν επικοινωνία εσωτερικού ελέγχου και καθολική εικόνα της κίνησης. Το Tor εφαρμόζει αποκεντρωμένο έλεγχο συμφόρησης, με την χρήση αναγνωριστικών από άκρο σε άκρο, διατηρώντας την ανωνυμία, ενώ επιτρέπει στους κόμβους, που βρίσκονται στις άκρες του δικτύου, να ανιχνεύουν τη συμφόρηση και να ρυθμίζουν την κίνηση των πακέτων, έως ότου υποχωρήσει η συμφόρηση. [11]

Η συμφόρηση στο δίκτυο μπορεί να προκληθεί είτε τυχαία είτε από πρόθεση. Χωρίς κάποιο μηχανισμό ελέγχου, η συμφόρηση μπορεί να μεταδοθεί σε όλο το δίκτυο. Για παράδειγμα, εάν μεγάλος αριθμός χρηστών επιλέξει για τα κυκλώματα του την ίδια σύνδεση από Onion Router σε Onion Router, τότε αυτή η σύνδεση είναι πολύ πιθανό να κορεστεί. Ο έλεγχος της συμφόρησης πραγματοποιείται με δυο τρόπους, με τον περιορισμό στο επίπεδο του κυκλώματος και τον περιορισμό στο επίπεδο ροής.[11]

Ο περιορισμός στο επίπεδο κυκλώματος πραγματοποιείται με έλεγχο της χρήσης του εύρους ζώνης του κυκλώματος. Για αυτή τη διαδικασία, ο κάθε Onion Router θα πρέπει

να παρακολουθεί δυο παράθυρα. Το πρώτο είναι το παράθυρο συσκευασίας που ελέγχει πόσα κελιά δεδομένων αναμεταδόσεως επιτρέπονται να συσκευαστούν και να μεταδοθούν πίσω στον Onion Router. Το δεύτερο είναι το παράθυρο μετάδοσης, που παρακολουθεί πόσα κελιά δεδομένων αναμεταδόσεως πρόκειται να παραδοθούν στις TCP ροές στο δίκτυο. [11]

Το κάθε παράθυρο αρχικοποιείται με κάποιον αριθμό κελιών. Όταν ένα κελί δεδομένων συσκευάζεται ή παραδίδεται, το αντίστοιχο παράθυρο μειώνεται. Όταν ένας Onion Router λάβει αρκετά κελιά δεδομένων, θα στείλει ένα κελί "relay sendme" στον Onion Router, με το streamID να είναι μηδέν. Όταν ένας Onion Router λάβει κελί "relay sendme" με streamID μηδέν, αυξάνει το παράθυρο συσκευασίας. Καθένα από αυτά τα κελιά αυξάνει το παράθυρο κατά 100. Εάν το παράθυρο συσκευασίας φτάσει το μηδέν, ο Onion Router σταματά να διαβάζει δεδομένα από τις TCP συνδέσεις των ροών του αντίστοιχου κυκλώματος και στέλνει το κελί "no more relay", μέχρι να λάβει κελί "relay sendme".[11]

Ο Onion Proxy συμπεριφέρεται παρόμοια, εκτός από το γεγονός ότι πρέπει να παρακολουθεί ένα παράθυρο επικοινωνίας και ένα παράθυρο παράδοσης για κάθε Onion Router στο κύκλωμα. Αν το παράθυρο συσκευασίας φτάσει το μηδέν, τότε σταματάει την ανάγνωση των ροών που προορίζονται για αυτόν τον Onion Router. [11]

Ο δεύτερος μηχανισμός ελέγχου συμφόρησης είναι επιπέδου ροής και είναι παρόμοιος με τον μηχανισμό επιπέδου κυκλώματος. Οι Onion Routers και οι Onion Proxies χρησιμοποιούν τα κελιά "relay sendme" για να εφαρμόσουν έλεγχο ροής από άκρο σε άκρο για κάθε ρεύμα (stream) μεταξύ των κυκλωμάτων. Κάθε ρεύμα ξεκινάει με ένα παράθυρο συσκευασίας (500 κελιά) και αυξάνει το παράθυρο με μια σταθερή τιμή (50), κατά την παραλαβή ενός κελιού "relay sendme". Μόλις φτάσουν αρκετά κελιά, ο έλεγχος συμφόρησης σε επίπεδο ροής ελέγχει εάν τα δεδομένα δόθηκαν με επιτυχία στην ροή TCP. Το κελί "relay sendme" αποστέλλεται μόνο όταν ο αριθμός των bytes που εκκρεμεί να αποσταλεί, είναι κάτω από κάποιο όριο (10 κελιά).[11]

8. Εξυπηρετητές καταλόγου

Σε προηγούμενες εκδόσεις του Tor εφαρμοζόταν η πλημμύρα (Flood) πληροφοριών κατάστασης μέσω του δικτύου. Αυτή η προσέγγιση ήταν αναξιόπιστη και περίπλοκη. Στην τρέχουσα έκδοση του Tor εφαρμόζεται μια πιο απλοποιημένη τεχνική. Οι πιο έμπιστοι κόμβοι λειτουργούν ως εξυπηρετητές καταλόγου, καθώς παρέχουν υπογεγραμμένους καταλόγους με την τρέχουσα κατάσταση γνωστών δρομολογητών. Περιοδικά, οι χρήστες λαμβάνουν τους καταλόγους μέσω του πρωτοκόλλου HTTP. [11]

Το Tor χρησιμοποιεί μια ομάδα πλεοναζόντων Onion Routers, οι οποίοι ανιχνεύουν τις αλλαγές στη τοπολογία του δικτύου και στην κατάσταση των κόμβων. Οι εξυπηρετητές καταλόγου λειτουργούν όπως οι εξυπηρετητές HTTP, έτσι οι πελάτες γνωρίζουν την τρέχουσα κατάσταση του δικτύου και τη λίστα με τους Routers. Οι Onion Routers μπορούν να ενημερώνουν τους εξυπηρετητές καταλόγου για την κατάσταση τους. Οι εξυπηρετητές καταλόγου συνδυάζουν αυτές τις πληροφορίες και την οπτική τους για την κίνηση του δικτύου και δημιουργούν ένα υπογεγραμμένο κατάλογο με την συνολική κατάσταση του δικτύου. Το λογισμικό του Tor έχει προεγκατεστημένη λίστα με τους εξυπηρετητές καταλόγου και τα κλειδιά τους, προκειμένου ο πελάτης να έχει οπτική του δικτύου. [11]

Όταν ο εξυπηρετητής καταλόγου λάβει μια υπογεγραμμένη κατάσταση για έναν Onion Router, ελέγχει εάν αναγνωρίζει το κλειδί ταυτότητας του Onion Router. Οι εξυπηρετητές καταλόγου δεν προβάλουν τους μη αναγνωρισμένους Onion Routers, γιατί συνέβαινε αυτό, θα αποσταθεροποιούσαν το δίκτυο. Οι καινούργιοι κόμβοι του δικτύου θα πρέπει να προστίθενται από τον διαχειριστή του εξυπηρετητή καταλόγου. [11]

Οι εξυπηρετητές καταλόγου θα πρέπει να είναι συγχρονισμένοι μεταξύ τους και να έχουν έναν κοινό κατάλογο. Οι πελάτες θα πρέπει να εμπιστεύονται αυτόν τον κατάλογο, μόνο αν είναι υπογεγραμμένος από συγκεκριμένο αριθμό διακομιστών καταλόγου. [11]

Η χρήση εξυπηρετητών καταλόγου είναι πιο απλή, πιο ευέλικτη και πιο οικονομική από την τεχνική της πλημμύρας (flooding). Οι υπογεγραμμένοι κατάλογοι μπορούν να αποθηκευτούν από άλλους Onion Routers, έτσι οι εξυπηρετητές καταλόγου δεν εμποδίζουν την απόδοση του δικτύου όταν υπάρχουν πολλοί χρήστες. [11]

9. Έλεγχος ακεραιότητας από άκρο σε άκρο

Στην αρχική έκδοση του Tor δεν υπήρχε έλεγχος ακεραιότητας στα δεδομένα. Κάθε κόμβος από τον οποίο διέρχονταν τα δεδομένα θα μπορούσε να αλλάξει το περιεχόμενο τους, όπως για παράδειγμα να αλλάξει την αίτηση μια σύνδεσης και να συνδεθεί σε άλλον εξυπηρετητή. Το Tor αντιμετωπίζει αυτές τις επιθέσεις με την επαλήθευση της ακεραιότητας των δεδομένων, πριν φύγουν για το δίκτυο.

Ο έλεγχος ακεραιότητας στο Tor, πραγματοποιείται στα άκρα της ροής. Όταν ένας χρήστης διαπραγματεύεται ένα κλειδί με ένα νέο αναμεταδότη, τότε και οι δυο έχουν μια τιμή κατακερματισμού SHA-1, την οποία γνωρίζουν μόνο αυτοί. Στη συνέχεια προσθέτουν σταδιακά στην τιμή κατακερματισμού το περιεχόμενο όλων των κελιών αναμετάδοσης που δημιουργούν. Επίσης διατηρούν μια τιμή SHA-1 για όλα τα δεδομένα που έλαβαν.

Ένας επιτιθέμενος για να μπορέσει να αφαιρέσει ή να τροποποιήσει κάποιο κελί, θα πρέπει να μπορεί να εξάγει την παρούσα τιμή κατακερματισμού. Το SHA-1, δεν είναι ευάλωτο σε επιθέσεις στις οποίες ο επιτιθέμενος προσθέτει σταδιακά τιμές κατακερματισμού ώστε να ανακαλύψει μια έγκυρη τιμή. Οι Onion Routers και Onion Proxies θα διακόψουν το κύκλωμα εάν λάβουν μη έγκυρη τιμή κατακερματισμού. [11]

10. Rendez-vous points και κρυφές υπηρεσίες

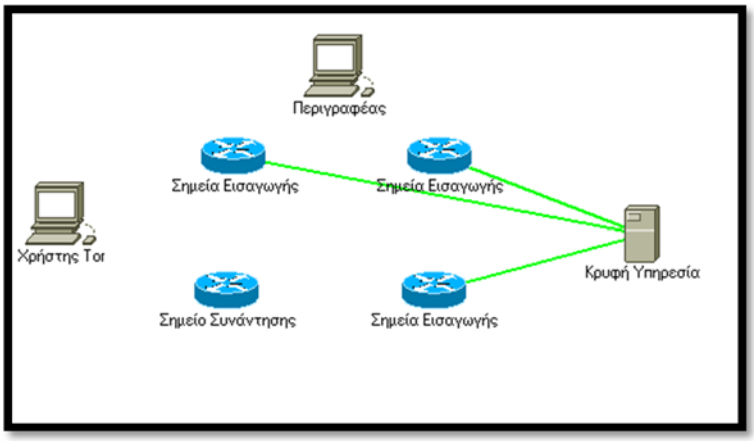
Το Tor προσφέρει έναν ολοκληρωμένο μηχανισμό ανωνυμίας μέσω διακομιστών, των οποίων η τοποθεσία είναι κρυφή. Οι προηγούμενες εκδόσεις του Tor περιλάμβαναν μακροχρόνια Onion απόκρισης, τα οποία μπορούσαν να χρησιμοποιηθούν για την κατασκευή κυκλωμάτων σε έναν κρυφό διακομιστή. Ωστόσο, δεν παρείχαν ασφάλεια και δεν είχαν κάποια χρησιμότητα όταν ένας κόμβος σταματούσε την λειτουργία του ή άλλαζε τα κλειδιά κρυπτογράφησης του. Στην τρέχουσα έκδοση του Tor, οι πελάτες διαπραγματεύονται τα Rendezvous Points για να συνδεθούν στους κρυφούς εξυπηρετητές. [11]

Στο δίκτυο Tor, τα Rendezvous Points λειτουργούν ως δομικά στοιχεία για τις κρυφές υπηρεσίες. Οι κρυφές υπηρεσίες επιτρέπουν σε έναν χρήστη να προσφέρει TCP υπηρεσίες, χωρίς να αποκαλύπτεται η IP του. Ο σχεδιασμός των κρυφών υπηρεσιών έχει τα παρακάτω χαρακτηριστικά:

α) Έλεγχο πρόσβασης: ο διαχειριστής της κρυφής υπηρεσίας μπορεί να φιλτράρει τα εισερχόμενα αιτήματα, έτσι ένας επιτιθέμενος δεν μπορεί να πραγματοποιήσει flooding στην κρυφή υπηρεσία, κάνοντας πολλαπλές συνδέσεις.
β) Ευρωστία: Η κρυφή υπηρεσία θα πρέπει να διατηρεί μια ψευδώνυμη ταυτότητα μεγάλης χρονικής διάρκειας. Η κρυφή υπηρεσία δεν θα πρέπει να είναι δεσμευμένη μόνο με έναν Onion Router, αλλά θα πρέπει να μπορεί να συνδέει την κρυφή υπηρεσία με άλλους Onion Routers.
γ) Αντίσταση στη παραπλάνηση : Ένας επιτιθέμενος δεν θα πρέπει να είναι σε θέση να χρησιμοποιεί ένα δρομολογητή συνάντησης, για παράνομη κρυφή υπηρεσία, κάνοντας τους χρήστες να πιστεύουν αυτή η υπηρεσία είναι νόμιμη.
δ) Διαφάνεια Εφαρμογής: Οι χρήστες για να έχουν πρόσβαση στις κρυφές υπηρεσίες πρέπει να χρησιμοποιούν συγκεκριμένο λογισμικό, ενώ οι διαχειριστές των υπηρεσιών δεν απαιτείται να τροποποιήσουν τις εφαρμογές τους. [11]

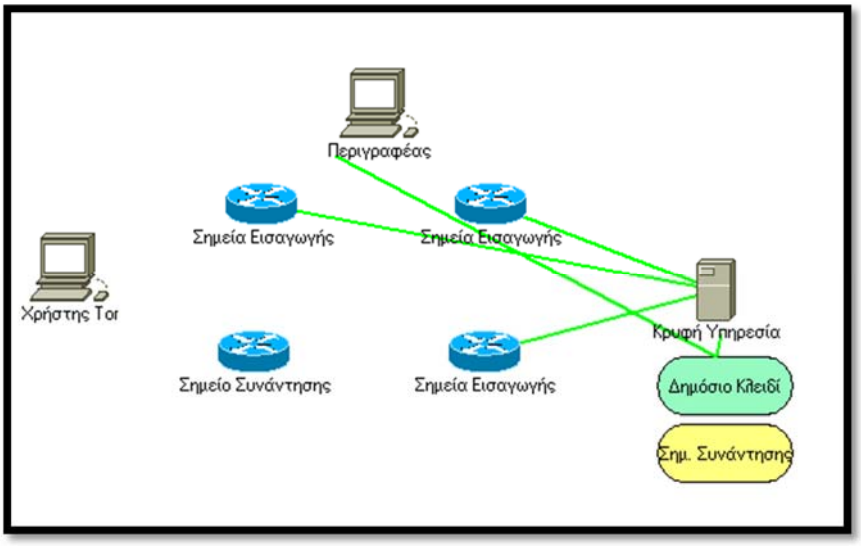
2.3 Κρυφές υπηρεσίες

Το δίκτυο TOR, προσφέροντας ανωνυμία, επιτρέπει στους χρήστες τη σύνδεση σε κρυφές υπηρεσίες, χωρίς να γίνονται γνωστά τα στοιχεία τους. Η λειτουργία των κρυφών υπηρεσιών έχει ως εξής:
α) Μια κρυφή υπηρεσία θα πρέπει να γνωστοποιήσει την ύπαρξη της στο δίκτυο Tor, έτσι ώστε οι πελάτες (clients) Tor να μπορούν να επικοινωνήσουν με αυτή. Η κρυφή υπηρεσία θα πρέπει να επιλέξει κάποιους αναμεταδότες δημιουργώντας κυκλώματα και να αιτηθεί να λειτουργούν ως σημεία εισαγωγής δίνοντας το δημόσιο κλειδί τους.



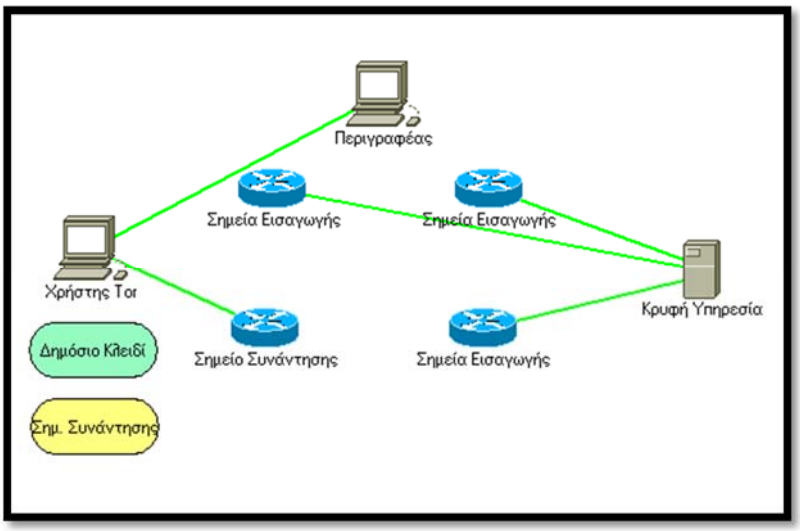
Εικόνα 2 Η κρυφή υπηρεσία γνωστοποιεί την υπαρξη της (Πηγή: https://www.torproject.org/docs/hidden-services.html.en)

β) Η κρυφή υπηρεσία δημιουργεί έναν "περιγραφέα" (descriptor) κρυφής υπηρεσίας, ο οποίος περιλαμβάνει το δημόσιο κλειδί, τα σημεία εισαγωγής και υπογράφεται από το ιδιωτικό κλειδί της. Η κρυφή υπηρεσία αποστέλλει τον περιγραφέα σε ένα πίνακα κατανεμημένων τιμών κατακερματισμού. Ο περιγραφέας θα έχει την μορφή XXXX.onion, όπου XXXX ένα όνομα 16 χαρακτήρων που προέρχεται από το δημόσιο κλειδί της κρυφής υπηρεσίας. Με αυτό τον τρόπο οι πελάτες μπορούν να προσπελάσουν την κρυφή υπηρεσία. Παρόλο που μοιάζει να μην είναι πρακτικό, η χρήση ενός αυτόματα παραγόμενου ονόματος εξυπηρετεί το γεγονός ότι όλα τα μέρη του δικτύου (σημεία εισαγωγής, πίνακας με τις τιμές κατακερματισμού και πελάτες) μπορούν να επιβεβαιώσουν ότι είναι η σωστή κρυφή υπηρεσία.



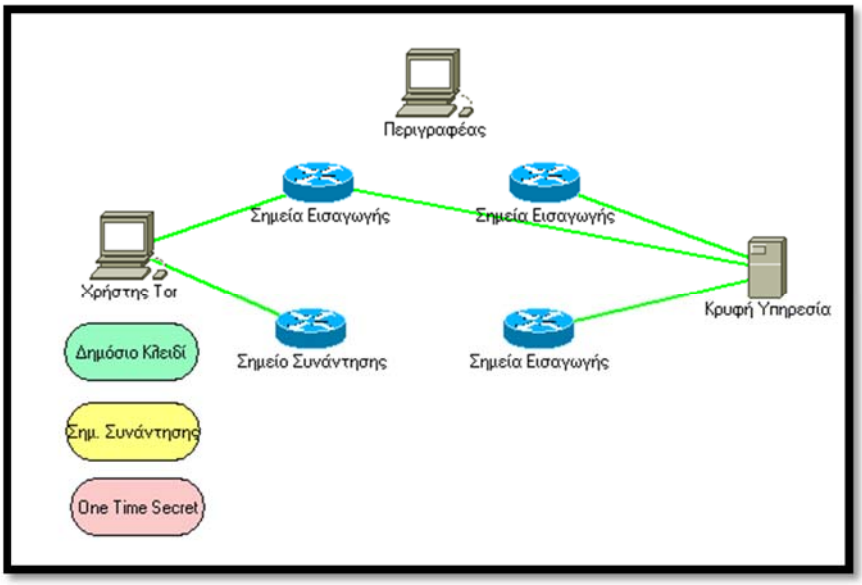
Εικόνα 3 Η κρυφή υπηρεσία δημιουργεί έναν "περιγραφέα" κρυφής υπηρεσίας (Πηγή: https://www.torproject.org/docs/hidden-services.html.en)

γ) Ένας client που θέλει να προσπελάσει μια κρυφή υπηρεσία θα πρέπει να μάθει την Onion διεύθυνση της. Στη συνέχεια, ο client θα πρέπει να ξεκινήσει τη δημιουργία μιας σύνδεσης με τον πίνακα τιμών κατακερματισμού και τον περιγραφέα. Εάν υπάρχει περιγραφέας για την XXXX.onion, τότε ο client γνωρίζει τα σημεία εισαγωγής και το δημόσιο κλειδί που θα χρησιμοποιήσει. Ακόμη ο client δημιουργεί ένα κύκλωμα με έναν τυχαία επιλεγμένο αναμεταδότη, ο οποίος λειτουργεί ως σημείο συνάντησης για ένα one-time secret.



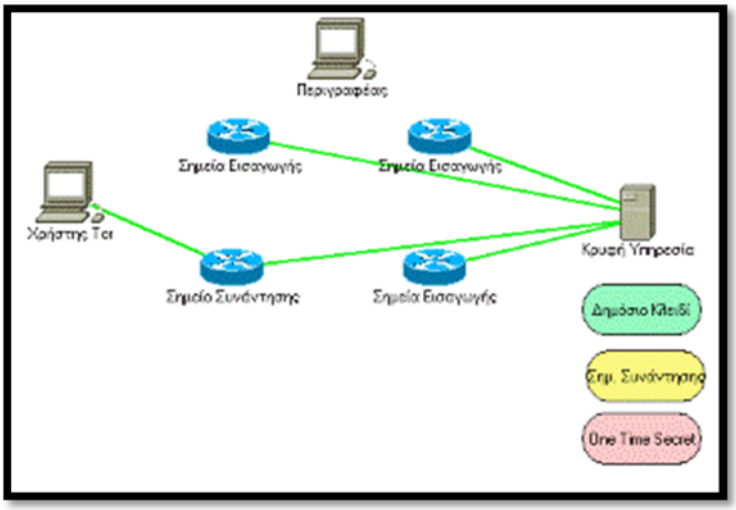
Εικόνα 4 Ο Client δημιουργεί νέα σύνδενση (Πηγή: https://www.torproject.org/docs/hidden-services.html.en)

δ) Όταν ληφθούν τα στοιχεία του περιγραφέα και οριστεί το σημείο συνάντησης, ο πελάτης δημιουργεί ένα εισαγωγικό μήνυμα, το οποίο είναι κρυπτογραφημένο με το δημόσιο κλειδί της κρυφής υπηρεσίας. Το τελευταίο περιλαμβάνει τη διεύθυνση του σημείου συνάντησης και το one- time secret. Ο client στέλνει το μήνυμα σε ένα από τα σημεία εισαγωγής, ζητώντας να παραδοθεί στην κρυφή υπηρεσία.



Εικόνα 5 Ο client στέλνει το μήνυμα σε ένα από τα σημεία εισαγωγής (Πηγή: https://www.torproject.org/docs/hidden-services.html.en)

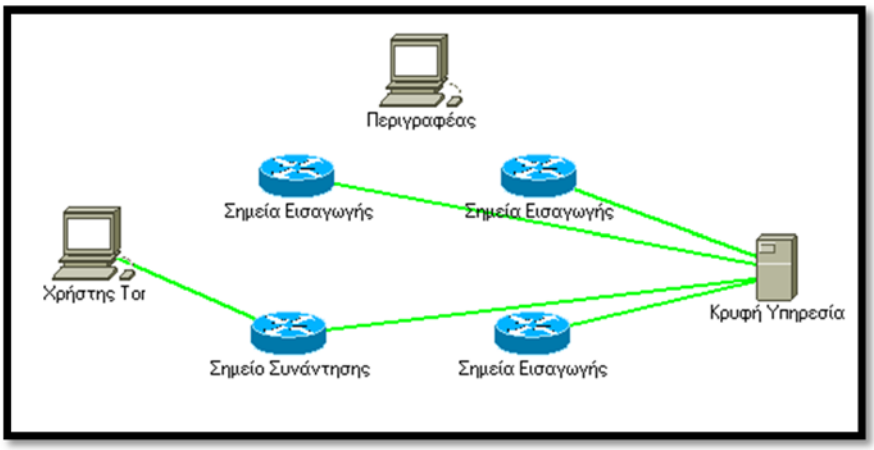
ε) Η κρυφή υπηρεσία αποκρυπτογραφεί το μήνυμα εισαγωγής του πελάτη και βρίσκει τη διεύθυνση του σημείου συνάντησης και το one time secret. Ακολούθως, δημιουργεί ένα κύκλωμα με το σημείο συνάντησης και στέλνει το one time secret.



Εικόνα 6 (Πηγή: https://www.torproject.org/docs/hidden-services.html.en)

στ) Τέλος, το σημείο συνάντησης ειδοποιεί τον client για την επιτυχή δημιουργία σύνδεσης. Μετά από αυτό, ο client και η κρυφή υπηρεσία χρησιμοποιούν τα κυκλώματα και το σημείο συνάντησης για περαιτέρω επικοινωνία μεταξύ τους και ανταλλαγή δεδομένων. Το σημείο συνάντησης αναμεταδίδει τα μηνύματα από τον client στην υπηρεσία και αντίστροφα. Η πλήρης σύνδεση μεταξύ του client και της κρυφής

υπηρεσίας αποτελείται από 6 αναμεταδότες. Τρεις από αυτούς χρησιμοποιεί ο client, με τον τρίτο να είναι το σημείο συνάντησης και τρεις χρησιμοποιεί η κρυφή υπηρεσία. [56]



Εικόνα 7 (Πηγή: https://www.torproject.org/docs/hidden-services.html.en)

2.3.1 Είδη κρυφών υπηρεσιών

1. Web Browsing

Ο Tor Browser χρησιμοποιείται για πλοήγηση τόσο στις κρυφές υπηρεσίες .onion όσο και στο υπόλοιπο διαδίκτυο προσφέροντας ανωνυμία και προστασία από την ανάλυση κίνησης. Οι κρυφές υπηρεσίες χρησιμοποιούνται τόσο για νόμιμους όσο και για παράνομους σκοπούς, όπως για παράδειγμα για εγκληματικές επιχειρήσεις, ομάδες «χακτιβισμού», υπηρεσίες επιβολής νόμου.

2. Chat και instant message

Υπάρχουν διάφορες εφαρμογές άμεσου μηνύματος που εκμεταλλεύονται την ανωνυμία του δικτύου Tor:

α) Torchat

Είναι μία αποκεντρωμένη ανώνυμη εφαρμογή ανταλλαγής άμεσων μηνυμάτων που χρησιμοποιεί το δίκτυο Tor. Προσφέρει κρυπτογραφημένη μεταφορά κειμένου και αρχείων. Η εκμετάλλευση του δικτύου Tor και η κρυπτογράφηση που χρησιμοποιείται, καθιστά δύσκολο τον εντοπισμό της πηγής και του προορισμού, τη τοποθεσία του αποστολέα και του παραλήπτη αλλά και το περιεχόμενο των μηνυμάτων που

ανταλλάσσονται. Κάθε χρήστης έχει για ταυτότητα μια αλφαριθμητική τιμή 16 χαρακτήρων η οποία δημιουργείται τυχαία.

β) Tormessenger

Το Tormessenger είναι ένας πελάτης ανταλλαγής άμεσων μηνυμάτων που σχεδιάστηκε για να πραγματοποιεί ανώνυμες συνδέσεις μέσω του δικτύου Tor. Το Tormessenger βασίζεται στο Instantbird IM client, στέλνει την κίνηση μέσω του δικτύου Tor και χρησιμοποιεί στις συνομιλίες κρυπτογραφία Off-the-Record. Υποστηρίζει διάφορα δίκτυα επικοινωνίας όπως Google Talk, IRC, Odnoklassniki, Twitter, Jabber (XMPP) και έχει μια εύχρηστη γραφική διεπαφή χρήστη σε διάφορες γλώσσες. Χρησιμοποιείται το πρωτόκολλο TLS για την κρυπτογράφηση της επικοινωνίας. [55]

γ) Facebookcorewwi

Το facebookcorewwi.onion είναι η επίσημη κρυφή υπηρεσία που επιτρέπει την πρόσβαση στο Facebook. Τον Απρίλιο του 2016, οι χρήστες έφτασαν το 1 εκατομμύριο. Ήταν η πρώτη σελίδα που χρησιμοποιούσε νόμιμο πιστοποιητικό για σύνδεση με πρωτόκολλο SSL στο δίκτυο Tor. Το πιστοποιητικό SSL χρησιμοποιείται προκειμένου οι χρήστες να είναι σίγουροι ότι συνδέονται στο Facebook και όχι σε κάποια άλλη κακόβουλη σελίδα. Διατηρεί όλες τις ιδιότητες του κοινωνικού δικτύου, όπως ανταλλαγή μηνυμάτων, κοινοποίηση περιεχομένου, σχολιασμό και αντιδράσεις. Η κρυφή υπηρεσία του Facebook επιτρέπει τη χρήση του σε χώρες στις οποίες απαγορεύεται.

3. Διαμοιρασμός Αρχείων

Vuze

Το Vuze είναι ένας BitTorrent Client, που χρησιμοποιείται για διαμοιρασμό μεταξύ ομότιμων χρηστών αρχείων πρωτοκόλλου BitTorrent. Επιπλέον, υπάρχει η δυνατότητα παρακολούθησης, λήψης και διαμοιρασμού βίντεο. Το περιεχόμενο παρουσιάζεται μέσω καναλιών και κατηγοριών πχ TV shows, μουσική, ταινίες, video games.

Παρόλο που υπάρχει η δυνατότητα όλη η κίνηση ενός υπολογιστή να πραγματοποιείται μέσω του δικτύου Tor, δεν προτείνεται η χρήση του δικτύου Tor για ανταλλαγή αρχείων

μεταξύ ομότιμων χρηστών όπως το torrent. Αυτό συμβαίνει διότι οι Socks Proxies που χρησιμοποιούνται στο δίκτυο Tor υποστηρίζουν το πρωτόκολλο TCP και όχι το UDP, το οποίο χρησιμοποιούν για επικοινωνία οι trackers των P2P δικτύων. Η χρήση των Bittorrent Clients μέσω του δικτύου Tor έχει ως αποτέλεσμα ο κόμβος εξόδου του Tor να στέλνει τη πραγματική IP στον tracker ανώνυμα. Έτσι, ένας κακόβουλος ομότιμος χρήστης να μπορεί να αποκαλύψει την πραγματική IP. Επιπλέον, όταν ένας χρήστης λαμβάνει δεδομένα από Bittorrent και ταυτόχρονα πλοηγεί στο διαδίκτυο μέσω του δικτύου Tor, υπάρχει η πιθανότητα ένας κακόβουλος κόμβος εξόδου να μπορέσει να καταρρίψει την ανωνυμία. Αυτό συμβαίνει διότι το δίκτυο Tor χρησιμοποιεί πολλαπλές ροές σε ένα κύκλωμα.

4. Email

Το Tor προσφέρει πολλές online υπηρεσίες email, οι οποίες προσφέρουν ανωνυμία. Μερικές από αυτές είναι Mail2Tor, Bitmessage email και το Proton Mail, το οποίο προσφέρει τη δυνατότητα αποστολής/λήψης κρυπτογραφημένων emails, επιπλέον υπάρχουν και κάποιες αναλώσιμες υπηρεσίες όπως το Guerrilla mail.

5. Δημοσίευση σε Forums, Blogs, Newsgroups

Στο δίκτυο Tor υπάρχουν πλήθος forums και blogs για διάφορα θέματα, τα οποία προσφέρουν την δυνατότητα της ανώνυμης δημοσίευσης περιεχομένων.

2.3.2 Κρυπτογραφία και ασφάλεια στο Tor

Οι επικοινωνίες στο Tor Network διασφαλίζονται με τη χρήση κρυπτογραφικού αλγόριθμου ροής, αλγόριθμου δημόσιου κλειδιού, αλγόριθμου κατακερματισμού και του πρωτοκόλλου Diffie- Hellman. Ως αλγόριθμος ροής χρησιμοποιείται ο 128 bit AES. Ως αλγόριθμος δημόσιου κλειδιού χρησιμοποιείται ο RSA με κλειδιά 1024 bits.

Όπως αναφέρθηκε και παραπάνω, το Tor Network είναι ένα κατανεμημένο επικαλυπτικό δίκτυο, που είναι σχεδιασμένο να προσφέρει ανωνυμία σε εφαρμογές, οι οποίες βασίζονται στο πρωτόκολλο TCP. Οι πελάτες (clients) επιλέγουν ένα μονοπάτι στο δίκτυο και δημιουργούν ένα κύκλωμα. Η κίνηση στο κύκλωμα γίνεται με σταθερού μεγέθους κελιά, τα οποία μειώνονται σε κάθε κόμβο κατά ένα με τη χρήση ενός

συμμετρικού κλειδιού και στη συνέχεια αναμεταδίδονται στον επόμενο κόμβο, όπου συμβαίνει η αντίστοιχη διαδικασία.

Κάθε κόμβος Tor έχει πολλαπλά ζευγάρια δημόσιων/ιδιωτικών κλειδιών. Ο αλγόριθμος RSA 1024-bit χρησιμοποιείται στα παρακάτω κλειδιά:
α) Σε ένα μακροχρόνιο κλειδί ταυτότητας, που χρησιμοποιείται αποκλειστικά για την υπογραφή εγγράφων και πιστοποιητικών και για την εγκατάσταση ταυτότητας ενός αναμεταδότη.
β) Σε ένα μεσοπρόθεσμο κλειδί onion, το οποίο χρησιμοποιείται για αποκρυπτογράφηση των επιπέδων onion, όταν το κύκλωμα του δικτύου επεκτείνεται. Τα παλαιά κλειδιά θα πρέπει να γίνονται αποδεκτά για τουλάχιστον μια εβδομάδα μετά από το πέρας της κοινοποίησης τους. Έτσι, οι αναμεταδότες του δικτύου θα πρέπει να διατηρούν και τα παλαιότερα κλειδιά.
γ) Σε ένα βραχυπρόθεσμο κλειδί σύνδεσης, που χρησιμοποιείται για τις συνδέσεις TLS. Αυτό το κλειδί μπορεί να εναλλάσσεται συχνά, ενώ θα πρέπει να αλλάζει τουλάχιστον μια φορά την ημέρα.
Ο αλγόριθμος Ed25519 χρησιμοποιείται:
α) Για μακροπρόθεσμο κλειδί κύριας ταυτότητας. Αυτό το κλειδί δεν αλλάζει ποτέ και χρησιμοποιείται για την υπογραφή του κλειδιού υπογραφής.
β) Για μεσοπρόθεσμο κλειδί υπογραφής. Αυτό το κλειδί υπογράφεται από το κλειδί της κύριας ταυτότητας και πρέπει πάντα να είναι online και θα πρέπει να ανανεώνεται περιοδικά.
γ) Για βραχυπρόθεσμο κλειδί, για αυθεντικοποίηση συνδέσμου.
Το κλειδί ταυτότητας RSA και το κλειδί κύριας ταυτότητας Ed25519 μαζί, δίνουν ταυτότητα σε ένα δρομολογητή του δικτύου.

Στις συνδέσεις μεταξύ δυο αναμεταδοτών Tor ή μεταξύ πελάτη και αναμεταδότη χρησιμοποιείται το πρωτόκολλο TLS/SSLv3, για αυθεντικοποίηση του συνδέσμου και για κρυπτογράφηση. Όλες οι εφαρμογές θα πρέπει να υποστηρίζουν την σουίτα SSLv3 TLS-DHE-RSA-WITH-AES-128-CBC-SHA, δηλαδή τα πρωτόκολλα TLS, Diffie-Hellman με αλγόριθμους κρυπτογράφησης RSA με AES 128 bit και CBC-SHA, ενώ θα πρέπει να υποστηρίζουν και τις προηγμένες σουίτες κρυπτογράφησης.

Υπάρχουν τρεις τρόποι για να πραγματοποιηθεί χειραψία TLS με έναν Tor Server:
α) Ο πρώτος τρόπος είναι ο "certificates up-front", δηλαδή στην αρχική χειραψία τόσο ο πομπός όσο και ο δέκτης δημιουργούν μια αλυσίδα δυο πιστοποιητικών. Σε αυτή τη μέθοδο το στοιχείο του δικτύου που ξεκινάει τη σύνδεση θα πρέπει να αποστείλει μια αλυσίδα δυο πιστοποιητικών. Στην αλυσίδα θα περιλαμβάνεται ένα πιστοποιητικό X.509 με βραχυπρόθεσμη σύνδεση δημόσιου κλειδιού και ένα δεύτερο αυτό- υπογραφόμενο κλειδί X. 509, το οποίο αποτελεί το κλειδί της ταυτότητας του, ενώ και ο δεύτερος χρήστης αποστέλλει την ίδια αλυσίδα πιστοποιητικών.

β) Ο δεύτερος τρόπος είναι ο παραλήπτης να δίνει ένα πιστοποιητικό και ο αποστολέας να πραγματοποιεί επαναδιαπραγμάτευση του TLS. Σε αυτή τη μέθοδο, το στοιχείο του δικτύου που ξεκινάει την σύνδεση δεν αποστέλλει κανένα πιστοποιητικό. Αυτός που αποστέλλει πιστοποιητικό είναι ο παραλήπτης. Μόλις ολοκληρωθεί η χειραψία TLS, το στοιχείο του δικτύου που ξεκινάει τη σύνδεση επαναδιαπραγματεύεται τη χειραψία, με κάθε μέρος να αποστέλλει πιστοποιητικά, όπως με την μέθοδο "certificates up-front". Ωστόσο, το στοιχείο του δικτύου που ξεκινάει την σύνδεση δεν θα πρέπει να περιλαμβάνει τις τρεις σουίτες που αναφέρθηκαν την μέθοδο "certificates up-front", προκειμένου να γνωρίζει ο παραλήπτης ποια μέθοδος ακολουθείται.

γ) Στον τρίτο τρόπο με την ολοκλήρωση της επαναδιαπραγμάτευσης TLS, τα μέρη που συμμετέχουν πραγματοποιούν επαλήθευση της ταυτότητας τους με τη χρήση του πρωτοκόλλου Tor. Σε αυτή τη μέθοδο (in "protocol"), το στοιχείο του δικτύου που ξεκινάει την σύνδεση δεν αποστέλλει κανένα πιστοποιητικό, ενώ αυτός που αποστέλλει ένα πιστοποιητικό είναι ο παραλήπτης. Το πιστοποιητικό σε αυτή τη μέθοδο θα πρέπει να είναι αυτό – υπογεγραμμένο.

Κάθε μέθοδος από αυτές που περιεγράφηκαν ανωτέρω, έχουν ως σκοπό όλα τα μέρη του δικτύου να μπορούν να επικοινωνούν μεταξύ τους, χωρίς να χρειάζεται να γνωρίζουν ποια έκδοση Tor χρησιμοποιεί ο καθένας. Σε όλες τις παραπάνω παραλλαγές χειραψίας, τα πιστοποιητικά αποστέλλονται σε καθαρό κείμενο και απαγορεύεται να περιλαμβάνονται δεδομένα τα οποία προδίδουν τη χρήση του πρωτοκόλλου TOR. Σε όλους τους τρόπους χειραψίας, όταν πραγματοποιηθεί ανταλλαγή των πιστοποιητικών πρέπει να γίνει επιβεβαίωση ότι το κλειδί ταυτότητας είναι αυτό που αναμένονταν. Όταν

πραγματοποιείται σύνδεση σε έναν Onion Router, όλα τα μέρη πρέπει να απορρίπτουν τη σύνδεση αν το πιστοποιητικό είναι ακατάλληλο ή εάν δεν υπάρχει πιστοποιητικό. [10]

2.4 I2P - Garlic Routing

Το I2P είναι ένα ανώνυμο δίκτυο επικάλυψης που χρησιμοποιεί την τεχνική Garlic Routing και έχει ως πηγή έμπνευσης το Tor. Ουσιαστικά πρόκειται για συνδυασμό ενός ή περισσότερων κελιών Onion με συμπληρωμένη επιπλέον πρόσθετη πληροφορία τυχαίου μεγέθους. Η μορφή των κελιών του I2P είναι ίδια με του Onion Routing, αλλά τα κελιά δεν αποστέλλονται ποτέ μόνα τους. Αντιθέτως, ομαδοποιούνται μαζί με επιπλέον πληροφορίες. Τα κελιά συσκευάζονται σε "σκελίδες σκόρδου" (Garlic cloves) και στη συνέχεια προωθούνται στους επόμενους κόμβους, σε κρυπτογραφημένη μορφή. Το μέγεθος της "σκελίδας" και ο αριθμός των Onion κελιών που περιλαμβάνονται σε μια σκελίδα, διαφέρει μεταξύ των κόμβων, προκειμένου να υπάρχει επιπλέον τυχαιότητα. Όταν ένας κόμβος I2P παραλαμβάνει κρυπτογραφημένες "σκελίδες", μπορεί να τις αποκρυπτογραφήσει και να ενεργεί σε κάθε κελί Onion ανεξάρτητα, είτε καθυστερώντας το, είτε δίνοντας προτεραιότητα, ανάλογα με τις ενσωματωμένες οδηγίες. Κάθε I2P κόμβος μπορεί να ανασκευάσει τα ληφθέντα κελιά onion χρησιμοποιώντας νέες κρυπτογραφημένες "σκελίδες σκόρδου" και να τις στείλει σε άλλους I2P κόμβους. Αυτό δημιουργεί ένα σύστημα που βασίζεται σε μηνύματα και όχι σε κυκλώματα, όπως γίνεται στο δίκτυο Tor. Εάν δυο χρήστες χρησιμοποιούν τον I2P Client, μπορούν να αποστείλουν πληροφορίες πλήρως κρυπτογραφημένες και έτσι μπορούν να αποφύγουν τις από άκρο σε άκρο επιθέσεις. [29]

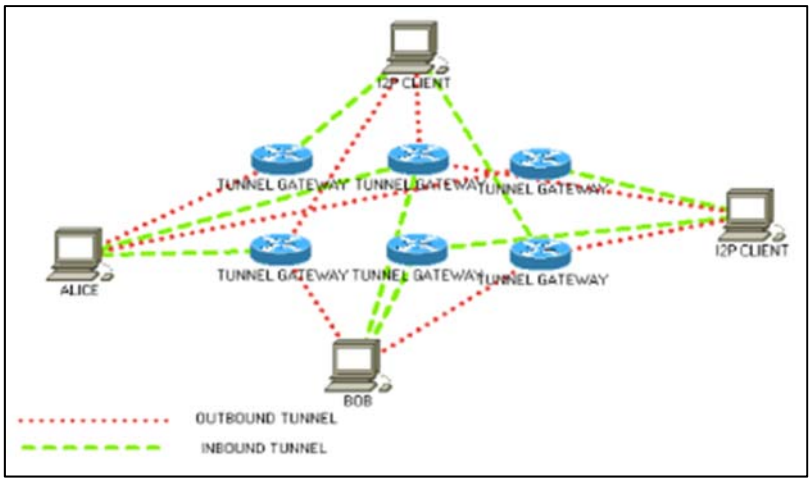
Αρχικά, οι χρήστες του I2P θα πρέπει ψάξουν κάποιο διαθέσιμο κόμβο I2P και έτσι να συνδεθούν στο ανώνυμο σύστημα I2P. Προκειμένου το δίκτυο να είναι αποδοτικό, χρησιμοποιούνται κάποιοι hosts, οι οποίοι θεωρούνται αξιόπιστοι, για να εισέλθουν οι χρήστες στο δίκτυο I2P. Εάν η διαδικασία με τους προκαθορισμένους hosts αποτύχει, τότε το λογισμικό πελάτης του I2P μπορεί να επιλέξει άλλες IP διευθύνσεις μέχρι να πραγματοποιηθεί σύνδεση. Όταν υλοποιηθεί η σύνδεση, ο πελάτης ψάχνει για άλλους κόμβους και ξεκινάει να υλοποιεί νέες σήραγγες. Με τη δημιουργία κάθε νέας σήραγγας, ο πελάτης στέλνει αιτήσεις σε ήδη υπάρχοντες κόμβους, προκειμένου να συνδεθεί μαζί τους.

Αρχικά, οι τελικοί χρήστες του I2P επιλέγουν γρήγορους ή με υψηλή χωρητικότητα I2P κόμβους, έτσι ώστε οι σήραγγες να είναι αξιόπιστες για την αποστολή και τη λήψη δεδομένων. Στη συνέχεια, δημιουργούν ακόμη ένα ζευγάρι εισερχόμενης και εξερχόμενης σήραγγας, που ονομάζονται ερευνητικές σήραγγες και επικοινωνούν με κόμβους μικρότερης χωρητικότητας. Αυτό συμβαίνει για να βρεθούν νέοι διαθέσιμοι κόμβοι και να αποκτηθούν πληροφορίες της NetDB (μια διαδικτυακή βάση δεδομένων που περιέχει πληροφορίες σχετικά με τους κόμβους του I2P) .

Η NetDB, έχει δυο είδη δεδομένων, το RouterInfo και το LeaseSets. Το RouterInfo δίνει στον χρήστη ή στον κόμβο του συστήματος πληροφορίες για να επικοινωνήσει με συγκεκριμένο κόμβο στο δίκτυο. Οι πληροφορίες στο RouterInfo δεν αλλάζουν συχνά, καθώς οι χρήστες είναι συνδεμένοι σε συγκεκριμένες πύλες (gateways).

Το LeaseSets δίνει πληροφορίες σχετικά με τους κόμβους από τους οποίους θα μεταφέρονται τα δεδομένα. Επιπλέον, περιέχει τη διεύθυνση της σήραγγας προορισμού, τα δημόσια κλειδιά και το χρόνο που η σήραγγα είναι online, προκειμένου να εξάγει συμπέρασμα σχετικά με την αξιοπιστία του δρομολογίου. Τα LeaseSets των κόμβων αλλάζουν συχνά, καθώς οι χρήστες αλλάζουν σήραγγες κάθε 10 λεπτά. [29]

Κάθε I2P κόμβος έχει εγκατεστημένες εισερχόμενες και εξερχόμενες σήραγγες, οι οποίες είναι συνδεδεμένες με I2P πύλες (gateways). Ο αριθμός των σηράγγων μπορεί να αυξηθεί για να σχηματιστούν νέα δρομολόγια με τη σύνδεση νέων πυλών I2P. Όταν ένα μήνυμα πρέπει να προωθηθεί από έναν αποστολέα σε έναν παραλήπτη, δρομολογείται από την εξερχόμενη σήραγγα στη πύλη I2P και από εκεί δρομολογείται μέσω διαφόρων αναπηδήσεων σε κόμβους, στην πύλη του παραλήπτη. Ακολούθως, στη σήραγγα εισερχόμενων του παραλήπτη και στην συνέχεια αποκρυπτογραφείται στον κόμβο του παραλήπτη. Ο αποστολέας δεν έχει καμιά πληροφορία για το δρομολόγιο που θα ακολουθήσει το μήνυμα, αλλά μόνο για την πύλη από την οποία θα αποσταλεί. Κάθε I2P δρομολογητής μπορεί να προσθέσει καθυστέρηση και νέες πληροφορίες σχετικά με το δρομολόγιο.



Εικόνα 8 [Πηγή: Zantout, B., & Haraty, R. (2011) I2P data communication system**]**

Στην εικόνα ο Bob αποστέλλει στην Alice πληροφορίες ακολουθώντας την παρακάτω διαδικασία:

1. Στέλνει ερώτημα στη βάση δεδομένων NetDB, προκειμένου να λάβει πληροφορίες σχετικά με την ταυτότητα και τα κλειδιά κρυπτογράφησης του Router, τα δημόσια κλειδιά του προορισμού και την προσβασιμότητα των πυλών (gateways) και των προορισμών. Αυτές οι πληροφορίες αποθηκεύονται στην NetDB σε δυο κατηγορίες: RouteInfo και LeaseSet.
2. Στέλνει μηνύματα μέσω της εξερχόμενης σήραγγας στον δρομολογητή, ο οποίος στέλνει την ροή των δεδομένων στην εισερχόμενη σήραγγα της Alice.
3. Λαμβάνοντας απόκριση από την Alice μέσω της εξωτερικής της σήραγγας ο I2P δρομολογητής στέλνει δεδομένα στην εισερχόμενη σήραγγα του Bob.

Παρατηρούμε ότι το δίκτυο I2P δεν έχει κόμβους εξόδου ή εισόδου, όπως συμβαίνει με το δίκτυο Tor, αλλά τα δεδομένα είναι κρυπτογραφημένα από άκρο σε άκρο μεταξύ των ομότιμων χρηστών του δικτύου. Προκειμένου να επιτευχθεί αυτό, και οι δυο χρήστες θα πρέπει να είναι συνδεδεμένοι στο I2P δίκτυο και τουλάχιστον σε ένα κόμβο I2P με μια εισερχόμενη και μια εξερχόμενη σήραγγα. Ο αριθμός των σηράγγων εξαρτάται από τον χρήστη, ωστόσο η προκαθορισμένη ρύθμιση είναι τέσσερις σήραγγες, δυο εισερχόμενες και δυο εξερχόμενες. Αυτό συμβαίνει προκειμένου να υπάρχει εναλλακτική λύση, σε περίπτωση που ένα από τα δυο ζευγάρια σταματήσει τη λειτουργία του. Επιπλέον, με τη δημιουργία νέων σηράγγων δημιουργούνται περισσότερα δρομολόγια για ένα

προορισμό. Οι χρήστες I2P έχουν τη δυνατότητα να επιλέξουν τον αριθμό των αναπηδήσεων (hops) της διαδρομής για ένα προορισμό. Η δημιουργία των σηράγγων εξαρτάται από τον χρόνο, καθώς κάθε 10 λεπτά γίνεται αλλαγή προς αποφυγή των επιθέσεων στην κρυπτογραφία των σηράγγων. Ακόμη και εάν η κρυπτογραφία στις σήραγγες παραβιαστεί, τα πακέτα σε ένα Garlic Clove, χρησιμοποιούν πολυεπίπεδα σύγχρονα και ασύγχρονα κρυπτογραφικά πρότυπα για να διασφαλίσουν την ακεραιότητα των δεδομένων και την ανωνυμία. [29]

Το I2P μπορεί να εξασφαλίσει από άκρο σε άκρο ιδιωτικότητα και ακεραιότητα ανάμεσα σε δυο ομότιμους χρήστες, που επικοινωνούν μέσω του δικτύου. Ωστόσο, κάποιοι κόμβοι στο δίκτυο διαθέτουν Proxies εξόδου, που επιτρέπουν στους χρήστες να συνδέονται με προορισμούς που βρίσκονται στο διαδίκτυο. Οι εξερχόμενες, από το σύστημα ανωνυμίας, συνδέσεις, δεν προσφέρουν καμία κρυπτογράφηση όταν φθάνουν στον προορισμό τους. Όταν υπάρξει απόκριση από τον τελικό προορισμό, αυτή αποστέλλεται πίσω στον αρχικό αποστολέα. Για να αποσταλούν πίσω στον αποστολέα τα Garlic Cloves, ο κόμβος εξόδου θα τα επανακρυπτογραφήσει και θα τα ανασκευάσει.

Το I2P προσφέρει στους χρήστες κρυφές υπηρεσίες, όπως προσφέρει το Tor. Κάποιες από αυτές τις κρυφές υπηρεσίες είναι δημοσιευμένες ανώνυμα και η IP ή ταυτότητα τους δεν αποκαλύπτεται στους επισκέπτες. [29] Προκειμένου οι χρήστες του I2P να έχουν εύκολη πρόσβαση στις κρυφές υπηρεσίες του, υπάρχει μια γενική βιβλιοθήκη ονομασίας, η οποία επεξεργάζεται και χαρτογραφεί τα ονόματα των υπηρεσιών και ένας κατάλογος διευθύνσεων (address book). Το I2P υποστηρίζει την Base32, για την ονομασία των hostnames.

Το βιβλίο διευθύνσεων είναι ένα ασφαλές, κατανεμημένο και αναγνωρίσιμο από το χρήστη σύστημα ονομασίας. Η αναγνωσιμότητα ισχύει μόνο τοπικά για τον χρήστη, καθώς δυο χρήστες μπορούν να έχουν καταχωρημένο με το ίδιο όνομα δυο διαφορετικές υπηρεσίες ή προορισμούς.

Δεν υπάρχει κάποια κεντρική αρχή για το σύστημα ονομασίας, γιατί τα hostnames είναι τοπικά. Το σύστημα ονομασίας είναι αρκετά απλό, το μεγαλύτερο μέρος του υλοποιείται σε εφαρμογές εκτός του δρομολογητή και είναι προεγκατεστημένο στη διανομή του I2P.

Τα συστατικά του μέρη είναι:

α. Η τοπική υπηρεσία ονοματοδοσίας που αναζητά και χειρίζεται τα ονόματα κεντρικών υπολογιστών.

β. Ο διακομιστής μεσολάβησης HTTP που οδηγεί τον χρήστη σε υπηρεσίες απομακρυσμένης βοήθειας όταν προκύψουν ανεπιτυχείς αναζητήσεις.

γ. Οι φόρμες HTTP για κεντρικούς υπολογιστές που επιτρέπουν στους χρήστες να προσθέσουν κεντρικούς υπολογιστές στους τοπικούς υπολογιστές τους

δ. Οι υπηρεσίες HTTP Jump που παρέχουν τις δικές τους αναζητήσεις.

ε. Η εφαρμογή addressbook που συγχωνεύει λίστες εξωτερικών κεντρικών υπολογιστών, ανάκτησης μέσω HTTP, με την τοπική λίστα.

στ. Η εφαρμογή SusiDNS, η οποία είναι ένα απλό front-end web για τη διαμόρφωση του καταλόγου διευθύνσεων και την προβολή των τοπικών λιστών υποδοχής.

Όλοι οι προορισμοί στο I2P αναπαρίστανται σε Base64 και περιέχουν ένα δημόσιο κλειδί μεγέθους 256 byte και ένα κλειδί υπογραφής μεγέθους128 bytes. Κάθε χρήστης έχει μια Blockfile υπηρεσία ονομασίας η οποία πραγματοποιεί μια απλή γραμμική αναζήτηση σε τρία τοπικά αρχεία (privatehosts.txt, userhosts.txt, hosts.txt), προκειμένου να αναζητήσει τα ονόματα των κεντρικών υπολογιστών και να τα μετατρέψει σε ένα κλειδί προορισμού μεγέθους 516 bytes. Η Blockfile υπηρεσία ονομασίας αποθηκεύει τα πολλαπλά "βιβλία διευθύνσεων" σε ένα ενιαίο αρχείο βάσης δεδομένων που ονομάζεται hostsdb.blockfile.

Η εφαρμογή addressbook λαμβάνει τα αρχεία hosts.txt άλλων χρηστών τακτικά και τα συγχωνεύει με το τοπικό hosts.txt, μετά από αρκετούς ελέγχους. Οι συγκρούσεις ονομάτων επιλύονται με βάση το first-come first-served. Η εγγραφή στο αρχείο hosts.txt ενός άλλου χρήστη συνεπάγεται τη διασφάλιση εμπιστοσύνης προς τον χρήστη. Το βιβλίο διευθύνσεων περιλαμβάνει μια δικτυακή διεπαφή, η οποία ονομάζεται SusiDNS και διαμορφώνει τις εγγραφές και την πρόσβαση στα τέσσερα αρχεία του βιβλίου διευθύνσεων. Διαχειρίζεται το address book και αποτελεί μέρος ενός απλού, ελεγχόμενου από τον χρήστη συστήματος ονοματοδοσίας του I2P, κάπως ανάλογου με το DNS (Domain Name System) του Διαδικτύου. Το βιβλίο διευθύνσεων αντιστοιχεί τους προορισμούς που αναπαρίστανται σε Base64, σε ονόματα τομέα, τα οποία είναι αναγνωρίσιμα από τους ανθρώπους και τελειώνουν με πρόθεμα .i2p. Ο I2P router μπορεί

να αναλύσει τοπικά αυτές τις διευθύνσεις σε Base64. Προς το παρόν υπάρχει ελάχιστη επιβολή των κανόνων ονοματοδοσίας του addressbook στο SusiDNS, οπότε ο χρήστης μπορεί να εισάγει τοπικά ονόματα κεντρικών υπολογιστών, τα οποία θα απορρίπτονται από τους κανόνες εγγραφής του βιβλίου διευθύνσεων. [38]

2.4.1 Εφαρμογές I2P

Το I2P σχεδιάστηκε ώστε να υποστηρίζει λογισμικό και εφαρμογές που χρησιμοποιούνται για ανώνυμη επικοινωνία. Οι εφαρμογές που υποστηρίζονται αναπτύχθηκαν ως plug-ins πάνω στο σύστημα I2P και είναι οι παρακάτω:

1. Chat

Το I2P υποστηρίζει την ανώνυμη επικοινωνία μεταξύ των χρηστών σε πραγματικό χρόνο με τις παρακάτω εφαρμογές:

α. I2P-Messenger

Αποτελεί ένα απλό και αποκεντρωμένο messenger βασισμένο στο λογισμικό Qt, που διασφαλίζει την κρυπτογραφημένη επικοινωνία από άκρο σε άκρο. Δεν υπάρχουν διακομιστές προκειμένου να καταγράψουν τα στοιχεία μιας συνομιλίας, ενώ με την κρυπτογραφημένη επικοινωνία αποτρέπεται κάποιος ενδιάμεσος κόμβος να έχει πρόσβαση σε μη-κρυπτογραφημένα δεδομένα. Μέσω του I2P-Messenger, μπορούν να επικοινωνήσουν χρήστες που είναι γνωστοί μεταξύ τους αλλά και χρήστες που είναι άγνωστοι. Προκειμένου να επιτευχθεί η επικοινωνία μεταξύ των χρηστών θα πρέπει να ανταλλάξουν τα κλειδιά προορισμού. Τέλος υποστηρίζει την μεταφορά αρχείων και την αναζήτηση άλλων χρηστών.

β. IRC Clients

Πολλοί πελάτες IRC διαρρέουν πληροφορίες ταυτοποίησης σε διακομιστές ή σε άλλους πελάτες. Οι I2P IRC και οι SOCKS IRC φιλτράρουν τα εξερχόμενα και εισερχόμενα μηνύματα για να καθαρίσουν δεδομένα όπως η τοπική διεύθυνση IP, οι εξωτερικές διευθύνσεις IP, τα τοπικά hostnames, το όνομα και την έκδοση του IRC client. Δύο είδη μηνυμάτων τα DCC (Direct Client-to-Client) και CTCP (Client-to-client protocol) δεν μπορούν να υποστηρίξουν πρωτόκολλα ανωνυμίας και για αυτό αποκλείονται.

Οι πιο γνωστοί πελάτες IRC είναι:

1) jIRCii ο οποίος έχει συνταχθεί στην γλώσσα προγραμματισμού sleep που βασίζεται στην Java και υποστηρίζει γραφικό περιβάλλον.
2) Xchat που αποτελεί ένα IRC client, με γραφικό περιβάλλον διεπαφής χρήστη που επιτρέπει την ταυτόχρονη συμμετοχή σε πολλαπλά κανάλια IRC, τον δημόσιο διάλογο και τις ιδιωτικές συνομιλίες, ενώ είναι δυνατή και η μεταφορά αρχείων.
3) Irssi που έχει συνταχθεί σε γλώσσα C, με περιβάλλον διεπαφής κειμένου. Περιέχει ενσωματομένες τις λειτουργίες της διαχείρησης παραθύρων, του εξομοιωτή, του πολυπλέκτη του τερματικού, της απομακρυσμένης σύνδεσης και του προσαρμογέα IRC.
4) WeeChat ο οποίος αποτελεί ένα IRC client με περιβάλλον διεπαφής κειμένου, έχει συνταχθεί σε C και υποστηρίζει IPv6, SSL, συνδέσεις Proxy, ενώ υπάρχει η δυνατότητα επέκτασής του με άλλες γλώσσες προγραμματισμού.

Οι υποστηριζόμενοι IRC servers είναι:

1) ngIRCd, ο οποίος είναι ένας δωρεάν, φορητός και ελαφρύς IRC διακομιστής για μικρά ή ιδιωτικά δίκτυα που αναπτύχθηκε υπό την GNU General Public License.

β) UnrealIRCd που αποτελεί ένα IRC διακομιστή ανοιχτού κώδικα. Τα κύρια χαρακτηριστικά του είναι ότι υποστηρίζει το SSL και έχει προηγμένα anti-flood και anti-spam συστήματα.

γ. Jabber ή Extensive Message and Presence Protocol (XMPP)

Είναι ένα ανοιχτό πρωτόκολλο άμεσης επικοινωνίας βασισμένο στο XML (Extensive Markup Language). Είναι σχεδιασμένο έτσι ώστε να είναι επεκτάσιμο και μπορεί να χρησιμοποιηθεί σε συστήματα δημοσίευσης και συνδρομής (subscribe), για VoIP, για επικοινωνία με φωνή και βίντεο, για μεταφορά αρχείων, για εφαρμογές του Internet of Things και για υπηρεσίες κοινωνικής δικτύωσης.

2. Διαμοιρασμός αρχείων

α. Bit Torrent Clients

Το I2P προσφέρει ένα ασφαλές στρώμα για εφαρμογές που επικοινωνούν ανώνυμα μεταξύ τους. Αυτό το στρώμα το εκμεταλλεύονται εφαρμογές διαμοιρασμού αρχείων και Bit Torrent Clients. Οι σημαντικότεροι Bit Torrent Clients στο δίκτυο I2P είναι οι παρακάτω:

1) I2Psnark

Το I2Psnark περιλαμβάνεται στο πακέτο εγκατάστασης του I2P (http://127.0.0.1:7657/i2psnark/), είναι ένα ελεύθερο λογισμικό και αποτελεί εισαγωγή του Bit Torrent Client Snark στο δίκτυο I2P. Προσφέρει ανώνυμο πρόγραμμα Bit Torrent client με δυνατότητες λήψης πολλαπλών Torrents. Το I2PSnark μπορεί να λειτουργήσει ως δημιουργός torrent, ως micro http διακομιστής για την μεταφορά αρχείων metainfo.torrent και έχει ενσωματωμένο Tracker για την διευκόλυνση της κοινής χρήσης αρχείων.

2) Robert

Το Robert αποτελεί Bit Torrent client, που ενισχύει την ασφάλεια και την κρυπτογράφηση των ομότιμων χρηστών και των σηράγγων του δικτύου I2P. Το λογισμικό χρησιμοποιεί Torrents, αλλά δεν είναι συμβατό με συνδέσμους magnet. Είναι ένα δωρεάν λογισμικό ανοιχτού κώδικα που βασίζεται στην γλώσσα προγραμματισμού Python. Το Robert μπορεί να αλληλοεπιδράσει με το Seedless, που αποτελεί μια εισαγωγή του NeoDatis Object DB στο δίκτυο I2P. Αυτό επιτρέπει στο Robert την περιήγηση, τη λήψη αρχείων από την βάση δεδομένων και τον εντοπισμό ομότιμων χρηστών από το Seedless.

Το Robert παρέχει Bit Torrent λειτουργία εντός του δικτύου I2P. Κάθε ομότιμος χρήστης βασίζεται στο ότι μπορεί να έχει πρόσβαση στο δίκτυο I2P και να λαμβάνει αρχεία Torrent. Οι χρήστες δε μπορούν να συνδεθούν σε Torrents εκτός δικτύου I2P και αντίστοιχα τα I2P torrents δεν μπορούν να διαμοιραστούν εκτός δικτύου.[45]

3) I2P Transmission

Το Transmission αποτελεί έναν Bit Torrent client ανοικτής πηγής που χρησιμοποιείται για τον διαμοιρασμό αρχείων μεταξύ ομότιμων χρηστών. Έχει τέσσερις διαφορετικούς πελάτες:

α) Daemon/Web, με τον οποίο μπορεί να εκτελεστεί ο Bit torrent πελάτης σε διακομιστή χωρίς κεφαλίδες και τα torrent μπορούν να προστεθούν και να ελεγχθούν με την χρήση ενός Web GUI.

β) GLI/Remote: είναι ένας client που λειτουργεί με εντολές και μπορεί να τρέξει μόνος του (stand alone) ή να ελέγχει το Daemon.

γ) GTK: είναι ένας stand alone πελάτης.

δ) QT: είναι ένας stand alone και απομακρυσμένος πελάτης για το daemon. [40]

4) Vuze

Το Vuze είναι ένας Bit Torrent Client, που χρησιμοποιείται για διαμοιρασμό αρχείων πρωτοκόλλου Bit Torrent, μεταξύ ομότιμων χρηστών. Επιπλέον, υπάρχει η δυνατότητα παρακολούθησης, λήψης και διαμοιρασμού βίντεο. Το περιεχόμενο παρουσιάζεται μέσω καναλιών και κατηγοριών πχ TV shows, μουσική, ταινίες, video games κλπ. Το Vuze είναι ο μόνος client που καθιστά τα torrents του Surface web, διαθέσιμα στο δίκτυο I2P και αντίστροφα. Αν ένας χρήστης προσθέσει ένα torrent από το I2P, θα γίνεται seeding τόσο από το δίκτυο I2P, όσο και από το Surface web. Τα Torrents που έχουν δημοσιοποιηθεί στο δίκτυο I2P, πρέπει να δημοσιεύονται και στο Surface Web, οι χρήστες του I2P μπορούν να λάβουν οποιοδήποτε torrent και παράλληλα να διατηρούν την ανωνυμία τους.[39]

β. ED2K

Imule

Αποτελεί ένα δωρεάν, ανοικτού κώδικα λογισμικό, που χρησιμοποιείται για τον ανώνυμο διαμερισμό αρχείων μεταξύ ομότιμων χρηστών. Το Imule βασίζεται στον κώδικα του aMule και χρησιμοποιεί τον αλγόριθμο Kademlia. Πρόκειται για ένα φορητό λογισμικό που λειτουργεί σε πολλαπλές πλατφόρμες με την χρήση της βιβλιοθήκης wxWidgets.

γ. Gnutella

I2Phex

Το Phex είναι ένας client διαμοιρασμού αρχείων μεταξύ ομότιμων χρηστών για το δίκτυο Gnutella. Το I2Phex αποτελεί μια ανώνυμη έκδοση του Phex, που εκμεταλλεύεται το δίκτυο I2P προκειμένου να αποκρύψει τα στοιχεία των χρηστών. Για να επιτύχει την ανωνυμία το I2Phex, αντί να χρησιμοποιεί την δημόσια IP του δικτύου, χρησιμοποιεί τις κρυπτογραφημένες σήραγγες του δικτύου I2P. Η κίνηση αναμιγνύεται με την υπόλοιπη κίνηση του δικτύου μέσω του Garlic Routing, αποτρέποντας από ένα τρίτο πρόσωπο να παρατηρήσει τα δεδομένα που ανταλλάσσονται και τα μέρη που συμμετέχουν στην διακίνηση. [43]

3. Δημοσίευση blogs, forums και newsgroups

Το I2P υποστηρίζει την δημιουργία και την δημοσίευση περιεχομένου σε blog. Τα υποστηριζόμενα εργαλεία είναι τα παρακάτω:

α) Pebble Plug-in

Το Pebble είναι ένα blogging εργαλείο, ανοιχτού κώδικα, γραμμένο σε Java. Το περιεχόμενο του blog αποθηκεύεται σε αρχεία με τη μορφή XML. Το Pebble περιλαμβάνει τις διεπαφές Blogger και MetaWeblog API και η δημοσίευση μπορεί να πραγματοποιηθεί μέσω συμβατών εργαλείων. Υποστηρίζει την κατηγοριοποίηση και την σήμανση του περιεχομένου, ενώ υπάρχει η δυνατότητα δημοσίευσης αρχείων και εικόνων. Παράλληλα, δίνει την δυνατότητα απόκρισης από τους αναγνώστες του blog και ειδοποίησης σε email όταν ληφθούν νέες αποκρίσεις. Η διαχείριση και συντήρηση μπορεί να γίνει μέσω Web browser, κάτι που διευκολύνει την πρόσβαση του από τον διαχειριστή**.** [42]

β) Syndie

Το Syndie είναι μια εφαρμογή ανοιχτού κώδικα, που χρησιμοποιείται για την δημοσίευση δεδομένων σε ανώνυμα και μη δίκτυα. Επιτρέπει την ιδιωτική και δημόσια ανάρτηση δεδομένων, ενώ όταν κοινοποιούνται ιδιωτικά δεδομένα μόνο εξουσιοδοτημένοι χρήστες μπορούν να έχουν πρόσβαση σε αυτά. Στις δημόσιες κοινοποιήσεις όλοι οι χρήστες μπορούν να σχολιάσουν ή να απαντήσουν σε σχόλιο. Τα δεδομένα αποθηκεύονται σε διακομιστές αρχείων στο δίκτυο I2P και ταυτόχρονα, αποθηκεύονται από όλους τους χρήστες που συμμετέχουν στο forum προσφέροντας τη δυνατότητα ανάκτησης τους από κάθε χρήστη. Τα παραπάνω δημιουργούν μια αποκεντροποιημένη μορφή. Το Syndie, επιτρέπει την συμμετοχή ενός χρήστη ακόμη και όταν είναι offline, συγχρονίζοντας τις αλλαγές όταν ο χρήστης επανέλθει online. Δεν σχεδιάστηκε για διαμοιρασμό αρχείων, ωστόσο μπορούν να επισυνάπτονται αρχεία με μέγιστο μέγεθος τα 512 kb.[50]

4. Email

α. I2P-Bote

Το I2P-Bote είναι ένα δωρεάν, αποκεντρωμένο, κατανεμημένο και ανώνυμο σύστημα email, που μπορεί να εγκατασταθεί ως I2P plug-in. Είναι προσβάσιμο μέσω της δικτυακής κονσόλας του I2P και λειτουργεί με τα πρωτόκολλα email IMAP και SMTP. Υποστηρίζει τις διαφορετικές ταυτότητες και δεν εκθέτει τις κεφαλίδες των email. Όλα τα bote-mails είναι κρυπτογραφημένα από άκρο σε άκρο, δεν χρειάζεται ρύθμιση κρυπτογράφησης των emails και η πιστοποίησή της γίνεται αυτόματα. Τα ηλεκτρονικά μηνύματα

υπογράφονται με το ιδιωτικό κλειδί του αποστολέα, επομένως δεν απαιτείται κάποια ρύθμιση με PGP (Pretty Good Privacy) ή με άλλο λογισμικό κρυπτογράφησης. Επειδή είναι αποκεντρωμένο σύστημα, δεν απαιτείται διακομιστής email. Οι κόμβοι που αναμεταδίδουν τα emails δεν γνωρίζουν τον αποστολέα και τον παραλήπτη, μόνο ο τελικός κόμβος και οι κόμβοι αποθήκευσης γνωρίζουν την διεύθυνση bote-email της πηγής και του δέκτη.

β. Susimail

Το Susimail είναι ένας Web-based email πελάτης για το δίκτυο I2P που βασίζεται στη γλώσσα προγραμματισμού Java. Το I2P διαθέτει μια ψευδώνυμη υπηρεσία email η οποία ονομάζεται «Postman» και υποστηρίζει τα πρωτόκολλα POP3 και SMTP. Το Susimail σχεδιάστηκε για να εκμεταλλεύεται τους διακομιστές του «Postman», δίνοντας μεγάλη σημασία στην ανωνυμία και την ασφάλεια. Περιλαμβάνεται στο πακέτο του I2P και ο χρήστης μπορεί να έχει πρόσβαση σε αυτό, μέσω της δικτυακής διεπαφής του I2P router. [49]

5. Υπηρεσίες Cloud

Το I2P προσφέρει ανώνυμες υπηρεσίες cloud μέσω του Tahoe-LAFS. Το Tahoe-LAFS cloud είναι ένα δωρεάν, ανοιχτού κώδικα αποκεντρωμένο και κατανεμημένο σύστημα αποθήκευσης αρχείων και δεδομένων. Πρόκειται για τη πρώτη τεχνολογία αποθήκευσης ανοιχτού λογισμικού που προσφέρει ασφάλεια ανεξάρτητη από τον πάροχο υπηρεσιών. Αυτό σημαίνει ότι η ακεραιότητα και η εμπιστευτικότητα των αρχείων είναι εγγυημένα από μαθηματικούς υπολογισμούς από τη πλευρά του πελάτη και είναι ανεξάρτητα από τους διακομιστές οι οποίοι μπορεί να λειτουργούν από κάποιο τρίτο μέρος. Όταν ένας χρήστης αποθηκεύσει ένα αρχείο στο cloud, θα κρυπτογραφηθεί, θα χωριστεί σε κομμάτια, τα οποία θα αποθηκευτούν σε πολλαπλούς διακομιστές. Όταν χρησιμοποιείται μέσω του δικτύου I2P οι τοποθεσίες των κόμβων είναι κρυφές και έτσι δημιουργούνται ανώνυμα κατανεμημένα πλέγματα. [51]

7. Web Browsing

Υπάρχουν δυο είδη ανώνυμων websites που μπορεί ένας χρήστης να επισκεφθεί:

α) Eepsite

Είναι ιστότοποι οι οποίοι βρίσκονται στο ανώνυμο δίκτυο I2P. Το όνομα των Eepsite τελειώνει σε .i2p. Το EepProxy μπορεί να εντοπίσει αυτά τα sites και ένας χρήστης μπορεί να τα προσπελάσει μέσω του HTTP proxy του I2P δρομολογητή.

β) Deepsites

Είναι κατανεμημένοι ανώνυμοι ιστότοποι οι οποίοι είναι προσβάσιμοι μέσω του Tahoe-LAFS-I2P client ή του Tahoe-LAFS-I2P HTTP proxy.

2.5 Σύγκριση I2P και Tor

Το Tor και το I2P είναι ανώνυμα δίκτυα proxy, τα οποία επιτρέπουν στον χρήστη να αποκρύψει την ταυτότητα του. Παρόλο που οι δημιουργοί του I2P έχουν ως πηγή έμπνευσης τους το Tor, τα δυο δίκτυα παρουσιάζουν διάφορες μεταξύ τους. Θα ακολουθήσουν οι παρατηρήσεις που έγιναν συγκρίνοντας τις διάφορες πτυχές τους:

1. Ανωνυμία των δικτύων

Η ανωνυμία δεν είναι ένα ποσοτικό μέγεθος για να συγκριθεί, ωστόσο τα δύο δίκτυα παρουσιάζουν διαφορετικά επίπεδα ανωνυμίας. Το δίκτυο Tor παρέχει το πρόγραμμα περιήγησης Tor (παραλλαγή του Mozilla Firefox) που λειτουργεί χρησιμοποιώντας ένα δίκτυο κρυπτογραφημένων σηράγγων μεταξύ των Onion Routers. Οι δρομολογητές επιλέγονται τυχαία και σχηματίζουν ένα κύκλωμα, όπου κανένας δρομολογητής, δεν έχει καμία πληροφορία για τίποτα άλλο, εκτός από τις προηγούμενες και τις επόμενες συνδέσεις του. Όταν ένας χρήστης θέλει να προσπελάσει μια κρυφή υπηρεσία, τότε η πλήρης σύνδεση μεταξύ αυτού και της κρυφής υπηρεσίας αποτελείται από 6 αναμεταδότες. Συγκεκριμένα, τρεις από αυτούς χρησιμοποιεί ο χρήστης (με τον τρίτο να αποτελεί το σημείο συνάντησης) και τρεις χρησιμοποιεί η κρυφή υπηρεσία. Στο κύκλωμα ο πρώτος κόμβος γνωρίζει τη πραγματική IP του αποστολέα, ενώ ο τελευταίος κόμβος γνωρίζει την πραγματική IP του δέκτη, κάτι που σημαίνει ότι η ανωνυμία εξαρτάται σε μεγάλο βαθμό από την αξιοπιστία των κόμβων εξόδου. Το πρόγραμμα περιήγησης Tor διαθέτει επίσης, ενσωματωμένες λειτουργίες που βελτιώνουν τις ρυθμίσεις απορρήτου και ασφαλείας, όπως για παράδειγμα, η δυνατότητα ιδιωτικής περιήγησης, ο περιορισμός των cookies τρίτου μέρους και η απενεργοποίηση της καταγραφής του ιστορικού του προγράμματος περιήγησης ή των δεδομένων ιστότοπου. Τα παραπάνω στοιχεία ενισχύουν την ανώνυμη περιήγηση και επικοινωνία των χρηστών.

Το I2P δεν διαθέτει πρόγραμμα περιήγησης, αλλά ένα δικτυακό γραφικό περιβάλλον χρήστη. Το l2P κρυπτογραφεί τα δεδομένα του σε τέσσερα στρώματα κρυπτογράφησης (κρυπτογραφούνται και οι σήραγγες). Έτσι, κανένας από τους παραλήπτες των δεδομένων δεν αποκαλύπτει τις διευθύνσεις του σε τρίτους παρατηρητές. Το Tor επιτρέπει στους χρήστες του να πλοηγήσουν το διαδίκτυο ανώνυμα, ενώ το l2P επικεντρώνεται στη ανταλλαγή δεδομένων εντός του δικτύου. Όταν ένας υπολογιστής εισέρχεται στο δίκτυο I2P λειτουργεί ως δρομολογητής του δικτύου, έτσι δημιουργείται ένα αποκεντρωμένο δίκτυο, στο οποίο είναι πολύ δύσκολο να βρεθεί ποιος επικοινωνεί με ποιον. Κατά συνέπεια, δημιουργείται ένα ανώνυμο δίκτυο.

2. Ταχύτητα

Χρησιμοποιώντας ένας χρήστης το πρόγραμμα περιήγησης Tor διαπιστώνει ότι είναι ιδιαίτερα αργό και αυτό είναι συνέπεια των πολλαπλών onion routers που χρησιμοποιούνται. Στον αντίποδα, το I2P είναι ταχύτερο στις αιτήσεις HTTP-GET σε σχέση με το δίκτυο Tor, καθώς σχεδιάστηκε για να αξιοποιεί με τον καλύτερο τρόπο τις κρυφές υπηρεσίες. Ωστόσο, αυτό που παρατηρείται είναι ότι το Tor είναι πιο γρήγορο στη λήψη του περιεχομένου των σελίδων και στην λήψη αρχείων από τις σελίδες.

3. Δημοτικότητα

Το Tor είναι η πιο δημοφιλής πλατφόρμα με μεγάλη υποστήριξη από την κοινότητα, με μεγάλη βάση χρηστών και με μεγαλύτερη χρηματοδότηση σε σχέση με το I2P. Ο βασικός λόγος για τη δημοτικότητα του είναι η ευκολία χρήσης του, καθώς ένας χρήστης απλά εγκαθιστά το πρόγραμμα περιήγησης, το εκτελεί και στη συνέχεια έχει αξιόπιστη ανώνυμη πρόσβαση στο δημόσιο διαδίκτυο. Επιπλέον, μπορεί να προσπελάσει κρυφές υπηρεσίες χωρίς κάποια άλλη ρύθμιση. Αντιθέτως, το I2P απαιτεί περαιτέρω ρυθμίσεις, προκειμένου ένας χρήστης να έχει πρόσβαση στις κρυφές υπηρεσίες του.

4. Περιεχόμενο

Το περιεχόμενο των δύο πλατφόρμων διαφέρει κυρίως, λόγω των διαφορετικών στόχων που έχουν θέσει. Το δίκτυο Tor σχεδιάστηκε για να διευκολύνει την ανώνυμη πρόσβαση στο σύνολο του διαδικτύου, οπότε το περιεχόμενο του είναι ολόκληρο το διαδίκτυο και επιπλέον κάποιες κρυφές υπηρεσίες. Αντιθέτως, το I2P επικεντρώνεται στη δημιουργία Darknet στο διαδίκτυο, με τους χρήστες να έχουν πρόσβαση σε κρυφές υπηρεσίες.

Επιπλέον, παρέχεται η δυνατότητα ανώνυμου διαμοιρασμού αρχείων εντός του δικτύου, κάτι το οποίο στο δίκτυο Tor μπορεί να προκαλέσει κίνδυνο στην ανωνυμία του δικτύου.

5. Υποστήριξη από την κοινότητα

Το Tor είναι πιο δημοφιλές δίκτυο από το I2P, διατίθεται υψηλότερη χρηματοδότηση και η βάση χρηστών είναι μεγαλύτερη. Για το δίκτυο Tor υπάρχουν πολλές ερευνητικές εργασίες, ενώ για το I2P είναι σχετικά λιγότερες και διατίθενται στον επίσημο ιστότοπο του. Επιπλέον, στο δίκτυο Tor απασχολούνται περισσότεροι προγραμματιστές σε σχέση με το I2P.

6. Δομή και τεχνικά χαρακτηριστικά

Το πρόγραμμα περιήγησης Tor είναι γραμμένο σε C, ενώ το I2P σε Java. Το δίκτυο Tor χρησιμοποιεί μεταγωγή κυκλώματος, ενώ το I2P βασίζεται στη μεταγωγή πακέτων. Επίσης, το δίκτυο Tor υποστηρίζει ανώνυμες εφαρμογές TCP, ενώ το δίκτυο I2P υποστηρίζει τόσο UDP όσο και TCP. Μάλιστα η χρήση εφαρμογών UDP (όπως P2P) στο δίκτυο Tor μπορεί να προκαλέσει απώλεια της ανωνυμίας. Το Tor λόγω του μεγέθους του είναι πιο ευάλωτο σε επιθέσεις DoS (Denial of Service) και σε επιθέσεις Man in the Middle.

Κεφάλαιο 3

Δίκτυα Friend to Friend

Σε αυτό το κεφάλαιο θα αναλυθούν τα δίκτυα Friend to Friend (F2F), αλλά και οι διάφοροι τρόποι υλοποίησης τους. Τα Friend to Friend δίκτυα είναι ανώνυμα Peer to Peer (P2P) δίκτυα, στα οποία ένας ομότιμος χρήστης συνδέεται με έναν μικρό αριθμό έμπιστων - γνωστών χρηστών, οι οποίοι είναι οι μόνοι που γνωρίζουν την ταυτότητα του χρήστη. Στα δίκτυα αυτά, οι χρήστες έχουν μια ψεύτικη ταυτότητα. Η ταυτότητα αυτή είναι δύσκολο να συνδεθεί με την πραγματική IP των χρηστών.

Όταν ένα χρήστης επιδιώκει την ανωνυμία, θέλει να αποκρύψει τη σχέση του με μια συγκεκριμένη πράξη, αλλά και με τα μέρη τα οποία είναι ενεργά στην επικοινωνία. [8]
Πολλά F2F δίκτυα υποστηρίζουν ανώνυμη ή ψευδώνυμη επικοινωνία μεταξύ χρηστών που δεν γνωρίζονται ή δεν εμπιστεύονται ο ένας τον άλλον. Για παράδειγμα, ένας κόμβος μπορεί να προωθεί τα δεδομένα μεταξύ δυο έμπιστων χρηστών, χωρίς να κοινοποιεί τη διεύθυνση IP τους ή το όνομα τους.

3.1 Oneswarm

Το Oneswarm είναι μια εφαρμογή P2P πελάτη, η οποία αναπτύχθηκε από το Πανεπιστήμιο της Ουάσιγκτον και σχεδιάστηκε ώστε οι χρήστες να μοιράζονται δεδομένα αποτελεσματικά, ανώνυμα και με ασφάλεια, προστατεύοντας την ιδιωτικότητα τους σε βάρος της απόδοσης.

Η χρήση του Oneswarm μπορεί να υποστηρίξει διάφορα επίπεδα ασφαλείας. Για παράδειγμα, μπορεί να χρησιμοποιηθεί για δημόσιο διαμερισμό δεδομένων που υπάρχουν στο Bit Torrent. Ταυτόχρονα, μπορεί να δημιουργήσει αντίγραφο αυτών των

δεδομένων και να τα διαμοιράσει σε ομότιμους χρήστες του Oneswarm μέσω ανώνυμων συνδέσεων.

Ένας χρήστης του Oneswarm μπορεί να επιλέξει τους χρήστες με τους οποίους θα επικοινωνήσει, ενώ έχει την δυνατότητα να ορίσει δικαιώματα, με τα οποία θα περιορίζει τη πρόσβαση και την διανομή των δεδομένων. Οι τρόποι διακίνησης των δεδομένων είναι τρείς: α) η δημόσια διακίνηση β) η διακίνηση με άδεια (with permission) και γ) διακίνηση χωρίς ένδειξη. Τα δεδομένα που διαμοιράζονται με άδεια, δίνουν άμεσα πληροφορίες σχετικά με την πηγή και ενδεχομένως τον προορισμό. Τα δεδομένα τα οποία μοιράζονται "χωρίς ένδειξη" (without attribution), εντοπίζονται με τη χρήση αναζήτησης λέξεων και διατηρούν την ιδιωτικότητα τους. Η μεταφορά των δεδομένων "χωρίς ένδειξη", γίνεται με την αναμετάδοση των δεδομένων σε άγνωστο αριθμό αναμεταδοτών, προκείμενου να πραγματοποιηθεί απόκρυψη της πηγής και του προορισμού.

Το Oneswarm διατηρεί τα ίδια στοιχεία με τα ήδη υπάρχοντα P2P συστήματα, ωστόσο διαφέρει σε τρία σημεία. Πρώτον, δεν γίνεται δημόσιος διαμερισμός αρχείων με όλους τους χρήστες του, αλλά οι χρήστες του Oneswarm είναι αυτοί που ορίζουν ρητά το επίπεδο αξιοπιστίας των ομότιμων χρηστών. Δεύτερον, δεν υπάρχει κεντρική διαχείριση των δεδομένων, αλλά οι ομότιμοι χρήστες εντοπίζουν τις πηγές των δεδομένων με τη μέθοδο αναζήτησης Flooding. Τρίτον, οι πηγές δεν αποστέλλουν απευθείας δεδομένα στους παραλήπτες, αλλά η μεταφορά των δεδομένων γίνεται από το αντίστροφο δρομολόγιο από αυτό που δημιουργείται κατά την διάρκεια της αναζήτησης των δεδομένων, (με επανεγγραφή των διευθύνσεων, με σκοπό την απόκρυψη των ταυτοτήτων, τόσο του αποστολέα όσο και του παραλήπτη).

Οι ομότιμοι χρήστες του OneSwarm συνδέονται ο ένας με τον άλλο χρησιμοποιώντας Secure Sockets SSLv3 με ζεύγη κλειδιών RSA. Όταν δυο ομότιμοι χρήστες συνδέονται, ανταλλάσσουν ένα μήνυμα με μια λίστα αρχείων. Το μήνυμα με τη λίστα αρχείων είναι ένα συμπιεσμένο αρχείο XML, το οποίο περιλαμβάνει στοιχεία, όπως το όνομα, το μέγεθος, την ημερομηνία και άλλα metadata για αρχεία που ο συγκεκριμένος ομότιμος χρήστης έχει δικαιώματα. Για κάθε αρχείο που διαμοιράζεται ιδιωτικά, τα metadata περιλαμβάνουν ένα κλειδί 512 bit, που χρησιμοποιείται για συμμετρική κρυπτογράφηση κατά την μεταφορά των δεδομένων.

Ο μηχανισμός αναζήτησης στο Oneswarm είναι σχεδιασμένος έτσι ώστε να εντοπίζει το συντομότερο δρομολόγιο. Με την επιλογή και χρήση του συντομότερου δρομολόγιου ελαχιστοποιούνται τα επιπλέον δεδομένα, υπάρχει όμως κίνδυνος φτωχής απόδοσης, σε περίπτωση που ο συντομότερος δρόμος είναι αργός ή εάν υπάρχει υπερφόρτωση σε αυτό. Αυτό το πρόβλημα αντιμετωπίζεται με τον χειρισμό της διάδοσης των αναζητήσεων. Το μονοπάτι που ακολουθείται, όταν αποστέλλεται μήνυμα αναζήτησης, καθορίζει και το μονοπάτι που θα γίνονται οι μεταφορές των δεδομένων. Για την εύρεση του συντομότερου μονοπατιού, το Oneswarm βασίζεται στην μέθοδο Flooding. Τα μηνύματα αναζήτησης περιλαμβάνουν μια τυχαία παραγόμενη ταυτότητα αναζήτησης και μια λίστα λέξεων κλειδιών.

Για την αποφυγή της διάδοσης κάθε αναζήτησης σε όλους τους χρήστες του δικτύου, κάθε χρήστης καθυστερεί το μήνυμα αναζήτησης για τουλάχιστον 150 ms πριν το προωθήσει στους ομότιμους χρήστες. Η πηγή της αναζήτησης μπορεί να τερματίσει τις δημοφιλείς αναζητήσεις για τις οποίες έχουν βρεθεί αποτελέσματα, με την αποστολή μηνύματος ακύρωσης αναζήτησης. Το μήνυμα ακύρωσης αποστέλλεται από το ίδιο δρομολόγιο που αποστέλλεται το αντίστοιχο μήνυμα αναζήτησης, χωρίς όμως καθυστέρηση προώθησης, επιτρέποντας έτσι το μήνυμα ακύρωσης να φτάσει γρήγορα στον προορισμό.

Εάν ένας κόμβος κατέχει ένα αρχείο που αντιστοιχεί σε ερώτημα αναζήτησης, δεν προωθεί την αναζήτηση σε άλλο κόμβο, αλλά αποστέλλει μήνυμα απόκρισης. Εάν γίνει η λήψη μηνύματος σε λιγότερο χρόνο από 150 ms, σημαίνει ότι, πιθανώς ο ανταποκριτής της πηγής δεδομένων είναι μη έμπιστος χρήστης. Για να αποφευχθεί αυτό, τα μηνύματα απόκρισης αναζήτησης των χρηστών, στέλνονται σε μη έμπιστους χρήστες για να γίνει εξομοίωση του μακρύτερου δρομολογίου.

Τα μηνύματα απόκρισης περιέχουν ένα αναγνωριστικό αναζήτησης, μια λίστα με τιμές κατακερματισμού, που αναγνωρίζει τα αντιστοιχιζόμενα αρχεία, τα metadata των αρχείων, και ένα αναγνωριστικό δρομολόγιου. Το αναγνωριστικό δρομολόγιου χρησιμοποιείται για να ξεχωρίζουν οι διάφορες διαδρομές, ακόμη και αν αυτές επικαλύπτονται μεταξύ τους. [14]

3.2 Retroshare

Το Retroshare είναι ένα δίκτυο διαμερισμού αρχείων μεταξύ ομότιμων χρηστών (Peer to Peer). Αποτελεί ένα Friend to Friend δίκτυο, καθώς δημιουργεί συνδέσεις μόνο μεταξύ αξιόπιστων χρηστών. Με αυτό τον τρόπο ο χρήστης μπορεί να ελέγξει τους χρήστες με τους οποίους ανταλλάσσει δεδομένα.

Το Retroshare εγκαθιστά κρυπτογραφημένες συνδέσεις μεταξύ των αξιόπιστων χρηστών οι οποίες βασίζονται στο GNU Privacy Guard (GPG). Οι συνδέσεις αυτές, μπορούν να χρησιμοποιηθούν για διάφορες υπηρεσίες, όπως ο διαμοιρασμός αρχείων, η ιδιωτική συνομιλία μεταξύ έμπιστων χρηστών, η ιδιωτική ή η δημόσια συνομιλία με τις επαφές των έμπιστων χρηστών, η δημοσίευση σε forums και η δυνατότητα Voice over IP. [7]

Το Retroshare επιλύει το πρόβλημα της ιδιωτικότητας με την εφαρμογή δυο αρχών. Η πρώτη αρχή είναι ότι η μεταφορά δεδομένων γίνεται μόνο μεταξύ έμπιστων χρηστών. Η δεύτερη αρχή είναι ότι οι μεταφορές των δεδομένων μεταξύ έμπιστων χρηστών γίνονται πάντα κρυπτογραφημένα, με την χρήση πιστοποιητικών SSL, έτσι αποτρέπεται η παρακολούθηση της διακίνησης των δεδομένων με μεθόδους όπως man in the middle attack.

Η μεταφορά των αρχείων στο Retroshare γίνεται με την χρήση ανώνυμου μοντέλου δρομολόγησης που ονομάζεται Turtle Router. Αυτό το μοντέλο επιτρέπει σε χρήστες που δεν είναι συνδεμένοι απευθείας μεταξύ τους, αλλά έχουν κοινούς ομότιμους χρήστες, να ανταλλάσσουν δεδομένα ανώνυμα και κρυπτογραφημένα.

Η αναζήτηση στο Retroshare πραγματοποιείται με την αποστολή broadcast αίτησης αναζήτησης πακέτων σε όλους τους συνδεδεμένους φίλους – έμπιστους χρήστες. Οι φίλοι προωθούν την αίτηση στους δικούς τους φίλους, μέχρι να βρεθεί το αρχείο. Εάν το αρχείο βρεθεί, τότε αποστέλλεται, με την αντίστροφη διαδικασία δρομολόγησης, μια λίστα με τα αρχεία που βρέθηκαν. Προκειμένου η διαδικασία να εκτελείται πιο γρήγορα, διατηρείται μνήμη cache με τις αναζητήσεις. Η cache εξετάζεται κάθε φορά που

πραγματοποιείται μια νέα αναζήτηση, εάν τα αποτελέσματα της αναζήτησης υπάρχουν ήδη, τότε δεν πραγματοποιείται εκ νέου αναζήτηση.

Στο Retroshare, εγκαθίστανται σήραγγες χρησιμοποιώντας το ίδιο πρωτόκολλο με την αναζήτηση. Μια ξεχωριστή μνήμη cache χρησιμοποιείται για να αποθηκεύσει τις αιτήσεις των σηράγγων και για να δρομολογήσει τα πακέτα "αποδοχής" των σηράγγων στον αρχικό χρήστη. Κάθε φορά που πραγματοποιείται μια αίτηση για σήραγγα, δίνονται δυο αριθμοί, η ταυτότητα της αίτησης (request id) και το half-id. Το request id χρησιμοποιείται για να κατατάξει τις αιτήσεις των σηράγγων προς τους ομότιμους χρήστες στην μνήμη cache. Το half-id της σήραγγας είναι μια τιμή που αποτελείται από την τιμή κατακερματισμού της ταυτότητας SSL του χρήστη, την τιμή κατακερματισμού του αρχείου για το οποίο θα χρησιμοποιηθεί η σήραγγα και επιπλέον προστίθεται ένας τυχαίος αριθμός. Η προσθήκη του τυχαίου αριθμού προσφέρει μεγαλύτερη ασφάλεια απέναντι σε επιθέσεις brute force. Όταν ο ομότιμος χρήστης ανταποκριθεί στην αίτηση της σήραγγας, τότε το half-id του συγχωνεύεται με το half-id του χρήστη και δημιουργείται το τελικό id του tunnel. Οι σήραγγες (tunnel) μεταξύ συγκεκριμένης πηγής και προορισμού διατηρούν πάντα το ίδιο tunnel id, παρόλο που η ταυτότητα της αίτησης (request id) αλλάζει κάθε φορά. Ενώ και η δρομολόγηση μπορεί να είναι διαφοροποιημένη σε σχέση με την αρχική. Το tunnel id δεν είναι συμμετρικό, αυτό σημαίνει ότι από μια πηγή Α προς ένα προορισμό Β το tunnel id δεν έχει την ίδια τιμή για την διαδρομή από το Β προς το Α. Η ασυμμετρία του tunnel id είναι πολύ σημαντική καθώς δυο ομότιμοι χρήστες μπορεί να έχουν εγκατεστημένες δυο σήραγγες από τον ένα στον άλλο και το ίδιο αρχείο να μεταφέρεται και προς τις δυο κατευθύνσεις. Οι σήραγγες στο Retroshare δεν χρησιμοποιούν Global addressing και μια σήραγγα μόλις εγκατασταθεί εμφανίζεται σε όλους τους ομότιμους χρήστες που βρίσκονται κατά μήκος της.

Οι σήραγγες αφαιρούνται από τον κατάλογο κάθε ομότιμου χρήστη όταν η κίνηση είναι μηδενική για 60 δευτερόλεπτα. Αυτή η τεχνική επιτρέπει τον ομαλό χειρισμό οποιασδήποτε τυχαίας αλλαγής στην τοπολογία του δικτύου. Εάν, για παράδειγμα, ένας ομότιμος χρήστης αποσυνδεθεί, τότε η σήραγγα του θα αφαιρεθεί από τους ομότιμους του χρήστες, μετά από 60 δευτερόλεπτα χωρίς την αποστολή κάποιου πακέτου.

Επιπλέον, οι σήραγγες δεν διαχειρίζονται το εύρος ζώνης της σύνδεσης, καθώς ο χρήστης είναι υπεύθυνος για την αίτηση των δεδομένων και την προσαρμογή της ταχύτητας. Από τη στιγμή κατά την οποία η ταχύτητα στη σήραγγα περιορίζεται στην ελάχιστη ταχύτητα μεταξύ των κόμβων, τα δεδομένα θα αποκτήσουν τη μέγιστη δυνατή ταχύτητα, έτσι ώστε η σήραγγα να εκμεταλλευτεί το μέγιστο εύρος ζώνης.

Οι τιμές της ταχύτητας μεταφοράς ενός αρχείου σε ένα μοντέλο Friend to Friend με πολλαπλούς κόμβους περιορίζονται από την ελάχιστη ταχύτητα uploading κατά μήκος της σήραγγάς και τον αριθμό των σηράγγων που εξυπηρετούν. Η ελάχιστη ταχύτητα uploading εξαρτάται από το είδος της σύνδεσης που έχουν οι ομότιμοι χρήστες κατά μήκος της σήραγγάς, για παράδειγμα η ταχύτητα περιορίζεται σημαντικά στις συνδέσεις ADSL σε σχέση με αυτές που χρησιμοποιείται οπτική ίνα. Είναι φυσιολογικό να υπάρχουν περισσότερες από μια σήραγγες για τη λήψη ενός αρχείου, το σύνηθες είναι 5 έως 15 σήραγγες, χωρίς όμως να υπάρχει κάποιος περιορισμός. Οι σήραγγες δεν φτάνουν τη μέγιστη ταχύτητα από τη στιγμή κατά την οποία ένας χρήστης μπορεί να δρομολογεί ταυτόχρονα από πολλές σήραγγες και να πραγματοποιείται διαμερισμός στην απόδοση των σηράγγων.[7]

3.3 GNUnet

Το GNUnet είναι μια εναλλακτική στοίβα δικτύου που χρησιμοποιείται για τη δημιουργία ασφαλών και αποκεντρωμένων εφαρμογών, που έχουν σχεδιαστεί για να αντικαταστήσουν τη μη ασφαλή στοίβα του πρωτοκόλλου Internet. Το GNUnet προσφέρει από άκρο σε άκρο κρυπτογραφημένη δικτύωση και παρέχει προστασία της ιδιωτικής ζωής. Η χρήση του παγκόσμιου και κατανεμημένου δικτύου του GNUnet, γίνεται με την χρήση του λογισμικού GNUnet.

Ο σκοπός του GNUnet είναι να προσφέρει μια διέξοδο από την ιεραρχική δικτύωση και να δημιουργήσει ένα δίκτυο μεταξύ ομότιμων χρηστών. Ο κάθε χρήστης για να χρησιμοποιήσει το δίκτυο συνεισφέρει ένα μικρό ποσοστό πόρων προς τους υπόλοιπους χρήστες, χωρίς να εγκαταλείψει την ιδιωτικότητα του.

Το GNUnet είναι επεκτάσιμο, προσφέρει υποστήριξη ανάπτυξης νέων Peer to Peer εφαρμογών και προσθήκης εναλλακτικών δικτύων στο βασικό σύστημα. Το GNUnet δεν είναι ένα κλασικό δίκτυο επικάλυψης καθώς δεν απαιτείται το πρωτόκολλο TCP/IP για να λειτουργήσει. Οι ομότιμοι χρήστες μπορούν να λειτουργήσουν και πέρα από τα κλασικά πρωτόκολλα του διαδικτύου όπως το TCP ή το UDP, καθώς μπορούν να ανταλλάσσουν δεδομένα άμεσα, μέσω WLAN ή Bluetooth, χωρίς την χρήση IP.

Η ανωνυμία στο GNUnet επιτυγχάνεται με τον μη διαχωρισμό μεταξύ των μηνυμάτων που δημιουργούνται από έναν ομότιμο χρήστη και των μηνυμάτων που ο ομότιμος χρήστης δρομολογεί. Όλοι οι ομότιμοι χρήστες ενεργούν ως δρομολογητές με κρυπτογραφημένες συνδέσεις και με σταθερή χρήση εύρους ζώνης για τη μεταξύ τους επικοινωνία.[30]

Τέλος, το GNU χρησιμοποιεί ένα σύστημα ονομάτων (GNU Name System - GNS), το οποίο είναι πλήρως αποκεντρωμένο. Τα ονόματα στο GNS είναι προσωπικά, καθώς κάθε χρήστης έχει πλήρη έλεγχο του ονόματος .gnu. Το GNS μπορεί να λειτουργήσει μαζί με το DNS και μπορεί να χρησιμοποιηθεί ως εναλλακτική λύση του X.509 ή του Web of Trust. [26]

3.4 Tribler

Το Tribler είναι ένας Bit Torrent P2P πελάτης που προσφέρει την δυνατότητα της ανώνυμης διακίνησης δεδομένων και υποστηρίζει διάφορες επεκτάσεις, όπως την ολοκληρωμένη αναζήτηση και το video on demand. Δημιουργεί ένα δίκτυο το οποίο προσομοιάζει το Onion Routing, που χρησιμοποιείται αποκλειστικά για διακίνηση αρχείων Torrent. Σύμφωνα με τους προγραμματιστές του, η ανωνυμία που προσφέρει, βρίσκεται ακόμη πρώιμο στάδιο. Προκειμένου να επιτευχθεί η ανωνυμία έχουν χρησιμοποιηθεί μέρη του κώδικα του πρωτοκόλλου Tor, ωστόσο το Tribler δεν είναι συμβατό με το δίκτυο Tor. Στο Tribler δεν χρησιμοποιείται το πρωτόκολλο TCP που χρησιμοποιείται στο Tor, αλλά γίνεται χρήση του πρωτοκόλλου UDP. Επιπλέον, χρησιμοποιείται έλεγχος συμφόρησης, από άκρο σε άκρο βασιζόμενος στο πρωτόκολλο UDP. Τέλος το Tribler βασίζεται στην αρχή, ότι ο χρήστης που λαμβάνει δεδομένα αποτελεί ταυτόχρονα και αναμεταδότη.[22]

3.5 Freenet

Το Freenet είναι ένα ελεύθερο λογισμικό το οποίο επιτρέπει τον ανώνυμο διαμερισμό αρχείων, την ανώνυμη πλοήγηση, την δημοσίευση περιεχομένου στις ιστοσελίδες του, την δημιουργία blog, την ανώνυμη επικοινωνία με chat, χωρίς το φόβο της λογοκρισίας. Οι επικοινωνίες στο Freenet είναι κρυπτογραφημένες και δρομολογούνται μέσω πολλαπλών κόμβων, προκειμένου να είναι δύσκολο να εντοπιστούν τα μέρη που συμμετέχουν στην επικοινωνία και να αποκαλυφθεί το περιεχόμενο της πληροφορίας. Οι χρήστες συμβάλλουν στο δίκτυο παραχωρώντας εύρος ζώνης και τομέα από τον σκληρό τους δίσκο για την αποθήκευση αρχείων. Τα αρχεία διατηρούνται ή διαγράφονται από το δίκτυο, ανάλογα με το εάν είναι δημοφιλή ή όχι. Τα λιγότερο δημοφιλή διαγράφονται προκειμένου να αντικατασταθούν από νέα αρχεία. Τα αρχεία είναι κρυπτογραφημένα και για αυτό είναι πολύ δύσκολο να αποκαλυφθεί το πραγματικό περιεχόμενο τους.

Επιπλέον, το Freenet έχει την δυνατότητα να δημιουργεί «έμπιστο» δίκτυο με την σύνδεση χρηστών που υπάρχει εμπιστοσύνη μεταξύ τους. Με αυτό τον τρόπο μειώνονται οι ευπάθειες και δημιουργείται ένα παγκόσμιο δίκτυο έμπιστων χρηστών, για αυτό το Freenet μπορεί να λειτουργήσει ακόμα και σε χώρες στις οποίες είναι απαγορευμένη η χρήση του.

Οι συνδέσεις των κόμβων στο δίκτυο Freenet, δημιουργούνται με την αποστολή προσκλήσεων από τους χρήστες. Με αυτό τον τρόπο δημιουργείται ένα δίκτυο το οποίο έχει μια συγκεκριμένη τοπολογία. Η δρομολόγηση του δικτύου λειτουργεί ανάλογα με το εάν οι χρήστες είναι μόνιμοι ή όχι. Οι συνδέσεις δεν δημιουργούνται τυχαία καθώς εάν γίνονταν αυτό, η τοπολογία θα ήταν εσφαλμένη και η δρομολόγηση μη λειτουργική. Η δρομολόγηση στο Freenet βασίζεται στο μοντέλο αξιόπιστης σύνδεσης, που θεωρεί τους κόμβους και τις συνδέσεις μεταξύ τους σταθερές και χωρίς τη δυνατότητα βελτίωσης. Η αποδοτικότητα της δρομολόγησης εξαρτάται από τη δομή του σταθερού δικτύου.

Οι δημιουργοί του συστήματος θεωρούν ότι το δίκτυο αξιόπιστης σύνδεσης θα λειτουργήσει ως “μικρός κόσμος”, δηλαδή ως ένα κοινωνικό δίκτυο, στο οποίο υπάρχουν σύντομα δρομολόγια μεταξύ δυο κόμβων και ότι υφίσταται τοπική ομαδοποίηση. Τοπική ομαδοποίηση σημαίνει ότι όπως τα άτομα που μοιράζονται κοινούς γνωστούς είναι πιθανότερο να γνωρίζονται μεταξύ τους, κατά αντιστοιχία το ίδιο θα συμβαίνει και στα

δίκτυα, όπου οι κόμβοι που γνωρίζουν τους γειτονικούς κόμβους γίνονται πιο αποδοτικοί.

Οι κόμβοι υπολογίζουν το συντομότερο δρομολόγιο και έχουν αποθηκευμένο ένα πίνακα δρομολόγησης, που υποδεικνύει μέχρι που θα φτάσουν τα ερωτήματα που προορίζονται για έναν συγκεκριμένο κόμβο. Κατά την δημιουργία των μονοπατιών απαιτείται υψηλός φόρτος εργασίας και εύρος ζώνης, καθώς χρειάζεται πίνακας δρομολόγησης στο μέγεθος του δικτύου για κάθε κόμβο. Κάθε φορά που ένας κόμβος εισέρχεται ή εξέρχεται στο δίκτυο χρησιμοποιείται η μέθοδος δρομολόγησης Greedy, δηλαδή σε κάθε βήμα, η δρομολόγηση γίνεται στον κόμβο που η ταυτότητα του μοιάζει με την επιθυμητή ταυτότητα.

Οι κόμβοι όταν εισέρχονται στο δίκτυο, λαμβάνουν τυχαίες ταυτότητες. Στην συνέχεια, αυτές οι ταυτότητες αλλάζουν, έτσι ώστε οι κόμβοι που είναι γειτονικοί να έχουν παρόμοιες ταυτότητες. Ιδεατά, θα πρέπει οι ταυτότητες να ανατίθενται, έτσι ώστε κατά μήκος μιας διαδρομής, σε κάθε βήμα, τα δεδομένα να βρίσκονται πιο κοντά στον προορισμό, σε σχέση με το προηγούμενο βήμα, μέχρις ότου βρεθεί ο κατάλληλος κόμβος του δικτύου. Αν υπάρχει συχνή αλλαγή των ταυτοτήτων, μπορεί να οδηγήσει στην ακύρωση μεγάλου μέρους της μνήμης cache και αυτό έχει ως αποτέλεσμα να καθίσταται η αναζήτηση αναποτελεσματική.

Το Freenet υποστηρίζει την λειτουργία opennet. Το opennet είναι ένα δίκτυο, στο οποίο οι κόμβοι δημιουργούν αυτόματα συνδέσεις. Οι κόμβοι έχουν μια αποθηκευμένη λίστα, η οποία περιέχει άλλους κόμβους, με τους οποίους συνδέονται και ανταλλάσσουν δεδομένα. Με την εγκατάσταση μιας σύνδεσης, οι κόμβοι που συμμετέχουν στη σύνδεση ανταλλάσσουν τη παραπάνω λίστα. Η διαδικασία αυτή γίνεται συνέχεια χωρίς κάποια παρέμβαση των χρηστών. [60]

Σε ότι αφορά τα κλειδιά κρυπτογράφησης, το Freenet χρησιμοποιεί δυο είδη κλειδιών το Content Hash Key (CHK) και το Signed Subspace Key (SSK). Για την ασφαλή ενημέρωση του περιεχομένου χρησιμοποιείται ένα κλειδί τύπου SSK, το Updatable Subspace Key (USK). Το CHK είναι μια τιμή κατακερματισμού SHA-256 ενός εγγράφου και

χρησιμοποιείται, ώστε ένας κόμβος του δικτύου να μπορεί να ελέγχει ότι το αρχείο που διακινεί είναι το σωστό, κάνοντας έλεγχο της τιμής κατακερματισμού.

Το SSK βασίζεται σε κρυπτογραφία δημόσιου κλειδιού (χρησιμοποιείται ο αλγόριθμος DSA). Τα έγγραφα που έχουν εισαχθεί στο δίκτυο υπογράφονται από τον εισαγωγέα με το SSK. Αυτή η υπογραφή μπορεί να επαληθευτεί από κάθε κόμβο, για να διασφαλιστεί ότι τα δεδομένα δεν έχουν παραβιαστεί. Τα SSKs μπορούν να επιτρέψουν την ασφαλή εισαγωγή εγγράφων από ένα άτομο.

Το Freenet, όπως και άλλες εφαρμογές του Dark Web, λειτουργεί με κατανεμημένο πίνακα κατακερματισμού, στον οποίο οι υπολογιστές που συμμετέχουν αποθηκεύουν πληροφορίες, που μπορούν να ανακτηθούν από άλλους συμμετέχοντες.

3.6 Zeronet

Το Zeronet είναι ένα αποκεντρωμένο δίκτυο ομότιμων χρηστών (P2P), που χρησιμοποιεί την κρυπτογραφία του Bitcoin και την τεχνολογία του Bit Torrent. Οι χρήστες του μπορούν να δημοσιεύσουν στατικούς ή δυναμικούς ιστότοπους, μπορούν να λειτουργήσουν ως διακομιστές των ιστότοπων, ενώ παραμένουν online ακόμη και αν υποστηρίζονται από έναν ομότιμο χρήστη. Είναι γραμμένο σε γλώσσα προγραμματισμού Python και περιέχει ενσωματωμένη μια βάση δεδομένων SQL. Αυτό καθιστά την ανάπτυξη των σελίδων με βαρύ περιεχόμενο εύκολη. Η ονομασία των ιστότοπων μπορεί να έχει την μορφή του δημοσίου κλειδιού του Bitcoin.

Η διαμόρφωση του Zeronet είναι σχετικά απλή. Για την προστασία του λογαριασμού των χρηστών, χρησιμοποιείται η ίδια κρυπτογράφηση ελλειπτικής καμπύλης που χρησιμοποιείται και για το Bitcoin Wallet. Επιπλέον, χρησιμοποιείται το πρωτόκολλο κρυπτογράφησης TLS. Υποστηρίζει την ανωνυμία καθώς υπάρχει η δυνατότητα χρήσης του Zeronet μέσω του Tor browser.

Όταν ένας χρήστης δημιουργεί ένα καινούργιο ιστότοπο λαμβάνει δυο κλειδιά ένα ιδιωτικό και ένα δημόσιο. Με το ιδιωτικό κλειδί μπορεί να υπογράψει νέο περιεχόμενο για τον ιστότοπο και χωρίς αυτό δε μπορεί να τροποποιηθεί. Το δημόσιο κλειδί ορίζει την

διεύθυνση του ιστότοπου και μπορεί να διασφαλίσει ότι το αρχείο δημιουργήθηκε από τον ιδιοκτήτη του ιστότοπου και δεν είναι κάποιο κακόβουλο αρχείο.

Όταν ένας χρήστης επισκέπτεται έναν ιστότοπο Zeronet, τότε ο ιστότοπος αιτείται την διεύθυνση IP του επισκέπτη από τον Bit Torrent tracker και τον καταγράφει ως επισκέπτη. Το Zeronet χρησιμοποιεί το Bit Torrent για να εντοπίσει χρήστες που πραγματοποιούν seeding στον ιστότοπο. Στην συνέχεια, ο χρήστης λαμβάνει το αρχείο content.json που περιέχει όλα τα ονόματα των υπόλοιπων αρχείων, τιμές κατακερματισμού και την υπογραφή του ιδιοκτήτη του ιστότοπου, ενώ λειτουργεί ως seeder. Το Zeronet επαληθεύει το αρχείο χρησιμοποιώντας την διεύθυνση του ιστότοπου και την υπογραφή του χρήστη. Στην συνέχεια λαμβάνει αρχεία με το περιεχόμενο του ιστότοπου (HTML,CSS, JS κλπ) και πιστοποιεί την αυθεντικότητα τους χρησιμοποιώντας την τιμή κατακερματισμού SHA512 από το περιεχόμενο του αρχείου content.json. Η λήψη αυτών των αρχείων, βελτιώνει την ταχύτητα προσπέλασης του περιεχομένου. Το Zeronet αν και δεν πρόκειται για δίκτυο F2F, αναλύεται σε αυτό το κεφάλαιο λόγω της P2P δομής του. [61]

Κεφάλαιο 4

Χρήση του Dark Web για κακόβουλους και παράνομους σκοπούς

4.1 Σκοπός Κεφαλαίου

Η ανωνυμία που προσφέρεται στο Dark Web, δίνει την δυνατότητα σε κακόβουλους χρήστες να προβούν σε παράνομες ενέργειες, χωρίς να αποκαλυφθεί η ταυτότητα τους. Χαρακτηριστικό παράδειγμα είναι το Hidden Wiki του δικτύου Tor, στο οποίο ένας χρήστης μπορεί να εντοπίσει διάφορες παράνομες υπηρεσίες. Πέρα από τις συγκεκριμένες υπηρεσίες, η δομή του Dark Web γίνεται αντικείμενο εκμετάλλευσης από κυβερνο-εγκληματίες, οι οποίοι δημιουργούν κακόβουλο λογισμικό (Worms, Botnets κλπ) που εκμεταλλεύεται την ανωνυμία του δικτύου. Στο κεφάλαιο θα παρουσιαστούν οι παράνομες υπηρεσίες οι οποίες προσφέρονται στο Dark Web και θα γίνει ανάλυση του κακόβουλου λογισμικού που εκμεταλλεύεται την δομή του Dark Web.

4.2 Botnets στο Dark Web

Ως Botnet μπορούμε να ορίσουμε ένα επικαλυπτικό δίκτυο, στο οποίο μηχανήματα, (που ονομάζονται Bots) που έχουν μολυνθεί από κακόβουλο λογισμικό, ελέγχονται από έναν επιτιθέμενο, ο οποίος ονομάζεται Botmaster. Υπάρχουν διάφοροι τρόποι μόλυνσης των μηχανημάτων, όπως Spam ή Zero Day Exploits, ενώ ο πιο συνηθισμένος τρόπος είναι με τη λήψη κάποιου μολυσμένου αρχείου. Ο Botmaster ελέγχει τα Bots μέσω του Botnet και αποστέλλει εντολές, με τις οποίες τα Bots εκτελούν κακόβουλες ενέργειες, όπως επιθέσεις DDoS, αποστολή Spam, κλοπή διαπιστευτηρίων κλπ.

Τα Botnets μπορούν να διαχωριστούν ανάλογα με την κακόβουλη εργασία που εκτελούν, το πρωτόκολλο που χρησιμοποιούν και την αρχιτεκτονική τους. Συνήθως η δομή των Botnets είναι σχετικά απλή, με τα Bots να είναι συνδεδεμένα με έναν κεντρικό Server, ο οποίος ελέγχεται από τον Botmaster. Οι Servers αυτοί ονομάζονται Command and Control Servers(C & C Server). Το πλεονέκτημα αυτού του είδους Botnet, είναι ο ευκολότερος έλεγχος του. Το μειονέκτημα της συγκεκριμένης δομής είναι ότι ο C & C Server αποτελεί έναν κεντρικό κόμβο που συνδέει όλα τα Bots, έτσι, εάν απενεργοποιηθεί τότε διαλύεται όλο το δίκτυο. Τα τελευταία χρόνια έχει εξελιχθεί η δομή των Botnets. Πλέον, χρησιμοποιούνται πολλαπλοί C & C Servers ή χρησιμοποιείται η τεχνική Fast Flux προκειμένου τα Botnets να είναι πιο ανθεκτικά. Επίσης, εφαρμόζεται το Domain Generation Algorithm, το οποίο επιτρέπει στο κακόβουλο λογισμικό να αναπτύσσει τυχαίο Domain Name όταν εκτελείται. Αυτό το Domain Name εντοπίζει τον C & C Server. Παρά τις συγκεκριμένες προσπάθειες αναβάθμισής τους, τα Botnet με κεντρική δομή είναι εύκολο να εντοπιστούν και να σταματήσει η λειτουργία τους.

Προκειμένου να αντιμετωπιστούν οι παραπάνω αδυναμίες της κεντρικής δομής των Botnets, γίνεται χρήση της αρχιτεκτονικής των P2P δικτύων, που αποτελούν μια πιο ευέλικτη και ανθεκτική μορφή δικτύου. Η αρχιτεκτονική P2P αντικαθιστά τον κεντρικό C & C Server, με ένα κατανεμημένο δίκτυο Bot. Τα Bots ανταλλάσσουν πληροφορίες μεταξύ τους και μεταδίδουν εντολές, κάνοντας χρήση προσαρμοσμένων πρωτοκόλλων. Ωστόσο, χρησιμοποιούν και κοινά πρωτόκολλα, όπως HTTP, DNS και άλλα, ώστε να αποκρύπτουν την λειτουργία τους. Η διαχείριση και ο έλεγχος της συγκεκριμένης δομής Botnet, εμφανίζει μεγαλύτερη δυσκολία σε σχέση με την κεντρική δομή. Τα P2P Botnets μπορεί να είναι πιο ανθεκτικά, αλλά αυτό δεν σημαίνει ότι δεν είναι ευπαθή σε επιθέσεις που θα οδηγήσουν στην διάλυση τους. Τα P2P Botnets μπορούν να εντοπιστούν με τη χρήση προγραμμάτων Crawler, με τα οποία μπορούν να εντοπιστούν όλα τα Bots.

Άλλη μέθοδος λειτουργίας είναι τα Botnets κεντρικής δομής, με C & C Servers, οι οποίοι χρησιμοποιούν διάφορες τεχνικές, ώστε να αποκρύπτουν την λειτουργία τους. Ένας από τους τρόπους για να επιτευχθεί αυτό είναι η χρήση του δικτύου Tor. Οι C & C servers εκμεταλλεύονται την ανωνυμία του δικτύου Tor και λειτουργούν όπως οι κρυφές υπηρεσίες του, προκειμένου να μην εντοπίζονται.

Το 2010, για πρώτη φορά, παρουσιάστηκε στο συνέδριο Defcon η δυνατότητα ανάπτυξης Botnet με την εκμετάλλευση του δικτύου Tor. Παρουσιάστηκαν τα πλεονεκτήματα των συγκεκριμένων Botnets, τα οποία είναι η διαθεσιμότητα αυθεντικοποιημένων κρυφών υπηρεσιών και η διαθεσιμότητα του ιδιωτικού δικτύου Tor. Παρουσιάστηκαν δυο τρόποι ανάπτυξης Botnet μέσω του δικτύου Tor, οι οποίοι είναι τα Tor2Web proxy και Proxy - aware Malware over Tor network.

Στο μοντέλο Tor2Web proxy ο μηχανισμός δρομολόγησης βασίζεται στον Tor2Web proxy, ο οποίος επαναδρομολογεί την κίνηση του δικτύου Tor. Το Bot συνδέεται στην κρυφή διεύθυνση onion του δικτύου Tor μέσω του Tor2Web proxy, η οποία αντιστοιχεί στον C&C server. Το βασικό πρόβλημα αυτού του μοντέλου είναι ότι είναι εύκολο να φιλτραριστεί η κίνηση του Tor2Web αλλά και η καθυστέρηση που υπάρχει στο δίκτυο Tor. [19]

Το δεύτερο μοντέλο βασίζεται στην χρήση ενός proxy- aware κακόβουλου λογισμικού. Με αυτή τη μέθοδο, λόγω της μη εμπλοκής του Tor2Web, οι μολυσμένοι υπολογιστές Bot θα πρέπει να εκτελούν Tor Client ή Tor Service και θα πρέπει να υποστηρίζουν το πρωτόκολλο SOCKS, προκειμένου να μπορέσουν να προσπελάσουν τις διευθύνσεις .onion μέσω του δικτύου Tor. Αυτή η μέθοδος είναι πιο αποδοτική, γιατί η κίνηση δεν δρομολογείται μέσω proxy, καθώς όλα τα δεδομένα μεταξύ των bots και του C&C server ανταλλάσσονται κατευθείαν μέσω του δικτύου Tor. Με αυτό τον τρόπο αποφεύγεται ο έλεγχος ή η παρεμβολή της κίνησης σε κόμβους εξόδου από το δίκτυο Tor. Ωστόσο, αυτή η μέθοδος είναι πιο σύνθετη σε σχέση με την πρώτη, καθώς είναι πιο δύσκολη η ρύθμιση του SOCKS και ο συγχρονισμός του Botnet.[19]

Τα πλεονεκτήματα της χρήσης του δικτύου Tor για τη λειτουργία Botnet είναι ότι η κυκλοφορία του Botnet εμφανίζεται ως νόμιμη κίνηση του δικτύου Tor και η κρυπτογράφηση εμποδίζει τα περισσότερα συστήματα ανίχνευσης εισβολών να εντοπίσουν την κυκλοφορία του. Επιπλέον, σε περίπτωση που το Botnet χρησιμοποιεί C & C server, ο εντοπισμός των Servers είναι πολύ δύσκολος, ενώ υπάρχει μεγαλύτερη ευελιξία στην αλλαγή των C & C Servers με την επαναχρησιμοποίηση του παραγόμενου ιδιωτικού κλειδιού της κρυφής υπηρεσίας. Τα μειονεκτήματα της της χρήσης του δικτύου

Tor για τη δημιουργία Botnet είναι η πολυπλοκότητα της διαχείρισης του Botnet, η καθυστέρηση στην επικοινωνία και ο κίνδυνος της εύκολης διάλυσης του.[20]

1. Skynet

Το 2012 ερευνητές της γερμανικής εταιρίας G Data Software και της εταιρίας Rapid 7 εντόπισαν το Skynet, ένα Botnet το οποίο ελεγχόταν μέσω ενός Internet Relay Chat Server, ο οποίος εμφανιζόταν ως κρυφή υπηρεσία του δικτύου Tor. Το Skynet μπορούσε να εκτελέσει διάφορες διεργασίες, όπως DDoS επιθέσεις, Spamming και Bitcoin Mining.
Το κακόβουλο λογισμικό διακινούνταν μέσω του Usenet και είχε μέγεθος 15 mb. Ο κώδικας περιείχε ένα Bot το οποίο ενεργοποιούσε IRC μέσω Tor, ενώ είχε τέσσερις ενσωματωμένες πηγές: α) το Zeus bot, β) τον Tor client για Windows, γ) το CGMiner, που είναι ένα εργαλείο bitcoin mining και δ) ένα αντίγραφο του OpenCL.dll που χρησιμοποιείται από το CGMiner για CPU και GPU hash cracking.

Όταν το κακόβουλο λογισμικό εκτελεστεί, τότε αντιγράφει τον εαυτό του σε ένα κατάλογο στο %AppData% και ξεκινάει διεργασίες οι οποίες εμφανίζονται ως Internet Explorer ή ως svchost. Για να εκτελέσει τα στοιχεία του, το κακόβουλο λογισμικό δημιουργεί πολλαπλές νόμιμες διεργασίες σε κατάσταση αναστολής.

Προκειμένου να συνεχίσει την εκτέλεση του, το κακόβουλο λογισμικό, και μετά την επανεκκίνηση του υπολογιστή, δημιουργεί μια είσοδο στο Run Registry Key. Οι C & C servers του Skynet εμφανίζονταν ως κρυφές υπηρεσίες του Tor, ενώ και οι μολυσμένοι υπολογιστές λειτουργούσαν ως μέρος του δικτύου Tor. Όλες οι επικοινωνίες μεταξύ των μολυσμένων υπολογιστών γινόταν μέσω του Tor SOCKS proxy, που εκτελούνταν τοπικά στους μολυσμένους υπολογιστές. Το κακόβουλο λογισμικό δημιουργούσε μια κρυφή υπηρεσία Tor στους μολυσμένους υπολογιστές στην θύρα 55080. Όταν ο επιτιθέμενος έστελνε εντολές μέσω του C & C server, το κακόβουλο λογισμικό άνοιγε SOCKS proxy στη θύρα 55080, η οποία ήταν προσβάσιμη μέσω ενός νέου δημιουργημένου .onion domain.
Σε ότι αφορά τις επιθέσεις DDoS, το κακόβουλο λογισμικό περιλάμβανε την υποστήριξη των μεθόδων SYN Flooding, UDP Flooding, Slowloris Flooding και HTTP Flooding. Οι εντολές δίνονταν μέσω IRC.

Όπως αναφέρθηκε παραπάνω, το Skynet περιλάμβανε και το κακόβουλο λογισμικό Zeus, το οποίο είναι ένα Banking Trojan, ο πηγαίος κώδικας του οποίου, είχε διαρρεύσει καιρό πριν το συγκεκριμένο Botnet. Όπως και ο IRC C&C Server, έτσι και ο Zeus C&C Server βρισκόταν στο δίκτυο Tor και εμφανιζόταν ως κρυφή υπηρεσία.

Το Skynet έχει ενσωματωμένο το CGMiner, ένα Open Source Bitcoin Miner, το οποίο υποστηρίζει GPU και CPU mining. Το Skynet εγκαθιστά WH_MOUSE και WH_KEYBOARD, τα οποία παρακολουθούσαν στα μολυσμένα συστήματα τι πληκτρολογεί ο χρήστης και τις κινήσεις του ποντικιού. Αυτό γινόταν με σκοπό το κακόβουλο λογισμικό να εντοπίζει την αδράνεια στο υπολογιστή του θύματος. Μετά από δυο λεπτά αδράνειας στο μολυσμένο μηχάνημα, το κακόβουλο λογισμικό ξεκινούσε την διαδικασία του Bitcoin Mining και όταν εντόπιζε κάποια δραστηριότητα από την πλευρά του χρήστη, τότε σταματούσε κατευθείαν την διαδικασία. Τα μολυσμένα συστήματα λάμβαναν αποστολές από τους Servers. Οι Servers εκτελούσαν την εφαρμογή Bitcoin Mining Proxy, η οποία χρησιμοποιείται για να ελέγξει τις εργασίες που έχουν μοιραστεί και για να αναθέσει νέες. [15]

2. Mevade/Sefnit

Τον Αύγουστο του 2013, ο αριθμός των χρηστών του Tor αυξήθηκε από 1 σε 5 εκατομμύρια. Αυτή η αύξηση οφειλόταν στο Botnet Mevade/Sefnit. Το κακόβουλο λογισμικό Mevade/ Sefnit ήταν γνωστό από το 2010, ωστόσο τον Αύγουστο του 2013 χρησιμοποιήθηκε το δίκτυο Tor για τον έλεγχο του Botnet. Τη συγκεκριμένη χρονική περίοδο, αυξήθηκαν δραματικά οι χρήστες του Tor κυρίως στις ΗΠΑ, Ρωσία και Ουκρανία. Το κακόβουλο λογισμικό Mevade/ Sefnit μπορούσε να εγκατασταθεί στον υπολογιστή του θύματος με διάφορους τρόπους. Κάποιοι αξιοσημείωτοι τρόποι είναι το Adware InstallBrain και τα Adware Bprotect και FileScout.

Το InstallBrain είχε εγκατασταθεί σε εκατομμύρια υπολογιστές, ενώ υπήρχαν πάνω από 5 εκατομμύρια διαφορετικές παραλλαγές του συγκεκριμένου adware και είχε εντοπιστεί σε σχεδόν 150 χώρες. Το Mevade/Sefnit και το InstallBrain είχαν πολλές ομοιότητες στον κώδικα τους και στον τρόπο με τον οποίο επικοινωνούσαν με τους Command and Control Servers. Το InstallBrain προέρχονταν από την εταιρία Adware iBario.

Το κακόβουλο λογισμικό BKDR_MEVADE.A αρχικά επικοινωνούσε με τον C &C Server χρησιμοποιώντας πρωτόκολλο HTTP, αλλά ο μολυσμένος υπολογιστής λάμβανε και εκτελούσε εντολές από άλλον C &C Server, μέσω SSH , προκειμένου να υπάρξει μεγαλύτερη ασφάλεια στην επικοινωνία. Οι μετέπειτα εκδόσεις του MEVADE (BKDR_MEVADE.B και BKDR_MEVADE.C) χρησιμοποιούσαν Tor client για την σύνδεση με τον C & C Server, η διάδοση τους και η συμπεριφορά τους ήταν παρόμοια με την αρχική έκδοση.[46]

Το λογισμικό Sefnit είναι ένα κακόβουλο λογισμικό που βασίζει τη λειτουργία του στην επικοινωνία μέσω του δικτύου Tor. Όταν εκτελείται το κακόβουλο αρχείο, τότε εγκαθίσταται ο Tor client, εκτελείται ως υπηρεσία των Windows και εμφανίζεται με την ονομασία win.exe. Η υπηρεσία αυτή ξεκινάει κάθε φορά που εκκινεί ο υπολογιστής και είναι ρυθμισμένη έτσι ώστε να δέχεται TCP συνδέσεις στις πόρτες 9050 και 9051.

Η πόρτα 9051 είναι η θύρα ελέγχου για τη τοπική υπηρεσία Tor και χρησιμοποιείται για τον έλεγχο των περισσότερων πτυχών του Tor Client. Το κακόβουλο λογισμικό χρησιμοποιεί τη συγκεκριμένη πόρτα, προκειμένου να αποκτήσει πληροφορίες σχετικά την κατάσταση σύνδεσης του δικτύου Tor. Αυτό επιτυγχάνεται με την περιοδική αίτηση ενημερώσεων της κατάστασης, χρησιμοποιώντας τον έλεγχο πρωτοκόλλου.

Η πόρτα 9050 χρησιμοποιείται ως σημείο επικοινωνίας για τον SOCKS Proxy και επιτρέπει κάθε εφαρμογή, που είναι ρυθμισμένη να χρησιμοποιεί Proxy Server, να συνδέεται στο δίκτυο Tor. Το κακόβουλο λογισμικό χρησιμοποιεί τη συγκεκριμένη μέθοδο, προκειμένου να επικοινωνεί με τους C & C servers. Με αυτόν τον τρόπο, παρακάμπτεται η κλασική δομή δικτύου, καθώς η κίνηση μέσω του δικτύου Tor είναι κρυπτογραφημένη και έτσι αποτρέπονται δικτυακά προγράμματα IDS (Instruction Detection System) να εντοπίσουν το κακόβουλο λογισμικό.

Προκειμένου, οι μολυσμένοι υπολογιστές να επικοινωνήσουν με τους C& C Servers, το κακόβουλο λογισμικό περιέχει λίστα με .onion domains που επικοινωνούν με πρωτόκολλο HTTP over SOCKS. Η λίστα αυτή είναι αποθηκευμένη σε ένα συνδυασμό αρχείου και φακέλου, που φαίνεται να είναι τυχαία δημιουργημένα. Συγκεκριμένα, το κακόβουλο λογισμικό δημιουργεί ένα φάκελο και μέσα σε αυτό τοποθετεί δυο αρχεία με

δυο διαφορετικές επεκτάσεις .ct και .ph. Ο τυχαία παραγόμενος φάκελος δημιουργείται με την χρήση του αλγόριθμου κατακερματισμού MD4. Το αποτέλεσμα μετατρέπεται σε δεκαεξαδική μορφή και χρησιμοποιείται για το όνομα του καταλόγου.

Το αρχείο PH, χρησιμοποιείται ως διαγνωστικό του Botnet, καθώς τα δεδομένα μέσα σε αυτό παραμένουν στατικά. Σε αυτό περιέχεται η αλφαριθμητική τιμή GUID, η οποία είναι κρυπτογραφημένη με αλγόριθμο AES-256. Το αρχείο CT περιέχει τα πραγματικά δεδομένα διαμόρφωσης, που είναι κρυπτογραφημένα και αυτά με τον αλγόριθμο AES-256, με το ίδιο κλειδί κρυπτογράφησης. Τα κρυπτογραφημένα δεδομένα δημιουργήθηκαν με την χρήση βιβλιοθήκης Boost C++, που περιέχει την δημόσια διεύθυνση IP του θύματος, μια αλφαριθμητική τιμή ως ID, τη λίστα με τους C & C Domains και τον τρέχοντα κατάλογο του κακόβουλου λογισμικού.

Το Botnet MEVADE/SEFNIT χρησιμοποιείται για Click Fraud, για Bitcoin και Litecoin Mining, ενώ κάποιες εκδόσεις του Sefnit μπορούν να παρακολουθήσουν Internet Explorer και τον Mozilla Firefox και να παρεμβάλουν τα αποτελέσματα των μηχανών αναζήτησης.[46]

4.3 Malware μέσω Dark Web

Το Dark Web εκτός από την δημιουργία Botnets, χρησιμοποιείται και από κακόβουλο λογισμικό με σκοπό την απόκρυψη της ταυτότητας του επιτιθέμενου. Τα είδη των κακόβουλων λογισμικών που εκμεταλλεύονται το Dark Web είναι:

1) Trojan (Δούρειος Ίππος)

Το Trojan είναι ένα είδος κακόβουλου λογισμικού, το οποίο ξεγελάει τον χρήστη ο οποίος νομίζει ότι είναι κάποιο λειτουργικό πρόγραμμα. Οι χρήστες ξεγελιούνται από κάποια μορφή κοινωνικής μηχανικής (χειραγώγηση του χρήστη με σκοπό την απόσπαση πληροφοριών) και εκτελούν το πρόγραμμα στα συστήματα τους. Μόλις εκτελεστεί το πρόγραμμα επιτυχώς, οι επιτιθέμενοι μπορούν να αποκτήσουν backdoor πρόσβαση στο μολυσμένο σύστημα, να παρακολουθήσουν τις κινήσεις του χρήστη και να κλέψουν ευαίσθητα δεδομένα. Επιπλέον, μπορεί ο επιτιθέμενος να διαγράψει και να τροποποιήσει δεδομένα του συστήματος. Τα Trojans σε αντίθεση με τους ιούς και τα worms δεν

αναπαράγουν τον εαυτό τους. Τα Trojans κατηγοριοποιούνται με βάση τις ενέργειες που εκτελούν στις παρακάτω κατηγορίες:

α) Backdoor

Ένας Backdoor Trojan δίνει την δυνατότητα σε ένα κακόβουλο χρήστη να έχει απομακρυσμένη σύνδεση στο μολυσμένο σύστημα. Ο επιτιθέμενος έχει την δυνατότητα να πραγματοποιήσει όποια ενέργεια επιθυμεί στο μολυσμένο σύστημα όπως να αποστείλει, να λάβει, να εκκινήσει και να διαγράψει δεδομένα. Συνήθως το Backdoor Trojan χρησιμοποιείται για να δημιουργήσει δίκτυο botnet.

β) Exploit

Είναι προγράμματα τα οποία περιέχουν κώδικα ο οποίος εκμεταλλεύεται τις ευπάθειες εφαρμογών που εκτελούνται στον υπολογιστή του θύματος.

γ) Rootkit

Τα Rootkits σχεδιάζονται για να αποκρύψουν συγκεκριμένες δραστηριότητες στο μολυσμένο σύστημα. Συνήθως, ο κύριος σκοπός τους είναι να αποφευχθεί η ανίχνευση των κακόβουλων προγραμμάτων προκειμένου να παραταθεί η περίοδος που εκτελούνται στον μολυσμένο υπολογιστή.

δ) Banking Trojan

Είναι προγράμματα τα οποία σχεδιάστηκαν για να αποσπάσουν δεδομένα από τους online λογαριασμούς τραπεζών, από τα ηλεκτρονικά συστήματα πληρωμών και από τις χρεωστικές και πιστωτικές κάρτες.

ε) Trojan – Ddos

Είναι προγράμματα τα οποία διεξάγουν επιθέσεις σε συγκεκριμένη διεύθυνση στο διαδίκτυο. Αυτό πραγματοποιείται με την αποστολή αιτήσεων από ένα μολυσμένο

υπολογιστή σε άλλους μολυσμένους υπολογιστές προκειμένου να επιτεθούν στον στόχο και έτσι να οδηγήσουν σε άρνηση παροχής υπηρεσίας.

στ) Trojan Downloader

Μπορούν να κατεβάσουν και να εγκαταστήσουν νέες εκδόσεις κακόβουλων προγραμμάτων στον μολυσμένο υπολογιστή - συμπεριλαμβανομένων των Trojans και adware.

ζ) Trojan Dropper

Χρησιμοποιούνται από τους κακόβουλους χρήστες για την εγκατάσταση των trojans και / ή των ιών ή για την αποτροπή της ανίχνευσης κακόβουλων προγραμμάτων.

η) Trojan-Fake Antivirus

Προσομοιώνουν τη δραστηριότητα λογισμικού προστασίας από ιούς. Σχεδιάστηκαν για να εξαπατούν τον χρήστη ότι ο υπολογιστής είναι μολυσμένος με κακόβουλο λογισμικό και ζητούν ως αντάλλαγμα χρήματα για την ανίχνευση και την αφαίρεση των ανύπαρκτων απειλών.

θ) Trojan Instant Messaging

Κλέβουν τα στοιχεία σύνδεσης και τους κωδικούς πρόσβασης από προγράμματα άμεσων μηνυμάτων, όπως το Facebook Messenger, το Yahoo Messenger, το Skype και λοιπά.

ι) Trojan Ransom

Μπορεί να τροποποιήσει δεδομένα στον μολυσμένο υπολογιστή, έτσι ώστε ο υπολογιστής να μην λειτουργεί σωστά ή να μην μπορεί ο χρήστης να χρησιμοποιεί συγκεκριμένα δεδομένα. Θα ακολουθήσει ξεχωριστή ανάλυση για τα Ransomware.

ια) Trojan Spy

Μπορεί να παρακολουθήσει τον τρόπο με τον οποίο χρησιμοποιείται ο μολυσμένος υπολογιστής, για παράδειγμα, μπορεί να παρακολουθήσει τα δεδομένα που εισάγονται μέσω του πληκτρολογίου, να λάβει εικόνες από την οθόνη ή να λάβει μια λίστα με τις εφαρμογές που εκτελούνται.

ιβ) Trojan Mail finder

Μπορούν να συγκεντρώσουν διευθύνσεις ηλεκτρονικού ταχυδρομείου από τον μολυσμένο υπολογιστή.[59]

Όπως παρατηρούμε οι διάφορες κατηγορίες Trojan μπορεί να υποκλέπτουν διαφορετικά είδη δεδομένων από τους μολυσμένους υπολογιστές, ωστόσο το κοινό σημείο τους είναι ότι επικοινωνούν με τον επιτιθέμενο. Με την χρήση του δικτύου Tor διασφαλίζεται κρυπτογραφημένη και ανώνυμη επικοινωνία του μολυσμένου συστήματος με τον επιτιθέμενο, καθώς ο επιτιθέμενος εμφανίζεται ως κρυφή υπηρεσία του Tor ή χρησιμοποιεί κάποιο κόμβο εξόδου.

2. Ransomware

Το Ransomware είναι ένας τύπος κακόβουλου λογισμικού που εμποδίζει ή περιορίζει την πρόσβαση των χρηστών στο σύστημά τους, είτε με κλείδωμα της οθόνης του συστήματος είτε με κλείδωμα των αρχείων των χρηστών, έως ότου πληρωθούν λύτρα. Οι πιο σύγχρονοι τύποι ransomware είναι τα crypto-ransomware, τα οποία κρυπτογραφούν ορισμένους τύπους αρχείων στα μολυσμένα συστήματα και υποχρεώνουν τους χρήστες να πληρώνουν λύτρα με συγκεκριμένες μεθόδους πληρωμής, μέσω διαδικτύου για να αποκτήσουν το κλειδί αποκρυπτογράφησης.

Οι τιμές για την απόκτηση του κλειδιού αποκρυπτογράφησης ποικίλλουν ανάλογα με την παραλλαγή ransomware και την τιμή ή τις συναλλαγματικές ισοτιμίες των ψηφιακών νομισμάτων. Χάρη στην ανωνυμία που προσφέρουν ορισμένα κρυπτονομίσματα, οι επιτιθέμενοι καθορίζουν συνήθως τις πληρωμές σε bitcoins. Θα πρέπει ωστόσο να σημειωθεί ότι η πληρωμή των λύτρων δεν εγγυάται ότι θα αποκτηθεί το κλειδί αποκρυπτογράφησης ή το εργαλείο ξεκλειδώματος που απαιτείται, για να ανακτηθεί η πρόσβαση στο μολυσμένο σύστημα ή σε αρχεία που έχουν κλειδωθεί.

Τα Ransomware μπορούν να μολύνουν ένα σύστημα μέσω κακόβουλων ιστότοπων. Μπορεί επίσης, να έχουν τη μορφή λειτουργικού προγράμματος ή να ληφθούν από άλλο κακόβουλο λογισμικό. Ορισμένα ransomware αποστέλλονται ως συνημμένα αρχεία με μηνύματα ηλεκτρονικού ταχυδρομείου.

Όταν εκτελεστεί σε ένα σύστημα, το ransomware μπορεί είτε να κλειδώσει την οθόνη του υπολογιστή είτε στην περίπτωση του crypto-ransomware, να κρυπτογραφήσει κάποια συγκεκριμένα αρχεία. Στη πρώτη περίπτωση, εμφανίζεται μια εικόνα ή ειδοποίηση πλήρους οθόνης στην οθόνη του μολυσμένου συστήματος, η οποία εμποδίζει τα θύματα να χρησιμοποιούν το σύστημά τους. Στην οθόνη υπάρχουν οδηγίες για τον τρόπο με τον οποίο, οι χρήστες μπορούν να πληρώσουν τα λύτρα. Ο δεύτερος τύπος ransomware εμποδίζει την πρόσβαση σε δυνητικά κρίσιμα ή πολύτιμα αρχεία, όπως εικόνες, έγγραφα και βίντεο.[44]

4.3.1 Malware μέσω Tor

1. Chewbacca Malware

Το 2014 ερευνητές της εταιρίας RSA εντόπισαν μια υποδομή Server που χρησιμοποιούταν για να εξυπηρετεί ένα κακόβουλο λογισμικό, που έπληττε συσκευές POS (Point of Sale) και ήταν υπεύθυνο για την ηλεκτρονική κλοπή καρτών πληρωμής και προσωπικών δεδομένων από τις συσκευές POS, κυρίως στις ΗΠΑ, αλλά και σε άλλες 10 χώρες. Αυτό το κακόβουλο λογισμικό ήταν το Chewbacca, ένα Trojan, το οποίο είχε την δυνατότητα key-logging και σάρωσης της μνήμης σε συγκεκριμένα μηχανήματα POS. Ο σαρωτής μνήμης κακόβουλου λογισμικού εξήγαγε αντίγραφο από την μνήμη της συσκευής και έψαχνε τα δεδομένα της μαγνητικής λωρίδας της κάρτας. Όταν βρίσκονταν οι αριθμοί των καρτών τότε εξάγονταν και αποθηκεύονταν στον Server.

Αυτό που παρατήρησαν οι ερευνητές είναι ότι η επικοινωνία γίνονταν μέσω του δικτύου Tor, προκειμένου να αποκρυφθεί η IP του C&C Server. Για να επιτευχθεί η συγκεκριμένη επικοινωνία απαιτούνταν η εγκατάσταση εφαρμογής Tor Proxy στο μολυσμένο μηχάνημα.

Το Trojan ήταν αυτοδύναμο και δεν είχε δυναμική διαμόρφωση. Συντάχθηκε με Free Pascal 2.7.1, είχε μέγεθος 5mb, στα οποία περιλαμβάνονταν εκτελέσιμο αρχείο του Tor. Όταν εκτελούνταν, εγκαθιστούσε ένα αντίγραφο του εαυτού του, σε ένα αρχείο με την ονομασία spoolsv.exe. Το Trojan μεταμφίεζε τον εαυτό του στην εκτελέσιμη υπηρεσία Windows Print Spooler και τοποθετούνταν στον φάκελο Startup, έτσι ώστε να ξεκινάει αυτόματα με την έναρξη του μηχανήματος. Μετά την εγκατάσταση, ο keylogger δημιουργούσε ένα αρχείο με το όνομα system.log στον φάκελο system%temp%, στο οποίο καταγράφονταν ότι πληκτρολογούσε ο χρήστης.

Αν και έμοιαζε να είναι αρκετά απλό ως κακόβουλο λογισμικό και χωρίς μηχανισμούς άμυνας, σύμφωνα με τους ερευνητές έχει υποκλέψει 40 εκατομμύρια αριθμούς καρτών πληρωμής και προσωπικές πληροφορίες από 70 εκατομμύρια ανθρώπους.[28]

2. Bifrose malware

Το κακόβουλο λογισμικό Bifrose είναι ένα γνωστό backdoor, το οποίο χρησιμοποιούταν για στοχευμένες επιθέσεις, όπως για παράδειγμα στην εκστρατεία Spam “Here you have” που έλαβε μέρος το 2010. Στόχος της εκστρατείας ήταν κυβερνητικά γραφεία, όπως της Αφρικανικής Ένωσης και του NATO. Το 2014 ερευνητές της TrendMicro εντόπισαν μια έκδοση του Bifrose, την BKDR_BIFROSE.ZTBG-A, η οποία είχε την δυνατότητα να εκτελέσει τις εξής διεργασίες: αποστολή και λήψη αρχείων, λήψη πληροφοριών σχετικά με το αρχείο, δημιουργία/ διαγραφή/μετονομασία φακέλου, άνοιγμα αρχείου με την χρήση ShellExecute, εκτέλεση γραμμής εντολών, αρίθμηση όλων των ανοικτών παραθύρων και των Id των διεργασιών, κλείσιμο/ απόκρυψη παραθύρων, μετακίνηση παραθύρου σε πρώτο πλάνο, αποστολή των δεδομένων που πληκτρολογεί ο χρήστης και των κινήσεων του ποντικιού, τερματισμό μιας διεργασίας, ανέβασμα περιεχομένων του %Windows%\winieupdates\klog.dat και λήψη screenshot και εικόνας από την webcam. Το κακόβουλο λογισμικό έχει μέγεθος 85kb. Η συγκεκριμένη έκδοση είχε την ιδιότητα ότι μπορούσε να εκτελέσει τις παραπάνω εργασίες και να επικοινωνήσει με τον C&C server μέσω του δικτύου Tor. [9]

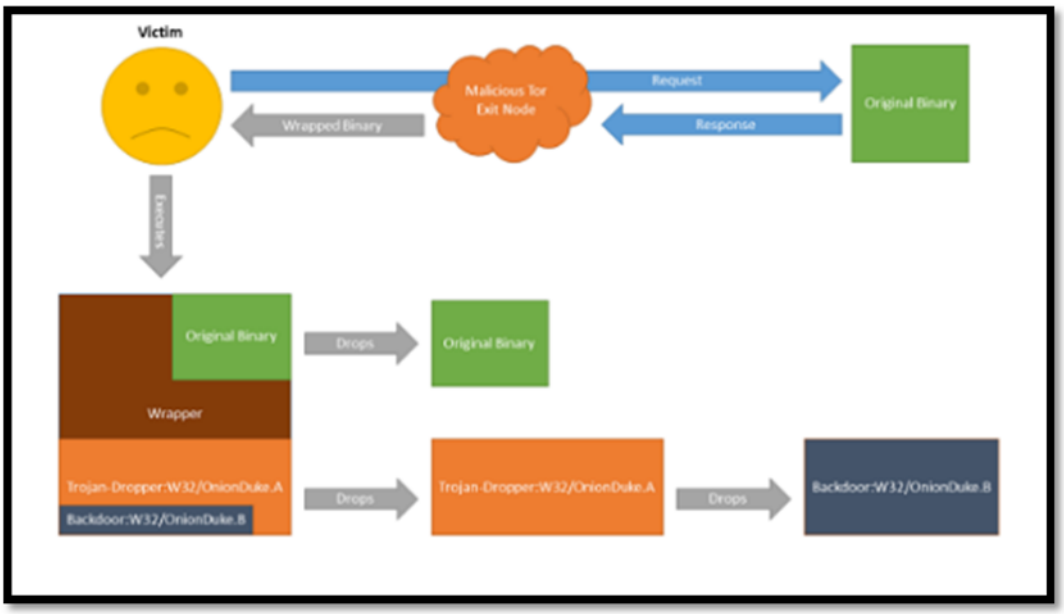
3. OnionDuke

Τον Νοέμβριο του 2014 ερευνητές της F- Secure ανακάλυψαν έναν κόμβο εξόδου του δικτύου Tor, που βρισκόταν στη Ρωσία, ο οποίος τροποποιούσε εκτελέσιμα αρχεία

Windows προσθέτοντας κακόβουλο λογισμικό κατά τη διάρκεια της λήψης. Ο κόμβος αυτός συνδέονταν με τους δημιουργούς του κακόβουλου λογισμικού Miniduke, το οποίο χρησιμοποιήθηκε για στοχευμένες επιθέσεις κατά του ΝΑΤΟ και ευρωπαϊκών κυβερνήσεων. Ωστόσο, το συγκεκριμένο κακόβουλο λογισμικό δεν αποτελεί κάποια έκδοση του Miniduke.

Όταν ένας χρήστης λάμβανε ένα εκτελέσιμο αρχείο, μέσω του κακόβουλου κόμβου εξόδου Tor, αυτό που λάμβανε ήταν ένα εκτελέσιμο "περιτύλιγμα" (Wrapper), που περιείχε το αρχικό εκτελέσιμο αρχείο αλλά και ένα δεύτερο ενσωματωμένο κακόβουλο εκτελέσιμο αρχείο. Με την χρήση ξεχωριστού περιτυλίγματος, παρακάμπτονταν οι έλεγχοι ακεραιότητας του αρχικού αρχείου. Όταν το αρχείο περιτύλιγμα εγγράφονταν στον σκληρό δίσκο, το αρχικό αρχείο εκτελούνταν ξεγελώντας τον χρήστη. Το κακόβουλο αρχείο ήταν ένας Dropper που περιείχε μια Portable Executable πηγή, η οποία εμφανιζόταν ως ενσωματωμένο αρχείο εικόνας GIF. Αυτή η πηγή, όμως, ήταν ένα κρυπτογραφημένο DLL (dynamically linked library) αρχείο. Ο Dropper αποκρυπτογραφούσε το DLL, το εγκαθιστούσε στον δίσκο και το εκτελούσε. Όταν εκτελούνταν το DLL (SHA1: b491c14d8cfb48636f6095b7b16555e9a575d57f, ανιχνεύονταν ως Backdoor:W32/OnionDuke.B), αποκρυπτογραφούσε ένα ενσωματωμένο αρχείο, το οποίο προσπαθούσε να συνδεθεί με C&C Servers. Το συγκεκριμένο κακόβουλο λογισμικό περιείχε στοιχεία τα οποία υπέκλεπταν διαπιστευτήρια login, συνέλλεγαν πληροφορίες σχετικά με το σύστημα όπως η ύπαρξη Antivirus, Firewall. Το πιο ενδιαφέρον αρχείο ήταν το αρχείο DLL Trojan-Dropper:W32/OnionDuke.A, καθώς υπήρχαν URL, τα οποία συνέδεαν το OnionDuke με το MiniDuke. Τέλος, το συγκεκριμένο κακόβουλο λογισμικό, καταδεικνύει τον κίνδυνο λήψης αρχείων από το δίκτυο Tor, καθώς ο χρήστης δεν γνωρίζει ποιος χειρίζεται τον κόμβο εξόδου και τι κίνητρα έχει. [2, 21]

.



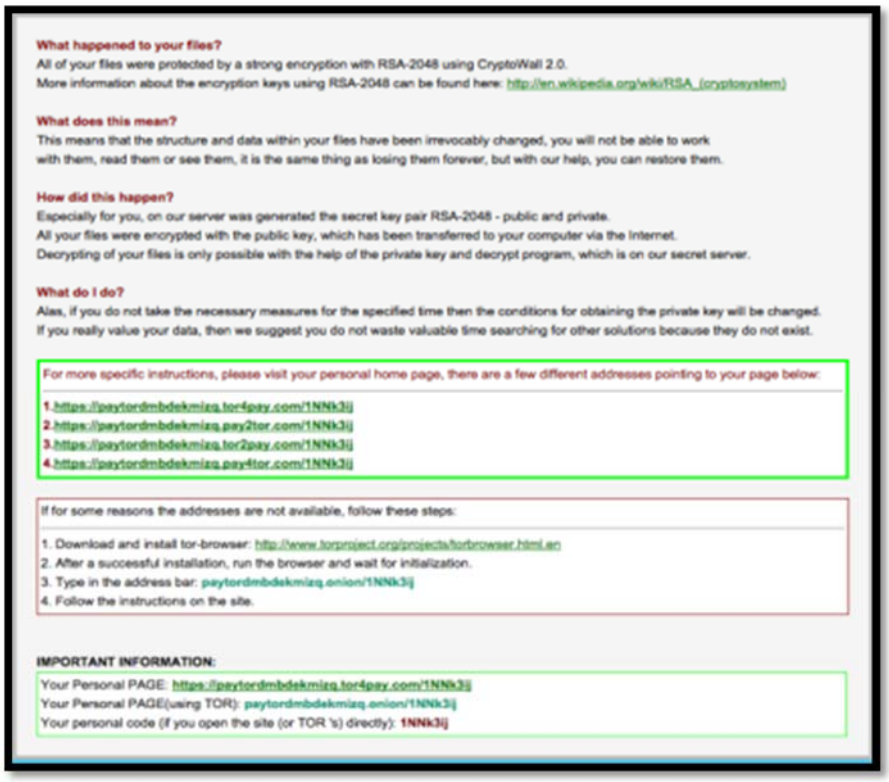
Εικόνα 9 Η λειτουργία του Onionduke (Πηγή: http://thehackernews.com/2014/11/onionduke-apt-malware-served-through_17.html)

4. Cryptowall 2.0

Το χαρακτηριστικό του Cryptowall 2.0 είναι ότι χρησιμοποιεί δίκτυο Tor, προκειμένου να αποκρύψει την επικοινωνία με το C&C server. Το κακόβουλο λογισμικό εκμεταλλεύεται ευπάθειες του λειτουργικού συστήματος Windows, προκειμένου να αποκτήσει πρόσβαση στον μολυσμένο υπολογιστή. Επιπλέον, εκτελεί ελέγχους Anti- VM και Anti-emulation, για να εμποδίσει την αναγνώριση του από Sandboxes. Ο Dropper και το Cryptowall διαθέτουν πολλαπλά επίπεδα κρυπτογράφησης. Το συγκεκριμένο Ransomware μπορεί να εκτελεστεί τόσο σε Windows 32-bit όσο και σε 64 bit.

Το Cryptowall 2.0 μπορεί να μολύνει έναν υπολογιστή με διάφορους τρόπους, όπως με συνημμένα αρχεία σε email και με μολυσμένα αρχεία pdf. Αρχικά, γίνεται εκμετάλλευση της ευπάθειας Win32k.sys Elevation of Privilege Vulnerability. Αυτή η ευπάθεια εμφανίζεται σε λειτουργικά συστήματα 32 bit, ενώ το Cryptowall περιλαμβάνει και 64 bit DLL, το οποίο μπορεί να εκμεταλλευτεί και ευπαθή AMD64 συστήματα Windows. Εάν γίνουν επιτυχώς οι έλεγχοι Anti-VM και Anti-emulation, το Cryptowall

αποκρυπτογραφείται και εγκαθίσταται στον μολυσμένο υπολογιστή, εμφανίζοντας τα ακόλουθα μηνύματα:



Εικόνα 10 (Πηγή: http://blogs.cisco.com/security/talos/cryptowall-2)

Το κακόβουλο λογισμικό είναι ένα Portable Executable (PE) αρχείο που είναι τρεις φορές κρυπτογραφημένο, αποκρυπτογραφείται, εξάγεται και εκτελείται. Το PE αυτό, είναι ουσιαστικά το Cryptowall με δυνατότητα επικοινωνίας μέσω του δικτύου Tor, καθώς υπάρχει Tor Client, ο οποίος υλοποιεί επικοινωνία με τους Command and Control Servers. Η σύνδεση με τον Server γίνεται με κρυπτογραφημένη SSL σύνδεση από τις πόρτες 443 και 9090. Μετά την επιτυχή σύνδεση, ξεκινάει να δημιουργεί Cryptowall Domain Names, χρησιμοποιώντας προσαρμοσμένο Domain Generation Algorithm (DGA). Εάν δεν υπάρξει κάποιο πρόβλημα με την κρυπτογραφημένη σύνδεση, τότε είναι εφικτή η επικοινωνία με τον Cryptowall Command and Control Server. Σε αντίθετη περίπτωση, μετά από κάποια δευτερόλεπτα προσπαθεί να συνδεθεί με άλλον server. Μετά την εγκατάσταση του, το Cryptowall 2.0 προσπαθεί να εντοπίσει την εξωτερική IP του δικτύου, χρησιμοποιώντας τη λειτουργία “GetExternalIpAddr”. [1]

5. CTB-Locker Ransomware

Το Ransomware CTB-Locker ή Citroni είναι ένα κακόβουλο λογισμικό, το οποίο μολύνει υπολογιστές με λειτουργικό σύστημα από Windows XP έως Windows 8. Επιπλέον, έπληξε και Web Servers με λειτουργικό σύστημα Linux. Η μόλυνση του υπολογιστή γίνεται είτε μέσω Spam emails, είτε με λήψη μολυσμένων αρχείων. Τα emails περιέχουν το Downloader με την ονομασία Dalexis ή Elenoocka, υπό την μορφή συνημμένου αρχείου, που έχει επέκταση cab. Το αρχείο περιέχει το κακόβουλο λογισμικό, συνήθως με επέκταση .scr, και ένα πλαστό έγγραφο σε μορφή κειμένου, προκειμένου να πείσει τον χρήστη ότι το αρχείο είναι ακίνδυνο. Το Dalexis χρησιμοποιεί διάφορες τεχνικές προκείμενου να αποφύγει τα Sandboxes και τα αυτόματα συστήματα ανάλυσης. Στη συνέχεια, το Dalexis λαμβάνει το CTB-Locker σε κρυπτογραφημένη μορφή μέσω HTTP, αποκρυπτογραφείται και εκτελείται. Όταν το CTB-Locker εκτελεστεί, τότε αντιγράφει τον εαυτό του στον φάκελο temp και δημιουργεί ένα προγραμματισμένο Task, προκειμένου να εκτελείται και μετά από επανεκκίνηση του υπολογιστή. Το CTB-locker δεν απαιτεί ενεργή σύνδεση με το διαδίκτυο προκειμένου να ξεκινήσει την κρυπτογράφηση των αρχείων του μολυσμένου υπολογιστή. Το CTB σημαίνει Curve-Tor-Bitcoin-Locker. Το Curve υποδεικνύει την χρήση της ελλειπτικής καμπύλης κρυπτογράφησης, η οποία είναι μια μορφή κρυπτογράφησης δημόσιου κλειδιού. Το CTB -Locker χρησιμοποιεί συνδυασμό συμμετρικής και ασύμμετρης κρυπτογράφησης. Η κρυπτογράφηση των αρχείων γίνεται με την χρήση του AES, όμως τα κλειδιά που χρησιμοποιούνται για την αποκρυπτογράφηση είναι κρυπτογραφημένα με ελλειπτική καμπύλη κρυπτογράφησης. Τα κρυπτογραφημένα αρχεία έχουν κατάληξη .ctbl και το CTB-Locker Rasnsomware δημιουργεί τα αρχεία AllFilesAreLocked.bmp και DecryptAllFiles.txt σε κάθε φάκελο που περιέχει κρυπτογραφημένα αρχεία. Προκειμένου να αποκρυπτογραφηθούν τα αρχεία του χρήστη, απαιτείται πληρωμή σε Bitcoins.

Οι δημιουργοί του συγκεκριμένου λογισμικού χρησιμοποιούν το δίκτυο Tor για να κρύψουν τα στοιχεία τους. Στα αρχεία AllFilesAreLocked.bmp και DecryptAllFiles.txt περιγράφεται πως να εγκαταστήσει ο χρήστης τον Tor browser, να επισκεφθεί τη διεύθυνση http://zaxseiufetlkwpeu.onion, να εισάγει ένα δημόσιο κλειδί (το οποίο δίνεται στο αρχείο) και στη συνέχεια να ακολουθήσει τις οδηγίες που εμφανίζονται στη σελίδα. Οι οδηγίες αυτές αφορούν τα bitcoins αλλά και την διεύθυνση στην οποία θα γίνει η κατάθεση. Τέλος, οι δημιουργοί του CTB-Locker προσφέρουν δωρεάν την αποκρυπτογράφηση 2 αρχείων. [53]

6. WannaCry Ransomware

Το 'WannaCry' ήταν μια παραλλαγή ransomware επηρέασε πολλές οργανώσεις ανά τον κόσμο, όπως τη Telefonica στην Ισπανία, την Εθνική Υπηρεσία Υγείας στο Ηνωμένο Βασίλειο και την FedEx στις ΗΠΑ. Το κακόβουλο λογισμικό σάρωνε τη θύρα 445 (Server Message Block / SMB), και εξαπλωνόταν όπως ένα worm, κρυπτογραφούσε τα αποθηκευμένα αρχεία στα συστήματα και στη συνέχεια απαιτούσε πληρωμή λύτρων με τη μορφή Bitcoin. Εκτός από την εξάπλωση του στα εσωτερικά δίκτυα είχε την δυνατότητα να εντοπίζει ευπάθειες και να εξαπλώνεται σε συστήματα μέσω του διαδικτύου. Επιπλέον, εγκαθιστούσε backdoor στα μολυσμένα συστήματα που επέτρεπε την εγκατάσταση κακόβουλου λογισμικού.

Όταν το κακόβουλο λογισμικό μόλυνε το σύστημα, τότε κρυπτογραφούσε τα έγγραφα και τα αρχεία εικόνων, ήχου και βίντεο με τον αλγόριθμο RSA 2048-bit και δημιουργούσε ένα νέο ευρετήριο /Tor/ στο οποίο τοποθετούσε ένα εκτελέσιμο αρχείο Tor. Στην συνέχεια δημιουργούσε συνδέσεις με το δίκτυο Tor, προκειμένου να διασφαλίσει την ανωνυμία του.

4.3.2 Malware μέσω I2P

CryptoWall 3.0

Το Cryptowall 3.0 είναι η εξέλιξη του Cryptowall 2.0. Ο βασικός τρόπος διασποράς του Cryptowall είναι με την αποστολή email. Το email έχει συνημμένο ένα αρχείο Rar το οποίο περιέχει ένα αρχείο μορφής CHM, που όταν ανοιχτεί λαμβάνει το Cryptowall. Το αρχείο CHM είναι ένα διαδραστικό αρχείο, το οποίο είναι συμπιεσμένο, ενώ μπορεί να περιέχει και Javascript ή αρχεία εικόνας. Όταν το Cryptowall εκτελεστεί, ξεκινάει μια νέα explorer.exe διαδικασία, εισάγει τον κώδικα του σε αυτή και τον εκτελεί. Στη συνέχεια, για να εξασφαλίσει ότι δεν μπορούν να ανακτηθούν τα κρυπτογραφημένα αρχεία, διαγράφει τα αντίγραφα volume shadow και χρησιμοποιεί το εργαλείο vssadmin.exe. Το αρχικό Binary του Cryptowall αντιγράφεται σε διάφορες τοποθεσίες, όπως είναι το appdata, startup, rootdrive. Αυτά τα αντίγραφα προστίθενται στο auto start key, ενώ προστίθενται και τιμές στο Run και στο RunOnce στο Registry, έτσι ώστε να εκτελούνται

και όταν πραγματοποιείται επανεκκίνηση του υπολογιστή. Στη συνέχεια, ξεκινάει μια νόμιμη διαδικασία svhost.exe με δικαιώματα χρήστη, στην οποία εισάγει τον κακόβουλο binary κώδικα. Ο αλγόριθμος κρυπτογράφησης που χρησιμοποιεί το Cryptowall 3.0 είναι ο AES 256. Κάθε αρχείο που προσβάλλει το κακόβουλο λογισμικό, αντιγράφεται με ένα τυχαίο χαρακτήρα, κρυπτογραφείται το περιεχόμενο του και ακολούθως το αρχικό αρχείο διαγράφεται. Κάθε κρυπτογραφημένο αρχείο ξεκινάει με την τιμή κατακερματισμού του δημόσιου κλειδιού, που λαμβάνεται από τον Server. Όλα τα κρυπτογραφημένα ονόματα αρχείων αποθηκεύονται στο Registry HKCU\Software\<unique Identifier>.

Το Cryptowall αποκτά πληροφορίες του συστήματος και δημιουργεί μια τιμή κατακερματισμού MD5, η οποία είναι το Victim ID. Ένα από τα καινούρια χαρακτηριστικά του Cryptowall 3.0 είναι ότι χρησιμοποιεί το δίκτυο I2P για επικοινωνία με τους C & C servers. Οι Urls που χρησιμοποιεί είναι οι proxy1-1-1.i2p, proxy2-2-2.i2p, proxy3-3-3.i2p, proxy4-4-4.i2p και proxy5-5-5.i2p. Σε αυτά στέλνει το Victim Id και ο C & C Server καταχωρεί το μολυσμένο μηχάνημα ζητώντας μια αλφαριθμητική τιμή, η οποία έχει την εξής μορφή: {<Request ID>|crypt1|<Victim PC MD5>|<OS Ver Index>.||External Ip Address}. Η παραπάνω τιμή είναι κωδικοποιημένη για το δίκτυο I2P και αποστέλλεται μέσω ενός I2P proxy. Η λίστα με τους I2P proxy περιέχει τις ακόλουθες διευθύνσεις: 91.121.12.127:4141, 5.199.165.160:8080, 94.247.28.26:2525, 94.58.109.158:2525, 195.29.106.157:4444, 94.247.31.19:8080, 194.58.109.137:3435, 94.247.28.156:8081, 209.148.85.151:8080. Το Cryptowall αναζητεί τις παραπάνω διευθύνσεις, από τις οποίες θα συνδεθεί στο I2P. Αποτελεί ακόμη ένα Ransomware το οποίο για να αποκρυπτογραφηθούν τα αρχεία, οι δημιουργοί του απαιτούν πληρωμή σε Bitcoins.[52]

4.4 Παράνομες ανώνυμες υπηρεσίες

Στην ενότητα αυτή θα αναφερθούν διάφορες παράνομες υπηρεσίες, που εκμεταλλεύονται την ανωνυμία του Dark Web. Αρχικά θα αναλυθεί ο τρόπος λειτουργίας του Silk Road, μια από τις μεγαλύτερες αγορές του Dark Web και θα γίνει αναφορά και σε άλλες υπηρεσίες που προσφέρονται στο Dark Web. Αξίζει να αναφερθεί η παρουσία διάφορων ομάδων στο Dark Web με κοινά ενδιαφέροντα, η δημιουργία των οποίων αποσκοπεί στην ανταλλαγή σχετικών πληροφοριών και απόψεων. Οι συμμετέχοντες στις παραπάνω ομάδες πωλούν τις υπηρεσίες τους

εκεί μεμονωμένα ή ως μέρος αυτών των ομάδων. Ενδεικτικά, κάποιες τέτοιες ομάδες είναι οι: xDedic, hackforum, Trojanforge, Mazafaka, dark0de και TheRealDeal darknet, The Hub. Πληροφορίες για σύσταση και διενέργεια ηλεκτρονικών εγκλημάτων καθώς και υπηρεσίες hacking για χρηματοπιστωτικά ιδρύματα και τράπεζες έχουν επίσης προσφερθεί μέσω των παραπάνω ομάδων επικοινωνίας. Τέλος, θα γίνει αναφορά στο Bitcoin, το οποίο αποτελεί τον βασικό τρόπο πληρωμής των παράνομων υπηρεσιών.

4.4.1 Black Markets

Η πώληση λαθραίων ή παράνομων προϊόντων εμφανίστηκε με την ευρεία εξάπλωση του διαδικτύου, με την ύπαρξη forums και συστημάτων με πίνακες ανακοινώσεων, όπου υπήρχε η αλληλεπίδραση πωλητών και αγοραστών. Οι online αγορές γνώρισαν σημαντική ανάπτυξη στην πολυπλοκότητα και στην κλίμακα τους. Πολλές διαδικτυακές ανώνυμες αγορές λειτουργούν ως κρυφές υπηρεσίες στο δίκτυο Tor, οι οποίες παρέχουν στους συμμετέχοντες, αγοραστές και πωλητές, ανώνυμη επικοινωνία. Οι ανώνυμες αγορές χρησιμοποιούν ως σύστημα πληρωμών Online ψευδώνυμα νομίσματα, όπως το Bitcoin, προκειμένου να πραγματοποιούν ανώνυμες συναλλαγές.

Το κοινό αυτών των αγορών είναι ότι κυρίως δεν κάνουν λαθρεμπόριο προϊόντων, αλλά πραγματοποιούν συναλλαγές παράνομων προϊόντων και υπηρεσιών. Οι ανώνυμες αγορές αναλαμβάνουν να διαχειριστούν διάφορα είδη ρίσκων. Πρώτον, αντικαθιστούν τις φυσικές συναλλαγές και αυτό έχει ως αποτέλεσμα να μειώνεται η πιθανότητα βίας κατά την διάρκεια της συναλλαγής. Δεύτερον, η ανωνυμία στις συναλλαγές προσφέρει την προστασία παρέμβασης από δυνάμεις επιβολής του νόμου. Τρίτον, οι ανώνυμες αγορές προσφέρουν ένα σύστημα χρηματικής εγγύησης, προκειμένου να αποτρέψουν τα οικονομικά ρίσκα και τις απάτες. Το σύστημα αυτό λειτουργεί με τον ίδιο τρόπο που λειτουργούν και οι εμπορικές αγορές, όπως το eBay και Amazon. Όταν ένας αγοραστής αγοράζει ένα προϊόν, δεν πληρώνει απευθείας τον πωλητή, αλλά κρατάει τα λεφτά ως εγγύηση η ηλεκτρονική αγορά. Ο αγοραστής πρέπει να δώσει θετικό Feedback προκειμένου να αποδεσμευθούν τα χρήματα προς τον πωλητή. Τέλος, με την ύπαρξη του Feedback, υπάρχει έλεγχος της ποιότητας των προϊόντων των οποίων πωλούν.

Μια από τις πιο ενεργές αγορές ήταν το Silk Road, το οποίο ήταν μια κρυφή υπηρεσία στο δίκτυο Tor. Το Silk Road ήταν μια online αγορά, η οποία έδινε την δυνατότητα σε πωλητές

να προσφέρουν παράνομα προϊόντα και υπηρεσίες, ενώ με την χρήση του δικτύου Tor διασφαλίζονταν η ανωνυμία τόσο των πωλητών όσο και των αγοραστών. Ιδιοκτήτης της σελίδας εμφανίζονταν με το ψευδώνυμο Dread Pirate Roberts (DPR) και είχε στην κατοχή του Bitcoin αξίας εκατοντάδων εκατομμυρίων δολαρίων. Την 1 Οκτωβρίου 2013 συνελήφθη ο 29 χρόνος Ross William Ulbricht, ο οποίος φέρεται να είναι ο DPR.

Οι μοναδικοί επισκέπτες του Silk Road υπολογίζονται σε εκατοντάδες χιλιάδες από όλο τον κόσμο, με το 30% από αυτούς να προέρχονται από τις ΗΠΑ. Η ανάπτυξη του ήταν ραγδαία και το Σεπτέμβριο του 2013 είχε καταχωρημένα σχεδόν 13000 είδη ναρκωτικών και παράνομων υπηρεσιών.

Η μοναδική μορφή πληρωμής που δέχονταν το SilkRoad ήταν τα Bitcoin. Το σύστημα πληρωμών αποτελούνταν από ένα εσωτερικό σύστημα Bitcoin, στο οποίο κάθε χρήστης θα έπρεπε να διατηρεί λογαριασμό, ώστε να πραγματοποιεί τις συναλλαγές του στη σελίδα. Οι λογαριασμοί αυτοί ήταν αποθηκευμένοι σε Wallets τα οποία βρίσκονταν σε Servers που διατηρούνταν από το Silk Road. Οι χρήστες θα έπρεπε να έχουν καταθέσει Bitcoins στον λογαριασμό του Silk Road. Έπειτα, ήταν ελεύθεροι να χρησιμοποιήσουν αυτά τα Bitcoin για να αγοράσουν προϊόντα ή υπηρεσίες από την σελίδα. Όταν πραγματοποιούνταν μια συναλλαγή, τότε ο αντίστοιχος αριθμός των Bitcoins μεταφέρονταν σε δεσμευμένο λογαριασμό, που διατηρούνταν από το Silk Road, αναμένοντας την ολοκλήρωση της συναλλαγής. Όταν η συναλλαγή ολοκληρωνόταν, τότε τα Bitcoins του αγοραστή μεταφέρονταν από τον δεσμευμένο λογαριασμό του Silk Road στην Bitcoin διεύθυνση του πωλητή. Η προμήθεια που λάμβανε το Silk Road κυμαίνονταν ανάλογα με το μέγεθος της συναλλαγής, αλλά συνήθως ήταν από 8 έως 15 τις εκατό της συνολικής αξίας της αγοράς. Με την χρήση του Tor και των Bitcoins εξασφαλίζονταν ανωνυμία, ωστόσο όταν ένας χρήστης αγόραζε ένα προϊόν θα έπρεπε να δηλώσει στον αγοραστή μια φυσική διεύθυνση αποστολής. Η σελίδα πρότεινε στους αγοραστές να δηλώνουν διευθύνσεις δημοσίων χώρων ή ταχυδρομικές θυρίδες. Μόλις ο πωλητής έστελνε το αντικείμενο και ενημέρωνε την σελίδα για την αποστολή, τότε το ιστορικό της διεύθυνσης διαγραφόταν. Όταν ο αγοραστής ενημέρωνε ότι έλαβε το αντικείμενο, τότε το Silk Road απελευθέρωνε τη πληρωμή προς τον πωλητή. Τέλος, ο αγοραστής έγραφε κριτική για τον πωλητή. Η ολοκλήρωση της αγοράς ήταν υποχρεωτική και στη

περίπτωση που ο αγοραστής ξεχνούσε να ολοκληρώσει την συναλλαγή, τότε η σελίδα την ολοκλήρωνε αυτόματα.

Λόγω της μορφής του url των σελίδων onion είναι δύσκολη η απομνημόνευση τους. Για αυτό το λόγο, υπάρχουν σελίδες οι οποίες περιέχουν λίστες με συνδέσμους .onion των κρυφών υπηρεσιών που υπάρχουν στο δίκτυο Tor. Μια από τις πιο γνωστές σελίδες είναι το Hidden Wiki (http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main Page), ενώ υπάρχουν και άλλες παρόμοιες ιστοσελίδες, όπως το Torlinks (http://torlinkbgs6aabns.onion/) και OnionDir (http://dirnxxdraygbifgc.onion/).

Μια ενδιαφέρουσα μηχανή αναζήτησης, το Grams (http://grams7enufi7jmdl.onion/), που ξεκίνησε τη λειτουργία της τον Απρίλιο του 2014, προσφέρει στους χρήστες τη δυνατότητα αναζήτησης παράνομων προϊόντων (όπλων, ναρκωτικών κλπ) και υπηρεσιών. Η αρχική σελίδα μοιάζει με αυτή του Google και έχει μια μπάρα αναζήτησης, ενώ χρησιμοποιεί ένα Application Programming Interface και αναζητεί τα περιεχόμενα από διάφορες αγορές όπως το London Underground και Alphabay .Ο χρήστης πληκτρολογεί στην μπάρα αναζήτησης το προϊόν για το οποίο ενδιαφέρεται και το Grams πραγματοποιεί την αναζήτηση και εμφανίζει τα αποτελέσματα. Επιλέγοντας το Infodesk το Grams, παρέχει πληροφορίες σχετικά με τους πωλητές και τις ανώνυμες αγορές, καθώς υπάρχουν οι λίστες Top Vendors - καλύτεροι πωλητές και Scammers - χειρότεροι πωλητές. Ακόμη, υπάρχει η επιλογή Market Status στην οποία φαίνεται αν οι πιο δημοφιλείς αγορές είναι online και η επιλογή Flow προκειμένου ο χρήστης να μεταφέρεται στις σελίδες των αγορών. Επίσης, προσφέρει την υπηρεσία Helix, που είναι ένα Bitcoin cleaner με το οποίο οι χρήστες μπορούν να λάβουν νέα Bitcoins, πληρώνοντας προμήθεια. Τέλος, από τον Μάρτιο του 2017, στην αρχική σελίδα εμφανίζεται Captcha, ώστε να αποφεύγονται Ddos επιθέσεις.

Διάδοχοι του Silk Road, μπορούν να θεωρηθούν τα Alpha Bay Market - http://pwoah7foa6au2pul.onion/login.php, Dream Market - http://lchudifyeqm4ldjj.onion/, Vahala http://valhallaxmn3fydu.onion/intl/categories/1000, Hansa - http://hansamkt2rr6nfg3.onion/, Tochka http://tochka3evlj3sxdv.onion/ .[37]

4.5 Crypto currency – Bitcoin

Στις ενότητες με τις κακόβουλες επιθέσεις Ransomware παρατηρούμε ότι οι κυβερνοεγκληματίες, προκειμένου να αποκρυπτογραφήσουν τα δεδομένα, απαιτούν τα "λύτρα" σε bitcoin. Ακόμη, ορισμένα botnets (Skynet, Mevade) έχουν ως λειτουργία το Bitcoin Mining. Επίσης, στις κρυφές υπηρεσίες του δικτύου Tor, οι πληρωμές γίνονται με Bitcoin. Το Bitcoin είναι το πιο γνωστό Cryptocurrency. Το λεξικό της Οξφόρδης ορίζει ως cryptocurrency "*ένα ψηφιακό νόμισμα στο οποίο οι τεχνικές κρυπτογράφησης χρησιμοποιούνται για να ρυθμίσουν την παραγωγή των μονάδων του νομίσματος και να ελέγξουν την μεταφορά κεφαλαίων. Τα κρυπτονομίσματα λειτουργούν ανεξάρτητα από μια κεντρική τράπεζα*".

Η πρώτη πρόταση για μη ανιχνεύσιμες συναλλαγές έγινε το 1983 από τον Chaum, ο οποίος πρότεινε ένα σύστημα με μετρητά που εκδίδονται από μια τράπεζα, υπό τη μορφή νομισμάτων που είναι υπογεγραμμένα "τυφλά". Τα μη "τυφλά¨ νομίσματα ανταλλάσσονται μεταξύ φυσικών προσώπων και εταιριών και είναι εξαγοράσιμα, αφού πρώτα η τράπεζα επαληθεύσει ότι δεν έχουν προηγουμένως εξαγοραστεί. Οι τυφλές υπογραφές δεν επέτρεπαν στις τράπεζες να συνδέσουν τα νομίσματα με αυτούς που τα χρησιμοποιούν. [4]

Την δεκαετία του 1990 υπήρξαν προτάσεις για τη δημιουργία ηλεκτρονικού νομίσματος χωρίς την διαμεσολάβηση τράπεζας. Εταιρίες όπως η Peppercoin και η Digicash δημιουργήθηκαν με αυτό τον σκοπό, όμως απέτυχαν. Την ίδια δεκαετία προτάθηκαν κάποια από τα χαρακτηριστικά τα οποία έχει το Bitcoin σήμερα, όπως οι Proof of Work γρίφοι, η δημόσια καθολική λογιστική με την οποία μπορεί να ανιχνευτεί τυχόν προηγούμενη χρήση των νομισμάτων και οι έξυπνες επαφές, οι οποίες επιτρέπουν σε δυο χρήστες να συνάπτουν επίσημη συμφωνία με την χρήση κρυπτογραφίας. [4]

Το 2008 ο Satoshi Nakamoto (ψευδώνυμο) περιέγραψε τη λειτουργία του Bitcoin[4]. Η δημιουργία του πρώτου Bitcoin block έγινε στις 3 Ιανουαρίου 2009, ενώ η πρώτη συναλλαγή πραγματοποιήθηκε το Μάιο του 2010, όπου ένας χρήστης παρήγγειλε μια πίτσα για 10000 Bitcoins. Από τότε πολλές εταιρίες και υπηρεσίες υιοθέτησαν τα Bitcoins ως τρόπο πληρωμής, ενώ η αξία τους αυξήθηκε κατακόρυφα [4].

Η κατάσταση των Bitcoins αναπαρίσταται με συναλλαγές. Οι συναλλαγές εκδίδονται κυρίως για ανταλλαγή νομισμάτων μεταξύ των χρηστών. Η συναλλαγή των Bitcoins κρυπτογραφείται με αλγόριθμο κατακερματισμού SHA-256 και η τιμή κατακερματισμού αποτελεί την ταυτότητα της συναλλαγής. Τα δεδομένα που εξάγονται από μια συναλλαγή περιέχουν μια ακέραια τιμή, η οποία αναπαριστά την ποσότητα των Bitcoins. Η ακρίβεια της συγκεκριμένης τιμής ορίζει τις υποδιαιρέσεις του νομίσματος, με τη μικρότερη υποδιαίρεση να είναι το Satoshi. Ένα Bitcoin υποδιαιρείται σε 10^8 Satoshis. Τα εξαγόμενα δεδομένα της συναλλαγής περιέχουν έναν κωδικό, ο οποίος ονομάζεται ScriptPubkey και καθορίζει τους όρους υπό τους οποίους τα εξαγόμενα δεδομένα συναλλαγής μπορούν να εξαργυρωθούν, ακόμη και ως δεδομένα που θα εισαχθούν σε μελλοντική συναλλαγή. [4]

Τα εισαγόμενα δεδομένα μιας συναλλαγής είναι:

α) Οι προηγούμενες συναλλαγές των Bitcoins, που φαίνονται από την τιμή κατακερματισμού των Bitcoins.

β) Ένας κατάλογος που περιέχει τα εξαγόμενα δεδομένα των συναλλαγών και ένα κομμάτι κώδικα, ο οποίος επικυρώνει ότι η συναλλαγή κάλεσε το scriptSig.
Το scriptSig είναι ένα δημόσιο κλειδί και μια υπογραφή. Για να εξαργυρωθεί μια προηγούμενη συναλλαγή, θα πρέπει να εκτελεστούν επιτυχώς το ScriptSig και το ScriptPubKey. [4]

Για την λειτουργία των Bitcoins δεν υπάρχει ιδιόκτητης ο οποίος κατέχει λογαριασμό με bitcoins, αλλά υπάρχει ένας χρήστης που γνωρίζει ένα ιδιωτικό κλειδί, το οποίο μπορεί να υπογράψει και να εξαργυρώσει τα δεδομένα εξόδου. Επομένως ο χρήστης κατέχει όσα Bitcoin μπορεί να εξαργυρώσει. Οι τιμές κατακερματισμού των δημόσιων κλειδιών των συναλλαγών “pay to pub key hash” λειτουργούν ως ψευδώνυμες ταυτότητες, οι οποίες είναι γνωστές ως διευθύνσεις- addresses και για αυτές δεν απαιτούνται τα πραγματικά στοιχεία των χρηστών.[4]

Προκειμένου, να εξασφαλισθεί ότι ένας χρήστης δεν θα εξαργυρώσει την ίδια συναλλαγή σε δυο διαφορετικούς χρήστες, το Bitcoin υιοθετεί μια απλή προσέγγιση, που είναι η υποχρεωτική δημοσίευση όλων των συναλλαγών σε ένα παγκόσμιο και μόνιμο αρχείο

καταγραφής συναλλαγών. Για να επικυρωθεί μια συναλλαγή, απαιτείται η επαλήθευση των Scripts της συναλλαγής, αλλά και η επιτυχής δημοσίευση της συναλλαγής στο αρχείο καταγραφής. Το αρχείο καταγραφής υλοποιείται ως μια σειρά από πακέτα-σύνολα συναλλαγών, που κάθε ένα πακέτο περιέχει τιμή κατακερματισμού του προηγούμενου πακέτου συναλλαγών, θεωρώντας το προηγούμενο πακέτο ως το μοναδικό προγενέστερο του. Το αρχείο καταγραφής συναλλαγών είναι γνωστό ως Block Chain. Ο σχεδιασμός απαιτεί καθολική αναγνώριση και συναίνεση στο περιεχόμενο του. Για αυτό το Bitcoin δημιούργησε ένα αποκεντρωμένο, ψευδώνυμο πρωτόκολλο, το οποίο ονομάζεται Nakamoto Consesus (γενική συναίνεση). Η λειτουργία του πρωτοκόλλου προβλέπει ότι κάθε χρήστης μπορεί να προσθέσει στην αλυσίδα (chain) ένα πακέτο (block) συναλλαγών συλλέγοντας έγκυρες συναλλαγές. Το βασικό στοιχείο είναι η χρήση ενός υπολογιστικού γρίφου, ο οποίος καθορίζει ποιου χρήστη το Block θα είναι το επόμενο Block στην αλυσίδα. Το Block το οποίο επιλέγεται είναι το πρώτο έγκυρο Block, που περιέχει σωστή λύση στον υπολογιστικό γρίφο. Όταν οι υπόλοιποι συμμετέχοντες μάθουν για το έγκυρο Block, ξεκινάνε να δουλεύουν για το επόμενο κοκ. Εάν κάποιο από τα Blocks περιέχει μη έγκυρες συναλλαγές ή περιέχει σφάλματα, οι υπόλοιποι συμμετέχοντες το απορρίπτουν και συνεχίζουν μέχρι να βρουν λύση για έγκυρο Block.

Ένα στοιχείο του πρωτοκόλλου είναι ότι ένας συμμετέχων που βρίσκει ένα Block μπορεί να παράγει συγκεκριμένο ποσό νομίσματος, το οποίο μεταφέρεται στη διεύθυνση της επιλογής του. Προηγουμένως αναφέρθηκε ο όρος Miners, οι οποίοι είναι οι συμμετέχοντες στην παραπάνω διαδικασία και ονομάζονται έτσι διότι εργάζονται για να λύσουν υπολογιστικούς γρίφους με αντάλλαγμα χρήματα. Το νόμισμα που παράγεται ονομάζεται ανταμοιβή Block (Block reward) και ουσιαστικά δίνει κίνητρο στους Miners να εργάζονται μόνο για έγκυρα Blocks. [4]

Ο υπολογιστικός γρίφος απαιτεί την εύρεση μιας τιμής κατακερματισμού SHA 256. Συγκεκριμένα, ο γρίφος είναι η εύρεση ενός συγκεκριμένου Block, η τιμή κατακερματισμού SHA 256 του οποίου είναι μικρότερη από την τιμή-στόχο. Το συγκεκριμένο Block αποτελείται από λίστα προηγούμενων συναλλαγών, την τιμή κατακερματισμού του προηγούμενου Block, μια χρονική σφραγίδα, τον αριθμό έκδοσης και μια τυχαία τιμή. Η τυχαία φύση του γρίφου είναι πολύ σημαντική, διαφορετικά ο Miner με την μεγαλύτερη υπολογιστική ισχύ θα εύρισκε πρώτος το Block. [4]

Το Bitcoin βασίζεται στην κρυπτογράφηση δημόσιου κλειδιού για αυθεντικοποίηση. Υπάρχουν διάφοροι τρόποι διατήρησης των κλειδιών των Bitcoins. Η πιο απλή μέθοδος διατήρησης των κλειδιών είναι η αποθήκευση τους σε σκληρό δίσκο, ωστόσο η συγκεκριμένη μέθοδος είναι ευάλωτη σε κακόβουλο λογισμικό, που μπορεί να υποκλέψει τα κλειδιά. Για να αποφευχθεί η αποθήκευση των κλειδιών σε ένα σημείο, υπάρχει η δυνατότητα αποθήκευσης με την χρήση Script με πολλαπλές υπογραφές, οι οποίες προσδιορίζουν δημόσια κλειδιά. [4]

Ο Bitcoin Client επιτρέπει την αποθήκευση των κλειδιών των Bitcoins σε αρχείο που είναι κρυπτογραφημένο με κλειδί που προκύπτει από κωδικό που επέλεξε ο χρήστης. Τα wallets που είναι προστατευμένα με password προσφέρουν ασφάλεια ενάντια σε διαφόρων τύπων κλοπές, όμως οι χρήστες δεν μπορούν να έχουν πρόσβαση στα χρήματα τους από άλλη συσκευή πέρα από αυτή που αποθήκευσαν τα κλειδιά. Υπάρχουν Wallets τα οποία επιλέγουν αυτά τον κωδικό, ο οποίος προκύπτει από φράση την οποία επιλέγει ο χρήστης. Είναι δυνατή η πρόσβαση στα χρήματα από διαφορετικές συσκευές, όμως εάν ο κωδικός ξεχαστεί, τότε χάνεται και η πρόσβαση στα χρήματα. [4]

Η τελευταία κατηγορία των Online Wallets είναι τα Hosted Wallets, τα οποία είναι διαδικτυακές υπηρεσίες που προσφέρουν λειτουργίες αποθήκευσης, διαχείρισης και συναλλαγών και είναι παρόμοια με τις υπηρεσίες Web Banking. Οι μηχανισμοί αυθεντικοποίησης είναι οι τυποποιημένοι μηχανισμοί πχ κωδικοί πρόσβασης ή επαλήθευση δυο βημάτων. [4]

Πέρα από την online αποθήκευση υπάρχει και η δυνατότητα της Offline αποθήκευσης σε φορητά μέσα πχ USB ή σε χαρτί ή QR κωδικοί οι οποίοι σαρώνονται και εμφανίζουν τα κλειδιά. Το πλεονέκτημα αυτού του είδους της αποθήκευσης είναι ότι είναι λιγότερο ευάλωτα σε κακόβουλα λογισμικά, όμως υπάρχει το ζήτημα της φυσικής ασφάλειας. Υπάρχει μια ειδική κατηγορία Offline αποθήκευσης, η οποία ονομάζεται αποθήκευση σε συσκευές με κενό αέρος. Οι συγκεκριμένες συσκευές μπορούν να εκτελέσουν υπολογισμούς για τα κλειδιά που κατέχουν. Τα Bitcoins, που είναι αποθηκευμένα σε αυτές τις συσκευές, προστατεύονται από διάφορα είδη κλοπών, καθώς δεν γίνεται έκθεση τους σε συσκευή που έχει πρόσβαση στο Internet. Επίσης, υπάρχουν και οι μονάδες ασφαλείας υλικού, οι οποίες προσομοιώνουν τις συσκευές κενός αέρος,

απομονώνοντας τα κλειδιά από την συσκευή υποδοχής (Host Device) και δίνοντας μόνο τη δυνατότητα υπογραφής της συναλλαγής.[4]

Η ιδιωτικότητα και η ανωνυμία του Bitcoin εξαρτάται από την χρήση του. Για παράδειγμα, οι έμποροι ή οι πωλητές, που παράγουν μια νέα διεύθυνση πληρωμής για κάθε πώληση, εξασφαλίζουν ότι οι ληφθείσες πληρωμές δεν είναι αυτομάτως συνδεδεμένες με το Block Chain. Ενώ οι πελάτες που ενδεχομένως να χρειάζεται να συγκεντρώσουν το ποσό της πληρωμής από διαφορετικές διευθύνσεις που κατέχουν, θα πρέπει να τις συνδέσουν στο Block Chain. Επιπλέον, άλλος ένας τρόπος που μπορεί να πληγεί η ανωνυμία του χρήστη είναι μέσω του δικτύου P2P, που χρησιμοποιεί το bitcoin, καθώς οι κόμβοι αποκαλύπτουν την διεύθυνση IP, όταν αναμεταδίδουν τις συναλλαγές. Η χρήση ανώνυμων δικτύων, όπως το Tor είναι σημαντική για την ιδιωτικότητα του νομίσματος.[4]

Κεφάλαιο 5

Δοκιμή Εργαλείων

5.1 Ανίχνευση του Dark Web

Ένα πρόγραμμα ανίχνευσης (crawler) είναι ένα πρόγραμμα που επισκέπτεται ιστότοπους και διαβάζει τις σελίδες τους και άλλες πληροφορίες για να δημιουργήσει καταχωρήσεις για το ευρετήριο των μηχανών αναζήτησης. Οι μεγάλες μηχανές αναζήτησης στο Διαδίκτυο διαθέτουν ένα τέτοιο πρόγραμμα, το οποίο είναι επίσης γνωστό ως "αράχνη-Spider" ή "bot". Τα προγράμματα ανίχνευσης είναι συνήθως προγραμματισμένα να επισκέπτονται νέους ή ενημερωμένους ιστότοπους. Ολόκληροι ιστότοποι ή συγκεκριμένες σελίδες μπορούν να επισκέπτονται και να αναπροσαρμόζονται επιλεκτικά.

>Η χρήση ενός crawler μπορεί δυνητικά να βοηθήσει στον εντοπισμό παράνομου περιεχομένου. Δεδομένου του τεράστιου μεγέθους του Dark Web, δεν είναι εφικτό στις αρμόδιες αρχές να επισκέπτονται με μη αυτόματο τρόπο κάθε τοποθεσία και να αξιολογούν το περιεχόμενό της για ενδεχομένως παράνομο περιεχόμενο. Η χρήση ενός crawler αποσκοπεί στην ανίχνευση και την ευρετηρίαση εκατομμυρίων τέτοιων ιστότοπων σε σύντομο χρονικό διάστημα, ενώ ταυτόχρονα είναι προγραμματισμένος να αναφέρει τον εντοπισμό ορισμένων λέξεων-κλειδιών. Αυτές οι λέξεις-κλειδιά μπορεί για παράδειγμα να είναι ονομασίες όπλων ή ναρκωτικών.

Τύποι ανιχνευτών

1. Ταξινόμηση με βάση τη μέθοδο ανίχνευσης

α. Η Breadth-Oriented ανίχνευση επικεντρώνεται κυρίως στην κάλυψη ενός ευρέος φάσματος πηγών δεδομένων / διευθύνσεων URL παρά στην πλήρη ανίχνευση περιεχομένου μέσα σε μεμονωμένους πόρους.
β. Η Depth-Oriented ανίχνευση εστιάζει στην εξαγωγή μέγιστων δεδομένων από μια μόνο πηγή.
2. Ταξινόμηση με βάση τη μέθοδο επιλογής λέξεων-κλειδιών
α. Τυχαία: Με αυτήν τη μέθοδο ανίχνευσης, η λέξη-κλειδί που χρησιμοποιείται για τη συμπλήρωση φόρμας λαμβάνεται από τυχαίο λεξικό.
β. Γενική συχνότητα: Με αυτή τη μέθοδο επιτυγχάνεται η γενική κατανομή συχνότητας κάθε λέξης-κλειδιού και χρησιμοποιείται η πιο συχνή λέξη-κλειδί για τη συμπλήρωση φόρμας. Αυτό βοηθά στο να επιστραφεί περισσότερο περιεχόμενο που ταιριάζει με την αναζήτησή μας και επίσης να αποθηκεύσετε το χρόνο συμπλήρωσης φόρμας.
γ. Προσαρμοστική μέθοδος: Με αυτή την μέθοδο αναλύονται τα έγγραφα που επιστρέφονται από τα ερωτήματα, καθώς και οι λέξεις-κλειδιά που επιστρέφουν το μεγαλύτερο μέρος του περιεχομένου σε λίστα. Με βάση αυτές τις πολλά υποσχόμενες λέξεις-κλειδιά, ο ανιχνευτής μπορεί να δημιουργήσει ερωτήματα για να αποκτήσει τα μέγιστα δεδομένα.

5.2 Δοκιμή εργαλείων Ahmia

Στο κεφάλαιο 1 το Dark Web αναφέρθηκε ως τμήμα του Deep Web το οποίο , το οποίο σκοπίμως έχει αποκρυφθεί και δεν είναι προσβάσιμο μέσω συμβατικών λογισμικών πλοήγησης και μηχανών αναζήτησης. Ωστόσο λόγω της ανάπτυξης και της αύξησης των χρηστών και των κρυφών υπηρεσιών των Darknets (κυρίως του δικτύου Tor), υπάρχουν διάφορες μηχανές αναζήτησης, προκείμενου να διευκολύνουν την πρόσβαση στις κρυφές υπηρεσίες.

Μια γνωστή μηχανή αναζήτησης είναι η Ahmia (https://ahmia.fi) την οποία ένας χρήστης μπορεί να προσπελάσει τόσο από το Clearnet όσο και από το Dark Web. Η μηχανή αναζήτησης Ahmia προσπαθεί να καταγράψει τις κρυφές υπηρεσίες του δικτύου Tor με σκοπό τον διαμοιρασμό στατιστικών, πληροφοριών και νέων σχετικά με το δίκτυο Tor αλλά και I2P. Το σύστημα αναζήτησης είναι ενσωματωμένο στο Globaleaks Project και

στο Tor2Web Project και επιτρέπει σε μη χρήστες της εφαρμογής περιήγησης Tor, να έχουν πρόσβαση στις κρυφές υπηρεσίες. Το Ahmia τηρεί μαύρες λίστες (blacklists) με σελίδες οι οποίες περιέχουν υλικό παιδικής κακοποίησης και τις αποκλείει από το ευρετήριό της. Αυτή η λίστα ενημερώνεται κάθε φορά που εντοπίζεται νέος ιστότοπος με υλικό κακοποίησης. Οι λίστες αυτές είναι κωδικοποιημένες με τον αλγόριθμό κατακερματισμού MD5. Η τιμή κατακερματισμού προκύπτει με βάση το όνομα του ιστότοπου.

Το Ahmia αποτελεί ένα ενεργό πεδίο έρευνας και τα εργαλεία που χρησιμοποιούνται είναι ανοιχτού κώδικα και διαθέσιμα δωρεάν στο GitHub. Τα εργαλεία του Ahmia Project χρησιμοποιήθηκαν σε λειτουργικό σύστημα Ubuntu 16.04 (Xenial Xerus). Αναλυτικά τα εργαλεία Ahmia τα οποία είναι διαθέσιμα είναι:

Ahmia Elasticsearch index

Η μηχανή αναζήτησης Ahmia χρησιμοποιεί την Elasticsearch. Η Elasticsearch είναι μια μηχανή αναζήτησης πραγματικού χρόνου και ανάλυσης δεδομένων, η οποία βασίζεται στην βιβλιοθήκη Apache Lucene. Τα κύρια χαρακτηριστικά της Elasticsearch είναι:

α) Κατανεμημένη, δηλαδή μπορεί να εκτελείται σε ξεχωριστούς διακομιστές, διαμοιράζοντας τις πληροφορίες σε διαφορετικούς κόμβους.
β) Κλιμακούμενη (Scalable), δηλαδή κατανέμει αυτόματα τα τμήματα σε κάθε κόμβο.
γ) Υψηλή Διαθεσιμότητα (High availability), δηλαδή όταν ένας κόμβος αποκοπεί, τα δεδομένα του μετατίθενται αυτόματα στους υπόλοιπους.
δ) REST API, οι λειτουργίες βασίζονται στην αρχιτεκτονική REST, προσφέροντας ευελιξία στην ανάπτυξη γρήγορου κώδικα.
ε) JSON αντί για HTTP, τα αιτήματα και οι απαντήσεις γίνονται με την χρήση των δομών JSON, προκειμένου να πραγματοποιείται πιο εύκολα η ανάγνωση του κώδικα.
Για να λειτουργήσει το Ahmia Index, θα πρέπει να εγκαταστήσουμε την Elasticsearch. Για να λάβουμε την Elasticsearch εκτελούμε την εντολή wget https://download.elastic.co/elasticsearch/release/org/elasticsearch/distribution/deb/elasticsearch/2.3.1/elasticsearch-2.3.1.deb. Στην συνέχεια εγκαθιστούμε το πρόγραμμα με την εντολή sudo dpkg -i elasticsearch-2.3.1.deb. Η Elasticsearch θα εγκατασταθεί στο /usr/share/elasticsearch/ και το αρχείο διαμόρφωσης θα βρίσκεται στο

/etc/elasticsearch. Προκειμένου να ξεκινήσει η λειτουργία της Elasticsearch, θα πρέπει να ρυθμιστεί το αρχείο /etc/elasticsearch/elasticsearch.yml και να οριστεί ως network.host 127.0.0.1 και http.port: 9200.

Τα αρχεία του Ahmia Index λαμβάνονται από το https://github.com/ahmia/ahmia-index.git. Στην συνέχεια θα πρέπει να τροποποιήσουμε κάποιες λειτουργίες ώστε να είναι πιο ασφαλής η λειτουργία της Elasticsearch. Έτσι εκτελούμε την εντολή $ sudo nano /etc/security/limits.conf και προσθέτουμε τ elasticsearch - nofile unlimited και το elasticsearch - memlock unlimited . Στην συνέχεια τροποποιούμε το αρχείο /etc/default/elasticsearch , εκτελώντας την εντολή $ sudo nano /etc/default/elasticsearch και προσθέτουμε ES_HEAP_SIZE= με το μισό της διαθέσιμης μνήμης, MAX_OPEN_FILES=1065535 και MAX_LOCKED_MEMORY=unlimited. Έπειτα, τροποποιούμε το αρχείο /etc/elasticsearch/elasticsearch.yml εκτελώντας $ sudo nano και προσθέτουμε bootstrap.memory lock: true, script.engine.groovy.inline.update: on, script.engine.groovy.inline.aggs: on. Στην συνέχεια για ξεκινήσει η Elasticsearch εκτελούμε την εντολή sudo systemctl start elasticsearch και εκτελούμε τις παρακάτω εντολές:

$ curl -XPUT -i "localhost:9200/crawl-2017-11/" -H 'Content-Type: application/json' -d "@./mappings.json"

$ curl -XPUT -i "localhost:9200/crawl-2017-12/" -H 'Content-Type: application/json' -d "@./mappings.json"

ή εκτελούμε αρχείο $ bash setup_index.sh. Προκειμένου να λάβουμε τους τελευταίους πίνακες δεδομένων εκτελούμε την εντολή $ python3 point_to_indexes.py. Ενώ για φιλτράρουμε τους προσβλητικούς ιστότοπους εκτελώντας την εντολή $ bash call_filtering.sh.[34]

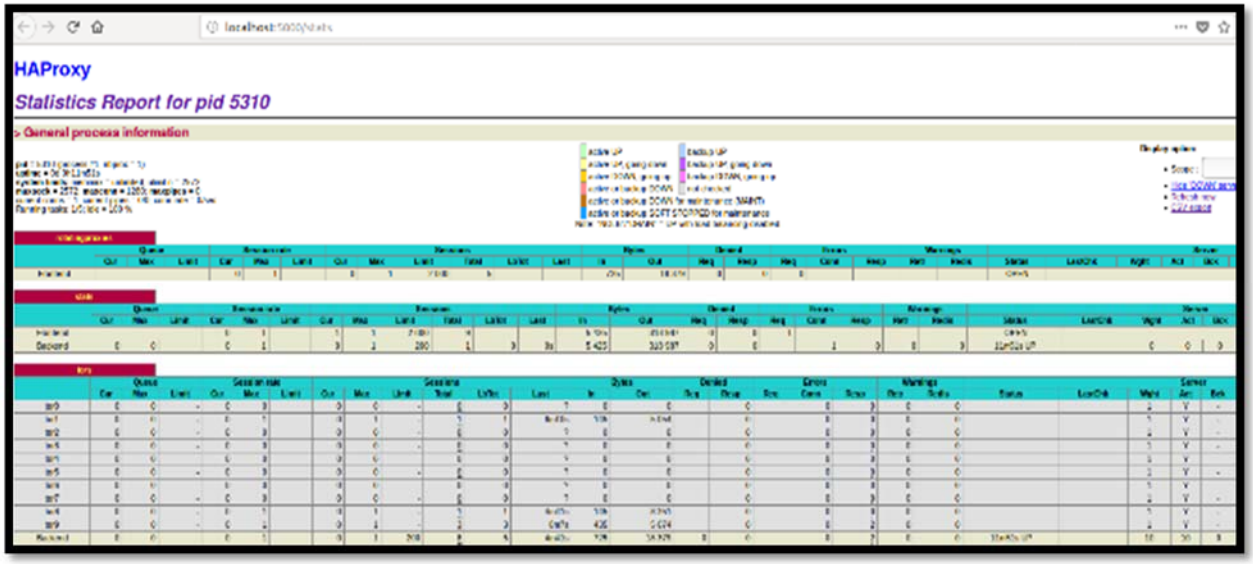
TorBalancer

Είναι ένα εργαλείο το οποίο ισορροπεί την κίνηση μεταξύ πολλαπλών πελατών Tor, καταγράφει τα κυκλώματα και τις συνδέσεις σύμφωνα με τις διευθύνσεις onion. Για να εγκαταστήσουμε το TorBalancer λαμβάνουμε συμπιεσμένο αρχείο από το https://github.com/ahmia/TorBalancer.git. Το αρχείο περιέχει δυο τρόπους λειτουργείας ένας είναι με το polipo και ο άλλος με το delegate. Η δοκιμή έγινε με το polipo, οπότε εκτελούμε την εντολή cd polipo-version και την εντολή sudo ./install.sh για

να εγκαταστήσουμε το πρόγραμμα. Μαζί θα εγκατασταθούν και τα HAProxy, Polipo και Tor (εάν δεν είναι ήδη εγκατεστημένα). Προκειμένου να ξεκινήσει το πρόγραμμα εκτελούμε την εντολή bash opentors.sh και την συνέχεια την εντολή curl -x localhost:3128 http://xxxxxxxx.onion/. Για να ελέγξουμε τα στατιστικά, σε έναν browser επισκεπτόμαστε την σελίδα http://localhost:5000/stats.[32]

Εικόνα 11

Η ανάλυση της σελίδας msydqstlz2kzerdg.onion μετά την εντολή curl -x localhost:3128



Εικόνα 12

Η γραφική εφαρμογή του HA Proxy

Ahmia-crawler

Πρόκειται για ένα πρόγραμμα οποίο χρησιμοποιείται για την ευρετηρίαση των σελίδων .onion και .i2p. Το συγκεκριμένο εργαλείο το λαμβάνουμε από το

https://github.com/ahmia/ahmia-crawler.git και για να λειτουργήσει θα πρέπει πρώτο να εκτελέσουμε το ahmia index. Επιπλέον θα πρέπει να εκτελέσουμε τις παρακάτω εντολές προκειμένου να εγκαταστήσουμε τα απαραίτητα προγράμματα και βιβλιοθήκες:

$ apt-get install build-essential python-pip python-virtualenv

$ apt-get install libxml2-dev libxslt1-dev python-dev libffi-dev libssl-dev

$ apt-get install tor polipo

Επιπρόσθετα, θα πρέπει σε εικονικό περιβάλλον να εγκατασταθούν επιπλέον προγράμματα τα οποία βρίσκονται στο αρχείο requirements.txt που βρίσκεται στο ahmia/crawler, εκτελώντας τις παραπάνω εντολές:

$ virtualenv /path/to/venv

$ source /path/to/venv/bin/activate

(venv)$ pip install -r requirements.txt

Στην συνέχεια θα πρέπει να τροποποιήσουμε το αρχείο polipo/config και να προσθέσουμε τα παρακάτω ρυθμίσεις:

logFile=/var/log/polipo/polipo.log

socksParentProxy = localhost:9050

diskCacheRoot=""

disableLocalInterface=true

Στην συνέχεια εκτελούμε τις παρακάτω εντολές προκειμένου να ενεργοποιήσουμε τις υπηρεσίες tor και polipo:

$ systemctl start tor

$ systemctl start polipo

Για να χρησιμοποιήσουμε τον Python Proxy που είναι διαθέσιμο από το ahmia/crawler εκτελούμε τις παρακάτω εντολές:

$ sudo pip3 install PySocks

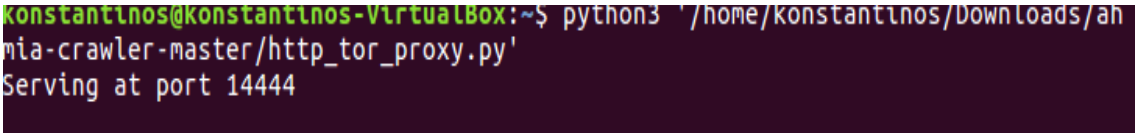
$ sudo pip3 install urlparse2

$ python http_tor_proxy.py

$ curl -x http://localhost:14444 http://xxxxxx.onion/

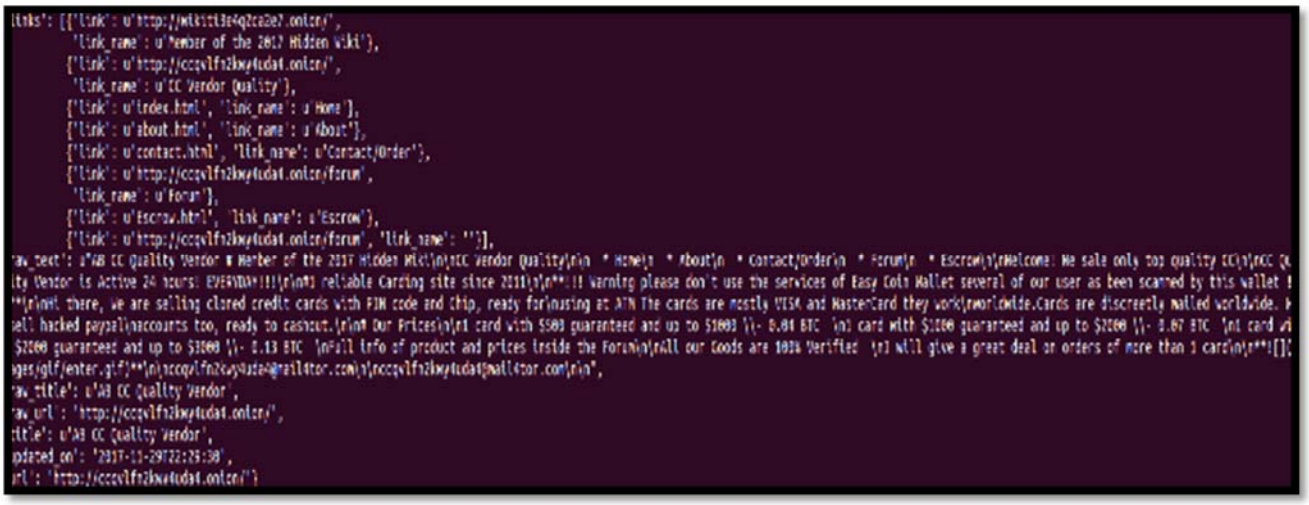
Τέλος μπορούμε να χρησιμοποιήσουμε το onionElasticBot πραγματοποιώντας διάφορες αναζητήσεις όπως: $ scrapy crawl ahmia-tor -s DEPTH_LIMIT=2 -s ROBOTSTXT_OBEY=0 ή scrapy crawl ahmia-i2p -s DEPTH_LIMIT=1 -s ROBOTSTXT_OBEY=0 -s ELASTICSEARCH_TYPE=i2p.

Επιπλέον υπάρχουν και άλλα έτοιμα spiders όπως το finder_spider. [33]



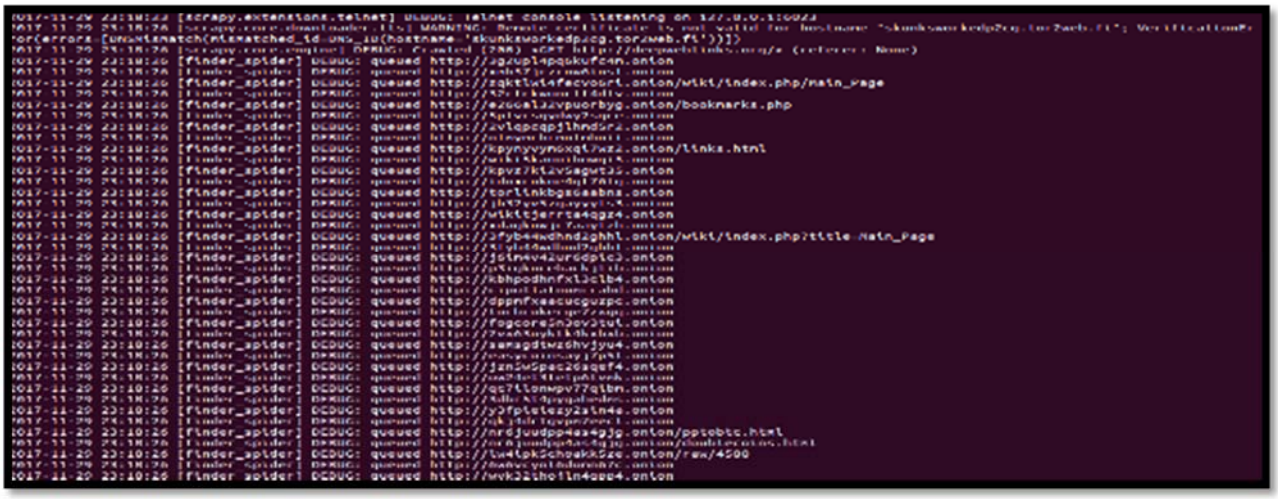
Εικόνα 13

Η εκτέλεση του αρχείου http_tor_proxy που δημιουργεί ένα http proxy στη θύρα 14444



Εικόνα 14

Η εκτέλεση του crawler ahmia-tor



Εικόνα 15

Οι onion σελίδες που εντόπισε το Finder_Spider

Εικόνα 16

Η εκτέλεση του finder_spider

Ahmia Site

Το Ahmia, δίνει την δυνατότητα της δημιουργίας της ιστοσελίδας σε τοπικό υπολογιστή. Προκειμένου να δημιουργηθεί ο ιστότοπος θα πρέπει να εγκαταστήσουμε κάποια προγράμματα και βιβλιοθήκες εκτελώντας τις παρακάτω εντολές:

sudo apt-get install build-essential python-pip python-virtualenv

sudo apt-get install libxml2-dev libxslt1-dev python-dev libpq-dev libffi-dev libssl-dev

Ακόμη πρέπει να εγκατασταθούν σε εικονικό περιβάλλον τα προγράμματα τα οποία βρίσκονται στο αρχείο dev.txt.

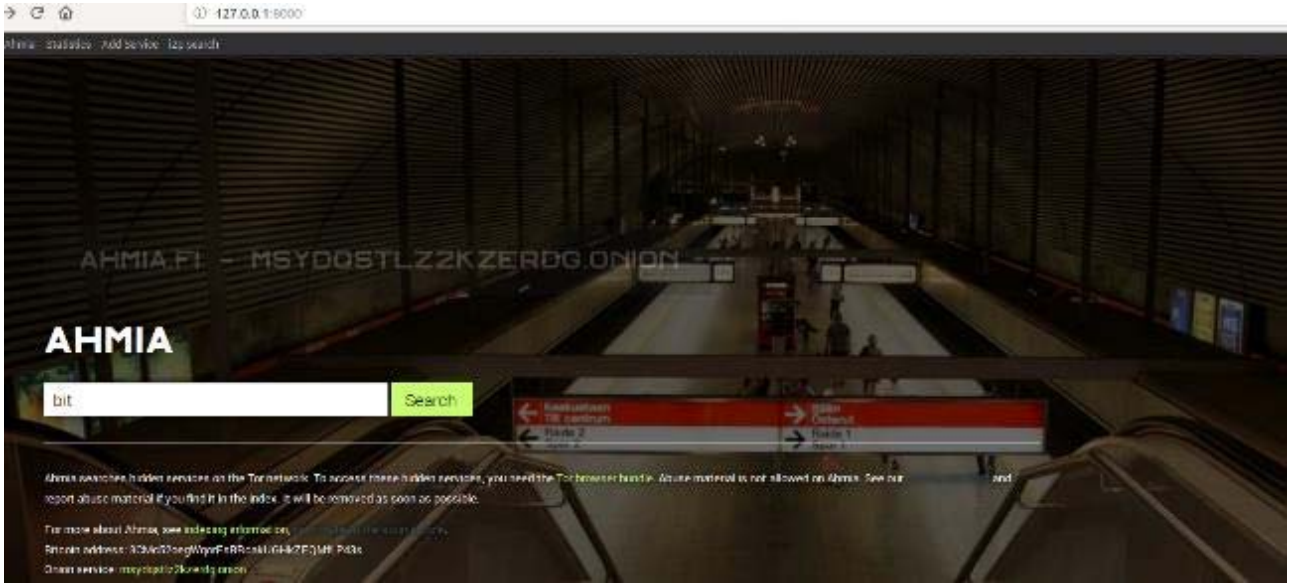
Στη συνέχεια θα πρέπει να μεταφέρουμε τη βάση δεδομένων εκτελώντας τις παρακάτω εντολές:

$ python ahmia/manage.py makemigrations ahmia

$ python ahmia/manage.py makemigrations search

$ python ahmia/manage.py migrate

Στη συνέχεια με την εντολή python ahmia/manage.py runserver ξεκινάει η λειτουργία του τοπικού διακομιστή. Η διεύθυνση του διακομιστή είναι η http://127.0.0.1:8000/. Ενώ στη γραμμή εντολών καταγράφονται οι ενέργειες που πραγματοποιούνται στον διακομιστή.[35]



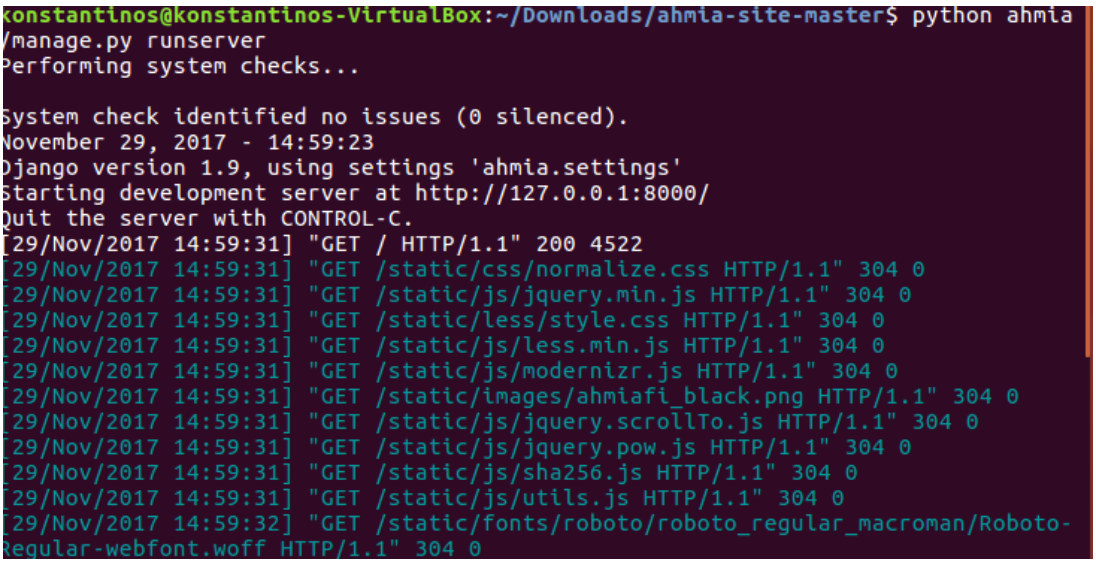
Εικόνα 17

Η σελίδα Ahmia σε τοπικό υπολογιστή

```
konstantinos@konstantinos-VirtualBox:~/Downloads/ahmia-site-master$ python ahmia/manage.py makenigrations ahmia
Migrations for 'ahmia':
  0001_initial.py:
    - Create model HiddenWebsite
konstantinos@konstantinos-VirtualBox:~/Downloads/ahmia-site-master$ python ahmia/manage.py makenigrations search
No changes detected in app 'search'
konstantinos@konstantinos-VirtualBox:~/Downloads/ahmia-site-master$ python ahmia/manage.py migrate
Operations to perform:
  Apply all migrations: contenttypes, ahmia, sites, auth
Running migrations:
  Rendering model states... DONE
  Applying ahmia.0001_initial... OK
  Applying contenttypes.0001_initial... OK
  Applying contenttypes.0002_remove_content_type_name... OK
  Applying auth.0001_initial... OK
  Applying auth.0002_alter_permission_name_max_length... OK
  Applying auth.0003_alter_user_email_max_length... OK
  Applying auth.0004_alter_user_username_opts... OK
  Applying auth.0005_alter_user_last_login_null... OK
  Applying auth.0006_require_contenttypes_0002... OK
  Applying auth.0007_alter_validators_add_error_messages... OK
  Applying sites.0001_initial... OK
  Applying sites.0002_alter_domain_unique... OK
```

Εικόνα 18

Η μεταφορά βάσης δεδομένων για τη σελίδα του Ahmia

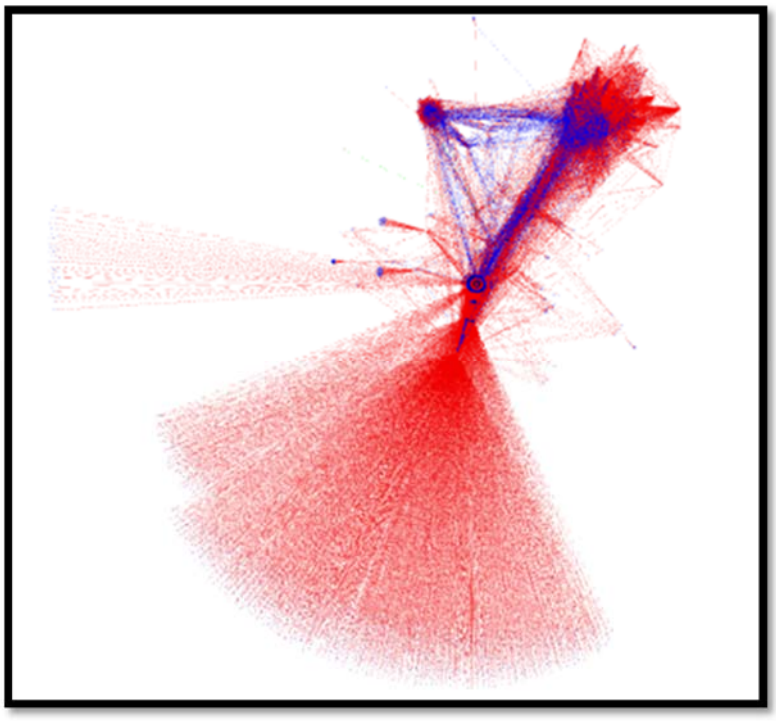


Εικόνα 19

Η καταγραφή των συμβάντων της σελίδας Ahmia

Onion Visual

Άλλο ένα εργαλείο είναι με το οποίο πραγματοποιείται γραφική αναπαράσταση των κόμβων. Περιέχει έτοιμα scripts ενώ απαιτείται η λήψη και εγκατάσταση το προγράμματος Gephi 0.9.2 προκειμένου να εκτελέσουμε τα αρχεία gexf, τα οποία λαμβάνουμε από το . (https://gephi.org/users/download/).[31]



Εικόνα 20

Η χρήση του αρχείου Ahmia.gfex με το πρόγραμμα Gephi και η αναπαράσταση 6920 onion κόμβων.

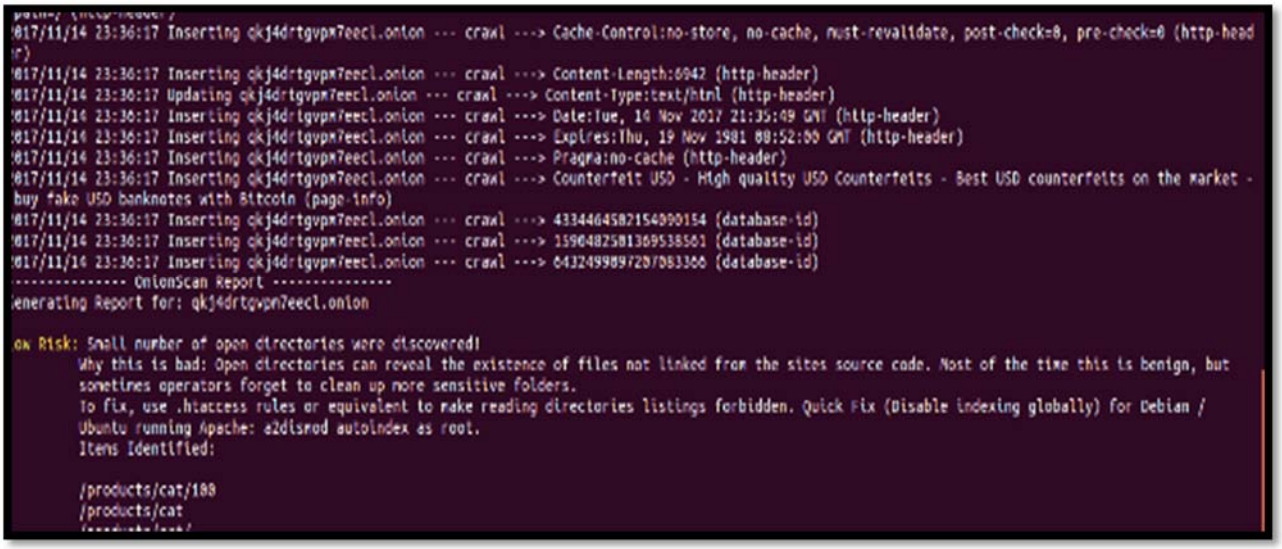
5.3 Δοκιμή OnionScan

Άλλο ένα εργαλείο το οποίο χρησιμοποιήθηκε είναι το OnionScan. Είναι ένα δωρεάν εργαλείο ανοιχτού κώδικα γραμμένο σε Go, το οποίο χρησιμοποιείται για την έρευνα του Dark Web. Οι δυο βασικοί στόχοι του εργαλείου είναι:
α) Η παροχή βοήθειας στους διαχειριστές των κρυφών υπηρεσιών για να εντοπίσουν και να διορθώσουν διάφορα θέματα ασφαλείας στις υπηρεσίες τους. Το εργαλείο βοηθάει στην ανίχνευση των λανθασμένων ρυθμίσεων, οι οποίες μπορεί να θέσουν σε κίνδυνο την ανωνυμία.
β) Η παροχή βοήθειας στους ερευνητές του Dark Web, προκειμένου να εξελιχθεί η τεχνολογία της ανωνυμίας.

Η εγκατάσταση και λειτουργία του OnionScan είναι πολύ απλή. Για την εγκατάσταση των απαιτούμενων προγραμμάτων εκτελούμε τις εντολές: go get github.com/HouzuoGuo/tiedot, go get golang.org/x/crypto/openpgp, go get golang.org/x/net/proxy, go get golang.org/x/net/html, go get github.com/rwcarlsen/goexif/exif, go get github.com/rwcarlsen/goexif/tiff. Στην συνέχεια λαμβάνουμε το Onionscan με την εντολή go get github.com/s-rah/onionscan και το εγκαθιστούμε με την εντολή go install github.com/s-rah/onionscan. Για να εκτελέσουμε το πρόγραμμα μεταβαίνουμε στο αρχείο που βρίσκεται το εκτελέσιμο αρχείο και εκτελούμε την εντολή ./onionscan -verbose -list onions. Το onions είναι ένα αρχείο που δημιουργήσαμε και περιέχει 891 διευθύνσεις onion, που εντοπίστηκαν με την χρήση του Onionscan και του Ahmia Crawler.

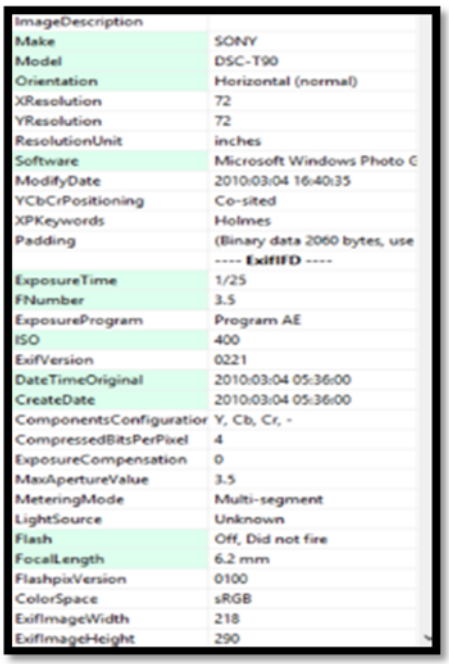
Το OnionScan εξετάζει διάφορα προβλήματα στις διαμορφώσεις των onion σελίδων, οι οποίες μπορεί να αποκαλύψουν την διεύθυνση IP του ιστότοπου, να αποκαλύψουν την κίνηση και την δραστηριότητα του ιστότοπου και να εντοπίσουν κρυφά σημεία του ιστότοπου. Ένα από το πιο σύνηθες λάθος στην διαμόρφωση διακομιστών που χρησιμοποιούν Apache, είναι στην διαμόρφωση του mod_status, η οποία αν ρυθμιστεί λάθος μπορεί να αποκαλύψει πλήθος πληροφοριών (ακόμη και την πραγματική IP).

Το OnionScan ελέγχει για ανοικτούς καταλόγους όπως το index.html, καταλόγους εικόνων ή αντίγραφα των backups. Επιπλέον ελέγχει τα αρχεία εικόνων για metadata (Exif Tags), όπως για παράδειγμα το μοντέλο της κάμερας ή του τηλεφώνου και συντεταγμένες της φωτογραφίας. Επίσης ελέγχει το αποτύπωμα του διακομιστή, τις ταυτότητες PGP (Pretty Good Privacy), αποτύπωμα του δημοσίου κλειδιού SSH, την ύπαρξη τυχόν Cryptocurrency Clients, ενώ εντοπίζει και πρωτόκολλα όπως IRC, XMOO, VNC και Ricochet. Τέλος, ελέγχει scripts από το Google Analytics, τα οποία μπορεί να χρησιμοποιούνται σε σελίδες Onion, αλλά και στο Surface Web. Μερικά αποτελέσματα από την χρήση του φαίνονται στις παρακάτω εικόνες. Επίσης χρησιμοποιήθηκε το exifguitool για να δούμε ποια metadata βρέθηκαν:

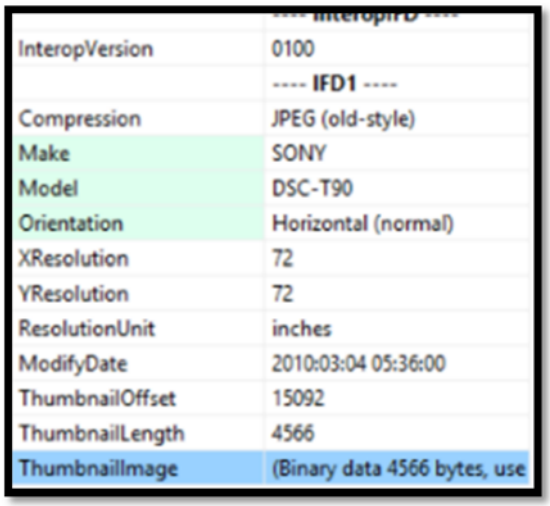


Εικόνα 21

Αναφορά του Onionscan και εντοπισμός metadata



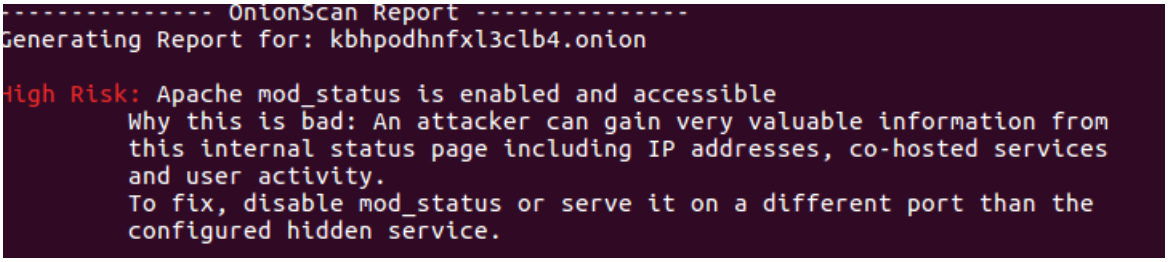
ImageDescription	
Make	SONY
Model	DSC-T90
Orientation	Horizontal (normal)
XResolution	72
YResolution	72
ResolutionUnit	inches
Software	Microsoft Windows Photo C
ModifyDate	2010:03:04 16:40:35
YCbCrPositioning	Co-sited
XPKeywords	Holmes
Padding	(Binary data 2060 bytes, use
	---- ExifIFD ----
ExposureTime	1/25
FNumber	3.5
ExposureProgram	Program AE
ISO	400
ExifVersion	0221
DateTimeOriginal	2010:03:04 05:36:00
CreateDate	2010:03:04 05:36:00
ComponentsConfiguratior	Y, Cb, Cr, -
CompressedBitsPerPixel	4
ExposureCompensation	0
MaxApertureValue	3.5
MeteringMode	Multi-segment
LightSource	Unknown
Flash	Off, Did not fire
FocalLength	6.2 mm
FlashpixVersion	0100
ColorSpace	sRGB
ExifImageWidth	218
ExifImageHeight	290



InteropVersion	0100
	---- IFD1 ----
Compression	JPEG (old-style)
Make	SONY
Model	DSC-T90
Orientation	Horizontal (normal)
XResolution	72
YResolution	72
ResolutionUnit	inches
ModifyDate	2010:03:04 05:36:00
ThumbnailOffset	15092
ThumbnailLength	4566
ThumbnailImage	(Binary data 4566 bytes, use

Εικόνα 22, 23

Η χρήση του εργαλείου exifguitool και τα στοιχεία που βρέθηκαν

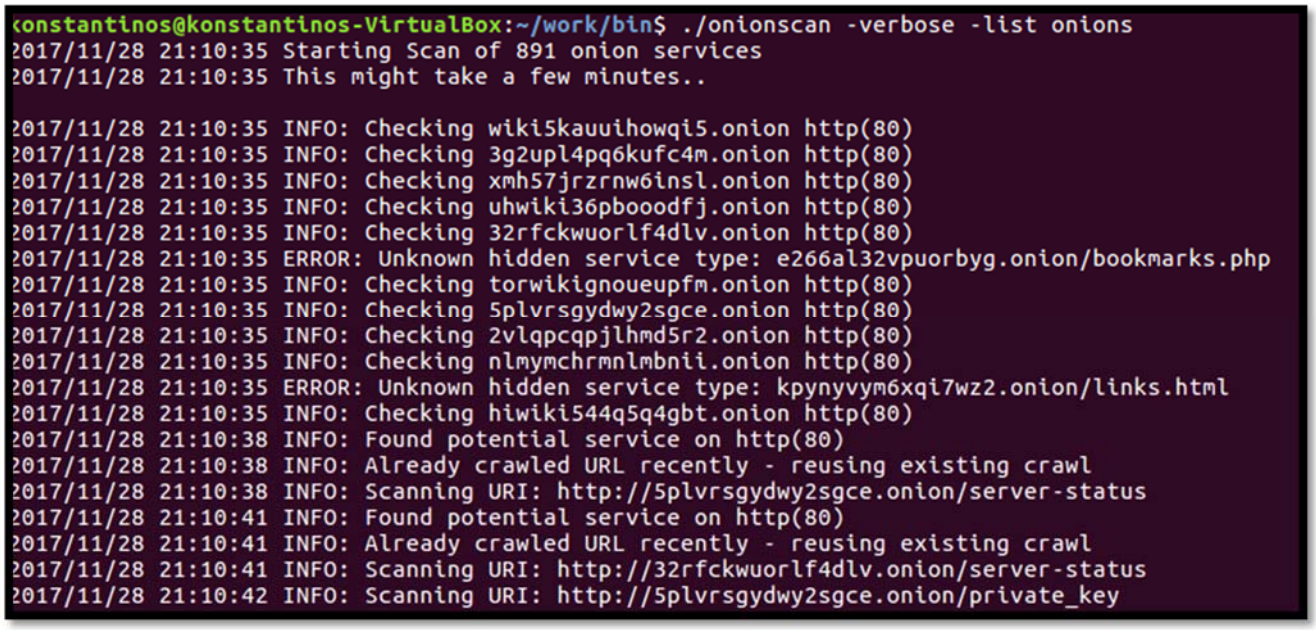


```
--------------- OnionScan Report ---------------
Generating Report for: kbhpodhnfxl3clb4.onion

High Risk: Apache mod_status is enabled and accessible
        Why this is bad: An attacker can gain very valuable information from
        this internal status page including IP addresses, co-hosted services
        and user activity.
        To fix, disable mod_status or serve it on a different port than the
        configured hidden service.
```

Εικόνα 24

Αναφορά του Onionscan και εντοπισμός ρύθμισης υψηλού ρίσκου



Εικόνα 25

Η χρήση του εργαλείου Onionscan και ο έλεγχος 891 διευθύνσεων onion

5.4 Δοκιμή Εργαλείων Osint

Maltego Community Edition

Το Maltego Community Edition είναι ένα εργαλείο εύρεσης δεδομένων που μπορεί να χρησιμοποιηθεί για διαδικασίες OSINT (Open Source Intelligence). Χρησιμοποιείται για online ερεύνα προκειμένου να εντοπίσει τη σχέση μεταξύ των πληροφοριών που συλλέγονται από το διαδίκτυο. Το Maltego μετατρέπει τις πληροφορίες που βρίσκονται σε κάποιο κόμβο σε γραφήματα τα οποία ενώνονται σε περίπτωση που υπάρχει σχέση μεταξύ τους. Το Maltego μπορεί να ερευνήσει διάφορες μορφές εισαγωγών όπως:

α) Ανθρώπους (Ονόματα, διευθύνσεις ηλεκτρονικού ταχυδρομείου)

β) Ομάδες Ανθρώπων (μέσω κοινωνικών δικτύων)

γ) Εταιρίες, Οργανισμούς

δ) Ιστοσελίδες

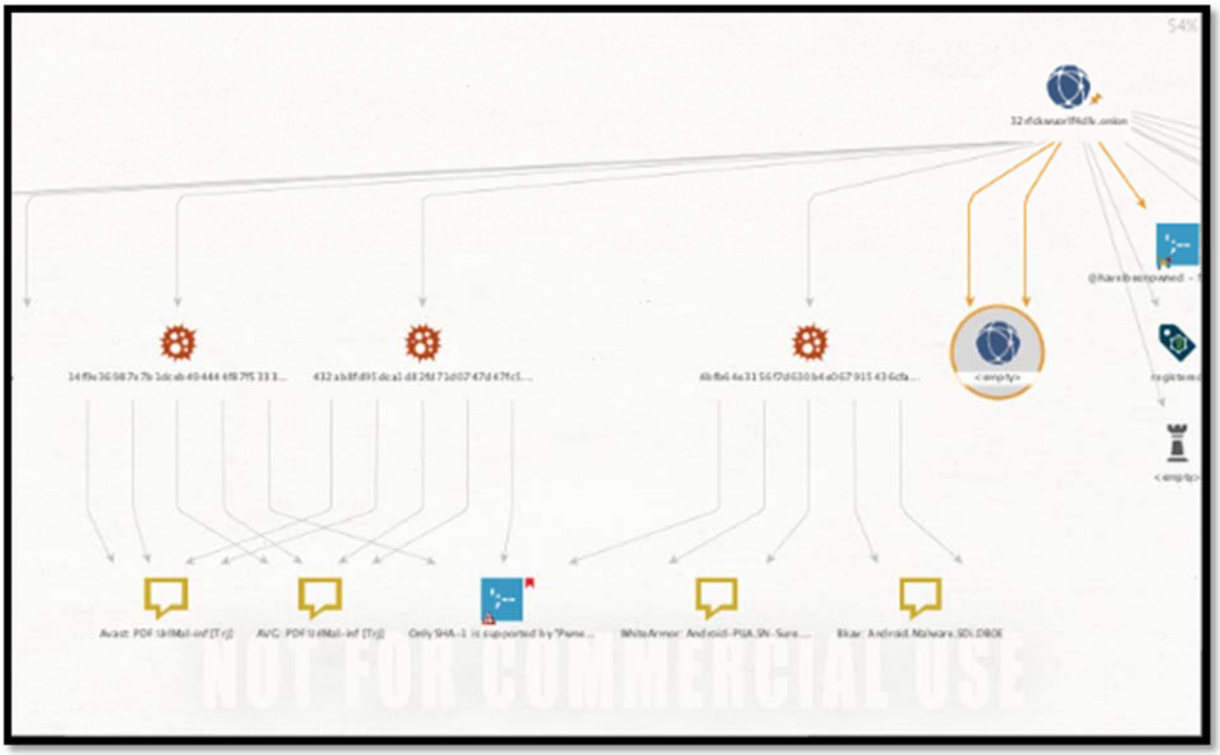
ε) Μέρη της δομής του Internet (Domains, DNS names, Netblocks, IP addresses)

Το Maltego διαθέτει διάφορες δωρεάν transformation, όπως το CaseFile Ententities και το Shodan, που εκτελούν διάφορους ελέγχους με σκοπό την εξαγωγή πληροφοριών. Με

την χρήση του συγκεκριμένου λογισμικού εντοπίστηκαν τιμές κατακερματισμού κακόβουλων αρχείων.

Εκτός από το Maltego δοκιμάστηκαν τα εργαλεία OSINT τα οποία είναι προ - εγκατεστημένα στο Kali Linux, όπως automater, theharvester, τα οποία δεν έδωσαν κάποια χρήσιμη πληροφορία.

Εικόνα 26
Αποτελέσματα της χρήσης του Maltego



Εικόνα 27
Αποτελέσματα της χρήσης του Maltego

5.4.1 Δημιουργία Onion Proxy

Για την ερεύνα χρησιμοποιήθηκαν κυρίως διευθύνσεις .onion, σε συνδυασμό με ένα Raspberry Pi το οποίο χρησιμοποιήθηκε ως Onion Proxy. Η χρήση του Raspberry Pi έγινε διότι το Maltego δοκιμάστηκε σε διάφορα λειτουργικά συστήματα σε διαφορετικούς υπολογιστές, με αυτό τον τρόπο οι υπολογιστές μπορούσαν να δρομολογούν την κίνηση μέσω του δικτύου Tor. Εναλλακτικά, θα έπρεπε σε κάθε υπολογιστή να εγκαταστήσουμε το Tor Service (σε Linux με την εντολή sudo apt-get install tor και σε Windows να λάβουμε το Tor bundle) και να ορίσουμε στις SOCKS proxy 127.0.0.1:9050. Το Raspberry Pi, προτιμήθηκε για αυτή την εργασία διότι είναι ένας οικονομικός μικροϋπολογιστής που προγραμματίζεται σχετικά εύκολα και υποστηρίζεται από μια δραστήρια κοινότητα που βοηθάει στην επίλυση τυχόν προβλημάτων. Το Raspberry Pi με βάση τις οδηγίες που βρίσκονται στον ιστότοπο https://learn.adafruit.com/onion-pi/overview, αρχικά προγραμματίστηκε ώστε να γίνει Wireless Access Point και στη συνέχεια προγραμματίστηκε έτσι ώστε να λειτουργεί ως Tor Proxy. Τα υλικά που χρησιμοποιήθηκαν είναι ένα Raspberry Pi model B, καλώδιο Ethernet, κεραία Wifi, κάρτα Sd με εγκατεστημένο το λειτουργικό σύστημα Raspbian. Αρχικά απαιτείται πρόσβαση στο Internet μέσω Ethernet. Στη γραμμή εντολών εκτελούμε τις εντολές sudo apt-get update και sudo apt-get install hostapd isc-dhcp-server, ενώ εγκαθιστούμε iptables manager με την εντολή sudo apt-get install iptables-persistent.

Στη συνέχεια εγκαθιστούμε DHCP server τροποποιώντας το αρχείο /etc/dhcp/dhcpd.conf, έτσι επιτρέπουμε τις συσκευές που συνδέονται ασύρματα στο Access Point να λαμβάνουν αυτόματα διεύθυνση IP, DNS κλπ. Προκειμένου να τροποποιήσουμε το συγκεκριμένο αρχείο εκτελούμε την εντολή sudo nano /etc/dhcp/dhcpd.conf και εντοπίζουμε το σημείο στο οποίο αναγράφεται option domain-name “example.org"; και option domain-name-servers ns1.example.org, ns2.example.org; και προσθέτουμε δίεση (#) ώστε να μην εκτελούνται. Έπειτα εντοπίζουμε το σημείο στο οποίο αναγράφεται:

If this DHCP server is the official DHCP server for the local
network, the authoritative directive should be uncommented.
#authoritative;

Αφαιρούμε την δίεση από #authoritative και στο τέλος του αρχείου προσθέτουμε, για να ορίσουμε το υποδίκτυο στο οποίο θα εισέρχονται οι υπολογιστές, τα εξής:

subnet 192.168.1.0 netmask 255.255.255.0 {

range 192.168.1.10 192.168.1.100;

option broadcast-address 192.168.1.255;

option routers 192.168.1.1;

default-lease-time 600;

max-lease-time 7200;

option domain-name “local";

option domain-name-servers 8.8.8.8, 8.8.4.4;

}

Αποθηκεύουμε τις αλλαγές επιλέγοντας Ctrl + X και Y και enter.

Τροποποιούμε το αρχείο /etc/default/isc-dhcp-server εκτελώντας την εντολή sudo nano /etc/default/isc-dhcp-server και ορίζουμε στο INTRFACES =“wlan0” ή το όνομα του δικτύου και αποθηκεύουμε το αρχείο.

Επόμενο βήμα είναι να ορίσουμε στατική διεύθυνση IP στο wlan0. Ανοίγουμε το αρχείο /etc/network/interfaces εκτελώντας την εντολή sudo nano /etc/network/interfaces, βρίσκουμε το auto wlan0 και προσθέτουμε δίεση, προκειμένου να μην εκτελείται. Ακολούθως προσθέτουμε μετά την εντολή allow-hotplug wlan0 τις εντολές:

iface wlan0 inet static

address 192.168.1.1

netmask 255.255.255.0

Αποθηκεύουμε και κλείνουμε το έγγραφο. Δίνουμε τη στατική IP εκτελώντας την εντολή sudo ifconfig wlan0 192.168.1.1.

Στη συνέχεια διαμορφώνουμε το Access Point, εκτελώντας την εντολή sudo nano /etc/hostapd/hostapd.conf και προσθέτουμε τις παρακάτω εντολές:

interface=wlan0

driver=nl80211

ssid=Pi_Onion

country_code=Gr

hw_mode=g

channel=6

macaddr_acl=0

auth_algs=1

ignore_broadcast_ssid=0

wpa=2

wpa_passphrase=Password

wpa_key_mgmt=WPA-PSK

wpa_pairwise=CCMP

wpa_group_rekey=86400

ieee80211n=1

Αποθηκεύουμε και κλείνουμε το αρχείο.

Έπειτα, καθορίζουμε στο Raspberry Pi που θα βρει το αρχείο διαμόρφωσης, εκτελώντας την εντολή sudo nano /etc/default/hostapd. Στη συνέχεια βρίσκουμε τη γραμμή #DAEMON_CONF="" και προσθέτουμε DAEMON_CONF="/etc/hostapd/hostapd.conf", αφαιρώντας την δίεση και αποθηκεύουμε. Τρέχουμε την εντολή sudo nano /etc/init.d/hostapd, βρίσκουμε την γραμμή DAEMON_CONF= και προσθέτουμε DAEMON_CONF=/etc/hostapd/hostapd.conf.

Επόμενη ενέργεια είναι να διαμορφώσουμε το Network Address Traslation (NAT). Τρέχουμε την εντολή sudo nano /etc/sysctl.conf και στο τέλος του εγγράφου προσθέτουμε net.ipv4.ip_forward=1, αποθηκεύουμε και κλείνουμε το αρχείο. Ύστερα εκτελούμε την εντολή sudo sh -c "echo 1 > /proc/sys/net/ipv4/ip_forward". Ενώ για να δημιουργήσουμε network translation μεταξύ του eth0 και του wlan0 εκτελούμε τις παρακάτω εντολές

sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

sudo iptables -A FORWARD -i eth0 -o wlan0 -m state --state RELATED, ESTABLISHED -j ACCEPT sudo iptables -A FORWARD -i wlan0 -o eth0 -j ACCEPT.

Επόμενες εντολές είναι οι sudo /usr/sbin/hostapd /etc/hostapd/hostapd.conf και οι εντολές sudo service hostapd start, sudo service isc-dhcp-server start.

Με αυτό τον τρόπο ρυθμίστηκε το Raspberry Pi, ώστε να λειτουργεί ως Wireless Access Point. Ο στόχος όμως είναι να λειτουργεί ως Tor proxy, οπότε εκτελούμε τις εντολές sudo apt-get update και sudo apt-get install tor, για να εγκαταστήσουμε το Tor. Μόλις ολοκληρωθεί η εγκατάσταση, τροποποιούμε το αρχείο config του Tor, εκτελώντας την εντολή sudo nano /etc/tor/torrc. Στο αρχείο που ανοίγει, προσθέτουμε τις παρακάτω ρυθμίσεις:

Log notice file /var/log/tor/notices.log

VirtualAddrNetwork 10.192.0.0/10

AutomapHostsSuffixes .onion,.exit

AutomapHostsOnResolve 1

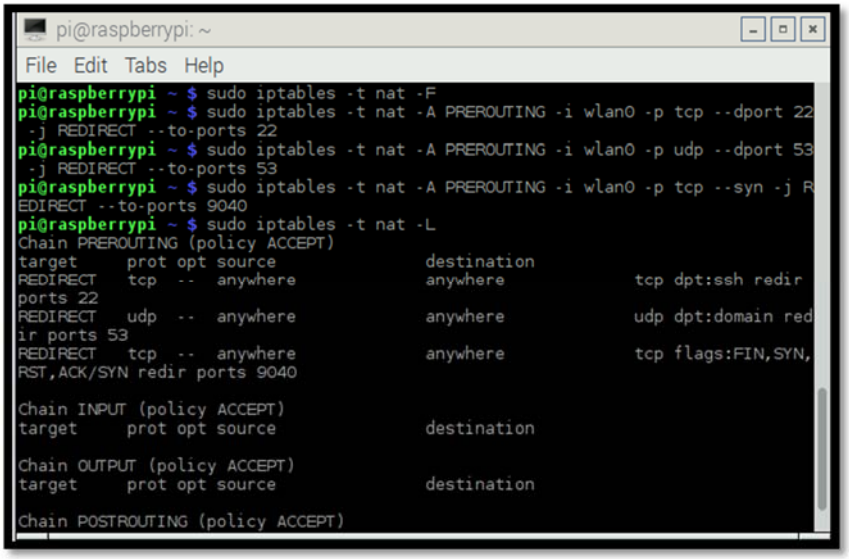
TransPort 9040

TransListenAddress 192.168.1.1

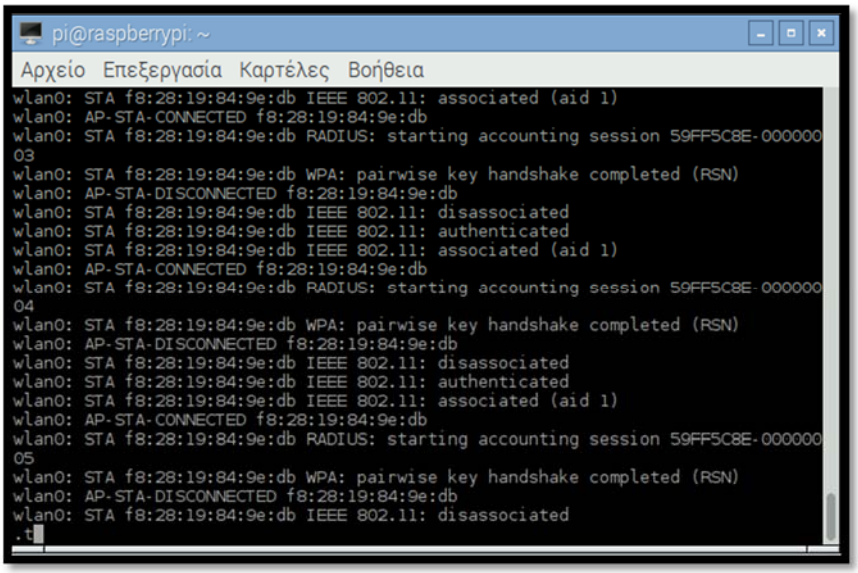
DNSPort 53

DNSListenAddress 192.168.1.1

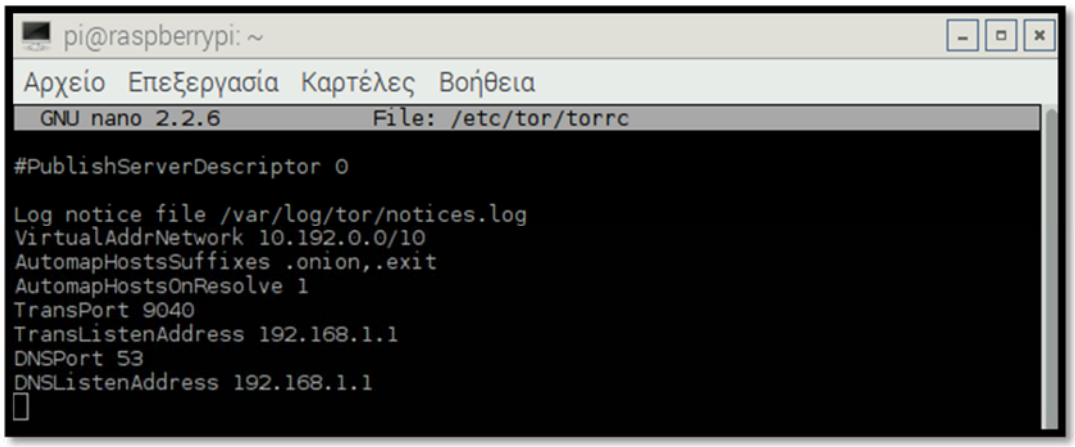
Στο επόμενο βήμα, ρυθμίζουμε τους πίνακες δρομολόγησης, ώστε οι ασύρματες συνδέσεις να δρομολογούνται μέσω του δικτύου Tor. Αρχικά εκτελούμε τις εντολές sudo iptables –F και sudo iptables -t nat –F και τις εντολές sudo iptables -t nat -A PREROUTING -i wlan0 -p tcp --dport 22 -j REDIRECT --to-ports 22. Εκτελούμε την εντολή sudo iptables -t nat -A PREROUTING -i wlan0 -p udp --dport 53 -j REDIRECT --to-ports 53, ώστε να δρομολογούνται τα δεδομένα DNS (UDP θύρα 53) από το wlan0 στην εσωτερική θύρα 53 (DNSPort στο torrc). Επόμενη εντολή είναι το sudo iptables -t nat -A PREROUTING -i wlan0 -p tcp --syn -j REDIRECT --to-ports 9040, με αυτήν όλη η TCP κίνηση δρομολογείται από το Wlan0 προς την θύρα 9040 (TransPort στο torrc). Η τελευταία εντολή που εκτελούμε είναι sudo service tor start, ώστε να ξεκινήσει η υπηρεσία Tor. Προκειμένου να δούμε ότι τα δεδομένα δρομολογούνται μέσω του δικτύου Tor, ελέγχουμε την εξωτερική IP.



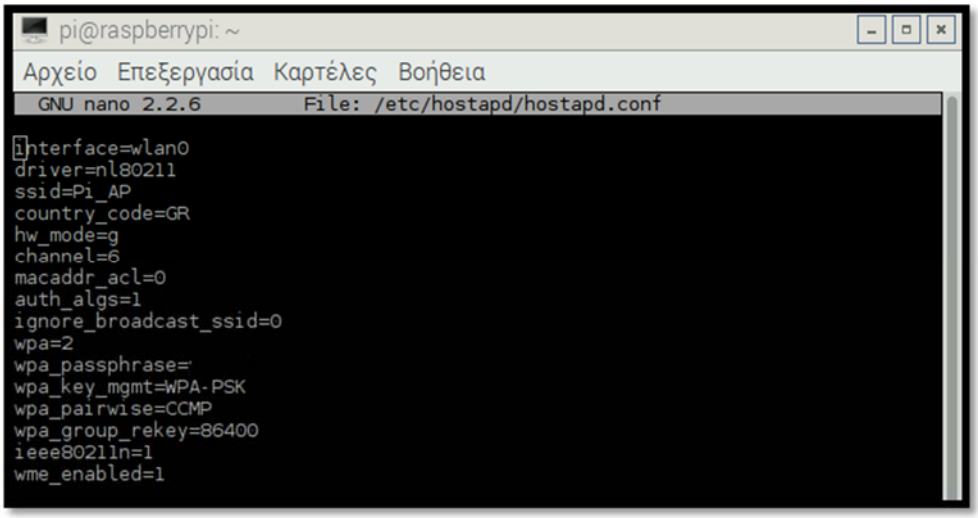
Εικόνα 28
Τα iptables του Onion Proxy



Εικόνα 29
Η καταγραφή των συμβάντων κατά τη λειτουργία του Onion Proxy



Εικόνα 30
Η διαμόρφωση του αρχείου /etc/tor/torrc στο Onion Proxy



Εικόνα 31
Η διαμόρφωση του αρχείου /etc/hostapd/ hostapd.conf στο Onion Proxy

Κεφάλαιο 6

Συμπεράσματα

Η παρούσα εργασία είχε ως σκοπό την εύρεση των εργαλείων με τα οποία μπορεί να πραγματοποιηθεί διερεύνηση του Dark Web, καθώς και η καταγραφή, η ανάλυση και η αξιολόγησή τους. Χρησιμοποιήθηκαν όλοι οι ευρέως διαδεδομένοι μηχανισμοί πρόσβασης στο Dark Web, αλλά και τα δίκτυα Friend to Friend. Στο Κεφάλαιο 1 έγινε θεωρητική θεμελίωση και ανάλυση των όρων Dark Web, Darknet, Deep Web και Surface Web, στο Κεφάλαιο 2 παρουσιάστηκαν οι τρόποι με τους οποίους επιτυγχάνεται η ανωνυμία και υλοποιούνται τα διάφορα Darknets. Στο κεφάλαιο 3 αναλύθηκαν τα δίκτυα Friend to Friend. Στο κεφάλαιο 4 αναλύθηκαν οι διάφοροι τρόποι κακόβουλης εκμετάλλευσης του Dark Web. Τέλος, στο Κεφάλαιο 5, πραγματοποιήθηκε η διερεύνηση του Dark Web με την χρήση κατάλληλων εργαλείων. Τα εργαλεία που χρησιμοποιήθηκαν ήταν το OnionScan, τα διαθέσιμα εργαλεία του Ahmia Project, το Maltego Community Edition και τα Automater, Theharvester με την χρήση του Raspberry Pi ως Onion Proxy. Στη παρούσα εργασία δόθηκε έμφαση κυρίως στο δίκτυο Tor. Αυτό συνέβη κυρίως γιατί αποτελεί τον πιο δημοφιλή τρόπο πρόσβασης στο Dark Web, αλλά και τον πιο εύκολο τρόπο πρόσβασης για έναν μέσο χρήστη. Σε ότι αφορά τη χρήση εργαλείων τα συμπεράσματα που εξήχθησαν είναι τα εξής:

α) Ahmia Project Tools

Το Ahmia Project προσφέρει διάφορα εργαλεία για την έρευνα του Dark Web. Ορισμένα από τα εργαλεία είναι σχετικά απλά στην εγκατάσταση και λειτουργία όπως πχ TorBalancer και το Onion Visual, ενώ άλλα είναι πιο πολύπλοκα. Τα περισσότερα εργαλεία είναι επεκτάσιμα, όμως προϋποθέτουν γνώση της γλώσσας προγραμματισμού Python. Από τα εργαλεία που δοκιμάστηκαν είναι το μόνο εργαλείο που δίνει τη δυνατότητα έρευνας και στο δίκτυο I2P.

β) Onionscan

Αποτελεί το εργαλείο του οποίου, η εγκατάσταση και η χρήση είναι πολύ πιο εύκολη σε σχέση με τα εργαλεία που χρησιμοποιήθηκαν. Επιπλέον, για τη λειτουργία του δεν απαιτούνταν κάποια ιδιαίτερη ρύθμιση του δικτύου ή η εκτέλεση της υπηρεσίας Tor. Εκτός, από την ευρετηρίαση των διευθύνσεων onion, πραγματοποιεί και ελέγχους οι οποίοι αφορούν το επίπεδο ασφάλειας και ανωνυμίας των ιστότοπων .onion και σε συνδυασμό με άλλα εργαλεία μπορούν να εξαχθούν χρήσιμες πληροφορίες.

γ) Maltego Community Edition

Αποτελεί ένα εργαλείο απλό στην εγκατάσταση και την χρήση. Για να ληφθούν πληροφορίες που αφορούν το δίκτυο Tor, απαιτείται η χρήση Onion Proxy. Οι πληροφορίες οι οποίες λήφθηκαν από το συγκεκριμένο εργαλείο, αφορούσαν κυρίως τιμές κατακερματισμού κακόβουλου λογισμικού που εντοπίστηκε στους ιστότοπους.

Τέλος, με την ανασκόπηση πηγών που αφορούσαν την κακόβουλη χρήση του Dark Web διαπιστώθηκε ότι τα τελευταία χρόνια πραγματοποιείται εκμετάλλευση του σκοτεινού διαδικτύου προκειμένου οι κυβερνοεγκληματίες να αποκρύψουν τη πραγματική τους ταυτότητα.

Βιβλιογραφία

[1] Allievi Andrea, & Carter Earl. (2015). Ransomware on Steroids: Cryptowall 2.0. Retrieved April 23, 2017, from http://blogs.cisco.com/security/talos/cryptowall-2

[2] Artturi. (2014). OnionDuke: APT Attacks Via the Tor Network. Retrieved April 23, 2017, from https://www.f-secure.com/weblog/archives/00002764.html

[3] Bergman, M. K. (2001). White Paper: The Deep Web: Surfacing Hidden Value. *The Journal of Electronic Publishing*, *7*(1), 1–17. https://doi.org/10.3998/3336451.0007.104

[4] Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., & Felten, E. W. (2015). Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. *IEEE Symposium on Security and Privacy*, 104–121. https://doi.org/10.1109/SP.2015.14

[5] Casenove, M., & Miraglia, A. (2014). Botnet over Tor: The Illusion of Hiding, 273–282.

[6] Clarke, I., Sandberg, O., Wiley, B., and Hong, T. W. (2001). A distributed anonymous information storage and retrieval system. *Journal of Chemical Information and Modeling*, *53*(9), 1689–1699. https://doi.org/10.1017/CBO9781107415324.004

[7] Cyril. (n.d.). RetroShare's anonymous routing model. Retrieved from https://retroshareteam.wordpress.com/2012/11/03/retroshares-anonymous-routing-model/

[8] Danezis, G., & Diaz, C. (2005). A Survey of Anonymous Peer-to-Peer File-Sharing. *Journal of Privacy Technology*. https://doi.org/10.1007/11596042_77

[9] Daniel So, C. (2014). TrendLabs Security Intelligence BlogBIFROSE Now More Evasive Through Tor, Used for Targeted Attack - TrendLabs Security Intelligence Blog. Retrieved April 23, 2017, from http://blog.trendmicro.com/trendlabs-security-intelligence/bifrose-now-more-evasive-through-tor-used-for-targeted-attack/

[10] Dingledine, R., & Mathewson, N. (n.d.). Torspec - Tor's protocol specifications. Retrieved April 23, 2017, from https://gitweb.torproject.org/torspec.git/tree/tor-spec.txt

[11] Dingledine, R., Mathewson, N., & Syverson, P. (n.d.). Tor : The Second-Generation Onion Router.

[12] Fachkha, C., Bou-Harb, E., Boukhtouta, A., Dinh, S., Iqbal, F., & Debbabi, M. (2012). Investigating the dark cyberspace: Profiling, threat-based analysis and correlation. *7th International Conference on Risks and Security of Internet and Systems, CRiSIS 2012*. https://doi.org/10.1109/CRISIS.2012.6378947

[13] Gehl, R. W. (2016). Power/freedom on the dark web: A digital ethnography of the Dark Web Social Network. *New Media & Society*, *18*(7), 1219 –1235. https://doi.org/10.1177/1461444814554900

[14] Isdal, T., Piatek, M., Krishnamurthy, A., & Anderson, T. (2010). Privacy-preserving P2P data sharing with OneSwarm. *ACM SIGCOMM Computer Communication Review*, *40*(4), 111. https://doi.org/10.1145/1851275.1851198

[15] Lucian Constantin. (2012). Tor network used to command Skynet botnet | Computerworld. Retrieved April 23, 2017, from http://www.computerworld.com/article/2493980/malware-vulnerabilities/tor-network-used-to-command-skynet-botnet.html

[16] Mittal, P., Caesar, M., & Borisov, N. (2012). X-Vine: Secure and Pseudonymous Routing Using Social Networks. *Network and Distributed System Security Symposium*, (April), 15. Retrieved from http://arxiv.org/abs/1109.0971

[17] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. *Www.Bitcoin.Org*, 9. https://doi.org/10.1007/s10838-008-9062-0

[18] Nunes, E., Diab, A., Gunn, A., Marin, E., Mishra, V., Paliath, V., … Shakarian, P. (2016). Darknet and Deepnet Mining for Proactive Cybersecurity Threat Intelligence. *arXiv Preprint arXiv:*, 1–6. https://doi.org/10.1109/ISI.2016.7745435

[19] Paganini, P. (2015). Hunting Malware in the Deep Web. Retrieved April 23, 2017, from http://resources.infosecinstitute.com/hunting-malware-deep-web/

[20] Pierluigi Paganini. (2012). Botnet, pro & cons of using Tor Networks - Security AffairsSecurity Affairs. Retrieved April 23, 2017, from http://securityaffairs.co/wordpress/8678/cyber-crime/botnet-pro-cons-of-using-tor-networks.html

[21] Pitts, J. (2015). Repurposing OnionDuke : A Single Case Study Around Reusing Nation State Malware. *Black Hat*.

[22] Pouwelse, J. (n.d.). Multi-Year Aim: create a censorship-free Internet. Retrieved from https://github.com/Tribler/tribler/wiki

[23] Roos, S., & Strufe, T. (2013). A contribution to analyzing and enhancing Darknet routing. *Proceedings - IEEE INFOCOM*, 615–619. https://doi.org/10.1109/INFCOM.2013.6566846

[24] Spies, T. (2014). Public Key Infrastructure. *Public Key Infrastructure*, *18*(3), 75–107. https://doi.org/10.1016/B978-0-12-416681-3.00003-3

[25] Tarakanov, D. (2013). The Inevitable Move – 64-bit ZeuS Enhanced With Tor. Retrieved from https://securelist.com/blog/events/58184/the-inevitable-move-64-bit-zeus-enhanced-with-tor/

[26] Toth, G. X. (2013). Design of a Social Messaging System Using Stateful Multicast, (August), 76. Retrieved from https://gnunet.org/design-social-messaging-system

[27] Varde, A. S., Suchanek, F. M., Nayak, R., & Senellart, P. (2009). Knowledge Discovery over the Deep Web , Semantic Web and XML • The Web is a vast source of information. *Agenda*, 784–788.

[28] Yotam Gottesman. (2014). RSA Uncovers New POS Malware Operation Stealing Payment Card & Personal Information - Speaking of Security - The RSA Blog. Retrieved April 23, 2017, from http://blogs.rsa.com/rsa-uncovers-new-pos-malware-operation-stealing-payment-card-personal-information/

[29] Zantout, B., & Haraty, R. (2011). I2P data communication system. *ICN 2011, The Tenth International Conference …*, (c), 401–409. Retrieved from http://www.thinkmind.org/index.php?view=article&articleid=icn_2011_19_10_10010

[30] About GNUnet. (n.d.). Retrieved from https://gnunet.org/about

[31] Ahmia Onion-Visual. (n.d.). Retrieved from https://github.com/ahmia/onion-visual

[32] Ahmia Torbalancer. (n.d.). Retrieved from https://github.com/ahmia/Torbalancer

[33] Ahmia-crawler. (n.d.). Retrieved from https://github.com/ahmia/ahmia-crawler

[34] Ahmia-index. (n.d.). Retrieved from https://github.com/ahmia/ahmia-index

[35] Ahmia-site. (n.d.). Retrieved from https://github.com/ahmia/ahmia-site

[36] *Anonymous Downloading and Streaming specifications*. (2014). Retrieved from https://github.com/Tribler/tribler/wiki/Anonymous-Downloading-and-Streaming-specifications

[37] Dark Net Markets Comparison Chart - Deep Dot Web. (n.d.). Retrieved April 25, 2017, from https://www.deepdotweb.com/dark-net-market-comparison-chart/

[38] I2P Naming. (n.d.). Retrieved from https://geti2p.net/en/docs/naming

[39] I2PHelper_HowTo. (n.d.). Retrieved from https://wiki.vuze.com/w/I2PHelper_HowTo

[40] I2pTransmission. (n.d.). Retrieved from http://www.i2pwiki.i2p/index.php?title=I2pTransmission

[41] Interview of Maj. Patrick Michaelis. (n.d.). Retrieved from https://www.pbs.org/wgbh/pages/frontline/shows/company/lessons/

[42] Pebble. (n.d.). Retrieved from http://pebble.sourceforge.net/

[43] Phex. (n.d.). Retrieved from https://en.wikipedia.org/wiki/Phex

[44] Ransomware. (n.d.). Retrieved from https://www.trendmicro.com/vinfo/us/security/definition/ransomware

[45] Robert (P2P_software). (n.d.). Retrieved from https://en.wikipedia.org/wiki/Robert_(P2P_software)

[46] Sefnit's Tor botnet C&C details – Microsoft Malware Protection Center Blog. (2014). Retrieved April 23, 2017, from https://blogs.technet.microsoft.com/mmpc/2014/03/05/sefnits-tor-botnet-cc-details/

[47] Sensitive But Unclassified IP Data. (n.d.). Retrieved from http://www.disa.mil/Network-Services/Data/SBU-IP

[48] Skynet, a Tor-powered botnet straight from Reddit | Rapid7 Community and Blog. (2012). Retrieved April 23, 2017, from https://community.rapid7.com/community/infosec/blog/2012/12/06/skynet-a-tor-powered-botnet-straight-from-reddit

[49] Susimail. (n.d.). Retrieved from https://en.wikipedia.org/wiki/Susimail

[50] Syndie. (n.d.). Retrieved from http://www.i2pwiki.i2p/index.php?title=Syndie

[51] Tahoe-Lafs. (n.d.). Retrieved from https://tahoe-lafs.org/trac/tahoe-lafs/wiki/FAQ

[52] The current state of ransomware: CryptoWall – Sophos Blog. (2015). Retrieved April 23, 2017, from https://news.sophos.com/en-us/2015/12/17/the-current-state-of-ransomware-cryptowall/

[53] The current state of ransomware: CTB-Locker – Sophos Blog. (2015). Retrieved April 23, 2017, from https://news.sophos.com/en-us/2015/12/31/the-current-state-of-ransomware-ctb-locker/

[54] The Invisible Internet Project (I2P). (n.d.). Retrieved from https://geti2p.net/el/about/intro

[55] Tor Messenger Design Document. (n.d.). Retrieved from https://trac.torproject.org/projects/tor/wiki/doc/TorMessenger/DesignDoc

[56] Tor: Hidden Service Protocol. (n.d.). Retrieved from https://www.torproject.org/docs/hidden-services.html.en

[57] Tor: Overview. (n.d.). Retrieved from https://www.torproject.org/about/overview.html.en

[58] TorBalancer. (n.d.). Retrieved from https://github.com/ahmia/TorBalancer

[59] What is a Trojan Virus | Trojan Virus Definition | Kaspersky Lab US. (n.d.). Retrieved November 30, 2017, from https://usa.kaspersky.com/resource-center/threats/trojans

[60] What_is_Freenet. (n.d.). Retrieved from https://github.com/freenet/wiki/wiki/FAQ#What_is_Freenet.3F

[61] Zeronet. (n.d.). Retrieved from https://zeronet.readthedocs.io/en/latest/#how-does-it-work