ΔΙΑΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ ΑΚΑΔΗΜΑΪΚΟΥ ΕΤΟΥΣ 2022-23

Τεχνοοικονομικά Συστήματα
(Techno-economic Systems)

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
Σχολή Ναυτιλίας & Βιομηχανίας του Τμήματος Βιομηχανικής Διοίκησης και Τεχνολογίας

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Μηχανισμοί Διείσδυσης Εισβολέων Υπολογιστών Συστημάτων - Εγκαθίδρυση μιας Καλοστημένης Επιχειρηματικής Μηχανής στο Σκοτεινό Διαδίκτυο (Dark Web)

Γεώργιος Τσαβδαρίδης
(ΑΜ: 03203386)

ΕΠΙΒΛΕΠΩΝ
Αναστάσιος Δουλάμης,
Αναπληρωτής Καθηγητής, Τομέα Τοπογραφίας
Σχολή Αγρονόμων και Τοπογράφων Μηχανικών - Μηχανικών Γεωπληροφορικής

Αθήνα, **Φεβρουάριος 2023**

ΔΙΑΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ ΑΚΑΔΗΜΑΪΚΟΥ ΕΤΟΥΣ 2021-23

Τεχνοοικονομικά Συστήματα
(Techno-economic Systems)

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
Σχολή Ναυτιλίας & Βιομηχανίας του Τμήματος Βιομηχανικής Διοίκησης και Τεχνολογίας

Μηχανισμοί Διείσδυσης Εισβολέων Υπολογιστών Συστημάτων - Εγκαθίδρυση μιας Καλοστημένης Επιχειρηματικής Μηχανής στο Σκοτεινό Διαδίκτυο (Dark Web)

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Γεώργιος Τσαβδαρίδης

Τριμελής Συμβουλευτική Επιτροπή:

Εγκρίθηκε από την Τριμελή Εξεταστική Επιτροπή την 7η Φεβρουαρίου 2023

(Επιβλέπων)	2ο Μέλος	3ο Μέλος
Αναστάσιος Δουλάμης	Νικόλαος Δουλάμης	Νικόλαος Β. Καραδήμας
Αναπληρωτής Καθηγητής	Καθηγητής	Αναπληρωτής Καθηγητής
Σχολή Αγρονόμων & Τοπογράφων Μηχανικών - Μηχανικών Γεωπληροφορικής	Σχολή Αγρονόμων & Τοπογράφων Μηχανικών - Μηχανικών Γεωπληροφορικής	Τομέας Μαθηματικών & Επιστημών Μηχανικού
Τομ. Τοπογραφίας, Εργαστήριο Φωτογραμμετρίας	Τομ. Τοπογραφίας	Τμήμα Στρατιωτικών Επιστημών
Εθνικό Μετσόβιο Πολυτεχνείο	Εθνικό Μετσόβιο Πολυτεχνείο	Στρατιωτική Σχολή Ευελπίδων

Η σελίδα αυτή σκόπιμα κενή

Γεώργιος Τσαβδαρίδης

ΥΔ Σχολής Ηλεκτρολόγων Μηχανικών και Μηχανικών Η/Υ,

Εθνικού Μετσόβιου Πολυτεχνείου

Αθήνα, Φεβρουάριος 2023

1. **Απόφοιτος Αξιωματικός Πυροβολικού Στρατιωτικής Σχολής Ευελπίδων** (Σ.Σ.Ε) [ΠΔ 19-06-2002, 70/2002 ΕΔΥΕΘΑ, Αριθμός Πτυχίου 2721]
2. **Διπλωματούχος Μεταπτυχιακών Σπουδών** «Μαθηματικής Προτυποποίησης σε Σύγχρονες Τεχνολογίες και τη Χρηματοοικονομική» της **Σχολής Εφαρμοσμένων Μαθηματικών Επιστημών & Φυσικών Επιστημών (ΣΕΜΦΕ)** του **Εθνικού Μετσόβιου Πολυτεχνείου (ΕΜΠ)**

   [Αριθμός Διπλώματος 219/2013]
3. **Τελειόφοιτος Διπλωματούχος Μεταπτυχιακών Σπουδών** «Τεχνο-Οικονομικά Συστήματα» της **Σχολής Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών (ΗΜΜΥ)** του **Εθνικού Μετσόβιου Πολυτεχνείου (ΕΜΠ)**

Copyright © Γεώργιος Τσαβδαρίδης, 2023

Με επιφύλαξη παντός δικαιώματος. All rights reserved.

Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας εργασίας, εξ ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μήνυμα. Ερωτήματα που αφορούν τη χρήση της εργασίας για κερδοσκοπικό σκοπό πρέπει να απευθύνονται προς τον συγγραφέα. Οι απόψεις και τα συμπεράσματα που περιέχονται σε αυτό το έγγραφο εκφράζουν τον συγγραφέα και τις απόψεις του Επιβλέποντα Καθηγητή και δεν πρέπει να ερμηνευθεί ότι αντιπροσωπεύουν τις επίσημες θέσεις του Εθνικού Μετσόβιου Πολυτεχνείου.

Η σελίδα αυτή σκόπιμα κενή

Καλὸν δὲ καὶ τὸ τακτικὸν εἶναι πολὺ γὰρ διαφέρει στράτευμα τεταγμένον ἀτάκτου, ὥσπερ λίθοι τε καὶ πλίνθοι καὶ ξύλα καὶ κέραμος ἀτάκτως μὲν ἐρριμμένα οὐδὲν χρήσιμά ἐστιν

Ξενοφών (430-355 π.Χ.)

«……*Η έκφραση προέρχεται από τα Απομνημονεύματα του Ξενοφώντος, όπου μιλάει ο Σωκράτης για τις ιδιότητες του Στρατηγού, θέλοντας να δείξει τη σπουδαιότητα της τακτικής τέχνης, είπε πως ο άτακτος στρατός θυμίζει υλικά για χτίσιμο ριγμένα ανάκατα κι επομένως άχρηστα για να κτιστεί καλά το σπίτι*….».

Η σελίδα αυτή σκόπιμα κενή

ΕΥΧΑΡΙΣΤΙΕΣ

Η παρούσα Διπλωματική Εργασία εκπονήθηκε στο Διαπανεπιστημιακό Πρόγραμμα Μεταπτυχιακών Σπουδών, ακαδημαϊκού έτους 2021-23 ‘’ Τεχνοοικονομικά Συστήματα (*Techno-economic Systems*) της Σχολής Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών (ΣΗΜΜΥ) του Εθνικού Μετσόβιου Πολυτεχνείου (Ε.Μ.Π) και της Σχολής Ναυτιλίας & Βιομηχανίας του Τμήματος Βιομηχανικής Διοίκησης και Τεχνολογίας του Πανεπιστημίου Πειραιώς, υπό την επίβλεψη του κ. Αναστάσιου Δουλάμη, Αναπληρωτή Καθηγητή Τομέα Τοπογραφίας της Σχολής Αγρονόμων και Τοπογράφων Μηχανικών - Μηχανικών Γεωπληροφορικής του Εθνικού Μετσόβιου Πολυτεχνείου, ο οποίος μου ανέθεσε το αντικείμενο της Διπλωματικής Εργασίας, αφού έλαβε εκ των προτέρων υπόψη τα ειδικά επαγγελματικά μου ενδιαφέροντα.

Με την παρούσα Διπλωματική Εργασία περατώνονται οι σπουδές σε Μεταπτυχιακό επίπεδο με τίτλο:

«Μηχανισμοί Διείσδυσης Εισβολέων Υπολογιστών Συστημάτων - Εγκαθίδρυση μιας Καλοστημένης Επιχειρηματικής Μηχανής στο Σκοτεινό Διαδίκτυο (Dark Web)»

Από τη θέση αυτή οφείλω να ευχαριστήσω θερμά τους ανθρώπους που συνέβαλλαν καθοριστικά στην ολοκλήρωσή της Εργασίας και συγκεκριμένα τους:

1. κ. **Αναστάσιο Δουλάμη**, *Αναπληρωτή Καθηγητή του Τομέα Τοπογραφίας της Σχολής Αγρονόμων και Τοπογράφων Μηχανικών - Μηχανικών Γεωπληροφορικής του Εθνικού Μετσόβιου Πολυτεχνείου*, ο οποίος ως επιβλέπων επέδειξε πλήρη εμπιστοσύνη στο πρόσωπό μου, δίνοντας μου ακαδημαϊκό βήμα συγγραφής της παρούσας Εργασίας. Η συνολική επιστημονική καθοδήγηση και υποστήριξη του, αλλά και η εξαίρετη συνεργασία μαζί μου, κατά τη διάρκεια της συγγραφής συνέβαλλαν, ώστε να περατώσω επιτυχώς τις Μεταπτυχιακές μου Σπουδές.

2. κ. **Νικόλαο Δουλάμη***, Καθηγητή του Τομέα Τοπογραφίας της Σχολής Αγρονόμων και Τοπογράφων Μηχανικών - Μηχανικών Γεωπληροφορικής του Εθνικού Μετσόβιου Πολυτεχνείου*, για την τιμή που μου έκανε να συμμετάσχει στη διαδικασία κρίσης της Διπλωματικής Εργασίας μου, ως μέλος της 3μελούς Εξεταστικής Επιτροπής. Πρόκειται για έναν Καθηγητή, ιδιαιτέρως ευγενή και ηθικό, ο οποίος κοσμεί την επιστημονική κοινότητα με την παρουσία του, ενώ μεταξύ άλλων ξεχωρίζει για το επιστημονικό βεληνεκές και το ακαδημαϊκό του υπόβαθρο.

3. κ. **Νικόλαο Καραδήμα**, *Αναπληρωτή Καθηγητή του Τμήματος Στρατιωτικών Επιστημών του Τομέα Μαθηματικών & Επιστημών Μηχανικού της Στρατιωτικής Σχολής Ευελπίδων*, για την τιμή που μου έκανε να συμμετάσχει στη διαδικασία κρίσης της Διπλωματικής Εργασίας μου, ως μέλος της 3μελούς Εξεταστικής Επιτροπής. Τον ευχαριστώ ιδιαιτέρως για την μέχρι τώρα διαρκή συμβουλευτική ακαδημαϊκή υποστήριξη που μου παρέχει και ειλικρινά του εύχομαι ένα λαμπρό επαγγελματικό μέλλον και να συναντά πάντα χαρές στη ζωή του.

4. κ. **Γεώργιο Παπαζαφειρόπουλο**, Δρ. ΕΜΠ και Επισμηναγό (Μηχανικό Εγκαταστάσεων) της Πολεμικής Αεροπορίας, για την στοχευμένη υποβοήθηση που μου παρείχε στην τελική φάση ολοκλήρωσης της παρούσας Διατριβής. Ιδιαίτερα δε, τον συγχαίρω για το ήθος, τον χαρακτήρα του, καθώς και για το ευρύτερο ακαδημαϊκό και αεροπορικό του υπόβαθρο και ειλικρινά του εύχομαι ένα λαμπρό ακαδημαϊκό και επαγγελματικό μέλλον.

Κλείνοντας, θα ήθελα να ευχαριστήσω την αγαπημένη μου οικογένεια αποτελούμενη από την σύζυγο μου Ειρήνη Παπάρα, Άξιο Στέλεχος της Πολεμικής Αεροπορίας, η οποία με αγόγγυστη και ακούραστη υπομονή με στήριξε, προκειμένου να περατώσω εκ νέου τις δεύτερες Μεταπτυχιακές μου Σπουδές στο Εθνικό Μετσόβιο Πολυτεχνείο.

Τέλος δε, αφιερώνω την παρούσα Διπλωματική Διατριβή στα παιδιά μου Άγγελο Τσαβδαρίδη, μαθητή της Α΄ Λυκείου και Αναστασία Τσαβδαρίδου, μαθήτρια ΣΤ΄ Δημοτικού, τα οποία συμβουλεύω να ακολουθήσουν τα λόγια του Ισοκράτη (436-338 π.Χ., Αθηναίου ρήτορα):

‘***’Ώσπερ γαρ την μέλιτταν ορώμεν εφ' άπαντα μεν τα βλαστήματα καθιζάνουσαν, αφ' εκάστου δε τα βέλτιστα λαμβάνουσαν, ούτω δει και τους παιδείας ορεγομένους μηδενός μεν απείρως έχειν, πανταχόθεν δε τα χρήσιμα συλλέγειν’’*,**

δηλαδή να μην σταματήσουν ουδέποτε να συλλέγουν επιλεκτικά, όπως η μέλισσα από όλα τα φυτά, ό,τι καλύτερο και ωφέλιμο σε γνώση και μόρφωση υπάρχει, ευχόμενος από καρδιάς να αποτελέσω τη φλογοβόλο σπίθα για το ξεκίνημα της δικής τους ακαδημαϊκής πορείας.

Γεώργιος Τσαβδαρίδης

Αθήνα, Φεβρουάριος 2023

ΠΕΡΙΛΗΨΗ
ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

Στην παρούσα Εργασία, παρουσιάζεται το τεχνολογικό και ερευνητικό προσκήνιο του Διαδικτύου, το οποίο σχηματικά να περιγράφεται ως ένα τεράστιο παγόβουνο, η κορυφή του οποίου είναι το Επιφανειακό Διαδίκτυο (*Surface Web*). Κάτω από την επιφάνεια της θάλασσας βρίσκεται το μεγαλύτερο μέρος του παγόβουνου, που ονομάζεται ως Βαθύ Διαδίκτυο (*Deep Web*), ενώ στον "πάτο" του παγόβουνου βρίσκεται το Σκοτεινό Διαδίκτυο (*Dark Web*).

Το Διαδίκτυο χρησιμοποιείται καθημερινά από εκατομμύρια Χρήστες παγκοσμίως. Οι περισσότεροι εξ΄ αυτών δεν γνωρίζουν ότι υπάρχει ένας άγνωστος χώρος, στον οποίο η πρόσβαση δεν είναι ορατή. Ο διαδικτυακός χώρος, που ονομάζεται Σκοτεινός Ιστός παρέχει κρυφές υπηρεσίες και μυστικά κανάλια επικοινωνίας, τα οποία έλκουν τους Χρήστες με τρόπο μη ελέγξιμο και διαχειρίσιμο. Εξ΄ ου και το σκοτεινό Διαδίκτυο γενικότερα, έχει χρησιμοποιηθεί από εγκληματικές ομάδες.

Το Σκοτεινό Διαδίκτυο στην πραγματικότητα είναι ένα τεράστιο πλέγμα από υπολογιστές υποδομές, πελάτες, αγαθά, προϊόντα, υπηρεσίες, συνεργασίες με τρίτους, μηχανισμών εσόδων, κτλ., το οποίο αποτελεί μία από τις πιο έξυπνες και καλοστημένες επιχειρηματικές μηχανές, που αποφέρει τεράστια κέρδη. Στην παρούσα μελέτη θα εφαρμοσθεί το μοντέλο Business Model Canvas για την τεκμηρίωση του γεγονότος ότι η αγορά του Dark Web είναι ταχέως εξελισσόμενη και σίγουρα επιφυλάσσει αχαρτογράφητες εκπλήξεις στο μέλλον.

Τέλος, παρουσιάζονται οι τακτικές και οι τεχνικές, που χρησιμοποιούν οι λεγόμενοι Κακόβουλοι Εισβολείς Υπολογιστικών Συστημάτων (*οι οποίοι στην πραγματικότητα είναι εξειδικευμένοι προγραμματιστές και κρυπταναλυτές*) στην πλατφόρμα του Σκοτεινού Ιστού, ώστε να εντοπίσουν τα κενά ασφάλειας των Συστημάτων και Δικτύων Υπολογιστών, με σκοπό να προχωρήσουν σε μη εξουσιοδοτημένες ηλεκτρονικές κακόβουλες ενέργειες ή και επιθέσεις σε κρίσιμα Πληροφοριακά Συστήματα και σε Μεγάλους Οργανισμούς.

Λέξεις-Κλειδιά: Σκοτεινό Διαδίκτυο (***Dark Web***), Βαθύ Διαδίκτυο (***Deep Web***), Αρχιτεκτονική Σκοτεινού Ιστού (***Dark Web Architecture***), Επιχειρηματικό Μοντέλο (***Business Model Canvas***), Κρυπτονόμισματα (***Crypto Currency***), Μαύρη Αγορά (***Blanc Market***), Παράνομες Δραστηριότητες (***Illegal Activities***), Τεχνικές Εισβολέων Συστημάτων και Δικτύων Υπολογιστών (***Hacking Techniques in Computer and Network Systems***)

Η σελίδα αυτή σκόπιμα κενή

ABSTRACT

TITLE: Hacking Mechanisms in Computing Systems Network – Establishment of a Well Built Enterprise in Dark Web

In the present work, we examined the technological and research state of art of the Internet, which could be, schematically, described by a huge Iceberg, the top of which is called the Surface Web. Under of the surface of the sea is the biggest part of this Iceberg, which is called Deep Web. On the bottom of the Iceberg is the part of Internet, which is called Dark Web.

It is well known that the internet is, daily, used by hundreds of users worldwide. Most of them, do not know that there is a secret and mystery place in which access is not visible. The Dark Web provides hidden services and secret communication channels, which attract many users in a uncontrollable and unmanageable way. Hence, the Dark Web, in general terms, has been used by criminal groups.

In fact, Dark Web is a huge grid of computers, customers, goods, products, services, partnerships with third parties, revenue mechanisms, etc., which functions as one of the most Intelligence and well-built Business Machine, with huge profits. In present study will be applied the Business Model Canvas model as evidence of the fact that the growing Market of the Dark Web is, rapidly, in progress and certainly reserves unpredictable surprises in the future.

Finally, in this work are presented the Hacking techniques, which invaders of Computer and Network Systems are using in malicious way. (Invaders are specialized in computer programming and cryptanalysis) on the Dark Web platform, in order to identify the vulnerable gaps of Computer and Network Systems for attacking on them to destroy Critical Information Systems or Big Organizations.

Keywords: Dark Web, Deep Web, Dark Web Architecture, Business Model Canvas, Crypto Currency, Blanc Market, Illegal Activities, Hacking Techniques in Computer and Network Systems

Η σελίδα αυτή σκόπιμα κενή

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Ευχαριστίες

Περίληψη Διπλωματικής Εργασίας

Abstract Διπλωματικής Εργασίας

Πίνακας Περιεχομένων…… **σελ. 15-16**

ΚΕΦΑΛΑΙΟ 1ο: Σκοπός της Διπλωματικής Εργασίας και Δομή της Παρουσίασης αυτής…….. **σελ. 17**

1.0 Σκοπός της Διπλωματικής Εργασίας

1.1 Δομή της Διπλωματικής Εργασίας

ΚΕΦΑΛΑΙΟ 2ο: Τεχνολογικό και Ερευνητικό Προσκήνιο στο Σκοτεινό Διαδίκτυο (Dark Net)…….. **σελ.19-40**

2.0 Σύντομο Ιστορικό του Σκοτεινού Διαδικτύου

2.1 Χρήσιμοι Ορισμοί: Επιφανειακό (Surface) - Σκοτεινό (Dark) - Βαθύ (Deep) Διαδίκτυο (Web)

2.2 Διαφορές μεταξύ Βαθύ (Deep) και Σκοτεινό (Dark) Διαδίκτυο

2.3 Τρόπος Λειτουργίας του Dark Web

2.4 Χρησιμότητα Dark Web για τους Χρήστες

2.5 Δρομολόγηση Onion Routing για Σύνδεση στο Dark Web

2.5.1 Κατανόηση Τρόπου Λειτουργίας Δρομολόγησης Onion Routing για Σύνδεση στο Dark Web

2.5.2 Παροχή Ανωνυμίας μέσω της TOR Κρυπτογράφησης και Αποκρυπτογράφησης στο Dark Web

2.5.3 Συνδυασμός Χρήσης VPN και TOR

2.6 Εναλλακτικοί Τρόποι Σύνδεσης στο Dark Web

ΚΕΦΑΛΑΙΟ 3ο : Εγκαθίδρυση μιας Καλοστημένης Επιχειρηματικής Μηχανής στο Σκοτεινό και Βαθύ Διαδίκτυο (Dark Web)……. **σελ. 41-58**

3.0 Το Επιχειρηματικό Μοντέλο (Business Model Canvas) του Σκοτεινού Ιστού (Dark Web)

3.1 Δομικοί Άξονες Επιχειρηματικού Μοντέλου για το Dark Web

3.1.1 Η Πρόταση Αξίας και τα Προϊόντα-Υπηρεσίες που παρέχονται στο Dark Web

3.1.2 Βασικοί Συνεργάτες (Key Partners)

3.1.3 Σχέσεις με Πελάτες (Customer Relationship)

3.1.4 Ροές Εσόδων (Revenue Streams)

3.1.5 Δομή Κόστους (Cost Structure)

3.1.6 Βασικές Δραστηριότητες (Key Activities)

3.1.6.1 Διαδικτυακά Δίκτυα Ρομπότ (Botnet) και Ηλεκτρονικό Ψάρεμα (Phishing)

3.1.6.2 Η Μαύρη Αγορά του Dark Web (Η περίπτωση του Silk Road)

3.1.6.3 Η Μαύρη Αγορά του Dark Web (Η περίπτωση του Sheep Marketplace)…

3.1.6.4 Παράνομη Πορνογραφία (Η περίπτωση του Playpen)

3.1.6.5 Τρομοκρατία (Η περίπτωση του Ισλαμικού Κράτους ISIS)

3.1.6.6 Υπηρεσίες Αντεκδίκησης (Η περίπτωση του Hitman Network)

3.1.6.7 Διαρροή Εικόνων Προσωπικών Δεδομένων Ατόμων προ-εφηβικής Ηλικίας (Η περίπτωση του Pink Meth)

3.1.6.8 Πώληση Πλαστών Εγγράφων (Διαβατήρια και Πιστωτικές Κάρτες)

3.2 Συνολική Αποτίμηση Business Model Canvas για το Σκοτεινό Διαδίκτυο

ΚΕΦΑΛΑΙΟ 4ο: Εισβολείς Υπολογιστικών Συστημάτων (Hackers) στο Dark Web……. **σελ. 59-79**

4.0 Ορισμοί -Χρήσιμη Ορολογία

4.1 Κατηγορίες Εισβολέων Υπολογιστικών Συστημάτων στο Dark Web

4.2 Υπολογιστικά Εργαλεία που Χρησιμοποιούν οι Hackers

4.3 Υπηρεσίες που παρέχονται από Hackers σε Τρίτα Άτομα

4.4 Χαρακτηριστικές Τακτικές και Τεχνικές Διείσδυσης σε Δίκτυα Υπολογιστών

ΚΕΦΑΛΑΙΟ 5ο: Συμπεράσματα – Κριτική…….... **σελ. 81-83**

ΒΙΒΛΙΟΓΡΑΦΙΑ: Διπλωματικής Διατριβής……... **σελ. 85-90**

ΚΕΦΑΛΑΙΟ 1ο :
ΣΚΟΠΟΣ ΤΗΣ ΔΙΠΛΩΜΑΤΙΚΗΣ ΔΙΑΤΡΙΒΗΣ ΚΑΙ ΔΟΜΗ ΤΗΣ ΠΑΡΟΥΣΙΑΣΗΣ ΑΥΤΗΣ

1.0 Σκοπός της Διπλωματικής Εργασίας

Ο σκοπός της παρούσης Διπλωματικής Διατριβής είναι να:

α) **Παρουσιάσει τον Σκοτεινό Ιστό** (Dark Web), **ως μία ταχέως εξελισσόμενη επιχειρηματική μηχανή**, η οποία αποτελεί ένα επιτυχημένο έξυπνο επιχειρηματικό μοντέλο στις μέρες μας, που παράγει ημερησίως τεράστια κέρδη επ΄ ωφελεία Χρηστών - πωλητών - πελατών και σίγουρα επιφυλάσσει αχαρτογράφητες και άγνωστες εκπλήξεις στο μέλλον.

β) **Συσχετίσει τη δράση των Εισβολέων Υπολογιστικών Συστημάτων** (Hackers) **στην πλατφόρμα του Σκοτεινού Ιστού**, η οποία παρέχει τεράστια ελευθερία κινήσεων για μυστικές δραστηριότητες που στοχεύουν, σε μη εξουσιοδοτημένες ηλεκτρονικές κακόβουλες ενέργειες ή και επιθέσεις σε κρίσιμα Πληροφοριακά Συστήματα και σε Μεγάλους Οργανισμούς.

1.1 Δομή της Διπλωματικής Εργασίας

Η παρούσα Διπλωματική Εργασία περιλαμβάνει τα εξής Κεφάλαια και Παραρτήματα:

Το **Κεφάλαιο «1»** είναι το παρόν Κεφάλαιο.

Στο **Κεφάλαιο «2»** παρουσιάζεται το τεχνολογικό και ερευνητικό προσκήνιο για το Σκοτεινό και Βαθύ Διαδίκτυο.

Στο **Κεφάλαιο «3»** αναλύονται οι δομικοί άξονες του Μοντέλου Business Model Canvas στο Σκοτεινό Ιστό ως μίας καλοστημένης επιχείρησης, η οποία αποφέρει τεράστια κέρδη.

Στο **Κεφάλαιο «4»** παρουσιάζονται οι τακτικές και οι τεχνικές, που χρησιμοποιούν Κακόβουλοι Εισβολείς Υπολογιστικών Συστημάτων στην πλατφόρμα του Σκοτεινού Ιστού, με σκοπό να προβούν σε κακόβουλες ενέργειες ή και επιθέσεις.

Στο **Κεφάλαιο «5»** παρατίθενται συμπεράσματα και γίνεται κριτική.

Τέλος, δίδεται η Βιβλιογραφία της Διπλωματικής Διατριβής.

Η σελίδα αυτή σκόπιμα κενή

ΚΕΦΑΛΑΙΟ 2ο:
Τεχνολογικό και Ερευνητικό Προσκήνιο στο Σκοτεινό Διαδίκτυο (Dark Net)

2.0 Σύντομο Ιστορικό του Σκοτεινού Διαδικτύου

Το Dark Web ή όπως αλλιώς "Darknet" πρωτοεμφανίστηκε πριν 20 χρόνια στις 20 Μαρτίου 2000 με την κυκλοφορία του "Freenet", ένα αποκεντρωμένο P2P δίκτυο, σχεδιασμένο με τέτοιο τρόπο, ώστε να είναι λιγότερο ευάλωτο σε επιθέσεις κατασκοπείας από άλλα κράτη. Το FREENET υπήρξε πνευματικό δημιούργημα του Ian Clarke, ο οποίος ανέπτυξε σχετικό εργαλείο λογισμικού κατά τη διάρκεια των σπουδών του στο Πανεπιστήμιο του Εδιμβούργο. Το εν λόγω λογισμικό αφορούσε ένα Κατανεμημένο, Αποκεντρωμένο Σύστημα Αποθήκευσης και Ανάκτησης Πληροφοριών (*Distributed, Decentralized Information Storage and Retrieval System*), το οποίο είχε ως σκοπό να παρέχει ελευθερία επικοινωνίας μεταξύ των χρηστών, χωρίς να επικρατεί ο φόβος της παρακολούθησης και ιχνηλάτησής τους στο Διαδίκτυο [SOA.1].

Στις μέρες μας, παρόλο που το FREENET είναι ακόμα διαθέσιμο δωρεάν σήμερα. Το FREENET αφορούσε κυρίως την ανταλλαγή πληροφοριών (*συμπεριλαμβανομένου πορνογραφικού και πειρατικού υλικού*). Εντούτοις, οι "σκληροπυρηνικοί" εγκληματίες του Κυβερνοχώρου εξακολουθούν να χρησιμοποιούν και άλλες πλατφόρμες για την εξυπηρέτηση των αναγκών τους π.χ. 4 Chan και IRC κανάλια [SOA.2].

Στις 20 Σεπτεμβρίου 2002, δημιουργήθηκε το Δίκτυο Onion Router (TOR) από τους Επιστήμονες Υπολογιστών, Roger Dingledine και Nick Mathewson. Παραδόξως, αυτό το λογισμικό χρηματοδοτήθηκε, ως επί το πλείστον, από το Ναυτικό Ερευνητικό Εργαστήριο των ΗΠΑ, με σκοπό τη δημιουργία ενός ασφαλέστερου τρόπου επικοινωνίας με πηγές πληροφοριών σε όλο τον κόσμο. Εξ΄ ου, είναι δυνατόν κατά μία έννοια να λεχθεί ότι το δίκτυο TOR δεν έχει σχεδιαστεί με κακή πρόθεση [SOA.3].

Υπήρχε πάντοτε η ανάγκη να δημιουργηθεί ένα δίκτυο επικοινωνιών με υψηλές προδιαγραφές ασφάλειας προστασίας ανώνυμων πηγών, ειδικά σε απολυταρχικά καθεστώτα. Παρόλα αυτά, το δίκτυο TOR υιοθετήθηκε από εγκληματίες και ως εκ τούτου συνδέθηκε η ύπαρξή του με παράνομες ενέργειες, χωρίς ωστόσο να μηδενίζεται το γεγονός της νόμιμης και εποικοδομητικής λειτουργίας του.

Το 2004, το Ναυτικό Ερευνητικό Εργαστήριο απελευθέρωση τη χρήση του Δικτύου TOR με δωρεάν άδεια. Το Ίδρυμα Electronic Frontier Foundation (EFF) άρχισε να χρηματοδοτεί επιστήμονες, όπως τον Dingledine Mathewson και άλλους, με σκοπό να συνεχίσουν την ταχεία ανάπτυξη του εν λόγω λογισμικού, έως ότου εν τέλει, ο Μη Κερδοσκοπικός Οργανισμός "The TOR Project" παρήγαγε το ομώνυμο λογισμικό [SOA.4].

Στις μέρες μας, το "Onion Router" είναι το πιο δημοφιλές μέσο, με το οποίο οι άνθρωποι έχουν πρόσβαση στο σκοτεινό Διαδίκτυο. Το TOR έχει πολλές μηχανές αναζήτησης, καταλόγους και κρυφά wikis, μέσω των οποίων οι Χρήστες μπορούν να περιηγηθούν στο σκοτεινό Διαδίκτυο για να βρουν οποιαδήποτε τοποθεσία επιθυμούν. Επί πλέον, υπάρχει επίσης και αντίστοιχο λογισμικό TOR για χρήση σε τηλέφωνα κινητής τηλεφωνίας [SOA.5].

Το TOR απλοποίησε σε μεγάλο βαθμό την ευκολία πρόσβασης και χρήσης του Dark Web. Εξαιτίας αυτού του γεγονότος, πολλοί Ιστότοποι προσαρμόστηκαν, με τέτοιο τρόπο ώστε να διασυνδεθούν με τις Υπηρεσίες Dark Web, ώστε να προσφέρουν κάθε είδους υπηρεσία που μπορεί κανείς να φανταστεί, είτε νόμιμη είτε παράνομη, χρησιμοποιώντας μία ευρεία ποικιλία διαδικτυακών πληρωμών, όπως Paypal και Western Union [SOA.6].

2.1 Χρήσιμοι Ορισμοί: Επιφανειακό (Surface) - Σκοτεινό (Dark) - Βαθύ (Deep) Διαδίκτυο (Web)

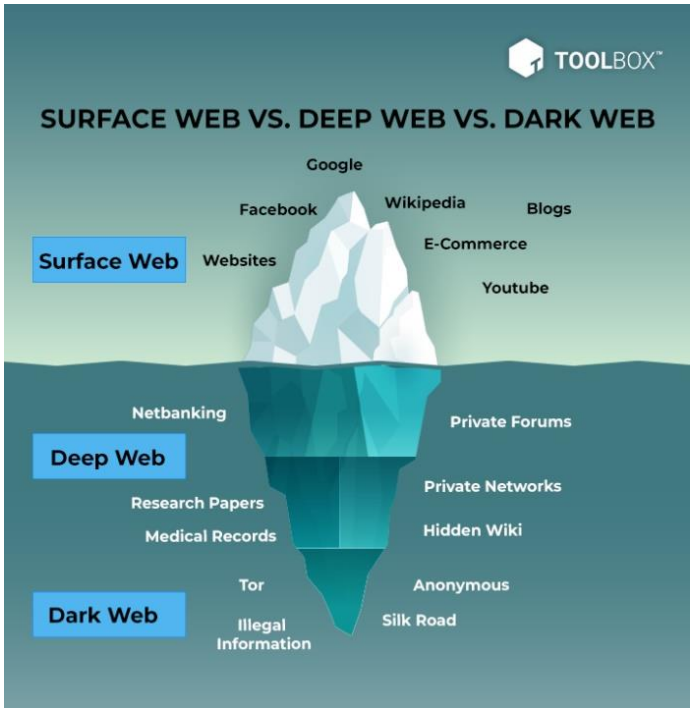
Το **Διαδίκτυο θα μπορούσε σχηματικά να περιγραφεί ως ένα πελώριο παγόβουνο**, η κορυφή του οποίου είναι το **Επιφανειακό Διαδίκτυο (Surface Web)**. Κάτω από την επιφάνεια της θάλασσας βρίσκεται το μεγαλύτερο μέρος του παγόβουνου, που ονομάζεται ως **Βαθύ Διαδίκτυο (Deep Web),** ενώ στον “πάτο” του παγόβουνου βρίσκεται το **Σκοτεινό Διαδίκτυο (Dark Web)**.

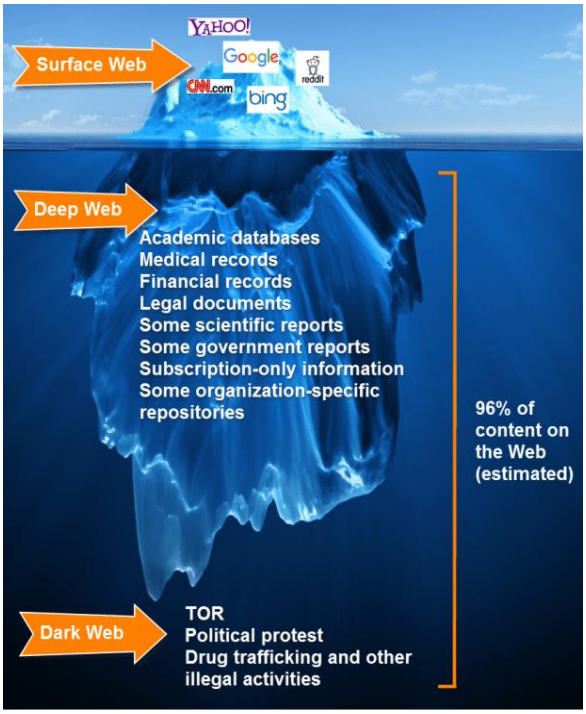
Ο επιφανειακός ιστός (**Surface Web)** ονομάζεται εξίσου και ως Common Web, Clearnet, Visible Web ή Lightnet. Είναι ο παραδοσιακός παγκόσμιος ιστός που περιέχει όλες τις γνωστές ιστοσελίδες, όπως το YouTube, το Facebook, τη Wikipedia, κλπ. Τα προγράμματα περιήγησης έχουν πρόσβαση σε αυτόν, ενώ μεταξύ άλλων δεν παρέχει υψηλή ανωνυμία, καθόσον οι Χρήστες ταυτοποιούνται μέσω της διεύθυνσης IP τους.

Ο βαθύς ιστός (**Deep Web)** εμπεριέχει το σύνολο των περιεχομένων των Βάσεων Δεδομένων, καθώς και των διαδικτυακών υπηρεσιών, τα οποία είναι αδύνατο τεχνικά να ανευρεθούν από τις κλασσικές μηχανές αναζήτησης, π.χ. το περιεχόμενο των προσωπικών ηλεκτρονικών ταχυδρομείων (emails) δεν εμφανίζονται στις μηχανές αναζήτησης, το περιεχόμενο των λογαριασμών e-banking, οι ρυθμίσεις των προσωπικών λογαριασμών

(accounts) στα μέσα κοινωνικής δικτύωσης. Συνεπώς, πρακτικά σημαίνει ότι κάθε φορά που ένας Χρήστης εισέρχεται στο Διαδίκτυο, ενδεχομένως είναι πολύ πιθανό να εισέρχεται ακούσια ταυτοχρόνως και στο βαθύ Διαδίκτυο.

Ο σκοτεινός ιστός (**Dark Web) ονομάζεται επίσης και** Charter Web ή Darknet. Είναι ένα πολύ μικρό υποσύνολο του Deep Web. Είναι ένα **κρυπτογραφημένο, δύσκολα ανιχνεύσιμο δίκτυο,** στο οποίο ο Χρήστης δεν μπορεί να συνδεθεί με τις κλασσικές μηχανές περιήγησης (browsers) Η σύνδεση απαιτεί ειδικό λογισμικό π.χ. *το TOR (The Onion Router), το οποίο αναπτύχθηκε αρχικά από το Ερευνητικό Εργαστήριο του αμερικανικού Πολεμικού Ναυτικού, για την προστασία των στρατιωτικών επικοινωνιών*. Επίσης, η σύνδεση στο Dark Web απαιτεί ειδικές ρυθμίσεις, συγκεκριμένα διαπιστευτήρια, πρωτόκολλα και μηχανές αναζήτησης π.χ. το Grams, το οποίο χρησιμοποιείται για online ‘’μαύρες αγορές’’ και αγγελίες. Όπως είναι προφανές παρέχει ισχυρή ανωνυμία στους Χρήστες. [SOA.7]





Εικόνα 2-1
Παγόβουνο Διαδίκτυο (Surface-Deep-Dark Web)

Πηγή: https://pimages.toolbox.com/wp-content/uploads/2022/05/05041109/surface-web-vs-deep-web-vs-dark-web.png

Πηγή: https://i0.wp.com/helloitsliam.com/wp-content/uploads/2021/09/67b7a 083118_2347_surfacedeep1.png?w=616&ssl=1

- Το **μέγεθος** του Deep Web (περίπου 91.000 terabytes) είναι 400 έως 600 φορές μεγαλύτερο από αυτό του Surface Web (περίπου 167 terabytes).
- Μόνο το 4 % του διαδικτύου είναι προσβάσιμο από τις μηχανές αναζήτησης, ενώ το υπόλοιπο 96 % των περιεχομένων του διαδικτύου είναι προσβάσιμα μόνο με ειδικά εργαλεία και λογισμικό - browsers και άλλα πρωτόκολλα ή διαπιστευτήρια.

2.2 Διαφορές μεταξύ Βαθύ (Deep) και Σκοτεινό (Dark) Διαδίκτυο (Web)

Το βαθύ Διαδίκτυο δεν είναι προσβάσιμο από τις κλασσικές μηχανές αναζήτησης, π.χ. Google, το Bing και Yahoo. Τα περιεχόμενα του βαθύ ιστού είναι ιστοσελίδες, οι οποίες δεν έχουν ευρετηριαστεί από μηχανές αναζήτησης, ιστότοποι επί πληρωμή, ιδιωτικές βάσεις δεδομένων, κτλ. Κάθε μηχανή αναζήτησης χρησιμοποιεί διαδικτυακά ρομπότ (Internet bot), δηλαδή προγράμματα που εκτελούν αυτοματοποιημένες εργασίες μέσω του διαδικτύου, με σκοπό να ανιχνεύσουν τον ιστό και να προσθέσουν το νέο περιεχόμενο που βρίσκουν στο ευρετήριο της μηχανής αναζήτησης. Πολλοί ειδικοί εκτιμούν ότι οι μηχανές αναζήτησης ανιχνεύουν και ευρετηριάζουν λιγότερο από το 1% όλου του περιεχομένου, στο οποίο μπορεί να προσπελαστεί μέσω του Διαδικτύου. Το περιεχόμενο του ιστού με δυνατότητα αναζήτησης αναφέρεται ως επιφανειακός ιστός (surface web).

Μεγάλο μέρος του περιεχομένου του βαθύ ιστού είναι νόμιμο και μη εγκληματικής φύσης. Το περιεχόμενο του βαθύ ιστού περιλαμβάνει μηνύματα ηλεκτρονικού ταχυδρομείου, μηνύματα συνομιλίας, ιδιωτικό περιεχόμενο σε ιστότοπους κοινωνικής δικτύωσης, ηλεκτρονικές τραπεζικές συναλλαγές, ηλεκτρονικά αρχεία υγείας, κ.ά [SOA.8].

Οποιοσδήποτε ιστότοπος είναι επί πληρωμή π.χ. ειδησεογραφικά άρθρα, εκπαιδευτικό περιεχόμενο που απαιτεί συνδρομή είναι αποκλεισμένα από τα bots μηχανών αναζήτησης. Για το λόγο, το Deep Web παρουσιάζει το κρίσιμο πλεονέκτημα του ζητήματος του απορρήτου, καθώς οι μηχανές αναζήτησης δεν δύναται να εισχωρήσουν σε αυτόν.

Η βασική διαφορά μεταξύ του βαθύ και του σκοτεινού ιστού είναι το γεγονός ότι ο Χρήστης για να έχει πρόσβαση στο Βαθύ Ιστό (Deep Web) χρειάζεται κατάλληλα διαπιστευτήρια (credentials) και εξουσιοδότηση (authorization).

Αντιθέτως, το Dark Web απαιτεί ένα ειδικό λογισμικό/πρόγραμμα περιήγησης με κατάλληλο κλειδί αποκρυπτογράφησης για πρόσβαση σε αυτό. Το μέγεθος του Dark Web είναι της τάξεως του 0,01% του Deep Web και περιέχει περιεχόμενο του Διαδικτύου που δεν είναι δυνατό να αναζητηθεί με τις κλασσικές μηχανές αναζήτησης.

Σε αρκετές περιπτώσεις, το Deep Web και το Dark Web τελούν υπό σύγχυση στον δημόσιο διάλογο. Οι περισσότεροι άνθρωποι δεν γνωρίζουν ότι το Deep Web περιέχει ως επί το πλείστον μη αβλαβείς ιστότοπους, π.χ. λογαριασμοί email, οι οποίοι προστατεύονται με κωδικό πρόσβασης, συνδρομητικές υπηρεσίες επί πληρωμή Netflix, ιστότοποι, όπου είναι δυνατή η πρόσβαση μόνο μέσω μιας ηλεκτρονικής φόρμας, κτλ.

Συγκριτικά, ο Σκοτεινός Ιστός (Dark Web) είναι αρκετά μικρός, καθώς οι ιστότοποι του Dark Web αριθμούνται μόνο σε μερικές χιλιάδες. Η χρήση τους διεξάγεται μόνο με κρυπτογραφημένο λογισμικό, το οποίο βοηθά στο να παραμένουν οι Χρήστες και οι αντίστοιχες τοποθεσίες τους ανώνυμες. Εξ΄ ου και ο λόγος που η παράνομη δραστηριότητα είναι τόσο συνηθισμένη στο Dark Web. Οι Χρήστες δύναται να αποκρύψουν την ταυτότητά τους, οι ιδιοκτήτες παράνομων ιστοσελίδων να αποκρύψουν την τοποθεσία τους, ενώ τα δεδομένα που διαχειρίζονται να μεταφερθούν από τοποθεσία σε τοποθεσία ανώνυμα.

Εντούτοις, το Dark Web χρησιμοποιείται, επίσης, από δημοσιογράφους, πολιτικούς ακτιβιστές και πληροφοριοδότες (whistle blowers), οι οποίοι τελούν υπό καθεστώς λογοκρισίας ή κινδυνεύουν με πολιτικά αντίποινα από τις εκάστοτε κυβερνήσεις τους. Χαρακτηριστικό παράδειγμα είναι ο ιστότοπος WikiLeaks, ο οποίος έχει βαθιές ρίζες στο Dark Web. [SOA.9].

Αναφορικά με τις μηχανές αναζήτησης, ανακτούν αποτελέσματα κάνοντας χρήση κάποιων αλγορίθμων που κατατάσσουν τις ιστοσελίδες σε λίστες και λέγονται ανιχνευτές (crawlers). Ωστόσο, υπάρχουν κρυφοί πόροι στο Διαδίκτυο που δεν είναι ανιχνεύσιμοι από τους Web Crawlers και που σε γενικές γραμμές, κατατάσσονται στις παρακάτω κατηγορίες [SOA.10]:

- **Δυναμικό Περιεχόμενο:** αφορά δυναμικές σελίδες με μοναδικό τρόπο πρόσβασης την συμπλήρωση στοιχείων μέσω φορμών. Στην ίδια κατηγορία κατατάσσονται οι ιστοσελίδες που δημιουργούνται με ένα αναγνωριστικό περιόδου σύνδεσης ή ένα διακριτικό περιόδου λειτουργίας (session ids) για επικοινωνίες δικτύου μίας συνεδρίας.
- **Μη Συνδεδεμένο Περιεχόμενο:** αφορά σελίδες, οι οποίες δεν συνδέονται με άλλες σελίδες, με αποτέλεσμα οι web crawlers να μην μπορούν να ανιχνεύσουν σελίδες, μέσω άλλων σελίδων. Το internet παρέχει πρόσβαση με συνδέσμους (links) και ως εκ τούτου όταν ένας σύνδεσμος που παραπέμπει σε κάποια άλλη σελίδα ακολουθείται

από μια μηχανή αναζήτησης, τότε η τελευταία ανακαλύπτει την νέα σελίδα και την ταξινομεί.

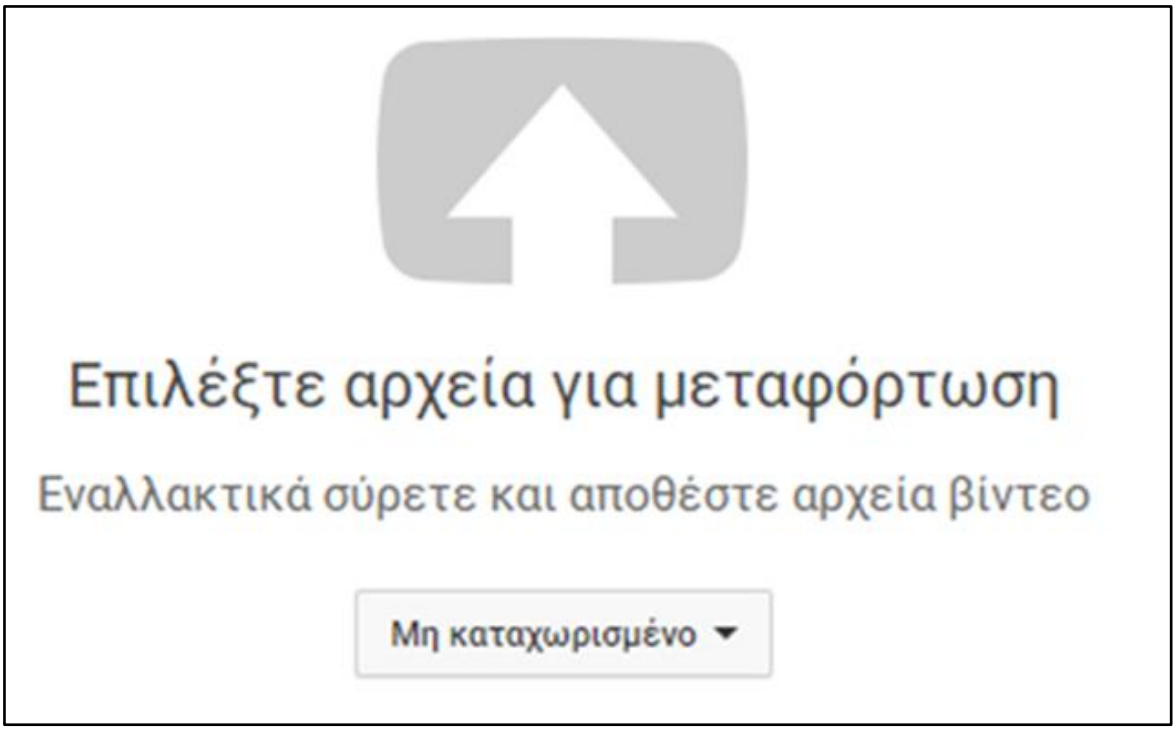
- **Private Web:** αφορά ιστοσελίδες που η πρόσβαση σε αυτές γίνεται με login, username και password.
- **Contextual Web:** αφορά ιστοσελίδες που το περιεχόμενο τους προσαρμόζεται ανάλογα με την ταυτότητα του Χρήστη. Για παράδειγμα, όταν η IP είναι από Ελλάδα ή ΗΠΑ, οι Χρήστες βλέπουν διαφορετικό περιεχόμενο.
- **Περιεχόμενο Περιορισμένης Πρόσβασης:** αφορά ιστοσελίδες που περιορίζουν, με τεχνικούς τρόπους, την πρόσβαση στο περιεχόμενό τους.
- **Scripted Content:** αφορά σελίδες στις οποίες η πρόσβαση γίνεται με συνδέσμους που παράγονται από JavaScript, καθώς και περιεχόμενο που κατεβαίνει από Web Servers μέσω Flash. Για το λόγο αυτό, το περιεχόμενο των Flash Sites είναι αόρατο από την Google.
- **Non-HTML/text content:** αφορά περιεχόμενο κειμένου που έχει δημιουργηθεί χωρίς τη χρήση HTML. Συχνά μπορεί να είναι κωδικοποιημένο σε αρχεία multimedia ή συγκεκριμένα formats (PDF, MS Office, κλπ) που δεν μπορούν να επεξεργαστούν οι μηχανές αναζήτησης.
- **Οτιδήποτε δεν ακολουθεί το πρότυπο HTTP/HTTPS:** δηλαδή μη προσπελάσιμα αρχεία από κάποια γλώσσα προγραμματισμού, π.χ. αρχεία που βρίσκονται σε διακομιστές FTP ή κείμενα που χρησιμοποιούν το παλαιότερο πρωτόκολλο Gopher.

Χαρακτηριστικό παράδειγμα Πρόσβασης στο Deep Web

Σελίδες στις οποίες η πρόσβαση γίνεται μόνο μέσω συνδέσμου

Τα Μη καταχωρισμένα βίντεο στο YouTube δεν είναι ορατά σε άλλους Χρήστες που επισκέπτονται την καρτέλα Βίντεο στη σελίδα ενός καναλιού και δεν πρέπει να εμφανίζονται στα αποτελέσματα αναζήτησης του YouTube, εκτός και αν κάποιος Χρήστης προσθέσει ένα Μη καταχωρισμένο βίντεο σε ένα Δημόσιο playlist.

Τα μη καταχωρισμένα βίντεο δεν μπορούν να εμφανιστούν ούτε στην αναζήτηση του YouTube, ούτε ως προτεινόμενα δίπλα σε άλλα βίντεο. Ωστόσο, μπορούν να είναι προσβάσιμα μόνο μέσω συνδέσμου ακόμα και από Χρήστες που δεν έχουν λογαριασμό στο YouTube, ενώ δεν είναι ορατά σε Χρήστες που δεν έχουν τον σύνδεσμο.

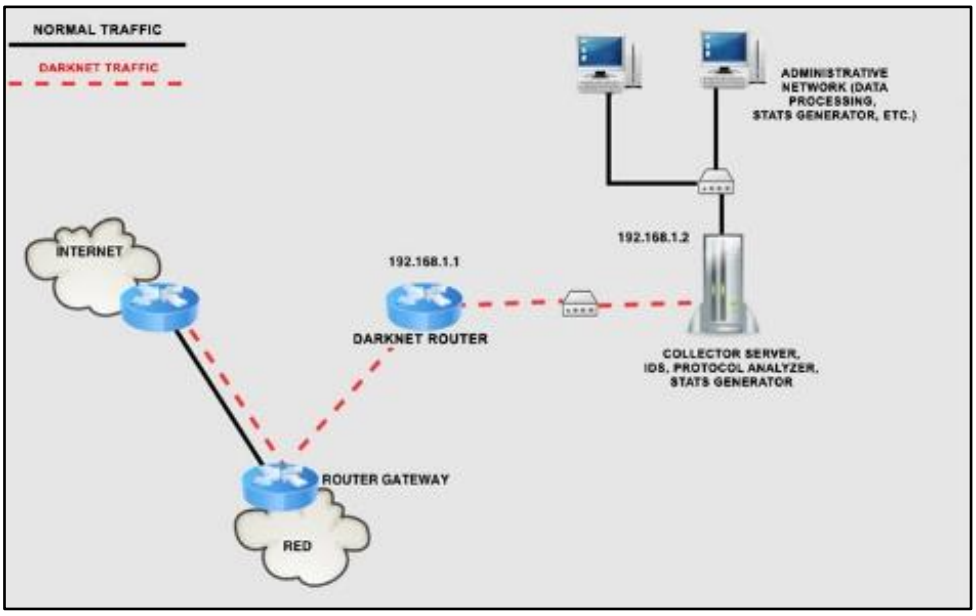


Εικόνα 2-2

Μη καταχωρισμένο βίντεο

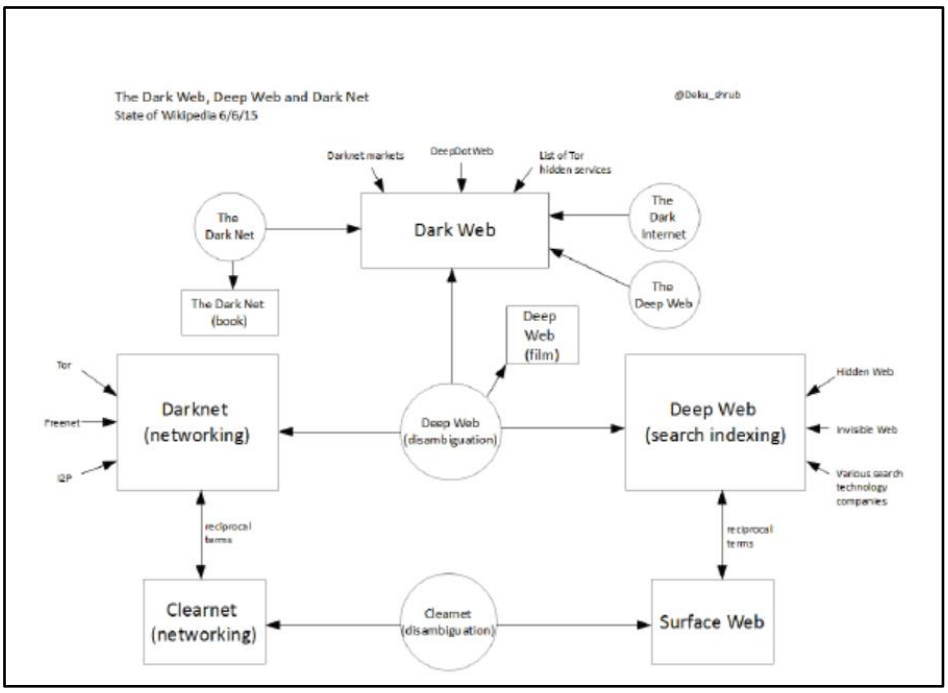
2.3 Τρόπος Λειτουργίας του Dark Web

Ο σκοτεινός ιστός λειτουργεί με το ίδιο πρωτόκολλο ελέγχου μετάδοσης και πρωτόκολλο Διαδικτύου (***Transmission Control Protocol/Internet Protocol (TCP/IP)***, καθώς και με το ίδιο πρωτόκολλο μεταφοράς αρχείων Hypertext Transfer Protocol Secure (HTTP) και File Transfer Protocol (FTP), εντός και μεταξύ δικτύων, μέσω του ίδιου τηλεφώνου, καλωδίου ή γραμμών FiOS που μεταφέρουν δεδομένα στο Διαδίκτυο.



Εικόνα 2-3

Πρωτόκολλα Επικοινωνίας Dark Web στο Διαδίκτυο



Εικόνα 2-4

Τρόπος Λειτουργίας του Dark Web στο Διαδίκτυο

2.4 Χρησιμότητα Dark Web για τους Χρήστες

Παρακάτω παρουσιάζονται τρείς βασικοί λόγοι για τους οποίους οι άνθρωποι μπορούν να χρησιμοποιούν το Dark Web [SOA.11]:

- **Ανωνυμία**

Οι άνθρωποι έχουν πολλούς λόγους για την προστασία της ταυτότητάς τους στο Διαδίκτυο, π.χ. σε χώρες όπου η κυβέρνηση απαγορεύει τον ελεύθερο τύπο ή όπου υπάρχει πολιτική λογοκρισία, σε περιπτώσεις που απαιτείται να μειωθεί ο κίνδυνος να πέσουν θύματα εγκληματικότητας, σε άλλες περιπτώσεις που άτομα έχουν δεχθεί κυβερνοπαρακολούθηση, για ασφάλεια ηλεκτρονικών τραπεζικών συναλλαγών τραπεζικής, κ.ά.

Σε ορισμένες περιπτώσεις σε χώρες με αυστηρό καθεστώς, αν μαθευτεί ότι κάποιος παρέχει πληροφορίες για φαινόμενα διαφθοράς δύναται να οδηγήσει κάποιον ακόμη και στη φυλακή, ενώ κινδυνεύει παράλληλα η σωματική ακεραιότητά του. Μέσω του Dark Web, όμως, μπορεί οποιοσδήποτε να παρέχει με ασφάλεια σε δημοσιογράφους, με τη μάσκα της ανωνυμίας πληροφορίες ευαίσθητου περιεχομένου. Επί πλέον, παράνομες οργανώσεις μπορούν να δίδουν σε μέλη τους εντολές, παράνομου περιεχομένου.

Το σκοτεινό Διαδίκτυο εξασφαλίζει την ελευθερία της έκφρασης σε ανθρώπους που θέλουν να αποκαλύψουν συνταρακτικά ντοκουμέντα, χωρίς τον φόβο πως θα διωχθούν ποινικά. Ενδεικτικά, στο Darknet έχουν κατά καιρούς φιλοξενηθεί αντίγραφα του Global Leaks και του Wikileaks [SOA.12].

Χρησιμοποιώντας το Dark Web η ταυτότητα του Χρήστη παραμένει κρυφή και ως εκ τούτου δεν δύναται να εντοπιστεί. Το γεγονός αυτό, ενδεχομένως, να εξιτάρει όσους εμπλέκονται σε παράνομες δραστηριότητες, π.χ. αγοραπωλησίες ναρκωτικών, όπλων και άλλων αντικειμένων. Επιπλέον, σε περιπτώσεις απαγορεύσεων πρόσβασης σε μέσα κοινωνικής δικτύωσης (*π.χ. λόγω κυβερνητικών μέτρων που αποσκοπούν στον κοινωνικό έλεγχο, κλπ*), το Dark Web είναι μια πρόσφορη λύση για ασφαλή πρόσβαση.

Το Strongbox είναι μια υπηρεσία στο σκοτεινό Διαδίκτυο που δημιουργήθηκε από το περιοδικό New Yorker, ώστε να παρέχει με εγγύηση ανωνυμίας σε όσους επικοινωνούν με τους συντάκτες του, με ασφάλεια μεγαλύτερη από αυτή των ηλεκτρονικών ταχυδρομείων [SOA.13].

- **Πρόσβαση σε "Κρυφές Υπηρεσίες"**

Χαρακτηριστικό παράδειγμα είναι η Υπηρεσία TOR Onion Service, με την οποία προστατεύεται με ανωνυμία όχι μόνο ο ίδιος ο Χρήστης αλλά και ο ίδιος ο ιστότοπος, που χρησιμοποιεί την υπηρεσία αυτή. Οι κρυφές υπηρεσίες ονομάζονται μερικές φορές "διευθύνσεις onion" επειδή το όνομα του ιστότοπου συχνά τελειώνει .onion. Η διεύθυνση IP του ιστότοπου δεν μπορεί να αναγνωριστεί, πράγμα που σημαίνει ότι οι πληροφορίες σχετικά με τον κεντρικό υπολογιστή, την τοποθεσία ή το περιεχόμενό του είναι κρυφές.

Το ίδιο το λογισμικό TOR δεν αποτελεί κρυφή υπηρεσία, αλλά οι ιστότοποι που φιλοξενεί είναι κρυφές υπηρεσίες, οι οποίες χρησιμοποιούνται για καταγγελίες ή και διακίνηση ευαίσθητων πληροφοριών, χωρίς κίνδυνο αντιποίνων.

Ωστόσο, είναι ευρέως γνωστό ότι η πλειοψηφία των κρυφών υπηρεσιών απαιτεί εγγραφή (*όνομα Χρήστη, κωδικός κ.λπ.*) και είναι προσβάσιμες μόνο κατόπιν πρόσκλησης από τους διαχειριστές ή μέσω αίτησης που γίνεται από το υποψήφιο μέλος και εγκρίνεται από τους διαχειριστές [SOA.14].

- **Παράνομη δραστηριότητα.**

Το Dark Web μπορεί να χρησιμοποιηθεί από άτομα που διεξάγουν παράνομες δραστηριότητες στο Διαδίκτυο, π.χ. πώληση όπλων ή ναρκωτικών. Οι ιστότοποι προσφέρουν τέτοιου είδους υπηρεσίες, οι οποίες ονομάζονται ‘’κρυφές’’ (*Hidden Services*).

Είναι προφανές ότι κίνδυνοι ελλοχεύουν είτε στο Σκοτεινό είτε και στο Επιφανειακό Διαδίκτυο. Οι άνθρωποι είναι εκτεθειμένοι εξίσου στην έκδηλη προβολή άσεμνων εικόνων και διαφημίσεων, ακόμη και πολύ σκληρών εικόνων π.χ. πορνογραφία, ναρκωτικά, όπλα, κ.ά.

Δεν είναι αμελητέο το γεγονός ότι ολοένα και οι νέοι εκτίθενται στον κίνδυνο να πέσουν θύματα εκμετάλλευσης και σεξουαλικής παραπλάνησης από επιτήδειους που χρησιμοποιούν το Διαδίκτυο προς αυτήν την κατεύθυνση.

Το Dark Web χρησιμοποιείται πιο συχνά για την πραγματοποίηση ελεύθερων σεξουαλικών συζητήσεων, καθώς και ανταλλαγής κατακριτέου σεξουαλικού υλικού που προσβάλλει την γενετήσιας αξιοπρέπειας. Είναι αρκετά δύσκολο, οι αρχές επιβολής του νόμου να εντοπίσουν με ευκολία τις έκνομες ενέργειες που λαμβάνουν χώρα στο σε ανώνυμες τοποθεσίες του Διαδικτύου.

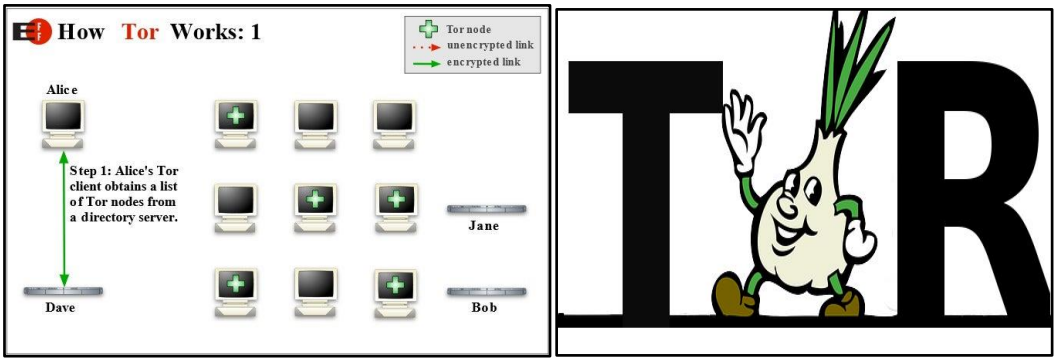
Χαρακτηριστικά Παραδείγματα Χρήσης του Dark Web

- Η οργάνωση “Δημοσιογράφοι Χωρίς Σύνορα” συμβούλευε τις υποψήφιες πηγές της να χρησιμοποιούν τον Σκοτεινό Ιστό, με σκοπό να διασφαλιστεί το απόρρητο της επικοινωνίας.
- Κατά τη διάρκεια της Αραβικής Άνοιξης, πλήθος ανθρώπων που συμμετείχαν στις εξεγέρσεις χρησιμοποίησε το Darknet για να μεταφέρει στο εξωτερικό μαρτυρίες και άλλες πληροφορίες.

2.5 Δρομολόγηση Onion Routing για Σύνδεση στο Dark Web

Ο πιο εύκολος και δημοφιλής τρόπος να συνδεθεί κανείς στο Dark Web είναι μέσω ενός ειδικού λογισμικού TOR (browser), το οποίο φέρει το λογότυπο του κρεμμυδιού. Το λογότυπο αυτό εξηγεί πως λειτουργεί ο μηχανισμός πρόσβασης σε δεδομένα. Τα δεδομένα αποκρυπτογραφούνται σε στρώσεις και μεταφέρονται σε τμήματα, με τρόπο παρόμοιο με αυτόν που ξεφλουδίζει κανείς ένα κρεμμύδι. Απαιτούνται πολλοί υπολογιστές για τη διαχείριση αυτών των δεδομένων, οι οποίοι έχουν εγκατεστημένο το συγκεκριμένο λογισμικό, και συνεπώς είναι αδύνατο να εντοπιστεί κάποιος Χρήστης.

Το όνομα του λογισμικού προέρχεται από τη φράση The Onion Routing (TOR). Το Tor είναι ένα κρυπτογραφημένο δίκτυο ανωνυμίας με διευθύνσεις που δεν έχουν συνηθισμένη κατάληξη π.χ. com, gr, org αλλά η κατάληξη της διεύθυνσης είναι onion. Οι περισσότερες διευθύνσεις δεν έχουν καμία λεκτική συνοχή και είναι και αρκετά μακροσκελείς που καθιστά δύσκολη την απομνημόνευση τους. Όπως θα εξηγηθεί αναλυτικά στα επόμενα, η σελίδα προορισμού ενός Χρήστη διέρχεται μέσα από ενδιάμεσους κόμβους (relays) ενός δικτύου και εξέρχεται από κόμβους εξόδου (exit nodes), σε αντίθεση με τους **Proxy Servers**, οι κόμβοι εξόδου δεν γνωρίζουν τη διεύθυνση IP και την τοποθεσία ενός Χρήστη.



Εικόνα 2-5 Λογότυπο Λογισμικού TOR

Πηγή: https://images.idgesg.net/images/article/2018/07/how_tor_works_1-100763523-orig.jpg?auto=webp&quality=85,70

Το Onion Routing είναι μια τεχνική για ανώνυμη επικοινωνία μέσω ενός δικτύου υπολογιστών. Σε ένα δίκτυο onion, τα μηνύματα ενσωματώνονται σε στρώματα κρυπτογράφησης, που παρέχονται από το TOR.

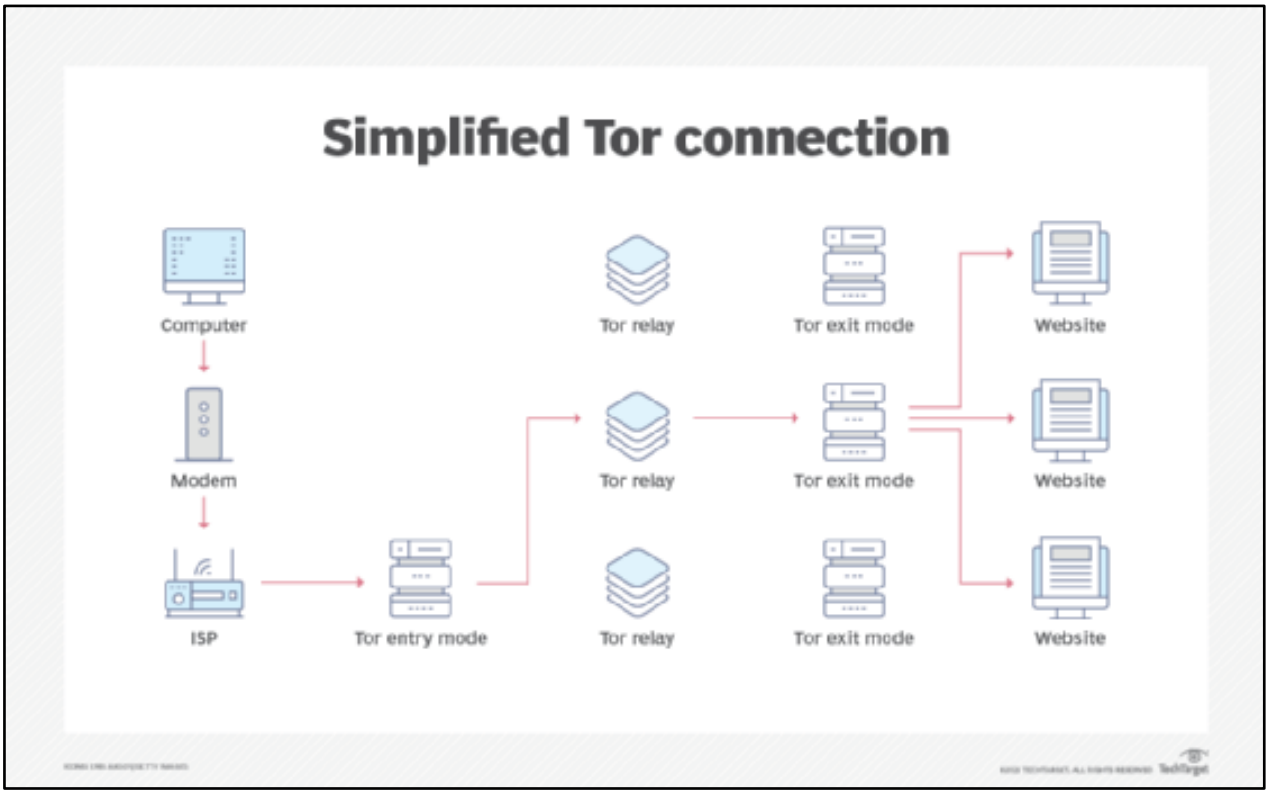
Στις αποστολές μηνυμάτων μέσω του HTTP, υπάρχει δυνατότητα κάποιος κακόβουλος εισβολές να εισχωρήσει, πλην όμως δεν έχει τη δυνατότητα να δει το περιεχόμενο αυτών επειδή είναι κρυπτογραφημένο. Με το Onion Routing διεξάγονται αιτήματα ανταλλαγής μηνυμάτων και δίδεται ένα επίπεδο ασφάλειας υψηλότερο, καθώς αποκλείει το ενδεχόμενο ο κακόβουλος επιβουλέας να υποκλέψει με ποιον διακομιστεί επικοινωνεί ο Χρήστης. Το Onion Routing προστατεύει από την ανάλυση κίνησης (traffic analysis), τις υποκλοπές, καθώς και από άλλες επιθέσεις π.χ. δρομολογητές Διαδικτύου, Hackers, κτλ.

Η δρομολόγηση Onion Routing χαρακτηρίζεται από την μεταπήδηση της σύνδεσης από έναν διακομιστή σε άλλον (από κόμβο σε κόμβο), μέχρι η μεταπήδηση να καταλήξει στον τελευταίο επιθυμητό διακομιστή, ο οποίος θα επεξεργαστεί το αίτημα ενός Χρήστη για είσοδο σε μία ιστοσελίδα και θα στείλει απάντηση προς τον Χρήστη χρησιμοποιώντας την ίδια διαδρομή κόμβων δικτύου. Τα μηνύματα που αποστέλλονται και λαμβάνονται είναι κρυπτογραφημένα με διαφορετικά κλειδιά. Σε κάθε κόμβο (αναπήδηση, διακομιστή) υπάρχει ένα μοναδικό κλειδί κρυπτογράφησης. Ο πελάτης έχει πρόσβαση σε όλα τα κλειδιά, πλην όμως οι διαχειριστές των εκάστοτε διακομιστών (Servers) έχουν πρόσβαση μόνο στα κλειδιά που αφορούν την κρυπτογράφηση και αποκρυπτογράφηση στον διακομιστή τους.

Η όλη διαδικασία στηρίζεται στη φιλοσοφία του Κρεμμυδιού (Onion), δηλαδή το κάθε μήνυμα Χρήστη τυλίγεται με στρώματα κρυπτογράφησης, τα οποία αποφλοιώνονται σε κάθε διαφορετική αναπήδηση από κόμβο σε κόμβο [SOA.15].

Παράδειγμα Χρήσης Onion Routing

Ένα ένας Χρήστης επιθυμεί να αποκτήσει πρόσβαση στο YouTube στην Κίνα, όπου η χρήση είναι απαγορευμένη, τότε η λύση είναι το λογισμικό TOR, μέσω των δρομολογητών TOR Onion Routers. Συνεπώς, ο υπολογιστής του Χρήστη, προκειμένου να συνδεθεί με τον διακομιστή της αρχικής σελίδας YouTube, χρησιμοποιεί 3 άλλους ενδιάμεσους κόμβους/διακομιστές/δρομολογητές του δικτύου TOR Onion Routers πριν από τον επιθυμητό διακομιστή, ώστε να μην γίνει αντιληπτή η διασύνδεση με τον διακομιστή του YouTube στην Κίνα.



Εικόνα 2-6 Απλοποίηση Τρόπου Λειτουργίας του Dark Web στο Διαδίκτυο

Πηγή: https://cdn.ttgtmedia.com/rms/onlineimages/whatis-simplified_tor_connection-f.png

2.5.1 Κατανόηση Τρόπου Λειτουργίας Δρομολόγησης Onion Routing για Σύνδεση στο Dark Web

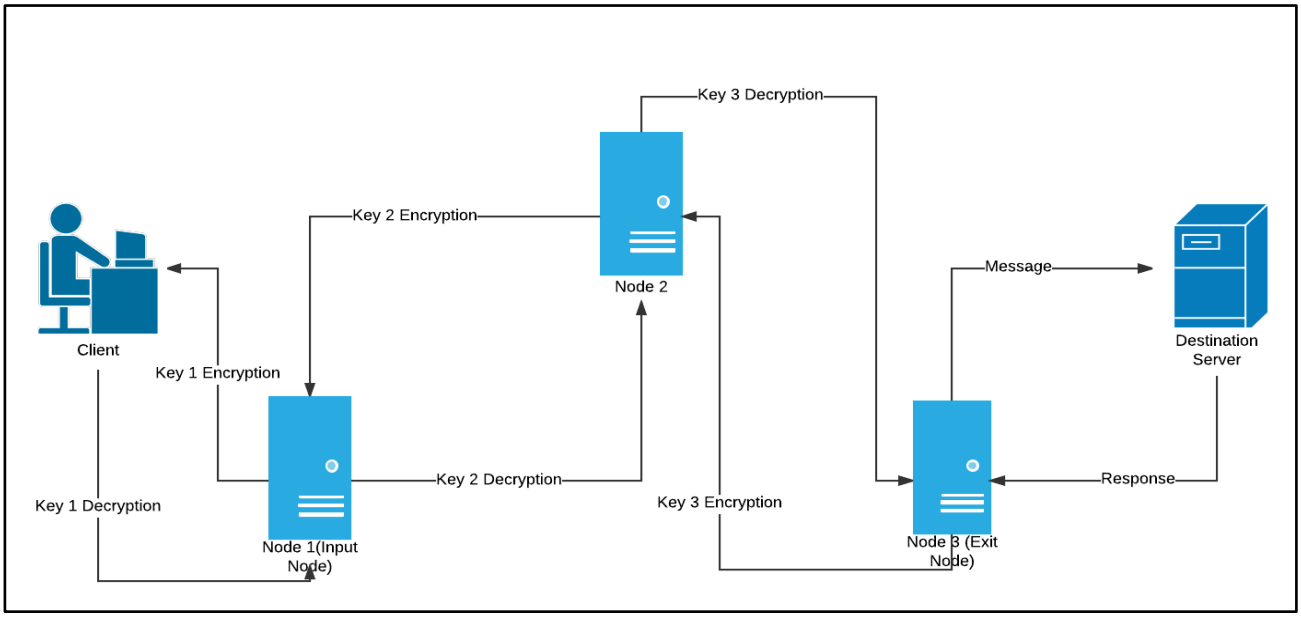
1. Ο πελάτης με πρόσβαση σε όλα τα κλειδιά κρυπτογράφησης, π.χ. κλειδί 1, 2 και 3 κρυπτογραφεί το αίτημα μηνύματος, ‘’τυλίγοντας’’ αυτό με 3 στρώσεις σαν κρεμμύδι, οι οποίες θα πρέπει να αποφλοιώνονται μία-μία κάθε φορά.
2. Εν συνεχεία, το κρυπτογραφημένο μήνυμα, τριών στρώσεων, αποστέλλεται στον πρώτο διακομιστή, π.χ. στον Κόμβο 1 (**Input Node**).
3. Ο **Κόμβος 1** διαθέτει μόνο τη διεύθυνση του Κόμβου 2 και το κλειδί 1, με σκοπό να αποκρυπτογραφήσει το μήνυμα, μέχρι το πρώτο στρώμα κρυπτογράφησης και εν συνεχεία το αποστέλλει στον Κόμβο 2.
4. Ο **Κόμβος 2** διαθέτει μόνο το κλειδί 2 και τις διευθύνσεις των Κόμβων εισόδου και εξόδου. Αποκρυπτογραφεί το μήνυμα χρησιμοποιώντας το Κλειδί 2 μόνο για το δεύτερο στρώμα κρυπτογράφησης και εν συνεχεία το αποστέλλει στον κόμβο 3, δηλαδή στον κόμβο εξόδου (**Exit node).**

5. Ο **Κόμβος 3** (κόμβος εξόδου) αποκρυπτογραφεί το μήνυμα στο τρίτο στρώμα κρυπτογράφησης και ανευρίσκει ένα αίτημα GET Request για σύνδεση με το youtube.com και ως εκ τούτου διαβιβάζει το εν λόγω αίτημα στον διακομιστή προορισμού (server destination).

6. Ο διακομιστής προορισμού επεξεργάζεται το αίτημα για πρόσβαση στην επιθυμητή ιστοσελίδα ως απάντηση (απόκριση).

7. Η απόκριση (response) διαγραφεί αντίστροφη πορεία κατεύθυνσης, περνώντας μέσα από τους ίδιους κόμβους (Nodes 1,2,3), οι οποίοι προβαίνουν σε κρυπτογράφηση ο καθένας με το δικό του κλειδί (Key 1,2,3).

8. Εν τέλη, στον πελάτη αφικνούνται μία μορφή απόκρισης, τριπλής κρυπτογράφησης, η οποία μπορεί να αποκρυπτογραφηθεί, καθώς ο πελάτης έχει πρόσβαση σε όλα τα προαναφερθέντα κλειδιά.



Εικόνα 2-7 Κρυπτογράφηση και Αποκρυπτογράφηση TOR στο Dark Web

Πηγή: https://media.geeksforgeeks.org/wp-content/uploads/Onion-Routing-Page-1.png

Αξίζει να σημειωθεί ότι η περιήγηση σε ένα δίκτυο TOR παρουσιάζει μειωμένη ταχύτητα (delay) σε σχέση με τα κλασσικά δίκτυα, λόγω της μεταπήδησης από κόμβο σε κόμβο. Ως βασικό μειονέκτημα εστιάζεται το γεγονός ότι στην περίπτωση που η ιστοσελίδα προορισμού δεν υιοθετεί το πρωτόκολλο HTTPS, ώστε να είναι κρυπτογραφημένο και το τελευταίο κομμάτι του μηνύματος (πληροφορίας) ανάμεσα στο κόμβο εξόδου (exit node) και στην ιστοσελίδα προορισμού, τότε ο κόμβος προορισμού δύναται να παρακολουθήσει οποιαδήποτε κίνηση (traffic analysis) διέρχεται από αυτόν. Επιπλέον, για να θεωρηθεί ένας

υπολογιστής ως κόμβος εξόδου θα πρέπει ο κάτοχός του να παραχωρήσει την σχετική άδεια η διεύθυνση IP που θα εμφανίζεται στην τελική σελίδα επιθυμίας του Χρήστη, να είναι εκείνη του κόμβου εξόδου. Αυτό το γεγονός καθιστά τον κάτοχο του εν λόγω κόμβου νομικά υπεύθυνο, στην περίπτωση που λάβει χώρα οποιαδήποτε παράνομη ή αξιόποινη από τον υπολογιστή αυτόν.

2.5.2 Παροχή Ανωνυμίας μέσω της TOR Κρυπτογράφησης και Αποκρυπτογράφησης στο Dark Web

Αν κάποιος Ιχνηλάτης Δικτύου (Sniffer) δύναται να παρακολουθεί τον Κόμβο 1, δηλαδή στην πρώτη φάση της σύνδεσης πελάτη – κόμβου εισόδου, το μόνο που μπορεί να γνωρίζει είναι τη διεύθυνση του κόμβου εισόδου και την ύπαρξη ενός κρυπτογραφημένου, τριών επιπέδων, μηνύματος. Συνεπώς, ο Sniffer γνωρίζει ότι ο Χρήστης περιηγείται (browsing) σε δίκτυο TOR.

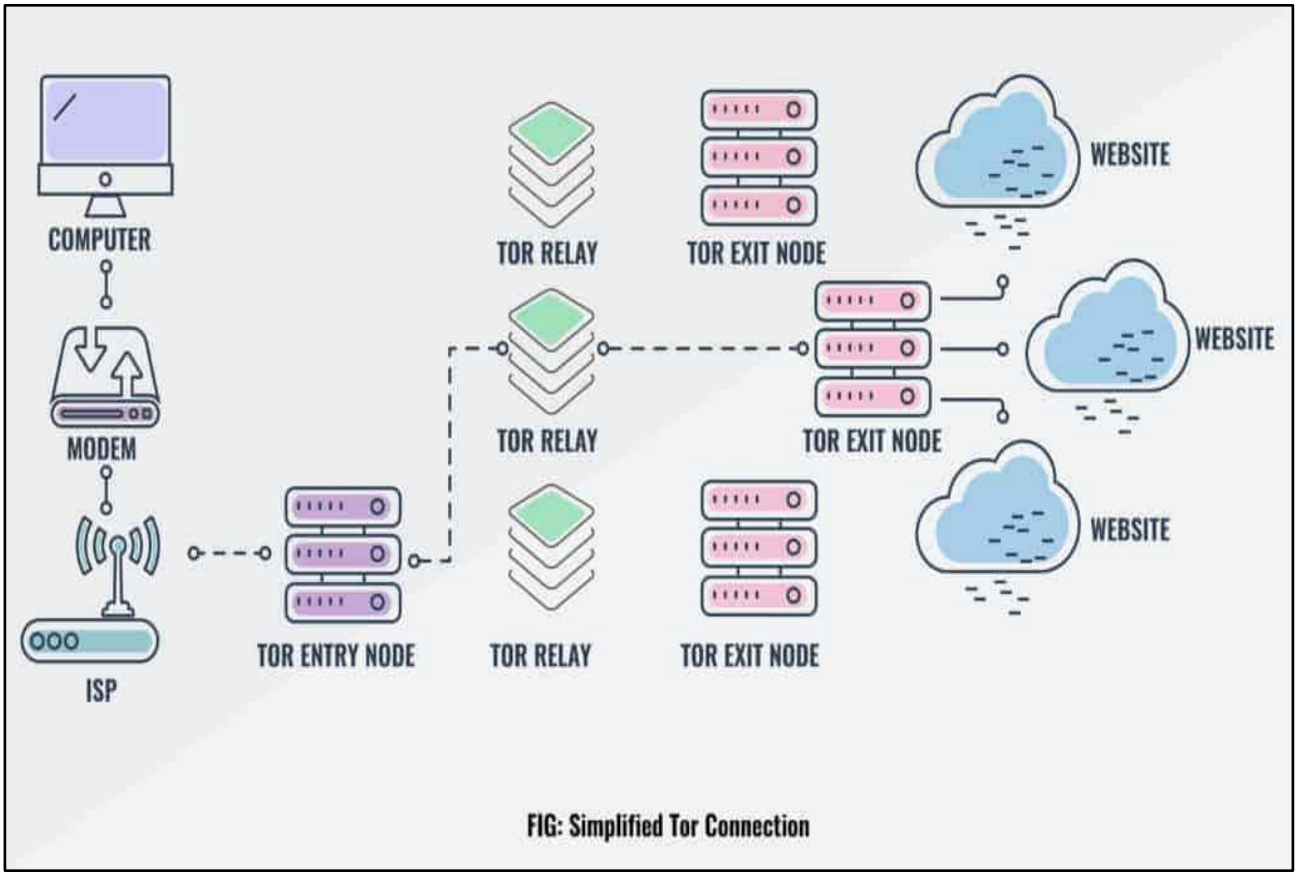
Ο Sniffer δεν μπορεί ούτε να παρακολουθήσει τον Κόμβο 2 ώστε να γνωρίζει τη διεύθυνση εισόδου και τη εξόδου, καθώς και ούτε να εντοπίσει τον πελάτη και διακομιστή προορισμού, διότι καθένας από αυτούς τους κόμβους έχει εκατοντάδες ταυτόχρονες συνδέσεις σε εξέλιξη, εν συνεπεία είναι πρακτικά πολύ δύσκολο έως ακατόρθωτο να γνωρίζει κανείς ποιος κόμβος οδηγεί στη σωστή πηγή και στον σωστό προορισμό.

Αν τέλος, ο Sniffer ιχνηλατεί τον κόμβο εξόδου, τότε το μόνο που παρατηρεί είναι το γεγονός ότι ένας διακομιστής επικοινωνεί με έναν άλλο διακομιστή, πλην όμως δεν δύναται να παρακολουθήσει τον Χρήστη πελάτη ή ακόμη και την πηγή που δημιούργησε το αίτημα.

Συμπερασματικά, το TOR αποτελεί ένα πολύ ισχυρό εργαλείο ανωνυμίας που υπόσχεται να καταστεί μία νέα επαναστατική μορφή διαδικτυακής ιδιωτικότητας. Ουδείς δύναται να καταλάβει ποιος φιλοξενεί μία διεύθυνση σκοτεινού ιστότοπου, ενώ όποιος την γνωρίζει δύναται να την επισκεφτεί ανώνυμα. Με αποτέλεσμα, μελλοντικά οποιοσδήποτε θα δύναται να δημιουργήσει την δική του ανώνυμη, μη ανιχνεύσιμη και σχεδόν αθέατη χωρίς πρόσκληση “γωνιά” στο Internet. Είναι ευρέως γνωστό ότι οι περισσότερες τοποθεσίες (διαδικτυακές διευθύνσεις) σκοτεινού διαδικτύου κοινοποιούνται δημόσια στο επιφανειακό Διαδίκτυο, ενώ η κοινοποίηση φθάνει μέχρι και τα Μέσα Κοινωνικής Δικτύωσης - Ενημέρωσης.

2.5.3 Συνδυασμός Χρήσης VPN και TOR

Όπως έχει ήδη περιγραφεί, η πρόσβαση στον Σκοτεινό Ιστό με χρήση λογισμικού TOR υλοποιείται με ένα δίκτυο στρωμάτων μετάδοσης, μέσω του οποίου δρομολογείται η σύνδεση του Χρήστη στο Διαδίκτυο. Η σύνδεση είναι κρυπτογραφημένη και όλη η κίνηση κυκλοφορίας αναπηδά μεταξύ στρωμάτων που βρίσκονται σε όλο τον κόσμο, προσδίδοντας έτσι τη δυνατότητα ανωνυμίας στον Χρήστη. Παρόλα αυτά, οι πάροχοι διαδικτύου δύναται να ανιχνεύσουν εάν ένας χρήστης χρησιμοποιεί δίκτυο TOR, διότι οι IP των κόμβων του εν λόγω δικτύων είναι δημόσιοι, χωρίς όμως να δύναται να αποκρυπτογραφήσουν το περιεχόμενο της κίνησης.



Εικόνα 2-8 Απλοποιημένο Δίκτυο TOR

Πηγή: https://cdn.comparitech.com/wp-content/uploads/2019/01/tor-diagram.jpg

Η VPN σύνδεση επιτρέπει σε έναν Χρήστη να κρυπτογραφεί όλη την κίνηση στο Διαδίκτυο, από και προς την συσκευή του και να τη δρομολογεί, μέσω ενός διακομιστή, σε μια τοποθεσία της επιλογής του. Συνεπώς, η κοινή χρήση των εργαλείων VPN με TOR προσδίδει περαιτέρω ασφάλεια στον Χρήστη. Στα επόμενα θα εξεταστούν οι περιπτώσεις σύνδεσης **VPN over TOR ή TOR over VPN:**

- Η πιο συνήθης μέθοδος είναι η σύνδεση με VPN σε πρώτη φάση και σε δεύτερη φάση η ενεργοποίηση ενός προγράμματος περιήγησης TOR (**VPN over TOR**). Συνεπώς, όλη η κίνηση κυκλοφορίας πηγαίνει πρώτα στον διακομιστή VPN και εν συνεχεία μεταπηδά, μέσω του δικτύου TOR, μέχρι να καταλήξει στον τελικό προορισμό της. Ο πάροχος του Διαδικτύου βλέπει μόνο την κρυπτογραφημένη κίνηση VPN, χωρίς να γνωρίζει ότι ο Χρήστης κάνει χρήση ενός TOR δικτύου, σε ιστότοπους .onion.Το VPN over TOR απαιτεί να υπάρχει υψηλό επίπεδο εμπιστευτικότητας από τον από τον Πάροχο Διαδικτύου και όχι κατ΄ ανάγκη από τον πάροχο VPN.

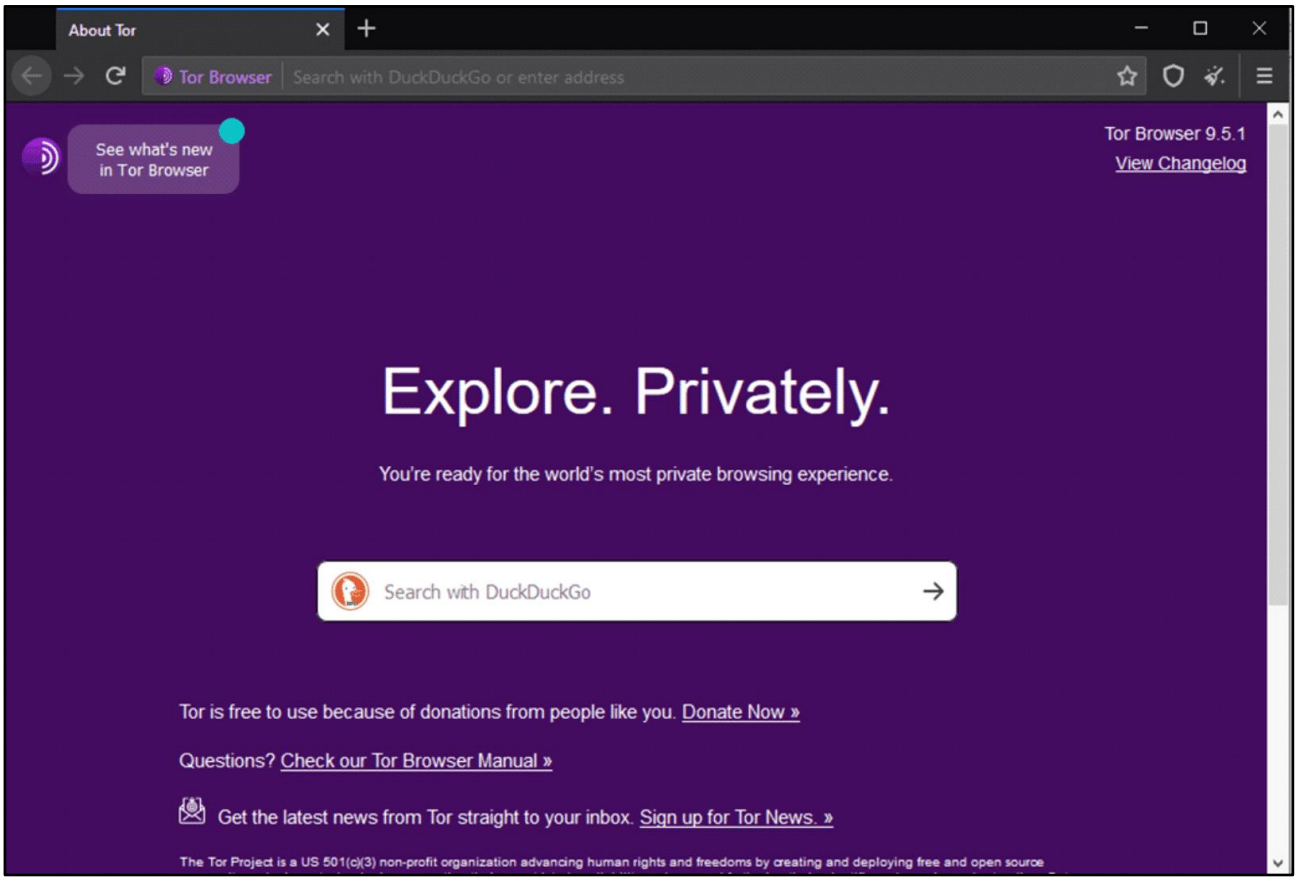
  Ορισμένοι θεωρούν το VPN over TOR πιο ασφαλές επειδή διατηρεί την ανωνυμία σε όλη τη διαδικασία σύνδεσης (με την υπόθεση ότι η VPN σύνδεση έχει συνδρομή και και παρέχει ανωνυμία).

- Υπάρχει και ο αντίστροφος τρόπος σύνδεσης (**TOR over VPN**), δηλαδή της χρήσης ενός δικτύου TOR πάνω σε μία σύνδεση VPN. Σε αυτή την περίπτωση, ο πάροχος VPN δύναται να καταλάβει ότι ο Χρήστης χρησιμοποιεί TOR δίκτυο, διατηρώντας αρχεία καταγραφής μεταδεδομένων, ανάλυσης κίνησης (**traffic logs**) ή και περιόδων σύνδεσης (**session logs**), χωρίς ωστόσο να έχει πρόσβαση στο κρυπτογραφημένο περιεχόμενο της TOR σύνδεσης.

  Η μέθοδος σύνδεσης TOR over VPN δεν μπορεί να προστατεύσει τους Χρήστες από κακόβουλους κόμβους εξόδου (malicious Tor exit nodes), διότι οι TOR κόμβοι εξόδου έχουν φιαχθεί από εθελοντές Χρήστης, χωρίς πάντοτε να τηρούνται οι στοιχειώδες κανόνες ασφάλειας δικτύων. Στον κόμβο εξόδου, όπου αποκρυπτογραφείται η κίνηση δικτύου ενός Χρήστη, αποτελεί και το σημείο όπου μπορεί να υλοποιηθεί η υποκλοπή των δεδομένων, μέσω κακόβουλου κώδικα. Για αυτό το λόγο, υπάρχουν ιστότοποι που αποκλείουν κόμβους εξόδου TOR, διότι δεν έχουν υψηλό επίπεδο εμπιστοσύνης.

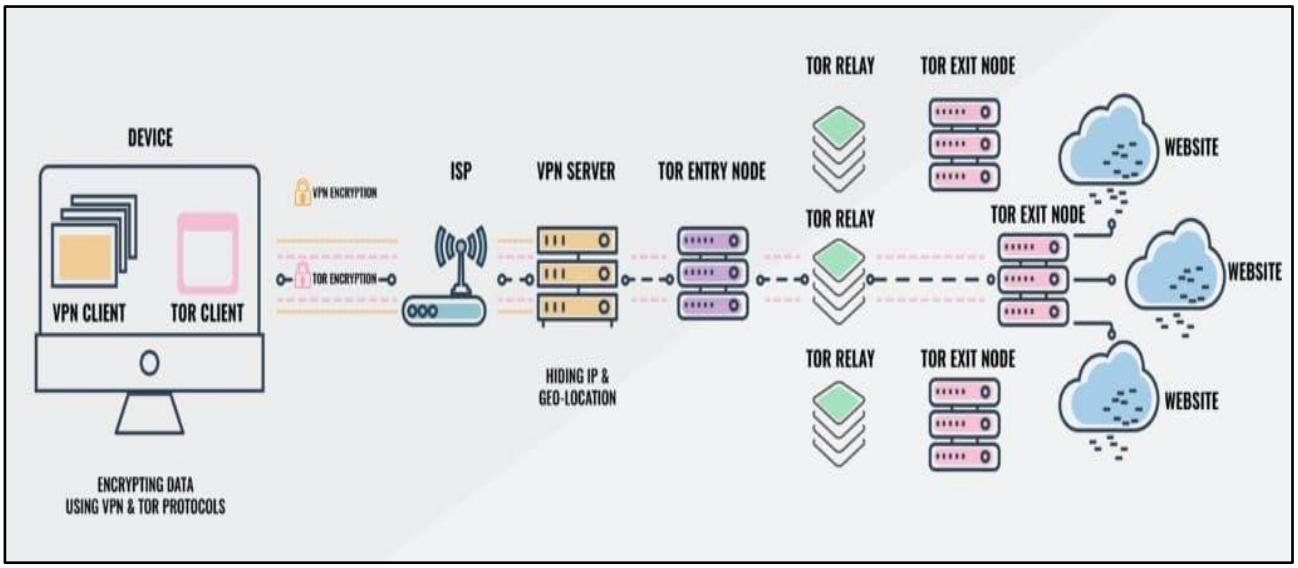
  Το Tor over VPN απαιτεί να υπάρχει υψηλό επίπεδο εμπιστευτικότητας από τον πάροχο VPN και όχι κατ΄ ανάγκη από τον Πάροχο Διαδικτύου.

Υπάρχουν και εξειδικευμένα λογισμικά που έχουν ενσωματωμένη τη δυνατότητα χρήσης VPN και TOP π.χ. το NordVPN, IPVanish, AirVPN, BolehVPN κτλ.



Εικόνα 2-9 Περιηγητής TOR

Πηγή: https://www.cryptopal.com/wp-content/uploads/2020/07/Tor-Explore-Privately.png.webp



Εικόνα 2-10 VPN σύνδεση και TOR Περιήγηση

Πηγή: https://cdn.comparitech.com/wp-content/uploads/2019/01/VPN-THEN-TOR.jpg

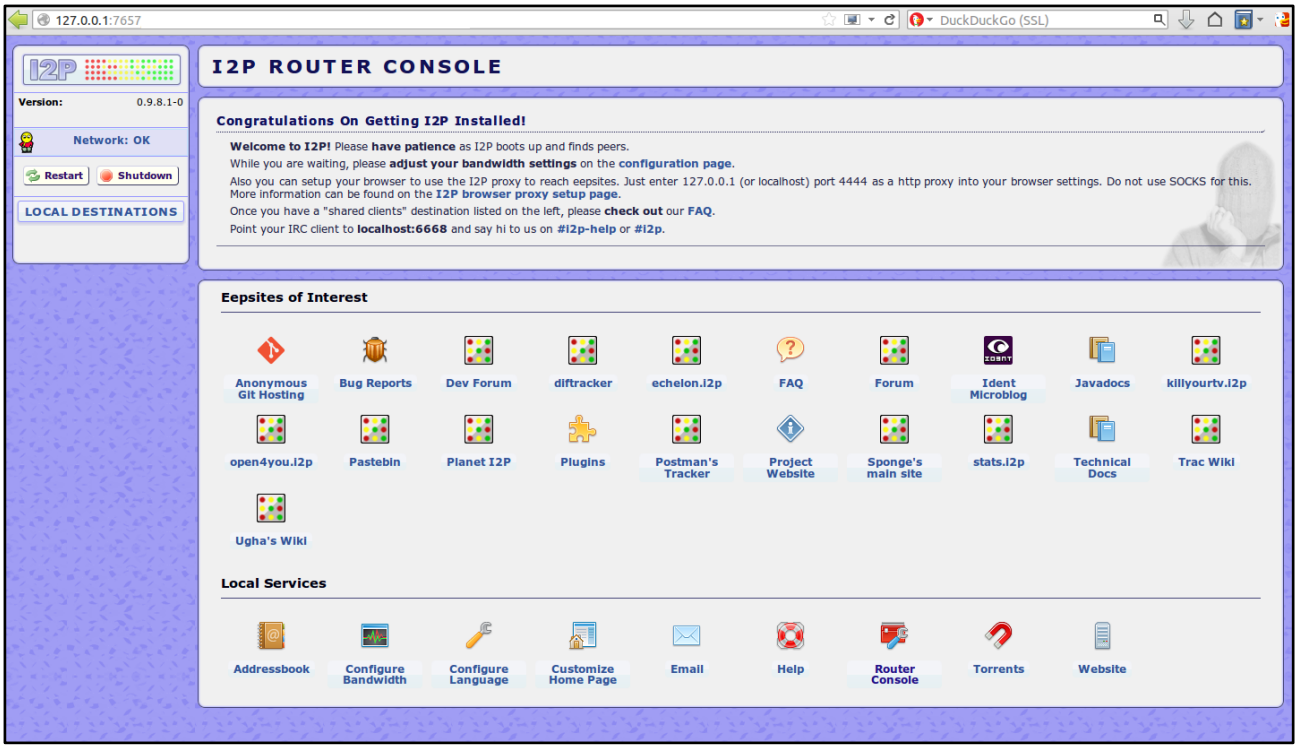
2.6 Εναλλακτικοί Τρόποι Σύνδεσης στο Dark Web

Το **Invisible Internet Project (I2P)** είναι ένα ανώνυμο δίκτυο με έμφαση την παρεμπόδιση της παρακολούθησης της πορείας των επικοινωνιών από τρίτους. Επιτρέπει την αποστολή μηνυμάτων με τη χρήση ψευδώνυμων μεταξύ χρηστών που είναι ανθεκτικές στη λογοκρισία, μέσω δημιουργίας ανώνυμων συνδέσεων κατόπιν κρυπτογράφησης της κίνησης δεδομένων του Χρήστη και τη διανομή τους σε δίκτυο περίπου 55000 υπολογιστών σε όλη την υφήλιο. Δεδομένου του μεγάλου αριθμού των πιθανών διαδρομών που μπορεί να ακολουθήσουν τα δεδομένα, είναι εξαιρετικά απίθανο ένα τρίτος να παρακολουθήσει την επικοινωνία στο σύνολό της.

Σε αντίθεση με το Tor, το I2P έχει ως κύριο στόχο να αποκρύψει την ταυτότητα τόσο των αποστολέων, όσο και των παραληπτών της δικτυακής κίνησης και όχι μόνο του αποστολέα. Το I2P λειτουργεί στο Στρώμα Δικτύου, διαχωρίζοντας την ταυτότητα του εκάστοτε Χρήστη από τη γεωγραφική του θέση (δηλαδή την IP Address του).

Το I2P για να επιτύχει την ανωνυμία των χρηστών του χρησιμοποιεί τεχνικές που βασίζονται στη **διαδικασία** δρομολόγησης σκόρδου (**Garlic Routing)**, αντίστοιχη με αυτή της δρομολόγησης κρεμμυδιού (Onion Routing) που χρησιμοποιεί το TOR. Το **Garlic Routing** κρυπτογραφεί πολλαπλά μηνύματα μαζί ώστε να δυσκολέψει τους εισβολείς να πραγματοποιήσουν ανάλυση κυκλοφορίας και να αυξήσουν την ταχύτητα μεταφοράς δεδομένων [SOA.16].

Αποτελεί ένα πλήρως κατανεμημένο και αυτόνομο P2P σύστημα που δεν βασίζεται σε καταλόγους και ευρετήρια που παρέχουν οι Directory Servers. Όπως και το Onion Routing, χρησιμοποιεί διαστρωματωμένη κρυπτογράφηση στα προς διακίνηση onion cells, τα οποία ομαδοποιεί, ενισχύει με padding (dummy messages), δημιουργώντας τα garlic cloves. Χρησιμοποιούνται διάφορα σχήματα κρυπτογράφησης, ενώ οι κόμβοι έχουν τη δυνατότητα να δεχθούν delay/no delay εντολές, αναλόγως των δικτυακών εφαρμογών προς τις οποίες απευθύνεται η δικτυακή κίνηση και τις απαιτήσεις σε low latency.



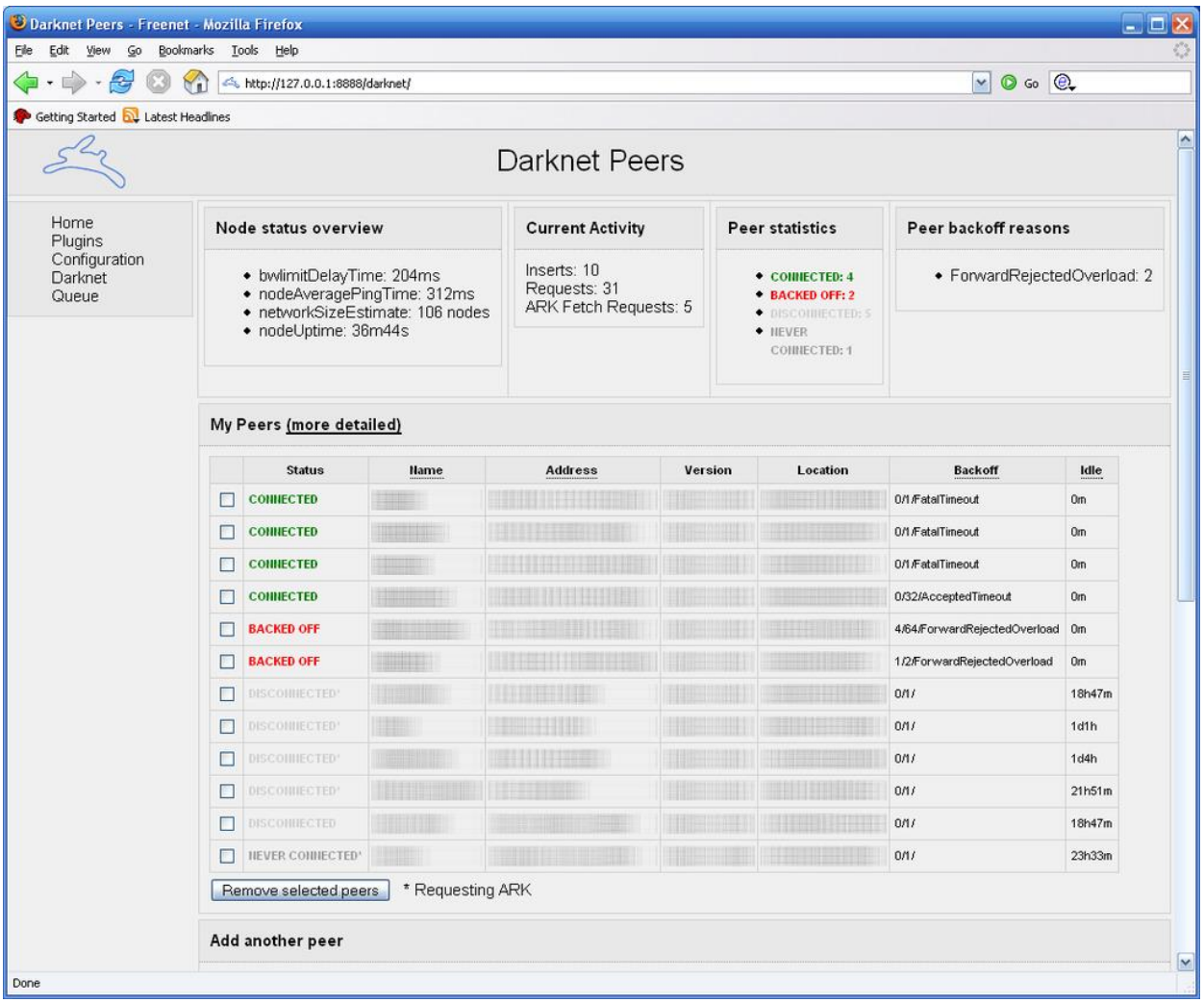
Εικόνα 2-11 I2P Garlic Routing

Πηγή: https://i.iinfo.cz/images/561/i2p-konzole-1.png

Ένας άλλος τρόπος σύνδεσης στο Dark Web είναι το αυτόνομο δίκτυο, μέσω του ελεύθερου λογισμικού **Freenet**, που καθιστά εφικτή τον ανώνυμο διαμοιρασμό αρχείων, την ελεύθερη περιήγηση, την συζήτηση σε φόρουμ, χωρίς την απειλή της λογοκρισίας, κτλ. Οι Χρήστες του συγκεκριμένου λογισμικού συμμετέχουν στο δίκτυο διαθέτοντας την σύνδεσή τους, καθώς και ένα τμήμα του σκληρού δίσκου τους στο οποίο αποθηκεύονται αρχεία. Τα δεδομένα που διακινούνται στο δίκτυο Freenet κρυπτογραφούνται και μεταφέρονται μέσω πολλαπλών κόμβων, γεγονός που καθιστά δυσκολότερο τον προσδιορισμό του περιεχομένου και του τελικού παραλήπτη τους.

Εξαιτίας της κρυπτογράφησης, ο εκάστοτε Χρήστης δεν δύναται να γνωρίζει εκ των προτέρων τι υπάρχει αποθηκευμένο στον δεσμευμένο χώρο του δίσκου του, χωρίς βέβαια να θεωρείται υπεύθυνος για το είδος και το περιεχόμενο των αρχείων που φιλοξενεί στο συγκεκριμένο τμήμα του υπολογιστή του. Συνεπάγεται από τα προαναφερθέντα ότι η χρήση του Freenet σημαίνει αποδοχή από τον Χρήστη η δέσμευση του χώρου του σκληρού του δίσκου.

Ο Χρήστης που κάνει χρήση του δικτύου Freenet δεν δύναται να συνδεθεί σε υπηρεσίες π.χ. του Facebook, διότι δεν είναι διακομιστής μεσολάβησης. Το Freenet αποτελεί ένα χώρο αποθήκευσης που κατανέμεται μεταξύ υπολογιστών, και οι πληροφορίες που ανεβαίνουν σε αυτό παραμένουν ανώνυμες και ασφαλείς.



Εικόνα 2-12 FreeNet Dark Web

Πηγή: https://upload.wikimedia.org/wikipedia/commons/thumb/b/b5/Freenet_darknet.png/1024px-Freenet_darknet.png

Η σελίδα αυτή σκόπιμα κενή

ΚΕΦΑΛΑΙΟ 3ο:
Εγκαθίδρυση μιας Καλοστημένης Επιχειρηματικής Μηχανής στο Σκοτεινό Διαδίκτυο (Dark Web)

3.0 Το Επιχειρηματικό Μοντέλο (Business Model Canvas) του Σκοτεινού Ιστού (Dark Web)

Στη σύγχρονη εποχή, η καινοτομία δεν εγγυάται την επιτυχία στην αγορά, δεδομένης της εμφάνισης νέων τεχνολογιών, αλλαγών στις προτιμήσεις των καταναλωτών και της δημιουργίας νέων κοινωνικών τάσεων. Οι μεταβαλλόμενες συνθήκες επιβάλλουν μια ολοκληρωμένη παρακολούθηση της επάρκειας των υπηρεσιών και ένα καλό επιχειρηματικό μοντέλο αποτελεί καθοριστικό παράγοντα για την επιτυχία [BUS.1].
Τα επιχειρηματικά μοντέλα έχουν θεμελιώδη ρόλο στην εξήγηση των τρόπων με τους οποίους οι επιχειρήσεις αλληλεπιδρούν και έρχονται σε επαφή με τους πελάτες τους, τους ανταγωνιστές τους και τους προμηθευτές, στην αλυσίδα αξίας την οποία έχουν δημιουργήσει [BUS.2].

Στην παρούσα μελέτη θα εφαρμοσθεί το μοντέλο Business Model Canvas, το οποίο αναπτύχθηκε από τους Alexander Osterwalder και Yves Pigneur και ανασχεδιάστηκε από τους Grant Smith και Ray Souder. Το Business Model Canvas είναι ένα πρότυπο στρατηγικής διαχείρισης που χρησιμοποιείται για την ανάπτυξη επιχειρηματικών μοντέλων και την τεκμηρίωση των υπαρχόντων. Προσφέρει ένα οπτικό διάγραμμα με στοιχεία που περιγράφουν την πρόταση αξίας μιας επιχείρησης, την υποδομή, τους πελάτες και τα οικονομικά, [BUS.3], [BUS.4], [BUS.5].

Το εν λόγω μοντέλο περιλαμβάνει 9 διαφορετικούς άξονες, μέσω των οποίων θα παρουσιασθούν, με άμεσο και ξεκάθαρο τρόπο οι λειτουργίες του Σκοτεινού Διαδικτύου, το οποίο στην πράξη αποτελεί μια καλοστημένη επιχειρηματική μηχανή. Το εν λόγω επιχειρηματικό μοντέλο δύναται να ακτινογραφήσει το Dark Web, καθώς παρουσιάζει το πως δημιουργεί αγαθά ή υπηρεσίες και το πώς εισπράττει κέρδος από αυτά. Απεικονίζει το στρατηγικό σχέδιο ανάπτυξης του Dark Web, τους άξονες στους οποίους αυτό λειτουργεί,

τον τρόπο που έρχεται σε επαφή με τους πελάτες και τις σχέσεις που αναπτύσσονται. Επί πλέον, θα αναλυθούν οι πόροι που απαιτούνται, οι ενέργειες που πρέπει να διεκπεραιωθούν, οι συνεργασίες με τρίτους που θα αναπτύξει, καθώς και οι τρόποι δημιουργίας εσόδων [BUS.6], [BUS.7], [BUS.8].

Οι άξονες του επιχειρηματικού μοντέλου, είναι όπως παρακάτω:

- **Πρόταση Αξίας (Value Propositions)**
- **Βασικοί Συνεργάτες** (Key Partners)
- **Τομείς - Ομαδοποίηση Πελατών** (Customer Segment Segments)
- **Κανάλια Προσέγγισης** (Channels)
- **Σχέσεις με Πελάτες** (Customer Relationships)
- **Ροές Εσόδων** (Revenue Streams)
- **Βασικές Δραστηριότητες** (Key Activities)
- **Πηγές Εσόδων** (Key Resources)
- **Δομή Κόστους (Cost Structure)**

3.1 Δομικοί Άξονες Επιχειρηματικού Μοντέλου για το Dark Web

Αναλυτικά οι δομικοί άξονες του Επιχειρηματικού Μοντέλου έχει όπως αναφέρθηκε 9 τμήματα, τα πιο σημαντικά παρουσιάζονται ακολούθως [BUS.9].

3.1.1 Η Πρόταση Αξίας και τα Προϊόντα-Υπηρεσίες που παρέχονται στο Dark Web

Εικόνα 3-1 Πρόταση Αξίας της Επιχειρηματικής Ιδέας του Dark Web

- **Who** (Ποιος): Το Dark Web (ή Dark Net) είναι μια εξειδικευμένη ομάδα ιστοσελίδων, της οποίας η ταυτότητα είναι δύσκολα ανιχνεύσιμη από τις αρχές επιβολής του νόμου, από κυβερνητικούς μηχανισμούς και ανιχνευτές (sniffers). Το ευρύ κοινό δεν δύναται να περιηγηθεί σε αυτές τις ιστοσελίδες μέσω των κανονικών μηχανών αναζήτησης (Web Browsers). Είναι ένας ιδιωτικός εικονικός χώρος, όπου οι Χρήστες κινούνται σε πλήρη ανωνυμία για καλούς ή και για κακούς σκοπούς.
- **What** (Τι): Η παροχή ενός ασφαλούς καταφυγίου ανωνυμίας στο Διαδίκτυο είναι κύρια πρόθεση του Dark Web. Σε αυτό υπάρχει αλληλεπίδραση μεταξύ των χρηστών, ανταλλαγή πληροφοριών, κλπ, χωρίς να υπάρχει ο φόβος της αποκάλυψης της ταυτότητάς τους από τρίτους. Στο Dark Web μπορεί κανείς να βρει blogs, forum συζήτησης, υπηρεσίες γνωριμιών, πηγές δεδομένων, επιστημονικά συγγράμματα, online αγορές, και πολλές άλλες υπηρεσίες.
- **How** (Πως): Ο πιο εύκολος τρόπος είναι να συνδεθεί κανείς μέσω του λογισμικού TOR, ενός ειδικού browser, χωρίς τη χρήση κάμερας και αποκάλυψης της IP του Χρήστη. Τα δεδομένα κρυπτογραφούνται και αποκρυπτογραφούνται σε στρώματα, ενώ μεταφέρονται σε τμηματικά, σε υπολογιστές που έχουν εγκατεστημένο το TOR, γεγονός που καθιστά αδύνατο να εντοπιστεί κάποιος Χρήστης.
- **Means** (Με τι μέσα): Χρησιμοποιεί τεχνολογία κρυπτογράφησης, servers, ειδικό λογισμικό, ειδικές ρυθμίσεις και διαπιστευτήρια, ειδικές μηχανές αναζήτησης, κτλ.
- **Income:** Το Dark Web χρησιμοποιεί κατά βάση ως μέσο συναλλαγής το εικονικό νόμισμα Bitcoin, το οποίο είναι λιγότερο ανιχνεύσιμο σε σχέση με τα μετρητά. Σε αρκετές περιπτώσεις χρησιμοποιεί ως πληρωμή την PayPal ή και πιστωτικές κάρτες.

  Σε άλλες περιπτώσεις**,** χρησιμοποιείται ένα είδος υπηρεσίας από τρίτους που ενεργεί ως εγγυητής για λογαριασμό τόσο του αγοραστή όσο και του πωλητή. Ουσιαστικά, η μέθοδος αυτή παίζει το ρόλο του αξιόπιστου μεσάζοντα, ο οποίος πληρώνεται με μια μικρή προμήθεια αναλόγως την συναλλαγή. Για τις συναλλαγές με Bitcoin απαιτείται η εγκατάσταση λογισμικού bitcoin.

  Ενδεικτικά αναφέρεται ότι σε μία εκ των ιστοσελίδων μαύρων online αγορών με την ονομασία ‘’Silk Road’’, οι προμήθειες για κάθε αγοραπωλησία άγγιξαν τα 80 εκατομμύρια δολάρια σε λιγότερο από 3 χρόνια λειτουργίας.
- **Costs:** Χρήση του υφιστάμενου μηχανισμού του παγκόσμιου διαδικτύου.

Θετική πλευρά και Αρνητική Πλευρά του Dark Web

Το Σκοτεινό Web, εν μέρει, δύναται να αποτελέσει ένα είδος καταφύγιου της δημοκρατίας, όπου πληροφοριοδότες και ακτιβιστές αποκαλύπτουν σε δημοσιογράφους ή στο ευρύ κοινό περιστατικά διαφθοράς από κρατικούς και δημόσιους λειτουργούς τους. Επίσης, σε καταπιεστικά θρησκευτικά καθεστώτα άτομα δύνανται να εντοπίσουν, δια μέσω του ανώνυμου δικτύου, ομοϊδεάτες τους, με σκοπό να ζητήσουν βοήθεια ώστε να δραπετεύσουν από τις καταπιεστικές συνθήκες που επικρατούν στη ζωή τους.

Αποτελεί μία τεράστια μαύρη αγορά παράνομων υπηρεσιών και λαθρεμπορίου. Στην εν λόγω αγορά αγοράζονται, πωλούνται και ανταλλάσσονται πληροφορίες, ναρκωτικά, όπλα, κλεμμένες πιστωτικές κάρτες, πορνογραφικό υλικό, ‘’μαύρο’’ χρήμα, κ.ά [BUS.10].

3.1.2 **Βασικοί Συνεργάτες** (Key Partners)

Υπάρχουν διάφοροι που ενδεχομένως να διαδραματίζουν το ρόλο των βασικών συνεργατών (προμηθευτές, επενδυτές, εταιρίες ιστοσελίδων, κτλ) του Dark Web. Χαρακτηριστικά παραδείγματα είναι τα ακόλουθα:

- **Hacker,** που αναλαμβάνουν, μεμονωμένα ή σε ομάδες, την εκτέλεση διαφόρων ηλεκτρονικών εγκλημάτων και πληρώνονται αδρά για να παρέχουν τις υπηρεσίες τους. Πολλές φορές έχει τύχει να παράσχουν βοήθεια στην εξαφάνιση κυκλωμάτων παιδεραστίας.
- **Επιχειρήσεις,** που διερευνούν ανώνυμα τον ανταγωνισμό και επιθυμούν να προστατεύσουν τις επιχειρηματικές τους στρατηγικές από τρίτους.
- **Δημοσιογράφοι,** που έχουν ως σκοπό την προστασία της έρευνας και των πηγών τους.
- **Στρατιωτικοί και αστυνομικοί οργανισμοί,** που θέλουν να προστατέψουν τις επικοινωνίες τους, τις έρευνές τους και τις πληροφορίες που συγκεντρώνουν.
- **Απλοί Χρήστες,** που προσπαθούν να αποκαλύψουν τη διαφθορά διατηρώντας την ανωνυμία τους.

3.1.3 **Σχέσεις με Πελάτες** (Customer Relationship)

Χώρες στις ο οποίες δραστηριοποιούνται Χρήστες του Dark Web είναι η οι Η.Π.Α, η Αγγλία, Αυστραλία, Γερμανία, Καναδάς, Σουηδία, Γαλλία, Ρωσία, Ιταλία και Ολλανδία. Οι πωλητές προωθούν τα προϊόντα τους με λεπτομέρειες, εικόνες και συγκεκριμένες τιμές. Οι πωλητές πληρώνουν ένα αρχικό ποσό για την πώληση προϊόντων τους, ενώ υπάρχει και αξιολόγηση πωλητών και προϊόντων. Οι προμήθειες ανέρχονται ανάλογα το μέγεθος της συναλλαγής. Μπορεί να υπάρχει σε ορισμένες περιπτώσεις αποκλεισμός συγκεκριμένων πελατών. Δεν υπάρχει κανένα στοιχείο ταυτότητας πωλητή και πελάτη [BUS.11].

3.1.4 **Ροές Εσόδων** (Revenue Streams)

Στις περισσότερες περιπτώσεις, οι συναλλαγές στο Dark Web γίνονται με online «μαύρες αγορές», δηλαδή μέσω ιστοσελίδων, όπου οι πωλητές αναρτούν τις αγγελίες τους και δέχονται παραγγελίες και εν συνεχεία τα προϊόντα αποστέλλονται ταχυδρομικά, στη διεύθυνση που θα επιλέξει ο αγοραστής (όπως λειτουργεί και το νόμιμο ηλεκτρονικό εμπόριο).

Ως βασική μέθοδος πληρωμής, συνήθως είναι χρησιμοποιούνται τα κρυπτονόμισματα (bitcoins)[1], πλην όμως υπάρχουν και άλλες περιπτώσεις τετ α τετ πληρωμής, ή και με μετρητά. Χρησιμοποιούνται κρυπτονομίσματα για την εκτέλεση των περισσότερων συναλλαγών/πληρωμών στο Dark Web. Διατηρείται με αυτόν τον τρόπο η ανωνυμία, διότι το κρυπτονόμισμα δεν είναι φυσικό νόμισμα και συνεπώς δεν εμπλέκεται κάποια κεντρική τράπεζα, με συνέπεια να είναι πιο δύσκολο να ανιχνευθούν οι συναλλαγές [BUS.12].

Γίνεται οι συναλλαγές να πραγματοποιούνται με ψηφιακά νομίσματα και έπειτα μεγάλα ποσά bitcoins να μεταφέρονται σε παιχνίδια, όπως το World Of Warcraft και το Second Life, διότι παιχνίδια τέτοιου είδους παρέχουν τη δυνατότητα μετατροπής των ψηφιακών νομισμάτων σε πραγματικά χρήματα, τα οποία μεταφέρουν σε κάποιον τραπεζικό λογαριασμό. Αυτή η διαδικασία εξυπηρετεί το ξέπλυμα μαύρου χρήματος [BUS.13].

Η παράδοση γίνεται με αποστολή των προϊόντων με συμβατικό ταχυδρομείο/ courier, στη διεύθυνση που θα επιλέξει ο αγοραστής. Τα προϊόντα αποστέλλονται σε κάποιες περιπτώσεις ως πολλαπλά πακέτα. Ορισμένα sites χρησιμοποιούν δικές τους εταιρείες courier, με σκοπό να τηρήσουν σε υψηλά ποσοστά την εχεμύθεια. Υπάρχου και περιπτώσεις που κάποιος από άλλο site μπορεί να αγοράσει, παραλάβει και να

[1] Η παραγωγή, η αποθήκευσή, η διακίνηση και όλες οι συναλλαγές με bitcoin γίνονται αποκλειστικά σε ηλεκτρονική μορφή. Το bitcoin είναι ένα ψηφιακό συνάλλαγμα ανοιχτού κώδικα, ένα peer-to-peer σύστημα πληρωμών.

ταχυδρομήσει κάποιο προϊόν, με μμικρή προμήθεια, επ΄ ωφέλεια τρίτου.

Εικόνα 3-2 Ροές Εσόδων (Revenue Streams) του Dark Web

Ο τρόπος αποθήκευσης bitcoins και υλοποίησης αγορών γίνεται μέσω ενός ψηφιακού πορτοφολιού (bitcoin wallet). Το εν λόγω πορτοφόλι αυτό δύναται να βρίσκεται σε ένα πρόγραμμα σε υπολογιστή ή να φιλοξενείται σε κάποια ιστοσελίδα π.χ. ένα Bitcoin Exchange [BUS.14].

Κάθε bitcoin wallet έχει μια μοναδική διεύθυνση, η οποία χρησιμοποιείται για να γίνουν οι μεταφορές ανώνυμα. Όταν γίνεται μια συναλλαγή με bitcoin το σύστημα επιβεβαιώνει τις διευθύνσεις των πορτοφολιών του αγοραστή και πωλητή και εν συνεχεία, μέσω περίπλοκων μαθηματικών υπολογισμών (*απαραίτητων για το σύστημα κρυπτογράφησης που προστατεύουν το σύστημα*) επιβεβαιώνεται η εγκυρότητα της συναλλαγής. Οι έγκυρες συναλλαγές καταγράφονται και τα δεδομένα της κάθε συναλλαγής προστίθενται σε ένα αρχείο καταγραφών (log) που ονομάζεται Blockchain. Η όλη διαδικασία είναι συνεχούς επιβεβαίωσης, που ουσιαστικά κάνει το ψηφιακό νόμισμα απρόσβλητο από τους Hackers [BUS.15].

3.1.5 **Δομή Κόστους** (Cost Structure)

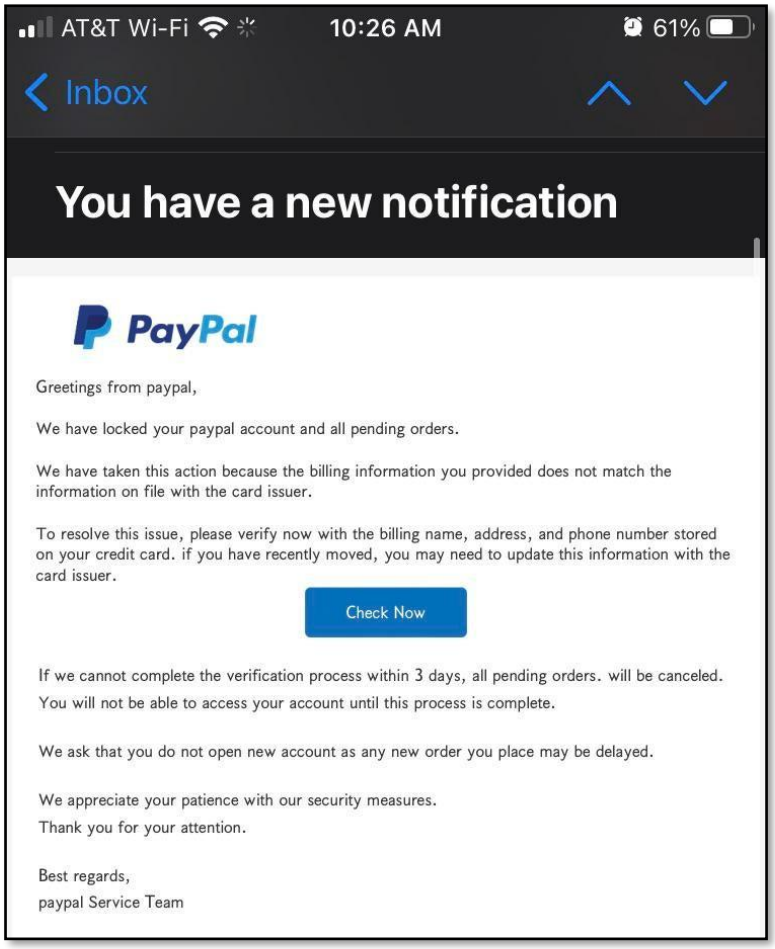
Το Dark Net αποτελείται από κρυπτογραφημένο δίκτυο server σε όλο τον κόσμο με υπηρεσίες και ιστοσελίδες. Το εν λόγω δίκτυο από server, βασίζεται σε τεχνολογίες κρυπτογράφησης ανταλλαγής δεδομένων π.χ. το TOR (The Onion Router), το οποίο αναπτύχθηκε αρχικά από το Ερευνητικό Εργαστήριο του αμερικανικού πολεμικού ναυτικού, για την προστασία των στρατιωτικών επικοινωνιών. Η πρόσβαση υλοποιείται με τη χρήση του υφιστάμενου μηχανισμού του παγκόσμιου διαδικτύου, με ειδικά λογισμικά, ειδικές ρυθμίσεις και διαπιστευτήρια, συγκεκριμένα πρωτόκολλα και ειδικές μηχανές αναζήτησης.

3.1.6 **Βασικές Δραστηριότητες** (Key Activities)

3.1.6.1 **Διαδικτυακά Δίκτυα Ρομπότ** (Botnet) **και Ηλεκτρονικό Ψάρεμα** (Phishing)

Στο Dark Web μπορεί κανείς να συναντήσει μια ομάδες συσκευών (Botnets) συνδεδεμένων στο Διαδίκτυο, καθεμία από τις οποίες εκτελεί ένα ή περισσότερα bot[2], το οποίο εκτελεί αυτοματοποιημένες εργασίες μέσω του διαδικτύου. Μία από τις πιο γνωστές χρήσεις των Botnet είναι οι επιθέσεις DDoS, η αποστολή Spam και η διάδοση malware [BUS.16].

Ο Σκοτεινός Ιστός περιέχει πολλές σελίδες "ψαρέματος" (Phishing**)** στοιχείων (κυρίως οικονομικών) των χρηστών, με σκοπό να εξαπατήσουν τους Χρήστες, οι οποίοι ανυποψίαστοι συμπληρώνουν τα στοιχεία του πραγματικού τους λογαριασμού. Οι περισσότερες σελίδες αυτού του είδους είναι πιστά αντίγραφα δημοφιλών υπηρεσιών, όπως το PayPal [BUS.17].



Εικόνα 3-3 Σελίδα Εξαπάτησης (Phishing) PayPal

Πηγή:

https://preview.redd.it/tgu1wu8flej81.jpg?width=750&format=pjpg&auto=webp&s=fef88dab45b041526ba3e3c6d538ce4e2d07366a

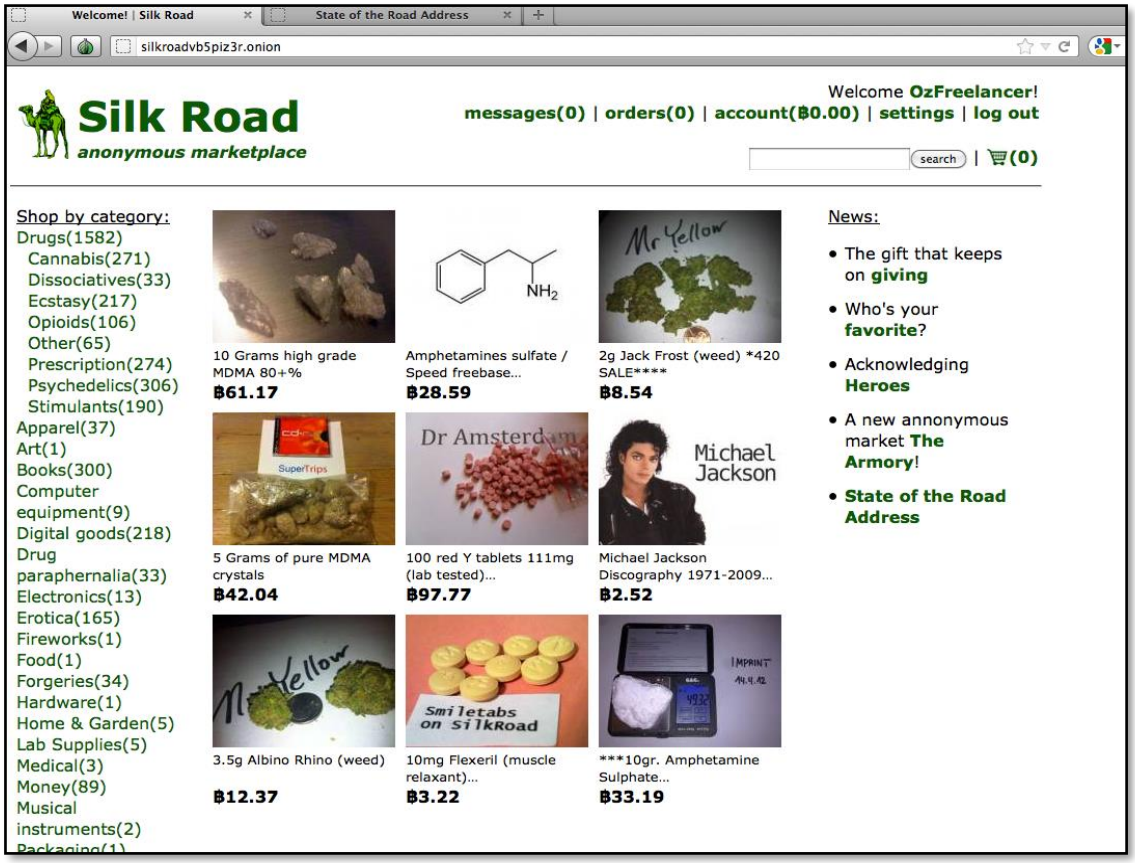
[2] Ονομάζεται διαδικτυακό ρομπότ (Internet bot) ή web bot ή web robot ή WWW robot ή απλά bot.

3.1.6.2 Η Μαύρη Αγορά του Dark Web (Η περίπτωση του Silk Road)

Η αρχή των μαύρων αγορών μέσα στο Dark Web έγινε τον Φεβρουάριο του 2011 με την Ιστοσελίδα Silk Road (Δρόμος του Μεταξιού), που δημιουργήθηκε από τον Ross William Ulbricht. Η σελίδα ήταν κρυμμένη πίσω από τις υπηρεσίες του TOR και η ταυτότητα των χρηστών ήταν μυστική.

Διέθετε πάνω από 9.600.000 εγγεγραμμένους Χρήστες και ο εν λόγω ιστότοπος εξελίχθηκε στην πιο εκτεταμένη εγκληματική αγορά στο Διαδίκτυο. Η εν λόγω ιστοσελίδα είχε και ως παρατσούκλι το eBay των ναρκωτικών, ένας παράδεισος ναρκωτικών πάνω από 10.000 προϊόντα ως επιλογή, ο οποίος διήρκησε έως και το 2013.

Οι αγοραστές εγγράφονταν δωρεάν στο Silk Road. Οι πωλητές αρχικά αγόραζαν λογαριασμούς, μέσω δημοπρασιών, και αργότερα πλήρωναν ένα ενιαίο ποσό. Το Silk Road ήταν μια πλατφόρμα στην οποία διάφοροι προμηθευτές όλων των ειδών ναρκωτικών και άλλων εμπορευμάτων, που δεν μπορεί κανείς να αγοράσει στην ελεύθερη αγορά, προωθούσαν μεγάλης ποικιλίας εμπορεύματα στους καταναλωτές. Οι πληρωμές γίνονταν σε Bitcoin [BUS.18].



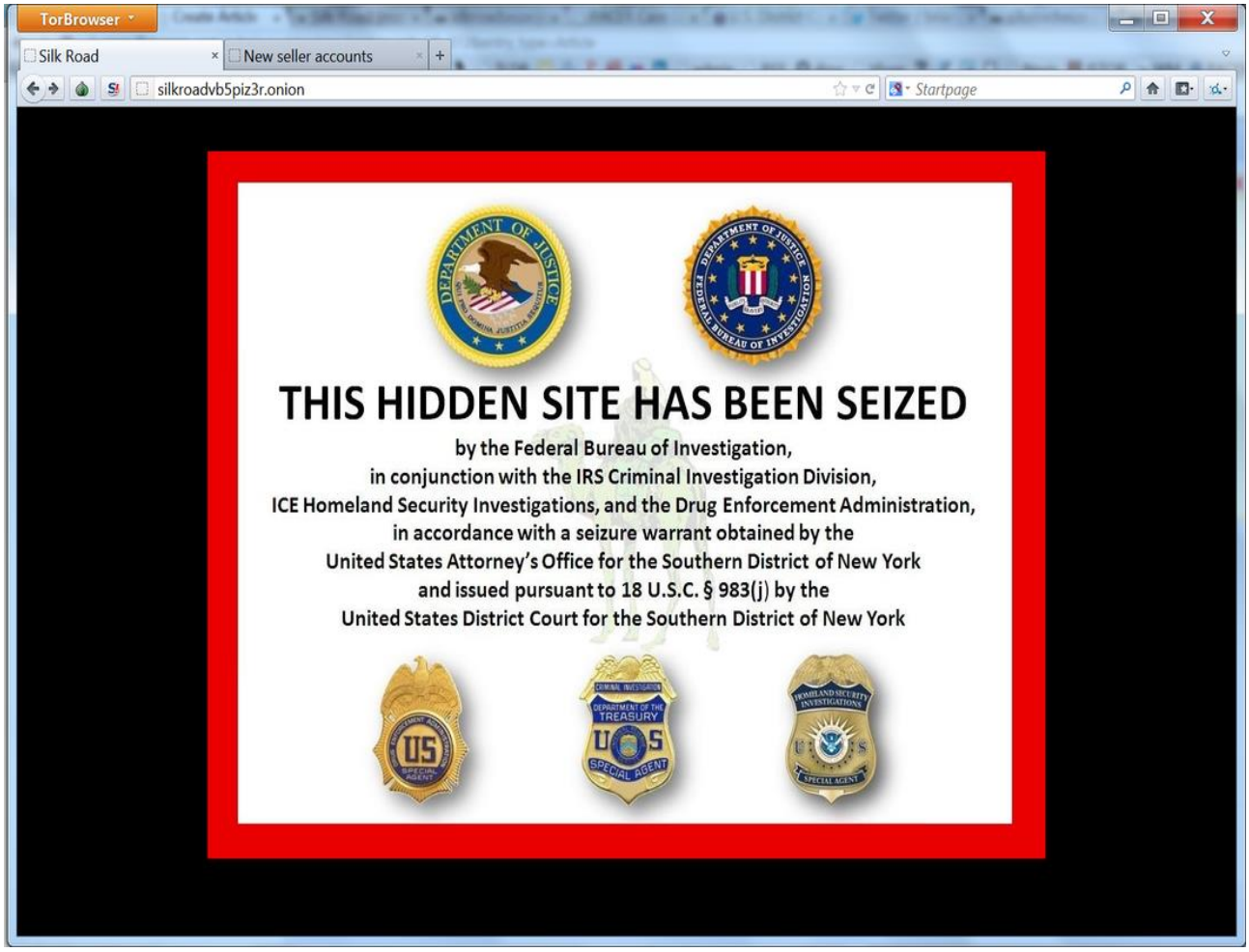
Εικόνα 3-4 Η Μαύρη Αγορά του Silk Road

Πηγή: https://www.techrepublic.com/wp-content/uploads/2017/05/screen-shot-2012-04-24-at-2-02-25-am.png

Το Silk Road βρισκόταν στο στόχαστρο των Αμερικανικών αρχών. Ο ιδιοκτήτης του Silk Road επικήρυξε υπάλληλό του, ονομαζόμενος Ross William Ulbricht (με το παρατσούκλι Dread Pirates Roberts), διότι υπεξαίρεσε μεγάλα ποσά bitcoins από πελάτες της Ιστοσελίδας.

Ο Ιδιοκτήτης του Silk Road, μέσω του Dark Web, βρήκε έναν εκτελεστή έναντι 40.000 δολαρίων, προκειμένου να δολοφονήσει τον παραβατικό υπάλληλο του. Εντούτοις, Οκτώβριο του 2013 το FBI συνέλαβε τον ιδιοκτήτη με την κατηγορία της απόπειρας δολοφονίας.

Τον Νοέμβριο του 2013, οι πρώην διαχειριστές της σελίδας Silk Road άνοιξαν το Silk Road 2.0, το οποίο όμως έκλεισε τον Νοέμβριο του 2014 στα πλαίσια της Operation Onymous του FBI [BUS.19].

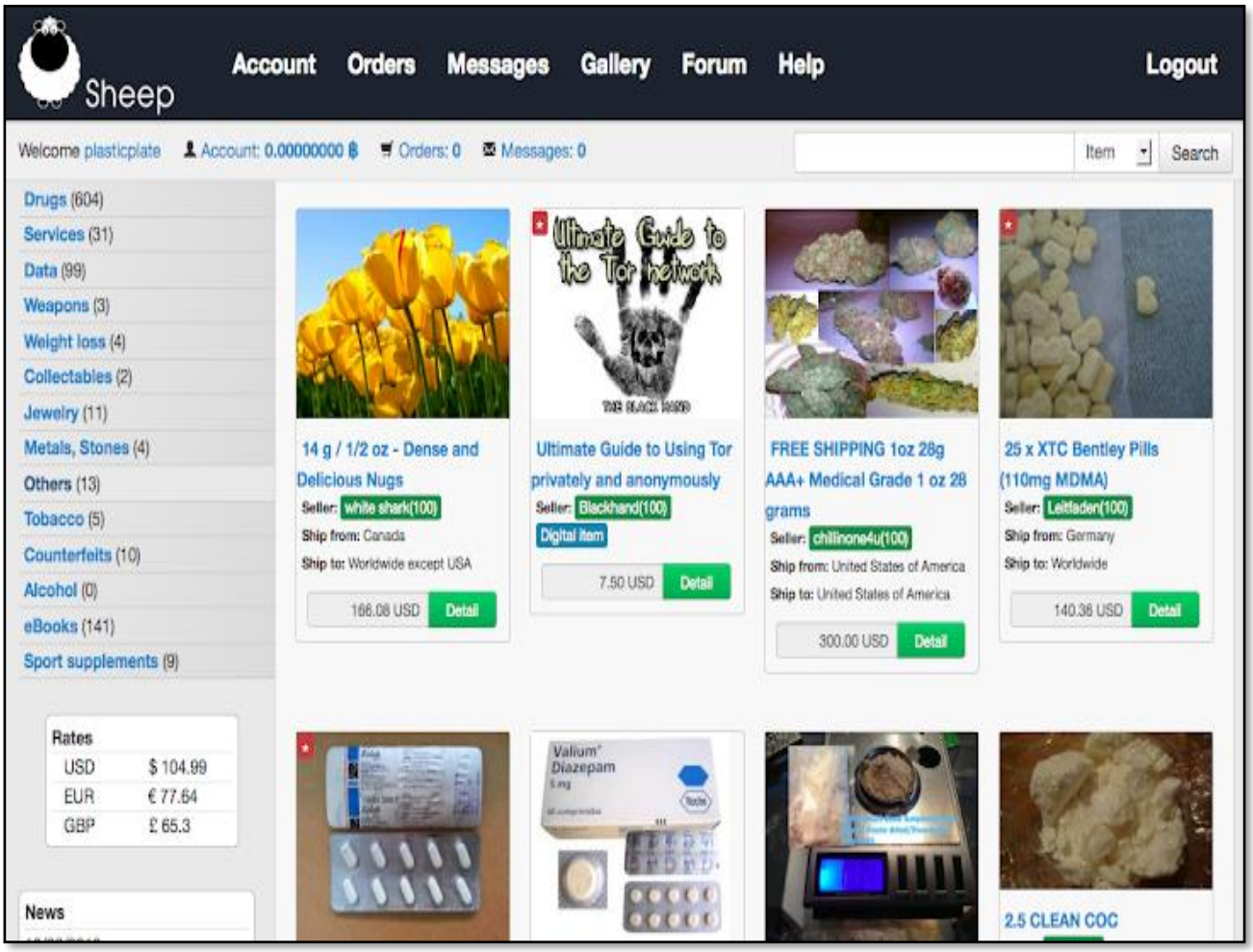


Εικόνα 3-5 Κλείσιμο του Silk Road από το FBI

Πηγή: http://cdn3.sbnation.com/assets/3325661/silk_road_seized.png

3.1.6.3 Η Μαύρη Αγορά του Dark Web (Η περίπτωση του Sheep Marketplace)

Το **Sheep Marketplace**, μια μικρότερη αγορά στο Dark Web, έγινε πολύ δημοφιλές μετά το κλείσιμο του Silk Road. Τον Δεκέμβριο του 2013, ανακοινώθηκε από ενός διαχειριστές του ιστότοπου ότι κάποιος από ενός πωλητές που δραστηριοποιούνταν σε αυτό, κατάφερε να κλέψει 5400 Bitcoins από Χρήστες ενός σελίδας. Εντούτοις, οι Χρήστες κατάφεραν να αποδείξουν πως το ποσό ήταν περίπου 40.000 Bitcoins, καθώς και ημέρες πριν την κλοπή, το site είχε μπλοκάρει ενός αποσύρσεις των Bitcoing. Τον Μάρτιο του 2015, η Τσεχική αστυνομία συνέλαβε έναν άνδρα ως ύποπτο για την κλοπή. Η αφορμή ήταν η αγορά ενός ακριβού σπιτιού με τη χρήση Bitcoins [BUS.20].



Εικόνα 3-6 Η Μαύρη Αγορά του Sheep Marketplace

Πηγή: https://news-cdn.softpedia.com/images/news2/96-000-Bitcoins-Reportedly-Stolen-from-Sheep-Marketplace-405486-2.png

3.1.6.4 Παράνομη Πορνογραφία (Η περίπτωση του Playpen)

Ο ιστοχώρος **Playpen** στο Dark Web υπήρξε ο έναν από τους μεγαλύτερους ιστοχώρους παιδικής πορνογραφίας. Τον Φεβρουάριο του 2015, τεχνικοί του FBI εντόπισαν περίπου 1.300 IP διευθύνσεις χρηστών απ' όλο τον κόσμο, μετρώντας περίπου 215.000 εγγεγραμμένους Χρήστες, οι οποίοι συσχετίζονται με τέτοιες δραστηριότητες.

Όπως ανακοίνωσαν οι αρχές η ιστοσελίδα διέθετε αρχεία με περισσότερα από 2.000 βίντεο και ακόμη περισσότερες φωτογραφίες από 250 παιδιά κυρίως αγόρια. Οι ηλικίες ήταν από 3 έως 17 χρονών και προέρχονταν από 39 αμερικάνικες πολιτείες. Εκδόθηκαν περίπου 150 εντάλματα σύλληψης εναντίων υπόπτων στις ΗΠΑ και άλλα 150 σε άλλες χώρες [BUS.21].

Σε άλλη παράλληλη επιχείρηση οι αμερικανικές αρχές εξάρθρωσαν ένα διεθνές δίκτυο παιδικής πορνογραφίας με 27.000 συνδρομητές απ' όλο τον κόσμο. 14 άτομα συνελήφθησαν με την κατηγορία της εκμετάλλευσης ανηλίκων. Το δίκτυο λειτούργησε από τον Ιούνιο του 2012 μέχρι τον Ιούνιο του 2013.

Μία άλλη γνωστή επιχείρηση εναντίον της παιδικής πορνογραφίας ήταν η "Operation Darknet" το 2011, με τη βοήθεια της ομάδας Hackers Anonymous εντοπίστηκε η εταιρία "Freedom Hosting", η οποία διαχειρίζονταν πάνω από 100 GB πορνογραφικού υλικού, με εγγεγραμμένα μέλη πάνω από 1500 άτομα [BUS.22].

Τέλος, οι Hackers Anonymous κατάφεραν να μπλοκάρουν τους Servers, μέσω μιας τεράστιας επίθεσης DDos, της εταιρίας **"**Lolita City**"**, η οποία διαχειρίζονταν ιστότοπο γνωστό στους κύκλους των παιδόφιλων [BUS.23].

3.1.6.5 Τρομοκρατία (Η περίπτωση του Ισλαμικού Κράτους ISIS)

Τα τελευταία χρόνια εμφανίστηκε απροκάλυπτα η τρομοκρατική οργάνωση ISIS, η οποία προέβη σε σειρά ψυχρών εκτελέσεων, οι οποίες έκαναν τον γύρο του διαδικτύου, προκαλώντας τον τρόμο σε εκατομμύρια ανθρώπους στον κόσμο. Ήταν απόρροιας άξιο πως τα μέλη αυτής της οργάνωσης έρχονταν σε επαφή μεταξύ τους, χωρίς να αποκαλύπτονται, διεξάγοντας ιερό πόλεμο, πολλαπλών μετώπων σε 5 χώρες και σε 2 ηπείρους. Ολόκληρος ο συνασπισμός των Εθνών είχε ελάχιστη επιτυχία στην ανίχνευσή τους. Ο ISIS χρησιμοποίησε για πρώτη φορά τα social media για να στρατολογήσει υποψήφιους τζιχαντιστές, ωστόσο και τώρα χρησιμοποιεί το Dark Web, όπου αναζητούνται ανώνυμες δωρεές και συναλλαγές με bitcoins [BUS.24].

Εικόνα 3-7 Η Μαύρη Αγορά του Sheep Marketplace

Πηγή: https://i0.wp.com/securityaffairs.co/wordpress/wp-content/uploads/2015/05/ISIS-funds.jpg

3.1.6.6 Υπηρεσίες Αντεκδίκησης (Η περίπτωση του Hitman Network)

Πρόκειται για ιστοσελίδες, που αναζητούνται τρίτα άτομα επί πληρωμή, οι οποίοι παρέχουν υπηρεσίες αντεκδίκησης. Οι τιμές εξαρτώνται από το άτομο, το οποίο είναι ο Στόχος. Χαρακτηριστικό παράδειγμα είναι η σελίδα η “Hitman Network”. Η σελίδα παρέχει και έκπτωση 1% στους Χρήστες που θα τη διαφημίσουν.

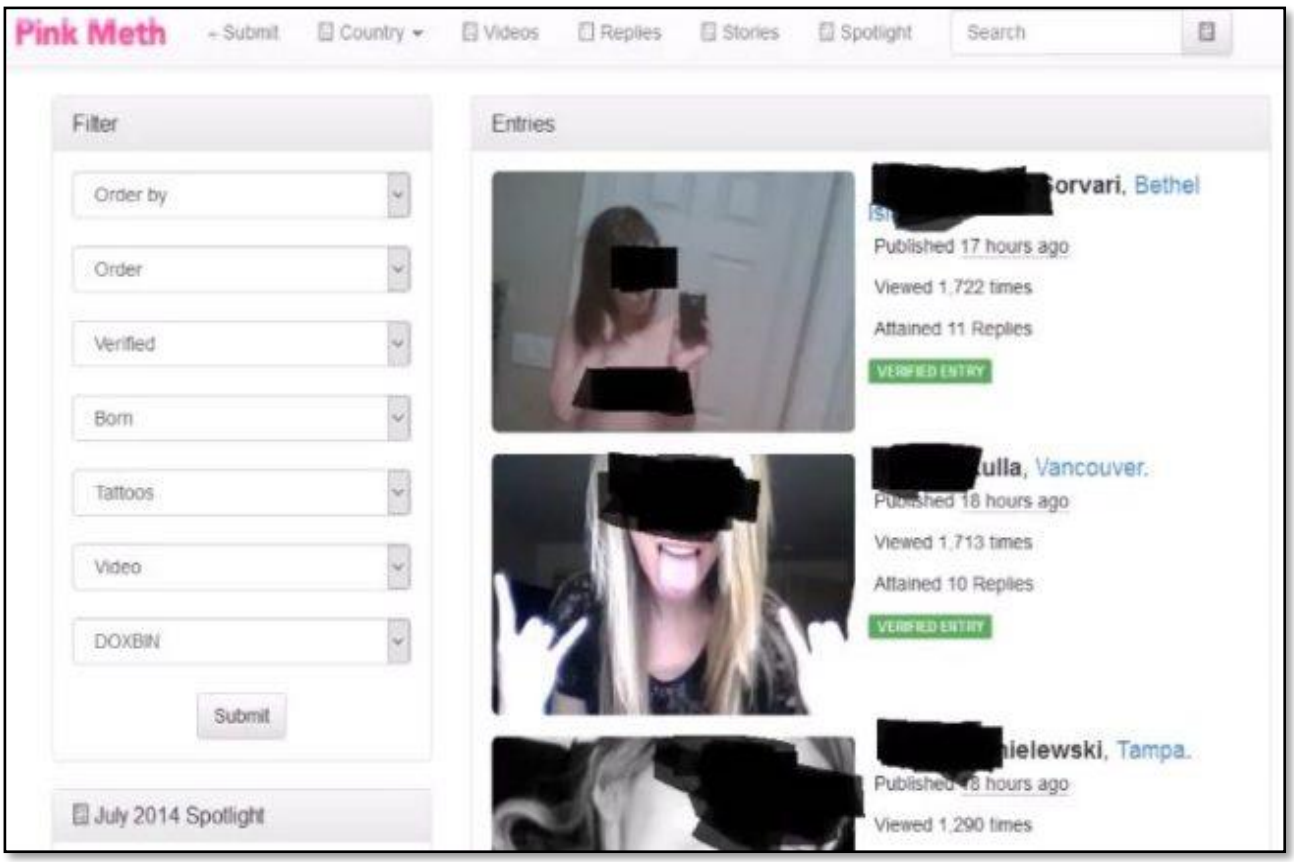
Γνωστός πωλητής υπηρεσιών εκδίκησης είναι ένα πρόσωπο με το ψευδώνυμο “Etimbuk”, ο οποίος για 700$ προσφέρει εκδίκηση σε όσους τους έχουν πειράξει. Η πράξη εκδίκησης μπορεί να πραγματοποιηθεί εναντίον οποιουδήποτε και ανώνυμα. Οι πελάτες αυτής της υπηρεσίας δεν έχουν καμία σχέση με την πράξη βίας που διαπραχθεί. Σε άλλες περιπτώσεις δύναται να δημιουργηθεί λίστα υποψήφιων Στόχων, ενώ η πληρωμή διεξάγεται με κρυπτονόμισματα BUS. [25].

Εικόνα 3-8 Ιστοχώρος Αντεκδίησης Hitman Network

Πηγή: https://static01.nyt.com/images/2020/03/02/business/00hitmen3/00hitmen3-superJumbo.jpg?quality=75&auto=webp

3.1.6.7 Διαρροή Εικόνων Προσωπικών Δεδομένων Ατόμων προ-εφηβικής Ηλικίας (Η περίπτωση του Pink Meth)

Το Pink Meth είναι μια ιστοσελίδα στην οποία οι Χρήστες πληρώνονται για να ανεβάζουν υλικό φωτογραφιών και βίντεο σχετικό με τις πρώην τους. Περιέχει φωτογραφίες και βίντεο κοριτσιών προ-εφηβικής ηλικίας μέχρι και ηλικιωμένων γυναικών. Μερικοί Χρήστες δημοσιεύουν πρόσθετα στοιχεία, όπως π.χ. προφίλ στο Facebook, κτλ. Η σελίδα έκλεισε από το FBI, πλην όμως φημολογείται ότι έχει ανοίξει πάλι ‘’βαθιά’’ στο Dark Web [BUS.26].



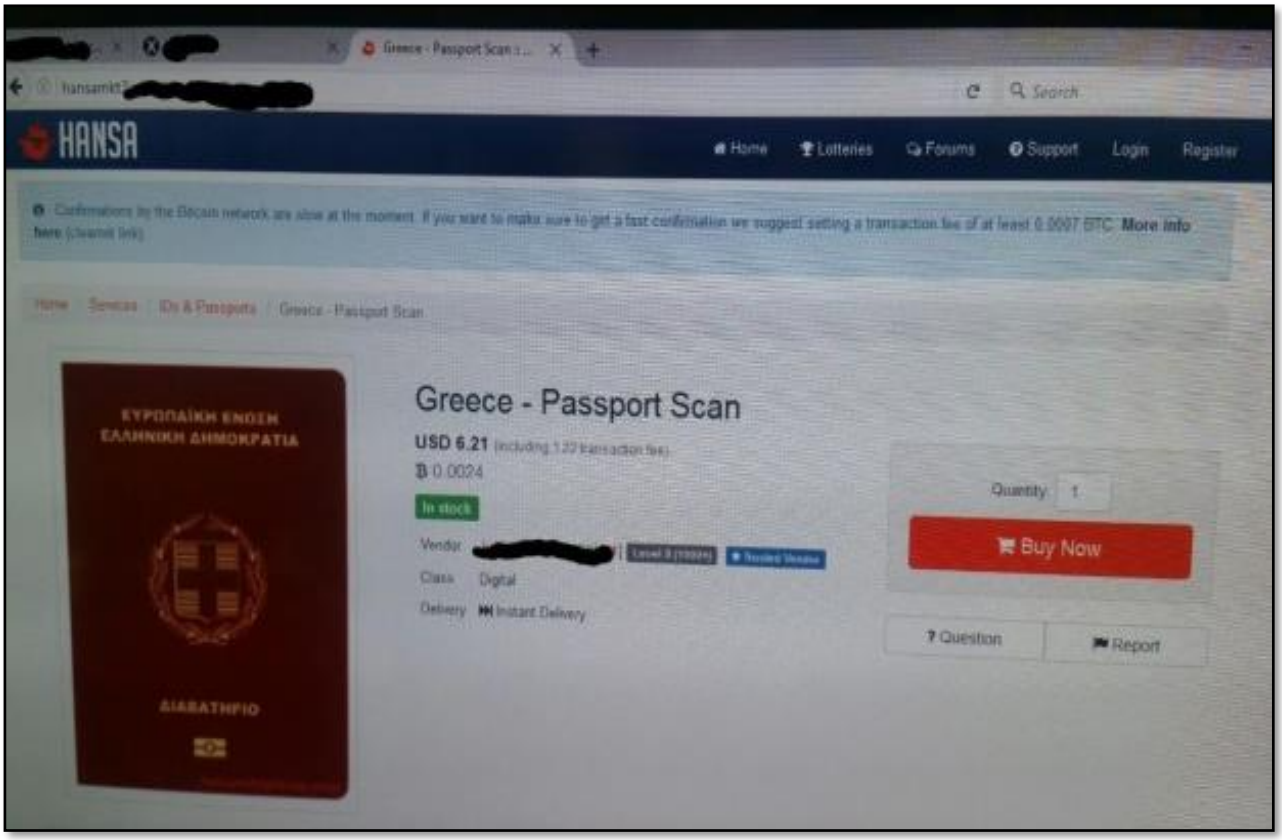
Εικόνα 3-9 Διαρροή Εικόνων Προσωπικών Δεδομένων Ατόμων προ-εφηβικής Ηλικίας

Πηγή: https://d2r8r0qhs4bt8m.cloudfront.net/wp-content/uploads/2019/10/18180032/desktop-1481571260.png

3.1.6.8 Πώληση Πλαστών Εγγράφων (Διαβατήρια και Πιστωτικές Κάρτες)

Η πώληση πλαστών διαβατηρίων αποτέλεσε αντικείμενο οικονομικής δραστηριότητας επιτήδειων κακόβουλων, οι οποίοι δραστηριοποιούνται στο Dark Web. Διέθεταν ταξιδιωτικά έγγραφα σε πολύ χαμηλότερες τιμές σε σχέση με αυτές των παραδοσιακών κυκλωμάτων διακίνησης παραχαραγμένων διαβατηρίων. Το ενδεχόμενο να μπορεί κάποιος να αγοράσει ηλεκτρονικά ένα πλαστό διαβατήριο διατηρώντας, σε μεγάλο βαθμό, την ανωνυμία του γεννά μεγάλους προβληματισμούς στην παγκόσμια κοινότητα. Το ερώτημα είναι αν πράγματι ο πωλητής διαθέτει πλαστά ταξιδιωτικά έγγραφα διαφόρων χωρών ή κατά πόσο πρόκειται για έναν πωλητή που απλώς εξαπατά τους αγοραστές που δραστηριοποιούνται στο σκοτεινό Διαδίκτυο, εισπράττοντας χρήματα σε ψηφιακό νόμισμα χωρίς τελικά να παραδίδεται το εμπόρευμα. Στην διακίνηση πλαστών διαβατηρίων, μέσω του Dark Web, συγκαταλέγονται και ελληνικά διαβατήρια. Σε έρευνα του «Ελεύθερου Τύπου» της Κυριακής στα «σκοτεινά» μονοπάτια του διαδικτύου εντοπίστηκε κρυπτογραφημένη σελίδα, η οποία διέθετε πώληση ελληνικά διαβατήρια έναντι 0,0024 bitcoin (ψηφιακό νόμισμα), ποσό που αντιστοιχεί σε πέντε ευρώ. Η σελίδα ανέφερε ότι τα ελληνικά διαβατήρια βρίσκονταν σε

απόθεμα και σε πολύ συμφέρουσα τιμή. Επίσημα, από τις ελληνικές Αρχές δεν είχε εντοπιστεί, ποτέ πώληση ελληνικών διαβατηρίων, χωρίς αυτό να σημαίνει απαραίτητα ότι δεν γινόταν, ειδικά σε μία περίοδο που παράνομα κυκλώματα λυμαίνονται το χώρο του ελέγχου της διακίνησης μεταναστών BUS. [27].



Εικόνα 3-10 Πώληση Διαβατηρίων στο Dark Web

Πηγή:

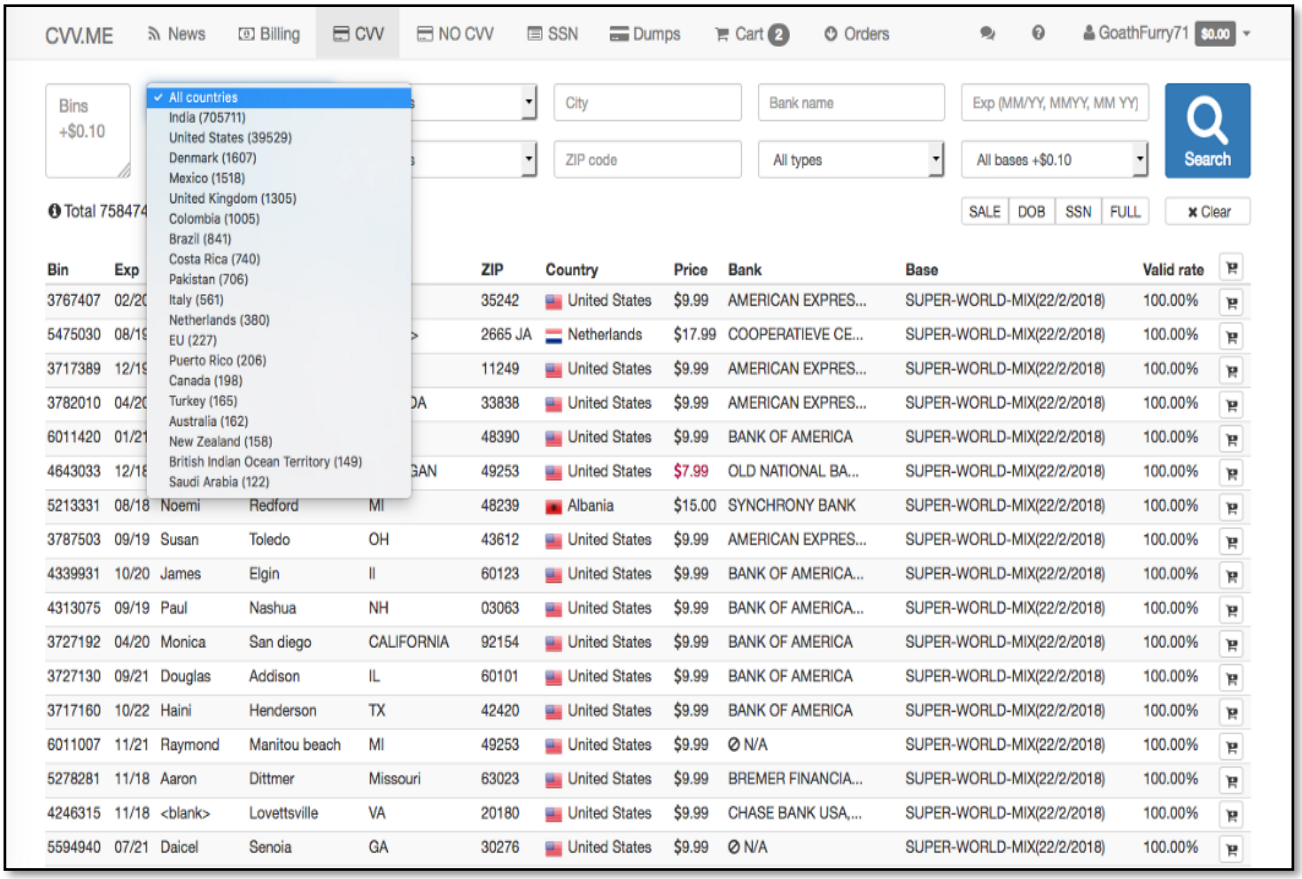
https://cdn.sofokleousin.gr/sites/default/files/styles/node_full/public/articles/2017/01//original_394215895.jpg?itok=AVCIspEQ

Είναι εξίσου σημαντικό να αναφερθεί ότι στο Dark Web λαμβάνει χώρα η πώληση πλήθους πιστωτικών καρτών. Οι επιτήδειοι χρησιμοποιούν σχετικές ιστοσελίδες, όπου αναρτούν στοιχεία πιστωτικών καρτών από πολίτες διαφόρων χωρών. Οι Hackers μπορούν να αποκτήσουν μαζική πρόσβαση σε κωδικούς καρτών παρακολουθώντας αφερέγγυα διαδικτυακά καταστήματα (e-shop), στα οποία η ασφάλεια των ηλεκτρονικών συναλλαγών είναι σε πολύ χαμηλό επίπεδο.

Οι πιστωτικές συνήθως πωλούνται από 0.40 bitcoin (περίπου 300 ευρώ) έως 2.40 bitcoin (περίπου 2.000 ευρώ), με πιστωτικό όριο από 4.000-5.000 δολάρια. Οι Hackers παρέχουν ως διαφημιστικό δόλωμα το πιστωτικό όριο της κάρτας, τη χώρα προέλευσης και τον κωδικό

για την αγορά της. Το χρονικό περιθώριο που δίνεται, συνήθως, για χρήση των καρτών, είναι 48 ώρες μετά την αγορά, διαφορετικά μετά οι κωδικού κλειδώνονται.

Η τιμή διαφέρει ανάλογα με τις ημέρες που μπορεί ο Χρήστης να τις χρησιμοποιήσει και το επιτρεπόμενο πιστωτικό όριο της κάθε κάρτας. Εκτός από την πώληση των κωδικών διατίθενται και κάρτες ‘’κλώνοι’’, με τετραψήφιο κωδικό, τις οποίες ο αγοραστής δύναται να χρησιμοποιήσει σε οπουδήποτε ATM, καταστήματα, καθώς και σε διαδικτυακές αγορές στον κόσμο. Μαζί με την κάρτα ο πωλητής αποστέλλει πλήρη οδηγό χρήσης για παροχή μέγιστης ασφάλειας [BUS.28].

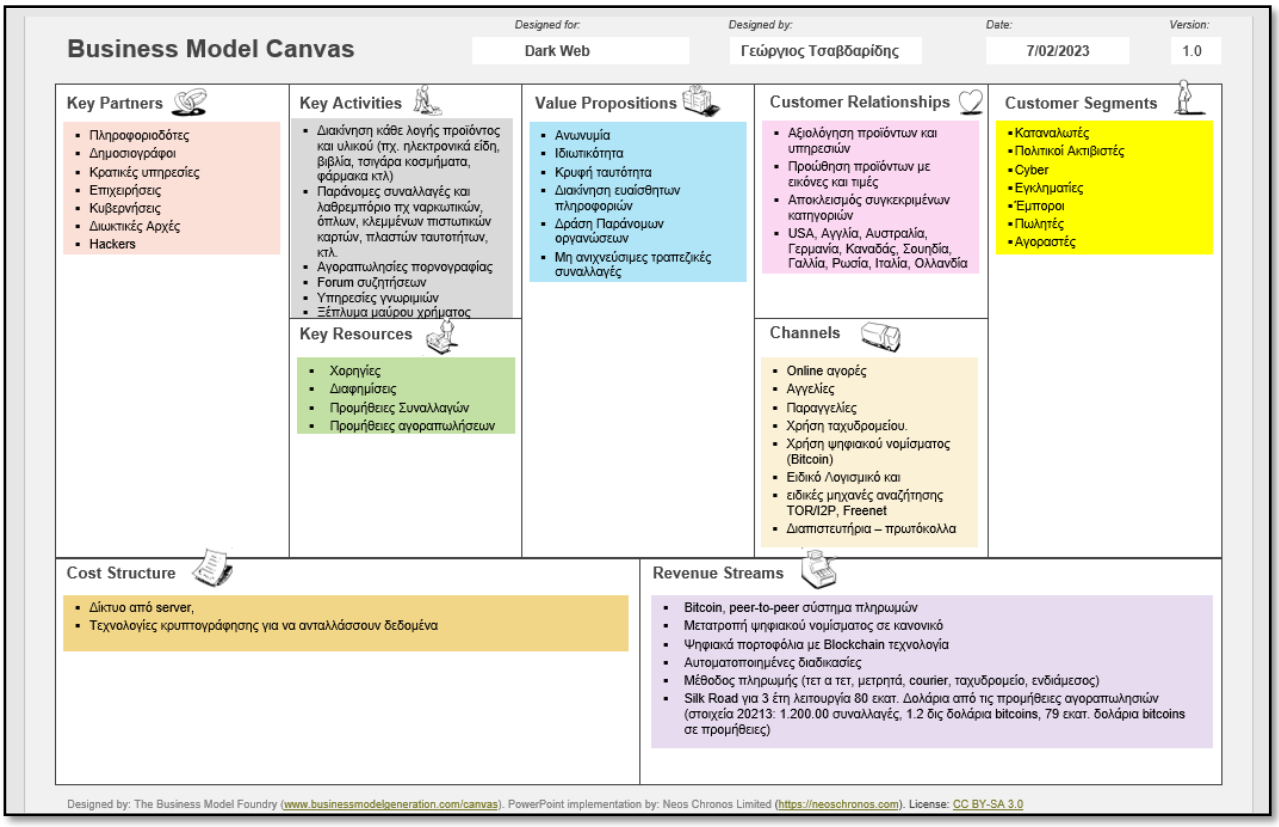


Εικόνα 3-10 Πώληση Πιστωτικών Καρτών στο Dark Web

Πηγή: https://miro.medium.com/max/1100/1*9BbDi8J921ZocdR8aEWWgA.webp

3.2 Συνολική Αποτίμηση Business Model Canvas για το Σκοτεινό Διαδίκτυο

Το Σκοτεινό Διαδίκτυο έχει, εν τέλει, καταλήξει να είναι μία καλοστημένη πολύ επικερδής επιχείρηση νόμιμων και παράνομων δραστηριοτήτων, οι οποίες ολοένα και αυξάνονται με γεωμετρική πρόοδο, στο βωμό της ανωνυμίας και της ελευθερίας κινήσεων και επιλογών πωλητών και αγοραστών. Οι 9 άξονες του Επιχειρηματικού Μοντέλου συνοψίζονται στην ακόλουθη Εικόνα.



Εικόνα 3-11 Business Model Canvas

Σύμφωνα με στοιχεία που έφερε στη δημοσιότητα η Reboot SEO Company, η Ελλάδα καταλαμβάνει την 8η θέση ανάμεσα στις χώρες που οι πολίτες τους φαίνεται να ενδιαφέρονται για τον Σκοτεινό Ιστό με βαθμολογία ενδιαφέροντος για το σκοτεινό Διαδίκτυο με 76,5 στα 100. Υπολογίζεται ότι υπάρχουν 718 Χρήστες ανά 100.000 άτομα, που πραγματοποιούν αναζήτηση στο Dark Web κάθε μήνα.

Με βάση τα ίδια δεδομένα, η Κροατία φαίνεται πως καταλαμβάνει την πρώτη θέση ανάμεσα στις χώρες που ενδιαφέρονται περισσότερο για τον σκοτεινό ιστό το 2022, με βαθμολογία ενδιαφέροντος 97,1 στα 100.

Παράλληλα, η Τσεχία καταλαμβάνει τη δεύτερη θέση με βαθμολογία ενδιαφέροντος για το σκοτεινό Διαδίκτυο 94,1 στα 100, απαριθμώντας πάνω από 8 εκατομμύρια ενεργούς Χρήστες του διαδικτύου και 1.027 Χρήστες ανά 100.000 που πραγματοποιούν αναζήτηση στο Dark Web κάθε μήνα.

Στην τρίτη θέση έρχεται η Ιρλανδία με βαθμολογία ενδιαφέροντος 91,2 στα 100, απαριθμώντας 953 Χρήστες για κάθε 100.000 Χρήστες του διαδικτύου

Τέλος, στην τέταρτη θέση βρίσκεται η Ουγγαρία με βαθμολογία ενδιαφέροντος για το Dark Web 88,2 στα 100 και την πρώτη πεντάδα συμπληρώνει η Ρουμανία με βαθμολογία 85,3 στα 100.

Rank	Country	Searches per 100,000 users	Dark web interest score (/100)
1	Croatia	1,083	**97.1**
2	Czech Republic	1,027	**94.1**
3	Ireland	953	**91.2**
4	Hungary	920	**88.2**
5	Romania	804	**85.3**
6	Slovakia	756	**82.4**
7	Albania	731	**79.4**
8	Greece	718	**76.5**
9	Netherlands	708	**73.5**
10	Italy	697	**70.6**

Εικόνα 3-2 Κατάταξη Χωρών Χρηστών του Dark Web

Πηγή: Reboot SEO Company

ΚΕΦΑΛΑΙΟ 4ο :
Εισβολείς Υπολογιστικών Συστημάτων (Hackers) στο Dark Web

4.0 Ορισμοί -Χρήσιμη Ορολογία

Η πλειοψηφία του κόσμου έχει συσχετίσει τους **Εισβολείς Υπολογιστικών Συστημάτων** (**Hacker)** με κακόβουλες πράξεις μέσω διαδικτύου. Γενικά, ο Hacker επικεντρώνεται στην εκμετάλλευση των κενών του Λειτουργικού Συστήματος ενός Υπολογιστή, καθώς και στην διείσδυση σε ένα Δίκτυο Υπολογιστών. Η δραστηριότητα αυτή είναι γνωστή ως Hacking.

Hacker ονομάζεται, συνήθως, το άτομο, το οποίο εισβάλλει σε υπολογιστικά συστήματα και πειραματίζεται με κάθε πτυχή τους. Ωστόσο, παλαιότερα είχε την έννοια του εφευρέτη, δηλαδή αυτού που ασχολείται να ανακαλύψει το πως λειτουργεί ένα σύστημα, να το βελτιώσει ή και να το αλλάξει, κάνοντας τροποποιήσεις σε αυτό. Οι Hackers έχουν τις κατάλληλες γνώσεις και ικανότητες να διαχειρίζονται σε μεγάλο βαθμό υπολογιστικά συστήματα. Συνήθως, οι Hackers είναι προγραμματιστές, σχεδιαστές συστημάτων αλλά και άτομα, τα οποία ενώ δεν ασχολούνται επαγγελματικά με τομείς τους πληροφορικής, έχουν αναπτύξει τέτοιες δεξιότητες και δουλεύουν είτε σε ομάδες (hacking-groups) είτε μόνοι τους. Αν οι πράξεις τους αυτές είναι κακόβουλες αποκαλούνται Crackers [HACK.1]

4.1 Κατηγορίες Εισβολέων Υπολογιστικών Συστημάτων στο Dark Web

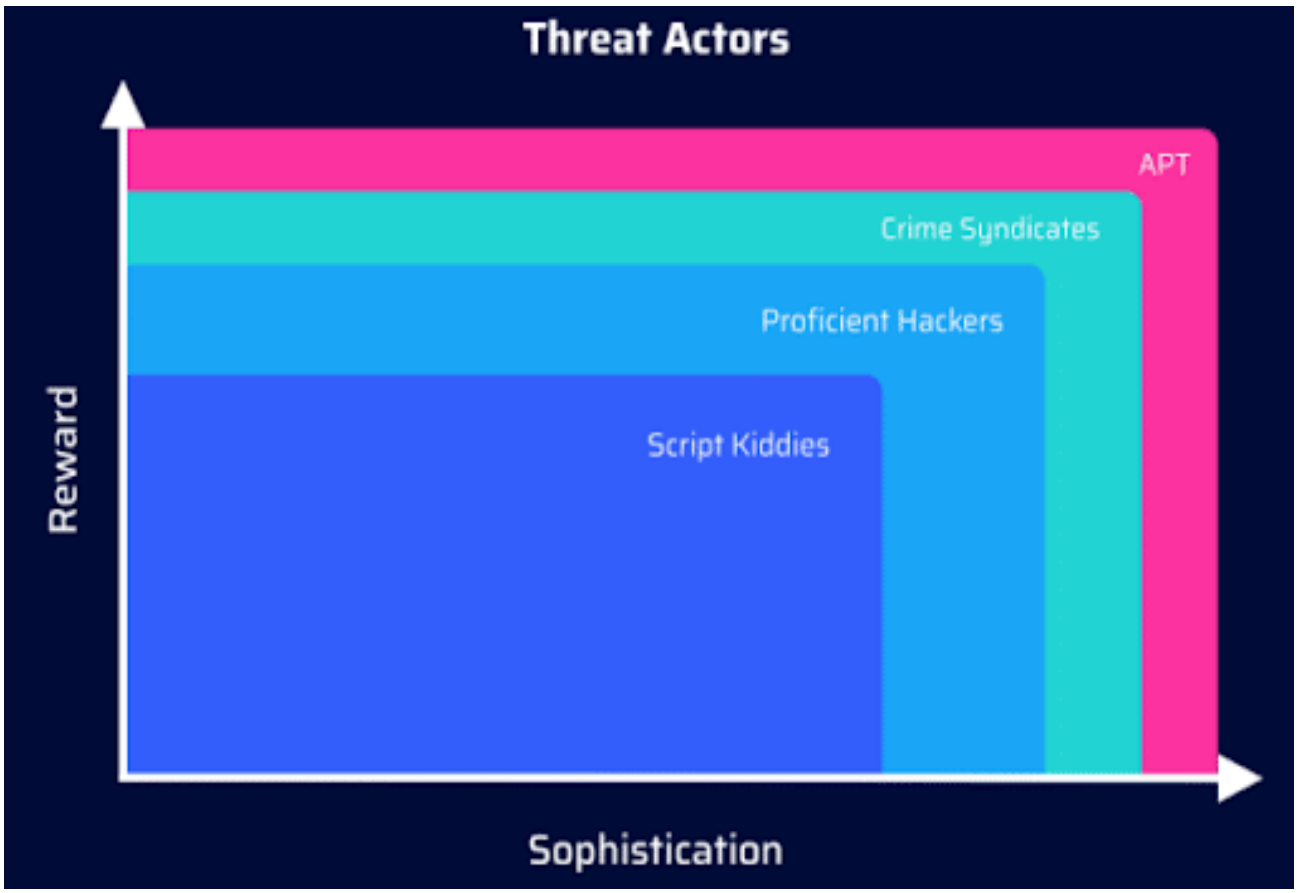
Οι κατηγορίες των Εισβολέων υπολογιστικών συστημάτων στον Σκοτεινό Ιστό, ποικίλλουν σε πολυπλοκότητα από τους εντελώς αρχάριους έως τους πλέον εξειδικευμένους Hackers, ορισμένοι εκ των οποίων υποστηρίζονται και από τα κράτη-έθνη. Μερικές από τις κύριες κατηγορίες Χάκερ στον σκοτεινό ιστό είναι οι εξής:

- **Script Kiddies:** Πρόκειται για σχετικά ανειδίκευτα άτομα, με ελάχιστη ή καθόλου γνώση και εμπειρία στο Hacking, που χρησιμοποιούν σενάρια ή προγράμματα που έχουν αναπτυχθεί από άλλους, κυρίως για κακόβουλους σκοπούς. Συνήθως, χρησιμοποιούν τον σκοτεινό ιστό για να βρουν εργαλεία Hacking και πληροφορίες σχετικά με τον τρόπο εκτέλεσης διαφορετικών τύπων επιθέσεων [HACK.2].

- **Proficient Hackers:** Πρόκειται για πολύ εξειδικευμένα άτομα, τα οποία εργάζονται μόνα τους ή σε μικρές ομάδες και διαθέτουν ένα πολύ καλό επίπεδο γνώσεων Hacking. Συνήθως χρησιμοποιούν τον σκοτεινό ιστό για αναζήτηση εργαλείων και σχετικών πληροφοριών για να διεισδύσουν σε υπολογιστικά συστήματα. Δύναται επί πλέον να αγοράσουν ή και να πουλήσουν πληροφορίες σχετικές για διάφορους οργανισμούς ή λογαριασμούς χρηστών εν δυνάμει Στόχους για επιθέσεις [HACK.3].
- **Crime Syndicates:** Οργανωμένα Συνδικάτα στον τομέα του Κυβερνοεγκλήματος, τα οποία έχουν υψηλό χρηματικό όφελος. Χρησιμοποιούν προηγμένη τεχνολογία και επιχειρούν σε ευρεία κλίμακας ηλεκτρονικής επίθεσης, σε σχέση με τους μεμονωμένους ή μικρές ομάδες Hackers.
- **Advanced Persistent Threats** (APT): Οι είναι ο πιο εξελιγμένος τύπος Hacker, που μπορεί κανείς να συναντήσει στο Dark Web. Μπορεί να αφορά ένα κράτος - έθνος ολόκληρο ή να είναι μία ομάδα, που να υποστηρίζεται από το κράτος. Αποκτούν μη εξουσιοδοτημένη πρόσβαση σε ένα δίκτυο υπολογιστών και παραμένουν απαρατήρητοι για πολύ μεγάλο χρονικό διάστημα, καθιστώντας την παρουσία τους δύσκολη ή αδύνατο να εντοπιστεί [HACK.4].

Οι προαναφερθέντες κατηγορίες Hackers έχουν διαφορετική προσέγγιση αναζήτησης κακόβουλων λογισμικών στον Σκοτεινό Ιστό, π.χ. οι Hacker, τύπου script kiddies είναι πιο πιθανό να αναζητούν λογισμικά που παρακάμπτουν τους κωδικούς πρόσβασης (crackers), ενώ οι Hackers, τύπου APT αναζητούν τρόπους για να σπάσουν τον κώδικα ενός λογισμικού μέσω μίας ευπάθειας (zero-day) του συστήματος. Η Google έχει δημιουργήσει μία την Ομάδα Project Zero, με σκοπό να εντοπίζει zero-day ευπάθειες και να διασφαλίζει την απόλυτη ασφάλεια στα προϊόντα της.

Τα Κακόβουλα λογισμικά είναι γενικά τα μόνα με πρόσβαση σε πολλά exploits zero-day. Στις περισσότερες περιπτώσεις, κακόβουλο λογισμικό επίθεσης (Ransomware), που "κλειδώνει" την οθόνη ή κρυπτογραφεί τα δεδομένα που είναι αποθηκευμένα σε ένα δίσκο, με σκοπό τον εκβιασμό ή να ζητηθούν λύτρα βρίσκεται στα χέρια είτε των **Crime Syndicates** είτε των APT.



Εικόνα 4-1 Κατηγορίες Εισβολέων Υπολογιστικών Συστημάτων

Πηγή: https://www.cybersixgill.com/wp-content/uploads/2021/10/Threat-Actors-Graph.png.webp

4.2 Υπολογιστικά Εργαλεία που Χρησιμοποιούν οι Hackers

Ορισμένα υπολογιστικά εργαλεία που χρησιμοποιούνται από τους Hackers για να εισβάλλουν σε ένα Δίκτυο Υπολογιστών είναι τα ακόλουθα:

- **Σκουλήκι υπολογιστή** (computer worm) είναι ένα αυτοαναπαραγόμενο και κακόβουλο πρόγραμμα υπολογιστή, το οποίο χρησιμοποιεί δίκτυο υπολογιστών για να στείλει αντίγραφα του εαυτού του σε κόμβους (υπολογιστές του δικτύου), που μπορεί να το πράξει χωρίς την παρέμβαση του Χρήστη. Το γεγονός αυτό οφείλεται σε κενά ασφαλείας του υπολογιστή προορισμού. Ο πραγματικός λόγος για τον οποίο δημιουργούνται είναι συνήθως κρυφός. Η φιλοσοφία της δημιουργίας ενός τέτοιου προγράμματος είναι να αποκτήσει κανείς πληροφορίες. Υπάρχουν περιπτώσεις όπου είναι δυνατή η ταυτόχρονη χρήση πολλών τέτοιων προγραμμάτων. Το μεγαλύτερο πλεονέκτημα των σκουληκιών είναι ότι μπορούν να λειτουργήσουν ανεξάρτητα από εξωτερικές «βοήθειες» ή από συνεχή επίβλεψη. Είναι δυνατόν να λειτουργήσουν με

εσωτερικό μηχανησμό, ο οποίος θα ‘’υποδείξει’’» την στιγμή που πρέπει να δράσουν [HACK.5].

- **Ιός Υπολογιστή** (Virus) είναι ένα κακόβουλο πρόγραμμα υπολογιστή, το οποίο μπορεί να αντιγραφεί και να «μολύνει» τον υπολογιστή, χωρίς τη γνώση ή την άδεια του Χρήστη του. Ο ιός μπορεί να τροποποιήσει τα αρχεία του υπολογιστή και να διαδοθεί από έναν υπολογιστή σε τρίτους. Οι ιοί ορισμένες φορές εσφαλμένα συγχέονται με τα ‘’σκουλήκια’’ υπολογιστών (worms) και τους δούρειους ίππους (trojan horses). Πολλοί προσωπικοί υπολογιστές συνδέονται, πλέον, με το Διαδίκτυο, καθώς και σε τοπικά δίκτυα, ώστε να διευκολύνουν έτσι τη διάδοση του κακόβουλου κώδικα. Σήμερα, οι ιοί μπορούν να εκμεταλλευθούν τις υπηρεσίες του Διαδικτύου, το World Wide Web, το ηλεκτρονικό ταχυδρομείο και την υπηρεσία συνομιλιών (Internet Relay Chat, IRC) [HACK.6].

- **Δούρειος Ίππος** (Trojan Horse) είναι προγράμματα που λειτουργούν ως κερκόπορτες σε ένα σύστημα υπολογιστή. Ο Hacker μεταμφιέζει τον ίππο σε ένα άλλο πρόγραμμα, π.χ. ένα παιχνίδι, με σκοπό ο Χρήστης να ξεγελαστεί και να εγκαταστήσει το πρόγραμμα. Μόλις, ο ίππος εγκατασταθεί στον υπολογιστή του θύματος, ο Hacker αποκτά πρόσβαση στο σκληρό δίσκο ή στο e-mail του Χρήστη. Με αυτόν τον τρόπο ο ο Hacker μπορεί να αποκτήσει πρόσβαση και σε άλλα συστήματα ή και να πραγματοποιήσει DoS επιθέσεις. Ο ίππος αντικαθιστά τα μηνύματα που εμφανίζονται όταν ζητείται ένα συνθηματικό από τον χρήστη. Οι Χρήστες παρέχουν τα ονόματα Χρήστη και τους κωδικούς πρόσβασης, πιστεύοντας ότι συνδέονται στο σύστημα, ενώ στην ουσία αυτά καταγράφονται από τον ίππο, επ΄ ωφελεία του Hacker [HACK.7].

- **Ανίχνευση Θυρών** (Port Scanning) είναι μία από τις πιο δημοφιλείς τεχνικές ανίχνευσης ανοικτών δικτυακών θυρών, που χρησιμοποιείται από τους εισβολείς με Στόχο την άντληση πληροφοριών σε ένα απομακρυσμένο δίκτυο (remote network) Όλα τα μηχανήματα που βρίσκονται συνδεδεμένα σε ένα τοπικό δίκτυο (LAN – Local Area Network) ή στο Διαδίκτυο τρέχουν υπηρεσίες, οι οποίες ‘’ακούνε’’ σε κάποιες γνωστές ή μη θύρες (ports). Η σάρωση της θύρας (port scanning) βοηθά τον εισβολέα να βρει όσες είναι διαθέσιμες και ελεύθερες, ώστε να αποκτήσει πρόσβαση στον υπολογιστή κάποιου Χρήστη και να λειτουργήσει κακόβουλα. Η τεχνική του «Port Scanning» προσπαθεί να ανιχνεύσει τις αδυναμίες του Χρήστη, ενώ η αποστολή μηνύματος ανίχνευσης σε μία θύρα, καθώς και η απάντηση στο απεσταλμένο μήνυμα καταδεικνύει την κατάσταση στην οποία βρίσκεται (ανοικτή ή κλειστή). Επιπλέον, συλλέγονται πληροφορίες για το είδος του λειτουργικού συστήματος, το οποίο

χρησιμοποιεί ο Χρήστης και δεδομένα τα οποία πιθανόν να χρησιμοποιηθούν μελλοντικά [HACK.8].

4.3 Υπηρεσίες που παρέχονται από Hackers σε Τρίτα Άτομα

Υπάρχει πλήθος υπηρεσιών που προσφέρονται από τους Hackers σε τρίτα πρόσωπα, με την καταβολή του κατάλληλου χρηματικού αντιτίμου. Ορισμένες εξ΄ αυτών είναι οι εξής:

- **Εκτεθειμένα Διαπιστευτήρια** (Credentials), δηλαδή ενός τμήματος οποιουδήποτε εγγράφου, ή πληροφορίας, που αφορά την εξουσιοδότηση που έχει εκδοθεί σε ένα άτομο από ένα άλλο ή από κάποια σχετική αρχή. Τα διαπιστευτήρια ως προϊόντα κυβερνοεπιθέσεων πωλούνται συνήθως σε αγορές του Σκοτεινού Ιστού.

  Τα εκτεθειμένα διαπιστευτήρια μπορούν να χρησιμοποιηθούν για την παράνομη πρόσβαση σε έναν λογαριασμό ή εναλλακτικά για επιθέσεις δοκιμής σε άλλους λογαριασμούς, οι οποίοι χρησιμοποιούν τα ίδια διαπιστευτήρια.

  Σχετικές πληροφορίες με κλεμμένα διαπιστευτήρια αποτελούν σημαντικό υλικό για να αναπτυχθούν αντίμετρα ή και να βελτιωθούν οι πολιτικές δημιουργίας κωδικών πρόσβασης στα Πληροφοριακά Συστήματα [HACK.9].

- **Στοχευμένες Επιθέσεις** (Targeted Attacks)

  Οι εγκληματίες του κυβερνοχώρου στοχεύουν προς την κατεύθυνση οι υπηρεσίες που προσφέρουν να τελούν υπό καθεστώς πώλησης, κυρίως στις αγορές του Σκοτεινού Ιστού. Χαρακτηριστικό παράδειγμα αποτελεί ένα χειριστής Botnet, ο οποίος δύναται να πουλά επιθέσεις κατανεμημένης άρνησης υπηρεσίας (DoS), όπου ο αγοραστής μπορεί να επιλέξει το χρόνο, τη διάρκεια και την ένταση της επίθεσης εναντίον ενός Στόχου της επιλογής του, με διαφορετικό χρηματικό αντίτιμο. Ένα άλλο παράδειγμα αποτελεί όταν ένας αγοραστής μπορεί να είναι σε θέση να αγοράσει ένα προσαρμοσμένο πακέτο ηλεκτρονικής επίθεσης σε έναν λογαριασμός ενός άλλου σε Μέσα Κοινωνικής Δικτύωσης.

  Πληροφορίες σχετικές με το ενδεχόμενο μίας στοχευμένη DoS επίθεσης από έναν αγοραστή είναι μείζονος σημασίας για τον οργανισμό που πρόκειται να στοχοποιηθεί και ως εκ τούτου κοστίζουν ακριβά όταν τίθενται προς πώληση [HACK.10].

- **Πληροφορίες Τρωτότητας** (Vulnerability Information)

  Τα τρωτά σημεία ενός λογισμικού δύναται να διευκολύνουν έναν εισβολέα να έχει πρόσβαση σε δίκτυα και συσκευές εταιριών. Στην περίπτωση που κάποιος ηθικός Hacker αναφέρει την ευπάθεια ενός συστήματος, τότε αυτή δεν κοινοποιείται μέχρι να διορθωθεί ο κώδικας με νέο λογισμικό αναβάθμισης.

  Στο Dark Web υπάρχουν ειδικά φόρουμ συζητήσεων, όπου οι Hackers ανταλλάζουν σχετικές πληροφορίες για τον τρόπο λειτουργίας μιας ευπάθειας ενός συστήματος, καθώς και για τους τρόπους πιθανής εκμετάλλευσης και χρήση αυτής σε διάφορες εκστρατείες κυβερνοεπιθέσεων, κτλ.

  Συνεπώς, η συμμετοχή σε αυτά τα κανάλια συζητήσεων δύναται να υποβοηθήσει έναν οργανισμό να προλάβει εγκαίρως τυχόν ευπάθειες του κώδικα ενός συστήματος, με συνεχείς βελτιωμένες ενημερώσεις του εν λόγω κώδικα.

- **Εσωτερικές Απειλές** (Insider Threats)

  Η εσωτερική απειλή σε έναν οργανισμό αποτελεί ένας, νυν ή πρώην, υπάλληλος, συνεργάτης, πωλητής ή και μεταπωλητές, οι οποίο έχουν πρόσβαση σε ‘’ευαίσθητα’’ δεδομένα της επιχείρησης. Οι εν λόγω απειλές δύναται να θέσουν τον οργανισμό σε κίνδυνο είτε εκ προθέσεως είτε από αμέλεια.

  Πληροφορίες που αφορούν ‘’ευαίσθητα’’ δεδομένα ενός οργανισμού μπορεί να βρεθούν στα χέρια Hackers, οι οποίοι έναντι αδρής αμοιβής να τα θέσουν προς πώληση σε αγορές σκοτεινού ιστού [HACK.11].

- **Παραβιασμένοι Λογαριασμοί** (Hacked Accounts)

  Λογαριασμοί τέτοιου τύπου, πωλούνται συνήθως σε αγορές στον Σκοτεινό Ιστό, δίνοντας πρόσβαση σε προσωπικούς ή εταιρικούς λογαριασμούς, email, μέσα κοινωνικής δικτύωσης, ιστότοπους ηλεκτρονικού εμπορίου, κτλ.

  Συνεπώς, είναι πολύ σημαντικό να προστατεύονται τα δίκτυα ενός οργανισμού από κακόβουλες ενέργειες που αφορούν την πώληση από τρίτους κωδικών πρόσβασης και επαναφοράς ηλεκτρονικών λογαριασμών ταχυδρομείου [HACK.12].

- **Διαδικτυακά Δίκτυα** (Botnet)

  Πρόκειται για ομάδες συσκευών συνδεδεμένων στο Διαδίκτυο , καθεμία από τις οποίες εκτελεί ένα ή περισσότερα bot. Τα botnets μπορούν να χρησιμοποιηθούν για την εκτέλεση αυτοματοποιημένων επιθέσεων Distributed Denial-of-Service (DDoS), την κλοπή δεδομένων, αποστολή ανεπιθύμητων μηνυμάτων και για να επιτρέψουν στον εισβολέα να έχει πρόσβαση σε μία συσκευή ή και δίκτυο. Ο εισβολέας μπορεί να ελέγξει το botnet χρησιμοποιώντας λογισμικό εντολών και ελέγχου, με σκοπό να εκμεταλλευτεί μια ευπάθεια σε μια συσκευή για να αποκτήσει τον έλεγχο ενός συνόλου ευάλωτων συσκευών. Αυτές οι συσκευές IoT μπορούν στη συνέχεια να χρησιμοποιηθούν για άρνηση υπηρεσίας (DoS), υποκλοπή κωδικών αυθεντικοποίησης και άλλων αυτοματοποιημένων επιθέσεων. Η λέξη "botnet" είναι σύνθετη των λέξεων "ρομπότ" και "δίκτυο". Ο όρος χρησιμοποιείται συνήθως με αρνητική ή κακόβουλη χροιά. Στο Σκοτεινό Ιστό δύναται να διεξαχθούν πωλήσεις μικρών ομάδων δικτύων bots σε άλλα σε εγκληματίες του κυβερνοχώρου, οι οποίοι θέλουν να τις χρησιμοποιήσουν σε ηλεκτρονικές επιθέσεις, δύσκολα ανιχνεύσιμες [HACK.13].

4.4 Χαρακτηριστικές Τακτικές και Τεχνικές Διείσδυσης σε Δίκτυα Υπολογιστών

Ορισμένες τακτικές και τεχνικές, που χρησιμοποιούνται από κακόβουλους εισβολείς σε Συστήματα και Δίκτυα Υπολογιστών είναι οι εξής [HACK.14 έως 18]:

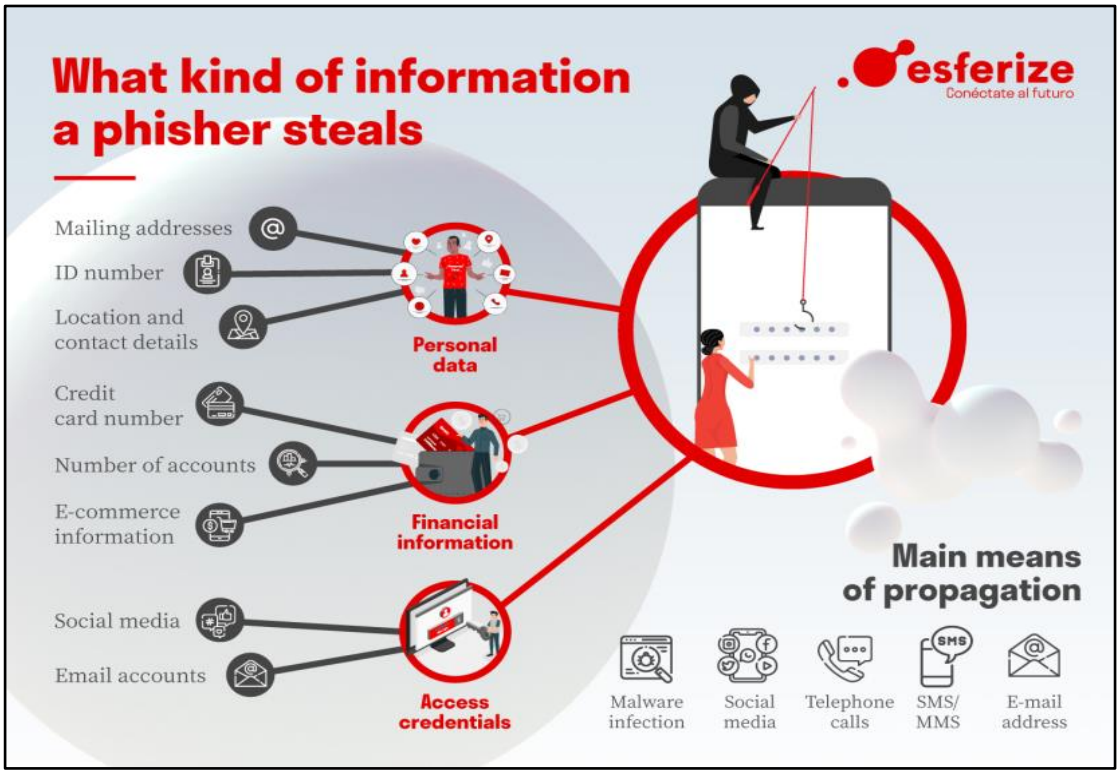
- Η **τακτική της Αναγνώρισης** (*Reconnaissance*): Είναι τακτική που αφορά τεχνικές σάρωσης, αποστολής κακόβουλου λογισμικού, κ.ά, για την συλλογή, ενεργητικά ή παθητικά, πληροφοριών, πλήρως αξιοποιήσιμων, σχετικών με την οργάνωση, υποδομή, αρχιτεκτονική, ευπαθών σημείων και άλλων συναφών διαπιστευτηρίων, DNS[3], IPs, emails, ονόματα χρηστών, με σκοπό την υποστήριξη μελλοντικών επιχειρήσεων προσβολής δικτύων. Ενδεικτικές τεχνικές Αναγνώρισης είναι οι ακόλουθες:

  - **Η τεχνική της Ενεργής Σάρωσης** (*Active Scanning*): Είναι τεχνική με την οποία ο αντίπαλος εκτελεί ενεργητικές αναγνωριστικές σαρώσεις ελέγχου της κυκλοφορίας δικτύων υπολογιστών για την συλλογή κρίσιμων πληροφοριών, με σκοπό την μελλοντική προσβολή τους. Οι σαρώσεις αυτές εκμεταλλεύονται

[3] https://en.wikipedia.org/wiki/Domain_Name_System

προϋπάρχοντα πρωτόκολλα, ανταλλαγής μηνυμάτων λάθους, π.χ. Internet Control Message Protocol (ICMP)[4], Transmission Control Protocol (TCP)[5], και User Datagram Protocol (UDP)[6], κτλ., με σκοπό την αποκάλυψη κενών ασφαλείας του Δικτύου - Στόχου.

- **Η τεχνική του Ψαρέματος Πληροφοριών** (*Phishing for Information*): Είναι τεχνική με την οποία ο αντίπαλος προβαίνει σε ηλεκτρονικό στοχευμένο (spear phishing) ή μη ψάρεμα, δηλαδή στην εξαπάτηση του Στόχου, με σκοπό την αποκάλυψη κρίσιμων πληροφοριών ευαίσθητου περιεχομένου π.χ. διαπιστευτηρίων, κωδικών, πιστοποιητικών, κτλ. Το ηλεκτρονικό ψάρεμα για πληροφορίες διαφέρει από το "ψάρεμα" καθώς ο σκοπός είναι η συλλογή δεδομένων από το Θύμα - Στόχος και όχι η εκτέλεση κακόβουλου κώδικα. Ο αντίπαλος δύναται να αποσπά πληροφορίες, μέσω ψεύτικών λογαριασμών, ανταλλαγής email, άμεσων, πολλαπλών και φαινομενικά επειγόντων μηνυμάτων ή άλλων μέσων ηλεκτρονικής συνομιλίας.



Εικόνα 4-2 Η τεχνική του Ψαρέματος Πληροφοριών

Πηγή:

https://www.esferize.com/wp-content/uploads/2021/07/What-information-steals-a-phisher.png

[4] https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol
[5] https://en.wikipedia.org/wiki/Transmission_Control_Protocol
[6] https://en.wikipedia.org/wiki/User_Datagram_Protocol

- Η **τακτική της Ανάπτυξης Πόρων** (*Resource Development*): Είναι τακτική μέσω της οποίας ο επιτιθέμενος προσπαθεί να δημιουργήσει πόρους, ώστε να τους χρησιμοποιήσει για να υποστηρίξει μελλοντικές επιχειρήσεις προσβολής δικτύων υπολογιστών. Περιλαμβάνει τεχνικές υποκλοπής κρίσιμων και αξιοποιήσιμων δεδομένων και πληροφοριών π.χ. υποδομών, λογαριασμών χρηστών, πιστοποιητικών υπογραφής, emails κτλ, με μακροπρόθεσμο σκοπό την μεμακρυσμένη Διοίκηση (*Command*) και τον εξ΄ αποστάσεως έλεγχο (*Control*) των δικτύων υπολογιστών. Ενδεικτικές τεχνικές Ανάπτυξης Πόρων είναι οι ακόλουθες:
  - **Η τεχνική της Απόκτησης Υποδομών** (*Acquire Infrastructure*): Είναι τεχνική με την οποία ο αντίπαλος προβαίνει σε αγορά, μίσθωση ή ενοικίαση υποδομής π.χ. διακομιστές, δίκτυα botnet[7], κ.ά, με σκοπό τη χρησιμοποίησή τους σε μελλοντική επιθετική ενέργεια εναντίον δικτύων υπολογιστών. Υπάρχει μεγάλη ποικιλία διαθέσιμων υποδομών για ενοικίαση ή αγορά με σκοπό την εκμετάλλευσή τους από κάποιον επιβουλέα. Ο αντίπαλος αποκαθιστά φυσική σύνδεση (*μερική, ολική ή για μικρό χρονικό διάστημα*) με την υποδομή.
  - **Η τεχνική της Υπονόμευσης Λογαριασμών** (*Compromise Accounts*): Είναι τεχνική με την οποία ο αντίπαλος παραβιάζει λογαριασμούς για να τους χρησιμοποιήσει μελλοντικά στην επιθετική ενέργειά του εναντίον ενός δικτύου υπολογιστών. Χρησιμοποιεί μέσα κοινωνικής δικτύωσης και ιστότοπους π.χ. Facebook, LinkedIn, Twitter, Google για να προβεί σε ηλεκτρονικό ψάρεμα (*phishing for Information*), σε δημιουργία ψεύτικων λογαριασμών, σε συλλογή ή και αγορά διαπιστευτηρίων από ιστότοπους τρίτων, σε υποκλοπές κωδικών εισόδου, κ.ά. Πριν την παραβίαση των λογαριασμών ο αντίπαλος προβαίνει σε αναγνωριστική προσέγγιση για το ποιοι λογαριασμοί θα παραβιαστούν ή όχι και για ποιο λόγο.

[7] https://en.wikipedia.org/wiki/Botnet

- Η **τακτική της Αρχικής Πρόσβασης** (*Initial Access*): Είναι τακτική μέσω της οποίας ο επιτιθέμενος προσπαθεί να εισέλθει σε πρώτο στάδιο στο Δίκτυο - Στόχος. Αποτελείται από τεχνικές π.χ. στοχευμένο ψάρεμα (spearphishing), εκμετάλλευση αδυναμιών διακομιστών ιστού, κ.ά, που χρησιμοποιούν διάφορα κανάλια εισόδου για να αποκτήσουν την πρώτη επαφή (*βάση*), συνεχόμενης ή περιορισμένης χρήσης, με το υποψήφιο δίκτυο υπολογιστών προς προσβολή. Ενδεικτικές τεχνικές Αρχικής Πρόσβασης είναι οι ακόλουθες:
  - **Η τεχνική Έγκυρων Λογαριασμών** (*Valid Accounts*): Είναι τεχνική μέσω της οποίας ο επιτιθέμενος προσπαθεί να υποκλέψει διαπιστευτήρια εισόδου έγκυρων ανενεργών χρηστών λογαριασμών τρίτων προσώπων, μειώνοντας την πιθανότητα εντοπισμού του, λόγω του ηλεκτρονικού αποτυπώματος που αφήνει. Τα διαπιστευτήρια αυτά υπηρεσιών, όπως VPN, Outlook Web Access, επιφάνεια εργασίας, κ.ά, μπορούν να χρησιμοποιηθούν για την παράκαμψη στοιχείων ελέγχου πρόσβασης, σε μόνιμη ή όχι βάση, σε απομακρυσμένα συστήματα δικτύων υπολογιστών. Ο αντίπαλος αποκτά με αυτήν τακτική ισχυρό πλεονέκτημα καθώς έχει πρόσβαση σε τοπικό και διαχειριστικό επίπεδο σε κρίσιμους λογαριασμούς.
  - Η **τεχνική των Εξωτερικών Απομακρυσμένων Υπηρεσιών** (*External Remote Services*): Είναι τεχνική μέσω της οποίας ο επιτιθέμενος προσπαθεί να αξιοποιήσει εξωτερικές απομακρυσμένες υπηρεσίες, με σκοπό να αποκτήσει αρχική πρόσβαση, προσωρινή ή συνεχόμενη, σε δίκτυα υπολογιστών. Τέτοιες σχετικές υπηρεσίες, όπως τα VPN, Citrix επιτρέπουν στους Χρήστες να συνδέονται με πόρους εταιρικών δικτύων υπολογιστών από εξωτερικές τοποθεσίες, μέσω απομακρυσμένων πυλών υπηρεσιών, οι οποίες διαχειρίζονται τις συνδέσεις και τον έλεγχο ταυτότητας διαπιστευτηρίων για αυτές τις υπηρεσίες. Η πρόσβαση σε απομακρυσμένες υπηρεσίες μπορεί να χρησιμοποιηθεί ως προσωρινός ή μόνιμος μηχανισμός κατά τη διάρκεια μιας επιθετικής ενέργειας.

- Η **τακτική της Εκτέλεσης** (*Execution*): Είναι τακτική μέσω της οποίας ο αντίπαλος προβαίνει σε τεχνικές για την αποστολή και τον έλεγχο κακόβουλου κώδικα, ο οποίος θα εκτελείται σε τοπικό ή απομακρυσμένο Σύστημα - Στόχο. Η τεχνική του κακόβουλου κώδικα, συνήθως, συνδυάζεται και με άλλες συναφείς π.χ. της εξερεύνησης δικτύου, της κλοπής δεδομένων, κ.ά., με σκοπό το αποτέλεσμα να καταστεί, κατά το μέγιστο δυνατόν, πιο διευρυμένο και συνεπώς επιτυχημένο. Χαρακτηριστικό παράδειγμα είναι ο αντίπαλος να χρησιμοποιήσει ένα εργαλείο απομακρυσμένης πρόσβασης, ώστε να εκτελέσει μια δέσμη ενεργειών (*PowerShell Script*)[8], που εκτελεί απομακρυσμένη ανίχνευση συστήματος (*Remote System Discovery*). Ενδεικτικές τεχνικές Εκτέλεσης είναι οι ακόλουθες:
    - Η **τεχνική των Υπηρεσιών Συστήματος** (*System Services*): Οι κακόβουλοι λειτουργούν ως διαχειριστές ενός Συστήματος και χρησιμοποιούν το δωρεάν εργαλείο PsExec[9] του Sysinternals της Microsoft, με σκοπό την εκτέλεση ενός προγράμματος εντολών (*scripts*)[10] σε άλλον υπολογιστή, μέσω μιας μεθόδου που αλληλοεπιδρά με την υπηρεσία Service Control Manager[11] των Windows (*είτε με τη δημιουργία μιας νέας υπηρεσίας είτε με την τροποποίηση μιας υπάρχουσας*). Η τεχνική εκτέλεσης κακόβουλου κώδικα συνήθως συνδυάζεται και με άλλες συναφείς τεχνικές π.χ. της κλιμάκωσης προνομίου (*privilege escalation*)[12], της επιμονής (*persistency*)[13], κ.ά.
    - **Η τεχνική του Κελύφους Εντολής και Κώδικα Διερμηνέα** (*Command and Scripting Interpreter*): Είναι η τεχνική με την οποία ο αντίπαλος χρησιμοποιεί ένα πρόγραμμα διαχείρισης αυτοματισμού και διαμόρφωσης εργασιών PowerShell[14] της Microsoft. Το εν λόγω PowerShell αποτελείται από ένα κέλυφος γραμμής εντολών και μία δέσμης ενεργειών. Χαρακτηριστικά παραδείγματα είναι τα Start-Process cmdlet, που μπορεί να χρησιμοποιηθεί για την εκτέλεση ενός εκτελέσιμου αρχείου και το Invoke-Command cmdlet, που εκτελεί μια εντολή τοπικά ή σε απομακρυσμένο υπολογιστή. Το PowerShell μπορεί επίσης να χρησιμοποιηθεί για την λήψη εκτελέσιμων αρχείων από το Διαδίκτυο και την

[8] https://en.wikipedia.org/wiki/PowerShell
[9] https://docs.microsoft.com/en-us/sysinternals/downloads/psexec
[10] https://en.wikipedia.org/wiki/Script
[11] https://docs.microsoft.com/el-gr/windows/win32/services/service-control-manager
[12] https://en.wikipedia.org/wiki/Privilege_escalation
[13] https://en.wikipedia.org/wiki/Persistence_(computer_science)
[14] https://en.wikipedia.org/wiki/PowerShell

εκτέλεση αυτών από το δίσκο ή στη μνήμη του συστήματος, χωρίς να έχει ο επιτιθέμενος πρόσβαση στο δίσκο.

- **Η τακτική της Επιμονής** (*Persistence*): Είναι τακτική μέσω της οποίας ο αντίπαλος προβαίνει σε τεχνικές για την τροποποίηση των παραμέτρων του συστήματος, με σκοπό την απόκτηση μόνιμης πρόσβασης σε αυτό. Σε περίπτωση συνεχών επανεκκινήσεων και συχνών αλλαγών των διαπιστευτηρίων του Συστήματος - Στόχου ο επιτιθέμενος ασκεί επίμονα προσπάθεια για την οριστική πρόσβαση στο Δίκτυο - Στόχος. Η πρόσβαση δύναται να χαθεί λόγω συχνών επανεκκινήσεων του συστήματος, της απώλειας των διαπιστευτηρίων ή άλλων ενεργειών του αμυνομένου. Ενδεικτικές τεχνικές Επιμονής είναι οι ακόλουθες:

  - Η **τεχνική της Δημιουργίας ή Τροποποίησης Λειτουργίας Συστήματος** (*Create or Modify System Process*): Είναι η τεχνική με την οποία ο αντίπαλος μπορεί να δημιουργήσει ή να τροποποιήσει τις διεργασίες π.χ. Launch Daemon[15] και Launch Agent, κ.τ.λ, που αφορούν στην προετοιμασία, εκκίνηση και φόρτωση των παραμέτρων ενός λειτουργικού συστήματος (*Windows και Linux*), με σκοπό να εκτελείται επαναλαμβανόμενα ένα κακόβουλο λογισμικό. Ο αντίπαλος δύναται να εγκαταστήσει ‘’δαίμονες – πράκτορες’’ με δικαιώματα διαχειριστή root/SYSTEM[16], κατάλληλα ρυθμίσιμους, ώστε να εκτελούνται κατά την εκκίνηση ή για ένα επαναλαμβανόμενο χρονικό διάστημα.

  - Η **τεχνική της Εμφύτευσης Εικόνας** (*Implant Internal Image*): Είναι η τεχνική με την οποία ο αντίπαλος μπορεί να αποστείλει ηλεκτρονικές εικόνες, με σκοπό να εμφυτεύσει διεπαφές, τύπου κέλυφους ιστού, Web Shell[17], οι οποίες να αλληλεπιδρούν με τον διακομιστή ιστού, ώστε να καταστεί ικανός να λαμβάνει, να εκτελεί και να διαγράφει αρχεία από και προς αυτόν. Τα εν λόγω WebShell, συνήθως, είναι γραμμένα σε γλώσσες προγραμματισμού PHP[18]. Ο εισβολέας μπορεί να βρει τρωτά σημεία των εφαρμογών, που εκτελούνται σε διακομιστές Web, καθώς και κενά ασφαλείας, προκειμένου να εμφυτέψει κέλυφα ιστού. Επιπλέον, ο επιτιθέμενος δύναται να χρησιμοποιεί και λογισμικά τύπου Docker[19], τα οποία θα λειτουργούν ως κερκόπορτα, με σκοπό να πετύχει τον απομακρυσμένο έλεγχο ενός δικτύου υπολογιστή.

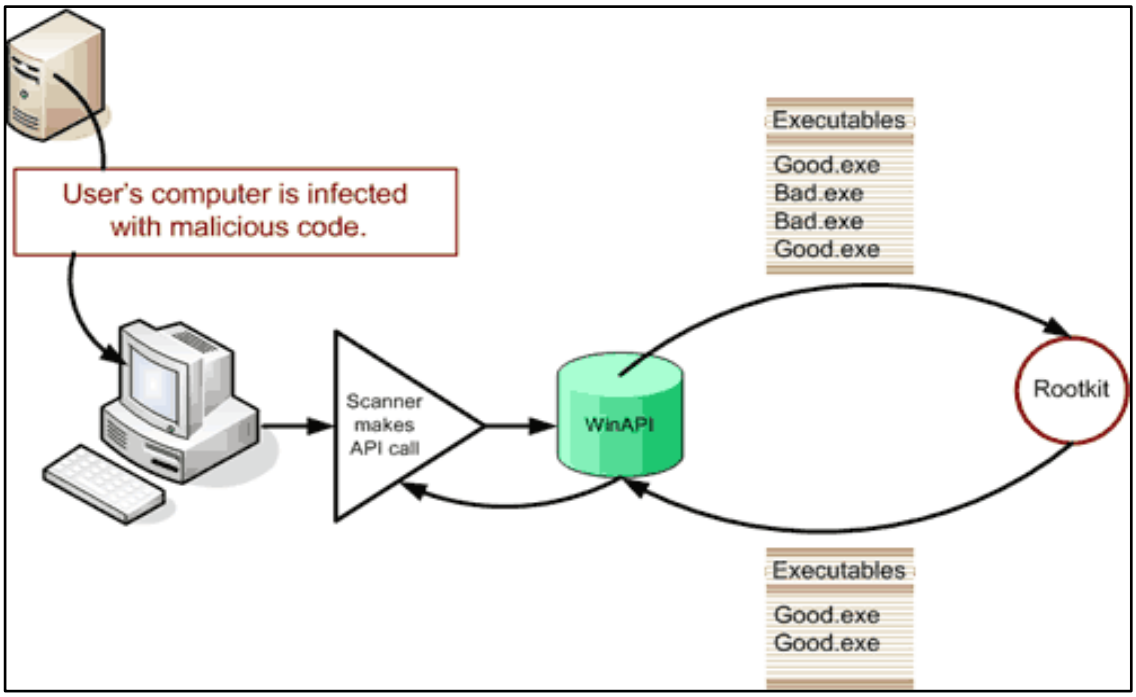
[15] https://en.wikipedia.org/wiki/Launchd
[16] https://en.wikipedia.org/wiki/Root_system
[17] https://en.wikipedia.org/wiki/Web_shell
[18] https://en.wikipedia.org/wiki/PHP
[19] https://en.wikipedia.org/wiki/Docker_(software)

- **Η τακτική της Επαύξησης Δικαιωμάτων** (*Privilege Escalation*): Είναι τακτική μέσω της οποίας ο αντίπαλος προβαίνει σε τεχνικές για την απόκτηση υψηλότερου επιπέδου δικαιωμάτων από ένα Χρήστη σε ένα υποψήφιο Σύστημα – Στόχος, με σκοπό την εκτέλεση απομακρυσμένης λειτουργίας αυτού. Ενδεικτικές τεχνικές Επαύξησης Δικαιωμάτων είναι οι ακόλουθες:
  - Η **τεχνική της Εκτέλεσης Πειρατείας** (*Hijack Execution Flow*): Είναι η τεχνική, με την οποία ο αντίπαλος μπορεί να εκτελέσει κακόβουλο κώδικα, με σκοπό να παραβιάσει τις άμυνες και τον μηχανισμό ασφαλείας των προγραμμάτων που εκτελούνται σε λειτουργικά συστήματα. Ο επιβουλέας δύναται να δηλητηριάζει με κακόβουλο λογισμικό τις βιβλιοθήκες, τους καταλόγους αρχείων, καθώς και το μητρώο των λειτουργικών συστημάτων. Συνήθως, η εν λόγω τεχνική επαναλαμβάνεται σε τακτά χρονικά διαστήματα.
  - Η **τεχνική της Έγχυσης Διαδικασίας** (*Process Injection*): Είναι η τεχνική, με την οποία ο αντίπαλος μπορεί να εγχύσει πολλαπλές διαδικασίες εκτέλεσης κώδικα σε τμηματικές μονάδες του συστήματος ή και σε μηχανισμούς διαδιεργασιακής επικοινωνίας, Inter-process communication (IPC)[20], προκειμένου να καταστείλει τις άμυνες ενός δικτύου υπολογιστών. Η ένεση κακόβουλου κώδικα είναι μία τεχνική εκτέλεσης γραμμών κώδικα, στο σύνολο του υπάρχοντος κώδικα, επιτρέποντας στον αντίπαλο να επιχειρεί σε νόμιμο πλαίσιο, αυξάνοντας τα δικαιώματα πρόσβασής του στο Δίκτυο - Στόχος και αποφεύγοντας τον εύκολο εντοπισμό του.
- **Η τακτική της Αποφυγής της Άμυνας Συστημάτων** (*Defense Evasion*): Είναι τακτική μέσω της οποίας ο αντίπαλος προβαίνει σε τεχνικές απεγκατάστασης, απενεργοποίησης και εγκατάστασης λογισμικού ασφαλείας, καθώς και σε τεχνικές συσκότισης, κρυπτογράφησης δεδομένων, αποφυγής πιστοποιημένων διεργασιών και εκτέλεσης κακόβουλου λογισμικού, με σκοπό την αποφυγή της ανίχνευσης του από τα διάφορα συστήματα άμυνας και ασφάλειας του Δικτύου - Στόχου. Ενδεικτικές τεχνικές Αποφυγής Συστημάτων Ασφαλείας είναι οι ακόλουθες:
  - Η **τεχνική του Προστατευτικού Κιγκλιδώματος** (*Execution Guardrails*): Είναι η τεχνική, με την οποία ο αντίπαλος μπορεί να διασφαλίσει ότι το κακόβουλο υλικό θα εκτελεστεί μόνο στο υποψήφιο Δίκτυο - Στόχο. Η προστασία κιγκλιδώματος χρησιμοποιείται για να οδηγήσει κακόβουλο υλικό να εκτελεστεί για το σκοπό,

[20] https://en.wikipedia.org/wiki/Inter-process_communication

που έχει σχεδιαστεί, όταν πληρούνται συγκεκριμένες συνθήκες στον υποψήφιο Στόχο, διαφορετικά δεν εκτελείται διότι υπάρχει ο κίνδυνος των παράπλευρων απωλειών και της ζημίας, τα οποία δεν είναι επιθυμητά από τον επιτιθέμενο.

- Η **τεχνική του Προνομιακού Υπερχρήστη** (*Rootkit*): Είναι η τεχνική με την οποία ο αντίπαλος μπορεί να έχει συνεχή πρόσβαση σε έναν υπολογιστή με προνόμια υπερχρήστη, χωρίς να γίνεται αντιληπτός από τους διαχειριστές του συστήματος διότι ενσωματώνεται σε βασικά στοιχεία του λειτουργικού συστήματος ή και σε άλλες εφαρμογές. Ο επιτιθέμενος εγκαθιστά ένα λογισμικό Rootkit[21], ώστε να αποκτήσει πρόσβαση σε κωδικούς και γενικά να αποκρυπτογραφήσει τα συστήματα του υπολογιστή, αποκτώντας με αυτόν τον τρόπο τον απόλυτο έλεγχο του υπολογιστή με δικαιώματα επίπεδου υπερχρήστη. Τα λογισμικά Rootkit έχουν την δυνατότητα να αποπροσανατολίσουν τα προγράμματα ασφαλείας των δικτύων υπολογιστών, διότι αποκρύπτουν την ύπαρξη κακόβουλου λογισμικού υποκλοπής, ενώ μεταξύ άλλων δύναται να τροποποιήσουν τις διεπαφές προγραμματισμού εφαρμογών, Application Programming Interface (API)[22], δηλαδή της μεταβίβασης δεδομένων μεταξύ εφαρμογών ενός λογισμικού με έναν τυποποιημένο τρόπο.



Εικόνα 4-3 Η τεχνική του RootKit

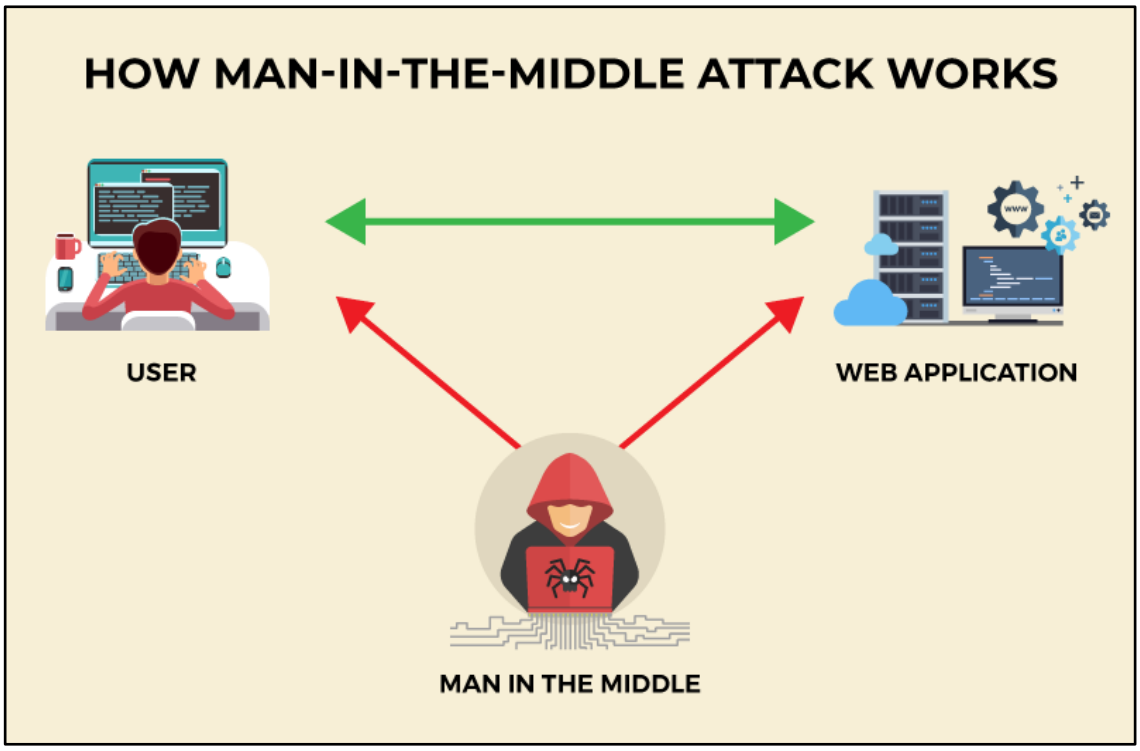
Πηγή:

http://wiki.cas.mcmaster.ca/images/2/22/Rootkit.gif

[21] https://en.wikipedia.org/wiki/Rootkit
[22] https://en.wikipedia.org/wiki/API

- **Η τακτική της Υποκλοπής Συνθηματικών** (*Credential Access*): Είναι τακτική μέσω της οποίας ο αντίπαλος προβαίνει σε τεχνικές για την πρόσβαση και τον έλεγχο ενός Συστήματος - Στόχος, μέσω υποκλοπής των διαπιστευτηρίων, των ονομάτων λογαριασμών, των κωδικών πρόσβασης και των κλειδιών, που χρησιμοποιούνται σε αυτό. Η χρήση νόμιμων διαπιστευτηρίων δίδει τη δυνατότητα στον επιτιθέμενο να αποκαλυφθεί δυσκολότερα και να δημιουργήσει νέους λογαριασμούς για την επίτευξη των τεθέντων στόχων του. Ενδεικτικές τεχνικές Υποκλοπής Συνθηματικών είναι οι ακόλουθες:

  - Η **τεχνική της Παρεμβολής του Αντίπαλου** (*Adversary-in-the-Middle*): Είναι η τεχνική με την οποία ο αντίπαλος μπορεί να προβεί σε παρεμβολή μεταξύ δύο συσκευών δικτύων, ώστε να καταστεί ικανός στην ανίχνευση δικτύων και στην μετάδοση/χειρισμό δεδομένων ενός δικτύου. Με την τεχνική αυτή, ο επιβουλέας αποκτά πρόσβαση σε κοινά πρωτόκολλα επικοινωνίας και δικτύου π.χ. ARP, DNS, LLMNR, κ.τ.λ και ως εκ τούτου δύναται να ελέγχει την ροή κυκλοφορίας του Δικτύου - Στόχος. Συνεπώς, ο επιτιθέμενος δύναται να αναγκάσει μία συσκευή να επικοινωνεί με την άλλη ώστε οι Χρήστες να λειτουργούν επ΄ ωφελεία του και να συλλέγει χρήσιμες πληροφορίες.



Εικόνα 4-4 Η τεχνική της Παρεμβολής του Αντίπαλου

Πηγή:

https://cisomag.eccouncil.org/wp-content/uploads/2021/09/MicrosoftTeams-image-28.png

- Η **τεχνική της Βίαιης Αυθεντικοποίησης** (*Force Authentication*): Είναι η τεχνική με την οποία ο αντίπαλος μπορεί να συλλέξει διαπιστευτήρια, αναγκάζοντας έναν Χρήστη να αποκαλύψει πληροφορίες αυθεντικοποίησης. Το πιο γνωστό πρωτόκολλο αυθεντικοποίησης και ελέγχου ταυτότητας Χρήστη είναι το Server Message Block (SMB)[23]. Όταν τα Windows επιχειρούν να συνδεθούν, το SBS ελέγχει την ταυτότητα Χρήστη αυτόματα, αποστέλλοντας πληροφορίες εισόδου στο σύστημα. Ο επιτιθέμενος μπορεί να εκμεταλλευτεί αυτόν τον μηχανισμό για να αποκτήσει πρόσβαση στον λογαριασμό του Χρήστη, μέσω αναγκαστικού ελέγχου ταυτότητας. Επί πλέον, ο αντίπαλος δύναται να αποστείλει ψεύτικο σύνδεσμο, μέσω μηχανισμού ψαρέματος, για να αναγκάσει τον Χρήστη να προβεί σε έλεγχο της ταυτότητάς του.

- Η **τακτική της Χαρτογράφησης Δικτύου** (*Discovery*): Είναι τακτική μέσω της οποίας ο αντίπαλος προβαίνει σε τεχνικές χαρτογράφησης του υποψήφιου Δικτύου - Στόχου, με σκοπό την απόκτηση πληροφοριών της εσωτερικής αρχιτεκτονικής αυτού ή άλλων συναφών ευρύτερων πληροφοριών για αυτό. Ο επιτιθέμενος παρατηρεί το δίκτυο που θα προσβάλει, εξετάζοντας τι μπορεί να ελέγξει και τι όχι και προσανατολίζει τις προσπάθειές του με τέτοιο τρόπο, ώστε να πετύχει το επιδιωκόμενο αποτέλεσμα με τον πιο βέλτιστο τρόπο. Ενδεικτικές τεχνικές Χαρτογράφησης Δικτύου είναι οι ακόλουθες:

  - Η **τεχνική της Ανακάλυψης Πληροφοριών Συστήματος** (*System Information Discovery*): Είναι η τεχνική με την οποία ο αντίπαλος μπορεί να συλλέξει λεπτομερείς πληροφορίες σχετικά με το λειτουργικό σύστημα και το υλικό του δικτύου, συμπεριλαμβανομένων και πληροφοριών σχετικών με την έκδοση, τις αναβαθμίσεις, την αρχιτεκτονική, κτλ., με σκοπό να διαμορφώσει πλήρη εικόνα του τρόπου ενεργείας για την προσβολή του δικτύου. Δύναται να χρησιμοποιήσει εργαλεία, όπως το Systeminfo[24] και του YaST (*System setup Configuration Tool*)[25].

[23] https://en.wikipedia.org/wiki/Server_Message_Block
[24] https://en.wikipedia.org/wiki/Systeminfo.exe
[25] https://en.wikipedia.org/wiki/YaST

- Η **τεχνική του Μητρώου Ερωτημάτων** (*Query Registry*)): Είναι η τεχνική με την οποία ο αντίπαλος μπορεί να επικοινωνήσει με το μητρώο Windows, με σκοπό να συλλέξει πληροφορίες για το σύστημα, τις ρυθμίσεις και τα εγκατεστημένα προγράμματα. Το μητρώο περιέχει σημαντικό όγκο κρίσιμων πληροφοριών, η αποκάλυψη των οποίων θα οδηγήσει τον επιτιθέμενο να ανακαλύψει τα κενά ασφαλείας του Δικτύου - Στόχου. Συνήθως, χρησιμοποιείται το εργαλείο Reg[26] για πρόσβαση στο μητρώο. Ο αντίπαλος αντλεί σοβαρές πληροφορίες για το σύστημα και δύναται να διαμορφώσει πλήρη εικόνα για το αν μπορεί να προσβάλλει τον Δτόχο ή όχι, καθώς και με ποιον τρόπο μπορεί να επιτύχει το επιδιωκόμενο αποτέλεσμα.

- Η **τακτική της Πλευρικής Κίνησης** (*Lateral Movement*): Είναι τακτική μέσω της οποίας ο αντίπαλος προβαίνει σε τεχνικές εξ΄ αποστάσεως ελέγχου των συστημάτων ενός Δικτύου - Στόχου. Ο επιτιθέμενος, αρχικά, εξερευνά το υποψήφιο δίκτυο, ώστε να ανακαλύψει τον τρόπο απόκτησης πρόσβασης σε αυτό. Συχνά, απαιτείται να μετακινείται από υποσύστημα σε υποσύστημα του δικτύου έως ότου καταφέρει να αποκτήσει πρόσβαση σε λογαριασμούς. Ο αντίπαλος δύναται να εγκαταστήσει δικά του εργαλεία απομακρυσμένης πρόσβασης ή και να χρησιμοποιήσει νόμιμα διαπιστευτήρια εισόδου στο λειτουργικό σύστημα και στους λογαριασμούς χρηστών και διαχειριστών. Ενδεικτικές τεχνικές Πλευρικής Κίνησης είναι οι ακόλουθες:

  - Η **τεχνική της Ανάπτυξης Εργαλείων Προγραμμάτων** (*Software Deployment Tools*): Είναι η τεχνική με την οποία ο αντίπαλος μπορεί να αποκτήσει πρόσβαση σε πακέτα προγραμμάτων του συστήματος και σε εφαρμογές τρίτων, που είναι εγκατεστημένα σε ένα δίκτυο. Χαρακτηριστικά παραδείγματα είναι οι εφαρμογές για διαχειριστικούς σκοπούς, όπως SCCM[27], HBSS[28], Altiris[29]. Ο αντίπαλος έχει δυνατότητα να προβεί σε εξ΄ αποστάσεως έλεγχο του κώδικα εκτέλεσης όλων των υποσυστημάτων που είναι συνδεδεμένα με το υποψήφιο Σύστημα - Στόχο. Ενδεχομένως, τα διαπιστευτήρια που θα έχει ο αντίπαλος από τοπικούς διαχειριστές να είναι επαρκή για άμεση πρόσβαση σε συστήματα τρίτων προγραμμάτων, διαφορετικά θα πρέπει να αναζητηθούν τα διαπιστευτήρια διαχειριστή.

[26] https://en.wikipedia.org/wiki/Windows_Registry
[27] https://en.wikipedia.org/wiki/Microsoft_Endpoint_Configuration_Manager
[28] https://en.wikipedia.org/wiki/HBSS
[29] https://en.wikipedia.org/wiki/Altiris

- Η **τεχνική του Εξ΄ αποστάσεως Ελέγχου Συνεδριών/Υπηρεσιών** με Πειρατεία (*Remote Service Session Hijacking*): Είναι η τεχνική με την οποία ο αντίπαλος μπορεί να αποκτήσει τον εξ΄ αποστάσεως έλεγχο προυπάρχουσων συνεδριών, κινούμενος εσωτερικά και πλευρικά εντός του υποψήφιου Δικτύου - Στόχου. Ο αντίπαλος μπορεί να χρησιμοποιήσεις έγκυρα διαπιστευτήρια για να συνδεθεί με υπηρεσίες ειδικά σχεδιασμένες για απομακρυσμένες συνδέσεις, όπως telnet[30], SSH[31] και RDP[32]. Η τεχνική Remote Service Session Hijacking διαφέρει από την Remote Services, διότι η πρώτη παραβιάζει προυπάρχουσα υπηρεσία, ενώ η δεύτερη δημιουργεί νέα.

- Η **τακτική της Συλλογής Δεδομένων** (*Collection)*: Είναι τακτική μέσω της οποίας ο αντίπαλος προβαίνει σε τεχνικές για την συλλογή ''ευαίσθητων'' πληροφοριών του υποψήφιου Δικτύου - Στόχος από πηγές, όπως Διαδίκτυο, αρχεία ήχου, εικόνας, video και emails. Συνήθως, ο επόμενος Στόχος μετά τη συλλογή είναι η διήθηση (exfiltrate) δεδομένων και πληροφοριών. Στη συλλογή περιλαμβάνονται και οι όροι στιγμιότυπα οθόνης (capturing screenshots) και χτυπήματα εισόδου σε πληκτρολόγιο (*keyboard input*). Ενδεικτικές τεχνικές Συλλογής Δεδομένων είναι οι ακόλουθες:

  - Η **τεχνική της Ηχογράφησης** (***Audio Capture***): Είναι η τεχνική με την οποία ο αντίπαλος μπορεί να αξιοποιήσει περιφερειακές συσκευές ενός υπολογιστή (π.χ. μικρόφωνα και κάμερες web) ή εφαρμογές (*π.χ. υπηρεσίες φωνητικών κλήσεων και βιντεοκλήσεων*) για τη λήψη ηχογραφήσεων, με σκοπό την ακρόαση ευαίσθητων συνομιλιών για τη συλλογή πληροφοριών. Τα αρχεία ήχου μπορεί να εγγραφούν στο δίσκο και να εξαχθούν αργότερα. Μπορούν να χρησιμοποιηθούν κακόβουλα προγράμματα για την αλληλεπίδραση με τις συσκευές μέσω ενός διαθέσιμου API[33] που παρέχεται από το λειτουργικό σύστημα ή μιας εφαρμογής για τη λήψη ήχου.

  - Η **<u>τεχνική του Στιγμιότυπου Επιφάνειας Εργασίας - Οθόνης</u>** (*Screen Capture*): Είναι η τεχνική με την οποία ο αντίπαλος μπορεί να λάβει στιγμιότυπα από την επιφάνεια εργασίας, με σκοπό να συλλέξει πληροφορίες, κατά τη διάρκεια της επιχείρησης εισόδου σε ένα Δίκτυο - Στόχο. Μπορεί η τεχνική αυτή να λειτουργήσει ως εργαλείο εξ΄ αποστάσεως πρόσβασης. Η λήψη στιγμιότυπου

[30] https://en.wikipedia.org/wiki/Telnet
[31] https://en.wikipedia.org/wiki/Secure_Shell
[32] https://en.wikipedia.org/wiki/Remote_Desktop_Protocol
[33] https://en.wikipedia.org/wiki/API

οθόνης είναι εφικτή με εργαλεία, όπως ‘’CopyFromScreen’’ και ‘’xwd’’ ή ‘’screencapture’’.

- Η **τακτική της Διοίκησης και του Ελέγχου** (*Command and Control*): Είναι τακτική μέσω της οποίας ο αντίπαλος προβαίνει σε τεχνικές για την διοίκηση, τον έλεγχο και τον τρόπο επικοινωνίας (*π.χ. με πρωτόκολλο HTTP, κ.ά*) με το Σύστημα - Στόχος, που έχει πρόσβαση. Ο επιτιθέμενος επιδιώκει να μιμηθεί την αναμενόμενη, από τον Χρήστη, κίνηση του δικτύου, ώστε να μην γίνει αντιληπτός από ασυνήθιστες λανθασμένες κινήσεις του. Ενδεικτικές τεχνικές Διοίκησης και Ελέγχου είναι οι ακόλουθες:

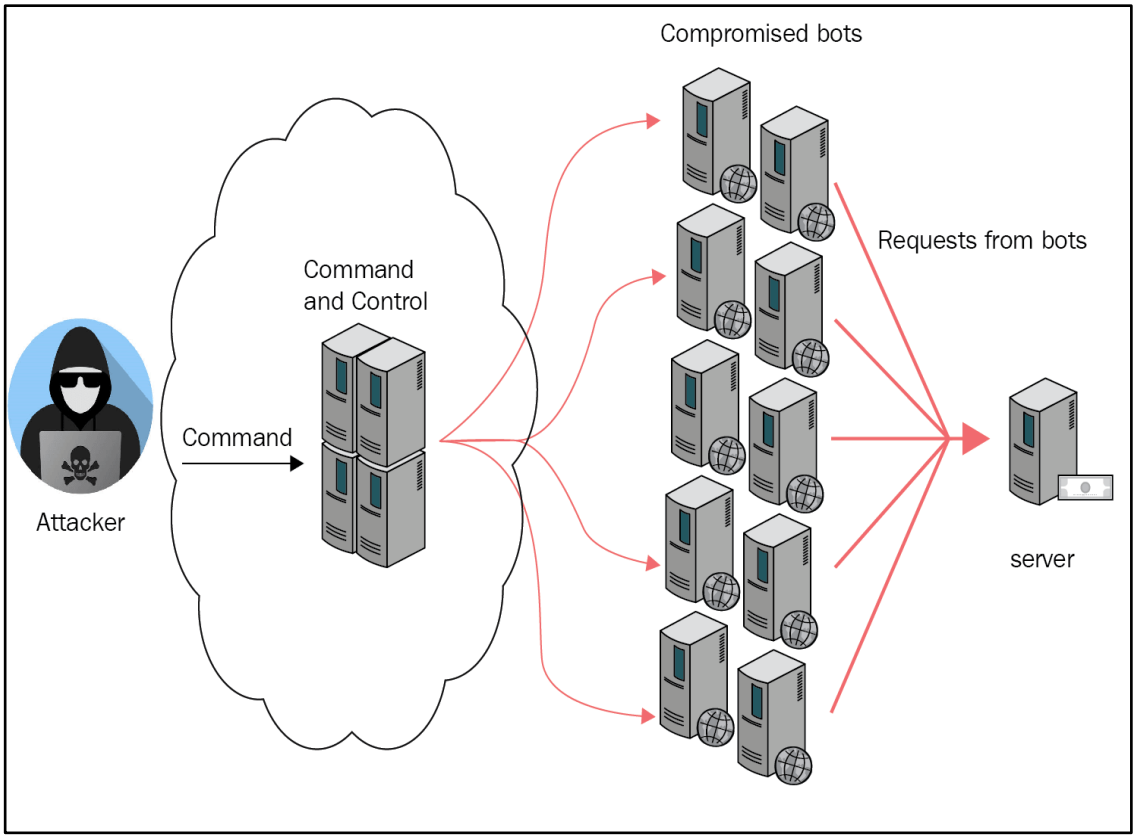
  - Η **τεχνική της Κωδικοποίησης Δεδομένων** (*Data Encoding*): Είναι η τεχνική με την οποία ο αντίπαλος μπορεί να κρυπτογραφεί δεδομένα με ένα τυπικό σύστημα κωδικοποίησης δεδομένων, με σκοπό να ελαχιστοποιήσει την πιθανότητα εντοπισμού του από τον Διαχειριστή του Δικτύου - Στόχου. Η εν λόγω κωδικοποίηση ακολουθεί, συνήθως, τα συστήματα ASCII[34], Unicode[35], Base64[36], MIME[37] ή και άλλα συναφή ή μη συστήματα κωδικοποίησης. Ορισμένα συστήματα κωδικοποίησης ενδεχομένως να οδηγήσουν σε συμπίεση δεδομένων gzip [38].

  - Η **τεχνική της Συσκότισης Δεδομένων** (*Data Obfuscation*): Είναι η τεχνική με την οποία ο αντίπαλος μπορεί να συσκοτίσει (να θαμπώσει) τον Διαχειριστή του Δικτύου, ώστε να ελαχιστοποιήσει την πιθανότητα να εντοπιστεί ως εχθρός. Οι δραστηριότητες επικοινωνιών είναι μυστικές, πλην όμως όχι απαραίτητα κρυπτογραφημένες, ώστε να μη δίδεται η παραμικρή υποψία ύποπτης, μη συνηθισμένης ή και μη φυσιολογικής κίνησης εντός των δικτύων. Μερικές συναφείς τεχνικές είναι η προσθήκη άχρηστων δεδομένων στο πρωτόκολλο κίνησης, η χρήση στενογραφίας και η πλαστογραφία νόμιμων πρωτοκόλλων, κτλ.

[34] https://en.wikipedia.org/wiki/ASCII
[35] https://en.wikipedia.org/wiki/Unicode
[36] https://en.wikipedia.org/wiki/Base64
[37] https://en.wikipedia.org/wiki/MIME
[38] https://en.wikipedia.org/wiki/Gzip

- Η **τακτική της Διήθησης Δεδομένων** (*Exfiltration*): Είναι τακτική μέσω της οποίας ο αντίπαλος προβαίνει σε τεχνικές υποκλοπής για τη διήθηση (*εξαγωγή*) δεδομένων, πληροφοριών και αρχείων από το Σύστημα - Στόχος. Μόλις γίνει η συλλογή, ο επιτιθέμενος πακετάρει τα δεδομένα ώστε να μην γίνει αντιληπτός. Αυτή η ενέργεια περιλαμβάνει συμπίεση αρχείων, κωδικοποίηση ή και κρυπτογράφηση, καθώς και μεταφορά από το κανονικό κανάλι Διοίκησης και Ελέγχου σε εναλλακτικό. Ενδεικτικές τεχνικές Εξαγωγής Δεδομένων είναι οι ακόλουθες:
  - Η **τεχνική της Διήθησης μέσα από το Κανάλι Διοίκησης και Ελέγχου** (*Exfiltration Over C2 Channel*): Είναι η τεχνική με την οποία ο αντίπαλος μπορεί να υποκλέψει δεδομένα για εξαγωγή χρήσιμων πληροφοριών μέσα ένα υπάρχον κανάλι εντολών και ελέγχου. Τα δεδομένα που συλλέγονται κρυπτογραφούνται εντός του καναλιού επικοινωνίας, χρησιμοποιώντας το ίδιο πρωτόκολλο επικοινωνιών, που χρησιμοποιείται για τη διοίκηση και τον έλεγχο.
  - Η **τεχνική της Αυτόματης Διήθησης** (*Automated Exfiltration*): Είναι η τεχνική με την οποία οι αντίπαλοι μπορεί να υποκλέψουν δεδομένα, ευαίσθητα έγγραφα, κτλ., με αυτοματοποιημένη διαδικασία συλλογής και διήθησης αυτών.
- **Η τακτική του Αντίκτυπου** (*Impact*): Είναι τακτική μέσω της οποίας ο αντίπαλος προβαίνει σε τεχνικές ώστε να χειραγωγήσει, να διακόψει ή να καταστρέψει τα συστήματα και τα δεδομένα αυτών. Ο επιτιθέμενος επιδιώκει να παραβιάσει ή και να καταστρέψει τα δεδομένα του υποψήφιου Δικτύου - Στόχος. Ο αντίπαλος εκτελεί άκρως επιθετική ενέργεια, προκειμένου να πετύχει τους τεθέντες στόχους ή και να καλύψει τα ίχνη από την παραβίαση του απορρήτου, που έχει προβεί. Ενδεικτικές τεχνικές Αντίκτυπου είναι οι ακόλουθες:
  - Η **τεχνική της Χειραγώγησης Δεδομένων** (*Data Manipulation*): Είναι η τεχνική με την οποία ο αντίπαλος μπορεί να εισάγει νέα δεδομένα, να διαγράψει ή και να χειραγωγήσει παλαιά δεδομένα, με σκοπό να αποκρύψει την παράνομη παρουσία του σε ένα Δίκτυο - Στόχο. Επί πλέον, ο επιτιθέμενος μπορεί με την χειραγώγηση δεδομένων να επηρεάσει δυσμενώς τις λειτουργίες ενός δικτύου και σαφέστατα να προκαλέσει μέγιστη σύγχυση, ώστε να μην δύναται οι ειδική να λάβουν ορθή και έγκυρη απόφαση ως προς τον τρόπο αντίδρασης για την προστασία του δικτύου.

- Η **τεχνική της Άρνησης Υπηρεσίας Δικτύου** (*Network Denial of Service*): Είναι η τεχνική με την οποία ο αντίπαλος μπορεί να πραγματοποιήσει επιθέσεις άρνησης υπηρεσίας δικτύου (*DoS*) για να υποβαθμίσει τους πόρους ενός Συστήματος - Στόχου π.χ. εξάντληση των υπηρεσιών εύρους ζώνης δικτύου, των πόρων που αφορούν ιστότοπους, υπηρεσίες email, τα DNS και τις εφαρμογές που βασίζονται στους ιστότοπους. Συνήθως, οι επιθέσεις DoS υλοποιούνται σε ένα ευρύτερο πλαίσιο κακόβουλων δραστηριοτήτων, χακτιβισμού (*hacktivism*)[39] και εκβιασμού.



Εικόνα 4-5 Άρνηση Υπηρεσίας Δικτύου (DoS)

Πηγή: https://exploitszone.com/wp-content/uploads/2020/06/ddos-attack.png

[39] https://en.wikipedia.org/wiki/Hacktivism

Η σελίδα αυτή σκόπιμα κενή

ΣΥΜΠΕΡΑΣΜΑΤΑ - ΚΡΙΤΙΚΗ

Αναμφίβολα, η ιδιωτικότητα των χρηστών και η απόκρυψη της δραστηριότητας τους στο Διαδίκτυο αποτελεί μείζον θέμα τα τελευταία χρόνια, έχοντας απασχολήσει τους απλούς Χρήστες, τους τεχνολογικούς κολοσσούς, αλλά και τις κυβερνήσεις και τα δικαστικά όργανα.

Ο κόσμος του Dark Web μπορεί να έλκει τους Χρήστες λόγω του μυστήριου που περιβάλλεται, πλην όμως ελλοχεύει σοβαρούς κινδύνους, καθώς σε αυτό τον κόσμο δραστηριοποιούνται κάθε είδους παραβατικές και εγκληματικές ομάδες, οι οποίες δεν έχουν κανέναν ενδοιασμό να στοχοποιήσουν οποιονδήποτε αρχάριο Χρήστη που περιηγείται ανώνυμα στον Σκοτεινό Ιστό.

Το Dark Web λυμαίνονται τεράστια δίκτυα διακίνησης ναρκωτικών, εμπορίας όπλων, παιδικής πορνογραφίας, καθώς και επικρατεί κάθε είδους παράνομη δραστηριότητα. Σύμμαχος αυτών των σκοτεινών δοσοληψιών είναι το Κρυπτονόμισμα, το οποίο διευκόλυνε όσο τίποτα άλλο τους Χρήστες του Διαδικτύου να πραγματοποιούν ανώνυμες συναλλαγές καλύπτοντας τα ίχνη τους.

Οι συναλλαγές στο Dark Web διεξάγονται με κρυπτονόμισμα, το οποίο έχει ήδη αντικαταστήσει κάθε άλλη μορφή πληρωμής, όπως κλεμμένες πιστωτικές κάρτες, τραπεζικά εμβάσματα και πληρωμή μέσω PayPal, που παραδοσιακά χρησιμοποιούνταν σε παράνομες δοσοληψίες, αλλά και στο ξέπλυμα μαύρου χρήματος.Αρκετές κυβερνήσεις αντιδρούν σθεναρά ως προς τη χρήση των κρυπτονομισμάτων, καθώς δεν έχουν κανέναν απολύτως έλεγχο πάνω σε αυτά. Αυτό φυσικά διασφαλίζει τους Χρήστες τους από κρατικό παρεμβατισμό και διάφορες άλλες απαγορεύσεις.

Οι Χρήστες γίνονται ολοένα και πιο ευαίσθητοι όσον αφορά την προστασία των προσωπικών δεδομένων τους, συνειδητοποιώντας ότι η ελεύθερη χρήση πολλών Υπηρεσιών Διαδικτύου έχει ως πραγματικό αντίτιμο τα προσωπικά τους δεδομένα, τα οποία σιωπηλά συλλέγονται από διάφορους οργανισμούς και αποτελούν αντικείμενο κοινωνικής, πολιτικής και κυρίως οικονομικής εκμετάλλευσης.

Υπάρχει και μία ολόκληρη κοινότητα Χρηστών, οι οποίοι υποστηρίζουν με ζέση το γεγονός ότι η πλοήγηση στο επιφανειακό Internet ισοδυναμεί με τον τερματισμό της ιδιωτικής τους ζωής, καθώς μεγάλες εταιρίες του μεγέθους της Google συσσωρεύουν μεγάλο αριθμό ευαίσθητων προσωπικών δεδομένων, μέσω των μηχανών αναζήτησης, του ηλεκτρονικού ταχυδρομείου (*Gmail*) και των χαρτών πλοήγησης (*Google maps*). Συνεπώς, η χρήση του Dark Web ισοδυναμεί με κάλυψη της ανάγκης της προστασίας της ηλεκτρονικής ιδιωτικής

ζωής.

Για το λόγο αυτό, τα τελευταία χρόνια έχει αναπτυχθεί πληθώρα τεχνολογιών που δίνουν βάρος στη διασφάλιση της ανωνυμίας και της ιδιωτικότητας των χρηστών, προσφέροντας μάλιστα υψηλού επιπέδου υπηρεσίες, οι οποίες μπορούν να ανταποκριθούν ακόμα και στις πιο σύγχρονες, απαιτητικές διαδικτυακές εφαρμογές. Η έρευνα γύρω από το συγκεκριμένο πεδίο έχει συγκεντρώσει τα βλέμματα πλήθους επιστημόνων και σχεδιαστών δικτύων επικοινωνιών, οι οποίοι αντιλαμβάνονται ότι οι Χρήστες πλέον τοποθετούν σε υψηλή προτεραιότητα την προστασία των δεδομένων τους, ιδιαίτερα σε μια εποχή όπου τα πάντα είναι διασυνδεδεμένα μεταξύ τους.

Το ζήτημα της ιδιωτικότητας και της ανωνυμίας στο Διαδίκτυο αναμένεται να απασχολήσει σημαντικά όλους τους εμπλεκόμενους φορείς, καθώς ήδη έχει ξεκινήσει η αντιπαράθεση μεταξύ αυτών που υποστηρίζουν την προστασία των δικαιωμάτων των Χρηστών με αυτούς που υποστηρίζουν ότι οι πάροχοι Υπηρεσιών Διαδικτύου θα πρέπει να έχουν ένα βαθμό ελέγχου πάνω στη δραστηριότητα που συντελείται σε αυτό. Επιπλέον, οι μεγάλοι τεχνολογικοί κολοσσοί επηρεάζονται, επίσης, καθώς η χρήση τέτοιων δικτύων τους στερεί τα πολύτιμα δεδομένα των χρηστών - πελατών τους, τα οποία τους επιφέρουν έσοδα δισεκατομμυρίων.

Δεν είναι καθόλου αμελητέο το γεγονός ότι ο κίνδυνος να πέσει κανείς θύμα ηλεκτρονικής απάτης από Hackers, οι οποίοι έχουν την ικανότητα να εμφυτεύουν ‘’αόρατους’’ ιούς, μέσα σε σπασμένα προγράμματα που έχει ο υποψήφιος Στόχος - Χρήστης δωρεάν και παράνομα εγκαταστήσει στον υπολογιστή του. Το μεγαλύτερο ποσοστό των ιών αυτών υποκλέπτουν usernames και passwords που χρησιμοποιεί ο Χρήστης σε διάφορες ιστοσελίδες, συμπεριλαμβανόμενων και των web banking των τραπεζών.

Έως σήμερα έχει εκτελεστεί πλήθος επιθέσεων, καθώς η διαρκής εξέλιξη των τεχνολογιών ανωνύμων επικοινωνιών ανάγκασε τους επιτιθέμενους να εξελίξουν τις ήδη υπάρχουσες αλλά και να προσθέσουν νέες στο οπλοστάσιο τους τακτικές και τεχνικές, προκειμένου να αντιμετωπίσουν τα εξελιγμένα μέτρα προστασίας και αποτροπής των σύγχρονων δικτύων υπολογιστών. Το σύνολο των επιθέσεων αυτών μπορεί να επιφέρει, όπως έχει αποδειχθεί, σημαντικά πλήγματα στην ασφάλεια των δικτύων, καθώς και να υπονομεύσει σοβαρά την ασφάλεια και την ανωνυμία των χρηστών τους.

Συμπερασματικά, οι τεχνολογίες ανωνύμων επικοινωνιών αποτελούν ένα εξαιρετικά ευρύ πεδίο έρευνας και εφαρμογής, το οποίο θα συνεχίσει να αναπτύσσεται δυναμικά.

ΒΙΒΛΙΟΓΡΑΦΙΑ ΔΙΠΛΩΜΑΤΙΚΗΣ ΔΙΑΤΡΙΒΗΣ

1. **Βιβλιογραφία Κεφαλαίου 2ου:** Τεχνολογικό και Ερευνητικό Προσκήνιο στο Σκοτεινό Διαδίκτυο (Dark Net)

[SOA.1]. Gehl, Robert W. Weaving the dark web: legitimacy on freenet, Tor, and I2P. MIT Press, 2018.

[SOA.2]. Schriner, John. "Monitoring the Dark Web and Securing Onion Services." (2017).

[SOA.3]. Jardine, Eric. "The Dark Web dilemma: Tor, anonymity and online policing." Global Commission on Internet Governance Paper Series 21 (2015).

[SOA.4]. Kavallieros, Dimitrios, et al. "Understanding the dark web." Dark Web Investigation. Springer, Cham, 2021. 3-26.

[SOA.5]. Dalvi, Ashwini, et al. "From Hidden Wiki 2020 to Hidden Wiki 2021: What Dark Web Researchers Comprehend with Tor Directory Services?." 2021 5th International Conference on Information Systems and Computer Networks (ISCON). IEEE, 2021.

[SOA.6]. Van Wegberg, Rolf, Jan-Jaap Oerlemans, and Oskar van Deventer. "Bitcoin money laundering: mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin." Journal of Financial Crime (2018).

[SOA.7]. Bethencourt, John, et al. "Establishing darknet connections: an evaluation of usability and security." Proceedings of the 3rd symposium on Usable privacy and security. 2007.

[SOA.8]. Hurlburt, George. "Shining light on the dark web." Computer 50.04 (2017): 100-105.

[SOA.9]. Pete, Ildiko, et al. "A social network analysis and comparison of six dark web forums." 2020 IEEE European symposium on security and privacy workshops (EuroS&PW). IEEE, 2020.

[SOA.10]. Fu, Tianjun, Ahmed Abbasi, and Hsinchun Chen. "A focused crawler for Dark Web forums." Journal of the American Society for Information Science and Technology 61.6 (2010): 1213-1231.

[SOA.11]. Murty, Ch AS, et al. "A Review of Web Application Security Risks: Auditing and Assessment of the Dark Web." 2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME). IEEE, 2021.

[SOA.12]. Pieterse, Jan Nederveen. "Leaking Superpower: WikiLeaks and the contradictions of democracy." Third World Quarterly 33.10 (2012): 1909-1924.

[SOA.13]. La Morgia, Massimo, et al. "Time-zone geolocation of crowds in the dark web." 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS). IEEE, 2018.

[SOA.14]. Elangovan, Ramanujam. "The Dark Web: Hidden Access to Internet Today." Encyclopedia of Criminal Activities and the Deep Web. IGI Global, 2020. 129-139.

[SOA.15]. Goldschlag, David, Michael Reed, and Paul Syverson. "Onion routing." Communications of the ACM 42.2 (1999): 39-41.

[SOA.16]. Shapiro, Anna P., et al. "Novel ways to acquire designer benzodiazepines: a case report and discussion of the changing role of the internet." Psychosomatics 60.6 (2019): 625-629.

2. **Βιβλιογραφία Κεφαλαίου 3ου**: Εγκαθίδρυση μιας Καλοστημένης Επιχειρηματικής Μηχανής στο Σκοτεινό και Βαθύ Διαδίκτυο (Dark and Deep Web)

[BUS.1]. Casadesus-Masanell, Ramon, and Joan Enric Ricart. "From strategy to business models and onto tactics." Long range planning 43.2-3 (2010): 195-215.

[BUS.2]. Magretta, Joan. "Why business models matter." (2002).

[BUS.3]. Osterwalder, Alexander, and Yves Pigneur. Business model generation: a handbook for visionaries, game changers, and challengers. Vol. 1. John Wiley & Sons, 2010.

[BUS.4]. Barquet, Ana Paula B., et al. "Business model elements for product-service system." Functional thinking for value creation. Springer, Berlin, Heidelberg, 2011. 332-337.

[BUS.5]. De Reuver, Mark, Harry Bouwman, and Timber Haaker. "Business model roadmapping: A practical approach to come from an existing to a desired business model." International Journal of Innovation Management 17.01 (2013): 1340006.

[BUS.6]. Osterwalder, Alexander, Yves Pigneur, and Christopher L. Tucci. "Clarifying business models: Origins, present, and future of the concept." Communications of the association for Information Systems 16.1 (2005): 1.

[BUS.7]. Osterwalder, Alexander. The business model ontology a proposition in a design science approach. Diss. Université de Lausanne, Faculté des hautes études commerciales, 2004.

[BUS.8]. Osterwalder, Alexander, et al. Value proposition design: How to create products and services customers want. John Wiley & Sons, 2015.

[BUS.9]. Putman, C. G. J., and Lambert JM Nieuwenhuis. "Business model of a botnet." 2018 26th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP). IEEE, 2018.

[BUS.10]. Sejfuli-Ramadani, Nexhibe, Florim Idrizi, and Florinda Imeri. "THE INFLUENCE OF THE DARK WEB." Journal of Natural Sciences and Mathematics of UT 4.7-8 (2019): 95-98.

[BUS.11]. Nguyen, Bang, Faten Jaber, and Lyndon Simkin. "A systematic review of the dark side of CRM: the need for a new research agenda." Journal of strategic marketing 30.1 (2022): 93-111.

[BUS.12]. Ormsby, Eileen. "Dealer's chance: The dark web, bitcoin and the fall of silk road." Griffith REVIEW 64 (2019): 184-194.

[BUS.13]. Kock, Ned. "E-collaboration and e-commerce in virtual worlds: The potential of Second Life and World of Warcraft." International Journal of e-Collaboration (IJeC) 4.3 (2008): 1-13.

[BUS.14]. Faizan, Mohd, and Raees Ahmad Khan. "Exploring and analyzing the dark Web: A new alchemy." First Monday (2019).

[BUS.15]. Tredinnick, Luke. "Cryptocurrencies and the blockchain." Business Information Review 36.1 (2019): 39-44.

[BUS.16]. Hurlburt, George. "Shining light on the dark web." Computer 50.04 (2017): 100-105.

[BUS.17]. Wang, Yunjia, and Ishbel Duncan. "A novel method to prevent phishing by using OCR technology." 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security). IEEE, 2019.

[BUS.18]. Lacson, Wesley, and Beata Jones. "The 21st century darknet market: lessons from the fall of Silk Road." International Journal of Cyber Criminology 10.1 (2016): 40.

[BUS.19]. Tsuchiya, Yoichi, and Naoki Hiramoto. "Dark web in the dark: Investigating when transactions take place on cryptomarkets." Forensic Science International: Digital Investigation 36 (2021): 301093.

[BUS.20]. Ansh, Samar, and Satwinder Singh. Analyze Dark Web and Security Threats. No. 8384. EasyChair, 2022.

[BUS.21]. Easttom, Chuck. "Conducting investigations on the Dark Web." Journal of Information Warfare 17.4 (2018): 26-37.

[BUS.22]. Spitters, Martijn, Stefan Verbruggen, and Mark Van Staalduinen. "Towards a comprehensive insight into the thematic organization of the tor hidden services." 2014 IEEE Joint Intelligence and Security Informatics Conference. IEEE, 2014.

[BUS.23]. Kaur, Shubhdeep, and Sukhchandan Randhawa. "Dark web: a web of crimes." Wireless Personal Communications 112.4 (2020): 2131-2158.

[BUS.24]. Gross, William F. "Monitoring and tracking ISIS on the dark web." Online Terrorist Propaganda, Recruitment, and Radicalization. CRC Press, 2019. 341-350.

[BUS.25]. Ranakoti, Pranshu, et al. "Deep web & online anonymity." 2017 International conference on computing and communication technologies for smart nation (IC3TSN). IEEE, 2017.

[BUS.26]. Schriner, John, and Melody Lee Rood. "The Internet Never Forgets: Image-Based Sexual Abuse and the Workplace." (2020).

[BUS.27]. Vargas, Vanesa-Madalina. "The new economic good: Your own personal data. An integrative analysis of the Dark Web." Proceedings of the International Conference on Business Excellence. Vol. 13. No. 1. 2019.

[BUS.28]. Chertoff, Michael. "A public policy perspective of the Dark Web." Journal of Cyber Policy 2.1 (2017): 26-38.

3. **Βιβλιογραφία Κεφαλαίου 4ου**: Εισβολείς Υπολογιστικών Συστημάτων (Hackers) στο Dark Web

HACK.1 Richet, Jean-Loup. "From young hackers to crackers." International Journal of Technology and Human Interaction (IJTHI) 9.3 (2013): 53-62.

HACK.2 Barber, Richard. "Hackers profiled—who are they and what are their motivations?." *Computer Fraud & Security* 2001.2 (2001): 14-17.

HACK.3 Hald, Sara LN, and Jens M. Pedersen. "An updated taxonomy for characterizing hackers according to their threat properties." *2012 14th International Conference on Advanced Communication Technology (ICACT)*. IEEE, 2012.

HACK.4 Chen, Ping, Lieven Desmet, and Christophe Huygens. "A study on advanced persistent threats." *IFIP International Conference on Communications and Multimedia Security*. Springer, Berlin, Heidelberg, 2014.

HACK.5 Pratama, Andhika, and Fauzi Adi Rafrastara. "Computer worm classification." *International Journal of Computer Science and Information Security* 10.4 (2012): 21.

HACK.6 Filiol, Eric. *Computer viruses: from theory to applications*. Springer Science & Business Media, 2006.

HACK.7 Jin, Yier, Nathan Kupp, and Yiorgos Makris. "Experiences in hardware Trojan design and implementation." 2009 IEEE International Workshop on Hardware-Oriented Security and Trust. IEEE, 2009.

HACK.8 De Vivo, Marco, et al. "A review of port scanning techniques." ACM SIGCOMM Computer Communication Review 29.2 (1999): 41-48.

HACK.9 Wen, Zikai Alex, et al. "What. hack: Learn phishing email defence the fun way." Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems. 2017.

HACK.10 Liu, Simon, and Bruce Cheng. "Cyberattacks: Why, what, who, and how." IT professional 11.3 (2009): 14-21.

HACK.11 Shaw, Eric D., Keven G. Ruby, and Jerrold M. Post. "The insider threat to information systems." Security Awareness Bulletin 2.98 (1998): 1-10.

HACK.12 Zangerle, Eva, and Günther Specht. "Sorry, I was hacked" a classification of compromised twitter accounts." Proceedings of the 29th annual acm symposium on applied computing. 2014.

HACK.13 Schiller, Craig, and James R. Binkley. Botnets: The killer web applications. Elsevier, 2011.

HACK.14 Xiong, Wenjun, et al. "Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix", Software and Systems Modeling, vol. 21.1, 2022, pp: 157-177.

HACK.15 Xiong, Wenjun, et al. "Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix", Software and Systems Modeling, vol. 21.1, 2022, pp: 157-177.

HACK.16 Oosthoek, Kris, and Christian Doerr. "Cyber threat intelligence: A product without a process?", International Journal of Intelligence and CounterIntelligence, vol. 34.2, 2021, pp: 300-315.

HACK.17 Blake Wolf and June. "Finding Cyber Threats with ATT \& CK TM-Based Analytics", MITRE TECHNICAL REPORT, 2017.

HACK.18 Alexander, Otis, Misha Belisle, and Jacob Steele. "MITRE ATT&CK® for industrial control systems: Design and philosophy", The MITRE Corporation: Bedford, MA, USA, 2020.

HACK.19 Hoang, Nguyen Phong, et al. "An empirical study of the I2P anonymity network and its censorship resistance." Proceedings of the Internet Measurement Conference 2018. 2018.