ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΔΥΤΙΚΗΣ ΕΛΛΑΔΑΣ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Η σκοτεινή πλευρά του διαδικτύου

Φοιτήτρια: Αυγέρη Σοφία (Α.Μ. 16339)

Επ.Καθηγητής: Χρήστος Τσουραμάνης

ΜΕΣΟΛΟΓΓΙ 2019

Περιεχόμενα

ΠΡΟΛΟΓΟΣ

Η παρούσα πτυχιακή εργασία με τίτλο «Η σκοτεινή πλευρά του διαδικτύου», εκπονήθηκε στα πλαίσια της ολοκλήρωσης, των προϋποθέσεων, για την λήψη του πτυχίου μου από το Τ.Ε.Ι. Δυτικής Ελλάδας στο τμήμα Διοίκησης Επιχειρήσεων.

Σκοπός αυτής της πτυχιακής εργασίας, είναι η κατανόηση της έννοιας του «Σκοτεινού Ιστού», η αλλιώς του Dark Web, η ανάλυση των χαρακτηριστικών του, της χρησιμότητας του περιεχομένου του, των κινδύνων που υπάρχουν, καθώς και της διάκρισής του από το Deep Web και το Surface Web. Τέλος, μελετάται η έννοια του hacking, και οι τρόποι αντιμετώπισης του φαινομένου αυτού.

Η εργασία αναπτύσσεται σε 6 κεφάλαια, καθένα από τα οποία έχει διαφορετική θεματολογία. Το πρώτο κεφάλαιο, αναφέρεται στην ηλεκτρονική εγκληματικότητα και τα είδη της.

Στο δεύτερο κεφάλαιο αναλύεται η έννοια του Σκοτεινού Ιστού, η λειτουργικότητα και το περιεχόμενό του.

Στο τρίτο κεφάλαιο περιγράφετε η έννοια του Deep Web, καθώς και το περιεχόμενό του.

Στο τέταρτο κεφάλαιο, γίνεται αναφορά στους μύθους και τις αλήθειες που υπάρχουν γύρω από το Dark Web και το Deep Web.

Το πέμπτο κεφάλαιο, αναφέρεται στον επιφανειακό ιστό και στις διαφορές του με το Dark και το Deep Web.

Τέλος, στο έκτο και τελευταίο κεφάλαιο αναλύεται η έννοια του hacker και του hacking γενικότερα, τα εργαλεία της δουλειάς του και οι τρόποι με τους οποίους μπορεί να αντιμετωπιστεί.

Σε αυτό το σημείο θα ήθελα να ευχαριστήσω τον καθηγητή μου κ. Χ.Τσουραμάνη, για την ευκαιρία που μου έδωσε να ασχοληθώ με το συγκεκριμένο θέμα. Για την εμπιστοσύνη που μου έδειξε, καθώς και για τις χρήσιμες ιδέες του, που συνέβαλαν στη βελτίωση της εργασίας, κατά όλη τη χρονική διάρκεια διεκπεραίωσης της πτυχιακής μου εργασίας.

ΚΕΦΑΛΑΙΟ 1^{Ο} ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

1.1 Ορισμός

Ως ηλεκτρονικό έγκλημα θα θεωρήσουμε κάθε παράνομη πράξη για τη διάπραξη, αλλά και για την αντιμετώπιση της οποίας θεωρείται απαραίτητη η γνώση της ψηφιακής τεχνολογίας. Στα ηλεκτρονικά εγκλήματα έχει διαπιστωθεί ότι συνήθως εμπλέκεται είτε από την πλευρά του δράστη, είτε από την πλευρά του θύματος, ένας τουλάχιστον ηλεκτρονικός υπολογιστής (Τσουραμάνη Χρ.Ε. και Κορολή Μαρ.-Ευγ., Τ.Ε.Ι Δυτικής Ελλάδας, σ.135).

Για τις ανάγκες της ετήσιας έρευνας που διεξάγεται από το Computer Security Institute και το FBI ως ηλεκτρονικά εγκλήματα θεωρούνται:

- οι επιθέσεις ιών
- η επίθεση άρνησης παροχής υπηρεσιών
- η κλοπή πνευματικής ιδιοκτησίας
- οι παραβιάσεις υπαλλήλων επιχειρήσεων που σχετίζονται με Η/Υ.
- οι παράνομες ακροάσεις τηλεπικοινωνιών
- οι οικονομικές απάτες
- οι κλοπές φορητών Η/Υ
- οι παράνομες εισβολές σε σύστημα Η/Υ
- οι τηλεπικοινωνιακές απάτες
- η παραποίηση ιστοσελίδων και
- το σαμποτάζ (Τσουραμάνη Χρ.Ε., Κορολή Μαρ.-Ευγ., Τ.Ε.Ι Δυτικής Ελλάδας, σ.140).

1.2 Είδη

Σύμφωνα με τη διεθνή σύμβαση για το κυβερνοέγκλημα του 2001 (Convention on Cyber Crime 2001) οι κύριες παραβάσεις είναι οι ακόλουθες:

- Παράνομη πρόσβαση
- Παράνομη υποκλοπή
- Παρεμβολή σε δεδομένα
- Παρεμβολή σε συστήματα

- Κακή χρήση συσκευών
- Κλοπή που σχετίζεται με υπολογιστή
- Απάτη που σχετίζεται με υπολογιστή
- Παιδική πορνογραφία
- Προστασία πνευματικών δικαιωμάτων ηλεκτρονικών πληροφοριών

(Τσουραμάνη Χρ.Ε. και Κορολή Μαρ.-Ευγ., Τ.Ε.Ι Δυτικής Ελλάδας, σ.140)

ΚΕΦΑΛΑΙΟ 2^{Ο} DARK WEB: Η ΣΚΟΤΕΙΝΗ ΠΛΕΥΡΑ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ

2.1 Τι είναι το Dark Web;

Το λεγόμενο «Σκοτεινό Διαδίκτυο», ή αλλιώς «Dark Web» αναπτύχθηκε το 2002 από hackers και αναφέρεται σε μια σειρά από ιστοσελίδες, το περιεχόμενο των οποίων είναι μεν ορατό, αλλά δεν συμβαίνει το ίδιο και με τις ιστοσελίδες των server που τις υποστηρίζουν. Έτσι οι σελίδες είναι προσβάσιμες από κάθε χρήστη, αλλά είναι εξαιρετικά δύσκολο, το να εντοπίσεις εκείνον που τις φιλοξενεί και τις διαχειρίζεται (Νικολαΐδης). Πιο συγκεκριμένα, είναι ένας καθαρά ανώνυμος διαδικτυακός ιστός, στον οποίο οι χρήστες μπορούν να έχουν πρόσβαση σε κρυφές ή παράνομες υπηρεσίες. Όταν όμως μιλάμε για χρήστες στο σκοτάδι, πρόκειται για σκιές που δεν αναγνωρίζονται. Συνεπώς, ελάχιστοι μπορούν να έχουν πρόσβαση σε αυτή τη «μαύρη ευκαιρία», μιας και ο ενδιαφερόμενος πρέπει να έχει γίνει αυθεντία στη χρήση συγκεκριμένου λογισμικού και κώδικα. Κι όμως, ο καθένας

μπορεί να καταλήξει μέσα στα σκοτεινά μονοπάτια του ίντερνετ, χωρίς καν να το καταλάβει.

Πιο συγκεκριμένα, το Youtube, έχει γεμίσει με βίντεο που δείχνουν κάποιους να ανοίγουν πακέτα με πράγματα που ισχυρίζονται πως έχουν αγοράσει μέσω Dark Web καθώς έχει γίνει «μόδα» το λεγόμενο Dark Web Challenge. Αξίζει να σημειωθεί πως οι συγκεκριμένες ενέργειες μπορούν να χαρακτηριστούν εύκολα αληθείς, μιας και το Dark Web έχει χαρακτηριστεί και ως το «supermarket της παρανομίας», αφού η ανωνυμία του, επιτρέπει σε πολλούς να έχουν πρόσβαση σε πράγματα που κανονικά δε βρίσκει κανείς στο νόμιμο εμπόριο. Σε μερικά από αυτά τα βίντεο βλέπουμε YouTubers να ισχυρίζονται πως έχουν πληρώσει ακόμα και μεγάλα ποσά για να λάβουν δέματα που περιέχουν περίεργες ουσίες, αντικείμενα με αίμα, και άλλα.

Αναλυτικότερα, πολλοί το χρησιμοποιούν για να βρουν ενημερωτικές σελίδες που απλά απαγορεύτηκαν από τη συνεχή ροή του διαδικτύου, ή ακόμα και πληροφοριοδότες τύπου Σνόουντεν που πωλούν τις πληροφορίες τους για μυστικά των κρατών, για χιλιάδες bitcoins καθημερινά. Στη σκοτεινή πλευρά του διαδικτύου εισέρχεστε με δική σας ευθύνη, ενώ χωρίς αμφιβολία, με την πρώτη σας επίσκεψη (είτε καταλάθος, είτε με τη δική σας συγκατάθεση), εκείνοι που βρίσκονται πίσω από τις αγοροπωλησίες, γνωρίζουν τα πάντα για σας, μιας και σας ζητούν εξαρχής την πιστωτική ή την prepaid σας κάρτα ή ακόμη τα bitcoin identity σας για μεγαλύτερα ποσά. Αν ακόμη δεν έχετε αντιληφθεί την επικινδυνότητα, πρέπει να γνωρίζετε ότι έρευνα απέδειξε πως μεγάλο ποσοστό των software που χρησιμοποιούμε καθημερινά, μπορεί να μας μεταφέρει εκεί με το λάθος πάτημα ενός κουμπιού (Τσακίρης).

2.2 Πώς λειτουργεί;

Η πλειοψηφία των σελίδων του Dark Web είναι κωδικοποιημένες. Αποκωδικοποιούνται με το λογισμικό Tor, που δημιουργήθηκε από hackers και στην πραγματικότητα είναι ένας browser σαν τον Firefox ή τον Chrome. Στο λογότυπο του Tor, στη θέση του γράμματος ο, βρίσκεται ένα κρεμμύδι. Αυτό συμβαίνει επειδή η παραπάνω διαδικασία ονομάζεται «onion routing», καθώς τα δεδομένα μεταφέρονται και αποκρυπτογραφούνται σε στρώσεις, σαν να ξεφλουδίζετε ένα κρεμμύδι. Ο Tor κρυπτογραφεί την κίνηση της κάθε σελίδας και

την «τέμνει» σε κομμάτια, μοιράζοντας το καθένα από αυτά σε τυχαίους υπολογιστές, με εγκατεστημένο το Tor, ανά τον κόσμο. Ο κάθε υπολογιστής αποκωδικοποιεί το κάθε κομμάτι προτού το στείλει στον επόμενο, ώστε τελικά να προβληθεί το περιεχόμενο. Με την παραπάνω διαδικασία είναι αδύνατο να εντοπιστούν τόσο οι δημιουργοί των σελίδων όσο και οι αναγνώστες τους και εξασφαλίζεται σχεδόν απόλυτη ανωνυμία (Νικολαΐδης).

2.3 Τι μπορώ να βρω στο Dark Web;

Το σκοτεινό μέρος του διαδικτύου δε δημιουργήθηκε με αποκλειστικό τρόπο την παρανομία. Όταν όμως φτιάχνεις ένα ολόκληρο κρυφό σύστημα που βασίζεται στη μυστικότητα και την ανωνυμία, δεν μπορεί δε θα χρησιμοποιηθεί από προσκόπους για πώληση μπισκότων (Αμπατζής).

Δεν πρέπει όσα αναφερθούν να μας φοβίζουν, αλλά να γίνουν η αφορμή για να είμαστε πιο προσεκτικοί σε περίπτωση που βρεθούμε σε αυτά τα μέρη του Σκοτεινού Ιστού (Αναγνωστόπουλος).

2.3.1 Botnet και ηλεκτρονικό «ψάρεμα»

Στο Dark Web μπορεί κανείς να βρει botnet, σύνολα συσκευών συνδεδεμένων στο διαδίκτυο που εκτελούν προγράμματα αυτόματων λειτουργιών. Παράλληλα, ο Σκοτεινός Ιστός περιέχει πολλές σελίδες «ψαρέματος» στοιχείων και οικονομικών δεδομένων των χρηστών. Οι περισσότερες από αυτές είναι πιστά αντίγραφα δημοφιλών υπηρεσιών, όπως το PayPal.

Σκοπός τους είναι να ξεγελάσουν τους ανυποψίαστους χρήστες στο να συμπληρώσουν τα στοιχεία του πραγματικού τους λογαριασμού (Αμπατζής).

2.3.2 Η μαύρη αγορά του Dark Web

Στις μαύρες αγορές του Dark Web πραγματοποιείται εμπόριο λευκής σαρκός, διακινούνται ναρκωτικές ουσίες, όπλα ακόμη και στρατιωτικός εξοπλισμός.

Silk Road, η πρώτη σύγχρονη μαύρη αγορά

Η αρχή των μαύρων αγορών μέσα στο Dark Web έγινε με το Silk Road, που δημιουργήθηκε από το Ross William Ulbricht.

Ο «Δρόμος του Μεταξιού», όπως αναφέρεται στα Ελληνικά ξεκίνησε τη λειτουργία του τον Φεβρουάριο του 2011. Ως κομμάτι του «Σκοτεινού Διαδικτύου», η σελίδα ήταν κρυμμένη πίσω από τις υπηρεσίες του Tor, κι έτσι η ταυτότητα των χρηστών του, θεωρούνταν απόλυτα ασφαλής. Η εγγραφή των αγοραστών Silk Road ήταν απολύτως δωρεάν. Οι πωλητές αρχικά αγόραζαν λογαριασμούς μέσω δημοπρασιών, και αργότερα πλήρωναν ένα ενιαίο ποσό.

Τον Οκτώβριο του 2013, το FBI έκλεισε την ιστοσελίδα, και ο Ross William Ulbricht συνελήφθη ως ιδρυτής της σελίδας, με το ψευδώνυμο «Dread Pirate Roberts».

Το Νοέμβριο του 2013, οι πρώην διαχειριστές της σελίδας άνοιξαν το Silk Road 2.0, όπου έκλεισε το Νοέμβριο του 2014 στα πλαίσια της Operation Onymous.

Το Φεβρουάριο του 2015, απαγγέλθηκαν στο Ross συνολικά οκτώ κατηγορίες. Αυτή τη στιγμή εκτίει ποινή ισόβιας κάθειρξης, χωρίς τη δυνατότητα επανεξέτασης (Αμπατζής).

Sheep Marketplace

Μια μικρότερη μαύρη αγορά που υπήρξε στο Dark Web ήταν το Sheep Marketplace, που έγινε πιο δημοφιλές μετά το κλείσιμο του Silk Road.

Το Δεκέμβριο του 2013, οι διαχειριστές του ιστοτόπου ανακοίνωσαν πως κάποιος από τους πωλητές που δραστηριοποιούνταν σε αυτό, κατάφερε να κλέψει 5.400 Bitcoin, από τους χρήστες της σελίδας. Οι χρήστες κατάφεραν να αποδείξουν πως το ποσό άγγιζε τα 40.000 Bitcoin από το site.

Το 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 Bitcoin. Η υπόθεση έκλεισε το Μάιο του 2016, καθώς εντοπίστηκαν δύο άνδρες από τη Φλόριντα, οι οποίοι πραγματοποίησαν συναλλαγές μέσω του Coinbase (Αμπατζής).

2.3.3 Παράνομη Πορνογραφία

Σεβαστό χώρο στο Σκοτεινό Ιστό καταλαμβάνει η παράνομη πορνογραφία (Αμπατζής).

Αποτελεί αναμφισβήτητο γεγονός ότι ανεξέλεγκτες διαστάσεις έχει πάρει σε όλο τον κυβερνοχώρο τα τελευταία χρόνια το φαινόμενο της διακίνησης παιδικής πορνογραφίας. Η πορνογραφία στο διαδίκτυο είναι ένα αδίκημα που έχει εμφανιστεί εδώ και χρόνια και έχει απασχολήσει πολλές φορές την επικαιρότητα. Η πορνογραφία δε θα μπορούσε να λεχθεί ότι αποτελεί άμεση προσβολή της γενετησίας ελευθερίας του ατόμου. Αναμφίβολα, όμως, επιφέρει κατάφορη προσβολή της ανθρώπινης αξιοπρέπειας. Στο Dark Web μπορεί κανείς να βρει πορνογραφικό υλικό για κάθε λογής γούστο (Τσουραμάνη Χρ.Ε. και Κορολή Μαρ.-Ευγ., Τ.Ε.Ι Δυτικής Ελλάδας, σ.155).

2.3.4 Hackers

Ο Σκοτεινός Ιστός είναι σίγουρα ο παράδεισος των hackers, οι οποίοι πληρώνονται αδρά για να παρέχουν τις υπηρεσίες τους. Οι hackers του Dark Web λειτουργούν μεμονωμένα ή σε ομάδες και αναλαμβάνουν την εκτέλεση ποικίλων ηλεκτρονικών εγκλημάτων. Επίσης πολλές φορές έχει τύχει να βοηθήσουν στην εξαφάνιση κυκλωμάτων παιδεραστίας (Αμπατζής).

2.3.5 Bitcoin, παιχνίδια και Dark Web

Το bitcoin είναι μια ηλεκτρονική μορφή χρήματος, η οποία βασίζεται πάνω στις αρχές της κρυπτογραφίας για την διασφάλιση του δικτύου και την επαλήθευση των συναλλαγών (Salih).

Οι περισσότερες συναλλαγές στο Dark Web γίνονται με τη χρήση κρυπτονομισμάτων. Ο λόγος είναι διότι η πληρωμή με ένα μη φυσικό νόμισμα βοηθά στη διατήρηση της ανωνυμίας. Πολλοί χρήστες πραγματοποιούν τις συναλλαγές τους με ψηφιακά νομίσματα, κι έπειτα μεταφέρουν τα ποσά αυτά σε παιχνίδια, όπως το World Of Warcraft και το Second Life. Παιχνίδια τέτοιου είδους παρέχουν τη δυνατότητα μετατροπής των ψηφιακών τους νομισμάτων σε πραγματικά χρήματα. Έτσι οι χρήστες μετατρέπουν το Bitcoin σε νόμισμα, το

οποίο και αποσύρουν σε κάποιο τραπεζικό λογαριασμό. Αυτή είναι μια διαδικασία που βοηθά στο ξέπλυμα χρήματος (Αμπατζής).

2.3.6 Τρομοκρατία

Υπάρχουν ιστότοποι που ισχυρίζονται ότι χρησιμοποιούνται από το ISIL και το ISIS, συμπεριλαμβανομένου ενός ψεύτικου, που κατασχέθηκε από την Operation Onymous. Κανείς δε γνωρίζει αν και ποιοι είναι, πραγματικοί ή ψεύτικοι, ένα είναι σίγουρο όμως, ότι υπάρχουν (Αμπατζής).

2.3.7 Δολοφόνοι επί πληρωμή

Πρόκειται για σελίδες στις οποίες μπορείτε να προσλάβετε πληρωμένους δολοφόνους. Οι τιμές εξαρτώνται από το άτομο το οποίο είναι ο στόχος, και κυμαίνονται από μερικές χιλιάδες έως και δεκάδες χιλιάδες δολάρια. Σε τέτοιες σελίδες μπορείτε να βρείτε από ψυχρούς εκτελεστές, μέχρι και βασανιστές που θα κάνουν το θύμα τους να υποφέρει μέχρι να πεθάνει (Αμπατζής).

2.3.8 Pink Meth

Το Pink Meth είναι ένας ιστότοπος που περιέχει φωτογραφίες και βίντεο κοριτσιών προεφηβικής ηλικίας μέχρι ηλικιωμένων γυναικών. Οι χρήστες πληρώνονται για να ανεβάζουν το υλικό των πρώην τους. Πολλοί δημοσιεύουν προσωπικές πληροφορίες, όπως ονοματεπώνυμο, διευθύνσεις και άλλα. Έχει γίνει γνωστό πως η ιστοσελίδα έκλεισε από το FBI, όμως φήμες λένε πως έχει ανοίξει πάλι βαθιά στο Dark Web (Αμπατζής).

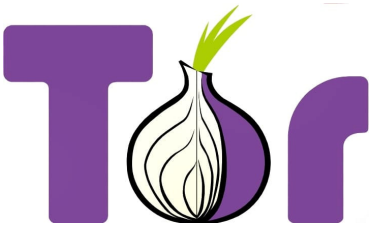
2.3.9 Ανθρώπινα πειράματα

Ένα άλλο είδος ιστοτόπων που βρίσκει κανείς στο Dark Web, είναι αυτές που προωθούν οργανισμούς που πραγματοποιούν βασανιστικά πειράματα σε ζωντανούς ανθρώπους. Το πιο σοκαριστικό κομμάτι είναι οι ακριβείς περιγραφές των πειραμάτων. Είτε είναι αληθινά, είτε ψεύτικα, οι περιγραφές των πειραμάτων είναι ανατριχιαστικές και οι εικόνες που τα συνδέουν ακόμη περισσότερο (Αμπατζής).

2.4 Είσοδος

Η είσοδος στο Dark Web είναι αρκετά εύκολη. Ανάλογα με το τι ακριβώς θέλετε να δείτε και σε τι ιστοσελίδες θέλετε να έχετε πρόσβαση, θα χρειαστείτε να χρησιμοποιήσετε διαφορετικές υπηρεσίες (Σακαλάκης).

2.4.1 Tor



Η πιο δημοφιλής υπηρεσία είναι ο Tor. Επισκεπτόμενοι το torproject.org, μπορείτε να κατεβάσετε δωρεάν το φυλλομετρητή του Tor και να τον εγκαταστήσετε στον υπολογιστή σας. Το δίκτυο θα εγκατασταθεί αυτόματα και ο Tor θα ανοίξει (Νικολαΐδης).

Ο Tor παρέχει ένα πολύ καλό εγχειρίδιο για το πώς λειτουργεί, αλλά κάποια απλά βασικά πράγματα θα τα εξηγήσουμε εδώ.

Το δίκτυο του Tor αντί να συνδέει τη συσκευή σας απευθείας στην ιστοσελίδα την οποία επισκέπτεστε, αλλάζει τη διαδρομή της συσκευής σας μέσα από μια σειρά servers και κρυπτογραφεί τα πάντα σε κάθε βήμα που ολοκληρώνει. Η γενική διαδικασία πίσω από την κρυπτογράφηση και την αλλαγή διαδρομής που κάνει ο Tor browser είναι πραγματικά απίστευτη και «απόλυτα» ανώνυμη (Σακαλάκης). Λειτουργεί διανέμοντας «πακέτα» με την πληροφορία που στέλνετε ή λαμβάνετε στο ίντερνετ μέσα από ένα δίκτυο που αποτελείται κυρίως από άλλους χρήστες του δικτύου, έτσι ώστε να χάνεται η πληροφορία της αρχικής προέλευσης του κάθε πακέτου. Εκτός από αυτά όμως, το δίκτυο Tor παρέχει κρυφές υπηρεσίες, δηλαδή ιστοσελίδες που λειτουργούν κανονικά χωρίς όμως να γίνεται να γνωρίσει κανείς από πού παρέχονται στον κόσμο. Εκεί εντοπίζουμε και τις ανώνυμες αγορές. Ο ασφαλέστερος τρόπος για να συνδεθείτε στο Tor είναι να κατεβάσετε το Tor Browser Bundle, που πρόκειται για ένα πακέτο με τον Firefox Web Browser, ειδικά τροποποιημένος για να παρέχει τη μέγιστη δυνατή ασφάλεια και ανωνυμία (Nssr).

Οι διευθύνσεις των ιστοσελίδων του Dark Web είναι δυσνόητες και έχουν πάντοτε την κατάληξη .onion. Έναν κατάλογο με κρυφά onion url θα βρείτε στο Hidden Wiki. Ο Tor δεν είναι το μοναδικό λογισμικό που μπορεί να σας βάλει στο Dark Web, αφού την ίδια δουλειά κάνουν μεταξύ άλλων και τα «Freenet» και «I2P» (Νικολαΐδης).

2.4.2 I2P

Το I2P (Invisible Internet Project) είναι ένα ακόμη δίκτυο που παρέχει ανωνυμία, αλλά με διαφορετική φιλοσοφία από τον Tor. Έχει αρκετά πλεονεκτήματα αλλά και λιγότερους χρήστες από τον Tor. Είναι απολύτως διανεμημένο και εστιάζει περισσότερο στην καλή απόδοση των κρυφών ιστοσελίδων που παρέχει.

Οι βασικές χρήσεις του πρωτοκόλλου αυτού είναι η πλοήγηση στο διαδίκτυο, οι συνομιλίες, οι μεταφορές αρχείων και το blogging. Για να συνδεθείτε θα χρειαστείτε να έχετε Java και να περάσετε το I2P. Αφού αυτό ολοκληρωθεί, θα χρειαστεί να ρυθμίσετε τον Browser σας κατά προτίμηση στο Firefox -> Option -> Advanced tab -> Network tab-> Connection Settings, έτσι ώστε να χρησιμοποιεί ως HTTP Proxy την IP 127.0.0.1 και το port 4444 και να μη χρησιμοποιεί Proxy για τις διευθύνσεις localhost 127.0.0.1 (Nssr).

2.4.3 Freenet

Το Freenet προσφέρει ένα διανεμημένο χώρο αποθήκευσης δεδομένων, ο οποίος μπορεί να φιλοξενεί οτιδήποτε, διότι κανείς δε μπορεί να περιορίσει το υλικό που περιέχει. Παρέχεται ανωνυμία, αλλά σε αντίθεση με τα Tor και το I2P, δεν μπορεί

να χρησιμοποιηθεί για πρόσβαση στο συνηθισμένο μας ίντερνετ. Μπορεί όμως να χρησιμοποιηθεί για την αποστολή και τη λήψη αρχείων, όπως και την πρόσβαση σε Freesites, ιστοσελίδες δηλαδή που βρίσκονται ως αρχεία στον χώρο αυτόν.

Η είσοδος στο Dark Web θα γίνει με την απάντηση στις παρακάτω τρεις λέξεις: ανωνυμία, ασφάλεια και μυστικότητα. Όλοι τα επιζητούμε, αλλά λίγοι έχουν την γνώση να τα χρησιμοποιήσουν σωστά.

Αν δεν ξέρετε τι να ψάξετε και πώς, πιθανότατα δε θα βρείτε τίποτα. Αν όμως ψάξετε αρκετά για το μέρος που σας δίνει τις τρεις παραπάνω επιθυμίες, μπορείτε πολύ εύκολα να βρεθείτε εκεί., και πολλές φορές δεν υπάρχει γυρισμός (Nssr).

2.5 Πάνω απ' όλα η ασφάλεια

Πριν από οτιδήποτε άλλο, είναι καλή ιδέα να εγκαταστήσετε μία εικονική μηχανή.

2.5.1 Δημιουργία εικονικής μηχανής

Μια εικονική μηχανή είναι πρακτικά ένας δεύτερος, ανεξάρτητος υπολογιστής, με το δικό του λειτουργικό σύστημα, μέσα στον υπολογιστή σας. Αυτό σημαίνει πως αν π.χ. η εικονική μηχανή μολυνθεί από κάποιον ιό, ακόμα και τα επικίνδυνα ransomware, η μόλυνση θα περιοριστεί σε αυτή και δεν θα περάσει στον υπόλοιπο υπολογιστή. Διαγράφοντας την εικονική μηχανή, θα εξαφανιστεί ό,τι κάνατε κατά τη χρήση της (Αναγνωστόπουλος).

2.5.2 Χρήση VPN

Η χρήση κάποιου προγράμματος VPN θα προσθέσει ένα ακόμη επίπεδο ασφαλείας. Τα VPN που προσφέρουν τη δυνατότητα χρήσης του Tor δεν είναι πολλά. Οι λύσεις που παρέχονται είναι αποκλειστικά επί πληρωμή. Το NordVPN είναι ένα από αυτά τα προγράμματα. Υπάρχουν όμως και άλλα VPN που υποστηρίζουν το δίκτυο Tor, συγκεκριμένα τα Privatoria και TorVPN (Αναγνωστόπουλος).

2.5.3 Γιατί VPN και μετά Tor, και όχι το αντίστροφο;

Αν χρησιμοποιήσετε VPN εντός του Tor, τότε απλά θα έχετε κρύψει τον εαυτό σας και την IP από τους χρήστες του δικτύου του Tor, όχι όμως και από το ίδιο το πρόγραμμα περιήγησης ή από τον πάροχό σας. Με άλλα λόγια, φαίνεται πως έχετε μπει στο δίκτυο Tor και έχουν υπάρξει περιπτώσεις που αυτό ήταν αρκετό για ενοχοποιηθεί ο χρήστης, εφόσον βέβαια είχε κάνει κάτι αξιόποινο.

Ξεκινώντας πρώτα το VPN και ύστερα το Tor, ούτε ο πάροχος δεν γνωρίζει πως κάνετε χρήση του Tor και σίγουρα η χρήση ενός VPN φαίνεται σαφώς πιο αθώα (Αναγνωστόπουλος).

2.5.4 Tor Browser

Στη συνέχεια κατεβάζετε από την επίσημη σελίδα τον Tor Browser. Με τη βοήθειά του θα αποκτήσετε πρόσβαση στο Dark Web (Αναγνωστόπουλος).

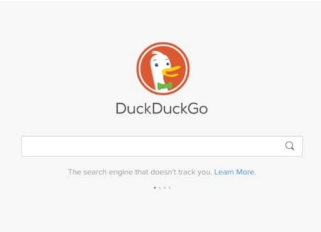
2.5.5 Απενεργοποίηση JavaScript

Στη συνέχεια, πρέπει να απενεργοποιήσετε τη JavaScript στον περιηγητή του Tor, διότι μπορεί να τρέξει οποιοδήποτε κομμάτι κώδικα στο σύστημά σας χωρίς καν να το γνωρίζετε και να γίνει μέσο συλλογής πληροφοριών. Ελέγχετε αν το «S» πάνω αριστερά έχει έναν κόκκινο κύκλο. Αν όχι, τότε η JavaScript είναι ενεργή. Για να την απενεργοποιήσετε, πατάτε στο «S» και επιλέγετε «Forbid scripts globally».

Ένας άλλος τρόπος απενεργοποίησης της JavaScript, είναι να μεταβείτε στο «about:config», να βρείτε την καταχώρηση «javascript.enabled» και κάνοντας διπλό κλικ στο «true», να το αλλάξετε σε «false» (Αναγνωστόπουλος).

2.6 Πώς βρίσκω ιστοσελίδες του Dark Web;

Έχοντας προετοιμάσει τον υπολογιστή σας, είστε έτοιμοι να συνδεθείτε σε σελίδες του Dark Web. Κάθε διεύθυνση που οδηγεί σε μια σελίδα του Σκοτεινού Ιστού είναι παρόμοια με αυτές των κανονικών ιστοσελίδων. Όπως αναφέρθηκα προηγουμένως, οι σελίδες αυτές έχουν κατάληξη .onion και το κύριο τμήμα τους είναι κρυπτογραφημένο. Οι πιο γνωστές μηχανές αναζήτησης του Tor είναι η DuckDuckGo Engine, και η Torch – Tor Search Engine.



Με αυτές βρίσκετε σελίδες του Tor, αλλά υπάρχουν όμως και διάφορα μέρη στο διαδίκτυο που διατηρούν λίστες με διευθύνσεις σελίδων Dark Web. Ίσως ο πιο ασφαλής χώρος για να πάρεις κάποιες διευθύνσεις, είναι η σελίδα της Wikipedia, που αφορά της κρυφές υπηρεσίες του Tor.

Ο μεγαλύτερος ιστότοπος με λίστες ενεργών σελίδων του Dark Web είναι το DeepWebLinks, και ένας λιγότερο γνωστός είναι το DeepWeb-Sites. Τα δύο αυτά site, εκτός από διευθύνσεις ιστοσελίδων, περιέχουν σημαντικό αριθμό από άρθρα και οδηγούς για το Σκοτεινό Ιστό. Αυτές είναι οι καλύτερες πηγές διευθύνσεων του Dark Web, και μια αναζήτηση στο Google θα σας επιστρέψει περισσότερες. Πάντα όμως πρέπει να είστε προσεκτικοί στην επιλογή των πηγών σας (Αναγνωστόπουλος).

2.7 Ασφαλείς ιστοσελίδες

Το Dark Web δεν είναι απαραίτητα ένας σκοτεινός κόσμος γεμάτος κινδύνους. Σε αυτόν μπορείτε να βρείτε πολλές ασφαλείς σελίδες και μάλιστα με αυθεντικό περιεχόμενο.

2.7.1 The Hidden Wiki

Μια πολύ ενδιαφέρουσα σελίδα υπήρξε το Hidden Wiki, το οποίο δυστυχώς δέχθηκε επίθεση από hackers το Μάρτιο του 2014 και λίγο καιρό αργότερα η διεύθυνσή του κατασχέθηκε στα πλαίσια της Operation Onymous.

Ευτυχώς το περιεχόμενό του έχει διασωθεί και συνεχίζει να εμπλουτίζεται. Πλέον φιλοξενούνται αντίγραφά του σε πολλές σελίδες, στις οποίες μπορείτε να αποκτήσετε πρόσβαση με μια αναζήτηση μέσω του Tor. Τα περιεχόμενα του Hidden Wiki δεν υπόκεινται σε λογοκρισία και είναι μια εκπληκτική πηγή γνώσεων (Αναγνωστόπουλος).

2.8 Άλλες υπηρεσίες

Στο Dark Web θα βρείτε πολλές υπηρεσίες που δεν είναι παράνομες. Το γεγονός ότι δεν λογοκρίνονται σίγουρα εγείρει ερωτήματα, όμως ο καθένας είναι υπεύθυνος για τον εαυτό του και τις πράξεις του.

Ο Σκοτεινός Ιστός διαθέτει υπηρεσίες διαμοιρασμού φωτογραφιών, ιστοσελίδες στις οποίες μπορεί κανείς να πραγματοποιήσει καταγγελίες χωρίς φόβο, ακόμη και συλλογές e-books, το περιεχόμενο των οποίων είναι λογοκριμένο στον «επιφανειακό κόσμο».

Ένα αρκετά προβληματικό τμήμα του Dark Web είναι αυτό των υπηρεσιών chat. Οι σελίδες που παρέχουν τέτοιες υπηρεσίες δέχονται πολλές επιθέσεις από τις αρχές και συχνά οδηγούνται στην απενεργοποίησή τους (Αναγνωστόπουλος).

ΚΕΦΑΛΑΙΟ 3^{Ο} DEEP WEB

3.1 Τι είναι το Deep Web

Ο «Βαθύς Ιστός», είναι το κομμάτι του διαδικτύου το οποίο δεν είναι ορατό από τις γνωστές μηχανές αναζήτησης. Ενώ αυτό ακούγεται περίπλοκο, στην πραγματικότητα είναι αρκετά απλό. Για παράδειγμα, τα προσωπικά σας email δεν εμφανίζονται στις μηχανές αναζήτησης, ειδάλλως ο καθένας θα είχε πρόσβαση με μια απλή αναζήτηση στο Google. Άρα, ο προσωπικός σας λογαριασμός email ανήκει πρακτικά στο Deep Web. Το ίδιο ισχύει για το προσωπικό σας e-banking, οι ρυθμίσεις του λογαριασμού σας στα social media, το διαχειριστικό περιβάλλον αν έχετε ένα δικό σας site κλπ. Στην πράξη, κάθε φορά που μπαίνετε στο ίντερνετ, είναι πολύ πιθανό να επισκέπτεστε τουλάχιστον μια σελίδα που αντικειμενικά ανήκει στο Deep Web. Εκτός από τους προσωπικούς σας λογαριασμούς, στο Deep Web ανήκουν και σελίδες στις οποίες έχετε πρόσβαση μόνο με κάποιον σύνδεσμο. Για παράδειγμα ένα βίντεο στο YouTube που έχει οριστεί ως «Μη καταχωρισμένο». Όποιος έχει το σύνδεσμο του βίντεο μπορεί να το δει κανονικά, ακόμα και αν δεν έχει λογαριασμό στο YouTube. Όμως, τα μη καταχωρισμένα βίντεο δεν εμφανίζονται ποτέ στην αναζήτηση του YouTube, ούτε ως προτεινόμενα δίπλα σε άλλα βίντεο. Στους χρήστες που δεν έχουν το σύνδεσμο θα λέγαμε ότι είναι εντελώς αόρατα.

Εξετάζοντας το περιεχόμενο του Deep Web, θα διαπιστώσετε πως είναι αυτό που περιέχει στη πραγματικότητα όλο το διαδίκτυο. Το μέγεθός του, σύμφωνα με μελέτες, είναι 400 έως 550 φορές μεγαλύτερο από το Surface Web (Αναγνωστόπουλος).

3.2 Είσοδος

Όπως και στο Dark Web, το κλειδί για να μπείτε σε αυτό το παράλληλο web είναι ο Tor. Ο Tor, όπως έχω ξανά αναφέρει, είναι ένα δίκτυο από μηχανήματα εθελοντών που επιτρέπει την ανώνυμη περιήγηση στο διαδίκτυο εφόσον ουσιαστικά, η πληροφορία που στέλνετε ή λαμβάνετε χρησιμοποιώντας το, περνά διάφορα στάδια κρυπτογράφησης και διάφορες διαδρομές, μέχρι τα δεδομένα να φτάσουν στον προορισμό που εσείς θέλετε. Είναι η πύλη για το Deep Web καθώς το δίκτυο λειτουργεί σε όλες τις πλατφόρμες (Lyberis).

3.3 Τι υπάρχει στο Deep Web;

- Δυναμικό περιεχόμενο: δυναμικές σελίδες στις οποίες έχει κάποιος πρόσβαση μόνο μέσα από φόρμες στις οποίες συμπληρώνει στοιχεία.
- Μη συνδεδεμένο περιεχόμενο: σελίδες που δε συνδέονται με άλλες σελίδες. Έτσι τα crawlers που χρησιμοποιούν οι μηχανές αναζήτησης, δε μπορούν να τις «βρουν» από άλλες σελίδες που εξετάζουν.
- Private Web: ιστοσελίδες που χρειάζεται να κάνετε login με username και password.
- Contextual Web: είναι οι σελίδες εκείνες. το περιεχόμενο των οποίων προσαρμόζεται ανάλογα με τον τρόπο που έχει κανείς πρόσβαση σε αυτό. Για παράδειγμα, στις σελίδες εκείνες που αν έχετε πρόσβαση με μια διεύθυνση IP από την Ελλάδα, τις βλέπετε με διαφορετικό περιεχόμενο από το αν θα επισκεπτόσασταν την ίδια σελίδα από μια IP των ΗΠΑ.
- Περιεχόμενο περιορισμένης πρόσβασης: ιστοσελίδες που περιορίζουν την πρόσβαση στο περιεχόμενό τους με τεχνικούς τρόπους.(Robots Exclusion , CHAPTCHAS και άλλα).
- Scripted content: σελίδες που είναι διαθέσιμες μόνο από συνδέσμους που παράγονται από JavaScript καθώς και περιεχόμενο που κατεβάζεται από Web servers μέσω Flash π.χ.
- Non-HTML/text content: περιεχόμενο κειμένου που είναι κωδικοποιημένο σε αρχεία multimedia ή συγκεκριμένα formats που δεν μπορούν να διαβάσουν οι μηχανές αναζήτησης.
- Οτιδήποτε δεν ακολουθεί το πρότυπο HTTP/HTTPS (Lyberis).

3.4 Είναι ασφαλές, είναι ανώνυμο;

Στο Deep Web δεν υπάρχουν φίλτρα που θα χαρακτηρίσουν ένα περιεχόμενο ως καλό ή κακό, ούτε υπάρχει κάποια διασφάλιση για τις συναλλαγές σας εκεί. Επομένως, αν περιμένετε από κάποιον να σας προστατεύει για το περιεχόμενο που θα δείτε, τότε δεν πρέπει να μπείτε καν στη διαδικασία.

Όσον αφορά για το αν είναι ανώνυμο ή όχι, τότε όχι δεν είναι. Όπως, όταν εξακολουθείτε να χρησιμοποιείται τις παλιές σας συνήθειες κατά τη διάρκεια του σερφαρίσματος. Παραδείγματος χάριν, αν αποφασίσετε για οποιονδήποτε λόγο να

κάνετε κάποια συναλλαγή που μπορεί να σας εκθέσει και δώσετε το λογαριασμό Gmail σας που δείχνει ξεκάθαρα το όνομά σας, δε μιλάμε για ανωνυμία.

Σε θέματα που αφορούν το κακόβουλο λογισμικό, δεν διατρέχετε τέτοιο κίνδυνο αν έχετε πρόσβαση στο Deep Web μέσω του Tails OS κυρίως. Επίσης, καθώς το πρόγραμμα τρέχει από τη RAM σας και δεν αφήνει ίχνη στον υπολογιστή που χρησιμοποιείτε, δεν έχετε κάποιο ζήτημα αναγνώρισης της ταυτότητάς σας (Lyberis).

3.5 Υπάρχει λόγος πρόσβασης στο Deep Web;

Αν πιστεύετε πως η ανωνυμία σας πλήττεται και εξακολουθείτε να θέλετε να χρησιμοποιήσετε το διαδίκτυο για να αναζητήσετε πληροφορίες και να επικοινωνήσετε, χωρίς να σας καταγράψει κάποιος για αυτό˙ αν ανήκετε σε μια πληθυσμιακή ομάδα που βρίσκεται σε κίνδυνο ή παρακολούθηση και θέλετε να επικοινωνήσετε ανώνυμα, τότε ναι.

Το Deep Web δεν είναι παιχνίδι. Αν πιστεύετε πως το διαδίκτυο είναι τα social media και τα selfies που μοιράζεστε μέσα από αυτό, δεν υπάρχει κανένας λόγος να ασχοληθείτε με το Deep Web. Επίσης, δεν υπάρχει κανένας λόγος να ασχοληθείτε αν η χρήση που κάνετε στο διαδίκτυο δεν έχει κάποιες πιο «ευρείες» αναζητήσεις. Και όχι, δεν υπάρχει κανένας λόγος να εμπλακείτε με το Deep Web, αν δε μπορείτε να αντιμετωπίσετε την εμπειρία ενός χαοτικού περιεχομένου με ότι προέκταση μπορεί να έχει αυτό. Από ενοχλητικές ή απειλητικές συζητήσεις, μέχρι παράνομο και επικίνδυνο υλικό (Lyberis).

3.6 Ιστορίες τρόμου μέσα από το Deep Web

- **Ιστορία 1η**

Το συμβάν έγινε καιρό πριν το Google. Οι ιστοσελίδες ήταν κατά κύριο λόγο πολύ βασική html με Javascript. Σπάνια χρησιμοποιούταν το CSS. Έβλεπα τυχαία blogs και σύντομα έφτασα σε μια περίεργη σελίδα. Έμοιαζε σαν να ήταν πολλές τυχαίες σκέψεις από διαφορετικούς ανθρώπους, αλλά για την εποχή του ήταν πολύ καλοσχεδιασμένη. Τα μηνύματα φαίνονταν να ήταν αινιγματικά σαν κάποιοι άνθρωποι να προσπαθούσαν να δώσουν κρυφά μηνύματα ο ένας στον άλλον. Έψαξα στη πηγή της και κρυμμένος στα σχόλια του Javascript υπήρχαν διάφορες

διευθύνσεις IP. Αφού τις μάζεψα όλες τις έβαλα σε ένα αρχείο κειμένου και ξεκίνησα τον αποκλεισμό. Κάποιοι ήταν routers με μηνύματα που μπορούσα να συνδεθώ. Σχεδόν όλες σε πανεπιστήμια, που δε προσπάθησα να μπω για λόγους ασφαλείας του δικτύου τους. Μερικά από τα IP ήταν άδειοι servers. Επιτέλους βρήκα ένα server, με ένα τεράστιο ευρετήριο με αρχεία HTML, με κάποια άλλα μικρότερα ευρετήρια που περιείχαν τα ίδια πράγματα. Δεν μπορούσα να βρω κάποιο άλλο IP. Ένα visual route εντόπισε το κέντρο στο Κολοράντο. Τα αρχεία φαινόντουσαν να είναι φάκελοι που θα κρατούσε ένας ψυχολόγος, ή εμπειρογνώμον γιατρός. Οι εικόνες ήταν φαξ. Ενώ έψαχνα από ευρετήριο σε ευρετήριο, στην κορυφή υπήρχε ένα καινούριο αρχείο με όνομα κάτι σαν γεια σου.html. Οι όροι δημιουργίας του έγιναν ακριβώς εκείνη τη στιγμή. Όταν το άνοιξα υπήρχε ένα απλό κείμενο που έγραφε…. σε βλέπουμε (Gloomy Gentlemen).

- **Ιστορία 2η**

Όλα ξεκίνησαν πριν από περίπου ένα χρόνο. Όταν τριγυρνούσα σε κάποια ανατριχιαστικά site στο Dark Web. Εκεί συνάντησα ένα ασυνήθιστο βίντεο που έδειχνε ένα σκοτεινό δωμάτιο, το οποίο φωτιζόταν μοναχά από ένα κερί. Θυμάμαι να βλέπω έναν άντρα να μπαίνει μέσα από μια πόρτα μέσα σε αυτό το δωμάτιο. Φορούσε μονάχα μαύρα και το πρόσωπό του ήταν βαμμένο με μαύρη μπογιά. Το μόνο που μπορούσα να ξεχωρίσω ήταν τα τεράστια άσπρα του μάτια να με κοιτάζουν από την οθόνη του υπολογιστή. Τον θυμάμαι να κουνάει τα χείλι του και να ψιθυρίζει κάτι που δεν μπορούσα να ακούσω. Έτσι ανέβασα τον ήχο στο λάπτοπ. Με το που το έκανα αυτό ο άντρας έτρεξε προς τη κάμερα φωνάζοντας. Αυτό με έκανε να πέσω από την καρέκλα και όταν σηκώθηκα ξανά, εκείνος άρχισε να γελάει με ένα δαιμονικό γέλιο που όμοιό του δεν είχα ξανακούσει. Ξαφνικά το γέλιο σταμάτησε και το λάπτοπ μου πάγωσε. Η οθόνη μαύρισε κι έμεινε έτσι για μερικά λεπτά, ώσπου μια λέξη με μεγάλα άσπρα γράμματα εμφανίστηκε και έγραφε….. επιλέχτηκες. Δεν μπορούσα να συνειδητοποιήσω τι έβλεπα. Έτσι έμεινα στη καρέκλα μου προσπαθώντας να βάλω τις σκέψεις μου σε μια σειρά. Η λέξη βρισκόταν ακόμη στην οθόνη και όσο και αν προσπάθησα δεν μπορούσα να τη βγάλω. Κατέληξα να πάρω ένα κατσαβίδι και να βγάλω την μπαταρία από το λάπτοπ και για τον επόμενο μήνα δε το ξαναακούμπησα. Ο καιρός περνούσε και

είχα αρχίσει να ξεχνάω το περίεργο εκείνο συμβάν, μέχρι που ο ήχος άρχισε να ακούγετε. Ένας αχνός χτύπος στο παράθυρο μου κάθε βράδυ. Αυτός ο χτύπος, επηρέαζε πραγματικά τη ζωή μου. Η κοινωνική μου ζωή χειροτέρεψε. Άρχισα να τα πηγαίνω χάλια στο σχολείο. Όλα αυτά εξαιτίας του αναθεματισμένου αυτού χτύπου που έκανε τη διάθεσή μου να χαλάσει. Ξέρω τι σκέφτεστε. Γιατί δεν κοίταξα έξω από το παράθυρο. Πράγματι το έκανα, αλλά κάθε φορά που πλησίαζα το παράθυρο, ο χτύπος σταματούσε και μόλις ξάπλωνα στο κρεβάτι, εκείνος ξεκινούσε πάλι. Το να φτάσει κανείς στο παράθυρό μου είναι αρκετά δύσκολο, γιατί είναι αρκετά ψηλά. Μετά από έξι μήνες αυτής της κατάστασης αποφάσισα να βρω ποιος ή τι ήταν αυτό που προκαλούσε αυτόν τον ήχο. Αυτό που έκανα ήταν να αγοράσω μια μικρή ψηφιακή κάμερα, την οποία τοποθέτησα έξω να καταγράφει το παράθυρο μου, κρυμμένη τόσο καλά σε ένα δέντρο που μονάχα αν ήξερες ότι ήταν εκεί θα μπορούσες να τη δεις. Όταν έφτασε η νύχτα ξάπλωσα στο κρεβάτι και περίμενα πότε θα ακουστεί αυτός ο ήχος. Προς μεγάλη μου έκπληξη ποτέ δεν ξεκίνησε. Έτσι, αποφάσισα να κοιτάξω έξω από το παράθυρο για να δω αν η κάμερα είχε κουνηθεί από τη θέση της. Μόλις άνοιξα τις κουρτίνες πάγωσα, γιατί αυτό που έβλεπα πίσω από το αχνό φως του φεγγαριού ήταν τα δυο κάτασπρα μάτια που με κοιτούσαν από το βίντεο πριν μήνες να με κοιτούν τώρα πίσω από το τζάμι του σπιτιού μου (Gloomy Gentlemen).

ΚΕΦΑΛΑΙΟ 4^{Ο} ΜΥΘΟΙ ΚΑΙ ΑΛΗΘΕΙΕΣ ΓΥΡΩ ΑΠΟ ΤΟ DEEP WEB ΚΑΙ ΤΟ DARK WEB

- **Μύθος 1: Το Deep Web και το Dark Web είναι το ίδιο πράγμα.**

Αλήθεια: Το Dark Web είναι υποσύνολο του Deep Web, οπότε η δήλωση ότι το Deep Web και το Dark Web είναι το ίδιο πράγμα είναι μια εσφαλμένη κατανόηση των δύο ορών.

- **Μύθος 2: Το Dark Web είναι αδιαπέραστο**

Αλήθεια: Το Dark Web μπορεί να προπελαστεί μέσω ειδικών δικτύων όπως ο Tor, I2P και Freenet. Αυτά τα δίκτυα προστατεύουν το απόρρητο του χρήστη, αποκρύπτοντας τη διεύθυνση IP τους και όλη η ηλεκτρονική τους δραστηριότητα

διατηρείται ανώνυμη. Αυτή η ανωνυμία επιτυγχάνεται με τη δρομολόγηση των δεδομένων του χρήστη μέσω ενός μεγάλου αριθμού ενδιάμεσων εξυπηρετητών, παρέχοντας κρυπτογράφηση σε κάθε στρώμα το οποίο δρομολογεί την κίνηση του χρήστη.

- **Μύθος 3 : Το Dark Web είναι γεμάτο κακόβουλη δραστηριότητα.**

Αλήθεια: Ναι θα βρείτε παράνομες δραστηριότητες στο Dark Web, αλλά αυτό δεν είναι η μόνη χρήση για μια πλατφόρμα που παρέχει ανωνυμία στον χρήστη. Για παράδειγμα, στις χώρες που υπάρχει λογοκρισία στο διαδίκτυο, μια πλατφόρμα όπως ο Tor, μπορεί να προσφέρει στο χρήστη πρόσβαση σε περιεχόμενο που μπορεί να «απαγορεύεται» από την εκάστοτε κυβέρνηση. Το Dark Web μπορεί επίσης, να είναι ένα εργαλείο για τους δημοσιογράφους που επιδιώκουν να μεταβιβάσουν με ασφάλεια τις ευαίσθητες πληροφορίες (Vasileiadis).

ΚΕΦΑΛΑΙΟ 5^{Ο} SURFACE WEB

5.1 Τι είναι το Surface Web;

Ένας ιδανικός τρόπος για να κατανοήσετε τις ταξινομήσεις του ιστού είναι να τον παρομοιάσετε με έναν ωκεανό. Ο επιφανειακός ιστός ή αλλιώς Surface Web είναι παρόμοιος με την επιφάνεια του ωκεανού, το τμήμα που είναι εύκολα ορατό και προσβάσιμο από υπηρεσίες όπως το Google Chrome, το Mozilla Firefox και το Microsoft Edge.

Ο επιφανειακός ιστός περιέχει όλα όσα είναι δημόσια προσβάσιμα μέσω μιας μηχανής αναζήτησης. Αυτό είναι το τμήμα του ιστού στο οποίο έχετε πρόσβαση όταν διαβάζετε ένα άρθρο σε ένα site ειδήσεων, όταν αγοράζετε κάτι από το Amazon ή παρακολουθείτε βίντεο στο YouTube (Absenta).

5.2 Οι διαφορές ανάμεσα στο Surface Web, Dark Web και Deep Web

Τον επιφανειακό ιστό όπως ανέφερα και παραπάνω μπορούμε να τον παρομοιάσουμε με την επιφάνεια του ωκεανού. Το Deep Web είναι ένα στρώμα κάτω από την επιφάνεια που θα χρειαζόσασταν εξοπλισμό κατάδυσης για να πάτε, ενώ το Dark Web είναι το στρώμα ακόμα πιο κάτω από το Deep Web. Ο πυθμένας του ωκεανού που μόνο με υποβρύχιο γίνεται προσβάσιμος. Το Dark Web είναι μέρος του Deep Web με τη μόνη διαφορά ότι είναι ειδικά σχεδιασμένος για να μην είναι προσβάσιμος από τα κανονικά προγράμματα περιήγησης.

Ο επιφανειακός ιστός θεωρείται ότι αποτελεί το 5% του συνόλου του παγκόσμιου ιστού. Ένας αριθμός που φαίνεται μικροσκοπικός αλλά δείχνει απλά πόσα δεδομένα υπάρχουν στον ιστό σήμερα. Το Deep Web πιστεύεται ότι είναι από 500 έως και 5.000 φορές μεγαλύτερο. Υπάρχουν περίπου είκοσι terabytes δεδομένων και περίπου ένα δισεκατομμύριο έγγραφα στον επιφανειακό ιστό σε σύγκριση με 7.500 terabytes δεδομένων και σχεδόν 600 δισεκατομμυρίων εγγράφων που ανακαλύφθηκαν στο Deep Web.

Το Deep Web είναι ουσιαστικά το αντίθετο του Surface Web, καθώς περιέχει δεδομένα που δεν μπορούν να ανακαλυφθούν από μια μηχανή αναζήτησης. Τα δεδομένα αυτά εξακολουθούν να είναι προσβάσιμα στο κοινό, αν και θα χρειαστείτε ειδική πρόσβαση, με τη μορφή διαπιστευτηρίων πρόσβασης. Ένα καλό παράδειγμα των δεδομένων στο Deep Web, είναι το pin που δημιουργείτε για να

αποκτήσετε πρόσβαση στον τραπεζικό σας λογαριασμό ή στα εισερχόμενα Gmail (Absenta).

ΚΕΦΑΛΑΙΟ 6^{Ο} HACKERS

6.1 Ορισμός hacking;

Η δραστηριότητα αυτή που είναι γνωστή σαν hacking προσδιορίζεται ως η

> «….πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή ή περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα ηλεκτρονικών τηλεπικοινωνιών, εφόσον οι πράξεις αυτές έγιναν χωρίς δικαίωμα, ιδίως με παραβίαση των μέτρων ασφαλείας που είχε λάβει ο νόμιμος κάτοχός τους…» (ά. 370Γ & 2 Π.Κ), (Κιούπης,1999).

Βλέπουμε λοιπόν ότι, η συγκεκριμένη εγκληματική συμπεριφορά αφορά απλά και μόνο την παράνομη διείσδυση σε συστήματα και επικοινωνίες υπολογιστών, η οποία τελείται με την παραβίαση των μέτρων ασφαλείας που είχε λάβει ο νόμιμος κάτοχός τους και ανεξάρτητα από τους λόγους για την οποία την επιχειρεί ο δράστης (Τσουραμάνη Χρ.Ε. και Κορολή Μαρ.-Ευγ., Τ.Ε.Ι Δυτικής Ελλάδας, σ.142).

6.2 Τι είναι hacker;

Ο περισσότερος κόσμος αποκαλεί λανθασμένα hackers, αυτούς που προβαίνουν σε κακόβουλες πράξεις μέσω διαδικτύου. Ένας hacker είναι εκείνος που ενδιαφέρεται έντονα για τις μυστικές και κρυφές λειτουργίες οποιουδήποτε λειτουργικού συστήματος υπολογιστή. Στην πλειοψηφία των περιπτώσεων οι

hackers είναι προγραμματιστές και για αυτό το λόγο έχουν εκτενή και σε βάθος γνώση των λειτουργικών συστημάτων και των γλωσσών προγραμματισμού. Προσπαθούν να ανακαλύψουν τα «κενά» στα συστήματα των υπολογιστών, καθώς και τους λόγους ύπαρξης αυτών των «κενών». Οι hackers αναζητούν σταθερά πρόσθετη γνώση, μοιράζοντας ελεύθερα ότι έχουν ανακαλύψει και ποτέ δεν καταστρέφουν δεδομένα σκοπίμως (ΕΡΓΑΣΤΗΡΙΟ ΕΦΑΡΜΟΓΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΣΤΑ ΜΜΕ).

6.3 Ομάδες hacker

6.3.1 Ο αληθινός

Ο αληθινός hacker διαθέτει τρομερά αποθέματα γνώσης, τα οποία είναι συνήθως σφαιρικά συνδεδεμένα στο μυαλό του, αλλά και μεταξύ τους, σαν θεματικές ενότητες. Δεν είναι απαραιτήτως πληροφορίες που έχουν να κάνουν αποκλειστικά και μόνο με τους ηλεκτρονικούς υπολογιστές. Μιλάμε για κατοχή γνώσης σε πολλά επίπεδα και σε πολλές θεματικές ενότητες. Δεν πρέπει να ξεχνάμε πως οι περισσότεροι hackers βλέπουν τους ηλεκτρονικούς υπολογιστές σαν ένα χόμπι, μια ενασχόληση για να περνά η ώρα τους. Απλώς τυχαίνει να είναι εξαιρετικοί σε αυτό που κάνουν.

Πολλές φορές ο αληθινός hacker έχει χαρακτηριστεί ως χαμαιλέοντας της σημερινής μας κοινωνίας. Είναι τρομερά επίμονος και υπομονετικός, αλλά με έναν καλό σχετικά χαρακτήρα. Συνήθως δεν ξοδεύει ενέργεια σε καταστάσεις που είναι χαμένες. Απλώς ακολουθεί το δικό του κώδικα τιμής και έχει ένα ιδιαίτερα καυστικό χιούμορ.

Τις περισσότερες φορές ένας hacker μοιάζει να παρακολουθεί αθέατος και άπραγος, αλλά συνήθως προτιμά να παίρνει με διακριτικό τρόπο τις πληροφορίες ή τις γνώσεις που χρειάζεται, και κατόπιν να παρακολουθεί τις εξελίξεις που θα επιφέρουν οι όποιες κινήσεις του. Τις γνώσεις ή τις πληροφορίες τις οποίες συλλέγει, τις καταγράφει ή τις αντιγράφει για τον εαυτό του.

Του αρέσουν πάρα πολύ τα καινούρια πράγματα που μαθαίνει. Έτσι έχει δύο τρόπους στης ευχέρειά του για να αποκτήσει τη γνώση. Ο πρώτος είναι να πληρώσει και να «σπουδάσει», αποκτώντας τη γνώση μέσα από βιβλία του εμπορίου κλπ, ενώ ο δεύτερος τρόπος είναι να καθίσει και να προσπαθήσει να

εκμαιεύσει τη γνώση μέσα από συζητήσεις με άτομα τα οποία είναι το ίδιο «δυνατά» με εκείνους τους τομείς που ενδιαφέρουν τον hacker. Υπάρχει κι ένας τρίτος τρόπος στον οποίο ο hacker πρέπει να τα βρει και να τα μάθει όλα μόνος του. Συμπερασματικά, ο hacker πρέπει να ξοδέψει αρκετό χρόνο, όχι μόνο για να διαβάσει τις εισερχόμενες πληροφορίες, αλλά και για να τις αξιολογήσει και στη συνέχεια να αποφασίσει αν όντως του είναι χρήσιμες και ενδιαφέρουσες (Σαράφας, 2008, σ.18).

6.3.2 Ο ρομαντικός

Ο ρομαντικός τύπος hacker είναι ο δεύτερος πιο ενδιαφέρων τύπος, μετά τον αληθινό. Ο ρομαντικός hacker έχει φιλοσοφικές κατευθύνσεις. Προτιμά να μην υπερηφανεύεται για τα κατορθώματά του ή για τις γνώσεις του. Φτάνει σε ένα πολύ καλό επίπεδο γνώσεων και μετά αρχίζει να λειτουργεί πιο αργά., και περνά πολύ ώρα σκεφτόμενος το δίλλημα αν αυτό που κάνει είναι σωστό ή όχι. Συνήθως χάνεται σε φιλοσοφικές και διανοητικές διαμάχες οι οποίες αφορούν στη θέση του στον πραγματικό κόσμο, πράγμα το οποίο πείθει τους γύρω του για την ανασφάλεια που τον διακατέχει. Είναι ο πλέον πολιτικά ορθός χαρακτήρας της ομάδας των hacker. Έχει συναισθήματα και αυτό τον κάνει ίσως πιο επικίνδυνο από τους άλλους χαρακτήρες της ομάδας αυτής, αφού κάτι σοβαρό και προσωπικό μπορεί να τον βγάλει από το καβούκι του, από την κατάσταση χειμερίας νάρκης με την οποία έχει επιλέξει να περιβληθεί για να έχει την ησυχία του. Πιστεύει και πραγματικά είναι σε θέση να αποδείξει πως οποιοσδήποτε μπορεί να είναι ή να γίνει hacker. Είναι συνήθως πάρα πολύ ειρωνικός χαρακτήρας, αλλά μπορεί πολύ εύκολα να μεταλλαχθεί σε έναν άνθρωπο χωρίς συναίσθημα και ψυχή.

Σκοπός του είναι να συγκαταλέγεται στους καλύτερους ή ακόμα και να γίνει ο καλύτερος hacker. Αυτό θέλει να το πετύχει με τη χρήση του μυαλού του και όχι με τη χρήση των γνώσεων που κατέχει.

Εν κατακλείδι, πρέπει να σημειωθεί πως αρκετοί είναι αυτοί που νομίζουν ότι η συγκεκριμένη ομάδα των hacker, είναι οι «τρομοκράτες» του σημερινού τους κόσμου (Σαράφας, 2008, σ.21).

6.3.3 Ο wannabe

Αυτή είναι η τρίτη ομάδα των hacker. Σε αυτή την ομάδα μπορεί κανείς να βρει πολλά άτομα τα οποία έχουν διαφορετικές ηλικίες, αλλά και προέρχονται από διαφορετικούς τομείς. Είναι ευερέθιστοι και τις περισσότερες φορές μοιάζουν να μη μπορούν να κρατήσουν μυστικές τις ικανότητες οι οποίες τους έφτασαν μέχρι αυτό το σημείο. Δε σταματούν μπροστά σε τίποτα στο δρόμο τους για την κορυφή, αλλά έχουν την κακή συνήθεια να μιλούν και να υπερηφανεύονται για αυτά που μπορούν να επιτύχουν. Αν βρεθούν στη δυσάρεστη θέση να ανακαλυφθούν την ώρα της «εργασίας» τους, συνήθως ζητούν συγνώμη κι έπειτα προτιμούν να εξαφανιστούν από το παρασκήνιο. Εάν κάποιος καλύτερος hacker ή απλώς ένας καλύτερος χρήστης των ηλεκτρονικών υπολογιστών εμφανιστεί στο δρόμο τους, τότε η επιλογή τους είναι να φύγουν αρκετά μακριά. Είναι τρομερά ανασφαλείς και δεν πιστεύουν πραγματικά στις ικανότητές που έχουν (Σαράφας, 2008, σ.23).

6.3.4 Ο lamer

Είναι μια ομάδα για την οποία οι ίδιοι οι hackers δεν είναι και τόσο περήφανοι. Το όνομα αυτής της ομάδας αποτελεί και το χαρακτηρισμό της. Κανένας hacker δε θέλει να χαρακτηριστεί ως lamer και ούτε θέλει να είναι ένα με αυτούς. Ο συνήθης τρόπος εργασίας τους δεν οφείλεται σε γνώσεις ή στη χρήση του μυαλού τους. Απλώς εισέρχονται σε συζητήσεις που γίνονται γύρω τους, όπου βροντοφωνάζουν ότι είναι hackers και ότι είναι σε θέση να κάνουν και να εφαρμόσουν χίλια δυο κόλπα με τους ηλεκτρονικούς υπολογιστές.

Ο καλύτερος τρόπος για να τους ξεφορτωθεί κανείς είναι να τους φωνάξει με το πραγματικό τους όνομα, lamer. Αυτός ο τρόπος φέρνει τα επιθυμητά αποτελέσματα, αφού οι lamers δε διαθέτουν τις γνώσεις του «επαγγέλματος» του hacker, αλλά ούτε και μπορούν να κάνουν κάτι άλλο εκτός από το να μιλούν.

Τις πιο πολλές φορές οι γνώσεις που κατέχουν είναι από άτομα, ιστορίες ή προγράμματα που τυχαία βρέθηκαν στα χέρια τους. Υποστηρίζουν ότι είναι hackers μόνο και μόνο για να εντυπωσιάσουν ή απλώς για να δείξουν ότι είναι κάποιοι.

Είναι τρομερά εύκολο να τους βρει κανείς και να τους κάνει να τρέχουν. Σχεδόν κανένας δεν προσέχει αυτά που λένε, εκτός ίσως από τα μέσα μαζικής ενημέρωσης, που προσπαθούν να βρουν αποκλειστικότητες από lamer-hackers, οι

οποίοι, με τη σειρά τους, είτε θέλουν να περάσουν ως hackers είτε προσφέρουν δικαιολογία για καλά νούμερα τηλεθέασης.

Οι ιστορίες οι οποίες περιβάλλουν αυτή την ομάδα κάνουν τους ανθρώπους που πραγματικά γνωρίζουν να αναρωτιούνται για το IQ που χαρακτηρίζει τους lamers ως ομάδα, αλλά και για το IQ το οποίο φαίνεται να έχουν και να προβάλλουν ορισμένα άτομα στα μέσα μαζικής ενημέρωσης (Σαράφας, 2008, σ.24).

6.3.5 Ο ονειροπόλος

Αυτοί οι ομάδα hacker αποτελείται από άτομα τα οποία είναι πολύ καλοί χρήστες των ηλεκτρονικών υπολογιστών, αλλά γνωρίζουν ελάχιστα για τους ηλεκτρονικούς υπολογιστές, εκτός από κάποια προγράμματα τα οποία χρησιμοποιούν καθημερινά και τυχαίνει να τα «κατέχουν» πάρα πολύ καλά.

Είναι ικανότατοι γνώστες και χειριστές κάποιων προγραμμάτων. Η γνώση τους ωστόσο είναι περιορισμένη, επειδή δε θέλουν ή δεν μπορούν να αποκτήσουν περισσότερη. Η γνώμη τους πάντα μετράει και μπορούν να βοηθήσουν σε αρκετές περιπτώσεις τις άλλες ομάδες, απλώς και μόνο με το να μοιραστούν τις γνώσεις τους και να επιταχύνουν έτσι την εκτέλεση των προγραμμάτων.

Σε πάρα πολλές περιπτώσεις μπορούν να μάθουν πολύ γρήγορα το χειρισμό ή ακόμα και τη φιλοσοφία που κρύβεται πίσω από τα προγράμματα που τους δίνονται. Θα ήθελαν και θα μπορούσαν να πάρουν μέρος σε άλλες ομάδες, αλλά είτε τους λείπει η θέληση, είτε δεν έχουν χρόνο.

Είναι ιδιαίτερα επιρρεπείς σε διάφορα καλοπροαίρετα σχόλια, πράγμα το οποίο τους κάνει εύκολους στόχους για την αποκάλυψη γνώσεων τις οποίες κατέχουν. Ονειροπολούν πολύ και περιμένουν τη στιγμή που θα διαπρέψουν πραγματικά στον κόσμο των ηλεκτρονικών υπολογιστών.

Η δημιουργικότητα που τους χαρακτηρίζει και τους διακρίνει είναι τόσο πολύ αυξημένη, ώστε μπορούν να εκφράζονται μέσα από κανάλια πρωτόγνωρα για τις υπόλοιπες ομάδες των hacker. Με λίγα λόγια, αυτοί αποτελούν τους «καλλιτέχνες» της κοινωνίας των hacker (Σαράφας, 2008, σ.25).

6.3.6 Ο θετικός

Αυτή είναι η ομάδα των hackers που είναι υπεύθυνη για την ασφάλεια και τη διατήρηση της ειρήνης και του πολιτισμού στη μικρή τους κοινωνία. Συνήθως

διακρίνονται για την ηρεμία και για τον τρόπο σκέψης τους, ο οποίος είναι σταθερός και αρκετά «άκαμπτος». Εισχωρούν στις διάφορες ομάδες των hackers και προσπαθούν να λύσουν προβλήματα τα οποία έχουν προκληθεί, είτε από τους υπόλοιπους hackers, είτε από τις μεγάλες πολυεθνικές εταιρίες.

Στο παρελθόν, τα άτομα τα οποία άνηκαν σε αυτή την ομάδα είχαν κατηγορηθεί ως προδότες και τσιράκια, αλλά ποτέ δεν έχει αποδεχθεί κάτι τέτοιο. Συνήθως έχουν τίμιες δουλειές σε σοβαρές εταιρίες ηλεκτρονικών υπολογιστών και αρκετές φορές είναι υπεύθυνοι για την ασφάλεια των εταιριών αυτών.

Είναι οι συνήθεις ύποπτοι για την επισκευή, επίδειξη και ανίχνευση λαθών σε συστήματα ή σε προγράμματα τα οποία κυκλοφορούν στο εμπόριο.

Σε αρκετές περιπτώσεις δεν ξεχνούν το σημείο από όπου ξεκίνησαν και ως αποτέλεσμα αποφεύγουν να κυνηγούν άλλους hackers. Ωστόσο, αυτό δε σημαίνει ότι δε θα το κάνουν.

Υπάρχει πάντα και η περίπτωση να τα παρατήσουν όλα και να γυρίσουν πίσω στην ομάδα των hackers, αν νιώσουν πως τους χρησιμοποίησαν ή ακόμα και αν υποψιαστούν ότι παίζονται διάφορα άσχημα παιχνίδια πίσω από την πλάτη τους (Σαράφας, 2008, σ.26).

6.3.7 Τα ξέρω όλα

Αυτή είναι η τελευταία και ενδεχομένως η πιο μισητή ομάδα που απαρτίζει τον κόσμο των hackers. Σίγουρα κατέχουν κάποιες γνώσεις, αλλά σχεδόν ποτέ δε μπορεί να είναι κανείς σίγουρος για αυτές ή για τις ικανότητες τις οποίες φωνάζουν πως κατέχουν.

Αποτελείται από άτομα τα οποία έχουν τελειώσει κάποια σχολή ή ανώτατη εκπαιδευτική βαθμίδα. Χαρακτηρίζονται από μια ακατάπαυστη στενομυαλιά, η οποία τους οδηγεί στην πλάνη να πιστεύουν ότι είναι οι καλύτεροι των καλυτέρων σε σημείο τέτοιο, ώστε να πιστεύουν πως όχι μόνο γνωρίζουν, αλλά και κατέχουν τα μυστικά της τέχνης των ηλεκτρονικών υπολογιστών.

Καθημερινά πραγματοποιούν πολλά λάθη και ιεροσυλίες, επειδή δίνουν λανθασμένες γνώσεις ή ακόμη και γνώσεις τις οποίες προηγουμένως έχουν «πειράξει». Προσπαθούν να κάνουν τους ανυποψίαστους χρήστες να πιστέψουν ότι ξέρουν από hacking, ενώ στην πραγματικότητα αποτελούν απλώς εξαιρετικό υλικό για ανέκδοτες ιστορίες.

Είναι χειρότεροι και από την ομάδα των lamers. Τουλάχιστον εκείνοι δεν υποστηρίζουν λάθος πράγματα ούτε και στηρίζονται σε κάποια χαρτιά που αποκόμισαν. Καλό είναι να τους αποφεύγει κανείς όσο πιο γρήγορα και να αποστασιοποιείται πολύ από αυτούς. Αλλιώς, διατρέχει μεγάλο κίνδυνο να ξεχάσει και αυτά τα λίγα τα οποία ξέρει (Σαράφας, 2008, σ.28).

6.4 Τι είναι cracker;

Ένας «κράκερ», είναι εκείνος που διεισδύει ή διαφορετικά παραβιάζει την ακεραιότητα συστήματος απομακρυσμένων μηχανημάτων, με κακή πρόθεση. Έχοντας αποκτήσει παράνομη πρόσβαση, οι crackers καταστρέφουν σημαντικά δεδομένα, αποτρέπουν την εξυπηρέτηση των νόμιμων χρηστών ή προξενούν σοβαρά προβλήματα τα θύματά τους. Οι crackers χαρακτηρίζονται γενικά από κακόβουλες πράξεις (ΕΡΓΑΣΤΗΡΙΟ ΕΦΑΡΜΟΓΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΣΤΑ ΜΜΕ).

6.5 Εργαλεία της δουλειάς

6.5.1 Σκουλήκια

Οι πιο πολλοί άνθρωποι, όταν ακούν τη λέξη «σκουλήκια», φέρνουν στο μυαλό τους μικρά, γλοιώδη και μακρόστενα ζωύφια, τα οποία ζουν στο έδαφος. Οι περισσότεροι δε από αυτούς δε θα σχολιάσουν καν τη λέξη, απλώς θα δείξουν τη δυσαρέσκειά τους. Εκείνοι, όμως, που γνωρίζουν την αργκό γλώσσα των ηλεκτρονικών υπολογιστών, στο άκουσμα αυτής της λέξης θα αφήσουν να φανεί ένα μικρό χαμόγελο, το οποίο θα τους πάει μίλια μακριά.

Με τον όρο σκουλήκι περιγράφονται μικρά και ανεξάρτητα από το δημιουργό τους προγράμματα, τα οποία μπορούν σε μικρό χρονικό διάστημα να δημιουργήσουν μεγάλο χάος και πανικό. Πρόκειται για πολύ ευέλικτα προγράμματα, τα οποία είναι δύσκολο έως απίθανο να εντοπιστούν. Ακόμη, και αν εντοπιστούν, είναι απίθανο έως ακατόρθωτο να μπορέσει να σταματήσει κάποιος τη λειτουργία τους.

Ο πραγματικός λόγος για τον οποίο δημιουργούνται είναι συνήθως συγκαλυμμένος και κρυφός. Η φιλοσοφία όμως της δημιουργίας ενός τέτοιου προγράμματος είναι να αποκτήσει κανείς πληροφορίες ή άλλα οφέλη, τα οποία το πρόγραμμα αυτό θα πολλαπλασιάσει και θα μοιράσει σύμφωνα με τον

προγραμματισμό του. Έτσι, οι τελικοί αποδέκτες θα είναι το λιγότερο κρυφοί, ενώ συνάμα το πρόγραμμα θα μπερδεύει αρκετά εκείνους οι οποίοι θα προσπαθήσουν να ακολουθήσουν την πορεία του και θα θελήσουν έτσι να τους βρουν. Συνήθως, τέτοιοι αποδέκτες έχουν οριστεί πολύ πριν δράσει το πρόγραμμα και είναι καμουφλαρισμένοι, αλλά και προστατευμένοι πάρα πολύ καλά.

Τα σκουλήκια είναι ένα από τα σημαντικότερα όπλα στο οπλοστάσιο των hacker. 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. Επίσης, είναι δυνατόν να λειτουργήσουν με εσωτερικό μηχανισμό, ο οποίος θα τους «δείξει» τη στιγμή που πρέπει να δράσουν. Μπορούν να χειριστούν οποιαδήποτε πληροφορία βρίσκεται σε δυαδική μορφή. Δυστυχώς όμως, είναι τρομερά δύσκολο να δημιουργηθούν και να εγκατασταθούν σε κάποιο πρόγραμμα (Σαράφας, 2008, σ.48).

6.5.2 Ιοί

Πολλοί τόμοι οδηγών και εγκυκλοπαιδειών έχουν γραφεί και αφιερωθεί στους ιούς. Είναι μικρά προγράμματα και καλύπτουν ένα ευρύ φάσμα από ενέργειες και αποτελέσματα. Το πιο πιθανό είναι να ενοχλήσουν μόνο το υποψήφιο θύμα, αλλά είναι επίσης δυνατόν να είναι καταστροφικοί. Αυτό εξαρτάται από τις ενέργειες που έχουν προγραμματιστεί να κάνουν.

Αποτελούν το τρίτο σε προτίμηση όπλο των hacker. Εκείνους που είναι απλώς ενοχλητικοί, είναι εύκολο να του πειράξει ή να τους εξαλείψει κανείς. Οι καταστροφικοί είναι λίγο πιο δύσκολο να αντιμετωπιστούν, αλλά όσοι ανήκουν στη κατηγορία των φονικών είναι πάρα πολύ δύσκολο να αντιμετωπιστούν, γιατί κάτι τέτοιο δεν είναι δυνατόν μέχρι να δράσουν.

Μπορεί κανείς να τους συναντήσει σε πάρα πολλές μορφές. Το αποτέλεσμα των ενεργειών ενός ιού είναι είτε η απομάκρυνσή του από το σύστημα, είτε η απομάκρυνσή του συστήματος. Σε περίπτωση που δοκιμάσει κανείς να αφαιρέσει τον ιό από το σύστημά του τότε πρέπει να γνωρίζει μερικά πράγματα, γιατί είναι πολύ πιθανό ο ιός να προσκολληθεί σε φακέλους η αρχεία του λειτουργικού συστήματος.

Η δύναμη των ιών οφείλεται στην άγνοια των χρηστών, καθώς και στη κρυφή δράση και εγκατάστασή τους στο σύστημα. Είναι αρκετά εύκολο για κάποιον να δημιουργήσει ιούς, αλλά θα πρέπει να θυμάται ότι είναι απαραίτητο να έχει δύο πράγματα στην κατοχή του. Το πρώτο είναι η υπομονή και το δεύτερο ένας ηλεκτρονικός υπολογιστής πάνω στον οποίο θα δημιουργήσει ιούς. Επίσης του χρειάζεται να επιβλέπει συνεχώς τα αποτελέσματα του ιού.

Ο ηλεκτρονικός υπολογιστής πάνω στον οποίο θα μάθει κανείς να δημιουργεί ιούς του είναι απαραίτητος, γιατί πρέπει κάπου να δοκιμάζει τα αποτελέσματά του (Σαράφας, 2008, σ.49).

6.5.3 Πολυμορφικοί ιοί

Αποτελούν το δεύτερο καλύτερο τρόπο επίθεσης. Βγαίνουν μόνο σε ένα είδος, το οποίο είναι πάρα πολύ καταστροφικό. Έχουν πολλαπλά αποτελέσματα και είναι σχεδόν αδύνατο να τους ανακαλύψει κανείς στο σύστημά του.

Αποτελούν τους φυσικούς απογόνους των απλών ιών. Από τη στιγμή που ενεργοποιηθούν είναι αδύνατο, να τους σταματήσει κανείς. Αυτό οφείλεται στο γεγονός ότι μπορούν να αλλάξουν το αρχικό σημείο επίθεσης ή ακόμα και το μέρος του ηλεκτρονικού υπολογιστή από το οποίο προήλθαν. Επίσης, είναι πολύ εύκολα να τους δημιουργήσει κανείς. Το μοναδικό αντικείμενο το οποίο χρειάζεται είναι ένας απλός ιός μαζί με κάποιες συγκεκριμένες αλλαγές σε αυτόν, ώστε να επιτευχθεί το επιθυμητό αποτέλεσμα. Δεν υπάρχει κάποιο πρόγραμμα προστασίας από τους πολυμορφικούς ιούς ή αν υπάρχει, δεν έχει μεγάλη αποτελεσματικότητα.

Το καλύτερο μοντέλο πολυμορφικού ιού που έχει δημιουργηθεί μέχρι σήμερα είναι ένα το οποίο μπορούσε να αλλάξει όχι μόνο τη μορφή του, αλλά και το σημείο στο οποίο είχε κάνει τις διάφορες εγγραφές του. Επίσης είχε τη δυνατότητα της φυσικής αλλαγής των εγγράφων του μέσα στο σκληρό δίσκο. Ένα αρκετά σεβαστό εργαλείο, αν το χρησιμοποιήσει κανείς με προσοχή (Σαράφας, 2008, σ.50).

6.5.4 Κρυφά αρχεία

Τα κρυφά αρχεία είναι σχεδόν πάντοτε μικρά προγράμματα τα οποία εμφανίζονται κυρίως κωδικοποιημένα μαζί με κάποια άλλα αρχεία, όπως είναι οι

φωτογραφίες κλπ. Υπάρχει δε και η πιθανότητα κρυφά αρχεία, όπως γνωστοί ιοί και άλλα προγράμματα, να αλλάζουν απλώς την ονομασία τους και κάποιες από τις ενέργειές τους.

Δεν υπάρχει συγκεκριμένος τρόπος για να ανακαλύψει κανείς τέτοια «φιλικά» προγράμματα. Ο καλύτερος τρόπος να τα περάσει κάποιος στον ηλεκτρονικό υπολογιστή του ανυποψίαστου χρήστη, είναι να τα περάσει είτε σαν αρχεία exe, είτε σαν αρχεία zip.

Το μειονέκτημά τους είναι ότι από τη στιγμή που είναι κάποιος προετοιμασμένος για αυτά, δεν υπάρχουν και πολλά που μπορούν να κάνουν για να τα απομακρύνουν από το σύστημα. Είναι αρκετά εύκολο να βρεθούν και να αντιμετωπιστούν (Σαράφας, 2008, σ.51).

6.5.5 Δημιουργία των ID

Εδώ έχουμε την παρουσία μια δέσμης προγραμμάτων, ή αλλιώς μιας ξεχωριστής κατηγορίας. Μπορεί επίσης, να περιέχει και τη χρήση της τεχνολογίας ή των μηχανημάτων που αυτή προσφέρει, εκτός από αυτά τα προγράμματα. Είναι μια από τις πλέον παράνομες κατηγορίες στις οποίες μπορεί να εισχωρήσει κανείς. Το άτομο το οποίο θα ασχοληθεί με τέτοιου είδους προγράμματα πρέπει να είναι έτοιμο να πληρώσει βαριά, αν τυχόν πιαστεί.

Τα συνήθη αποτελέσματα είναι ψεύτικες ταυτότητες, διαβατήρια, πιστωτικές κάρτες κλπ. Είναι λοιπόν αρκετό να σκεφτεί κανείς ότι ελάχιστοι hackers είναι αυτοί οι οποίοι απασχολούνται εδώ. Κι αυτό δε συμβαίνει μόνο γιατί παρανομούν, αλλά και γιατί το ρίσκο να τους πιάσουν είναι πολύ μεγάλο. Έτσι όσοι ασχολούνται με αυτό, δεν αφήνουν περιθώρια για λάθη (Σαράφας, 2008, σ.52).

6.5.6 Δημιουργία των συνθηματικών

Είναι μια κατηγορία προγραμμάτων, η οποία είναι εφάμιλλη της κατηγορίας που χρησιμοποιείται για τη δημιουργία των ID. Τέτοια προγράμματα μπορούν να χρησιμοποιηθούν για τη δημιουργία συνθηματικών, για την εύρεσή τους κλπ. Είναι και αυτά παράνομα και πρέπει κανείς να είναι ιδιαίτερα προσεκτικός όταν ασχολείται με αυτά.

Τα αποτελέσματα των προγραμμάτων αυτών είναι απεριόριστη πρόσβαση σε πληροφορίες, ή τουλάχιστον τόσο «απεριόριστη» όσο επιτρέπει το ψεύτικο συνθηματικό, μέχρι να βρεθεί και να αφαιρεθεί.

Οι επιπτώσεις που επιφέρουν τέτοια προγράμματα δεν είναι και τόσο σοβαρές, σε σχέση πάντα με εκείνες που επιφέρουν τα προγράμματα που δημιουργούν ψεύτικα ID. Αυτή η κατάσταση, όμως, μοιάζει να αλλάζει πολύ γρήγορα, αφού όλο και περισσότεροι φορείς και οργανισμοί ζητούν τη δημιουργία νομοθεσίας για την προστασία τους.

Τις περισσότερες φορές, οι άνθρωποι οι οποίοι κατηγορούνται για τέτοια εγκλήματα δεν έχουν καμία σχέση με αυτά. Απλά βρίσκονται σε λάθος σημείο τη λάθος στιγμή.

Τέτοια προγράμματα είναι πολύ εύκολο να δημιουργηθούν και να μοιραστούν. Επίσης, είναι πολύ εύκολο για κάποιον να τα βρει στο διαδίκτυο, και ακόμη πιο εύκολο να τα χρησιμοποιήσει και να δημιουργήσει όλα εκείνα που τέτοια προγράμματα υπόσχονται. Αυτοί που χάνουν τις πιο πολλές φορές δεν είναι παρά δημόσιοι φορείς και οι μεγάλοι οργανισμοί (Σαράφας, 2008, σ.53).

6.5.7 Port scanners

Αυτή είναι μια ειδική κατηγορία προγραμμάτων τα οποία βρίσκονται στην ευχέρεια των hacker και των άλλων ομάδων από τη σκοτεινή πλευρά των ηλεκτρονικών υπολογιστών. Είναι από τα εύκολα προγράμματα τα οποία μπορεί κανείς να δημιουργήσει και να χρησιμοποιήσει. Δίνουν στο χρήστη τη δυνατότητα να τα αφήσει να λειτουργήσουν αυτόματα και από μόνα τους, ειδικά όταν γίνονται συνδέσεις μέσω αυτών. Με λίγα λόγια, αυτά τα προγράμματα είναι δυνατόν να λειτουργήσουν κάτω από αρκετά αντίξοες συνθήκες για άλλα προγράμματα. Αυτό που κάνουν είναι να παρακολουθούν, να βρίσκουν και να στέλνουν στο στόχο, ο οποίος τους έχει προσδιοριστεί, πληροφορίες που δείχνουν σε ποια κι πόσα σημεία γίνεται η ανταλλαγή των πληροφοριών από τον έναν ηλεκτρονικό υπολογιστή στον άλλο.

Σε περίπτωση που κάποιος θελήσει να βρει τα κανάλια ή τις πόρτες επικοινωνίας των ηλεκτρονικών υπολογιστών στους οποίους θέλει να επιτεθεί, χρησιμοποιεί το συγκεκριμένο πρόγραμμα. Αυτό μπορεί να αλλάξει και να μεταφέρει ό,τι είδους

πληροφορίες θέλει από τον έναν ηλεκτρονικό υπολογιστή στον άλλον (Σαράφας, 2008, σ.54).

6.5.8 Είμαι administrator στη θέση του administrator

Σε αυτή την κατηγορία βρίσκονται αρκετά καλά και χρήσιμα εργαλεία hacker. Αυτά τα προγράμματα λειτουργούν από το εσωτερικό ενός ηλεκτρονικού υπολογιστή, καθώς είναι ευκολότερο να βρεθούν πληροφορίες από τον εσωτερικό παρά από τον εξωτερικό χώρο ενός υπολογιστή.

Λειτουργούν με την ίδια φιλοσοφία με την οποία λειτουργούν και τα προγράμματα των port scanners. Η διαφορά τους έγκειται στο γεγονός ότι τα προγράμματα αυτά δεν παρακολουθούν τις πόρτες μεταφοράς δεδομένων, αλλά τους φακέλους και τα αρχεία στα οποία καταγράφονται και μπορεί να περιέχονται συνθηματικά κάποιου administrator. Σε περίπτωση που οι επιτιθέμενοι ξέρουν σίγουρα ότι το υποψήφιο θύμα τους είναι κάποιος administrator, τότε κοιτάζουν όλους τους φακέλους και όλα τα αρχεία τα οποία εμπεριέχονται στον ηλεκτρονικού του υπολογιστή. Αυτό συμβαίνει γιατί σε τέτοιες περιπτώσεις είναι δυνατόν να εντοπίσουν και άλλα συνθηματικά ή άλλες καλές και χρήσιμες πληροφορίες. Το να αλλάζει κανείς συνθηματικά ή άλλες πληροφορίες σε αυτό τον τομέα και επίπεδο δουλειάς είναι ο καλύτερος τρόπος για να μην πιαστεί. Τα συνθηματικά δεν αλλάζουν σχεδόν ποτέ, είτε γιατί αυτοί που τα πρωτοέθεσαν είναι πολύ σίγουροι για αυτά, είτε γιατί δεν υπάρχει κάποιος σημαντικός λόγος για αλλαγή.

Είναι ένας από τους πιο απλούς τρόπους επίθεσης εναντίον ενός φορέα ή ενός μεγάλου οργανισμού. Μπορεί να γίνεται και με τη βοήθεια ειδικών προγραμμάτων. Σε περιπτώσεις κατά τις οποίες κάποιος δέχεται μια τέτοια επίθεση με αρνητικά αποτελέσματα για αυτόν, τότε το μόνο πράγμα το οποίο μπορεί να κάνει, είναι να αλλάξει το λειτουργικό του σύστημα ή τα άτομα τα οποία είναι υπεύθυνα για την ασφάλειά του (Σαράφας, 2008, σ.55).

6.5.9 Πυρηνικά

Αυτή είναι μια κατηγορία προγραμμάτων η οποία προορίζεται για μικρά παιδιά ή για άτομα τα οποία μπαίνουν για πρώτη φορά στον κόσμο των ηλεκτρονικών

υπολογιστών. Είναι πάρα πολύ εύκολο για οποιονδήποτε ενδιαφέρεται για τέτοια εργαλεία να τα βρει, αλλά και να μάθει να τα χρησιμοποιεί.

Υπάρχουν και ειδικά μέρη στο Διαδίκτυο, όπου ο ενδιαφερόμενος μπορεί να εντοπίσει μια μεγάλη γκάμα τέτοιων προγραμμάτων ή ακόμα και υλικό για τη δημιουργία και τη χρήση τους. Η χρήση τέτοιων προγραμμάτων περιορίζεται στο μπλοκάρισμα και στην προσωρινή αχρήστευση του ηλεκτρονικού υπολογιστή του στόχου.

Δεν χρειάζεται κανείς να έχει ειδικές γνώσεις για να μάθει να λειτουργεί τέτοια προγράμματα. Υπάρχουν σε πολλές μορφές, αλλά κυρίως κυκλοφορούν σε παραθυρικές μορφές. Είναι δυνατόν να βρεθούν τέτοια προγράμματα ακόμα και στο εμπόριο (Σαράφας, 2008, σ.56).

6.5.10 Σβήνω τα firewalls

Αυτή είναι ίσως η πιο καινούρια κατηγορία των προγραμμάτων τα οποία κυκλοφορούν και αποτελούν μέρος του οπλοστασίου ενός hacker. Πρωτοεμφανίστηκε μαζί με τα πρώτα firewalls, αλλά μόλις πρόσφατα ξεκίνησε να παίρνει διατάσεις και να αναπτύσσεται. Αυτό οφείλεται στο γεγονός ότι το εμπόριο και η τέχνη των firewalls είναι σχετικά καινούρια.

Δεν χρειάζεται να είναι κάποιος ιδιαίτερα ενήμερος για να λειτουργήσει τέτοιου είδους προγράμματα. Είναι δε δυνατόν να λειτουργούν είτε στο στιλ των ιών, είτε στο στιλ των port scanners. Είναι αρκετά εύκολο να βρει ή να δημιουργήσει κανείς τέτοια προγράμματα για έναν καλό hacker.

Αυτό συμβαίνει επειδή ένα firewall δεν είναι ο τελειότερος τρόπος άμυνας που υπάρχει για ένα σύστημα. Πάντα θα είναι ανοιχτό για να επιτρέψει τη μεταφορά δεδομένων από τον ηλεκτρονικό υπολογιστή που βρίσκετε προς τα έξω, αλλά και το αντίστροφο. Η χρησιμότητα των προγραμμάτων αυτών είναι εμφανής μόνο σε περιπτώσεις που χρειάζεται κανείς ταχύτητα για να μπει σε ένα σύστημα ή σε περιπτώσεις που χρειάζεται να κρατηθεί ένα πολύ καλό firewall απασχολημένο για αρκετή ώρα (Σαράφας, 2008, σ.57).

6.6 Πώς τους κρατάμε μακριά;

6.6.1 Αστυνόμευση

Είναι πολύ δύσκολο να μιλήσει κανείς για αστυνόμευση σε μια ομάδα όπου η έννοια της αστυνομίας είναι σχεδόν ανύπαρκτη. Πάντως, υπάρχει κάτι που μοιάζει με αστυνομία και αποτελείται από εκείνους τους hackers οι οποίοι έχουν μια κάποια ηλικία και πολύ μεγάλη εμπειρία σε τέτοια θέματα. Τέτοια άτομα δεν αναζητούν εκείνους που είναι ή ανήκουν στην ομάδα των hacker και υπήρξαν τα «κακά παιδιά». Απλώς προσπαθούν να τιμωρήσουν εκείνους τους hacker, οι οποίοι αξίζει πραγματικά να τιμωρηθούν. Όπως και να έχει και ανεξάρτητα από τον τρόπο με τον οποίο μπορεί να βλέπει κάθε άνθρωπος την ομάδα αυτή, τα άτομα τα οποία την απαρτίζουν έχουν τους δικούς τους τρόπους τιμωρίας εκείνων που πραγματικά είναι παράνομοι.

Εκτός από αυτού το είδος αστυνόμευσης, κάποιες συγκεκριμένες χώρες έχουν δημιουργήσει ή και αποδεχθεί ειδικές νομοθεσίες οι οποίες τιμωρούν τα επονομαζόμενα ηλεκτρονικά εγκλήματα. Όπως είναι φυσικό, οι ίδιες χώρες δημιουργούσαν και ειδικές μονάδες αστυνόμευσης.

Σε περιπτώσεις, όμως, που κάποιο ηλεκτρονικό έγκλημα χαρακτηριστεί ως κοινό έγκλημα κλοπής ή ως ένα πιο βαρύ έγκλημα εναντίον της παγκόσμιας ειρήνης κλπ., τότε οι ίδιες υπηρεσίες αστυνόμευσης που υπάρχουν για όλους, ισχύουν και εδώ (Σαράφης, 2008, σ.79).

6.6.2 Firewalls

Είναι ένα από τα καλύτερα όπλα που δίνονται στον απλό χρήστη για προστασία από τους hackers. Τα firewalls είναι απλά προγράμματα τα οποία έχουν πάρει το όνομά τους από έναν τρόπο με τον οποίο η άνθρωποι προφυλάσσονταν και αμύνονταν στα αρχαία χρόνια. Άναβαν και συντηρούσαν μεγάλες φωτιές, οι οποίες έμοιαζαν με αδιαπέραστα για εκείνη την εποχή τείχη.

Τα προγράμματα αυτά είναι σχεδιασμένα να είναι αδιαπέραστα σε επιθέσεις από hackers ή τουλάχιστον έτσι διατείνονται οι κατασκευές τους. Δεν έχουν ένα συγκεκριμένο μέγεθος ούτε και συγκεκριμένο τρόπο κατασκευής. Οποιοσδήποτε με γνώσεις και καλά εργαλεία μπορεί να δημιουργήσει καλά firewalls. Έχουν αρκετά πλεονεκτήματα και όντως μοιάζουν σε θέση να κρατήσουν μακριά τους

hackers για αρκετό διάστημα. Ωστόσο, έχουν και παρουσιάζουν και αρκετά μειονεκτήματα. Το κόστος δημιουργίας και συντήρησης, το λειτουργικό σύστημα κάτω από το οποίο θα δημιουργηθούν και η συμβατότητά τους με τα οποία λειτουργικά συστήματα είναι μόνο μερικά από αυτά.

Σήμερα μοιάζει και είναι πιο εύκολο να δημιουργήσει κανείς μηχανήματα τα οποία κάνουν τη δουλειά των firewalls. Μέχρι και το κόστος τους ή ο τρόπος εγκατάστασής τους δεν απαιτούν πλέον τη βοήθεια υπεύθυνων ατόμων. Ο καλύτερος τρόπος προστασίας είναι τα δοκιμασμένα και κλασσικά firewalls (Σαράφας, 2008, σ.80).

6.6.3 Port controllers

Αυτή είναι η δεύτερη κατηγορία όπλων τα οποία προσφέρονται στον απλό χρήστη εναντίον επιθέσεων που ίσως δεχτεί από hackers. Αυτά τα προγράμματα δεν είναι δυνατόν να αντέξουν για πολύ καιρό σε μια μακρόχρονη και δημιουργική επίθεση. Εάν όμως χρησιμοποιηθούν με σύνεση και σε συνδυασμό με ένα καλό firewalls, τότε μπορούν να δημιουργήσουν πονοκεφάλους στους hackers.

Τα προγράμματα αυτά είναι μικρά σε μέγεθος τις περισσότερες φορές και αυτό που κάνουν είναι να δίνουν μια σχεδόν συνεχόμενη αναφορά των «επιθέσεων», οι οποίες γίνονται στις «πόρτες» επικοινωνίας του υπολογιστή. Επίσης, αν είναι πολύ καλά φτιαγμένα, μπορεί να έχουν και τη δυνατότητα να μπλοκάρουν κάποια σημεία επικοινωνίας του υπολογιστή. Το λιγότερο που μπορούν να κάνουν αυτά τα προγράμματα είναι να αναφέρουν και να δείξουν στο χρήστη τα σημεία επικοινωνίας του υπολογιστή τα οποία δέχονται τις περισσότερες επιθέσεις και ίσως και τον τόπο προέλευσης. Υπάρχει μεγάλη δυνατότητα αυτά τα προγράμματα να ελέγξουν τα πακέτα πληροφοριών τα οποία έρχονται στον υπολογιστή και, πριν τα δει ο ανυποψίαστος χρήστης, να στείλουν ένα μήνυμα απάντησης στον αποστολέα. Έτσι, ο υπολογιστής του αποστολέα είναι δυνατόν να μπλοκάρει, εάν το πακέτο πληροφοριών είναι πολύ μεγάλο.

Στην ίδια κατηγορία με αυτά τα προγράμματα βρίσκονται και οι IP scanners. Δεν αναγνωρίζουν πακέτα πληροφοριών, αλλά τη διεύθυνση IP του αποστολέα. Σε περίπτωση κατά την οποία την αναγνωρίσουν, αφήνουν το πακέτο των πληροφοριών να περάσει. Σε αντίθετη περίπτωση, απλώς δεν επιτρέπουν στο άγνωστο πακέτο να προχωρήσει (Σαράφας, 2008, σ.81).

ΕΠΙΛΟΓΟΣ

Το Διαδίκτυο χρησιμοποιείται καθημερινά από εκατομμύρια χρήστες παγκοσμίως. Πολλοί όμως από αυτούς δεν γνωρίζουν πως εκτός από το «ορατό» ίντερνετ, υπάρχει ένα άλλο δίκτυο το οποίο λειτουργεί κανονικά, αλλά μπορεί να μην έχουν πρόσβαση σε αυτό. Ο Σκοτεινός Ιστός είναι το μέρος του διαδικτύου στο οποίο σκιώδεις χρήστες έχουν πρόσβαση σε κρυφές υπηρεσίες. Είναι συχνά διαθέσιμο στο κοινό, απλά πρέπει να γνωρίζει κανείς πώς να το βρει. Το Deep Web συντίθεται από ιστοσελίδες προσβάσιμες μεν στο κοινό του διαδικτύου, αλλά όχι μέσω των μηχανών αναζήτησης. Το σκοτεινό διαδίκτυο γενικότερα, έχει χρησιμοποιηθεί και για εγκληματικές δραστηριότητες, όπως είναι το hacking και πολλά άλλα. Υπάρχουν διάφορες τεχνικές αντιμετώπισης για την εξάλειψη της σκοτεινής πλευράς, όπως διάφορα προγράμματα ελέγχου και προστασίας, ακόμη και νομοθεσίες που προστατεύουν τα προσωπικά δικαιώματα του χρήστη.

Με βάση όσον έχουν προαναφερθεί στη συγκεκριμένη πτυχιακή εργασία, συμπεραίνουμε ότι το Deep Web και το Dark Web δεν είναι το ίδιο, αλλά το δεύτερο αποτελεί το υποσύνολο του πρώτου. Το Dark Web δεν είναι ο ποιο επικίνδυνος τόπος που μπορεί να βρεθεί κανείς, αλλά χρειάζεται προσοχή. Μέσα στο Dark Web, η ανωνυμία είναι δική μας ευθύνη και μόνο. Ένα καλό πρόγραμμα που περιέχει μεγάλο ποσοστό ανωνυμίας είναι ο Tor. Ειδικά αν χρησιμοποιηθεί σε συνδυασμό με κάποιο VPN. Με το I2P θα έχετε την ίδια ανωνυμία, ίσως και μεγαλύτερη, απλά ο δρόμος είναι πιο δύσκολος. Για τη δημιουργία ενός μικρού ασφαλούς και ανώνυμου δικτύου, μπορείτε να χρησιμοποιήσετε το Freenet.

Συνοψίζοντας, το σκοτεινό διαδίκτυο δεν είναι απαραίτητα ένας σκοτεινός κόσμος γεμάτος κινδύνους. Θα ήταν χρήσιμο ο κάθε χρήστης να γνωρίζει καλά τις ιστοσελίδες στις οποίες κάνει αναζήτηση, να είναι ενήμερος για την πρόληψη για κάθε μορφή επίθεσης και να υπάρχει στοιχειώδης εκπαίδευση για τη σωστή χρήση του κυβερνοχώρου, ώστε να μειωθεί σε ένα μεγάλο βαθμό η ηλεκτρονική εξαπάτηση.

ΠΗΓΕΣ

ΒΙΒΛΙΑ

Σαράφας Κώστας, (2008), Hackers:Μύθος ή Πραγματικότητα, Αθήνα, Πρόπομπος

Τσουραμάνη Χρ.Ε. και Κορολή Μαρ.-Ευγ., ΟΙΚΟΝΟΜΙΑ ΚΑΙ ΕΓΚΛΗΜΑΤΙΚΟΤΗΤΑ, Αθήνα, σελ.135,140-143,155, Τ.Ε.Ι Δυτικής Ελλάδας, (διδακτικές σημειώσεις)

Misha Glenny, (2012), Dark Market, CyberThieves, CyberCops and You, «μτφρ. Ε.Βιδάλη», Αθήνα, Πάπυρος

ΙΣΤΟΣΕΛΙΔΕΣ

Αμπατζής Κωνσταντίνος, Καλύτερα να μην μάθεις ποτέ τι συμβαίνει στο Dark Web, https://www.oneman.gr/keimena/diabasma/megala_keimena/kalutera-na-mhn-matheis-pote-ti-symvainei-sto-dark-web.4851953.html, 2017

Αναγνωστόπουλος Χάρης, Τι είναι το Deep Web και το Dark Web, Μύθοι κι Αλήθειες, https://www.pcsteps.gr/200164-τι-είναι-το-deep-web-και-το-dark-web-μύθοι-αλήθειες/, 5 Αυγούστου 2017

Νικολαΐδης Ηλίας, Τι είναι το Dark Web;, https://insidestory.gr/article/ti-einai-dark-web?token=FJO9KG2F53, Τετάρτη 13 Απριλίου 2016

Σακαλάκης Παναγιώτης, Ο υπόκοσμος του διαδικτύου και οι παράνομες ιστοσελίδες, https://www.tsouk.gr/dark-web-ypokosmos-diadiktyou-paranomes-istoselides/, 31 Οκτωβρίου 2016

Τσακίρης Άκης, Dark Web: Η σκοτεινή πλευρά του Internet που δεν έχει γυρισμό – Ένα ανεξέλεγκτο κομμάτι του διαδικτύου που αν μπεις θα γίνει ο «εφιάλτης» σου, http://labelnews.gr/dark-web-η-σκοτεινή-πλευρά-του-internet-που-δεν-έχει-γ/, Παρασκευή 12 Απριλίου 2019

Absenta Mia, Ποια η διαφορά μεταξύ surface, deep και dark web;, https://www.secnews.gr/157824/ποια-διαφορά-μεταξύ-surface-deep-dark-web/, 2 Ιανουαρίου 2017

Gloomy Gentlemen, 4 ΣΟΚΑΡΙΣΤΙΚΕΣ ιστορίες από το Deep Web, https://www.youtube.com/watch?v=43bnW3Pmrbg, 30 Νοεμβρίου 2018

Lyberis Elpiniki, Τι είναι το Deep Web; Όλα όσα θα ήθελες να ξέρεις, https://www.digitallife.gr/all-you-need-to-know-about-the-deep-web-39141 , 26 Ιανουαρίου 2014

Nassr Eddin, Ανωνυμία στο Διαδίκτυο, http://ancap.gr/anonimia-sto-diadiktio/, 30 Ιανουαρίου 2015

Vasileiadis Anastasis, Μύθοι και αλήθειες γύρω από το Darknet- Deepweb-Darkweb, https://cerebrux.net/2018//11/09/μύθοι-και-αλήθειες-γύρο-από-το-darknet-deepweb-darkweb/ , 9 Νοεμβρίου 2018

Salih, Τι είναι το Bitcoin, πως λειτουργεί και που θα φτάσει η τιμή και η αξία του, https://cerebrux.net/2017/12/13/τι-είναι-το-bitcoin-πως-λειτουργεί-και-που-θα/, 13 Δεκεμβρίου 2017

ΕΡΓΑΣΤΗΡΙΟ ΕΦΑΡΜΟΓΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΣΤΑ ΜΜΕ, "Χάκερς" και "κράκερς", http://pacific.jour.auth.gr/security/page.htm, 2005