Ανάλυση τεχνουργημάτων σκοτεινού διαδικτύου

Πάνος Μαλτσινιώτης, Επόπτης Χρήστος Λιάμπας
Σχολή Πληροφορικής

Εισαγωγή

Η παρούσα πτυχιακή εργασία εστιάζει στην ανάλυση του προγράμματος Tor και του λειτουργικού συστήματος Tails, καθώς και στη χρήση τους στο λειτουργικό περιβάλλον των Windows 10. Στόχος είναι η κατανόηση της λειτουργίας αυτών των εργαλείων και η εξέταση των ψηφιακών ιχνών (artifacts) που αφήνουν, καθώς και των μεθόδων πρόσβασης στο dark web.

Μεθοδολογία

Η Μεθοδολογία που χρησιμοποιήθηκε για την εύρεση των ψηφιακών ιχνών ήταν η εξερεύνηση των αρχείων του συστήματος Windows 10. Αρχικά, πραγματοποιήθηκε κάποια περιήγηση σε ισότοπους μέσω του Tor browser, σύνδεση με email και λήψη εικόνων από το διαδίκτυο. Σκοπός ήταν να γίνει εντοπισμός και ανίχνευση από ίχνη μετά το τέλος της περιήγησης του Tor Browser. Στη συνέχεια, πραγματοποιήθηκε εντοπισμός πιθανόν ιχνών μέσω διάφορων τρόπων και εργαλείων, όπως το εργαλείο Autopsy και η συγγραφή script με την γλώσσας προγραμματισμού python.



Αποτελέσματα

Εργαλείο	Λειτουργικό/Πρόγραμμα	Τόπος Ευρήματος	Έυρημα
Aytophy	Tor	Tor Browser/Browser	scriptCache-child-current.bin
Script PowerShell	Windows	Downloads/ERP-System-Laravel-5.4-master/ERP-System-Laravel-5.4-master/public/js/plugins/codemirror/mode/tornado	Tornado.js
Script PowerShell	Windows	Desktop/Tor Browser/Data/Browser/profile.default/cookies.sqlite	Cookies.sqlite

Συμπεράσματα

Η έρευνα αυτή αναδεικνύει ότι, παρά τις δυνατότητες ανωνυμίας που προσφέρουν το Tor και το Tails, υπάρχουν ακόμα ψηφιακά ίχνη που μπορούν να αποκαλυφθούν με την κατάλληλη τεχνική ανάλυση. Σε γενικές γραμμές, η ανάλυση των ψηφιακών ιχνών που αφήνονται από τη χρήση του Tor και του Tails αποδεικνύει ότι, παρά τις δυνατότητες ανωνυμίας, η απόλυτη προστασία από την ανίχνευση απαιτεί προσεκτική διαχείριση και γνώση των εργαλείων που χρησιμοποιούνται.

Βιβλιογραφία

https://tails.net/about/index.en.html

https://www.torproject.org/about/reports/

Jadoon, Abid & Iqbal, Waseem & Amjad, Muhammad & Afzal, Hammad & Bangash, Yawar. (2019). *Forensic Analysis of Tor Browser: A Case Study for Privacy and Anonymity on the Web.*