ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ & ΠΛΗΡΟΦΟΡΙΚΗΣ

ΕΡΓΑΣΙΑ ΕΞΑΜΗΝΟΥ

ΓΙΑ ΤΟ ΜΑΘΗΜΑ

ΔΙΚΤΥΑ ΔΗΜΟΣΙΑΣ ΧΡΗΣΗΣ ΚΑΙ ΔΙΑΣΥΝΔΕΣΗ ΔΙΚΤΥΩΝ

ΑΣΦΑΛΕΙΑ ΣΤΟ INTERNET

ΓΡΑΜΜΑΤΙΚΟΠΟΥΛΟΣ ΑΛΕΞΑΝΔΡΟΣ

Α.Μ 1054291

ΔΙΔΑΣΚΩΝ: ΧΡΗΣΤΟΣ ΜΠΟΥΡΑΣ

ΠΑΤΡΑ 2020

ΠΕΡΙΕΧΟΜΕΝΑ

ΑΚΡΩΝΥΜΙΑ

LAN = LOCAL AREA NETWORKS

WAN = WIDE AREA NETWORKS

MAN = METROPOLITAN AREA NETWORK

TOR = THE ONION ROUTER

OSI = ΜΟΝΤΕΛΟ ΔΙΑΣΥΝΔΕΣΗΣ ΑΝΟΙΚΤΩΝ ΣΥΣΤΗΜΑΤΩΝ

HTTP = HYPERTEXT TRANSFER PROTOCOL

DNS = DOMAIN NAMING SYSTEMS

UDP = USER DATAGRAM PROTOCOL

TCP = TRANSMISSION CONTROL PROTOCOL

IP = INTERNET PROTOCOL

DoS = DENIAL OF SERVICE

DDoS = DISTRIBUTED DENIAL OF SERVICE

ΚΕΦΑΛΑΙΟ 1: ΕΙΣΑΓΩΓΗ

1.1 Τι είναι δίκτυο

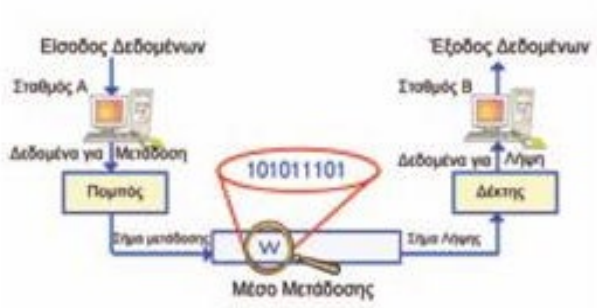
Ο άνθρωπος χρησιμοποιεί δίκτυα για να ικανοποιήσει ή να διευκολύνει κάποιες ανάγκες της καθημερινότητας του. Από μια απλή μετακίνηση μέσω του οδικού δικτύου έως την κατανάλωση νερού και ρεύματος μέσω του δικτύου ύδρεσυσης και ηλεκτροδότησης. Τι περιγράφει όμως η έννοια δίκτυο;

Δίκτυο είναι η διασύνδεση πολλών σημείων μεταξύ τους με σκοπό την μεταφορά υλικών και άυλων αγαθών προς και από όλα τα σημεία αυτά. Η ανάγκη να μεταφέρουμε δεδομένα από ένα σημείο σε ένα άλλο με το καλύτερο δυνατό τρόπο, μας οδηγεί να συνδέσουμε, με καλώδια και ραδιοκύματα, συσκευές μεταξύ τους [4]. Το σύστημα που ενώνει τις εφαρμογές και τους χρήστες με άλλες εφαρμογές και χρήστες ονομάζεται δίκτυο υπολογιστών. Η διασύνδεση αυτόνομων υπολογιστών και περιφεριακών συσκευών που μπορούν μεταξύ τους να ανταλλάξουν πληροφορίες δημιουργεί ένα σύστημα επικοινωνίας δεδομένων που ονομάζεται δίκτυο υπολογιστών [1].

1.2 Ταξινόμηση των Δικτύων

Τα δίκτυα ηλεκτρονικών υπολογιστών ταξινομούνται με βάση το φυσικό μέσο διασύνδεσης, τον τρόπο πρόσβασης σε αυτά και την γεωγραφική τους κάλυψη. Αναλόγως το φυσικό μέσο μετάδοσης χωρίζονται σε :

- **Ενσύρματα δίκτυα**, όπου οι υπολογιστές συνδέονται μεταξύ τους με καλώδια και με την βοήθεια της κάρτας δικτύου κάθε υπολογιστή [2].



Εικόνα 1. Ενσύρματο Δίκτυο [2].

- **Ασύρματα δίκτυα**, όπου η σύνδεση υπολογιστών γίνεται με την βοήθεια ασύρματων καρτών δικτύου [2].

Εικόνα 2. Ασύρματο Δίκτυο [2].

Με βάση τον τρόπο πρόσβασης σε αυτά χωρίζονται σε :

- **Ιδιωτικά δίκτυα** είναι δίκτυα που ανήκουν σε ιδιώτες ή σε ιδιωτικούς οργανισμούς. Η ανταλλαγή των δεδομένων γίνεται μέσω αποκλιστικών-ιδιωτικών γραμμών επικοινωνίας οι οποίες είναι δημοσίων τηλεπεικοινωνιακών φορέων. Η πρόσβαση σε αυτές τις γραμμές είναι εφικτή μόνο από χρήστες εντός του εκάστοτε ιδωτικού δικτύου. [3].

- **Δημόσια δίκτυα** δημιουργούνται σε περιπτώσεις τις οποίες λόγω απόστασης η διασύνδεση σημείων είναι δύσκολη και κοστοβόρα. Μέσω των δημόσιων δικτύων μεταφέρονται δεδομένα μικρού όγκου και με μεγάλη ταχύτητα.[3].

Με βάση την γεωγραφική κάλυψη του δικτύου διακρίνονται σε :

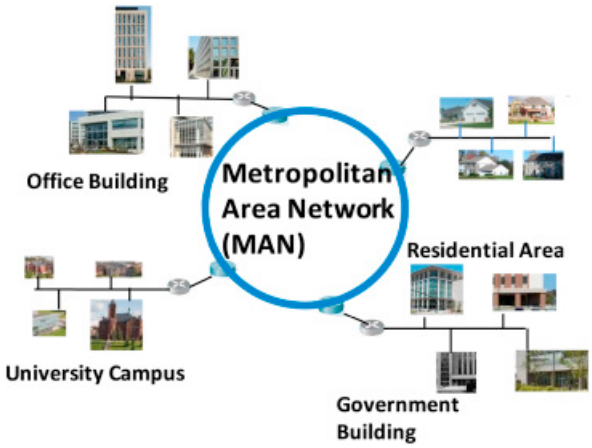
- **Τοπικά δίκτυα:** Καλύπτουν μικρές αποστάσεις και περιορίζονται στα πλαίσια μιας επιχείρησης. Η διαφορά τους από τα WAN είναι στις διαφορετικές τεχνικές που χρησιμοποιούν για να λειτουργήσουν [2].

Εικόνα 3 [2].

- **Δίκτυα ευρείας περιοχής** : Αναφερόμαστε σε δίκτυα μεγάλου γεωγραφικού πλάτους, τα οποία συνδέουν μεταξύ τους χώρες ακόμα και ηπείρους [2].

Εικόνα 4 [2].

- **Μητροπολιτικό δίκτυο**: Το εύρος του είναι ανάμεσα στο τοπικό και στο δίκτυο ευρείας περιοχής. Η ισχύς του φτάνει να καλύψει το μέγεθος μιας πόλης [2].



Εικόνα 5 [8].

1.3 Εφαρμογές των δικτύων

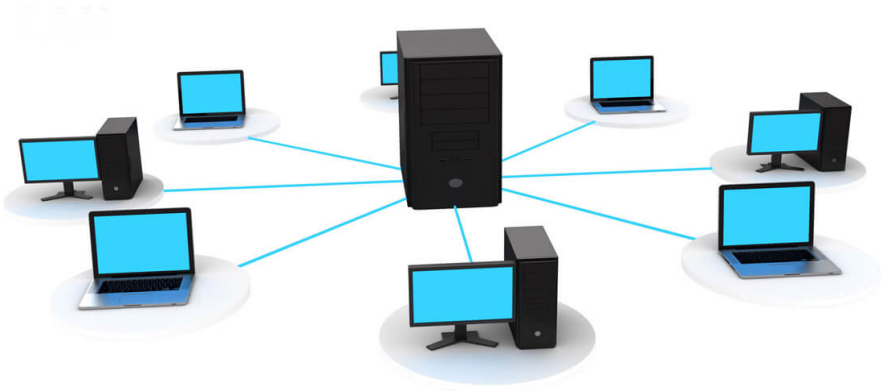
Εφαρμογές των δικτύων [4] :

1. Επικοινωνία μεταξύ χρηστών (VOIP, Video Conferencing, Messaging).
2. Διαμοιρασμός πόρων (Printing, Cloud Sharing).
3. Διανομή Υλικού (Video Streaming, Apps & Upgrades, Web Pages).
4. Επικοινωνία μεταξύ συστημάτων (E-commerce, Reservations).
5. Διασύνδεση της τεχνολογίας με το περιβάλλον(Webcams, Locations).

1.4 Δίκτυο και Διαδίκτυο

Όπως αναφέραμε και παραπάνω, ένα δίκτυο είναι ένα σύστημα σύνδεσης υπολογιστών οι οποίοι ανταλλάσουν δεδομένα μεταξύ τους. Όταν θέλουμε να

φτιάξουμε ένα δίκτυο με πολλούς υπολογιστές χρειαζόμαστε ένα υπολογιστή που θα κάνει όλες τις δουλειές του δικτύου. Ο υπολογιστής αυτός στην ουσία, εξυπηρετεί την επικοινωνία των άλλων υπολογιστών, για αυτό και ονομάζεται και εξυπηρετητής ή αλλιώς server. (βλ. Εικόνα 6). Εάν θέλουμε να επικοινωνήσουν μεταξύ τους εκατομμύρια υπολογιστές, χρειαζόμαστε ένα πολύ μεγάλο δίκτυο με πάρα πολλούς εξυπηρετητές. Το γνωστό σε όλους μας διαδίκτυο (Internet) [6]. Το διαδίκτυο αποτελείται από διασυνδεδεμένα δίκτυα υπολογιστών σε ολόκληρο τον κόσμο, τα οποία για να επικοινωνήσουν μεταξύ τους και να ανταλλάξουν πακέτα χρειάζονται πρωτόκολλα τα οποία είναι υλοποιήσιμα και σε υλικό και σε λογισμικό [5]. Για τη λειτουργία του Internet χρειάζονται μερικοί πολύ μεγάλοι εξυπηρετητές που ονομάζονται κορμός του Internet (Internet back bone) (βλ. Εικόνα 7). Πάνω σε αυτόν τον κορμό συνδέονται μικρότεροι server και πάνω σε αυτούς όλοι οι υπολογιστές μας. Για να συνδεθούμε στο Internet πρέπει να αποκτήσουμε μια συνδρομή σε κάποιον πάροχο πρόσβασης στο Internet (ISP- Internet Service Provider) όπως είναι η cosmote, η wind κτλπα [6].



Εικόνα 6 [9].

Εικόνα 7 [10].

Εικόνα 8. INTERNET BACKBONE [11]

1.5 Η Ιστορία του διαδικτύου

Κατά την διάρκεια του Ψυχρού πολέμου ανάμεσα στην Αμερική και την Ρωσία, οι ΗΠΑ φοβούμενες μια πιθανή πυρηνική επίθεση ιδρύουν την Υπηρεσία Προηγμένων Έργων Έρευνας (APRA). Σκοπός της ΥΠΕΕ ήταν να διαφυλάξει την επικοινωνία του Αμεικανικού στρατού σε περίπτωση πυρηνικής απειλής. Το 1961 ο Leonard Kleinrock ανέπτυξε την Θεωρία Μεταγωγής Πακέτων η οποία υποστήριζε πως είναι δυνατόν να σταλούν πακέτα πληροφοριών με συγκεκριμένη προέλευση και προορισμό μεταξύ υπολογιστών. Βσιζόμενοι στην θεωρία αυτή, η ΥΠΕΕ δημιούργησε το APRAnet με 23 κόμβους (Μνήμης 12K) διαφορετικού λειτουργικού συστήματος και ταχύτητα γραμμής 50kbps. Το 1973 το Internet απαριθμεί περίπου 2000 χρήστες. Σιγά σιγά δημιουργήθηκε η ανάγκη για σύνδεση όλων των μέχρι τότε δικτύων, με την βοήθεια πρωτοκόλλων. Το 1974, οι Βιντ Σερφ και Μπομπ Κάαν δημοσιεύουν μια μελέτη πάνω στην οποία βασίστηκε η δημιουργία του μοναδικού πρωτοκόλλου που υπήρχε στο δίκτυο APRAnet, το TCP/IP, Transmission Control Protocol/Internet Protocol. Πλέον, το 1988 το Διαδίκτυο είχε επεκταθεί

παγκοσμίως καθώς μέσα σε αυτό είχαν συνδεθεί μικρότερα υποδίκτυα, οπώς τα εθνικά δίκτυα κτλπα. Στις αρχές του 90 σταματάει η λειτουργία του δικτύου ARPANET καθώς οι περισσότεροι κόμβοι του APRAnet έχουν ήδη υποκατασταθεί με άλλα δίκτυα και ο πρώτος Internet Provider είναι γεγονός, με το όνομα «The World comes on-line (world.std.com)».Έτσι οποιοδήποτε δίκτυο χρησιμοποιούσε το πρωτόκολλο TCP/IP για την μεταφορά πακέτων πληροφορίας ήταν στο “Internet”.Το Διαδίκτυο, έγινε ευρύτερα γνωστό με την εφαρμογή της υπηρεσίας του Παγκόσμιου Ιστού από τον Τιμ Μπέρνερς-Λι στο ερευνητικό ίδρυμα CERN, ο οποίος είναι στην ουσία, η "πλατφόρμα", η οποία κάνει εύκολη την πρόσβαση στο Ιντερνέτ, ακόμη και στη μορφή που είναι γνωστό σήμερα [6][7].

ΚΕΦΑΛΑΙΟ 2: ΔΙΑΔΙΚΤΥΟ

2.1 Web – Deep Web – Dark Web

Στο προηγούμενο κεφάλαιο αναλύσαμε ποία είναι η σχέση μεταξύ δικτύου και Διαδικτύου και καταλήξαμε πως το Διαδίκτυο είναι ουσιαστικά ένα τεράστιο δίκτυο υπολογιστών. Για να μπορέσουν οι υπολογιστές να αλληλεπικοινωνήσουν και να μεταβιβάσουν ο ένας στον άλλο δεδομένα, χρησιμοποιούν πρωτόκολλα επικοινωνίας [12].

2.1.1 Web

Τα πρωτόκολλα επικοινωνίας κάνουν δυνατή την επικοινωνία ανάμεσα σε δύο συστήματα. Για παράδειγμα, ενός υπολογιστή και ενός server. Δηλαδή, δημιουργούν τις κατάλληλες προϋποθέσεις για να γίνει κάποια δουλεία μεταξύ τους. Ένα τέτοιο πρωτόκολλο είναι το www (world wide web) που εν συντομία το αποκαλούμε web ή αλλιώς Παγκόσμιος Ιστός ή Surface Web [12]. Για να εισέλθουμε στο web χρειαζόμαστε περιηγητές ή αλλιώς browsers, οι οποίοι γνωρίζουν αυτό το πρωτόκολλο, τέτοιοι είναι το Chrome, ο Mozilla και το Safari. Δουλειά των περιηγητών είναι να πάρουν τα αιτήματα μας, να τα στείλουν στους server και αυτοί με την σειρά τους αφού λάβουν κάποια απάντηση, εμφανίζουν τα αποτελέσματα στην οθόνη μας.

Χρησιμοποιώντας τους browsers μπορούμε να επισκεφθούμε τις ιστοσελίδες που μας ενδιαφέρουν με δύο τρόπους. Είτε γνωρίζοντας το URL (UNIQUE RESOURCE LOCATOR) της ιστοσελίδας, είτε χρησιμοποιώντας μια μηχανή αναζήτησης όπως την Google, την Bing κτλ. Οι μηχανές αναζήτησης χρησιμοποιούν ένα ειδικό λογισμικό που ονομάζεται crawler ή spider για να καταχωρήσει αυτόματα όλες τις ιστοσελίδες που επισκέπτεται . Σε κάθε ιστοσελίδα που εισερχόμαστε ο crawler ελέγχει αν υπάρχουν σύνδεσμοι τους ακολουθεί και τους αποθηκεύει, δημιουργώντας έτσι έναν κατάλογο (ο οποίος σήμερα μετρά 2,71 δις ιστοσελίδες) στον οποίο ανατρέχει με βάση κάποιες λέξεις κλειδιά που έχουν δοθεί από εμάς. Τα

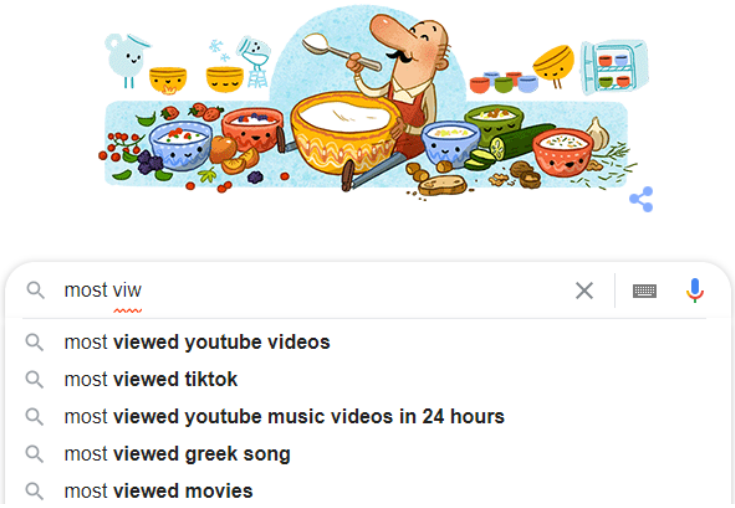
κλειδιά αυτά είναι τα λεγόμενα search, μέσω των οποίων επέρχονται τα αποτελέσματα της αναζήτησης [13].

Οι πιο δημοφιλείς ιστοσελίδες στο Διαδίκτυο :

1. Apple.com
2. Youtube.com
3. Google.com
4. Blogger.com

Οι ιστοσελίδες με τους περισσότερους επισκέπτες για το 2020 :

1. Youtube.com με 8.564δις επισκέπτες/μήνα
2. Facebook.com με 3.483ις επισκέπτες/μήνα
3. Wikipedia.org με 2.223δις επισκέπτες/μήνα
4. Twitter.com
5. Amazon.com
6. Play.google.com
7. Instagram.com
8. Pinterest.com



Εικόνα 9. Search στη Google, η λέξη most λειτουργεί ως λέξη κλειδί για αναζήτηση στο κατάλογο-βιβλιοθήκη της.

2.1.2 Deep Web

Υπάρχουν όμως κάποιες ιστοσελίδες που προστατεύονται με κωδικούς και ο crawler δεν μπορεί να φτάσει σε αυτές με αποτέλεσμα να μην μπορούν να αποθηκευτούν στην βιβλιοθήκη μιας μηχανής αναζήτησης, άρα εμείς δεν μπορούμε να ψάξουμε αυτές τις ιστοσελίδες σε μια μηχανή αναζήτησης καθώς δεν υπάρχουν κάπου αποθηκευμένες, αυτό είναι το Deep Web. Για παράδειγμα, μπορούμε να μπούμε στην σελίδα του Gmail (surface web) αλλά για να δούμε τα εισερχόμενα mail μας πρέπει να δώσουμε προσωπικά μας στοιχεία ώστε να συνδεθούμε στο λογαριασμό μας (Deep Web). Το Deep Web (επίσης γνωστό και ως Deepnet, Undernet) είναι ότι δεν ανήκει στον Επιφανειακό Web (Surface Web), το οποίο μπορούμε να το αναζητήσουμε σε συνηθισμένη μηχανή αναζήτησης και θεωρείται πως αποτελεί το 95% του συνολικού web [14].

Παραδείγματα ιστοσελίδων που βρίσκονται στο Deep Web:

- Facebook, Forums, Email, iCloud.
- Ιστοσελίδες που παράγονται δυναμικά όπως ebay, car.gr.
- Ιστοσελίδες που έχουν εξαιρέσει τον εαυτό τους από μηχανές αναζήτησης μέσω ενός αρχείου που ονομάζεται robot.txt το οποίο μόλις ο crawler το διαβάσει δε θα αποθηκεύσει τίποτα στην βιβλιοθήκη της Google.
- Ιστοσελίδες που δεν της έχει αναζητήσει ποτέ κανένας.

2.1.3 Dark Web

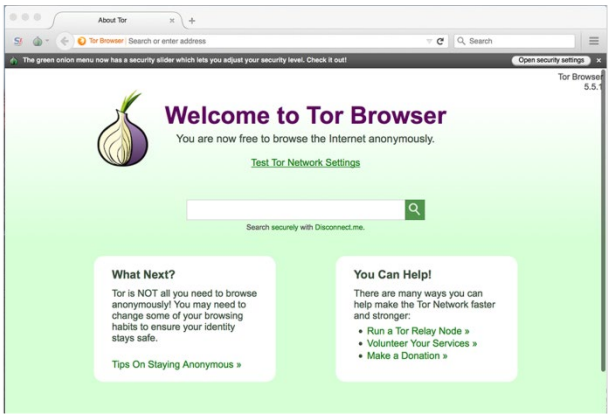
2.1.3.1 Ορισμός

Το Dark Web αποτελεί κομμάτι του Deep Web και συγκεκριμένα είναι υποσύνολο του. Πιο πάνω αναφέραμε πως για να επισκεφθούμε μια ιστοσελίδα μπορούμε να χρησιμοποιήσουμε το URL της, είτε να την αναζητήσουμε σε μια μηχανή αναζήτησης. Το Deep Web, είναι το κομμάτι του διαδικτύου που δεν μπορούμε να βρούμε μέσω μηχανών αναζήτησης. Το Dark Web είναι το κομμάτι του διαδικτύου που δεν έχουν πρόσβαση ούτε οι browser (μέθοδος URL), δε χρησιμοποιεί το πρωτόκολλο HTTP για να επικοινωνήσει με το server αλλά ένα άλλο πρωτόκολλο που ονομάζεται ONION. Το σκοτεινό διαδίκτυο, είναι ένας διαδικτυακός ιστός, στον οποίο οι χρήστες μπορούν να κρατήσουν την ανωνυμία τους σε υπηρεσίες. Μπορεί να χρησιμοποιηθεί είτε για θετικούς είτε για αρνητικούς

σκοπούς. Η ανωνυμία διασφαλίζεται με την βοήθεια δικτύων επικάλυψης που η προσέγγιση τους γίνεται με συγκεκριμένα λογισμικά και άδειες με την βοήθεια πρωτοκόλλων. Χαρακτηριστικά τέτοια σκοτεινά δίκτυα είναι τα F2F που ανταλλάσουν μηνύματα με peer to peer σύνδεση [17]. Το μεγαλύτερο χαρακτηριστικό του Dark Web είναι η ανωνυμία, δηλαδή η απόκρυψη στοιχείων του χρήστη, κάτι που θα αναλύσουμε εκτενέστερα παρακάτω.

2.1.3.2 Πρόσβαση

Για να προσπελάσουμε ιστοσελίδες του Dark Web χρησιμοποιούμε ειδικό browser όπως το TOR (The Onion Router). Για να μπορέσει ο browser να διατηρήσει την ανωνυμία μας, κάθε φορά που στέλνουμε ένα μήνυμα στο server, αυτό ταξιδεύει ανά τον κόσμο σε διάφορους κόμβους οι οποίοι κωδικοποιούν το μήνυμα και μόλις φτάσει στο server ακολουθεί την αντίστροφη διαδικασία μέσω των κόμβων αποκρυπτογραφώντας το μήνυμα, μέχρι τελικά να φτάσει σε εμάς. Οι κόμβοι είμαστε εμείς οι ίδιοι, δηλαδή όλοι οι χρήστες του TOR, άρα ο ένας ουσιαστικά βοηθάει τον άλλον για να διατηρηθεί η ανωνυμία [16]. Η ανωνυμία δεν άργησε να προσελκύσει την κακή βούληση και το Dark Web συνδέθηκε άμεσα με το κακό, το έγκλημα και την παρανομία. Πολλοί θεωρούν ότι το Dark Web είναι κατασκεύασμα κάποιας εγκληματικής οργάνωσης, όμως στη πραγματικότητα είναι δημιούργημα του Αμερικανικού Πολεμικού Ναυτικού για να επικοινωνούν οι πράκτορες μεταξύ τους με ασφάλεια [15]. Η επιβολή του νόμου στο Dark Web καθίσταται υπερβολίκα δύσκολη καθώς η ανωνυμία που προσφέρει, αποκρίπτει όλα τα στοιχεία του χρήστη από τα νομικά όργανα.



Εικόνα 10. The Onion Router (TOR) [18].

Εικόνα 11. Χαρακτηριστική εικόνα που αναπαριστά τον όγκο του web με την μορφή παγόβουνου [19].

2.2 Πρωτόκολλα του Διαδικτύου

Στα δίκτυα υπολογιστών, οποιαδήποτε επικοινωνία μεταξύ απομακρυσμένων συσκευών απαιτεί την ανταλλαγή μηνυμάτων σύμφωνα με ένα συγκεκριμένο πρωτόκολλο. Για παράδειγμα, όταν συνδέεστε στο διαδίκτυο και ανοίγετε μια σελίδα, ο φυλλομετρητής σας (browser) στέλνει μια αίτηση στον κατάλληλο εξυπηρετητή με βάση τη διεύθυνση που πληκτρολογήσατε. Αυτή η αίτηση είναι ένα κατάλληλα διαμορφωμένο μήνυμα GET του πρωτοκόλλου HTTP . Το πρωτόκολλο είναι υπεύθυνο για την μορφή και την σειρά των ανταλλασόμενων μηνυμάτων μεταξύ συσκευών. Επιπλέον καταγράφει και τις ενέργειες που γίνονται κατά την αποστολή και την λήψη των μηνυμάτων [20]. Τα πρωτόκολλα του Internet έχουν 3 επίπεδα, το επίπεδο Εφαρμογής, το επίπεδο Μεταφοράς και το επίπεδο Δικτύου. Το επίπεδο εφαρμογής στο Internet καλύπτει τα επίπεδα εφαρμογής και παρουσίασης του OSI, Τα πιο συχνά πρωτόκολλα που χρησιμοποιούνται από τους χρήστες είναι.

- Telnet (Χρήση από απόσταση).
- FTP (Μεταφορά αρχείων).

- SMTP (Μεταφορά Email).
- POP/IMAP (Ανάγνωση Email).
- HTTP/HTML (Πρόσβαση στο Web).

Πρωτόκολλα αυτού του επιπέδου που υποστηρίζουν την λειτουργία και διαχείριση του δικτύου :

- DNS (Κατανεμημένος κατάλογος ονομάτων).
- SNMP (Διαχείριση από απόσταση).
- BOOTP (Αρχικό φόρτωμα κώδικα).
- RARP (Αντίστροφη μετατροπή διευθύνσεων).

Στο επίπεδο της μεταφοράς χρησιμοποιούνται δυο πρωτόκολλα:

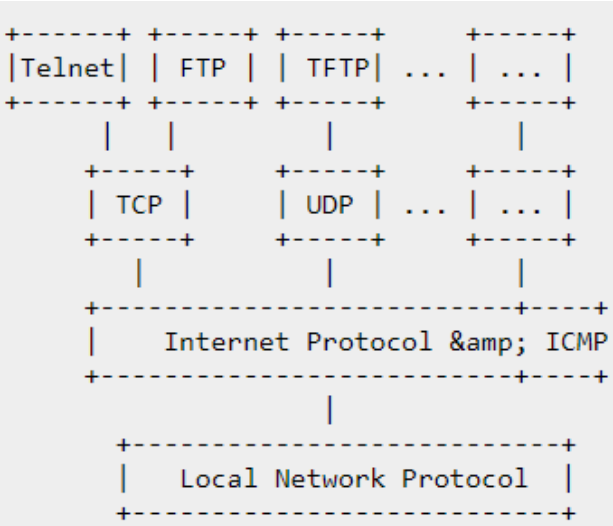
- TCP (Transmission Control Protocol).
- UDP (User Datagram Protocol).

Στο επίπεδο του δικτύου:

- IP (Internet Protocol).

Το μοντέλο Αναφοράς για την διασύνδεση ανοικτών συστημάτων OSI, ορίστηκε από τον Διεθνή Οργανισμό Τυποποίησης ISO και προδιαγράφει 7 επίπεδα. Αυτό γίνεται για να είναι εφικτή η διασύνδεση διαφορετικών υπολογιστικών συστημάτων εφόσον στα αντίστοιχα επίπεδα χρησιμοποιούν συμβατές ή ίδιες τεχνικές και κανόνες, δηλαδή τα ίδια πρωτόκολλα. Στην πραγματικότητα το OSI είναι μια πρώτη προσπάθεια στην βιομηχανία των υπολογιστών για να συμφωνήσει στα κοινά πρότυπα δικτύωσης και έτσι καταλήγει στην δημοσίευση του μοντέλου OSI το 1984 που φαίνεται παρακάτω [21].

Εικόνα 12 [23].



Εικόνα 13 [22].

2.2.1 HTTP – TCP – UDP – DNS – IP

2.2.1.1 HTTP

Οι φυλλομετρητές του Παγκόσμιου Ιστού για να μεταφέρουν δεδομένα από έναν server σε έναν client χρησιμοποιούν το πρωτόκολλο επικοινωνίας HTTP, ή

αλλιώς Πρωτόκολλο Μεταφοράς Υπερκειμένου. Το πρόθεμα http πριν από τον σύνδεσμο, κάνει την σύνδεση ασφαλή, ενώ το πρόθεμα https χρησιμοποιείται για να δηλώσει μια δικτυακή σύνδεση, που τα δεδομένα που ανταλλάσονται θα είναι σε κρυπτογραφημένη μορφή και η σύνδεση θα γίνει σε διαφορετική πόρτα. Τα πρωτόκολλα https δεν είναι πανομοιότυπα μεταξύ τους και ως εκ τούτου δε παρέχει την ίδια ασφάλεια και αποτελεσματικότητα στις αναζητήσεις.Η πρώτη εταιρία που σχεδίασε αυτό το πρωτόκολλο είναι η Netscape Communications Corporation και η εφαρμογή αυτού του πρωτοκόλλου έγινε σε ιστοσελίδες που χρειάζεται αυθεντικοποίηση και κρυπτογραφία. Πλέον, το συναντάε σε όλες τις ιστοσελίδες που απαιτείται ιδιαίτερη ασφάλεια [24][25].

2.2.1.2 DNS

Οι servers ανα τον πλανήτη, που μας εμφανίζουν σελίδες ανάλογα τις αναζητήσεις, στέλνουν κάποιες κωδικοποιημένες διευθύνσεις τις οποίες είναι δύσκολο να θυμόμαστε. Δηλαδή, είναι δύσκολο να ξέρουμε σε ποια IP διεύθυνση (123.X.XX.XX) βρίσκεται ο server του youtube (www.youtube.gr). Οι DNS servers αναλαμβάνουν να αντιστοιχήσουν διευθύνσεις IP με ένα μοναδικό όνομα στο χώρο του διαδικτύου, δηλαδή την διεύθυνση που πληκτρολογούμε (Domain Name). Οι DNS servers είναι οι τηλεφωνικοί κατάλογοι του Internet [26].

2.2.1.3 UDP – TCP

Η ονομασία του μοντέλου αναφοράς TCP/IP προκύπτει από τα πρωτόκολλα του επιπέδου δικτύου και μεταφοράς. Επιτρέποντας ένα λογισμικό να τρέχει πάνω από ένα εσωτερικό δίκτυο. Το επίπεδο δικτύου διαχειρίζεται τα πακέτα ενός εσωτερικού δικτύου όσον αφορά την παράδοση και δρομολόγηση αυτών, προς τον τελικό προορισμό, ενώ το επίπεδο μεταφορας (TCP) διαχειρίζεται τις συνδέσεις και παρέχει αξιοπιστία. Το γεγονός ότι το πρότυπο επικοινωνίας TCP/IP φέρει το όνομα του πρωτοκόλλου του διαδικτύου και πρωτόκολλου ελέγχου μετάδοσης, υποδεικνύει ότι αυτά τα δύο πρωτόκολλα αναλαμβάνουν την βασική λειτουργία του μοντέλου αυτού. [27]. Το TCP όμως δεν χρησιμοποιείται παντού, για παράδειγμα, θα ήταν πρακτικά άχρηστο να έχουμε τους μηχανισμούς αξιοπιστίας και επιβεβαίωσης αποστολής μηνυμάτων για να δούμε ένα video στο διαδύκτιο καθότι μας ενδιαφέρει άμεσα μόνο η πληροφορία και όχι τα σφάλματα. Σε αυτή την περίπτωση χρησιμοποιείται το πρωτόκολλο UDP το οποίο δεν παρέχει μηχανισμό επιβεβαίωσης,

ελέγχου ροής δεδομένων κλπ για πακέτα που στέλνονται μεταξύ δύο οντοτήτων, απλά προωθεί τα πακέτα στην άλλη μεριά χωρίς να ελέγχει αν αυτά έφτασαν ή όχι [27].

2.2.1.4 IP

Το επίπεδο δικτύου περιλαμβάνει το πρωτόκολλο IP το οποίο ορίζει τα πεδία ενός IP πακέτου καθώς και το πως τα τερματικά συστήματα και οι δρομολογητές ενεργούν σε αυτά τα πεδία. Το επίπεδο δικτύου παρέχει επίσης πολλά πρωτόκολλα δρομολόγησης τα οποία καθορίζουν δυναμικά τις διαδρομές που ακολουθούν τα IP πακέτα από την πηγή στο προορισμό. Το διαδίκτυο είναι ένα δίκτυο δικτύων που αποτελείται από κόμβους. Για κάθε κόμβο που είναι συνδεδεμένος στο διαδίκτυο εκχωρείτε ένας μοναδικός αριθμός που είναι γνωστός ως IP διεύθυνση και το κάθε IP πακέτο θα πρέπει να διαθέτει με την σειρά του μια μοναδική διεύθυνση προορισμού για να μπορέσει να δρομολογηθεί προς έναν άλλο υπολογιστή. Η διεύθυνση αυτή αποτελείται από 4 ακεραίους αριθμούς χωρισμένους με μια τελεία και σε κάθε υπολογιστή αποδίδεται μια ξεχωριστή μοναδική IP διεύθυνση (123.X.XX.XX) [28].

2.3 Προσωπικά Δεδομένα

Προσωπικά δεδομένα είναι κάθε πληροφορία που αναφέρεται στο πρόσωπο κάθε ατόμου, όπως το όνομα και το επάγγελμα του, η οικογενειακή του κατάσταση, η ηλικία του, ο τόπος κατοικίας του και άλλα. Έτσι, ένα σημαντικό θέμα που πρέπει να έχουν υπόψη τους οι χρήστες και οι διαχειριστές των υπηρεσιών του διαδικτύου είναι η προστασία της ιδιωτικότητας και των προσωπικών δεδομένων, καθώς προσωπικά δεδομένα θεωρούνται και η διεύθυνση του ηλεκτρονικού ταχυδρομείου αλλά και οι κωδικοί πρόσβασης που χρησιμοποιούμε για την πρόσβαση μας σε υπηρεσίες διαδικτύου. Η προστασία αυτή, αποτελεί θεμελιώδες ανθρώπινο δικαίωμα και ρυθμίζεται από σχετική νομοθεσία. Πλέον, πρέπει να είμαστε ιδιαίτερα προσεκτικοί καθώς αρκετές δραστηριότητες στο διαδίκτυο βασίζονται στην επεξεργασία των προσωπικών δεδομένων όπως για παράδειγμα, η εγγραφή σε ένα διαδικτυακό κατάστημα, σε ένα παιχνίδι ή σε κάποια πλατφόρμα κοινωνικής δικτύωσης. Για να χρησιμοποιήσει κάποιος τα προσωπικά μας δεδομένα, για κάποιο σκοπό, πρέπει να έχει την συγκατάθεση μας. Γενικά, πρέπει να είμαστε προσεκτικοί με την δημοσιοποίηση προσωπικών μας δεδομένων σε κοινωνικούς ιστότοπος και υπηρεσίες

καθώς κάθε στοιχείο που ανεβάζουμε στο διαδίκτυο είναι δυνατόν να υποπέσει στην αντίληψή οποιοδήποτε. Επιπρόσθετα, η δραστηριότητα μας στο διαδίκτυο μπορεί να αφήσει ίχνη που δύσκολα σβήνονται. Πρέπει να διαβάζουμε την πολιτική απορρήτου στην ιστοσελίδα που βρισκόμαστε ώστε, να ενημερωνόμαστε για το πως θα χρησιμοποιηθούν τα προσωπικά μας δεδομένα και για το αν εγκαθιστούν cookies στον υπολογιστή. Τα cookies είναι μικρά αρχεία που μία ιστοσελίδα αποθηκεύει στον υπολογιστή ενός χρήστη ώστε κάθε φορά που ο χρήστης συνδέεται στην ιστοσελίδα να ανακτά πληροφορίες προσαρμοζμένες σε αυτόν.Υπάρχει ειδική νομοθεσία που προστατεύει τους χρήστες από την ανεξέλεγκτη χρήση των προσωπικών τους δεδομένων στην Ελλάδα και στην υπόλοιπη Ευρωπαική Ένωση. Η Αρχή Προστασίας Προσωπικών Δεδομένων ιδρύθηκε το 1997 με το νόμο 2472/1997 και λειτουγεί ως ανεξάρτητος φορέας με σκοπό την προστασία του χρήστη και των προσωπικών του δεδομένων στο διαδίκτυο. Άλλες αρχές που έχουν τον ίδιο σκοπό είναι η Αρχή Διασφάλισης Απορρήτου των Επικοινωνιών και ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων. Ο νέος γενικός κανονισμός GDPR - 2016/679 της ΕΕ που έχει εφαρμογή σε όλα τα κράτη μέλη της, χωρίς την προυπόθεση κρατικής νομοθεσίας έχει σαν σκοπό τα παρακάτω [29].

- Ενίσχυση της παιδικής προστασίας.
- Αύξηση των δικαιωμάτων των υποκείμενων των δεδομένων.
- Γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα.
- Προστασία δεδομένων από το σχεδιασμό και εξ ορισμού.
- Αυστηροποίηση των προυποθέσεων της παροχής συγκατάθεσης των υποκείμενων των δεδομένων.
- Αρχεία δραστηριοτήτων επεξεργασίας.
- Ορισμός υπευθύνου προστασίας δεδομένων.

ΚΕΦΑΛΑΙΟ 3: HACKING

3.1 Εισαγωγή στο Hacking

Το hacking μπορούμε να πούμε ότι έκανε την πρώτη εμφάνιση του στην δεκαετία του 60’ στο Πανεπιστήμιο του MIT. Τότε το μέγεθος ενός υπολογιστή και οι συνθήκες κάτω από τις οποίες έπρεπε να βρίσκεται για να λειτουργήσει, καθιστούσαν τη λειτουργία του κοστοβόρα και μη-αποδοτική. Λύση σε αυτό το πρόβλημα, δώσανε μερικοί φοιτητές του MIT οι οποίοι δημιούργησαν μερικά προγράμματα για να αυξήσουν την απόδοση των υπολογιστών, τα λεγόμενα hacks. Αξιοσημείωτο είναι το γεγονός πως τα προγράμματα που κατασκεύαζαν ήταν πολύ καλύτερα από τα αρχικά που είχε ένας υπολογιστής. Το πρώτο hack στην ιστορία των υπολογιστών είναι το γνωστο σε όλους μας σημερινό λειτουγικό σύστημα UNIX, το οποίο δημιουργήθηκε από 2 υπαλλήλους της Bell με σκοπό την αύξηση της ταχύτητας των υπολογιστών τους. Για να γίνει κάποιος χάκερ πρέπει να έχει το γνωστικό υπόβαθρο και τις ικανότητες ώστε να μπορεί να διαχειρίζεται υπολογιστικά συστήματα και να πειραματίζεται με αυτά, χωρίς απαραίτητα να τα καταστρέφει ή να δημιουργεί προβλήματα σε αυτά. Οι χάκερς χτίζουν πράγματα ενώ οι κράκερς σπάνε. Η πλειοψηφία αυτών των ατόμων είναι προγραμματιστές ή ακόμα και σχεδιαστές υπολογιστικών συστημάτων που γνωρίζουν τον τρόπο με τον οποίο κατασκεύαζονται και έτσι μπορούν να τα επεξεργάζονται. Όμως υπάρχουν και χάκερς οι οποίοι χωρίς κάποιο μεγάλο προγραμματιστικό ή γνωστικό υπόβαθρο βελτιώνουν συνεχώς τις ικανότητες τους αυτοδίδακτα και εμπειρικά. Οι χάκερ δρούν ως μονάδες ή ως ομάδες (hacking-groups) [30].

3.2 Οφέλη των Hackers

Σχετικά με τα οφέλη των χάκερς, εισβάλουν σε υπολογιστές και υπολογιστικά συστήματα, πιστεύοντας ότι η είσοδος πρέπει να είναι ελεύθερη (Open-source) καθώς και το hacking αποτελεί ένα είδος τέχνης και ευρηματικότητας που παρουσιάζει το μεγαλείο της πληροφορικής. Η τακτική των hackers, είναι ένα μέσο ή ένας τρόπος

διαμαρτυρίας για να νιώσουν την ικανοποίηση που τους δίνει η κτήση ενός δυνατου εργαλείου. Μέσω του hacking, καταφέρνουν να αποσπάσουν χρήματα, στοιχεία πιστωτικών καρτών, διευθύνσεις e-mail και ότι άλλο μπορεί να θεωρηθεί ως σημαντκή πληροφορία ή δεδομένο το οποίο με την σειρά του μπορεί να τους φέρει σε πλεονεκτική θέση απέναντι στο μηχανισμό ασφαλείας των υπολογιστικών συστημάτων. Επίσης, εισβάλουν σε κρατικούς μηχανισμούς και υπηρεσίες, πολλές φορές υποκινούμενοι από συμφέροντα και μυστικές υπηρεσίες, με απώτερο σκοπό την απόσπαση μυστικών πληροφοριών και την κατασκοπεία. Τα συμφέροντα και τα κίνητρα των χάκερς ποικίλουν.Όμως, κατά κοινή ομολογία κατατάσονται σε 2 κατηγορίες. Η πρώτη αφορά τα κοινωνιολογικά/ψυχολογικά κίνητρα και η δέυτερη τα τεχνικά κίνητρα.

Τα κοινωνιολογικά/ψυχολογικά κίνητρα είναι:

- Μυστήριο.
- Η κοινωνικη καταξίωση των άνομων πράξεων στο διαδύκτιο.
- Αρωγός για μελλοντικούς χρήστες υπολογιστών βρίσκοντας κενά ασφαλείας υπολογιστικών συστημάτων.
- Η προσδοκία για την κατάκτηση εξουσίας στο κόσμο των υπολογιστικών συστημάτων.

Τα τεχνικά κίνητρα τα οποία είναι:

- Να αρχίσουν επιθέσεις άρνησης της εξυπηρέτησης (Distributed Denial of Service).
- Για να διατηρίσουν την ανωνυμία τους.
- Για να διατηρήσουν τα δικαιώματα διαχειριστή στο IRC (Internet Relay Chat), το οποίο είναι ένα απαραίτητο εργαλείο για την επικοινωνία μεταξύ των επιτιθέμενων.
- Για να αποκτίσουν τα δικαιώματα κατοχύρωσης και διάδοσης πληροφορίας.
- Και να χρησιμοποιήσουν το δίκτυο, με σκοπό να διατηρίσουν αποθηκευμένα αρχεία εντός αυτού, χωρίς κάποιο κόστος [31].

3.3 Τρόπος Δράσης – Είδη Hacking

Όσες περισσότερες πληροφορίες έχει για το σύστημα που θέτει ως στόχο κάθε φορά, τόσο αυξάνονται οι πιθανότητες του για να εισβάλει σε αυτό διατηρώντας την ανωνυμία του και την ύπαρξη του.Αυτές οι πληροφοριές που θα πρέπει να συλέξει αναφέρονται στους διαχειριστές του συστήματος αλλά και στο ίδιο το σύστημα

(hardware, λειτουργικό σύστημα).Ο χάκερ μπορεί να αρπάξει αυτές τις ευαίσθητες πληροφορίες από τον ευρύτερο κύκλο χρήσης, όπως από την επιχείρηση στην οποία ανήκει ή από τους τεχνικούς.Ένα απαραίτητο στοιχείο που πρέπει να έχει ένα πληροφοριακόο σύστημα για να πούμε ποως λειτουργεί με ασφάλεια είναι η καλή πιστοποίηση των δικαιούχων πρόσβασης.Οπότε πρωταρχικός στόχος στο πλάνο ενός χάκερ για να εισέλθει εντός κάποιου συστήματος είναι να καταστρέψει ή να ξεγελάσει το μηχανισμό ταυτοποίησης.Αποκτώντας πρόσβαση λοιπόν ο χάκερ μπορεί να βάλει σε αφαρμογή το σχέδιο του με τα δικαιώματα ενός νόμιμου χρήστη. Ανεξάρτητα από τον σκοπό για τον οποίο έκανε την επίθεση, ένας χάκερ προσπαθεί να συγκεντρώσει όσον το δυνατόν πρισσότερες πληροφορίες και στοιχεία αλλά και να αξιοποιήσει στο έπακρον τις λειτουργίες που εκτελεί το σύστημα σαν ένας νόμιμος χρήστης.

3.3.1 Μέθοδοι Επιθέσεων

Packet Sniffer: Τα πακέτα δικτύου είναι μονάδες δεδομένων που έχουν μια συγκεκριμένη προέλευση και προορισμό ή μπορούμε να πούμε ότι μεταφέρονται από έναν αποστολέα σε έναν δέκτη. Αυτά τα πακέτα μεταφέρουν δεδομένα μέσω πρωτοκόλλων επικοινωνίας του Διαδικτύου. Κάθε πακέτο περιλαμβάνει πληροφορίες για την πηγή και τον προορισμό ή για τις ταυτότητες τους όταν μεταφέρονται ή όταν γίνεται «λήψη» Η μέθοδος packet sniffing είναι η διαδικασία κατά τη οποία οι χάκερς συλλέγουν αυτά τα πακέτα ενός ολόκληρου δικτύου και τα χρησιμοποιούν όπως θέλουν. Επίσης αυτή η μέθοδος χρησιμοποιείται και από κυβερνήσεις και διαφημιστικές εταιρίες για να κατηγοριοποιήσουν τις καταναλωτικές μας συνήθιες .

Δούρειοι Ίπποι: Ο εισβολέας κρύβει το κακόβουλο πρόγραμμα σε ένα αθώο email ή λήψη. Με ένα κλίκ ή λήψη, το πρόγραμμα μεταφέρει κακόβουλο λογισμικό στη συσκευή του θύματος και ο κακόβουλος κώδικας μπορεί να εκτελέσει οποιαδήποτε διεργασία σκοπεύει ο εισβολέας. Μόλις ένας δούρειος ίππος μεταφερθεί και ενεργοποιηθεί, μπορεί να επηρεάσει την αρνητικά την απόδοση του υπολογιστή και να θέσει το θύμα σε κίνδυνο με πληθώρα τρόπων. Οι δούρειοι ίπποι μπορούν να δώσουν τον έλεγχο της συσκευής στον εισβολέα χωρίς αυτό να γίνει αντιληπτό, όπως την κάμερα, το μικρόφωνο και το πληκτρολόγιο. Τέλος, δούρειοι ίπποι χρησιμοποιούνται από νομικά όργανα για να αποκτήσουν πληροφορίες που σχετίζονται με κάποια έρυενα.

Ιοί και σκουλήκια: Τα σκουλίκια μοιάζουν με ιούς που αυτοαναπαράγονται και κρύβονται, αλλά είναι λίγο διαφορετικά στο ότι συνήθως αντί να έχουν κάποιο είδος καταστροφικού φορτίου όταν καταστέφουν αρχεία ενός σκληρού δίσκου ή όταν γίνεται εκκίνηση του υπολογιστή, στέλνουν αρχεία που δημιουργούν κίνηση και καταναλώνουν εύρως ζώνης.

Denial of Service (DoS attack): Είναι ένας όγκος προγραμμάτων που στέλνουν μηνύματα αυτοματοποιημένα και ρυθμισμένα από τον εισβολέα, με σκοπό την υπερφόρτωση του συστήματος που λόγω των πολλών ταυτόχρονων λειτουργιών δεν μπορεί να αποδώσει ή να ανταποκριθεί.

Distributed denial of service (DDoS attack): Επιθέσεις στον κυβενοχώρο σε συγκεκριμένο διακομιστή ή δίκτυο με την επιδίωξη να διαταράξουν τη κανονική λειτουργία του δικτύου ή του διακομιστή. Μια επίθεση DDoS το κάνει αυτό πλημμυρίζοντας το στοχευμένο δίκτυο ή διακομιστή με μια συνεχή κίνηση αδιάφορης πληροφορίας, με την βοήθεια trojans και worms, όπως ψευδή αιτήματα.

DNS Spoofing: Το DNS αντιστοιχίζει domain names με διευθύνσεις IP. Ορισμένες απαντήσεις από το DNS αποθηκεύονται στην cache της συσκευής, οπότε την επόμενη φορά που θα επισκεφθούμε τον ίδιο ιστότοπο, αντί να αναζητήσουμε ξανά το DNS, θα πάρει άμεσα την IP από την cache. Οι χάκερ πλαστογραφούν τον διακομιστή DNS και στέλνουν μια διαφορετική IP στο χρήστη, την IP του δικού τους διακομιστή. Δηλαδή αποκλείουν την πραγματική απάντηση DNS και στέλνουν τις δικές τους απαντήσεις. Ο εισβολέας θα ξέρει τι αίτημα υποβάλλεται.

IP Spoofing: Στην περίπτωση αυτή ο χάκερ αντικαθιστά τη διεύθυνση IP σε ένα πακέτο πληροφορίας για να καλύψει την πηγή των δεδομένων. Αυτό μπορεί να εξυπηρετήσει διάφορους κακόβουλους σκοπούς. Ένας εισβολέας μπορεί να ξεγελάσει τον υπολογιστή ώστε να σκεφτεί ότι τα πακέτα προέρχονται από μια αξιόπιστη πηγή και τοον μολύνουν με κακόβουλο λογισμικο. Μπορούν να παρακολούθουν τη διαστηριότητα μας στο διαδίκτυο και να εξαγάγουν τους κωδικούς πρόσβασης χωρίς να το γνωρίζουμε (phising) .

3.3.2 Είδη Hackers

- **Crackers** ή black hat hakers είναι άτομα που επεξεργάζονται την είσοδο σε έναν υπολογιστή ή σε ένα δίκτυο. Ένας κράκερ έχει ως σκοπό την κακόβουλη δραστηριότητα και ως στόχο την πρόσβαση σε εμπιστευτικά αρχεία.

- Οι **white hack hackers** εντοπίζουν τις αδυναμίες ενός συστήματος με το να το «χακάρουν», έχοντας βέβαια την έγκριση των διαχειριστών. Αύτο γίνεται με σκοπό να ενδυναμώσουν το σύστημα ασφαλείας. Αυτό το είδος χάκινγκ είναι απολύτως νόμιμο και ηθικό, έτσι οι χάκερς που ασχολούνται με αυτόν το τομέα ονομάζονται και ethical hackers. Την βοήθεια τέτοιων χάκερ ζητούν και οι μυστικές υπηρεσίες κυβερνήσεων για να εξιχνιάσουν εγκλήματα

- Μεταξύ των white hats και black hats βρίσκονται οι **Gray hats**. Οι Gray hat hackers, εντοπίζουν σημεία στα οποία η ασφάλεια του συστήματος είναι ευάλωτη και τα αναφέρουν στον ιδιοκτήτη του συστήματος. Όμως, όταν το κάνουν αυτό, δεν ζητούν την έγκριση του και πολλές φορές ζητούν και αντάλλαγμα. Επίσης, χαρακτηρίστηκαν και ως «hacktιβιστές (hacktivists)», καθώς χρησιμοποιούν τους υπολογιστές και το διαδίκτυο για να περάσουν πολιτικά και ανθρωπιστικά μηνύματα, όπως οι Anonymous [31].

- Οι **Old School Hackers** είναι αυτοί οι οποίοι ασχολούνται με τη δημιουργία προγραμμάτων και την ανάλυση/σχεδιασμό συστημάτων. Δεν έχουν κακές προθέσεις και εκτιμούν σε βάθος το απόρρητο των πληροφοριών.

- Ως **Script Kiddies** χαρακτηρίζονται οι ανειδίκευτοι χάκερς, με λίγες γνώσεις προγραμματισμού και πληροφοριακών συστημάτων, οι οποίοι θέτουν σε κίνδυνο ένα σύστημα χρησιμοποιώντας έτοιμα scripts, εργαλεία και λογισμικο που αναπτύχθηκα από άλλους χάκερ.

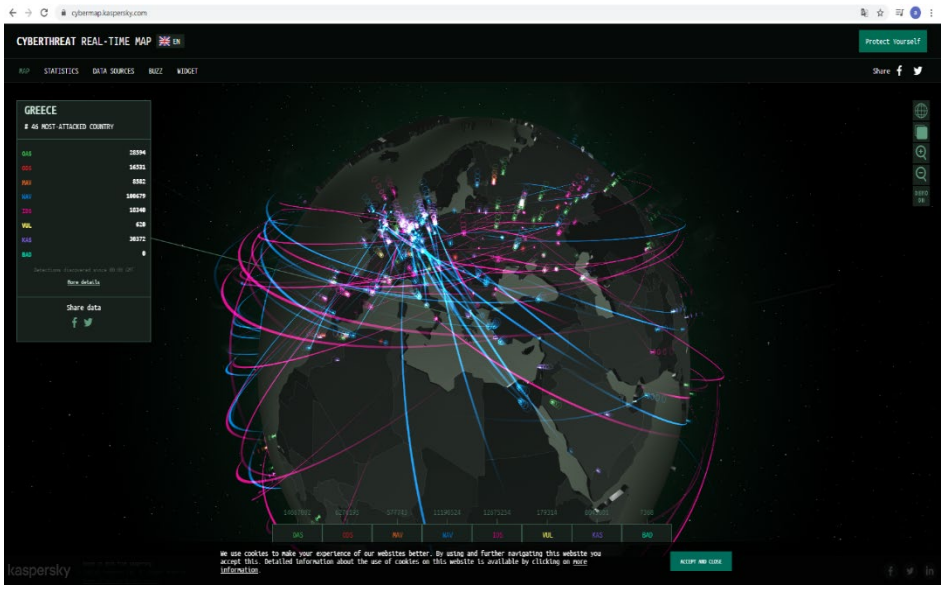
- Οι **Professional Criminals** στοχεύουν να καταστρέψουν υποδομές πληροφοριακών συστημάτων χωρίς κάποιον ενδιασμό όσον αφορά τις ποινές που θα επιβληθούν.

- Οι **Coders** γνωρίζουν πολύ καλά το αντικείμενο του προγραμματισμού και δημιουργούν λογισμικό, βλαβερό για τον υπολογιστή. Συνήθως, δεν τα χρησιμοποιούν οι ίδιοι αλλά τα διαθέτουν μέσω της αγοράς σε τρίτους.

3.4 Σημασία του hacking στον 21ο αιώνα σε συλλογικό επίπεδο

Πλέον κάθε χώρα έχει μια ομάδα ατόμων θεσμικά ορισμένη που επιτελεί έναν συγκεκριμένο έργο στο επίπεδο του hacking. Συνήθως είναι για την ασφάλεια και την άμυνα και μπορεί και να κάνει επιθέσεις για διάφορους λόγους. Το 2010 χρησιμοποιήθηκε για πρώτη φορά στην ιστορία ένα ψηφιακό όπλο για να παραλύσει μια πυρηνική εγκατάσταση στο Ιράν. Αυτό, ήταν ένας ιός με το όνομα Stuxnet ο οποίος ήταν ένα ψηφιακό σκουλήκι που μπορούσε να προκαλέσει διάφορες ζημιές στο σύστημα. Η επίθεση οργανώθηκε από τις ΗΠΑ και το Ισραήλ. Η διάδοση του ιού έγινε μέσω των υπολογιστών που χρησμιποιούσαν εταιρίες στη Ευρώπη οι οποίες συνεργαζόντουσαν με το Ιράν.Οι μηχανικοί αυτών των εταιριών θα επισκέπτονταν τις εγκαταστάσεις της Natanz και με το μολυσμένο από το Stuxnet usb τους θα μετέδιδαν τον ιό στα συστήματα της Natanz. Μόλις έμπαινε σε ένα σύστημα δεν ενεργοποιούταν αμέσως, ήταν θαμμένος στον κώδικα αναζητώντας ένα συγκεκριμένο στόχο αλλιώς παρέμενε αδρανής. Αύτο που ήθελε να καταστρέψει ήταν οι φυγοκεντρικές συσκευές αυξάνοντας τον ρυθμό με τον οποίο στροβιλίζονταν. Δεν άφηνε κανένα ίχνος. Το Stuxnet χρειάστηκε 13 μέρες για να εντοπίσει και να σκιαγραφήσει την λειτουγία τους και έπειτα απορύθμισε την συχνότητα περιστροφής τους. Αξιοσημείωτο είναι πως ο ιός καθόλη την διάρκεια της επίθεσης έστελνε παραπλανητικά δεδομένα στους διαχειριστές και ως εκ τούτου δεν μπορούσαν να καταλάβουν τα αίτια του προβλήματος που αντιμετώπιζαν. Σήμερα ο Stuxnet θεωρείται η μεγαλύτερη κυβερνοπεπίθεση στην ιστορία. Ο ιός δεν ανακαλύφθηκε παρά μόνο το 2010 από το Kaspersky Lab (17 Ιουνίου 2010) [35]. Άλλο ψηφιακό όπλο είναι το flame, επίσης γνωστό ως Flamer, sKyWIper και Skywiper, και είναι ένα αρθρωτό κακόβουλο λογισμικό υπολογιστή που ανακαλύφθηκε το 2012 και έχει ως στόχο υπολογιστές που έχουν εγκατεστημένα τα Windows. Είναι ευρέως γνωστό στις χώρες της Μέσης Ανατολής, οι οποίες το χρησιμοποιούν για κατασκοπεία στο Internet. Η συνεχιζόμενη άνοδος των υποστηριζόμενων από το κράτος hackers υπήρξε μια από τις πιο δραματικές εξελίξεις στον κυβερνοχώρο των τελευταίων ετών. Και τώρα φαίνεται ότι ένα νέο σύνολο χωρών είναι πρόθυμο να χρησιμοποιήσει την ίδια τακτική με μερικούς από τους μεγαλύτερους και ισχυρότερους ανταγωνιστές τους. Η κυβερνητική κατασκοπεία ξεκινάει πολύ από την αρχή του διαδικτύου, με τη Ρωσία, την Κίνα, το Ιράν και τη Βόρεια Κορέα γενικά να θεωρούνται ως οι χώρες που πιθανότατα θα συμμετάσχουν σε εκστρατείες για κατασκοπεία στον

κυβερνοχώρο ενάντια σε δυτικούς στόχους. Οι ομάδες hacking Advanced Permanent Threat (APT) στοχεύουν κυβερνήσεις και οργανισμούς σε όλο τον κόσμο. Οι δυτικές κυβερνήσεις ξοδεύουν μεγάλο μέρος της δικής τους εμπειρίας στον κυβερνοκατασκοπεία. Αλλά δεν είναι μόνο οι μεγάλες υπερδυνάμεις και οι συνηθισμένοι ύποπτοι που προσπαθούν να επωφεληθούν από το διαδίκτυο για πληροφορίες και άλλα κέρδη – και καθώς μπαίνουμε στα 2020, περισσότερες κυβερνήσεις προσπαθούν να ανεβάσουν επίπεδο στις ικανότητές τους στον κυβερνοχώρο. "Τα τελευταία πέντε χρόνια έχετε δει όλο και περισσότερες χώρες να κερδίζουν επιθετικές cyber-ικανότητες. Υπάρχουν πολλά διαφορετικά επίπεδα, αλλά κανένας από αυτούς δεν βρίσκεται στο επίπεδο των τεσσάρων μεγάλων επιτιθέμενων για τους οποίους μιλάμε", λέει ο Sahar Naumaan, αναλυτής απειλών στη BAE Systems [37]. Η διεύθυνση κυβερνοάμυνας της Ελλάδος κάθε χρόνο διοργανώνει μια εξωτερική εθνική άσκηση προσομοίωσης κυβερνοεπιθέσεων, τον «Πανόπτη», στην άσκηση συμμετέχουν στελέχη των ενόπλων δυνάμεων και του ακαδημαϊκού χώρου καθώς και ερευνητές. Έχει ως στόχο τη δημιουργία ενός δικτύου και την εξάσκηση των συμμετεχόντων σε θέματα που αφορούν την ασφάλεια. Οι επιθέσεις μέσω phishing σε οργανισμούς είναι το πρώτο βήμα, επειδή όλοι οι υπολογιστές που έχουν οι χρήστες δεν έχουν απευθείας πρόσβασης το Ιντερνέτ, είναι από τους λίγους τρόπους που μπορείς να έχεις πρόσβαση σε ένα εσωτερικό δίκτυο ενός οργανισμού.



Εικόνα 14. Online εργαλείο που δείχνει σε πραγματικό χρόνο επιθέσεις από τη μια χώρα στην άλλη https://cybermap.kaspersky.com/ [39].

3.5 Κακόβουλο λογισμικό

Το πρόγραμμα που είναι σχεδιασμένο να προκαλέσει άμμεσο ή έμμεσο πρόβλημα σε ένα υπολογιστικό σύστημα ονομάζεται κακόβουλο λογισμικο ή malicious software ή malware. Το κακόβουλο λογισμικό στοχέυει να διακόψει, να απενεργοποιήσει ή να λάβει τον έλγχο του υπολογιστή. Έχει πολλές μορφές συνήθως είναι κρυμμένο σε ένα άλλο αρχείο ή μεταμφιεσμένο ώς αβλαβή εφαρμογή. Δουλεύει εκμεταλεύοντας τεχνικά κενά ή αδυναμίες στο λειτουργικό συστήματος και στο λογισμικό. Το κακόβουλο λογισμικό μπορεί να χωριστεί σε δύο κατηγορίες. Σε αυτά που μπορούν να εκτελεστούν μόνα τους και κάποια που χρειάζονται ένα πρόγραμμα «ξενιστή» για να ενεργοποιηθούν [41].

3.5.1 Πως να αναγνωρίσετε το malware

Όταν το κακόβουλο λογισμικό αρχίσει να επιδρά στον υπολογιστή αυτό θα γίνει αντιληπτό από το ανθρώπινο μάτι μέσω της ταχύτητας ανταπόκρισης και εκτέλεσης των εντολών που δίνουμε. Συνήθως εμφανίζονται περίεργες διαφημίσεις και ειδοποιήσεις ή ανεπιθύμητες αλλαγές στους φυλλομετρητές [40].

3.5.2 Πως λειτουργεί το κακόβουλο λογισμικό

Με την πάροδο του χρόνου η ευρηματικότητα των κακόβουλων προγραμματιστών έχει πλέον αυξηθεί. Χρησιμοποιώντας πιο ενημερωμένα λογισμικα, ξεπερνώντας τα μέτρα ασφαλείας αλλά και μιμούμενοι νόμιμα συστήματα, καταφέρνουν να εξαπλωθούν. Βέβαια ο πιο αποτελεσματικός τρόπος εξάπλωσης των κακόβουλων λογισμικών είναι ο αδύναμος κρίκος, οποίος είναι ο άνθρωπος. Καλογραμμένα mail στα οποία στα οποία επισυνάπτονται κακόβουλα λογισμικά είναι από τις πιο αποτελεσματικές και φθηνές μεθόδους διάδοσης, καθώς ένα λάθος κλίκ αρκεί [40].

3.6 Είδη κακόβουλων λογισμικών

- **Ιός (Virus):** Όταν εκτελείται επαναλαμβάνεται τροποποιώντας αρχεία για άλλα προγράμματα και ενδεχομένως συμπεριλαμβανομένου του ίδιου του λειτουργικού συστήματος. Έτσι, επειδή τα αρχεία τροποποιούνται για να συμπεριλάβουν τον ιό κάθε φορά που ξεκινά αυτό το πρόγραμμα ή το λειτουργικό σύστημα, θα εκτελεί επίσης και το κώδικα του ιού στοχεύοντας την βλάβη του υπολογιστή. Ο κύριος διαφοροποιητής για έναν ιό είναι ότι

παραμένει αδρανής εως ότου εκτελεστεί από την χρήστη, όταν γίνει αυτό ξεκινά να αναπαράγεται και μπορει να έχει την μορφη ενός εκτελέσιμου αρχείου ή ενός εγγράφου που αρχικά κατεβάζουμε από το διαδύκτιο και στην συνέχεια εκτελούμε ή ανοίγουμε.[41].

- **Trojan (Δούρειος Ίππος):** Είναι ο τύπος του κακόβουλου λογισμικου που εμφανίζεται ως κανονικό πρόγραμμα, αλλά στο παρασκήνιο θα κάνει κακόβουλα πράγματα. Έτσι, αρχικά ξεγελά και τον χρήστη να το εγκαταστήσει επειδή πιστεύει ότι είναι κάτι άλλο. Τα Trojians είναι ο πιο συνηθισμένος τύπος κακόβουλου λογισμικού και μπορεί να μοιάζει για παράδειγμα με μια αριθμομηχανή, αλλά ο κύριος σκοπός του είναι να σας κάνει να το κατεβάσετε βασιζόμενοι πως είναι απλά μια αριθμομηχανή. Τα Trojans δεν αναπαράγονται και δεν στέλνονται σε άλλα άτομα του ίδιου δικτύου [41].

- **Worm («σκουλήκι»):** Τα σκουλήκια είναι και αυτά αυτοαναπαραγόμενα αλλά έχουν μια μεγάλη διαφορά, σε αντίθεση με έναν ιό που πρέπει να εκτελείται χειροκίνητα από έναν χρήστη, ένα σκουλήκι υπολογιστή μπορεί να εξαπλωθεί αυτόματα χωρίς παρέμβαση του χρήστη. Αυτό σημαίνει ότι δεν χρειάζεται να εκτελεστεί κάποιο πρόγραμμα του υπολογιστή. Απλά σαρώνει τους υπολογιστές που βρίσκονται στο δίκτυο βρίσκει τις αδυναμίες του και δρα [42].

- **Rootkit:** Λογισμικό που πολύ εύκολα πέρνει αυξημένα δικαώματα η δικαιώματα διαχειριστή ενός υπολογιστή. Αποκτά το έλεγχο των βαθύτερων και πιο ασφαλών τμημάτων του λειτουργικού συστήματος με αποτέλεσμα να μπορεί να κρύψει βαθιά ακόμα και τον ίδιο του τον εαυτό [42].

- **Λογισμικό Κατασκοπίας (Spyware):** Είναι κακόβουλο λογισμικό ή απλά λογισμικό που κατασκοπεί ή συλλέγει πληροφορίες από τον υπολογιστή και μετά τις στέλνει κάπου αλλού. Τεχνικά το spyware θα μπορούσε να περιλαμβάνει προγράμματα που δεν είναι κάν παράνομα, δηλαδή να τους δίνουμε άδεια να μας κατασκοπεύουν, απλά τις περισσότερες φορές αυτό γίνεται εν αγνοία μας και για αυτό είναι στην κατηγορία κακόβουλων λογισμικών [42].

4.0 Προστασια Προσωπικων Δεδομενων

Στις μέρες μας οι κυβερνοεπιθέσεις αυξάνονται δραμματικά με θύμματα συνήθως μεγάλες εταιρίες που εκτελούν όλες τους τις λειτουργίες με την βοήθεια του Διαδικτύου. Οσο περνάνε τα χρόνια οι γνώσεις των χάκερ αυξάνονται, άρα και η αποτελεσματικότηταα τους. Έτσι, εντοπίζουν μεγαλύτερους στόχους να επιτεθούν, οι οποίοι θα τους προσφέρνουν μεγαλύτερο κέρδος. Χαρακτηριστικό είναι το πρόσφατο παράδειγμα της Sony, η οποία έχασε 170 εκ λόγω κλοπής των δεδομένων της. Πλέον, υπάρχουν άνθρωποι που θέλουν να αντιταχθούν στους crackers και εμβαθύνουν τις γνώσεις τους στο τομέα του ethical hacking και στη συνέχεια προσλαβάνονται από εταιρίες για να διαφυλλάξουν τα δεδομένα τους .

4.1 Antivirus

Τα λογισμικά προστασίας από ιούς είναι κατηγορία προγραμμάτων που έχει σχεδιαστεί για την πρόληψη, τον εντοπισμό και την αφαίρεση μολύνσεων από κακόβουλα προγράμματα σε μεμονωμένες υπολογιστικές συσκευές, δίκτυα και συστήματα πληροφορικής. Μπορεί να προστατέψει από μια μεγάλη γκάμα απειλών, όπως τα σκουλίκια, οι Δούρειοι Ίπποι, το Spyware κα. Το λογισμικό προστασίας εκτελείται ως μια διαδικασία στο παρασκήνιο. Σαρώνει την συσκευή για τον εντοπισμό και περιορισμό της εξάπλωσης κακόβουλου λογισμικού. Πολλά λογισμικά προστασίας περιλαμβάνουν ανίχνευση και αντιμετώπιση απειλών σε πραγματικό χρόνο. Για την πλήρη σάρωση συστημάτων, το λογισμικό προστασίας από ιούς πρέπει γενικά να έχει προνομιακή πρόσβαση σε ολόκληρο το σύστημα. Αυτό καθιστά το ίδιο το λογισμικό προστασίας από ιούς κοινό στόχο για τους εισβολείς. Τέλος ερευνητές έχουν εντοπίσει σοβαρές ευπάθειες στα προιόντα λογισμικού προστασίας από τους ιούς τα τελευταία χρόνια, όπως το RCE (Remote Code Execution).

Το λογισμικό προστασίας από ιούς διανέμεται σε διάφορες μορφές, συμπεριλαμβανομένων αυτόνομων σαρωτών προστασίας από ιούς και σουίτες

ασφαλείας στο διαδίκτυο που προσφέρουν προστασία από ιούς, μαζί με τείχη προστασίας, ελέγχους απορρήτου και άλλες προστασίες ασφαλείας. [43].

4.2 Firewall

Το τείχος προστασίας είναι πρόγραμμα ασφαλείας δικτύου που παρακολουθεί την εισερχόμενη και εξερχόμενη κίνηση του δικτύου και επιτρέπει ή αποκλείει πακέτα δεδομένων βάσει ενός συνόλου κανόνων ασφαλείας. Σκοπός του είναι να δημιουργήσει ένα εμπόδιο μεταξύ του εσωτερικού σας δικτύου και της εισερχόμενης κίνησης από εξωτερικές πηγές (όπως το Διαδίκτυο), προκειμένου να αποκλείσει την κακόβουλη κίνηση, όπως ιούς και εισβολείς. Τα τείχη προστασίας αναλύουν προσεκτικά την εισερχόμενη επισκεψιμότητα με βάση προκαθορισμένους κανόνες και φιλτράρουν την επισκεψιμότητα που προέρχεται από μη ασφαλείς ή ύποπτες πηγές για την αποτροπή επιθέσεων. Τα τείχη προστασίας προστατεύουν την κυκλοφορία στο σημείο εισόδου του υπολογιστή, που ονομάζεται θύρες, όπου ανταλλάσσονται πληροφορίες με εξωτερικές συσκευές. Για παράδειγμα, "επιτρέπεται η διεύθυνση προέλευσης 172.18.1.1 να φτάσει στον προορισμό 172.18.2.1 μέσω της θύρας 22." Σκεφτείτε τις διευθύνσεις IP ως σπίτια και τους αριθμούς θύρας ως δωμάτια εντός του σπιτιού. Μόνο αξιόπιστα άτομα (διευθύνσεις προέλευσης) επιτρέπεται να εισέλθουν στο σπίτι (διεύθυνση προορισμού) καθόλου - στη συνέχεια φιλτράρεται περαιτέρω, ώστε τα άτομα εντός του σπιτιού να έχουν πρόσβαση σε συγκεκριμένα δωμάτια (θύρες προορισμού), ανάλογα με το αν είναι ο ιδιοκτήτης, παιδί ή επισκέπτης. Ο ιδιοκτήτης επιτρέπεται σε οποιοδήποτε, ενώ τα παιδιά και οι επισκέπτες επιτρέπεται σε ένα συγκεκριμένο σύνολο δωματίων. Τα τείχη προστασίας μπορεί να είναι είτε λογισμικό είτε υλικό, αν και είναι καλύτερο να έχετε και τα δύο. Ένα τείχος προστασίας λογισμικού είναι ένα πρόγραμμα εγκατεστημένο σε κάθε υπολογιστή και ρυθμίζει την κυκλοφορία μέσω αριθμών και εφαρμογών θύρας, ενώ ένα φυσικό τείχος προστασίας είναι ένα κομμάτι εξοπλισμού εγκατεστημένο μεταξύ του δικτύου και της πύλης σας. [44].

4.3 Τρόποι Προστασίας Δεδομένων.

- Ενημερωμένο λειτουργικό σύστημα με τα τελευταία patches.

- Εγκατεστημένο πρόγραμμα Firewall (Zone Alarm, Comodo). Ωστόσο, μην τρέχετε δύο τείχη προστασίας ταυτόχρονα για να αποφύγετε τις ενδεχόμενες συγκρούσεις και δυσλειτουργίες.
- Πρόγραμμα, που μοναδικός σκοπός του είναι ο συχνός καθαρισμός δεδομένων που προέρχονται από το Internet , όπως είναι τα cookies, το ιστορικό κα.
- Λογισμικό Αντικατασκοπείας το οποίο καταγράφει τις κινήσεις μας στο Διαδύκτιο και θα πρέπει να είναι συνεχώς ενημερωμένο. Επιπλέον, χρειάζεται και άλλα προγράμματα αντικατασκοπείας τα οποία θα επεμβαίνουν όταν χρειάζεται και όχι κατά την εκκίνηση (Spyware Doctor, XoftSpy, Ewido, NoAdware, SpySweeper, ScanSpyware)
- Να υπάρχει εγκατεστημένο λογισμικό προστασίας με ενεργή άδεια χρήσης και όχι δωρεάν καθώς αυτές οι εκδόσεις δεν είναι εγγυημένες και δεν προσφέρουν την ίδια ποιότητα προστασίας.
- Σωστή επιλογή παρόχου Internet μετά από μια καλή έρευνα αγοράς ως προς την ασφάλεια την ταχύτητα και την τιμή. Να προτιμάτε πιστοποιημένους παρόχους καθώς είναι πιο αξιόπιστοι ως προς την ασφάλεια.
- Για τη μεταφορά δεδομένων από μια βάση σε μια ιστοσελίδα χρησιμοποιήστε το πρωτόκολλο SSL. Αυτό το πρωτόκολλο ευθύνεται για την ασφαλή μεταφορά.
- Να αποφεύγετε την χρήση της αυτόματης συμπλήρωσης και να προτιμάτε να βάζετε μόνοι σας τα στοιχεία που απαιτούνται για ταυτοποίηση.
- Επιλέγετε να επισκέπτεστε ιστοσελίδες με το πρωτόκολλο https καθώς το s σημαίνει εγγυημένη προστασία. Να αποφεύγετε να κάνετε λήψη αρχείων από ιστοσελίδες που δεν χρησιμοποιούν αυτό το πρωτόκολλο.
- Να αποφεύγετε να εισέρχεστε σε δημόσια wifi, καθώς αν δεν είναι σωστά ρυθμισμένα τα routers, είναι ευάλωτα σε hackers.
- Ο καλύτερος τρόπος για την προστασία των δεδομένων είναι να τα αποθηκεύσετε με ασφάλεια σε άλλη τοποθεσία εκτός από το σύστημά σας. [45] [46].

Αν προσβληθείτε, υπάρχουν πολλοί δρόμοι που μπορεί να ακολουθήσει κάποιος για την αντιμετώπιση του προβλήματος, οι οποίοι εξαρτώνται από τον τρόπο και τον τύπο της μόλυνσης. Αρχικά με την βοήθεια κάποιου προγράμματος πρέπει να γίνει απομάκρυνση των προσωρινών αρχείων που προέρχονται από το Internet, καθώς συνήθως από εκεί μολύνονται οι υπολογιστές. Στη συνέχεια, θα πρέπει να γίνει ολική σάρωση του υπολογιστή με τα εργαλεία που αναφέρθηκαν παραπάνω και τέλος να απομακρυνθούν αρχεία που επηρεάζουν την εκκίνηση του υπολογιστή.

Αυτό μπορεί να γίνει από το Έναρξη – εκτέλεση – msconfig – OK. Στην καρτέλα εκκίνησης βγάλτε ότι σας φαίνεται περίεργο. Επαναλάβετε τους καθαρισμούς. Αν χρειαστεί μπείτε και σε Ασφαλή λειτουργία και επαναλάβετε και

εκεί. (Ασφαλή λειτουργία μπορείτε να μπείτε πατώντας F8 κατά την εκκίνηση των Windows και επιλέγοντας Ασφαλή λειτουργία). Στο Διαδίκτυο υπάρχει μεγάλος όγκος πληροφορίας και λύσεων για συγκεκριμένους ιούς, όταν ξέρετε το όνομά τους [45].

ΒΙΒΛΙΟΓΡΑΦΙΑ

URLs:

1. https://sites.google.com/site/efaliagka/diktio

2.http://ebooks.edu.gr/ebooks/v/html/8547/2759/Pliroforiki_A-B-G-Gymnasiou_html-empl/indexB_1_4.html

3. https://www.slideshare.net/basflor/ss-37010337

4.https://www.youtube.com/watch?v=YjNI7dur6Fg

5.https://el.wikipedia.org/wiki/%CE%94%CE%B9%CE%B1%CE%B4%CE%AF%CE%BA%CF%84%CF%85%CE%BF [5]

6.https://www.youtube.com/watch?v=uRlEXfx8nW4

7.http://edu-gate.minedu.gov.gr/index.php?option=com_sppagebuilder&view=page&id=370&Itemid=137

8.https://www.sciencedirect.com/topics/computer-science/metropolitan-area-networks

9.https://www.nexdatacenter.com/it-terminology-what-is-a-server-based-network/

10.https://www.kingston.com/en/solutions/servers-data-centers

11.https://en.wikipedia.org/wiki/Internet_backbone

12.https://coolweb.gr/diafora-internet-web/

13.https://www.youtube.com/watch?v=mVHYZKDF3hg

14. https://el.wikipedia.org/wiki/Deep_Web

15. https://www.youtube.com/watch?v=q9gz5at3Y-E

16. https://www.wlearn.gr/index.php/articles/1391-what-is-dark-web

17. https://el.wikipedia.org/wiki/Dark_Web

18.https://www.alphr.com/technology/1002667/how-to-access-the-dark-web-what-is-tor-and-how-do-i-use-it/

19.https://medium.com/@smartrac/the-deep-web-the-dark-web-and-simple-things-2e601ec980ac

20. https://sites.google.com/site/eisagogestadiktyaypologiston1/protokolla

21.https://el.wikipedia.org/wiki/%CE%9C%CE%BF%CE%BD%CF%84%CE%AD%CE%BB%CE%BF_%CE%B1%CE%BD%CE%B1%CF%86%CE%BF%CF%81%CE%AC%CF%82_OSI

22. https://www2.dmst.aueb.gr/dds/norma/internet/intro.htm

23.http://users.sch.gr/jabatzo/files/yliko/live%20ebooks/diktya_ypolog_G_2018_final/m_osi.html

24.https://el.wikipedia.org/wiki/%CE%A0%CF%81%CF%89%CF%84%CF%8C%CE%BA%CE%BF%CE%BB%CE%BB%CE%BF_%CE%9C%CE%B5%CF%84%CE%B1%CF%86%CE%BF%CF%81%CE%AC%CF%82_%CE%A5%CF%80%CE%B5%CF%81%CE%BA%CE%B5%CE%B9%CE%BC%CE%AD%CE%BD%CE%BF%CF%85

25. https://el.wikipedia.org/wiki/HTTPS

26.https://www.ip.gr/Domains/%CE%A4%CE%B9_%CE%B5%CE%AF%CE%BD%CE%B1%CE%B9_%CF%84%CE%BF_DNS-2.html

27. https://el.wikipedia.org/wiki/UDP

28.https://el.wikipedia.org/wiki/%CE%A0%CF%81%CF%89%CF%84%CF%8C%CE%BA%CE%BF%CE%BB%CE%BB%CE%BF_%CE%94%CE%B9%CE%B1%CE%B4%CE%B9%CE%BA%CF%84%CF%8D%CE%BF%CF%85

29.https://www.dpa.gr/pls/portal/docs/PAGE/APDPX/YOUTH/YOUTH_INTRO/YOUTH_BOOKLET.PDF

30. http://1ogelasaferinternet.weebly.com/hackers.html

31.https://el.wikipedia.org/wiki/%CE%A7%CE%AC%CE%BA%CE%B5%CF%81

32.https://www.safer-internet.gr/%CF%84%CE%B9-%CF%83%CE%B7%CE%BC%CE%B1%CE%AF%CE%BD%CE%B5%CE%B9-hacker-%CF%84%CE%B9-%CE%B5%CE%AF%CE%BD%CE%B1%CE%B9-%CF%84%CE%BF-hack-ing/

33. https://www.sigmaweb.gr/hackers-motivation/

34.https://www.in2life.gr/features/notes/article/212308/hackers-oi-theamatikoteres-epitheseis-olon-ton-epohon.html

35.https://kedisa.gr/%CE%BF-%CE%B9%CF%8C%CF%82-stuxnet-%CE%BA%CE%B1%CE%B9-%CF%84%CE%BF-%CF%80%CF%85%CF%81%CE%B7%CE%BD%CE%B9%CE%BA%CF%8C-%CF%80%CF%81%CF%8C%CE%B3%CF%81%CE%B1%CE%BC%CE%BC%CE%B1-%CF%84%CE%BF%CF%85-%CE%B9/

36.https://www.google.com/search?sxsrf=ALeKk02XI7nErRDTTROG1FeY-ClWP7JztQ%3A1605385587903&ei=cz2wX_TUNqv2kgXa4q3oBQ&q=flame+virus&oq=flame+virus&gs_lcp=CgZwc3ktYWIQAzIFCAAQywEyBQgAEMsBMgYIABAWEB4yBggAEBYQHjIGCAAQFhAeMgYIABAWEB4yBggAEBYQHjIGCAAQFhAeMgYIABAWEB46BAgjECc6AggAOgIIJjoECAAQQzoICAAQsQMQgwE6BQgAELEDOgYIIxAnEBM6BwgjEOoCECc6BAgAEEM6BQguELEDOggILhCxAxCDAToCCC46BwgAELEDEM6BQguEMsBOggILhDLARCTAlDoO1ia6AFg4-sBaBpwAHgAgAGZAogBkh6SAQYwLjIwLjOYAQCgAQGqAQdnd3Mtd2l6sAEKwAEB&sclient=psy-ab&ved=0ahUKEwi02sat74LtAhUru6QKHVpxC10Q4dUDCA0&uact=5

37.https://www.secnews.gr/204873/hacking-kai-kyvernokataskopeia-oi-chores-pou-anamenetai-na-apotelesoun-apeili-to-2020/

38.https://www.youtube.com/watch?v=R0BX58IK_IM

39. https://cybermap.kaspersky.com/

40. https://www.eset.com/gr/malware/

41.https://el.wikipedia.org/wiki/%CE%9A%CE%B1%CE%BA%CF%8C%CE%B2%CE%BF%CF%85%CE%BB%CE%BF_%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CE%BC%CE%B9%CE%BA%CF%8C

42.https://sites.google.com/site/bkasiolas/asphaleia-ypologistikou-systematos/kakoboulo-logismiko

43.https://el.wikipedia.org/wiki/%CE%91%CE%BD%CF%84%CE%B9%CE%B9%CE%B9%CE%BA%CF%8C_%CF%80%CF%81%CF%8C%CE%B3%CF%81%CE%B1%CE%BC%CE%BC%CE%B1

44.https://el.wikipedia.org/wiki/Firewall

45.http://greekmoney.gr/%CF%84%CF%81%CF%8C%CF%80%CE%BF%CE%B9-%CF%80%CF%81%CE%BF%CF%83%CF%84%CE%B1%CF%83%CE%AF%CE%B1%CF%82-%CE%B1%CF%80%CF%8C-%CE%BA%CE%B1%CE%BA%CF%8C%CE%B2%CE%BF%CF%85%CE%BB%CE%B1-%CE%BB%CE%BF%CE%B3%CE%B9/

46.https://www.secnews.gr/207322/10-tropoi-prostatepsete-data-hackers/