ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΔΥΤΙΚΗΣ ΕΛΛΑΔΑΣ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

Η σκοτεινή Πλευρά του Διαδικτύου

The Dark Side of Internet

Πτυχιακή Εργασία των :

Αλέξανδρος Γάλλος (ΑΜ: 11359)

Βασιλική Κεφαλά (ΑΜ: 12586)

Γιώργος Σισμανίδης (ΑΜ: 12559)

Επιβλέπων καθηγητής: Δρ. Ηλίας Κ. Σταυρόπουλος

ΠΑΤΡΑ, Ιούνιος 2015

Περίληψη

Στις μέρες μας, η τεχνολογία του Διαδικτύου έχει ραγδαία εξέλιξη υποθέτοντας έναν ιδανικό κόσμο όπου όλοι οι χρήστες να είναι έντιμοι χωρίς να ενεργούν εις βάρος των άλλων χρηστών, για το δικό τους συμφέρον. Ωστόσο, πλέον η σκοτεινή πλευρά του Διαδικτύου έχει πάρει μεγάλη έκταση και ταλαιπωρεί τους χρήστες. Αυτό περιλαμβάνει το spam, malware (κακόβουλο λογισμικό), hacking, phising, επιθέσεις άρνησης υπηρεσίας, παραβίαση της ιδιωτικής ζωής, απάτες κλπ.

Αντίθετα, διάφορες τεχνολογίες, νομοθεσίες και με την προσπάθεια ευαισθητοποίησης του κοινού προσπαθούν να εξαλείψουν το φαινόμενο αυτό. Επίσης, προσπαθούν να ταξινομήσουν τα αίτια που αναγκάζουν τους χρήστες να μεταχειρίζονται αρνητικά τις παροχές του Διαδικτύου, όπως και τα κόστη των επιθέσεων μετά από τις ηλεκτρονικές απάτες των χρηστών του.

Απώτερη επιδίωξη, είναι αυτή η εργασία να αποτελέσει ένα κίνητρο για να ευαισθητοποιήσει τους χρήστες στην νόμιμη χρήση του Διαδικτύου.

Περιεχόμενα

Ευχαριστίες

Αισθανόμαστε την ανάγκη να ευχαριστήσουμε θερμά τον συνεργάτη καθηγητή και επιβλέποντα της πτυχιακής μας κ.Ηλία Σταυρόπουλο, για την βοήθεια και την στήριξή του αυτούς τους μήνες. Η καθοδήγησή του από την αρχή και το υλικό που μας δόθηκε ήταν πολύτιμο για την ολοκλήρωση της πτυχιακή μας.

Εισαγωγή

Τα τελευταία χρόνια ζούμε σε μια μεγάλη επανάσταση που επικρατεί στο χώρο του διαδικτυακού κόσμου. Κατά την επανάσταση αυτή μπορούμε να πούμε ότι γίνεται διαχωρισμός αυτής σε τρεις κατηγορίες: την καλή την κακή και την άσχημη. Η κάθε κατηγορία περιλαμβάνει ξεχωριστές ικανότητες που δραστηριοποιούνται οι χρήστες. Στην καλή πλευρά του διαδικτύου υπάρχουν όλα τα οφέλη που μπορεί να λάβει ένας νόμιμος χρήστης. Οφέλη όπως είναι να διασκεδάζουν, να μεταφέρουν αρχεία, να επικοινωνούν με ανθρώπους μειώνοντας αποστάσεις και κόστος καθώς και να εκπαιδεύονται κ.α.

Στην κακή πλευρά του διαδικτύου τώρα, υπάρχουν δραστηριότητες που μπορούν να βλάψουν τον άνθρωπο, κάποια επιχείρηση, ιδρύματα ακόμα και την ιδία την κυβέρνηση. Η άσχημη πλευρά είναι παρόμοια με την κακή καθώς περιέχει παράνομες δραστηριότητες που δεν καλύπτονται από τον νόμο. Δραστηριότητες όπως είναι για παράδειγμα το ηλεκτρονικό έγκλημα, η ηλεκτρονική απάτη σε λογαριασμούς, τα ηλεκτρονικά στοιχηματικά παίγνια καθώς και η ηλεκτρονική βία Σε αυτή την εργασία θα εξευρενήσουμε τη σκοτεινή πλεύρα του Διαδικτύου, δηλαδή όλα τα άσχημα πράγματα που έχει επιφέρει τόσο στον διαδικτυακο κόσμο όσο και στον πραγματικό. Η σκοτεινή πλευρά αυτών των δύο κόσμων είναι συνέπεια των ανθρώπων για διάφορους λόγους και επιθυμίες όπως οικονομικά οφέλη, ζήλεια, ανασφάλεια κ.λπ. Όλα τα στοιχεία της σκοτεινής πλευράς του διαδικτύου είναι παράνομα, ανήθικα και κατακριτέα. Η παγκόσμια εμβέλεια, η ταχύτητα διάδοσης, η ανωνυμία και η έλλειψη κατάλληλων νομοθετικών ή διεθνών συμφωνιών έχουν γίνει λόγοι για να τη δυσκολία δίωξης τέτοιων ανθρώπων που ενεργούν παράνομα. Στην σκοτεινή πλευρά του διαδικτύου θα πρέπει να υπάρξει ευαισθητοποίηση και προσοχή από τους χρήστες για το πως το διαχειρίζονται αλλά και η κατάλληλη προστασία και ασφάλεια από τον συγκεκριμένο χώρο. Επίσης, οι κατάλληλες νομοθεσίες και οι απαραίτητες διώξεις σε όποιον κάνει παράνομη χρήση του ώστε να περιοριστεί αυτό το «φαινόμενο».

Έχουν γραφτεί πολλά σχετικά με ορισμένα στοιχεία της σκοτεινής πλευράς του διαδικτύου. Ελπίζουμε ότι αυτή η εργασία θα γίνει μια από τις εκτενείς αναφορές για το θέμα της σκοτεινής πλευράς του διαδικτύου. Η εργασία παρέχει μια ευρεία κάλυψη του θέματος συμπεριλαμβανομένων των στοιχείων της σκοτεινής πλευράς,

τα είδη των ζημιών, τους τρόπους αντιμετώπισης και πρόληψης. Η εργασία είναι οργανωμένη ως εξής: Η ενότητα 1 περιγράφει την σκοτεινή πλευρά του διαδικτύου καθώς και τις ζημιές που γίνονται από ανθρώπους οι οποίοι κάνουν κατάχρηση του διαδικτύου. Η ενότητα 2 εξετάζει τα αίτια της σκοτεινής πλευράς. Η ενότητα 3 περιγράφει τις κύριες τεχνολογίες της σκοτεινής πλευράς. Η ενότητα 4 έχει να κάνει με την νομοθεσία και τους τρόπους πρόληψης κατά της σκοτεινής πλευράς του διαδικτύου. Η ενότητα 5 αναφέρεται στις επιθέσεις που έχουν πραγματοποιηθεί στον ελληνικό χώρο του διαδικτύου. Για την εκπόνηση της πτυχιακής εργασίας βασιστήκαμε στο άρθρο The dark side of internet από τους συγγραφείς Won Kim, Ok-Ran Jeong, Chulyun Kim, Jungmin So.

ΚΕΦΑΛΑΙΟ 1 Η σκοτεινή πλευρά

Σε εκατομμύρια χρήστες του διαδικτύου έχει παραβιαστεί η προστασία της ιδιωτικής τους ζωής,η σωματική τους βλάβη,έχουν χάσει πολλά χρήματα και έχει δυσφημιστεί η προσωπικότητά τους. Ο διαδικτυακός εκφοβισμός είναι άλλη μία κύρια αιτία της ψυχικής οδύνης που νοιώθουν οι χρήστες αφού έχει αυξηθεί η εγκληματική αυτουργίαν, η οποία χωρίζεται σε δύο κατηγορίες, στα είδη των ζημιών και στην ταξινόμηση της σκοτεινής πλευράς του διαδικτύου. Η σκοτεινή πλευρά μπορεί να χωρίζεται σε δύο ομάδες: τεχνολογίας και μη τεχνολογίας. Τα είδη των ζημίων που προκλήθηκαν από τη σκοτεινή πλευρά θα είναι τα εξής:

1. Απώλεια χρημάτων: από κλοπή των ταμείων.
2. Δυσφήμιση: προκαλείται από τη διάδοση ψευδών πληροφοριών.
3. Παραβίαση της ιδιωτικής ζωής: προκαλείται από τη διάδοση των ιδιωτικών πληροφοριών και προσωπικών δεδομένων.
4. Σωματική βλάβη: να πέσουν θύματα παιδεραστών,να πέσουν θύματα στη πορνεία όπως και αυτοκτονίες παιδιών που τους επηρεάζουν μέσω του διαδικτύου
5. Χάσιμο χρόνου: για την εγκατάσταση και τη διαχείριση αμυντικής τεχνολογίας και για τη νομική δράση για να ζητηθούν επιστροφή τα περισσότερα είδη των ζημιών.
6. Ψυχική οδύνη ή ψυχολογική βλάβη: προκαλείται από τον εκφοβισμό στον κυβερνοχώρο .
7. Αύξηση της εγκληματικότητας: προκαλείται από πληροφορίες εγκληματικής αυτουργίας που δημοσιεύτηκαν στο διαδίκτυο.

Η ομάδα της κύριας τεχνολογίας αποτελείται από επτά στοιχεία:

1. Spam
2. malware (κακόβουλο λογισμικό)
3. hacking
4. επίθεση άρνησης υπηρεσιών
5. phishing
6. click fraud(ψευδοκλίκ)
7. Παραβίαση των ψηφιακών δικαιωμάτων ιδιοκτησίας

Η ομάδα της μη κύριας τεχνολογίας αποτελείται από οχτώ στοιχεία:

1. Συνδεδεμένη κλοπή
2. Διαδικτυακές απάτες
3. Σωματική βλάβη
4. Cyber εκφοβισμός
5. Διάδοση ψευδών ή ιδιωτικές πληροφορίες
6. Παράνομα online τυχερά παιχνίδια
7. Υποβοήθηση του εγκλήματος
8. Άλλες καταδικαστέες συμπεριφορές

Συνοψίζοντας, μέσα από το χώρο του διαδικτύου διαπιστώνουμε ότι αυτό που πιστεύουμε ως «η σκοτεινή πλευρά του διαδικτύου» είναι πολύ πιο κοντά στους χρήστες από οτι νομίζαμε.[1]

1.1. Κλοπή στο διαδίκτυο

Στο χώρο του διαδικτύου υπάρχουν κρούσματα για online κλοπή των ηλεκτρονικών δεδομένων, ταυτότητας και ψηφιακών ιδιοτήτων. Η κλοπή δεδομένων αναφέρεται στην κλοπή όπως αριθμών πιστωτικών και χρεωστικών καρτών, ονόματα χρήστη, κωδικούς πρόσβασης στοιχεία λογαριασμών,προσωπικά προφίλ κ.λ.π. Η κλοπή των δεδομένων μπορεί να δεσμευτεί μέσω διάφορα offline μέσα, όπως πακέτων sniffing, τηλεφωνική υποκλοπή, hacking, phishingκαι με τη χρήση του κακόβουλου λογισμικού. Η κλοπή ταυτότητας αναφέρεται στην κλοπή των λεπτομερών δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων των αριθμών κοινωνικής ασφάλισης (για τους πολίτες των Η.Π.Α και των κατοίκων) ή αριθμοί διαβατηρίου, πιστοποιητικά γεννήσεως, φορολογικά μητρώα κ.λπ. Όλα αυτά διαπράττονται σε μεγαλό βαθμό για οικονομικά οφέλη με την απόσυρση των τραπεζικών καταθέσεων του θύματος και τη χρέωση των πιστωτικών καρτών. Για τα θύματα, είναι δύσκολη και χρονοβόρα διαδικασία για να ανακαλύψουν τον υπαίτιο για τις επιπτώσεις της κλοπής.

Από το Κέντρο Πληροφόρησης (http://www.idtheftcenter.org) οι εκτιμήσεις είναι ότι κατά μέσο όρο χρειάζονται περίπου 330 ώρες για ένα θύμα να ακυρώσει τις οικονομικές του υποχρεώσεις και τα ποινικά μητρώα, που είχαν συσσωρευτεί από τους κλέφτες. Θα ήταν χρήσιμο να αναφερθεί ότι τα αρχεία φυλάσσονται από την αστυνομία. Το έτος 2008 στις Ηνωμένες Πολιτείες υπήρχαν 9,9 εκατομμύρια θύματα σε αντίθεση με το έτος 2007 όπου ήταν 8,1 εκατομμύρια. Τα κακόβουλα λογισμικά έχουν πολλαπλασιαστεί και οι εταιρείες antivirus έχουν αγωνιστεί για να εντοπίσουν κάθε νέα επίθεση. Επίσης, ένα προϊόν από την εταιρεία λογισμικού ασφαλείας Authentium προστατεύει τους χρήστες ακόμη και αν υπάρχει κακόβουλο λογισμικό στον υπόλογιστη. Περιλαμβάνει απογυμνωμένα και ασφαλή browser για τη συναλλαγή και διαπραγμάτευση μετόχων ή προβολή πληροφοριών σε απευθείας σύνδεση. Τέλος, μία άλλη εναλλακτική είναι να αποφευχθεί η ανταλλαγή πληροφοριών σε απευθείας σύνδεση. Η kemesa, είναι μία εταιρεία λογισμικού, που έχει δημιουργήσει ένα προϊόν για online παραγγελίες με την ασφάλεια που ονομάζεται κατάστημα ασπίδα, η οποία ξεκινά με μια οικεία browser-based, εργαλείο για τη διαχείριση των κωδικών και αυτόματη συμπλήρωση εντύπων web, που βοηθά στην προστασία του από τα keyloggers (η οποία μπορεί να καταγράψει κάθε πληκτρολόγηση που γίνεται) [1]

1.2. Απάτη στο διαδίκτυο

Ηλεκτρονικές απάτες είναι παιχνίδια εμπιστοσύνης που έχουν ως στόχο να ξεγελάσουν τους χρήστες ότι θα λάβουν χρήματα ή κάποιο δώρο και στο τέλος να μην λαμβάνουν τίποτα. Έτσι, γίνεται και στον offline κόσμο, υπάρχουν πολλοί απαταώνες που ξεγελάνε τους χρήστες. Η απάτη του διαδικτύου μπορεί να συμβεί σε chatrooms, email, message boards ή και σε διάφορες ιστοσελίδες πώλησης προϊόντος. Η πιο συνηθισμένη σε απάτη τελείται με τη χρήση πιστωτικών καρτών, που αποσύρουν τα χρήματα από το θύμα-χρήστη π.χ μέσω Paypal. Για παράδειγμα, τύποι σε απευθείας σύνδεσης είναι σε αγορές αυτοκινήτων, μεταφορών χρημάτων, επενδύσεων και στον τομέα της λιανικής. Σύμφωνα με το μάρκετινγκ στο διαδίκτυο και της λιανικής απάτης, το θύμα παρασύρεται ώστε να δώσει τα στοιχεία της πιστωτικής κάρτας ή την αποστολή μετρητών, σε αντάλλαγμα τα αγαθά ή τις υπηρεσίες στις οποίες έχουν συμφωνήσει. Τα προϊόντα δεν φτάνουν ποτέ, αποδεικνύεται ότι η αξία του προϊόντιος ήταν πολύ πιο χαμηλή και ένα κοινό παράδειγμα αυτού του τύπου απάτης είναι οι πορνογραφικές ιστοσελίδες που διαφημίζουν δωρεάν πρόσβαση αλλά απαιτούν στοιχεία των πιστωτικών καρτών «για τους σκοπούς της επαλήθευσης της ηλικίας μόνο». Ο απατεώνας κάνει μεγάλες επιβαρύνσεις στη πιστωτική κάρτα όπως και μέσω των τηλεμάρκετινγκ (cramming) που τις χρεώνει ή στον τραπεζικό λογαριασμό ή στο λογαριασμό του τηλεφώνου. Ο απατεώνας συλλαμβάνει τον αριθμό τηλεφώνου του καταναλωτή, χρησιμοποιώντας την αυτόματη αναγνώριση αριθμού, ένα σύστημα παρόμοιο με αναγνώριση κλήσης. Στη συνέχεια, δελεάζοντας τον καταναλώτη να κάνει τις κλήσεις, προκαλώντας του επιβαρύνσεις για ένα προϊόν ή μια υπηρεσία που θα περιλαμβάνονται στο λογαριασμό του τηλεφώνου του εν λόγω προσώπου. Το 1998 ήταν το νούμερο ένα η απάτη μέσω του τηλεμάρκετινγκ. Οι απατεώνες έχουν βρεί το τηλέφωνο χρέωσης να είναι μια εύφορη περιοχή με σκοπό την εξαπάτηση των καταναλωτών. Μερικές φορές, η χρέωση μπορεί να είναι σε ένα λογαριασμό του τηλεφώνου για κάποια υπηρεσία που χρησιμοποίησε ο καταναλωτής. Άλλες φορές μπορεί να είναι μία επαναλαμβανόμενη μηνιαία χρέωση. Οι χρεώσεις αυτές χωρίζονται σε δύο γενικές κατηγορίες:

1. Την ιδιότητα μέλους σε σύλλογο, όπως ψυχικές λέσχες, ταξιδιωτικών συλλόγων,τηλεπικοινωνιών προϊόντων.

2. Προγράμματα παροχής υπηρεσιών, όπως το φωνητικό ταχυδρομείο, τηλεκάρτες.

Οι χρεώσεις ακριβώς εμφανίζονται στο λογαριασμό του τηλεφώνου του καταναλωτή ως επιβάρυνση συνήθως ως υπεραστική κλήση. Οι άνθρωποι που λαμβάνουν αυτους τους λογαριασμούς δεν έχουν καμία δυνατότητα να γνωρίζουν ότι τα τέλη είναι στην πραγματικότητα για μία γραμμή (ρόζ υποστήριξης τηλεπώλησης) π.χ. ο αριθμός κλήσης 900. Επιπλέον βρίσκουν τον αριθμό του τηλεφώνου του κάθε καταναλωτή και με ένα σύστημα (ANI-σύστημα παρόμοιο με αναγνώρισης κλήσης) και με το που απαντήσουν στην κλήση χρεώνονται. Για παράδειγμα, ο αριθμός κλήσεων 800 είναι γραμμή που προσφέρει διάφορες υπηρεσίες ψυχαγωγίας και υποστηρίζεται ως ελεύθερη γραμμή. Ένα ηχογραφημένο μήνυμα ζητά να δώσουν το όνομα του καταναλωτή και να πεί ποιά υπηρεσία θέλει και αυτομάτως εγγράφονται στο συγκεκριμένο πρόγραμμα ή υπηρεσία όπως και οι αριθμοί που αρχίζουν από το 011ή 500.[2] [1]

1.3. Σωματική βλάβη σε ανθρώπους

Υπάρχουν διάφοροι τρόποι με τους οποίους η χρήση ή κατάχρηση του Διαδικτύου μπορεί να οδηγήσει σε σωματική βλάβη σε ανθρώπους. Υπάρχουν ιστοσελίδες αυτοκτονίας που ενθαρρύνουν τα μέλη να πάρουν μέρος μαζί για να αυτοκτονήσουν. Στη Νότια Κορέα, κατά τη διάρκεια των τελευταίων ετών, υπήρξαν αρκετές αναφορές για δύο ή τρία άτομα που συνεδρίασαν στις ιστοσελίδες αυτοκτονίας και αυτοκτόνησαν μαζί. Πολλοί άνθρωποι έχουν ενταχθεί σε ιστοσελίδες κοινωνικής δικτύωσης στο Διαδίκτυο για να κυνηγήσουν θύματα του σεξ. Αυτά περιλαμβάνουν παιδική πορνογραφία, παιδεραστές, και έμποροι του σεξ που παρασύρουν τα παιδιά στην πορνεία, κλπ., Ο αριθμός των ατόμων αυτών είναι απίστευτα υψηλός. Μετά την παρέμβαση από την κυβέρνηση, το site κοινωνικής δικτύωσης MySpace έπρεπε να παραδώσει κατάλογο των μελών που έχουν καταδικαστεί για σεξουαλικά αδικήματα. Ο κατάλογος περιείχε 90.000 μέλη. Δεν είναι γνωστό πόσοι παραβάτες του σεξ δεν χρησιμοποιούν το πραγματικό τους όνομα στο MySpace. Εκφράζονται φόβοι ότι πολλοί από αυτούς τους ανθρώπους μπορεί να είναι ύποπτοι για τα νέα μέλη του MySpace. Στις 4 Φεβρουαρίου 2009 στη New York Times, η Jenna Wortham ανακάλυψε 90.000

μέλη που ήταν εγγεγραμένοι δράστες σεξουαλικών εγκλημάτων. Το 12% των ιστοσελίδων έχουν ή διακινούν πορνογραφικό υλικό.

Έρευνες σε παιδιά ευρωπαϊκων χωρών διαπιστώθηκε ότι έρχονται σε επαφή με πορνογραφικό υλικό σε ηλικία 11 χρονών, ενώ περίπου το 35% εκτίθεται χωρίς τη θέληση τους σε εικόνες και σε βίντεο πορνογραφικού υλικού. Πρόκειται,για μία βιομηχανία η οποία βγάζει το δευτερόλεπτο περίπου 3.000$ ετησίως κέρδη που ξεπερνούν μεγάλες εταιρείες όπως της Google ή της Microsoft. Σύμφωνα με έρευνα της Αμερικής, 200 εικόνες παιδικής πορνογραφίας ταχυδρονομούνται καθημερινά και 1 στα 7 παιδιά έχει υποστεί σεξουαλική διαδικτυακή παρενόχληση. Τέλος θα ήταν χρήσιμο να αναφερθεί, ότι ένα 35% των παραβατών είναι γονείς κακοποιημένων παιδιών, ενώ το 10% απαρτίζεται από άλλα συγγενικά πρόσωπα. [1] [3] [4]

1.4. Εκφοβισμός

Ο Διαδικτυακός εκφοβισμός πληγώνει ή φέρνει σε δύσκολη θέση το άλλο άτομο που χρησιμοποιεί το Διαδίκτυο, τα κινητά τηλέφωνα ή άλλες συσκευές με την αποστολή ή τη δημοσίευση κειμένων ή εικόνων. Ο ηλεκτρονικός εκφοβισμός ορίζεται σε νομικά γλωσσάρια ως δράσεις που χρησιμοποιούν τις τεχνολογίες της πληροφορίας και της επικοινωνίας για την υποστήριξη της σκόπιμης επαναλαμβανόμενης και εχθρικής συμπεριφοράς από ένα άτομο ή ομάδα, που έχει ως στόχο να βλάψει άλλον ή άλλους. Χρήση των τεχνολογιών επικοινωνίας όπως των υπηρεσίων του διαδικτύου, των κινητών τεχνολογιών, ιστοσελίδες με ομαδικές συζητήσεις (ανταλλαγή άμεσων μηνυμάτων) που έχουν ως στόχο να βλάψουν το άλλο πρόσωπο. Ο ηλεκτρονικός εκφοβισμός περιλαμβάνει ανακοινώσεις που επιδιώκουν να εκφοβίσουν, να δυσφημίσουν ή να ταπεινώσουν τον παραλήπτη με εχθρική συμπεριφορά. Η πρακτική του εκφοβισμού στον κυβερνοχώρο δεν περιορίζεται μόνο στα παιδιά αλλά και στους ενήλικες σε διάφορα δημόσια φόρουμ κοινωνικών μέσων μαζικής ενημέρωσης. Οι συμπεριφορές που χρησιμοποιούν είναι είτε να ενθαρρύνουν ή να παρενοχλήσουν το θύμα με διάφορους προσβλητικούς τρόπους όπως ψευδείς κατηγορίες. Αυτά τα άτομα τα παρακολουθεί η δίωξη ηλεκτρονικού εγκλήματος και καταφεύγει στη δίωξη αυτών των ατόμων. Χρησιμοποιούν ψευδώνυμαστα chatrooms, προγράμματα

ανταλλαγής, προσωρινούς λογαριασμούς, άμεσων μηνυμάτων και άλλους χώρους του Διαδικτύου για να συγκαλύψουν την ταυτότητά τους.

Ένα πιθανό πλεονέκτημα για τα θύματα διαδικτυακού εκφοβισμού έναντι του εκφοβισμού είναι ότι μερικές φορές μπορεί να είναι σε θέση να το αποφύγει απλά αποφεύγοντας το site-δωμάτιο συνομιλίας. Επιπλέον, οι περισσότεροι λογαριασμοί ηλεκτρονικού ταχυδρομείου προσφέρουν υπηρεσίες φιλτραρίσματος μηνυμάτων από τους αποστολείς πριν καν φτάσουν στα εισερχόμενα. Επίσης τα τηλέφωνα προσφέρουν παρόμοιες λειτουργίες ταυτότητας του καλούντος. Μερικοί δράστες μπορούν να δημοσιεύουν επεξεργασμένες φωτογραφίες θυμάτων ή επικόλληση προσώπων σε γυμνά σώματα, πλαστοπροσωπία και του σκόπιμου αποκλεισμού από μία online ομάδα.

Επιπλέον, ο χρήστης μπορεί να συνεχίζει τον εκφοβισμό στέλνοντας απειλητικά μηνύματα στο θύμα, σεξουαλικές παρενοχλήσεις, να πείθει τους άλλους ώστε να αντιπαθήσουν το θύμα και να συμμετάσχουν και αυτοί σε online δυσφήμηση, όπως και σε υποτιμητικούς χαρακτηρισμούς ενώ έχει δηλώσει ότι δεν θέλει καμία επαφή με τον αποστολέα. Συνήθως αυτό το φαινόμενο το συναντάμε σε ιστοσελίδες κοινωνικής δικτύωσης όπως το Facebook και το Twitter. Μέχρι το 2008, το 93% των νέων ηλικίας μεταξύ 12 και 17 χρόνων ήταν σε απευθείας σύνδεση. Στην πραγματικότητα, οι νέοι περνούν περισσότερο χρόνο με τα μέσα ενημέρωσης από ότι οποιαδήποτε άλλη μεμονωμένη δραστηριότητα. Υπάρχουν πολλοί κίνδυνοι που συνδέονται με δικτυακούς τόπους κοινωνικής ενημέρωσης και ο ηλεκτρονικός εκφοβισμός είναι ένα από τους μεγαλύτερους κινδύνους. Ένα εκατομμύριο παιδιά υπέστησαν παρενοχλήσεις, απειλές ή υποβλήθηκαν σε άλλες μορφές του ψηφιακού εκφοβισμού στο Facebook κατά τη διάρκεια του περασμένου έτους ενώ το 90% των κοινωνικών μέσων μαζικής ενημέρωσης που χρησιμοποιούν οι έφηβοι έχουν γίνει μάρτυρες σε απευθείας σύνδεση αυτού του φαινομένου και το αγνοούν. Ενώ το 35% το έχουν πράξει. Η πιο πρόσφατη περίπτωση της παρενόχλησης στον κυβερνοχώρο και της παράνομης δραστηριότητας στο Facebook περιελάμβανε σελίδες για τα νεαρά αγόρια που έχασαν τη ζωή τους αυτοκτονώντας λόγω του αντι-γκέι εκφοβισμού. Υπάρχουν σελίδες με διάφορα σχόλια για την ενθάρρυνση των γκέι εφήβων στην αυτοκτονία ή απειλές για την σωματική τους ακεραιότητα.

Παράλληλα, η ασφάλεια των σχολείων είναι όλο και περισσότερο στο επίκεντρο της κρατικής νομοθετικής δράσης. Το 2012, μια ομάδα των εφήβων στο New Haven, Connecticut ανέπτυξε μια εφαρμογή για να βοηθήσει στην καταπολέμηση του εκφοβισμού που ονομάζεται "Back Off Bully" (BOB). Το web app είναι μια ανώνυμη πηγή για τον υπολογιστή ή για το iPad και όταν κάποιο άτομο είναι θύμα εκφοβισμού, μπορεί να το αναφέρει αμέσως το περιστατικό και η εφαρμογή θέτει ερωτήματα σχετικά με την ώρα, την τοποθεσία κ.α. Ακόμη, υπάρχουν συμβουλευτικές τηλεφωνικές γραμμές που βοηθάνε τα θύματα του εκφοβισμού και τα άτομα που το διαπράττουν να έχουν ποινικές συνέπειες. Μία καναδική μελέτη διαπίστωσε:

1. Το 23% της μέσης σχολικής ηλικίας των ερωτηθέντων είχαν υποστεί εκφοβισμό μέσω e-mail.
2. Το 35% σε chat rooms.
3. Το 41% από τα μηνύματα κειμένου στα κινητά τηλέφωνα τους.
4. Πλήρως το 41% δεν γνώριζαν την ταυτότητα των δραστών.

Ο Διαδικτυακός εκφοβισμός, δημιουργεί στα θύματα κατάθλιψη, χαμηλή αυτοεκτίμηση, απροθυμία να συμμετάσχουν σε ομαδικές δραστηριότητες κλπ. Συγκεκριμένα, το 2008 ψευδείς φήμες στο Διαδίκτυο στη Νότια Κορέα οδήγησε διάσημη ηθοποιό να αυτοκτονήσει. Θα ήταν χρήσιμο να αναφερθεί ότι πολύ συχνό φαινόμενο είναι και στα σχολεία, μεταξύ των παιδιών που έχουν οδηγηθεί και αυτά σε αυτοκτονίες. [1] [5]

1.5. Δυσφήμιση και προβολή ιδιωτικής ζωής

Το Διαδίκτυο μπορεί να ενισχύσει σε μεγάλο βαθμό τις ευκαιρίες για δυσφήμιση και παραβίαση της ιδιωτικής ζωής για τα άτομα και τους οργανισμούς. Πρώτον, λόγω της παγκόσμιας εμβέλειας και της ταχύτητας διάδοσης των πληροφοριών, δεύτερον οι μεγάλες εταιρείες του διαδικτύου που βασίζονται σε συλλογή δεδομένων από ανθρώπους και τρίτον από την υποκλοπή σημαντικών δεδομένων από τους χάκερς. Υπάρχουν άτομα που συμμετέχουν σε ιστότοπους κοινωνικής δικτύωσης και μοιράζονται όλες τις λεπτομέρειες της καθημερινότητας τους ή απλά κάνουν χρήση σε αυτούς τους ιστότοπους όπως πχ. το Facebook για να δελεάσουν μικρά παιδιά στο σεξ ή κάνοντας check in μέσω του κινητού,

δείχνοντας ακριβώς τη τοποθεσία που είναι ο κάθε χρήστης. Επιπλέον, η Google περιλαμβάνει τη λειτουργία StreetView στην υπηρεσία Google Maps, που δείχνει τις εικόνες των δρόμων, τα σπίτια, τα κτίρια, τα αυτοκίνητα ακόμα και τους ανθρώπους στους δρόμους. Μερικά από τα δευτερεύοντα πλευρικά οφέλη είναι ότι με αυτό το σύστημα μπορούν να εντοπίζουν τους ληστές ή διάφορες εγκληματικές ενέργειες. Ωστόσο, το StreetView έχει προκαλέσει ανησυχίες για την προστασία της ιδιωτικής ζωής του ανθρώπου σε όλο τον κόσμο. Τέσσερα στελέχη της Google είχαν παρεπεμφθεί στην Ιταλία για ποινικές διώξεις για δυσφήμιση και παραβίαση της ιδιωτικής ζωής, διότι θεωρήθηκαν υπεύθυνοι για 3 λεπτών βίντεο που αναρτήθηκε δείχνοντας κάποιους νέους να εκφοβίζουν ένα παιδί με σύνδρομο Down. Το θέμα αυτό έχει καταλήξει στις Ηνωμένες Πολιτείες για την δίωξη των πνευματικών δικαιωμάτων που έχει ως σκοπό να προστατεύσει online υπηρεσίες. [1]

1.6. Στοχευμένα εγκλήματα

Μέσα στο διαδίκτυο, υπάρχουν πολλές πληροφορίες είτε αληθινές είτε ψευδείς και αλλότε καλές ή εις βάρος του χρήστη. Πολλές τεχνικές αποσκοπούν σε πράξεις που παραβαίνουν το νόμο ή την εξάπλωση κακόβουλου λογισμικού ή ιού. Πολλοί χρήστες του διαδικτύου παίρνοντας αυτές τις πληροφορίες ενεργούν εγκληματικά όπως: να φτιάχνουν τα ναρκωτικά, τρόποι παραβίασης σπιτιών ή τρόποι αυτοκτονίας. Αυτά τα φαινόμενα έχουν εξαπλωθεί αρκετά και έτσι πλέον το Διαδίκτυο δεν είναι και τόσο ασφαλές, διότι οι χρήστες παρασύρονται και ωθούνται σε εγκληματικές πράξεις. [1]

1.7. Παράνομα τυχερά παιχνίδια στο διαδίκτυο

Ο τζόγος στο διαδίκτυο στις ΗΠΑ έχει 29.300.000.000 δολλάρια συνολικά έσοδα σε επιχειρήσεις το 2010, εκ των οποίων το μερίδιο της Ευρώπης είναι 12.5 δισεκατομμύρια από online ιστοσελίδες τυχερών παιχνιδιών. Οι επιχειρήσεις για να αποφύγουν τη υψηλή φορολογία από τα παράνομα παιχνίδια λειτουργούν σε χώρους όπως η Κόστα Ρίκα, Αντίκουα κλπ. Επίσης, χρησιμοποιώντας ένα μεγάλο ποσό χρημάτων πίεσαν τις Ηνωμένες Πολιτείες να νομιμοποιήσουν offshore

εταιρείες τυχερών παιχνιδιών. Οι εταιρείες όπως η Merrill Lynch, η Goldman Sachs κλπ, ήταν οι επενδυτές σε αυτές τις επιχειρήσεις. Η online ανάπτυξη έρχεται σε αντίθεση με την κατάσταση των καζίνο επιχειρήσεων σε πολλές ευρωπαϊκές χώρες. Στη Γαλλία, για παράδειγμα, χαρτοπαικτικές λέσχες έχουν υποστεί διψήφια πτώση των εσόδων κατά τα τελευταία χρόνια. Στη Βρετανία, τα σχέδια για ένα γιγαντιαίο, καζίνο του Λας Βέγκας είχαν διαλυθεί πριν από δύο χρόνια και παρόμοια καταστήματα στοιχημάτων έχουν αρχίσει να υποφέρουν. Σε άλλες μεγάλες αγορές τυχερών παιχνιδιών, όπως οι Ηνωμένες Πολιτείες και η Κίνα το online στοίχημα είναι επίσης ευρέως διαδεδομένη πρακτική, αν και επισήμως απαγορεύεται. Ακόμη ένας νόμος των ΗΠΑ απαγοεύει τις οικονομικές συναλλαγές που συνδέονται με τα τυχερά παιχνίδια σε απευθείας σύνδεση, η οποία ψηφίστηκε το 2006 και τέθηκε σε ισχύ το τρέχον έτος.

Αντιπρόσωπος της Barney Frank, ένας δημοκράτης από τη Μασαχουσέτη, έχει προτείνει νομοθεσία για να ανατρέψει αυτόν το νόμο και να νομιμοποιήσει τα online τυχερά παιχνίδια. Η Βουλή των Αντιπροσώπων της Επιτροπής Χρηματοπιστωτικών Υπηρεσιών συζήτησε το θέμα αλλά δεν κατάφερε κάτι. Παράλληλα, οι νομοθέτες σε πολλές πολιτείες των ΗΠΑ συμπεριλαμβανομένων των New Jersey, Καλιφόρνια και τη Φλόριντα, έχουν επιπλεύσει ανεξάρτητα προτάσεις για νομιμοποίηση ορισμένα είδη των online τυχερών παιχνιδιών, αξιοποιώντας κάθε παράμετρο του νόμου. Ωστόσο, οι πολιτείες των ΗΠΑ δεν έχουν προχωρήσει τόσο πολύ όσο η British Columbia, στον Καναδά, η οποία νομιμοποίησε ορισμένα είδη των online τυχερών παιχνιδιών. Επιπλέον, η Γαλλία άρχισε να επιτρέπει σε ιδιωτικές εταιρείες να προσφέρουν online αθλητικών στοιχημάτων και είχε απήχηση περισσότερα από 1,2 εκατομμύρια νέους λογαριασμούς ποντάροντας σε 83.000.000 ευρώ, ή και σε 108 εκατομμύρια δολλάρια σε εγκεκριμένους χώρους. Η Γαλλική κυβέρνηση δεν έχει αναφέρει πόσα φορολογικά έσοδα προέκυψαν από την αλλαγή της νομοθεσίας, αλλά η Ιταλία αναφέρει ότι συγκεντρώθηκαν περίπου 150 εκατομμύρια ευρώ σε φόρους περασμένου έτους, ως αποτέλεσμα της μερικής απελευθέρωσης της επιχείρησης.

Με αυτά τα αποτελέσματα η Ιταλία η οποία νομιμοποιήσε τα αθλητικά στοιχήματα στο διαδίκτυο εξουσιοδότησε πρόσφατα υψηλότερο ρίσκο στο πόκερ καθώς και στο καζίνο του Διαδικτύου που προσφέρουν παιχνίδια όπως η ρουλέτα. Θα ήταν χρήσιμο να αναφερθεί, ότι η ιταλική κυβέρνηση ήταν πιο ειλικρινής από

τους άλλους σχετικά με την πρόθεσή της να αυξήσει τα έσοδα από τα παιχνίδια αυτά σε απευθείας σύνδεση, που συνδέει την πιο πρόσφατη νομοθεσία σε ένα πακέτο άντλησης κεφαλαίων για μία συγκεκριμένη περιοχή της Ιταλίας, που είχε οικονομικό πρόβλημα. Όμως το πρόβλημα είναι ότι παρότι που έχουν νομιμοποιηθεί στη Βρετανία στοιχήματα στο διαδίκτυο δεν πληρώνουν τους φόρους διότι δεν έχουν βγάλει την αντίστοιχη άδεια, ενώ οι εταιρείες που θέλουν να λειτουργούν νόμιμα στη Γαλλία αν και υπάρχουν πολλές παράνομες ιστοσελίδες πρέπει να εξασφαλίσουν μια τοπική άδεια, να τηρούν τους κανονισμούς και να πληρώνουν τους αντίστοιχους φόρους. Επίσης, ο κ.Phillips στην εταιρεία Betfair, δήλωσε πως μέσα από αυτά τα τυχερα online παιχνίδια με έδρα την Ευρώπη θα μπορούσε να τονώσει την ευρωπαϊκή οικονομία και να διατηρήσει το ανταγωνιστικό πλεονέκτημα που τώρα απολαμβάνουν εταιρείες στοιχημάτων που η πρακτική τους είναι παράνομη. [1] [6]

1.8. Διάχυτες καταδικαστέες συμπεριφορές

Στο Διαδίκτυο υπάρχουν πολλοί τύποι κατακριτέων διαδικτυακών συμπεριφορών που οι άνθρωποι δεν μπορούν να προσφύγουν στην επιβολή του νόμου. Οι λόγοι είναι από τη σκοπιά του δικαίου σύμφωνα με τις ενέργειες τους και από τη σκοπιά των προσώπων που υπόκεινται στη κατακριτέα συμπεριφορά. Οι υποθέσεις όμως μπορεί να μην είναι αρκετά ισχυρές σύμφωνα με την νομοθεσία, να πάρει πολύ χρόνο στη δίωξη και να είναι πολύ δαπανηρή στην επίλυση των διαφορών. Για παράδειγμα, πολλοί άνθρωποι αγοράζουν αντικείμενα στις δημοπρασίες του Διαδικτύου, και δεν πληρώνουν μετά την παραλαβή των αντικειμένων ή αντίθετα πληρώνουν για τα αντικείμενα που έχουν αγοράσει αλλά δεν τα παραλαμβάνουν ποτέ. Ακόμη, σε διάφορα online φόρουμ συζήτησης ή πίνακες ανακοινώσεων, οι χρήστες χρησιμοποιούν υμβριστική γλώσσα, και προσωπικές επιθέσεις. Σε διάφορες μεγάλες ιστοσελίδες του Διαδικτύου όπως το Facebook, MySpace, MSN, Yahoo, Youtube, κλπ δημοσιεύονται διεφθαρμένες δημοσιεύσεις όπως φωτογραφίες από πορνογραφικό υλικό, φωτογραφίες από κακοποίηση των ζωων κλπ. Για αυτό το λόγο, πρέπει να υπάρχει αναθεώρηση συγκεκριμένων δημοσιεύσεων ώστε να μην υπάρχει τόσο διεφθαρμένο και προσβλητικό υλικό. [1] [7]

ΚΕΦΑΛΑΙΟ 2 Αιτίες

Η φύση του Διαδικτύου, διευκολύνει τη σκοτεινή πλευρά. Πρώτη είναι η ανωνυμία. Οι περισσότερες ιστοσελίδες δεν απαιτούν περισσότερο από μία έγκυρη διεύθυνση e-mail για ένα άτομο για να γίνει μέλος. Οι άνθρωποι μπορούν να χρησιμοποιούν μια σειρά από προσωρινούς λογαριασμούς e-mail, ψευδώνυμα σε chatrooms, άμεσα μηνύματα και άλλα μέσα για να κρύψουν την ταυτότητά τους. Η ανωνυμία έχει ως αποτέλεσμα ο χρήστης να μην νοιώθει καμία ενοχή ξεκινώντας προσωπικές επιθέσεις σε, άλλους υποστηρίζοντας αβάσιμες ιστορίες για τους άλλους διαδίδοντας ψευδείς πληροφορίες κλπ. Επίσης η εύκολη πρόσβαση σε διάφορους ιστότοπους από διάφορες μηχανές αναζήτησης (π.χ. Google ,Yahoo, κλπ.), σε ελεύθερα λογισμικά και υπηρεσίες αποθήκευσης (π.χ. Google Apps ,Gmail κλπ.), σε ιστότοπους κοινωνικής δικτύωσης (π.χ. Facebook, Twitter) ακόμα και σε παράνομες ιστοσελίδες ανταλλαγής αρχείων (π.χ. Kazaa κλπ.). Αυτό έχει οδηγήσει στη μαζική παραβίαση των νόμων περί πνευματικής ιδιοκτησίας στο διαδίκτυο. Υπάρχουν τέσσερις κατηγορίες αιτιών που οι άνθρωποι εντάσσονται στη σκοτεινή πλευρά. Περιλαμβάνουν, την επιθυμία για οικονομικά οφέλη, για τη ψυχολογία, για την αλλαγή των ηθών και διάφορα άλλα. Τα αίτια για τη χρήση των ανθρώπων στη σκοτεινή πλευρά είναι τα εξής:

1. Οικομικά Κέρδη: spam, phishing, click fraud(ψευδοκλικ), hacking, malware (κακόβουλο λογισμικό), online απάτες, παραβίαση των ψηφιακών δικαιωμάτων ιδιοκτησίας, online τυχερά παιχνίδια, πορνογραφία κλπ.
2. Ψυχολογία: spam, malware (κακόβουλο λογισμικό), απόσπαση διαφόρων πληροφοριών εγκληματικότητας.
3. Αλλαγή ηθών: παραβίαση των ψηφιακών δικαιωμάτων ιδιοκτησίας, διάδοση ψευδών πληροφοριών, εκφοβισμός μέσω του spam, malware (κακόβουλο λογισμικό) κλπ.
4. Διάφορα: στοιχεία της σκοτεινής πλευράς.

Στην ψυχολογία έχει τουλάχιστον εφτά στοιχεία μεταξύ των οποίων είναι έμφυτη η σκοτεινή πλευρά των ανθρώπων, συμπεριλαμβανομένων διάφορα αρνητικά συναισθήματα όπως το μίσος, η ζήλεια, και ο θυμός κλπ. Η έμφυτη κακία αναγκάζει τους ανθρώπους να κάνουν άσχημα πράγματα εις βάρος του άλλου. Αυτό καθιστά ευκολότερο για τους ανθρώπους, ειδικά τους έφηβους να

εκφοβίσουν τους συμμαθητές τους διαδίδοντας ψευδείς φήμες, αναρτώντας υβριστικά σχόλια κλπ. Τα ψυχολογικά στοιχεία πίσω από την σκοτεινή πλευρά είναι τα εξής:

1. Η σκοτεινή πλευρά των ανθρώπων
2. Ασθενής αίσθηση της πραγματικότητας
3. Ανάγκη για καθησύχαση για την προσωπική αξία
4. Επιθυμία για αυτοπροβολή
5. Εκδήλωση υπεροχής
6. Επιθυμία απελευθέρωσης άγχους
7. Σεξουαλική δυσλειτουργία

Η ανάγκη για καθησύχαση της αίσθησης της αυτοαξίας οδηγεί ορισμένα άτομα να δοκιμάσουν malware (κακόβουλα λογισμικά) ή διάφορες αρνητικές επιθέσεις μόνο για να αναδείξουν την τεχνική ανδρεία τους. Επίσης διαδίδουν ψευδείς πληροφορίες για να αναδείξουν κάποια ιδιαίτερη γνώση για κάτι ή και για αυτοπροβολή. Ακόμη, η εκδήλωση υπεροχής προκαλεί κάποιους ανθρώπους στο να ανακαλύψουν και να διαδώσουν τρόπους για να εμποδίσουν τα μέτρα για την καταπολέμηση της σκοτεινής πλευράς. Επιπλέον, πολλοί άνθρωποι κάνουν αυτά μόνο και μόνο για να απελευθερώσουν το άγχος τους και να διασκεδάσουν εις βάρος του άλλου. Με το πέρασμα του χρόνου τα ήθη των ανθρώπων αλλάζουν και σε αυτό συνέβαλε η παγκοσμιοποίηση του κόσμου κατά τη διάρκεια της τελευταίας δεκαετίας, ταινίες φαντασίας βίας και σεξουαλικού περιεχομένου, τηλεοπτικές εκπομπές κλπ. Όλα αυτά συνέβαλαν στην αλλαγή των ηθών των ανθρώπων και ειδικά των νέων. Τέλος, οι αλλαγές αυτές αντανακλώνται στο πως οι άνθρωποι συμπεριφέρονται στο Διαδίκτυο. [1]

ΚΕΦΑΛΑΙΟ 3 Οι κύριες τεχνολογίες στην σκοτεινή πλευρά

Η τεχνολογία είναι υπεύθυνη για την άνοδο της σκοτεινής πλευράς του Διαδικτύου. Μερικά από τα στοιχεία της σκοτεινής πλευράς δεν έχουν σύνδεση μεταξύ τους και δυστυχώς η τεχνολογία έχει εγκλωβιστεί στο αέναο κύκλο εναντίον των επινοητικών και δημιουργικών απατεώνων του κυβερνοχώρου. Υπάρχουν εκατομμύρια υπολογιστές που έχουν μολυνθεί με κακόβουλα λογισμικά και οι χάκερς χρησιμοποιούν αυτούς τους υπολογιστές για να ξεκινήσουν το spam, διάφορες επιθέσεις άρνησης υπηρεσιών, phishing και ψευδοκλικ. Ο εντοπισμός των πηγών αυτών καθιστάτε πολύ δύσκολος διότι υπάρχουν πολλές πηγές των τεχνολογιών στο Διαδίκτυο που βοηθούν τους απατεώνες του κυβερνοχώρου. Αυτά περιλαμβάνουν λογισμικά που επιτρέπουν στους spammers να συγκεντρώνουν διευθύνσεις email και να ξεκινάνε spam σε μαζική κλίμακα. Οι απαντήσεις που απαιτούνται για την αντιμετώπιση κάθε στοιχείου της σκοτεινής πλευράς περιλαμβάνουν τα άτομα, λειτουργίες έθνους και θεσμικές ιστοσελίδες και κυβερνητικούς δικτυακούς τόπους. Στην ενότητα αυτή, γίνεται αναφορά στο πως λειτουργεί το κάθε στοχείο της σκοτεινής πλευράς καθώς και τις τεχνολογικές απαντήσεις σε αυτό. [1]

3.1 Spam

Η προέλευση του όρου spam δεν είναι σαφής. Σήμερα, περισσότερο από το 80% του συνόλου των spam προέρχεται από όλο τον κόσμο από υπολογιστές ζόμπι που ανήκουν σε επιχειρήσεις, πανεπιστήμια, και κατά μέσο όρο ιδιοκτήτες ηλεκτρονικών υπολογιστών. Περιλαμβάνει «άσκοπα» μηνύματα χωρίς ουσία, πορνογραφικά υλικά για εμπορική χρήση κλπ. Υπάρχουν πολλοί τύποι μηνυμάτων spam:

1. Ηλεκτρονικού ταχυδρομείου (e-mail) spam
2. Κοινωνικά spam
3. Μηνυμάτων spam
4. Τηλέφωνα spam συνδεδεμένα με το διαδίκτυο

Τα κοινωνικά spam περιλαμβάνουν μηχανή αναζήτησης spam, κοινωνικής δικτύωσης spam, καθώς και την κοινωνική ανεπιθύμητη αλληλογραφία στο διαδίκτυο. Επίσης, ανεπιθύμητο κοινωνικό περιεχόμενο ιστού περιλαμβάνει το spam σε πίνακες ανακοινώσεων, διάφορα φόρουμ συζητήσεων στο διαδίκτυο, ομάδες ειδήσεων, κλπ. [1]

3.1.1 Spam μέσω ηλεκτρονικού ταχυδρομείου

Ο Gary Thuerk έστειλε ένα ψηφιακό εξοπλισμό της Corpπου ανακοινώθηκε το 1978 σε 600 χρήστες του ARPANET φτάνοντας το ήμισυ των χρηστών. Ήταν το πρώτο e-mail spam στην ιστορία. Σύμφωνα με ορισμένες εκτιμήσεις υπάρχουν 200 δισεκατομμύρια ηλεκτρονικά ταχυδρομεία (e-mail) spam, το 97% είναι e-mail spam ανεπιθύμητα και το 85% των e-mail spam είναι προσβλητικό ηλεκτρονικό ταχυδρομείο. Τα spam e-mail είναι η ανεπιθύμητη αλληλογραφία που αφορούν σχεδόν πανομοιότυπα μηνύματα που αποστέλλονται σε πολλούς παραλήπτες μέσω e-mail. Το κόστος αποστολής spam e-mails είναι σημαντικά μικρότερο από εκείνη του κανονικού ταχυδρομείου. Κάνοντας κλίκ σε συνδέσμους σε spam e-mail μπορεί να στείλει τους χρήστες σε κακόβουλα προγράμματα που μπορεί να περιλαμβάνουν κακόβουλο λογισμικό e-mail spam ή άλλα σενάρια ως εκτελέσιμα συννημένα αρχεία. Επίσης το νομικό καθεστώς αυτών των μηνυμάτων ποικίλλει από μία διαδικασία στην άλλη.

Στις Ηνωμένες Πολιτείες, η ανεπιθύμητη αλληλογραφία κρίθηκε νόμιμη από το CAN-SPAM Act του 2013 εφόσον τα μηνύματα τηρούσαν ορισμένες προδιαγραφές. Υπάρχουν περίπου 200 spammers που συλλέγουν διευθύνσεις ηλεκτρονικού ταχυδρομείου από chatrooms, ιστοσελίδες, καταλόγους πελατών, ομάδες συζήτησης με ψεύτικα ονόματα, αριθμούς τηλεφώνου, διευθύνσεις και άλλα στοιχεία επικοινωνίας για τη δημιουργία ενός λογαριασμού για την παροχή υπηρεσιών. Μεγάλο μέρος των μηνυμάτων spam στέλνονται σε μη έγκυρες διευθύνσεις ηλεκτρονικού ταχυδρομείου. Κάθε spammer στέλνει 10 έως 100.000.000 την ημέρα σε διάφορους υπολογιστές (έως και 15) και λίστες διευθύνσεων ηλεκτρονικού ταχυδρομείου (1.200$ για 10 εκατομμύρια διευθύνσεις). Το ποσοστό ανταπόκρισης για τα συγκεκριμένα είναι μικρότερη από 0,1% και έτσι οι spammers πρέπει να δουλέψουν πιο σκληρά. Κερδίζουν, 1000-

10.000 δολάρια την εβδομάδα και εκτιμάται ότι τα spam κοστίζουν στις επιχειρήσεις 100$ δισεκατομμύρια το 2007. Το spam αποτελείται από:

1. Spam εικόνας: είναι μία μέθοδος στην οποία το κείμενο του μηνύματος αποθηκεύεται ως GIF ή JPEG εικόνα και εμφανίζεται στο μήνυμα ηλεκτρονικού ταχυδρομείου. Αυτό αποτρέπει το κείμενο με βάση τα φίλτρα spam από την ανίχνευση και το μπλοκάρισμα μηνυμάτων spam. Το spam εικόνας με πληροφορίες χρησιμοποιήθηκε στα μέσα της δεκαετίας του 2000. Συχνά, περιέχει παράλογο κείμενο που ενοχλεί την ανάγνωση, αλλά με τη νέα τεχνολογία σε ορισμένα προγράμματα προσπαθούν να διαβάσουν τις εικόνες.
2. Κενό Spam: λείπει η διαφήμιση, το σώμα του μηνύματος λείπει εντελώς, καθώς και η γραμμή θέματος. Παρόλα αυτά ταιριάζει με τον ορισμό του spam, διότι από τη φύση του είναι ως χύμα και αυτόκλητων μηνυμάτων ηλεκτρονικού ταχυδρομείου. Το κενό spam μπορεί να προέλθει με διάφορους τρόπους είτε εκ προθέσεως είτε ακούσια. Συμβαίνει, όταν ένας spammer ξεχνά ή παραλείπει να προσθέσει το ωφέλιμο φορτίο. Ακόμη, κενό συχνά εμφανίζεται στις κεφαλίδες γεγονός που υποδηλώνει ότι οι δυσλειτουργίες του υπολογιστή προήλθαν από την κακή σύνταξη του λογισμικού, ενώ άλλα φαίνονται ότι είναι κενά αλλά δεν είναι. Ένα παράδειγμα, είναι η VBS Davinia Be-mail σκουλήκι η οποία διαδίδεται μέσω μηνυμάτων που δεν έχουν καμία γραμμή περιεχομένου όταν στην πραγματικότητα χρησιμοποιεί κώδικα HTML για το κατέβασμα αρχείων.
3. Backscatter (οπισθοδιασποράς) e-mail: είναι μία παρενέργεια του ηλεκτρονικού ταχυδρομείου, ιούς και σκουλήκια (worms) όπου οι servers του ηλεκτρονικού ταχυδρομείου λαμβάνουν.

Τέλος θα ήταν χρήσιμο να αναφερθεί ότι το 2004 το παγκόσμιο κόστος της παραγωγικότητας των μηνυμάτων αυτών ήταν 50 δισεκατομμύρια δολάρια. [1]

3.1.2 Πως λειτουργεί το spam μέσω ηλεκτρονικού ταχυδρομίου

Οι spammers δεν είναι απαραίτητα εμπειρογνώμονες της τεχνολογίας. Διάφορες εταιρείες στέλνουν μήνυμα υποστήριξης της βιομηχανίας που περιλαμβάνει spam εμπορεύματα από εταιρείες καταλόγους των εμπορευμάτων,

έτσι δημιουργούν, συλλέγουν και διανέμουν το spam λογισμικού υποβοήθησης. Αυτά περιλαμβάνουν εργαλεία για τη συγκομιδή διευθύνσεων ηλεκτρονικού ταχυδρομείου, εργαλεία για την απόκρυψη της ταυτότητας του αποστολέα για την αποστολή της ανεπιθύμητης αλληλογραφίας, για το anti-spam, για συγκέντρωση διευθύνσεων ηλεκτρονικού ταχυδρομείου από τα chatrooms, δρομολόγηση των spam e-mails χρησιμοποιούν όπως και για τη χρήση «ζόμπι» υπολογιστών κλπ.

Υπολογιστές «ζόμπι» είναι αυτοί που έχουν μολυνθεί από backdoor σκουλήκια (worms) ή κακόβουλο κώδικα το οποίο επιτρέπει την παράκαμψη της γνήσιας ταυτότητας ή να τροποποίησει υπάρχων πρόγραμμα του κάθε υπολογιστή για να μπορούν οι spammers να στέλνουν e-mails. Η χρήση των «ζόμπι» από τους spammers και τους hackers δεν είναι νέα μέθοδος. Όμως σύμφωνα με τους ειδικούς η πρακτική αυτή έχει γίνει και πιο οργανωμένη και πιο κερδοφόρα από τα προηγούμενα χρόνια. Η εταιρεία ασφάλειας Sophos εκτιμά ότι περίπου το 50% των μηνυμάτων spam προέρχεται από «ζόμπι» υπολογιστές μια αύξηση 25%. Την αύξηση αυτή την προκαλούν οι νέοι νόμοι anti-spam, όπως και τα καλύτερα φίλτρα spam που έχουν καταστήσει δυσκολότερη την αποστολή της ανεπιθύμητης ηλεκτρονικής αλληλογραφίας, έτσι ώστε οι spammers, ψάχνουν για νέους και δημιουργικούς τρόπους για να στείλουν τα μηνύματά τους. Πολλοί βρίσκουν βοήθεια από τους hackers και από αυτούς που μολύνουν τους υπολογιστές με διάφορους ιούς που καταστρέφουν το λογισμικό τους. Με τη δρομολόγηση των μηνυμάτων e-mail μέσω υπολογιστών «ζόμπι» αποφεύγουν το κόστος δαπανών και παράλληλα κρύβουν την προέλευση των μηνυμάτων καθιστώντας πιο δύσκολο τον εντοπισμό τους. Πολλές φορές, αυτά τα δίκτυα «ζόμπι» χρησιμοποιούνται και για να ξεκινήσει denial-of-service (η άρνηση των υπηρεσιών) στις επιθέσεις.

Επίσης, το Μάιο, η αμερικανική Ομοσπονδιακή Επιτροπή Εμπορίου και μία σειρά από άλλες κυβερνητικές υπηρεσίες στο εξωτερικό ξεκίνησε με στόχο «ζόμπι» με ένα πρόγραμμα που ονομάζεται «Λειτουργία Spam ζόμπι». Για να αυξήσει την προβολή του συστήματος, η FTC απέστειλε επιστολές σε περίπου 3.000 ISP sπροτρέποντάς τους να χρησιμοποιούν προστατευτικά μέτρα για να εμποδίσει τους υπολογιστές των πελατών τους από να καταληφθεί από spammers. Εκτός, όμως από τη FTC για να μειωθεί ο κίνδυνος πρέπει να εγκατασταθεί μία προσωπική αντιπυρική ζώνη και λογισμικό προστασίας από ιούς και κρατώντας το αντίγραφο των Windows ενημερωμένο. Τα συμπτώματα ενός «ζόμπι» υπολογιστή

περιλαμβάνουν ξαφνικά αργή ευρυζωνική σύνδεση, υπερβολική δραστηριότητα του σκληρού δίσκου και μη ανταπόκριση του ποντικιού ή του πληκτρολογίου.

Τα ISPs spam παρέχουν υπηρεσίες που επιτρέπουν μια ποικιλία των εγκλημάτων στον κυβερνοχώρο όπως το spam, πορνογραφία και κακόβουλα λογισμικά. Επίσης, το SMPT (απλό πρωτόκολλο μεταφοράς ταχυδρομείου) είναι το πρότυπο σε ευρεία χρήση σήμερα για τη διαβίβαση ηλεκτρονικού ταχυδρομείου μέσω δικτύων IP διευθύνσεων για να παραδίδουν τα μηνύματα από τον ένα ξενιστή στον άλλο και ο διακομιστής αναμετάδοσης αποδέχεται τα μηνύματα. [1] [8] [9] [10]

3.1.3 Τεχνικές αντιμετώπισης του spam

Υπάρχουν πολλές τεχνικές αντιμετώπισης (anti-spam) για την ανεπιθύμητη αλληλογραφία. Η OpusOne είναι μία εταιρεία τεχνολογίας πληροφοριών με έδρα στο Tucson στην Αριζόνα που ιδρύθηκε το 1989. Με 24 χρόνια εμπειρίας δοκιμών προϊόντων που έχουν δοκιμαστεί στο κοινό τα αποτελέσματά του έχουν γίνει γνωστά στη βιομηχανία για την αμεροληψία και την πληρότητά τους. Ο εταιρικός στόχος της είναι να βοηθήσει τους πελάτες για την καλύτερη δυνατή χρήση της τεχνολογίας των πληροφοριών. Έχουν επικεντρωθεί στην εξεύρεση αποτελεσματικών λύσεων για το ηλεκτρονικό ταχυδρομείο και την ασφάλεια. Το Φεβρουάριο του 2007 έδειξε ότι ο μέσος ρυθμός διήθησης του κόστους από τα spam ήταν περίπου στο 86,93% και το μέσο ποσοστού ψευδών θετικών αποτελεσμάτων ήταν 0,3%.

Ο παρακάτω πίνακας δείχνει το ποσοστό των αλιευμάτων spam και τα ψευδή θετικά αποτελέσματα για πολλές και διάφορες υπηρεσίες καλής φήμης. Οι υπηρεσίες αυτές μπορεί να χρησιμοποιηθούν από τις λύσεις των τεχνικών αντιμετώπισης για διαφορετικές λειτουργίες συμπεριλαμβανομένων την απόλυτη άρνηση των μηνυμάτων ή απλά ως ένα συστατικό σε ένα πιο σύνθετο spam. Αυτή η δοκιμή δείχνει το ποσοστό των spam που ταυτοποιήθηκε θετικά με το reputation-based μια υπηρεσία από μόνη της χωρίς να ληφθούν υπόψη άλλα χαρακτηριστικά φιλτραρίσματος. Με βάση τις πληροφορίες IP περιλαμβάνουν χαρακτηριστικά, όπως η δήθεν αποστολή ενός μηνύματος ή οποιοδήποτε περιεχομένου.

Υπηρεσία Φήμης	Ποσοστό	Ψευδής
	Αποκλεισμένοι spam	Θετικός ρυθμός
TrendMicroE-mail Φήμης Υπηρεσίας Αναλυτική	72, 70%	0, 08%
TrendMicroEmail Φήμη Υπηρεσίες Πρότυπο	47, 40%	0, 00%
Spamhause ABO-XBL	51, 90%	0, 03%
IronPort SenderBase	51, 80%	0, 02%
SpamcopBL	41, 20%	0, 00%

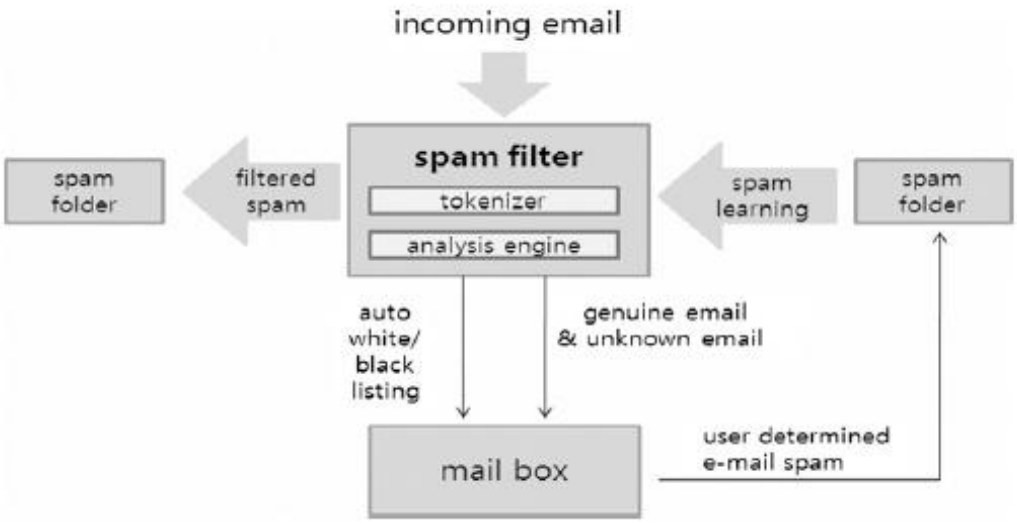
Εικόνα 1 Σύγκριση των anti-spam

Σε αυτή τη δοκιμή, η Trend Micro Email Φήμης Υπηρεσίες Αναλυτική έχει το υψηλότερο ποσοστό αλιευμάτων. Πολλοί πωλητές προσφέρουν λύσεις σε κακόβουλα λογισμικά που περιλαμβάνουν τεχνικές αντιμετώπισης. Πολλές περιλαμβάνουν McAfee Internet Security 2010 και McAfee Total Protection 2010. Η McAfee, είναι η μεγαλύτερη εταιρεία τεχνολογίας αφιερωμένη στην ασφάλεια του κόσμου, παρέχοντας δοκιμασμένες λύσεις, προληπτικές και υπηρεσίες που βοηθούν ασφαλή συστήματα και δίκτυα σε όλο τον κόσμο. Επίσης, προστατεύει τους καταναλωτές και τις επιχειρήσεις όλων των μεγεθών από τα κακόβουλα λογισμικά και τις αναδυόμενες ηλεκτρονικές απειλές. Έχουν σχεδιαστεί οι λύσεις αυτές να λειτουργούν μαζί, με την ενσωμάτωση anti-malware, anti-spyware και antivirus λογισμικά με δυνατότητες διαχείρισης της ασφάλειας που προσφέρουν απαράμιλλη ορατότητα σε πραγματικό κόσμο και αναλύσεις που μειώνουν τον κίνδυνο, βελτιώνουν την ασφάλεια του Διαδικτύου και βοηθούν στις επιχειρήσεις να επιτύχουν στην επιχειρησιακή αποτελεσματικότητα.

Επίσης το Kaspersky Antivirus 2015 προσφέρει παρόμοια προστασία από ιούς και λογισμικά spyware και παράλληλα αυτοματοποιεί τη διαδικασία κωδικών πρόσβασης και έτσι ο χρήστης δεν χρειάζεται να θυμάται και να φτιάχνει κωδικούς πρόσβασης.

Στην εικόνα 2 απεικονίζεται η διαδικασία φιλτραρίσματος ανεπιθύμητων μηνυμάτων. Αρχικά χωρίζει τα εισερχόμενα e-mail σε μάρκες. Στη συνέχεια, η

μηχανή ανάλυσης φίλτρων ηλεκτρονικού ταχυδρομείου τσεκάρει τη διεύθυνση ηλεκτρονικού ταχυδρομείου του αποστολέα που βρίσκεται στη μαύρη λίστα ή ένα χαρακτηριστικό spam που ίσως βρίσκεται στον τίτλο ή στο περιεχόμενο του e-mail. Χαρακτηριστικά spam περιλαμβάνουν σημεία έμφασης, όπως κεφαλαία γράμματα, θαυμαστικά, επανάληψη ειδικών συμβόλων χωρίς νόημα κλπ. Οι διευθύνσεις των e-mails που περιέχουν χαρακτηριστικά spam προστίθενται αυτόματα στη μαύρη λίστα. Ο χρήστης μπορεί να μετακινήσει αφιλτράριστο spam e-mails στο φάκελο spam. Η μηχανή ανάλυσης μαθαίνει συνεχώς από τα χαρακτηριστικά spam από τέτοια μηνύματα ηλεκτρονικού ταχυδρομείου.



Εικόνα 2 E-mail διαδικασίας φίλτρα ανεπιθύμητης αλληλογραφίας

Τεχνικές anti-spam μπορούν να ταξινομηθούν σε τουλάχιστον επτά κατηγορίες, ως εξής:

1. Κατάλογος με βάση φιλτραρίσματος: Αυτή η τεχνική χρησιμοποιεί μια μαύρη λίστα και μία λευκή με τις διευθύνσεις e-mail. Το πρόβλημα με αυτή την τεχνική είναι ότι οι κατάλογοι πρέπει να ενημερώνονται διαρκώς, καθώς οι spammers συνεχίζουν να αλλάζουν τις διευθύνσεις των e-mails τους.

2. Φιλτράρισμα που βασίζεται σε κανόνες: Σε αυτή την τεχνική αναλύεται η διεύθυνση του αποστολέα, η διεύθυνση επιστροφής, αντικείμενο στην επικεφαλίδα και το μήνυμα του e-mail για γνωστές λέξεις spam.
3. Φιλτράρισμα με βάση το περιεχόμενο: Η τεχνική αυτή προσπαθεί υπολογιστικά να διακρίνει την ανεπιθύμητη αλληλογραφία με μία νόμιμη χρησιμοποιώντας τεχνικές μηχανικής μάθησης. Οι spammers για αυτό το λόγο χρησιμοποιούν άσχετες λέξεις σε μηνύματα ηλεκτρονικού ταχυδρομείου και με την εισαγωγή JPEG ή κινούμενες εικόνες GIF στα μηνύματα. Επίσης, γράφουν το κείμενο σε λευκή γραμματοσειρά σε λευκό φόντο προκειμένου να αποφύγουν την ανίχνευσή τους.
4. Συνεργατικό φιλτράρισμα: Κατηγοριοποιεί τα e-mails που έλαβε ως spam από τα e-mails που έλαβε ένας άλλος χρήστης στον ίδιο διακομιστή ηλεκτρονικού ταχυδρομείου. Το πρόβλημα με αυτή την τεχνική είναι ότι μπορεί να χρησιμοποιηθεί μόνο για τον ίδιο διακομιστή ηλεκτρονικού ταχυδρομείου, μέχρι οι διακομιστές ηλεκτρονικού ταχυδρομείου να μην μοιράζονται τις ίδιες πληροφορίες. Επιπλέον, οι spammers μπορούν να δημιουργήσουν πολλές εκδοχές του ίδιου spam e-mail με τη χρήση τυχαίων λέξεων, έτσι ώστε να αναγνωρίζονται ως διαφορετικά e-mails και να αλλάζουν συνεχώς τη διεύθυνση τους.
5. Ταξινόμηση spam μέσω των κοινωνικών δικτύων: Η μέθοδος αυτή βασίζεται στην ανάλυση των κοινωνικών δικτύων. Αντιπροσωπεύει αποστολείς των e-mail ως κόμβους σε ένα γράφημα και τη σχέση μεταξύ των ανθρώπων που στέλνουν και λαμβάνουν e-mails ως συνδέσμους στο γράφημα. Οι κόμβοι που δεν ανήκουν στη συνδεδεμένη λίστα στη γραφική παράσταση θεωρείται ως spam. Το πρόβλημα με αυτή την τεχνική είναι ότι δεν απαιτεί τον εντοπισμό της ιστορίας του ηλεκτρονικού ταχυδρομείου η οποία μπορεί να γίνει μόνο με τον ίδιο διακομιστή του e-mail και χαρακτηρίζεται ως spammer.
6. Έλεγχος ταυτότητας: Αυτή η τεχνική χρησιμοποιείται για να βεβαιωθεί ότι στον τομέα ενός αποστολέα e-mails η ταυτότητα του είναι έγκυρη. Είναι εύκολο για έναν αποστολέα να χρησιμοποιήσει άλλη ταυτότητα και έτσι επωφελεί τους spammers. Υπάρχουν διάφορα πρωτόκολλα για τον έλεγχο της ταυτότητας της διεύθυνσης του αποστολέα. Το SPF (Sender Policy Framework) πρωτόκολλο πλαισίου πολιτικής του αποστολέα, έχει εξελιχθεί

αρκετά και χρησιμοποιεί μία αντίστροφη μέθοδο αναζήτησης για την εγγραφή MX του DNS για να επαληθεύσει τον τομέα του αποστολέα. Η λήψη, διακομιστή αλληλογραφίας εξάγει τη διεύθυνση του αποστολέα, και στέλνει ένα ερώτημα DNS και από την απάντηση του DNS περιέχει την IP διεύθυνση του αποστολέα που έχει εγκριθεί από την αποστολή e-mail server.

7. Ανάλυση της δομής του Link: Είναι δύσκολο να αναλύσεις το περιεχόμενο ενός spam e-mail εάν περιέχει μόνο μια μικρή ποσότητα του κειμένου. Ως εκ τούτου, η μέθοδος αυτή διακρίνει το αυθεντικό e-mail και το spam e-mail από το πρώτο υπολογισμό του αριθμού των συνδέσεων που ένα έγγραφο Web έχει συνδεθεί με άλλα έγγραφα στο Web και τον αριθμό των υπερ συνδέσμων που περιλαμβάνονται στο e-mail. Τέλος, στη συνέχεια, χρησιμοποιεί δέντρο απόφασης και μια αλλαγμένη δομή των συνδέσμων χρησιμοποιώντας διευθύνσεις διακομιστή.

Υπάρχουν τουλάχιστον πέντε προβλήματα που περιορίζουν ουσιαστικά τεχνικές anti-spam:

1. Οι τεχνικές anti-spam βασίζονται στη κατανόηση του κειμένου και στις τεχνολογίες αναγνώρισης εικόνας. Τα spam e-mails περιέχουν μηνύματα κειμένου ή και εικόνων, κειμένων αναγνώρισης και κατανόησης εικόνας τα οποία δεν μπορούν να αποφευχθούν. Ωστόσο, οι τεχνολογίες αυτές έχουν θεμελιώδη όρια που κατά πάσα πιθανότητα δεν θα πρέπει να ξεπεραστούν στο άμεσο μέλλον.
2. Τα σημερινά συστήματα ηλεκτρονικού ταχυδρομείου βασίζονται στο SMTP και η τεράστια κυκλοφορία e-mailστον κυβερνοχώρο.
3. Υπάρχουν πολλοί διακομιστές μεσολάβησης, αναμεταδόσεις ανοικτές και δίκτυα προγραμμάτων που είναι ουσιαστικά αδύνατον να εξαλειφθούν. Μια μεγάλη πλειοψηφία των ιδιοκτητών ηλεκτρονικών υπολογιστών που δεν γνωρίζουν καν ότι οι υπολογιστές τους έχουν μολυνθεί, δεν έχουν anti-malware και υπάρχουν κακόβουλα προγράμματα.
4. Η βιομηχανία του spam-aiding έχει εξαπολύσει με επιτυχία έναν πόλεμο εναντίον του anti-spam και οι κυβερνήσεις μέχρι τώρα δεν ήταν σε θέση να το αντιμετωπίσει.

5. Τα προϊόντα anti-spam ανταποκρίνονται στη διπλή απαίτηση της επιβολής κυρώσεων spam και στην έγκριση των νόμιμων μάρκετινγκ και της ελευθερίας του λόγου. Μερικοί άνθρωποι, περισσότερο από το 0,01% των δικαιούχων που γίνονται στους πελάτες βρήκαν το spam χρήσιμο. Η γραμμή ανάμεσα στη νόμιμη εκστρατεία μάρκετινγκ και spam δεν είναι σαφής σε κάποιο σημείο στο φάσμα των e-mails. Η δυσκολία αυτή είναι παρόμοια με εκείνη της σχεδίασης της γραμμής μεταξύ πορνογραφίας και της τέχνης.[1] [11] [12] [13]

3.2 Κοινωνικά Spam

Spam είναι η μαζική αποστολή μεγάλου αριθμού μηνυμάτων τα οποία είναι ανεπιθύμητα για τους παραλήπτες. Τα μηνύματα μπορεί να έχουν το ίδιο περιεχόμενο σε παραπάνω από έναν παραλήπτη. Επιπλέον, μπορούμε να τα βρούμε και με τις ονομασίες «Αυτόκλητη Εμπορική Ηλεκτρονική Αλληλογραφία» (Unsolicited Commercial E-mail-UCE) καθώς και η «Αυτόκλητη Μαζική Ηλεκτρονική Αλληλογραφία» (Cusolicited Bulk E-mail-UBE). Πρωτοεμφανίστηκαν, την δεκαετία του 90΄. Συγκεκριμένα, το 1994 δυο Αμερικανοί δικηγόροι, με τη βοήθεια ενός προγραμματιστή, αποφάσισαν να κάνουν διαφήμιση της επιχείρησης τους στέλνοντας πολλαπλά ηλεκτρονικά μηνύματα σε χιλιάδες ειδησεογραφικούς οργανισμούς. Επιπλέον η μηχανή αναζήτησης spam έχει ως στόχο να ξεγελάσει τις μηχανές αναζήτησης σε ανάθεση υψηλών κατατάξεων στα αποτελέσματα αναζήτησης σε μία σελίδα ανεπιθύμητης αλληλογραφίας στο Web. Οι spammers για να το επιτύχουν αυτό χρησιμοποιούνε δημοφιλείς λέξεις-κλειδιά (π.χ. iPhone) ή ετικέτες για μία ιστοσελίδα (π.χ. blog για μία διαφήμιση), έτσι ώστε οι χρήστες που αναζητούν σελίδες Web για iPhone να ανατρέχουν σε αυτά. Η κοινωνική δικτύωση των spam σχετίζεται με ιστοσελίδες όπως Facebook, Twitter, κλπ. Μερικά spam παράγουν νέους επισκέπτες στα προσωπικά τους blogs ή τα χρησιμοποιούν και για άλλους λόγους.[1]

3.2.1 Πως λειτουργούν τα κοινωνικά spam

Υπάρχουν δύο τεχνικές για τη δημιουργία των spam μηχανής αναζήτησης: βασισμένο στο περιεχόμενο και στους συνδέσμους. Με βάση τον HITS αλγόριθμο

Hyperlink–Induced θέμα αναζήτησης είναι μία ανάλυση του αλγόριθμου που βαθμολογεί τις ιστοσελίδες που αναπτύχθηκε από τον Jon Kleinberg. Η ιδέα πίσω από Hubs και Αρχές προήλθε από μία συγκεκριμένη εικόνα για τη δημιουργία ιστοσελίδων, όταν το Διαδίκτυο σε ορισμένες ιστοσελίδες γνωστοί ως κόμβοι υπηρέτησε ως μεγάλος κατάλογος με μη έγκυρες πληροφορίες αλλά χρησιμοποιήθηκε ως συλλογές για ένα ευρύ κατάλογο πληροφοριών, που οδήγησαν τους χρήστες απευθείας σε άλλες έγκυρες σελίδες. Με άλλα λόγια με ένα καλό κόμβο-ιστοσελίδας αντιπροσώπευε μια σελίδα που επεσήμανε σε πολλές άλλες σελίδες. Άρα, το πρόγραμμα αποδίδει δύο βαθμολογίες για κάθε σελίδα, η οποία εκτιμά την αξία του περιεχομένου της σελίδας, και η αξία κόμβου, η οποία εκτιμά την αξία των δεσμών της με άλλες σελίδες.

Στον αλγόριθμο HITS, το πρώτο βήμα είναι να ανακτήσει τις πιο σχετικές με το ερώτημα αναζήτησης. Αυτό το σύνολο ονομάζεται το σύνολο της ρίζας και μπορούν να ληφθούν με τη λήψη των κορυφαίων σελιδών ή σελίδες που επιστρέφονται από ένα κείμενο με βάση τον αλγόριθμο αναζήτησης. Οι ιστοσελίδες στο σύνολο βάσης και όλες οι υπερ-συνδέσεις μεταξύ των σελίδων αυτών αποτελούν ένα εστιασμένο υπογράφημα. Ο υπολογισμός HITS γίνεται μόνο σε αυτό το εστιασμένο υπογράφημα. Σύμφωνα με τον Kleinbergo λόγος για την κατασκευή ενός σετ βάσης είναι να εξασφαλιστούν οι πιο ισχυρές θεωρίες που περιλαμβάνουν. Επίσης, ο αλγόριθμος εκτελεί μια σειρά από επαναλήψεις, το καθένα αποτελούμενο από δύο βασικά στάδια:

1. Αρχή Ενημέρωση: Ενημέρωση Αρχής βαθμολογίας κάθε κόμβου να είναι ίσο με το άθροισμα των Hub του κάθε κόμβου που οδηγεί σε αυτό. Δηλαδή, ένας κόμβος δίνεται με υψηλή βαθμολογία Αρχή με το να συνδέονται από σελίδες που αναγνωρίζονται ως κόμβοι πληροφοριών.
2. Hub Ενημέρωση: Ενημέρωση σκόρ κάθε κόμβου, να είναι ίσο με το άθροισμα της Αρχής του κάθε κόμβου. Δηλαδή, ένας κόμβος δίνει μία υψηλή βαθμολογία με τη σύνδεση με τους κόμβους.

Η βαθμολογία Hub και Αρχή βαθμολογίας για έναν κόμβο υπολογίζεται με τον ακόλουθο αλγόριθμο:

1. Θεωρητικά κάθε κόμβος έχει μία βαθμολογία και βαθμό

2. Εκτέλεση του άρθρου Αρχή Ενημέρωση.
3. Εκτέλεση του άρθρου Hub Ενημέρωση.
4. Ομαλοποίηση των τιμών διαιρώντας κάθε όρο Hub με τετραγωνική ρίζα του αθροίσματος των τετραγώνων όλων των βαθμολογιών Hub, και διαιρώντας κάθε βαθμολογία της Αρχής με τετραγωνική ρίζα του αθροίσματος των τετραγώνων όλων των βαθμολογιών της Αρχής.
5. Επανάληψη από το δεύτερο στάδιο όπως απαιτείται.

Αρχή Ενημέρωσης Κανόνας

$\forall p$, Ενημερώνουμε$\text{auth}(p)$ να είναι το άθροισμα:

$$auth(p) = \sum_{i=1}^{n} hub(i)$$

Όπου n είναι ο συνολικός αριθμός των σελίδων που συνδέονται με p και i. Δηλαδή, η βαθμολογία της Αρχής είναι το άθροισμα όλων των βαθμολογιών Hub των σελίδων που οδηγούν σε αυτό.

Hub Ενημέρωση Κανόνας

$\forall p$, Ενημερώνουμε $hub(p)$ να είναι το άθροισμα:

$$hub(p) = \sum_{i=1}^{n} auth(i)$$

Όπου n είναι ο συνολικός αριθμός των σελίδων p και i. Έτσι, Hub βαθμολογία μιας σελίδας είναι το άθροισμα των βαθμολογιών Αρχής για τη σύνδεση των σελίδων.

Κανονικοποίηση

Οι τελικές βαθμολογίες Hub-Αρχή κόμβων καθορίζεται μετά από άπειρες επαναλήψεις του αλγορίθμου. Εφαρμόζεται άμεσα και επαναληπτικά Hub Ενημέρωση Κανόνα και Αρχή Ενημέρωση Κανόνα που οδηγεί σε αποκλίνουσες τιμές για αυτό είναι απαραίτητη η ομαλοποίηση της μήτρας μετά από κάθε

επανάληψη. Έτσι, οι τιμές που λαμβάνονται από τη διαδικασία αυτή τελικά θα συγκλίνουν.

Ψευδοκώδικας

1. G:=Ρύθμιση των σελίδων
2. Για κάθε σελίδα στο Gκάνουμε
3. P.auth=1 // p .authείναι η βαθμολογία αρχή της σελίδας p
4. P.hub=1 // p .hubείναι η βαθμολογία κομβικό σημείο της σελίδας p
5. HubsAndAuthorities λειτουργία (G)
6. Για το βήμα από 1 εώς k κάνει //τρέξει τον αλγόριθμο kβήματα
7. Κανόνας = 0
8. Για κάθερ σελίδα στο G κάνουμε // ενημερώστε όλες τις τιμές αρχή πρώτη
9. P.auth = 0
10. Για κάθε Gσελίδα στο p.incomingNeighborsκάνουμε // p.incomimgNeighborsείναι το σύνολο των σελίδων που συνδέονται με s
11. P. Auth + = q. Hub
12. Κανόνας+ = τετράγωνο (p.auth) // υπολογίζει το άθροισμα των τετραγώνων ΑΠΘ τιμές για την εξομάλυνση
13. Νόρμα = sqrt (νόρμα)
14. Για κάθε σελίδα στο G κάνουμε // ενημερώστε τις βαθμολογίες ΑΠΘ
15. P.auth = p. Auth / νόρμα // ομαλοποίηση τιμών ΑΠΘ
16. Νόρμα = 0
17. Για κάθε σελίδα στο Gδεν // στη συνέχεια ενημερώστε όλες τις τιμές κόμβου
18. P.hub = 0
19. Για κάθε σελίδα rσε p.outgoingNeighborsκάνουμε // p.outgoingNeighborsείναι το σύνολο των σελίδων
20. P. Hub + = r auth

21. Κανόνας + = τετράγωνο (p.auth) // υπολογίζει το άθροισμα των τετραγώνων των τιμών των κόμβων για την εξομάλυνση
22. Νόρμα = sqrt (νόρμα)\
23. Για κάθε ρσελίδα στο G δεν // στη συνέχεια ενημερώστε όλες τις τιμές κόμβου
24. P. Hub = p .hub / νόρμα // ομαλοποιήση τιμών κόμβου

Οι τιμές διανομέα και το κύρος συγκλίνουν στον παραπάνω ψευδοκώδικα.

Επίσης, μια μηχανή αναζήτησης που χρησιμοποιεί τον αλγόριθμο HITS που ταξινομεί τις σελίδες επιστρέφοντας ως ερώτημα που έχει ως αποτέλεσμα ένα συνδυασμό των σελίδων με τα υψηλότερα hub και τις αυθεντικές βαθμολογίες. Οι spammers θα προσθέσουν πολλές εξερχόμενες συνδέσεις με την ιστοσελίδα στόχο για να αυξήσει το σκόρ του κόμβου του. Τεχνικές που χρησιμοποιούνται για να δημιουργήσουν με βάση το περιεχόμενο spam περιλαμβάνουν λέξεις-κλειδιά που τις εισάγει σε μία ιστοσελίδα. Στην πληροφορική, spamdexing γνωστό ως spam μηχανή αναζήτησης, είναι η σκόπιμη χειραγώγηση των μηχανών αναζήτησης. Πρόκειται για μια σειρά από μεθόδους όπως η επανάληψη άσχετων φράσεων, χειραγώγηση της σχετικότητας και της προβολής των πόρων αναπροσαρμόζοντας κατά τρόπο που δε συνάδει με το σκοπό του συστήματος ευρετηρίασης. Θα μπορούσε να θεωρηθεί ως μέρος της αναζήτησης η βελτιστοποίηση μηχανών, αν και υπάρχουν πολλές μέθοδοι βελτιστοποίησης που βελτιώνουν την ποιότητα και την εμφάνιση του περιεχομένου των ιστοσελίδων .

Οι μηχανές αναζήτησης χρησιμοποιούν μια ποικιλία από αλγορίθμους για να καθορίσει τη σχετικότητα κατάταξης. Ορισμένες από αυτές περιλαμβάνουν τον προσδιορισμό αν ο όρος αναζήτησης εμφανίζεται στο σώμα του κειμένου ή της διεύθυνσης URL μιας ιστοσελίδας. Πολλές μηχανές αναζήτησης ελέγχουν για περιπτώσεις spamdexing και έτσι αφαιρούν ύποπτες σελίδες από ευρετήριά τους. Επίσης, οι άνθρωποι που εργάζονται για μια οργάνωση μηχανών αναζήτησης μπορούν να μπλοκάρουν γρήγορα τα αποτελέσματα από τον κατάλογο από ολόκληρες ιστοσελίδες που χρησιμοποιούν το spamdexing. Χρησιμοποιώντας

ανήθικες μέθοδοι για να κάνουν ιστοσελίδες, κατατάσσονται σε υψηλότερη θέση στα αποτελέσματα των μηχανών αναζήτησης από ό,τι θα ήταν διαφορετικά. Κοινές τεχνικές spamdexing μπορούν να ταξινομηθούν σε δύο μεγάλες κατηγορίες: ανεπιθύμητο περιεχόμενο και spam σύνδεσμο. Spamdexing είναι η πρακτική του spamming μηχανής αναζήτησης. Είναι μια μορφή της βελτιστοποίησης μηχανών αναζήτησης (SEO) spamming, η οποία είναι η τέχνη του να κάνεις ένα δικτυακό τόπο ελκυστικό για τις μεγάλες μηχανές αναζήτησης για τη βέλτιστη ευρετηρίαση. Spamdexing είναι η πρακτική της δημιουργίας δικτυακών τόπων που παράνομα αναπροσαρμόζονται με μια υψηλή θέση στις μηχανές αναζήτησης. Μερικές φορές χρησιμοποιείται για τη χειραγώγηση, την κατανόηση μιας μηχανής αναζήτησης μιας κατηγορίας.

Ο στόχος ενός σχεδιαστή Ιστού είναι να δημιουργήσει μια ιστοσελίδα που θα έχει ευνοϊκή κατάταξη στις μηχανές αναζήτησης, και να δημιουργήσουν τις σελίδες τους σύμφωνα με τα πρότυπα που πιστεύουν ότι θα βοηθήσει. Κάποιοι από αυτούς καταφεύγουν σε spamdexing, συχνά εν αγνοία από τους πελάτες τους. Ενώ, το spamdexing έχει παρέμβει με τη διαπίστωση των πληροφοριών στο διαδίκτυο, έχουν ληφθεί μέτρα για την καταπολέμησή της με κάποια επιτυχία. Ήταν ένα μεγάλο πρόβλημα στη δεκαετία του 1990, και οι μηχανές αναζήτησης ήταν άχρηστες επειδή επηρεαζόντουσαν από το spamdexing. Όταν η Google ήρθε στη σκηνή, όλα άλλαξαν, ανέπτυξε μια σελίδα κατάταξης, με ένα σύστημα εναντίον του spamdexing που είχε ως συνέπεια να προεξοφλήσει τοποθεσίες spam, σχετικές ιστοσελίδες με υψηλές βαθμολογίες. Τέλος, οι spammers στέλνουν μηνύματα γράφοντας απαντήσεις σε άλλα μέλη με ενσωματωμένες συνδέσεις στις ιστοσελίδες της επιλογής τους. [1] [14] [15]

3.2.2 Τεχνικές αντιμετώπισης

Η σημερινή World Wide Web (WWW) έχει εξελιχθεί σε μια τεράστια πλατφόρμα πληροφοριών και αναζήτησης. Οι μηχανές έχουν ήδη αποκτήσει τεράστια επιτυχία. Χρήστες βασίζονται σε μηχανές αναζήτησης για να εντοπίζουν πληροφορίες στο Διαδίκτυο. Και οι ιδιοκτήτες των ιστοσελίδων που βασίζονται σε μηχανές αναζήτησης για τη διάδοση πληροφοριών επισημαίνουν ότι η υψηλότερη κατάταξη στα αποτελέσματα των μηχανών αναζήτησης, είναι πολύ πιθανό να

παράγει κέρδος στο Διαδίκτυο, έτσι ώστε να αυξηθεί η κατάταξη των ιστοσελίδων τους χρησιμοποιώντας διάφορα spamming, που εξαπατούν το σύστημα ταξινόμησης μηχανών αναζήτησης.

Υπάρχουν δύο τεχνικές για την αντιμετώπιση των spam μηχανής αναζήτησης, η μία να αυξηθεί η ακρίβεια και η αξιοπιστία των αποτελεσμάτων αναζήτησης, εξουδετερώνοντας την παρεμβολή από spam μηχανής αναζήτησης. Αυτό λαμβάνει υπόψη τους διαφορετικούς τύπους των μηνυμάτων spam μηχανής αναζήτησης. Αρχικά, αυτές οι προσεγγίσεις περιλαμβάνουν TrustRank και SpamRank, TrustRank είναι μία ανάλυση της τεχνικής που περιγράφεται στο έγγραφο καταπολέμισης του Web spam με TrustRank από τους ερευνητές Zoltan Gyongyi και Hector Garcia-Molina. Η τεχνική αυτή χρησιμοποιείται για ημι-αυτόματο διαχωρισμό των χρήσιμων ιστοσελίδων από spam. Πολλές σελίδες ανεπιθύμητων μηνυμάτων δημιουργούνται μόνο με την πρόθεση της παραπλάνησης. Οι σελίδες αυτές κυρίως δημιουργήθηκαν,για λόγους εμπορικούς, χρησιμοποιώντας διάφορες τεχνικές για να επιτύχουν υψηλότερες αποδοχές από ό,τι άξιζε, σχετικά με τις σελίδες αποτελεσμάτων μηχανών αναζήτησης. Μια δημοφιλής μέθοδος για τη βελτίωση της κατάταξης είναι να αυξήσει την αντιληπτή σημασία ενός εγγράφου μέσω περίπλοκων συστημάτων σύνδεσης Google PageRank και άλλους αλγόριθμους αναζήτησης. Το TrustRank επιδιώκει την καταπολέμηση των spam φιλτράροντας το διαδίκτυο με βάση την αξιοπιστία. Η μέθοδος απαιτεί την επιλογή ενός μικρού συνόλου των σελίδων πόρων που πρέπει να αξιολογηθούν από έναν εμπειρογνώμονα. Μόλις εντοπιστούν οι αξιόπιστες σελίδες πόρων, μια αναζήτηση που εκτείνεται προς τα έξω από το σύνολο των πόρων αναζητά με τον ίδιο τρόπο αξιόπιστες σελίδες. Η αξιοπιστία TrustRank μικραίνει με την αύξηση της απόστασης μεταξύ εγγράφων και του πόρου. Η λογική λειτουργεί με τον αντίθετο τρόπο, καθώς και αυτό ονομάζεται Anti-TrustRank.

Θα ήταν χρήσιμο να σημειωθεί ότι πολλοί ιδιοκτήτες επιχειρήσεων τείνουν ώστε να δείξουν τον αλγόριθμο αναζήτησης της Google ως ένα μυστηριώδες «μαύρο κουτί» του οποίου η εσωτερική λειτουργία δεν μπορεί να είναι γνωστή. Επίσης, το TrustRank βασίζεται στο PageRank που είναι το όνομα για τον αρχικό αλγόριθμο και οι ιδρυτές της είναι της Google Larry Page και Sergey Brinto 1998. Αυτοί, οι δύο μηχανικοί υπολογιστών προσπάθησαν να απαντήσουν στο ερώτημα για το πως θα μπορέσουν να προσδιορίσουν την αξία μιας ιστοσελίδας χωρίς λάθη

για διάφορα τεχνάσματα. Έτσι,δημιουργήσανε ένα πρόγραμμα με ένα χάρτη του συνόλου Web και στη συνέχεια κατατάσσονται σε κάθε σελίδα που βασίζεται, στον αριθμό εισερχόμενων συνδέσεων που είχε και στη δημοτικότητα των χωρών παροχής αυτών των δεσμών. Αποδείχθηκε, εξαιρετικά επιτυχής βοηθώντας έτσι την Google στην παγκόσμια κυριαρχία. Όμως η PageRank είχε ένα μοιραίο ελάττωμα. Όταν οι web masters κατάλαβαν ότι οι συνδέσεις ήταν το κλειδί για υψηλότερες βαθμολογίες, άρχισαν να αγοράζουν και να πωλούν. Έτσι γεννήθηκε η TrustRank που λειτουργεί ουσιαστικά το ίδιο όπως και η PageRank, με μία βασική διαφορά: σε κάθε ιστοσελίδα που υποπτεύεται ότι αγοράζουν ή πωλούν συνδέσμους τιμωρούνται και τοποθετούνται στο τέλος των αποτελεσμάτων αναζήτησης. Αυτό το σύστημα καθιερώθηκε το 2007. Η Google προχώρησε τόσο πολύ ώστε να απελευθερώσει ένα εύχρηστο πρόγραμμα περιήγησης Page Rank plug-in που παρέχει αξιοπιστία για κάθε ιστοσελίδα που επισκέπτεται ο κάθε χρήστης.

Μια άλλη προσέγγιση είναι η ανίχνευση spam για κάθε spam γενιά τεχνική και spam περιβάλλον. Για παράδειγμα, οι δεσμοί μεταξύ των σελίδων Web αναλύονται για την ανίχνευση σύνδεσης με βάση το spam, ενώ η ανάλυση λέξεων-κλειδιών και η σύγκριση με το νόμιμο έγγραφο γίνονται με βάση το περιεχόμενο ανεπιθύμητης αλληλογραφίας. Επιπλέον, υπάρχουν τεχνικές ανίχνευσης που έχουν σχεδιαστεί ειδικά για spam που εμφανίζονται σε συγκεκριμένα περιβάλλοντα, όπως τα blogs. Παράλληλα, τα HubSpot βοηθούν τους χρήστες να χρησιμοποιούν τεχνικές ανίχνευσης σε ανεπιθύμητη αλληλογραφία. Συγκεκριμένα, είναι μια εταιρεία που αναπτύσει και εμπορεύεται ένα προϊόν λογισμικού. Το λογισμικό, διαθέτει δυνατότητες για κοινωνικό μάρκετινγκ, μέσων μαζικής ενημέρωσης το e-mail marketing, διαχείριση περιεχομένου, web ανάλυση, και τη βελτιστοποίηση μηχανών αναζήτησης, μετάξυ άλλων.

Το HubSpot ιδρύθηκε από το Brian HubSpot και Dharmesh Shah από το ινστιτούοτο Τεχνολογίας της Μασαχουσέτης το 2006. Αρχικά χρηματοδοτήθηκε από τον Shah και μέλος ΔΕΠ στο MIT, συγκέντρωσε περισσότερα από 100 εκατομμύρια δολάρια σε χρηματοδότηση από Larry Bohn, General Catalyst Partners, David Skok, Matrix Συνεργάτες, Rob Theis, Κλίμακα Venture Partners, Sequoia Capital, το Google Ventures, Salesforce και η Fidelity. Η εταιρεία υποστηρίζει την εισερχόμενη έννοια μάρκετινγκ στη δική του μάρκετινγκ μέσα

από ιογενή βίντεο, Twitter, σεμινάρια και μια ετήσια έκθεση εισερχόμενα μάρκετινγκ. Η εταιρεία παρουσίασε το λογισμικό αυτό το 2006 και ξεκίνησε επίσημα τον Δεκέμβριο του 2007. Το πρώτο γραφείο της εταιρείας ήταν στο Cambridge Κέντρο Καινοτομίας και μέχρι το 2008 η εταιρεία κατείχε πάνω από το μισό του 5ου ορόφου του CIC.Το 2011 αύξησε $ 32.000.000 σε χρηματοδότηση μέσω επιχειρηματικών κεφαλαίων. Αργότερα εκείνο το έτος η HubSpot ανακοίνωσε την εξαγορά της στην one forty. Η one forty ξεκίνησε ως ένα κατάστημα app για το Twitter, αλλά μετακινήθηκε σε μια διαδικτυακή πηγή πληροφοριών για το κοινωνικό μάρκετινγκ μέσων μαζικής ενημέρωσης.

Η εταιρεία παρουσίασε επίσης το νέο λογισμικό για την εξατομίκευση των δικτυακών τόπων σε κάθε επισκέπτη. Σύμφωνα με το Forbesη HubSpot ξεκίνησε με στόχο να αποτελείται από 1-10 εργαζόμενους, αλλά αργότερα έως 1000 εργαζόμενους. Η HubSpot έθεσε 32 εκατομμύρια δολάρια σε πρόσθετη χρηματοδότηση επιχειρήσεων τον Φεβρουάριο του 2012 από την Sequoia Capital, το Google Ventures, Salesforce κ.α. Τον Μάρτιο του 2012, η HubSpot, απέκτησε την Google Chrome εταιρέια κέντρο κοινοποίησης. Στο Ετήσιο Συνέδριο Μάρκετινγκ του 2012, η HubSpot ανακοίνωσε ένα προϊόν λογισμικού για το προσωπικό πωλήσεων εντός της εταιρείας. Η HubSpot κατέθεσε ένα χρηματικό ποσό για μια αρχική δημόσια προσφορά με την Επιτροπή Κεφαλαιαγοράς στις 25 Αυγούστου 2014 για εισαγωγή στο Χρηματιστήριο Αξιών της Νέας Υόρκης υπό την HUBS σύμβολο ticker. Στο χώρο του μάρκετινγκ η HubSpot δημοσιεύει «Η αναφορά στο χώρο του εισερχόμενου μάρκετινγκ» ετησίως. Η έκθεση αυτή του 2012 διαπίστωσε ότι το 89%των επιχειρήσεων είναι η διατήρηση ή αύξηση των εισερχόμενων προϋπολογισμών του μάρκετινγκ τους. Το 2011 βρέθηκε ότι το 65 τοις εκατό των εταιρειών είχε ένα εταιρικό blog, πάνω από το 28% το προηγούμενο έτος. Επιπλέον, το 44% των εμπόρων δήλωσε ότι το Facebook ήταν κρίσιμης σημασίας για τη στρατηγική μάρκετινγκ τους από 24% το 2009. Η έκθεση του 2010 διαπίστωσε ότι το 77% των χρηστών του Διαδικτύου διαβάζουν blogs. Επίσης δημοσιεύει ένα μέλος της έκθεσης Twittersphere. Στην έκθεση Twittersphere έχει βρεθεί ότι τα προφίλ Twitter με μια εικόνα προσελκύει έξι φορές περισσότερους οπαδούς κατά μέσο όρο. Επιπλέον, η έρευνα HubSpot διαπίστωσαν ότι η Νέα Υόρκη, το Σικάγο, το Λος Άντζελες και το Λονδίνο ήταν οι κορυφαίες πόλεις tweeting στον κόσμο. Το 2008 η εταιρεία εκτιμάται ότι η Twitter

είχε 4 έως 5.000.000 χρήστες, το 30% των οποίων ήταν «καινούργια. Ακόμη η HubSpot παρέχει ένα προϊόν λογισμικού για εισερχόμενο μάρκετινγκ που ονομάζεται και αυτό HubSpot. Περιλαμβάνει εργαλεία για κοινωνικό μάρκετινγκ μέσων μαζικής ενημέρωσης το email marketing, διαχείριση περιεχομένου, ανάλυση των σελίδων και βελτιστοποίηση μηχανών αναζήτησης, μεταξύ άλλων. Η HubSpot σουίτα των online εργαλείων έχει τρεις κύριες εφαρμογές: εργαλεία διαχείρισης περιεχομένου για τη δημιουργία ή τη διαχείριση των blogs, τα πρότυπα, τις μορφές και τις καταληκτικές σελίδες.

Επίσης εφαρμογές βελτιστοποίησης της έκθεσης, βοηθούν το περιεχόμενο να βρεθεί, όπως μέσω της βελτιστοποίησης μηχανών αναζήτησης, όπως και να οδηγήσει στην παρακολούθηση για τη διαχείριση των e-mail marketing, τις αλληλεπιδράσεις των πελατών, τις συγκεκριμένες προοπτικές, αναφορές και αναλύσεις. Από το 2012, περίπου 8000 εταιρείες χρησιμοποιούν HubSpot και το 85% των πελατών είναι με έδρα τις ΗΠΑ. Η HubSpot έχει μια εταιρική κουλτούρα παρόμοια με πολλές εταιρείες τεχνολογίας για την Δυτική Ακτή των ΗΠΑ.

Κατά επανάληψη έχει ονομαστεί ως Best Place to Work από το Boston Business Journal. Η εταιρεία ξεκίνησε μια απεριόριστη πολιτική ημέρες διακοπών το 2010 και άρχισε ένα πρόγραμμα κατάρτισης των εργαζομένων, που ονομάζεται HubSpot Fellows Program, το ίδιο έτος. Η εκκίνηση HubSpot του προγράμματος ξεκίνησε το 2008 και σε ένα πρόγραμμα συνεργατών έγινε πλήρες ωράριο εργασίας τους. Μέχρι το 2011 το πρόγραμμα συνεργατών ήταν υπεύθυνη για το 20% των εσόδων HubSpot του. Επιπλέον η HubSpot προσφέρει ένα $ 2,500 ως γενναιοδωρία για την παραπομπή ενός επιτυχόντα,το οποίο αυξήθηκε σε $ 10,000 το 2011, ενώ η εταιρεία έψαχνε για HTML 5 προγραμματιστές. Ανώτερους νεοσύλλεκτους που προέρχονται από μεγάλες επιχειρήσεις προσφέρεται ένα "jailbreak" μπόνους των $ 1000 για κάθε χρόνο που δαπανάται σε μια μεγάλη εταιρεία. Τέλος υπάρχουν διάφορες τεχνικές για την αντιμετώπιση των spam κοινωνικής δικτύωσης. Πρώτη είναι να ελέγχει τις διευθύνσεις IP των spammers, δεύτερη είναι να εμποδίζει spammers που χρησιμοποιούν συγκεκριμένες λέξεις spam και τρίτο είναι η χρήση ενός τέστ αντίστροφου. [1] [16] [17]

3.3 Κακόβουλο λογισμικό

Κακόβουλο λογισμικό (malware) είναι ένας όρος για οποιαδήποτε λογισμικό που εγκαθίσταται στον υπολογιστή και εκτελεί ανεπιθύμητες εργασίες. Κακόβουλα προγράμματα μπορεί να κυμαίνονται από το να είναι απλές ενοχλήσεις (pop-up διαφημίσεις) ή βλάβες όπως (κλέψιμο κωδικών και δεδομένων ή να μολύνει άλλους υπολογιστές στο δίκτυο). Επιπλέον, ορισμένα τέτοιου είδους προγράμματα έχουν σχεδιαστεί για τη μετάδοση πληροφοριών σχετικά με το περιεχόμενο Web-περιήγηση, συνήθως σε διαφημιστές ή για άλλα συμφέροντα τρίτων εν αγνοία τους. Ορισμένες κατηγορίες κακόβουλων λογισμικών είναιοι εξείς:

1. Virus: Λογισμικό το οποίο μπορεί να εξαπλωθεί σε άλλους υπολογιστές ή έχουν προγραμματιστεί να βλάψουν έναν υπολογιστή με τη διαγραφή αρχείων, την επαναδιαμόρφωση του σκληρού δίσκου, ή χρησιμοποιώντας τη μνήμη του υπολογιστή.

2. Adware: Λογισμικό που υποστηρίζεται οικονομικά (ή στηρίζει οικονιμικά ένα άλλο πρόγραμμα) από την προβολή διαφημίσεων όταν είναι συνδεδεμένοι στο Διαδίκτυο.

3. Spyware: Λογισμικό που συγκεντρώνει κρυφά πληροφορίες και το μεταδίδει στα ενδιαφερόμενα μέρη. Τύποι των πληροφοριών που συγκεντρώνονται περιλαμβάνουν ιστοσελίδες που επισκέπτονται, το πρόγραμμα περιήγησης, το σύστημα πληροφόρησης και η διεύθυνση IP του υπολογιστή σας.

4. Browser λογισμικό πειρατεία: Λογισμικού διαφήμιση που τροποποιεί τις ρυθμίσεις του προγράμματος περιήγησης σας (π.χ. αρχική σελίδα προεπιλογή, γραμμές εργαλειών), δημιουργεί συντομεύσεις στην επιφάνεια εργασίας και εμφανίζει διαφημιστικά pop-ups. Επίσης μπορεί να ανακατευθύνει συνδέσεις με άλλες ιστοσελίδες που διαφημίζουν ή ιστοσελίδες που συλλέγουν πληροφορίες χρήσης Ιστού.

Θα ήταν χρήσιμο να αναφερθεί ότι το λογισμικό που έρχεται συσσωρευμένο με το «άλλο λογισμικό» συχνά αποκαλείται ως Δούρειος Ίππος. Για παράδειγμα, ένα λογισμικό ανταλλαγής άμεσων μηνυμάτων με ένα πρόγραμμα όπως WilTanget, ένα γνωστό spyware. Το λογισμικό peer-to-peer ανταλλαγής αρχείων, όπως Kaaza, το Lime Wire και το eMule, συνένωσης διαφόρων τύπων κακόβουλων λογισμικών

που κατηγοριοποιούνται ως spyware ή adware. Το λογισμικό που υπόσχεται να επιταχύνει τη σύνδεση στο Διαδίκτυο ή για να βοηθήσει διάφορες λήψεις (π.χ. αναζήτησης Ιστού) και αυτό περιέχει adware.

Επίσης, ένα κακόβουλο λογισμικό μπορεί να εκμεταλλευτεί τα κενά ασφάλειας στον browser για να εισβάλει στον υπολογιστή. Μερικές φορές ιστοσελίδες αναφέρουν ότι απαιτείται λογισμικό για να δουν το περιεχόμενο, σε μία προσπάθεια να ξεγελάσουν τους χρήστες να πατήσουν κλικ στο «NAI» και έτσι έχουν την εγκατάσταση του συγκεκριμένου λογισμικού στον υπολογιστή τους και μερικά δεν παρέχουν καμία επιλογή απεγκατάστασης ή τροποποίηση του λειτουργικού συστήματος καθιστώντας έτσι πιο δύσκολη την αφαίρεσή του. Το κακόβουλο πρόγραμμα, ή botnet, μπορεί να επιτάξει τα λειτουργικά συστήματα τόσο σε οικιακούς όσο και των εταιρικών συστημάτων πληροφορικής μέσω του Διαδικτύου.

Ο όρος botnet χρησιμοποιείται ευρέως όταν αρκετές bots IRC έχουν συνδεθεί και ενδεχομένως με τους τρόπους των καναλιών σε άλλα bots και τους χρήστες διατηρώντας παράλληλα κανάλια IRC δωρεάν από ανεπιθύμητους χρήστες. Αυτό είναι όπου ο όρος είναι αρχικά από, δεδομένου ότι οι πρώτες παράνομες botnets ήταν παρόμοια με νομική botnets. Μια κοινή bot που χρησιμοποιείται για τη δημιουργία botnets στο IRC. Οι υπολογιστές μπορούν να αφομοιωθούν σε ένα botnet που εκτελούν κακόβουλο λογισμικό. Αυτό μπορεί να επιτευχθεί με να δελεάσει τους χρήστες να κάνουν μια κίνηση μέσω λήψης, αξιοποιώνταςτα τρωτά σημεία του προγράμματος περιήγησης web, ή ξεγελώντας τον χρήστη ώστε να τρέξει ένα δούρειο ίππο πρόγραμμα, το οποίο μπορεί να προέρχεται από ένα συνημμένο ηλεκτρονικού ταχυδρομείου. Αυτό το κακόβουλο λογισμικό θα εγκαθιστήσει τυπικά ενότητες που επιτρέπουν στον υπολογιστή να διατάζεται και να μην ελέγχεται από το χειριστή του botnet του.

Πολλοί χρήστες ηλεκτρονικών υπολογιστών αγνοούν ότι ο υπολογιστής τους έχει μολυνθεί με bots. Ανάλογα με το πώς είναι γραμμένο, ένα Trojan μπορεί στη συνέχεια να διαγράψει το ίδιο, ή μπορεί να παραμείνει για να ενημερώσει και να διατηρήσει τις ενότητες. Η πρώτη botnet για πρώτη φορά αναγνώρισε και εκτίθεται από Earthlink κατά τη διάρκεια μιας δίκης με spammer Χαν C. Smith το 2001 για το σκοπό του χύμα spam που αντιπροσωπεύουν σχεδόν το 25% του συνόλου των

spam κατά το χρόνο. Τέτοια botnets χρησιμοποιούνται για μια σειρά από, δραστηριότητες παράνομες συμπεριλαμβανομένης της αποστολής spam e-mail, κλοπή ψηφιακών εγγράφων και κωδικούς πρόσβασης από μολυσμένους υπολογιστές. Η τρέχουσα μόλυνση είναι μικρή σε σύγκριση με μερικά από τα μεγαλύτερα γνωστά botnets.

Για παράδειγμα, ένα σύστημα γνωστό ως Conficker, που δημιουργήθηκε στα τέλη του 2008, έχει μολυνθεί όσο 15 εκατομμύρια υπολογιστές στο αποκορύφωμά της και συνεχίζει να μολύνει περισσότερους από επτά εκατομμύρια συστήματα παγκοσμίως. Οι botnet επιθέσεις δεν είναι ασυνήθιστες. Επί του παρόντος Shadow server, μια οργάνωση που παρακολουθεί δραστηριότητα botnet, παρακολουθεί 5.900 ξεχωριστό botnets. Η έρευνα της εταιρείας καθορίστηκε ότι το botnet ήταν σε θέση να θέσει σε κίνδυνο τις δύο εμπορικών και κυβερνητικών συστημάτων, συμπεριλαμβανομένων 68.000 εταιρικά διαπιστευτήρια σύνδεσης. Τέλος έχει επίσης αποκτήσει πρόσβαση σε συστήματα ηλεκτρονικού ταχυδρομείου, σε απευθείας σύνδεση τραπεζικούς λογαριασμούς το Facebook, το Yahoo, το Hotmail και άλλα διαπιστευτήρια κοινωνικών δικτύων, μαζί με περισσότερα από 2.000 πιστοποιητικά ψηφιακής ασφάλειας και ένα σημαντικό χώρο προσωρινής αποθήκευσης των προσωπικών πληροφοριών ταυτότητας. [18] [19] [20] [21]

3.3.1 Η λειτουργία του κακόβουλο λογισμικού

Ένα κακόβουλο λογισμικό μπορεί να εγκατασταθεί σε ένα σύστημα υπολογιστή με διάφορους τρόπους. Ένα επισόδιο του 2008 στο οποίο ένας παράγοντας ξένων μυστικών χρηαιμοποιεί μία μονάδα flash για να μολύνει τους υπολογιστές των αμερικών στρατιωτών, οι οποίοι χρησιμοποιούνταν από τη Κεντρική Διοίκηση. Με την εγκατάσταση στο λειτουργικό σύστημα, κρυπτογραφεί διάφορα αρχεία όπως έγγραφα, φωτογραφίες κ.α. Έπειτα, εμφανίζει ένα μήνυμα στον υπολογιστή που δείχνει ότι έχει μπλοκαριστεί και ενημερώνει το χρήστη ότι για να ξεμπλοκαριστεί ο υπολογιστής του θα πρέπει να καταβάλει κάποιο χρηματικό ποσό (ransom). Η πληρωμή γίνεται με ψηφιακό νόμισμα bitcoin και άν ο χρήστης-θύμα δεν διαθέτει, του παρέχουν κάποιες πληροφορίες αυτοί που δημιούργησαν το λογισμικό ώστε να τα αποκτήσει.

Το κακόβουλο λογισμικό δημιουργεί ένα ζεύγος ιδιωτικού και δημόσιου «κλειδιού» το οποίο αποτελείται ουσιαστικά από κωδικούς αριθμούς οι οποίοι ξεμπλοκάρουν τον μολυσμένο υπολογιστή. Το δημόσιο «κλειδί» αποθηκεύεται στο μολυσμένο σύστημα και δίνεται στο χρήστη χωρίς να πληρώσει, ενώ το ιδιωτικό «κλειδί» αποθηκεύεται στο διακομιστή διοίκησης και ελέγχου και το δίνουν στο θύμα-χρήστη για να αποκρυπτογραφήσουν τα αρχεία, μετά την καταβολή του χρηματικού ποσού που έχουν συμφωνήσει, σε ψηφιακό νόμισμα bitcoin. Ενώ Trojans και backdoors δεν είναι εύκολα ανιχνεύσιμες από τον εαυτό τους, οι υπολογιστές μπορεί να φαίνεται ότι τρέχουν πιο αργά λόγω της χρήσης του δικτύου. Κακόβουλα προγράμματα ταξινομούνται ως Trojans, αν δεν προσπαθούν να βλάψουν άλλα αρχεία (ιούς υπολογιστών) ή με άλλο τρόπο για να τους διαδίδουν οι ίδιοι (σκουλήκι). Ένας υπολογιστής μπορεί να φιλοξενήσει ένα Trojan μέσω ενός κακόβουλου προγράμματος που ένας χρήστης μπορεί να εξαπατηθεί (συχνά με ένα συνημμένο σε e-mail π.χ., ένα έντυπο που πρέπει να συμπληρωθεί). Η Δίωξη Ηλεκτρονικού Εγκλήματος ενημερώνει τους χρήστες του Διαδικτύου να είναι πρσεκτικοί και να ακολουθούν κάποια μέτρα:

1. Να έχουν ενημερωμένη την έκδοση του λειτουργικού συστήματος.
2. Αντίγραφα ασφαλείας σε εξωτερικό μέσο αποθήκευσης.
3. Να χρησιμοποιούν εφαρμογές ασφαλείας όπως antivirus.
4. Να μην κατεβάζουν συνημμένα αρχεία στα οποία δεν γνωρίζουν τον αποστολέα [22] [23] [24]

3.3.2 Ιοί

Ένας ιός υπολογιστών είναι ένα κακόβουλο λογισμικό πρόγραμμα που όταν εκτελεστεί, αναπαράγει εισάγοντας αντίγραφα του εαυτού του (ίσως τροποποιημένα) σε άλλα προγράμματα ηλεκτρονικού ταχυδρομείου, τα δεδομένα αρχεία ή τον τομέα εκκίνησης του σκληρού δίσκου. Όταν αυτή η αναπαραγωγή ολοκληρώνεται οι πληγείσες περιοχές στη συνέχεια μολύνονται. Οι ιοί συχνά εκτελούν κάποιο είδος επιβλαβούς δραστηριότητας σε μολυσμένους ξενιστές όπως η κλοπη του σκληρού δίσκου χώρου ή CPU χρόνου, την πρόσβαση σε ιδιωτικές πληροφορίες, διαφθείρει τα δεδομένα εμφανίζοντας πολιτική ή χιουμοριστικά

μηνύματα στην οθόνη του χρήστη, spamming, καταγραφή των πληκτρολογήσεων τους, ή ακόμα και καθιστώντας τον υπολογιστή άχρηστο.

Επίσης, πολλοί ιοί δημιουργούνται για να προξενήσουν ζημιά στον υπολογιστή, είτε καταστρέφοντας τα προγράμματα, με τη διαγραφή των αρχείων ή με τη μορφοποίηση (format) του σκληρού δίσκου. Ακόμη, άλλοι δεν έχουν σκοπό να δημιουργήσουν προβλήματα, απλά κάνουν εμφανή την παρουσία τους με διάφορα βίντεο ή ηχητικών μηνυμάτων. Ακόμα και αυτοί όμως οι ιοί δημιουργούν προβλήματα καταλαμβάνοντας μνήμη, ασταθή συμπεριφορά του συστήματος και κατάρρευσή του.

Η συντριπτική πλειοψηφία των ιών στοχεύει συστήματα που εκτελούν τα Microsoft Windows, χρησιμοποιώντας μια ποικιλία μηχανισμών για να μολύνουν νέους ξενιστές και χρησιμοποιώντας συχνά πολύπλοκες αντι-ανίχνευσης στρατηγικές για να αποφύγει το λογισμικό προστασίας από ιούς. Τα κίνητρα για τη δημιουργία ιών επιδιώκουν το κέρδος, την αποστολή ενός μηνύματος πολιτικού, την προσωπική διασκέδαση, να αποδείξουν ότι υπάρχει ένα θέμα ευπάθειας στο λογισμικό, για σαμποταζ και άρνηση υπηρεσίας, ή απλά επειδή επιθυμούν να διερευνήσουν την τεχνητή ζωή και τους εξελικτικούς αλγορίθμους.

Οι ιοί των υπολογιστών προκαλούν σήμερα δισεκατομμύρια δολάρια σε οικονομική ζημιά κάθε χρόνο, λόγω του ότι προκαλεί την αποτυχία των συστημάτων, σπαταλώντας τους πόρους του υπολογιστή, διαφθείρει τα δεδομένα κλπ. Τέλος, ένα μεγάλο ποσοστό των ιών δεν έχει μόνο ως σκοπό την καταστροφή των δεδομένων, αλλά την κλοπή των δεδομένων του κάθε χρήστη ή την εισαγωγή του σε κάποιο παράνομο δίκτυο χώρις την έγκριση από το χρήστη.

Η πλειοψηφία των ιών στοχεύει σε συστήματα που που εκτελούνται τα Microsoft Windows. Αυτό οφείλεται στο μεγάλο μερίδιο αγοράς της Microsoft στην επιφάνεια εργασίας των χρηστών. Η ποικιλομορφία των συστημάτων λογισμικού σε ένα δίκτυο περιορίζει τις καταστροφικές δυνατότητες των ιών και κακόβουλων προγραμμάτων. Λειτουργικά συστήματα όπως το Linux επιτρέπει στους χρήστες να επιλέξουν από μια ποικιλία του περιβάλλοντα εργασίας, εργαλεία συσκευασίας κ.λπ., που σημαίνει ότι το κακόβουλο πρόγραμμα στοχεύει σε οποιαδήποτε από αυτά τα συστήματα και θα επηρεάσει μόνο ένα υποσύνολο του συνόλου των χρηστών.

Πολλοί χρήστες των Windows τρέχουν το ίδιο σύνολο των εφαρμογών, ώστε οι ιοί να εξαπλωθούν γρήγορα ανάμεσα σε συστήματα Windows. Μόνο λίγοι ιοί έχουν χτυπήσει Macs τα τελευταία χρόνια. Η διαφορά στην ευπάθεια του ιού μεταξύ Mac και Windows είναι επικεφαλής σημείο πώλησης. Ενώ το Linux (και Unix γενικά) εμπόδισαν τους χρήστες να κάνουν αλλαγές στο περιβάλλον του λειτουργικού συστήματος χωρίς άδεια, ενώ οι χρήστες των Windows μπορούν να κάνουν αυτές τις αλλαγές πράγμα που σημαίνει ότι οι ιοί μπορούν εύκολα να αποκτήσουν τον έλεγχο ολόκληρου του συστήματος στα Windows.

Επίσης, οι ιοί υπολογιστών μολύνουν μια ποικιλία διαφορετικών υποσυστημάτων για τους οικοδεσπότες τους. Ένας τρόπος ταξινόμησης των ιών είναι να εξεταστεί αν κατοικούν σε εκτελέσιμα αρχεία (Exe), αρχεία δεδομένων όπως (PDF) ή στοντομέα εκκίνησης σκληρού δίσκου (ή κάποιος συνδυασμός όλων αυτών). Οι ιοί μπορούν να ταξινομηθούν ως μόνιμοι κάτοικοι ή μη μόνιμοι κάτοικοι με βάση τον τρόπο που μολύνει τα αρχεία. Ένας μη-κάτοικος του ιού ψάχνει για νέα αρχεία ώστε να τα μολύνει. Ένας ιός που κατοικεί κατά την εκτέλεση φορτώνει στη μνήμη μια ενότητα που μολύνει τα αρχεία, και εξασφαλίζει για να εκτελεστεί κάθε φορά το λειτουργικό σύστημα, που εκτελεί μία συγκεκριμένη λειτουργία. Αντίθετα οι ιοί μόνιμοι κάτοικοι έχουν σχεδιαστεί για να μολύνουν όλους τους πιθανούς χρήστες «οικοδεσπότες» που έρχονται σε επαφή. Για παράδειγμα, ένας τέτοιος ιός μπορεί να συνδεθεί με ένα πρόγραμμα ανίχνευσης ιών που ελέγχει όλα τα αρχεία στο σύστημα του υπολογιστή, και μολύνει όλα τα αρχεία που ελέγχονται. Πολλοί χρήστες εγκαθιστούν λογισμικό προστασίας από ιούς. Οι χρήστες πρέπει να ενημερώνουν το λογισμικό τους τακτικά ώστε να αναγνωρίζουν τις πιο πρόσφατες απειλές.

Επιπλέον, υπάρχουν δύο κοινές μέθοδοι που χρησιμοποιεί μια εφαρμογή λογισμικού προστασίας από ιούς για την ανίχνευσή τους. Η πρώτη και η πιο κοινή μέθοδος ανίχνευσης ιών γίνεται με την εξέταση του περιεχομένου της μνήμης του υπολογιστή (μνήμης RAM) και τα αρχεία που είναι αποθηκευμένα σε σταθερές ή αφαιρούμενες μονάδες δίσκου συγκρίνοντας τα αρχεία βάσεων δεδομένων του ιού. Το μειονέκτημά της είναι όμως ότι δεν προστατεύονται από νέους ιούς. Μια δεύτερη μέθοδος για να βρουν τους ιούς είναι να χρησιμοποιήσουν ένα ευρετικό αλγόριθμο που βασίζεται σε κοινές συμπεριφορές του ιού. Αυτή η μέθοδος έχει τη δυνατότητα να εντοπίζουν νέους ιούς για τους οποίους οι επιχειρήσεις προστασίας

δεν έχουν ακόμη καθορίσει μια «υπογραφή», και οδηγεί σε περισσότερα ψευδή αποτελέσματα από τη χρήση υπογραφών. Κάποιος μπορεί επίσης να μειώσει τη ζημία που γίνεται από τους ιούς κάνοντας τακτικά αντίγραγα ασφαλείας των δεδομένων (και τα λειτουργικά συστήματα) με διαφορετικά μέσα, που κρατούνται στο σύστημα (τις περισσότερες φορές). Με αυτό τον τρόπο, αν τα δεδομένα χάνονται μέσα από έναν ιό, μπορεί κανείς να ξεκινήσει και πάλι χρησιμοποιώντας το αντίγραφο ασφαλείας. Όμοίως, ένα λειτουργικό σύστημα σε ένα bootable CD μπορεί να χρησιμοποιηθεί για την εκκίνηση του υπολογιστή, εάν τα εγκατεστημένα λειτουργικά συστήματα έχουν καταστεί άχρηστα. Αντίγραφα ασφαλείας σε αφαιρούμενα μέσα πρέπει να επιθεωρούνται με προσοχή πριν από την αποκατάσταση.

Ο ιός Gammima, για παράδειγμα, διαδίδεται μέσω αφαιρούμενων δίσκων. Πολλές ιστοσελίδες που διαχειρίζονται οι εταιρείες λογισμικού αντιμετώπισης ιών λογισμικού παρέχουν δωρεάν σάρωση σε απευθείας σύνδεση του ιού, με περιορισμένες εγκαταστάσεις καθαρισμού (ο σκοπός των χώρων είναι να πωλούν τα προϊόντα antivirus). Ορισμένες ιστοσελίδες όπως θυγατρική Google Virus Total που επιτρέπουν στους χρήστες να ανεβάζουν ένα ή περισσότερα ύποπτα αρχεία που θέλουν να σαρώσουν και να ελέγχουν από ένα ή περισσότερα προγράμματα προστασίας από ιούς σε μία λειτουργία. Επιπλέον, πολλά ικανά προγράμματα λογισμικού προστασίας από ιούς είναι διαθέσιμα για δωρεάν download από το Internet (συνήθως περιορίζεται σε μη εμπορική χρήση).

Η Microsoft προσφέρει μια προαιρετική χρησιμότητα δωρεάν antivirus που ονομάζεται, Microsoft Security Essentials ένα εργαλείο αφαίρεσης κακόβουλου λογισμικού των Windows που ενημερώνεται ως μέρος του κανονικού καθεστώτος του Windows Update, και μεγαλύτερης ηλικίας προαιρετικό anti-malware (απομάκρυνση του κακόβουλου λογισμικού) εργαλείο Windows Defender που έχει αναβαθμιστεί σε ένα προϊόν εντοπισμού ιών στα Windows8. Μερικοί ιοί απενεργοποιούν την επαναφορά συστήματος και άλλα σημαντικά εργαλεία των Windows, όπως Διαχείριση Εργασιών. Πολλοί τέτοιοι ιοί μπορούν να αφαιρεθούν από την επανεκκίνηση του υπολογιστή, εισάγοντας τα Windows με τη δικτύωση, και στη συνέχεια, χρησιμοποιώντας τα εργαλεία του συστήματος ή τα Microsoft συστήματα ασφαλείας. Συχνά ένας ιός θα προκαλέσει ένα σύστημα για να κρεμάσει, και μια επακόλουθη σκληρή επανεκκίνηση θα καταστήσει ένα σημείο

επαναφοράς συστήματος από την ίδια ημέρα διεφθαρμένη. Επαναφορά στα σημεία από την προηγούμενη ημέρα θα πρέπει να εργαστούν υπό την προϋπόθεση ότι ο ιός δεν έχει σχεδιαστεί για να αλλοιώσει τα αρχεία. [1] [25] [26]

3.3.3 Worms

Ένας ιός τύπου worm είναι ένα αυτόνομο malware πρόγραμμα υπολογιστή που αναπαράγει τον εαυτό του, προκειμένου να εξαπλωθεί και σε άλλους υπολογιστές. Είναι ένα αυτοαναπαραγόμενο και κακόβουλο πρόγραμμα υπολογιστή που χρησιμοποιεί διάφορα δίκτυα υπολογιστών για να στείλει κάποια αντίγραφα του εαυτού του σε άλλα δίκτυα υπολογιστών (κόμβους) χωρίς τη θέληση και την παρέμβαση του χρήστη. Πολλές φορές το σκουλήκι (worm) με τον ιό (virus) συγχέεται λόγω του ότι έχουν αρκετές ομοιότητες στη λειτουργία τους. Συχνά, χρησιμοποιεί ένα δίκτυο υπολογιστών για να εξαπλωθεί η ίδια. Σε αντίθεση με έναν ιό υπολογιστή, δεν χρειάζεται να συνδεθεί με ένα υπάρχον πρόγραμμα. Τα σκουλήκια σχεδόν πάντα προκαλούν τουλάχιστον κάποια βλάβη στο δίκτυο, έστω και μόνο με την κατανάλωση εύρους ζώνης, ενώ οι ιοί σχεδόν πάντα τροποποιούν αρχεία σε έναν υπολογιστή και το δίκτυο παραμένει αβλαβές. Πολλά σκουλήκια που έχουν δημιουργηθεί έχουν σχεδιαστεί μόνο για να εξαπλωθούν και δεν προσπαθούν να αλλάξουν τα συστήματα που διέρχονται.

Ωστόσο,το σκουλήκι Morris και Mydoom μπορούν να προκαλέσουν σοβαρές διαταραχές από την αύξηση της κυκλοφορίας του δικτύου και άλλες απρόβλεπτες συνέπειες. Η Mydoom είναι επίσης γνωστή ως W32.MyDoom@mm, Novarg, Mimail.R και Shimgapi που επηρεάζει τα Microsoft Windows. Μεταδίδεται κυρίως μέσω e-mail, εμφανίζεται ως ένα σφάλμα μετάδοσης. Το μήνυμα περιέχει ένα συνημμένο αρχείο που όταν εκτελεστεί ξαναστέλνει το σκουλήκι (worm).

Επίσης, ένα «ωφέλιμο φορτίο» είναι ο κωδικός του worm σχεδιασμένο να κάνει περισσότερα από την εξαπλώση του σκουλήκιου, να διαγράψει τα αρχεία σε ένα σύστημα υποδοχής (π.χ., η ExploreZip σκουλήκι), κρυπτογράφηση των αρχείων, ή να στείλει έγγραφα μέσω e-mail. Ένα πολύ συχνά ωφέλιμο φορτίο για τα σκουλήκια είναι να εγκαταστήσει μια κερκόπορτα στον μολυσμένο υπολογιστή για να επιτρέψει τη δημιουργία ενός «ζόμπι» υπό τον έλεγχο του συγγραφέα σκουλήκι. Τα δίκτυα τέτοιων μηχανών που συχνά αναφέρονται ως botnets και

χρησιμοποιούνται πολύ συχνά από τους spam αποστολείς για την αποστολή ανεπιθύμητης αλληλογραφίας ή στην διεύθυνση της ιστοσελίδας τους.

Οι spammers εκ τούτου θεωρείται ότι είναι μια πηγή χρηματοδότησης για τη δημιουργία αυτών των σκουληκιών. Οι χρήστες μπορούν να ελαχιστοποιήσουν την απειλή από τα σκουλήκια, διατηρώντας το λειτουργικό σύστημα των υπολογιστών τους και άλλο λογισμικό, αποφεύγοντας το άνοιγμα μη αναγνωρισθέντα μηνύματα ηλεκτρονικού ταχυδρομείου, καθώς και τη λειτουργία firewall και antivirus λογισμικού. Θα ήταν χρήσιμο να αναφερθεί, πως υπάρχουν και σκουλήκια καλού σκοπού, όπως το Nachi που προσπάθησε να κατεβάσει και να εγκαταστήσει ενημερωμένες εκδόσεις κώδικα από την ιστοσελίδα Microsoft, για να διορθώσει τα τρωτά σημεία του συστήματος. Αν και με αυτόν τον τρόπο τα συστήματα έγιναν πιο ασφαλή, δημιουργήθηκε πρόβλημα στην κυκλοφορία των δικτύων, που είχε ως αποτέλεσμα την επανεκκίνηση του συστήματος, χωρίς την άδεια του χρήστη. Επίσης, πολλά σκουλήκια (worms), όπως XSS (worm) σκουλήκια έχουν δημιουργηθεί για να την έρευνα εξάπλωσής τους (κοινωνική δραστηριότητα, αλλαγή συμπεριφορά χρηστών). Θα ήταν χρήσιμο να αναφερθεί, πως και μια άλλη ερευνητική ομάδα πρότεινε το πρώτο σκουλήκι που λειτουργεί με το δεύτερο επίπεδο του μοντέλο OSI για να διερευνήσει τους ευάλωτους κόμβους και όλο το δίκτυο της επιχείρησης του να είναι καλυμμένο. [27] [28] [29]

3.3.4 Δούρειος Ίππος

Εμπνευσμένη η ονομασία του από την Ελληνική μυθολογία ο Δούρειος Ίππος, είναι ένα κακόβουλο πρόγραμμα που σκοπό έχει την κρυφή «είσοδο» στον υπολογιστή μας όπως οι Αχαιοί στην Τροία. Πρώτη εμφάνιση του «Δούρειου Ίππου» ήταν το 1983 σε μια ομιλία του Κέν Τόμσον στην τελετή απονομής των βραβείων Turing. Η τακτική του Trojan είναι να γίνεται η εγκατάσταση ενός προγράμματος από τον χρήστη και όταν εκείνος το ανοίξει τότε ξεκινάει η δράση του κακόβουλου κώδικα με αποτέλεσμα την μόλυνση του υπολογιστή μας. Τα Trojans μπορούμε να τα συναντήσουμε και με την ονομασία backdoor. Με όποια ονομασία και αν τα βρούμε παραμένει το ίδιο κακόβουλο για τα αρχεία μας και τον υπολογιστή μας. Οι υπολογιστές που είναι μολυσμένοι με κάποιο Trojan, ονομάζονται botnet, δηλαδή υπολογιστές που χρησιμοποιούνται εν άγνοια των χρηστών τους.

Υπάρχουν δυο τύποι Δούρειων Ίππων: τα πρώτα αποτελούνται από κανονικά προγράμματα που τα αλλάζουν χάκερς προσθέτοντας έτσι κακόβουλο κώδικα. Τέτοια προγράμματα είναι εκείνα που βοηθούν στην ανταλλαγή αρχείων (peer-to-peer). Η δεύτερη μορφή του Δούρειου Ίππου είναι με μεμονωμένα προγράμματα που σκοπό έχουν να κάνουν τον χρήστη να νομίζει πως πρόκειται το πρόγραμμα που εκτελεί για κάποιο παιχνίδι η εικόνα. Τα Trojan σε σχέση με άλλα προγράμματα ίδιου περιεχόμενου (worms, ιούς κ.α.) εξαρτώνται από το χρήστη και τις ενέργειες του. Μπορούμε να χωρίσουμε τον Δούρειο Ίππο σε περισσότερες κατηγορίες όπως είναι :

1) Απομακρυσμένη πρόσβαση
2) E-mail
3) Καταστροφή αρχείων
4) Κατέβασμα αρχείων
5) Proxy Trojan
6) FTP Trojan
7) Απενεργοποίηση firewall, antivirus
8) Επιθέσεις άρνησης υπηρεσιών (DoS)
9) URL Trojan

Με τα Trojans οι χάκερς μπορούν να ελέγχουν την κάθε κίνηση μας στον υπολογιστή μας καθώς και οι ίδιοι να κάνουν ενέργειες στον υπολογιστή μας την ίδια στιγμή, φαινόμενο σπάνιο γιατί δεν θέλουν να γίνουν αντιληπτοί. Οι πιο γνωστοί Δούρειοι Ίπποι είναι οι εξής :

1. Downloader- EV
2. Dropper – EV
3. Pest trap
4. Y3K Remote Administration Tool (φτιαγμένο από Έλληνες)
5. NetBus
6. Flooder
7. Tagasaurus
8. Vundo Trojan
9. Gromozon Troja
10. Sub-7

11. Cuteqq_Cn.exe

Τα Trojan μπορούμε να τα καταπολεμήσουμε με τα Antivirus όπως είναι τα: McAfee, Norton που είναι τα πιο αξιόπιστα καθώς και τα AVP και τα TrendMicro. Χρήσιμες είναι και ιστοσελίδες όπως είναι η http://www.grc.com που βοηθούν βήμα-βήμα για να ελέγξουμε τον υπολογιστή μας για τυχόν μολυσμένα αρχεία καθώς και να ρυθμίσουμε κάποια firewall για παραπάνω προστασία. [30][31][32][33]

3.3.5 Spyware

Το spyware είναι λογισμικό κατασκοπίας όπως προκύπτει και από την ονομασία του. Η φόρτωση του γίνεται και σε αυτήν την περίπτωση επίθεσης κρυφά, εν άγνοια δηλαδή του χρήστη. Σκοπός του είναι να μην μπορέσει κάποιος να το αναγνωρίσει έτσι ώστε να μπορεί να συγκεντρώσει στοιχεία όπως διευθύνσεις e-mails, κωδικούς πρόσβασης κωδικούς από κάρτες πιστωτικές και άλλα. Το spyware μπορεί να επηρεάσει τον υπολογιστή μας αλλάζοντας τον browser. Πιο συνοπτικά μπορούμε να αναφέρουμε τις κύριες δραστηριότητες του spywareπιο κάτω :

1) Αλλαγή της αρχικής σελίδας του browser
2) Τροποποίηση της λίστας αγαπημένων σελιδοδεικτών του browser
3) Προσθέτει νέες γραμμές εργαλείων
4) Εμφάνιση ανεπιθύμητων διαφημίσεων
5) Με την εκκίνηση του υπολογιστή ενεργοποιείτε και το spywareto όποιο λαμβάνει μνήμη από τον υπολογιστή
6) Μπορεί να απενεργοποιήσει το firewall

Οι κατηγορίες spyware είναι 3:

1. Στο marketingόπου γίνεται συλλογή πληροφοριών και αποστολή αυτών στον προγραμματιστή με σκοπό την καλύτερη στόχευση των διαφημίσεων .
2. Στην παρακολούθηση, όπου στελέχη εταιριών τα εγκαθιστούν εσκεμμένα ελέγχοντας τον ισότοπο που επισκέπτονται οι υπάλληλοι .
3. Στην τελευταία κατηγορία είναι σαν να έχουμε μια μολυσμένη μηχανή αναζήτησης μετατρεπόμενη σε μια στρατιά από ζόμπι.

Η μόλυνση στον υπολογιστή μας μπορεί να προσέλθει από:

1. Με εγκατάσταση προγραμμάτων.
2. Με εγκατάσταση πρόσθετων.
3. Με επίσκεψη wed sites.

Για να αποτρέψουμε την επίθεση στον υπολογιστή μας είναι απαραίτητο να πραγματοποιήσουμε κάποιες σημαντικές ενέργειες όπως είναι οι εξής:

1. Να έχουμε σε ισχύ κάποιο ενημερωμένο λογισμικό προστασίας.
2. Να κάνουμε τις απαραίτητες ενημερώσεις που αφορούν την ασφάλεια του υπολογιστή μας.
3. Θα πρέπει πάντα να διαβάζουμε τις άδειες χρήσης του προγράμματος που πρόκειται να κάνουμε εγκατάσταση.
4. Να είμαστε προσεκτικοί στις διαφημίσεις που κλατάρουμε.
5. Να ελέγχουμε τα αρχεία που κάνουμε download.

Τέλος, όταν γίνει αντιληπτό το spyware ο καλύτερος τρόπος αντιμετώπισης-αφαίρεσης του είναι να τρέξουμε την εκτέλεση κάποιου ενημερωμένου λογισμικού ασφάλειας.[34][35][36].

3.3.6 Adware

Το Adware, πρόκειται για λογισμικό μη κακόβουλο για τον υπολογιστή μας. Η ιδιότητα του είναι να μας εμφανίζει διαφημίσεις, πολλές φορές ανεπιθύμητες για εμάς, που σκοπό έχουν να επωφεληθούν οικονομικά οι δημιουργοί τους. Η εμφάνιση τους μπορεί να γίνει χωρίς να είναι απαραίτητη η σύνδεση μας στο internet. Η διαδικασία που χρειάζεται για την αφαίρεση τους είναι η εγκατάσταση κάποιου λογισμικού antivirus καθώς και κάποια έξτρα που παρέχονται από συγκεκριμένους browsersόπως είναι για παράδειγμα το Adblock για το chrome, όπου απαγορεύει την εμφάνιση διαφημίσεων.[37][38]

3.3.7 Τεχνολογίες αντιμετώπισης των κακόβουλων προγραμμάτων

Στις προηγούμενες ενότητες έχουμε αναφερθεί για την κάθε κατηγορία ξεχωριστά τους τρόπους αντιμετώπισης τους. Ένα γενικό τελικό συμπέρασμα για

τις τεχνολογίες αντιμετώπισης μπορούμε να πούμε ότι είναι η πιο αξιόπιστη λύση η χρήση των antivirus. Τα πιο αξιόπιστα antivirus είναι τα εξής:

1. McAfee
2. Kaspersky
3. Norton
4. Avast
5. AVG
6. Avira
7. Panda

3.4 Hacking

Το hacking είναι η εισβολή από προγραμματιστές σε υπολογιστικά συστήματα. Οι προγραμματιστές αυτοί έχουν την ονομασία hackers. Τους διακρίνουμε σε δυο κατηγορίες όπου μπορούν να εργαστούν. Άλλες φορές μόνοι τους και άλλες φορές σε ομάδες. Υπάρχουν περιπτώσεις που μπορούμε να τους βρούμε και με την ονομασία crackers. Η διαφορά τους είναι ότι οι crackers έχουν κακόβουλο χαρακτήρα.

Σε αντίθεση το hacking δεν είναι απαραίτητα επίθεση κακόβουλου χαρακτήρα. Υπάρχουν πολλές περιπτώσεις hackers να εργάζονται σε μεγάλες εταιρίες, οργανισμούς, ακόμα και για χάρη της κυβέρνησης, διεισδύοντας στα αντίστοιχα πληροφοριακά τους συστήματα και στους serversπου διαθέτουν για να ανακαλύψουν και να διορθώσουν τυχόν κενά που μπορεί ν υπάρχουν. Οι λόγοι που γίνονται αυτές οι ενέργειες είναι για να δυσκολέψουν την πρόσβαση από άλλους hackers και για να υπάρχει μεγαλύτερη σιγουριά και ασφάλεια στις πληροφορίες που έχουν στα πληροφοριακά τους συστήματα.

Η πρώτη εμφάνιση του hacking ξεκινά το 1960 από φοιτητές του MIT. Το αίτιο που έκανε τους φοιτητές να ασχοληθούν με το hacking ήταν, ότι λόγο της χρήσης- διάθεσης υπολογιστών mainframe (μηχανήματα κλειδωμένα σε δωμάτια με ελεγχόμενη θερμοκρασία), περιορίζοντα τους σε κάποιο συγκεκριμένο χρονικό όριο χρήσης καθώς και το μεγάλο κόστος που υπήρχε για την χρήση τους, να δημιουργήσουν τα πρώτα hacks. Τα hacks αποτελούσαν προγράμματα που

βοηθούσαν στο να γίνονται πιο γρήγορα υπολογισμοί με αποτέλεσμα να κερδίσουν όσο πιο πολύ χρόνο μπορούσαν καθώς και να μειώσουν το κόστος χρήσης που είναι πολύτιμο. Αξίζει να αναφερθεί ότι κάποιο από τα μεγαλύτερα hacks που υπάρχει έως και σήμερα είναι το UNIX. Το UNIX ήταν αποτέλεσμα από τον συνδυασμό εντολών με σκοπό την αύξηση της ταχύτητας των υπολογιστών. Αυτό το κατάφεραν δυο υπάλληλοι της εταιρίας Bell το έτος 1969.

Κατά την δεκαετία 70΄-80΄ και ύστερα, το hacking άλλαξε χαρακτήρα χρήσης και χρησιμοποιούνταν πλέον για να κάνουν υποκλοπές σε πληροφοριακά συστήματα, τηλεφωνικές συσκευές. Στόχος των hackers έγιναν μεγάλες εταιρείες όπως είναι: Google, Adobe, NOKIA, Fujitsu, Motorola. Επίσης κάποιος άλλος σημαντικός στόχος τους υπήρξε το Υπουργείο Αμύνης της Αμερικής. Προς το τέλος της δεκαετίας του 80΄, το hacking θεωρήθηκε ως μια πράξη παράνομη και εγκληματική σύμφωνα με τον νόμο που δημιουργήθηκε στο Κογκρέσο της Αμερικής. Στη συνεχεία το έτος 1988 ο πρώτος hacker που τιμωρήθηκε με βάση την νομοθεσία, ήταν ο Robert Morris ο οποίος έκανε εισβολή σε 6000 συνδεδεμένους υπολογιστές. Η ποινή του ήταν πρόστιμο αξίας 10.000 δολάρια καθώς και η προσφορά του με ατελείωτες ώρες εργασίας σε δημόσια έργα. Πλέον το hacking είναι εγκληματική ενέργεια.

Μερικοί από τους πιο γνωστούς hackers στην ιστορία είναι οι εξής:

1. Kevin Mitnick: Ξεκίνησε δημιουργώντας πλαστές κάρτες λεωφορείων για δωρεάν μετακίνηση. Στη συνεχεία στράφηκε ως προς την κινητή τηλεφωνία κλέβοντας λογισμικά. Το τέλος της πορείας του ήρθε στην απόπειρα του να παραβιάσει το σύστημα άλλου hacker. Πλέον, εργάζεται ως υπεύθυνος ασφαλείας πληροφοριακών συστημάτων, σχολιαστής και σύμβουλος.
2. Adrian Lamo: Δεύτερο του όνομα στο χώρο του hacking είναι το «άστεγος hacker» για τον λόγο ότι η κάθε ενέργεια του πραγματοποιούταν από διαφορετική τοποθεσία ώστε να είναι δύσκολος ο εντοπισμός του με βάση την IP του διεύθυνση. Ο στόχος του ήταν τα πληροφοριακά συστήματα της Microsoft, της NewYorkTime, της Yahoo, της Citigroup καθώς και της τράπεζας της Αμερικής . Η ποινή του ήταν δυο χρόνια φυλάκισης.

3. Jonathan James: Στην παιδική του ηλικία και συγκεκριμένα στο 16^{ο} έτος του, συλλαμβάνεται για ηλεκτρονικό έγκλημα, κερδίζοντας τον τίτλο του πρώτου ανήλικου hacker που καταδικάζεται. Οι στόχοι του ήταν η NASA και το υπουργείο Δικαιοσύνης.
4. Robert Tappan Morris: Δημιουργός του worms με σκοπό της ύπαρξης του να παρατηρήσει το μέγεθος του internetτην εποχή εκείνη. Εκποίησε ποινή φυλάκισης 3 ετών με αναστολή, πρόστιμο 10.500 δολάρια και 400 ώρες προσωπικής κοινωνικής εργασίας .
5. Kevin Poulsen: Εισβολέας στο τηλεφωνικό κέντρο του ραδιοφωνικού σταθμού KISS-FM του Λος Άντζελας συμμετέχοντας και κερδίζοντας παράνομα στους διαγωνισμούς του σταθμού. Ένα από τα μεγαλύτερα δώρα που κέρδισε με τον τρόπο αυτό ήταν ένα αυτοκίνητο της εταιρείας Porche. Συνελήφθει από το FBI στην προσπάθεια του να παραβιάσει το πληροφοριακό τους σύστημα . Καταδικάστηκε σε 5 χρόνια φυλάκισης καθώς ταυτόχρονα δούλευε ως δημοσιογράφοςκαι αργότερα εκδότης των Wired News.

3.4.1 Η λειτουργία του hacking

Για να πραγματοποιηθεί το hacking είναι απαραίτητο να μεσολαβήσουν δυο στάδια:

1. Προκατασκευαστικό στάδιο
2. Κύριο στάδιο

Το προκατασκευαστικό στάδιο είναι το 1^{ο} βήμα που ξεκινούν οι hackers και θα συλλέξουν πληροφορίες για το σύστημα που πρόκειται να κάνουν επίθεση. Θα προσπαθήσουν να αποσπάσουν κωδικούς από κάποιον που είναι ήδη χρήστης στο σύστημα, με αποτέλεσμα να έχουν το δικαίωμα πρόσβασης στο σύστημα.

Στο κύριο στάδιο, οι hackers πλέον τελειοποιούν τον σκοπό τους και αποχωρούν από το σύστημα αφήνοντας όσο το δυνατόν λιγότερες πληροφορίες για την επίθεση τους ώστε να μην γίνουν αντιληπτοί. Συγχρόνως απαραίτητο είναι να μπορούν να κάνουν επανασύνδεση στο σύστημα όποτε αυτό είναι επιθυμητό.

Επιπλέον τρόποι επίθεσης των hackers είναι:

1. Sniffer
2. Denial of service
3. Distributed denial of service
4. DNS spoofing
5. Packet sniffers
6. Οι Δούρειοι ίπποι που έχουμε αναφερθεί σε προηγούμενο κεφάλαιο καθώς και οι
7. Ιοί και worms.

Η μέθοδος sniffer πρόκειται για πρόγραμμα που εισχωρεί σε κάποιο σύστημα χωρίς να γίνει αντιληπτό από τον ιδιοκτήτη του και πραγματοποιεί έρευνα στα αρχεία, συλλέγοντας πληροφορίες.

Το Denial of service το χρησιμοποιούν οι hackers τρέχοντας ταυτόχρονα πολλά προγράμματα και.στέλνοντας αυτόματα μηνύματα δημιουργώντας υπερφόρτωση του συστήματος και έλλειψη ανταπόκρισης αυτού.

Με την χρήση του Distributed denial of service οι hackers έχοντας εισχωρήσει σε πολλούς ανυποψίαστους ηλεκτρονικούς χρήστες, αποστέλλουν ταυτόχρονα αιτήματα σε κάποιο σύστημα, με αποτέλεσμα να μην μπορεί να ανταπεξέλθει λόγο του μεγάλου αριθμού αιτημάτων ζήτησης και να προκύπτει έτσι το σύστημα να καταρρέει.

Στην περίπτωση του DNS spoofing οι hackers κάνουν τροποποίηση του Domain Name Code του site. Έτσι σε περίπτωση που κάποιος χρήστης γράψει κάποια λάθος διεύθυνση ή παραπλήσια αυτής που θέλει, τότε είναι πιθανό να οδηγηθεί σε κάποια απομίμηση αυτής που ζητούσε αρχικά, με αποτέλεσμα οι hackers να έχουν την δυνατότητα να ερευνήσουν τα προσωπικά δεδομένα καθώς και να πάρουν κωδικούς και άλλα στοιχειά που θα του φάνουν χρήσιμα, από τους ανυποψίαστους χρήστε.

Τα packetsniffers είναι προγράμματα που δίνουν την δυνατότητα στους hackers να λαμβάνουν πακέτα δεδομένων όπως είναι τα ονόματα χρηστών, κωδικούς εισόδου, ηλεκτρονικές διευθύνσεις, διευθύνσεις ηλεκτρονικού ταχυδρομείου κλπ, κάνοντας έτσι το έργο τους πιο εύκολο.[40][41]

3.4.2 Exploitation of weak authentication

Στην ενότητα αυτή γίνεται αναφορά στους κωδικούς που χρησιμοποιούνται συχνά, και στον τρόπο ώστε ο κωδικός μας να είναι πιο ισχυρός.

Από το ξεκίνημα του διαδικτύου η πιο συχνή εμφάνιση κωδικού ήταν το «12345». Δηλαδή αποτελούταν από μια σειρά αριθμών που είναι εύκολο για τους hackers να τον εντοπίσουν και να τον σπάσουν. Στις μέρες μας υπάρχουν ακόμα χρήστες που έχουν τέτοιους κωδικούς, με την διάφορα ότι προσθέτουν ένα επιπλέον ψηφίο. Το 6, και πλέον είναι ο εξής κωδικός «123456». Έτσι ο κωδικός γίνεται πιο ασφαλής αλλά και πάλι είναι μια εύκολη δουλειά για τους hackers να τον μαντέψουν και να αποκτήσουν πρόσβαση στα προσωπικά μας δεδομένα.

Έρευνα δείχνει ότι ένας στους πέντε χρήστες του Παγκοσμίου Ιστού χρησιμοποιούν πολύ εύκολους κωδικούς και συμφώνα με το άρθρο παρομοιάζει την προτίμηση αυτή με την τοποθέτηση του κλειδιού της πόρτας ενός σπιτιού κάτω από το χαλάκι της εισόδου. Θέλει να μας δείξει με την αναφορά αυτή ότι όσο ασφαλές μπορεί να είναι η τοποθέτηση του κλειδιού στο χαλάκι άλλο τόσο μπορεί να είναι ασφαλές η χρήση ενός εύκολου κωδικού πρόσβασης.

Σε πολλά sites όπου είναι απαραίτητο να είσαι μέλος για να σερφάρεις στο περιβάλλον τους, χρειάζεται να έχεις ένα όνομα χρηστή καθώς και έναν μοναδικό κωδικό πρόσβασης. Συχνά στο πεδίο συμπλήρωσης του κωδικού πρόσβασης αποτρέπει ο server, τον χρήστη να αποκτήσει κάποιον κωδικό που προτείνει για τον λόγο ότι μπορεί να χρησιμοποιείται από άλλον χρηστή. Επίσης αναγκάζει τους χρήστες να έχουν κωδικούς όπου θα περιέχουν κάποιον αριθμό , χαρακτήρες καθώς και σύμβολα. Για παράδειγμα ένας τέτοιος κωδικός θα μπορούσε να είναι ο εξής: W2_hellO!. Έτσι ο κωδικός μας γίνεται πιο δύσκολος ώστε να γίνει αντιληπτός στους hackers.[43]

3.4.3 Καταπολέμηση του hacking

Πλέον οι επιχειρήσεις και οι εταιρίες είναι ο κύριος στόχος των hackers, λόγο των μεγάλων οικονομικών συναλλαγών που πράττουν τα άτομα του κλάδου αυτού Έτσι θα πρέπει κάθε επιχείρηση να ακολουθεί κάποιους κανόνες για την καλύτερη αντιμετώπιση σε κάποια ανεπιθύμητη εισβολή .

Αρχικά θα πρέπει να γίνεται προληπτική προστασία του συστήματος, προστατεύοντας έτσι το πληροφοριακό σύστημα της επιχείρησης, τα προσωπικά δεδομένα των ατόμων που δουλεύουν πάνω σε αυτό (ονόματα πρόσβασης , κωδικούς πρόσβασης). Ακόμα , θα πρέπει να προστατεύουν ότι αφορά τα λειτουργικά συστήματα όπως λογισμικά και προγράμματα. Οποιαδήποτε πληροφορία μπορέσουν να αποσπάσουν, είτε είναι πολύ σημαντική ή μη για τα δικά μας δεδομένα, για τους hacker θα είναι μια πληροφορία «μεγάλης αξίας» για την συλλογή πληροφοριών δράσης τους στην επιχείρηση. Για αυτό χρειάζεται τεράστια προσοχή σε κάθε κίνηση που πραγματοποιούμε. Στην συνέχεια σαν δεύτερο στάδιο θα πρέπει η πρόσβαση στο σύστημα να είναι περιορισμένη ακόμα και για τους ίδιους τους χρήστες αυτού. Αυτό το μέτρο μπορεί να επιτευχτεί περιορίζοντας τους χρήστες είτε είναι εσωτερικοί είτε εξωτερικοί σε κάποιες συγκεκριμένες λειτουργιές σύμφωνα με τα δικαιώματα που τους παρέχονται από την επιχείρηση .Το τρίτο μέτρο προστασίας και καταπολέμησης του hacking είναι να γίνετε χρήση σύγχρονου λογισμικού. Με την εγκατάσταση και χρήση κάποιου σύγχρονου λογισμικού αυξάνεται και ο βαθμός ασφάλειας του συστήματος μας και δυσκολεύει την πρόσβαση στους hackers. Επίσης θα πρέπει να διαγράφονται προγράμματα, αρχεία, δεδομένα και λογαριασμοί χρηστών που πλέον δεν χρησιμοποιούν. Το κυριότερο είναι η διαγραφή των λογαριασμών χρηστών που δεν απασχολούνται πλέον από την επιχείρηση, για τον λόγο ότι μπορούν να διαρρεύσουν στοιχεία, διευκολύνοντας έτσι την πρόσβαση σε hackers. Σε περίπτωση που κάποιος hacker έχει αποκτήσει πρόσβαση από κάποιον παλιό λογαριασμό χρήστη και δεν γίνει αντιληπτός από τα άτομα της επιχείρησης, αυτό μπορεί να είναι καταστροφικό για όλη την επιχείρηση.

Επόμενο βήμα, είναι η χρήση antivirus, firewalls καθώς και η μέθοδος της κρυπτογράφησης των δεδομένων. Τα antivirus είναι προγράμματα που υπάρχουν στην αγορά και προστατεύουν το σύστημα μας. Τα firewalls βρίσκονται στο δίκτυο μας με σκοπό την προστασία των δεδομένων του εξυπηρετητή μας. Σαν μειονέκτημα των antivirusκαι των firewalls μπορούμε να πούμε ότι είναι το υψηλό τους κόστος. Όμως ποια επιχείρηση δεν θα επένδυε για την πιο αξιόπιστη ασφάλεια του συστήματος και των πληροφοριών του; Άρα το υπολογίζουμε σαν κάτι αναγκαίο . Άλλος κύριος παράγοντας είναι η μέθοδος της κρυπτογράφησης.

Με την κρυπτογράφηση μπορούμε να εξασφαλίσουμε το απόρρητο των προσωπικών μας πληροφοριών. Η κρυπτογράφηση γίνεται με τον συνδυασμό μαθηματικών για την κωδικοποίηση καθώς και την αποκωδικοποίηση των δεδομένων. Στα κρυπτογραφημένα αρχεία έχουν πρόσβαση μόνο όσοι είναι εξουσιοδοτημένη με συγκεκριμένη άδεια που τους παρέχεται από την επιχείρηση η την εταιρία. Κατά την διαδικασία της κρυπτογράφησης ένα αρχικό κείμενο έχει την ονομασία «απλό κείμενο» ή με τον αγγλικό όρο «plaintext» ενώ το κρυπτογραφημένο κείμενο έχει την ονομασία «κρυπτογράφημα» ή αλλιώς «ciphertext». Η αντίστροφη διαδικασία της κρυπτογράφησης ονομάζεται αποκρυπτογράφηση.[44]

3.5 Επίθεση άρνησης υπηρεσιών

Ονομάζεται DoS η επίθεση που γίνεται σε κάποιον υπολογιστή ή σε κάποια υπηρεσία με σκοπό να κάνουν είτε τον υπολογιστή είτε την υπηρεσία αντίστοιχα ανίκανη να εξυπηρετεί πιθανούς πελάτες καθώς και να δέχεται περεταίρω συνδέσεις. Οι DoS επιθέσεις έκαναν την εμφάνιση τους την δεκαετία του 90΄. Αρχικό θύμα ήταν μεμονωμένα hosts καθώς επίσης και μεμονωμένες υπηρεσίες. Την περίοδο του 1996 με 2000 , και κατά την διάρκεια της άνθισης του διαδικτύου παρατηρούνται μεγαλυτέρου αριθμού επιθέσεις DoS και η πιο χαρακτηριστική είναι η SYNFlood. Στη συνεχεία το 1997 οι επιθέσεις DoS κάνουν την εμφάνιση τους στα IRC δίκτυα και με συνδυασμό προγραμμάτων όπως είναι το boink, teardrop,bonk και την επίθεση smurf πραγματοποιούν τις επιθέσεις μέσω των windows. Το έτος 2000 πραγματοποιούνται κατανεμημένες επιθέσεις και χρησιμοποιούνται δίκτυα υπολογιστών για τις επιθέσεις.[45]

3.5.1.1 Πως λειτουργεί η επίθεση άρνησης υπηρεσιών

Τρόπος λειτουργίας των DoS επιθέσεων είναι η αποστολή πακέτων δεδομένων πραγματοποιώντας το σε μεγάλη συχνότητα με αποτέλεσμα το σύστημα να τεθεί σε ανικανότητα ανταπόκρισης. Οι κύριοι μέθοδοι επίθεσης είναι οι εξής:

1. Ping flood
2. Smurf flood

3. UDP flood
4. TCP SYN flood
5. DNS flood

[45]

3.5.1.2 Μέθοδος ping

Πρόκειται για την πιο γνωστή μέθοδο επίθεσης. Η χρήση της ήταν πιο αυξημένη τα παλαιοτέρα χρόνια. Ο τρόπος επίθεσης της μεθόδου αυτής βασίζεται στην αποστολή δεδομένων υπερβαίνοντας το επιτρεπτό όριο από bytes του πρωτόκολλου TCP/IP (65.536 bytes). Η μέθοδος αυτή εξακολουθεί να είναι γνωστή στα δίκτυα IRC.[45]

3.5.1.3 Μέθοδος Smurf

Η μέθοδος smurf λειτούργει χρησιμοποιώντας διευθύνσεις IP broadcast από δίκτυα αποστέλλοντας στο θύμα πλήθος μηνυμάτων ICMPEcho_Reply. Στη διάρκεια ο θύτης αποστέλλει δεδομένα ICMP EchoRequest σε διευθύνσεις IPbroadcast. Προηγουμένος έχει γίνει τροποποίηση αυτών των δεδομένων ώστε στο πεδίο source της IP να εμφανίζεται η IP του θύματος και όχι του θύτη. Με την αποστολή των δεδομένων, όσοι υπολογιστές είναι συνδεδεμένοι στο δίκτυο θα παραλάβουν τα ίδια δεδομένα με αποτέλεσμα να ανταποκριθούν στο Ping με πακέτα ICMPEchReply. Η μέθοδος του smurf βασίζεται στο γεγονός ότι με την χρήση των δικτύων και την αποστολή δεδομένων μπορεί να πτυχή τον σκοπό του που είναι η κατάρρευση του συστήματος. Αυτό το πτωχαίνει κύριος με την χρήση των δικτύων πολλαπλασιάζοντας τα πακέτα δεδομένων που θα αποσταλθούν στον υποψήφιο στόχο. Η ονομασία των δικτύων αυτών είναι Ενισχυτές Smurf .Ονομασία όπου οφείλεται στην δραστηριότητα του πολλαπλασιασμού των δεδομένων όπως προαναφέραμε.[45]

3.5.1.4 Μέθοδος UDP

Στην περίπτωση των επιθέσεων UDP γίνεται η χρήση UDP πακέτων που βρίσκουμε στο πρωτόκολλο TCP/IP στο επίπεδο Μεταφοράς. Σκοπός της UDP επίθεσης είναι η αποστολή των UDP πακέτων σε μεγάλο αριθμό, σε τυχαία ports κάποιου υπολογιστή. Στην συνεχεία ο υπολογιστής–στόχος με την σειρά του θα ανταπεξέλθει στην αποστολή των δεδομένων και θα ανακαλύψει εάν σε κάποιο από τα ports υπάρχει ανταπόκριση . Σε περίπτωση που δεν υπάρχει ανταπόκριση από κάποιο συγκεκριμένο port τότε θα χρειαστεί να γίνει αποστολή ICMP πακέτων. Όπως στην μέθοδο του UDP και στην μέθοδο smurf, ο επιτιθέμενος χρησιμοποιεί διαφορετική IP, με την διαφορά ότι τώρα αναγράφεται κάποια τυχαία διεύθυνση IP. Με τον τρόπο αυτό επιτυγχάνεται η ανωνυμία του υπολογιστή του επιτιθέμενου. [46]

3.5.1.5 Μέθοδος TCPSYN

Άλλη μια κατηγορία των DoS επιθέσεων είναι η επίθεση TCPSYN κατά την οποία ο επιτιθέμενος αποστέλλει στο θύμα πληθώρα αιτημάτων SYN. Για την πραγματοποίηση της επίθεσης αυτής χρειάζεται το πρωτόκολλο TCP όπως προκύπτει και από την ονομασία της. Με το πρωτόκολλο TCP δημιουργείται μια σύνδεση μεταξύ δυο ή και περισσότερων υπολογιστών και βοηθάει στη σωστή αποστολή πακέτων δεδομένων. Το πρωτόκολλο TCP ακολουθεί κάποια επίπεδα που είναι τα εξής:

1. Επίπεδο γραμμής δεδομένων
2. Επίπεδο διαδικτύου
3. Επίπεδο μεταφοράς
4. Επίπεδο εφαρμογής

Οι δυο υπολογιστές που θα χρειαστεί να συνδεθούν μεταξύ τους θα ακολουθούσουν την διαδικασία της τριμερής χειραψίας. Κατά την διαδικασία αυτή εμπλέκονται και τα SYN. Λέξη που προέρχονται από την αγγλική ορολογία και είναι η λέξη synchronize που σημαίνει συγχρονισμός. Στα βήματα που ακολουθούντα στη τρίμερη χειραψία αρχικά ο πελάτης (client) αναζητά την δημιουργία μιας σύνδεσης με τον διακομιστή (server) αποστέλλοντας του ένα πακέτο TCPSYN. Στην συνεχεία ο διακομιστής απαντά και αποδέχεται το αίτημα

του πελάτη αποστέλλοντας με την σειρά του ένα πακέτο TCPSYN-ACK (acknowledge=αναγνώριση, αποδοχή). Το τελικό βήμα το πραγματοποιεί ο πελάτης καθώς στέλνει και εκείνος το ίδιο πακέτο TCP SYN-ACK για να δηλώσει την αποδοχή της σύνδεσης. Στην περίπτωση της επίθεσης μας αυτής ο επιτιθέμενος –πελάτης αποστέλλει στον διακομιστή αίτημα αποδοχής σύνδεσης, ο SERVER αποδέχεται την σύνδεση και στην συνεχεία ο πελάτης δεν ακολουθεί το τελικό βήμα αποδοχής της σύνδεσης με αποτέλεσμα ο server να είναι σε αναμονή και να μην μπορεί να εξυπηρετήσει τους νόμιμους χρηστές.[46]

3.5.1.6 Μέθοδος DNS

Η λειτουργιά του DNS (Domain Name System) είναι να κάνει την μετάφραση των διευθύνσεων IP ώστε να είναι ξεκάθαρες στον server. Μετατρέπει για παράδειγμα την διεύθυνση της Google.com σε ψηφία δυαδικής μορφής ώστε να είναι αναγνωρίσιμη από τον server. Σκοπός της επίθεσης είναι να γίνετε αόρατη από τον στόχο της. Για να επιτευχτεί η DNS επίθεση χρειάζεται να ληφθεί υπόψη η εκμετάλλευση που θα υποστούν μερικά πρωτοκόλλα όπως είναι το UDP πρωτόκολλο μεταφοράς όπου συντελεί ένα βασικό ερώτημα DNS. Σκοπός των DNS επιθέσεων είναι να διακοπεί η αντιστοίχιση των IP διευθύνσεων ως προς τον server. Στην συνεχεία ο server δέχεται πολλά αιτήματα για κάποια IP που πιθανόν να μην αντιστοιχεί κάπου και έτσι προκύπτει κατάρρευση του συστήματος.[45]

3.5.1.7 Application levelattack

Στην Application level attack ο επιτιθέμενος στοχεύει το επίπεδο εφαρμογής του μοντέλου OSI. Κατά την επίθεση προσπαθούν να απενεργοποιήσουν κάποιες λειτουργιές. Η επίθεση γίνεται σε τοποθετημένους σκοπούς. Συμπεριλαμβάνει την παρέμβαση σε συναλλαγές καθώς και σε βάσεις δεδομένων.

3.5.1.8 Mail bomb

Στην επίθεση mailbomb μπορούμε να πούμε ότι είναι σαν την επίθεση Spam. Σκοπός της επίθεσης είναι να αποστέλλονται e-mails σε μεγάλο αριθμό, σε κάποια διεύθυνση ηλεκτρονικού ταχυδρόμου με αποτέλεσμα να γεμίσει ο χώρος του

δίσκου και στην συνεχεία να υπάρξει κατάρρευση του mailserver. Από τις πιο συνηθισμένες μορφές του mailbomb είναι το ZIPbomb. Η ονομασία του φανερώνει εξαρχής ότι εμπλέκονται αρχεία μορφής ZIP (συμπιεσμένα αρχεία). Πλέον πολλοί mailserver κατά την λήψη ενός αρχείου ,για τον έλεγχο για ιούς θα αναγκαστούν να κάνουν αποσυμπιέσει του αρχείου ZIP. Το ZIP αρχείο για την επίθεση μπορεί να περιέχει κάποιο κείμενο μεγάλης χωρητικότητας GB, το οποίο ο mailserver θα το κάνει αποσυμπιέσει. Στην ουσία το ZIPbomb είναι ότι ένα αρχείο έχει διαφορετικό μέγεθος πριν από την αποσυμπίεση και διαφορετικό μετά. Έτσι το αποσυμπιεσμένο αρχείο θα συμπεριλάβει μεγάλη χωρητικότητα στη RAM, στο σκληρό δίσκο και θα δεσμεύσει μεγάλη υπολογιστική μνήμη και ισχύ. Αυτό θα έχει σαν αποτέλεσμα να μην ανταπεξέρχεται ο υπολογιστής.[45]

3.5.1.9 Peer to peer επίθεση

Αρχικά το peer to peer είναι αρχιτεκτονική δικτύων που επιτρέπει την επικοινωνία σε μεμονωμένους υπολογιστές. Τους παρέχεται η δυνατότητα να μοιράζονται επικοινωνίες , επεξεργαστική ισχύ καθώς και αρχεία δεδομένων. Ένα μεγάλο ελάττωμα των P2P δικτύων είναι η έλλειψη δομής και έτσι γίνεται πιο εύκολη η πρόσβαση σε νέους χρήστες στο σύστημα και πιθανών σε κακόβουλους χρήστες. Η ανεξέλεγκτη εισαγωγή νέων χρηστών και πιο συγκεκριμένα κακόβουλων χρηστών μπορούν να εκμεταλλευτούν το σύστημα χρησιμοποιώντας μεγάλο αριθμό κόμβων και στην συνεχεία να εκτελέσουν αιτήσεις ως προς το θύμα το οποίο δεν είναι απαραίτητο ότι ανήκει σε κάποιο P2P σύστημα. Αυτό έχει σαν αποτέλεσμα την εξάντληση πόρων, κατά την όποια υπάρχει δυσκολία στην αναγνώριση του αρχικού επιτιθέμενου καθώς είναι και σε μεγάλο βαθμό δυσκολίας ο τερματισμός της επίθεσης.[46]

3.5.1.10 Μόνιμες επιθέσεις άρνησης υπηρεσιών

Οι μόνιμες DoS επιθέσεις είναι γνωστές και με την ονομασία phlasing. Πρόκειται για μια επικίνδυνη μορφή επίθεσης όπου στην πραγματοποίηση της αναγκάζει την αντικατάσταση ή επανατοποθέτηση του υλικού. Στην δράση της εκμεταλλεύεται κενά ασφαλείας. Σκοπός του επιτιθέμενου είναι να εκμεταλλευτεί τα κενά ασφαλείας για να μπορέσει να αλλάξει το firmware της συσκευής με

κάποιο τροποποιημένο, μη γνήσιο ή ελαττωματικό. Σε σύγκριση με άλλες επιθέσεις οι μόνιμες DoS επιθέσεις δεν χρειάζονται πολλούς πόρους και bonnets για να πραγματοποιήσουν την επίθεση τους για τον λόγο ότι πρόκειται για μια γρήγορη επίθεση και είναι στο επίκεντρο των hackers. Για την ανίχνευση μόνιμων επιθέσεων, υπάρχει ένα εργαλείο το PhlasDance όπου ο δημιουργός του είναι ο RichSmithυπάλληλος της HP.[47]

3.5.2.1 Προληπτικά μέτρα

Υπάρχουν πολλοί μηχανισμοί για την πρόληψη και τον εντοπισμό των επιθέσεων Dos. Παρακάτω παρουσιάζονται κάποια μέτρα που μπορούν να ληφθούν προκειμένου να περιοριστούν οι επιθέσεις Dos.

3.5.2.2 Αφαίρεση τρωτών σημείων

Η αφαίρεση των τρωτών σημείων μπορεί να μειώσει την πιθανότητα των επιθέσεων άρνησης υπηρεσιών (Dos). Η επίθεση SYNflood είναι συνηθισμένη και αντιμετωπίζεται με επιτυχία. Ο επιτιθέμενος στέλνει στον διακομιστή πολλά πακέτα TCPSYN. Ο διακομιστής απαντά με πακέτα SYN-ACK σύμφωνα με την διαδικασία της τριμερής χειραψίας. Ο επιτιθέμενος όμως δεν αποστέλλει τα πακέτα ACK για να ολοκληρωθεί η χειραψία και αφήνει τον διακομιστή να περιμένει ξοδεύοντας τους υπολογιστικούς του πόρους. Μετά από κάποιο αριθμό τέτοιων συνδέσεων ο διακομιστής δεν μπορεί πλέων να εξυπηρετήσει τους χρήστες και καταρρέει. Για την αντιμετώπιση αυτής της επιθέσεις είναι σημαντική η καταγραφή του αριθμού των συνδέσεων που έχει ξεκινήσει ο κάθε πελάτης και η απαγόρευση δημιουργίας νέων όταν ο αριθμός ξεπεράσει κάποιο συγκεκριμένο όριο.

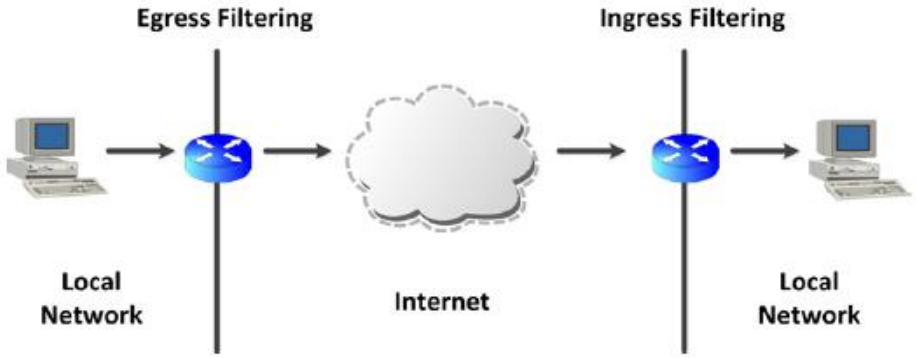
SYN cookie είναι η τεχνική που χρησιμοποιείται για την αντιμετώπιση των επιθέσεων SYN fload. Οι διακομιστές που χρησιμοποιούν τις λειτουργείς SYN cookie δεν διακόπτουν την σύνδεση εάν γεμίσει η ουρά SYN σε μια πιθανή επίθεση Dos. SYN cookie είναι μια ακολουθία αριθμών που κατασκευάστηκε μα βάση τους παρακάτω κανόνες:

1. 5 ανώτερα bits: t mod 32 όπου t μετρητής χρονικών διαστημάτων

2. 3 μεσαία bits: μια κωδικοποιημένη τιμή που αντιπροσωπεύει το m
3. 24 κατώτερα bits: s μια κρυπτογραφημένη τιμή βασισμένη στην IP διεύθυνση και τον αριθμό θύρας του διακομιστή και του πελάτη.[48]

3.5.2.3 Φιλτράρισμα κυκλοφορίας

Οι ακραίοι δρομολογητές μπορούν να φιλτράρουν την κυκλοφορία εντοπίζοντας τα ύποπτα πακέτα κατά την είσοδο η την έξοδό τους από το τοπικό δίκτυο (Εικόνα 3).



Εικόνα 3. Φιλτράρισμα κυκλοφορίας

Για την αντιμετώπιση του IPspoofing που χρησιμοποιείτε κυρίως σε επιθέσεις άρνησης υπηρεσιών (Dos) είναι αποτελεσματική η χρήση ενός υπολογιστή που θα βρίσκεται ανάμεσα στο τοπικό δίκτυο και το διαδίκτυο. Ο υπολογιστής θα απορρίπτει όλα τα πακέτα που προέρχονται από το διαδίκτυο και έχουν ως διεύθυνση προέλευσης την διεύθυνση IP ενός υπολογιστή του τοπικού δικτύου. Έτσι εξασφαλίζεται ότι ένας εξωτερικός εισβολέας δεν θα χρησιμοποιήσει κάποια από τις διευθύνσεις IP του τοπικού δικτύου ως ψεύτικη στα πακέτα του.

Ακόμη ο υπολογιστής θα πρέπει να απορρίπτει όλα τα πακέτα που προέρχονται από το τοπικό δίκτυο και έχουν διεύθυνση προέλευσης μια διεύθυνση IP που δεν ανήκει στους υπολογιστές του τοπικού δικτύου. Με αυτόν τον τρόπο εξασφαλίζεται ότι κάποιος χρήστης του τοπικού δικτύου δεν πρόκειται να χρησιμοποιήσει την τεχνική του IPspoofing για να επιτεθεί σε κάποιον άλλον υπολογιστή έκτος του τοπικού δικτύου. [49]

3.5.2.4 Ανίχνευση επιθέσεων

Τα συστήματα αποτροπής εισβολέων μπορούν να ανιχνεύσουν επιθέσεις παρακολουθώντας την συμπεριφορά των υπολογιστικών συστημάτων ή και ολόκληρων δικτύων. Τα συστήματα δημιουργούν προφίλ αναλύοντας την συμπεριφορά του δικτύου υπό κανονικές συνθήκες. Μόλις ανιχνεύσουν μια ύποπτη συμπεριφορά σημάνουν συναγερμό και επικαλούνται μηχανισμοί πρόληψης όπως είναι το φιλτράρισμα. Είναι δύσκολο να δημιουργηθεί ένα προφίλ λόγο της ανάγκης να συλλαμβάνει και να παρακολουθεί διάφορους παραμέτρους του συστήματος και του δικτύου σε πραγματικό χρόνο. Είναι επίσης δύσκολο να προσδιοριστεί το όριο ώστε να χαρακτηριστεί μια συμπεριφορά ως επίθεση. Αν δεν γίνουν αυτά μπορεί να υπάρχουν πάρα πολλά εσφαλμένα θετικά και αρνητικά αποτελέσματα και ενδεχομένως να καταστεί ο μηχανισμός ανίχνευσης άχρηστος.[50]

3.6 Ηλεκτρονικό ψάρεμα

Το ηλεκτρονικό ψάρεμα (επίσης γνωστό και ως «Phishing») είναι μια μορφή άπατης που συμβαίνει όταν κακόβουλες ιστοσελίδες προσπαθούν να υποκλέψουν ευαίσθητες πληροφορίες όπως κωδικούς πρόσβασης, πληροφορίες του χρήστη και τον αριθμό πιστωτικών καρτών. Οι επιθέσεις συχνά επιτυγχάνονται μέσω μηνυμάτων του ηλεκτρονικού ταχυδρομείου και προσπαθούν να κάνουν τον χρήστη να ανανεώσει τις πληροφορίες του λογαριασμού του σε πλαστές ιστοσελίδες που φαίνονται όπως ακριβώς και οι νόμιμες ιστοσελίδες.

Ο όρος Phishing που στα Ελληνικά αποκαλείτε Ηλεκτρονικό Ψάρεμα προέρχεται από το αγγλικό fishing (ψάρεμα) καθώς η διαδικασία με την οποία ο θύτης παρουσιάζεται ως η αξιόπιστη οντότητα ώστε να προσελκύσει τους χρήστες θυμίζει την διαδικασία του δολώματος στο ψάρεμα.

Το ηλεκτρονικό ψάρεμα αναφέρεται στην προσπάθεια απόσπασης προσωπικών στοιχείων, οικονομικού συνήθως χαρακτήρα από τους χρήστες τουδιαδικτύου. Ο επιτιθέμενος υποδύεται μία αξιόπιστη οντότητα εκμεταλλευόμενος την ελλιπή προστασία που παρέχουν τα προγράμματα προστασίας και την άγνοια του χρήστη θύματος, με σκοπό την απόκτηση των προσωπικών του δεδομένων, όπως κωδικούς

πρόσβασης από τραπεζικούς λογαριασμούς καθώς και στοιχεία πιστωτικών καρτών.[51]

Η τεχνική του pharming αποτελεί μέθοδο εξαπάτησης μέσω του διαδικτύου παρόμοια με το ηλεκτρονικό ψάρεμα αλλά πιο επικίνδυνη από αυτό. Ένα ειδικό πρόγραμμα εκμεταλλεύεται κενά ασφαλείας του συστήματος, διεισδύει στον υπολογιστή του θύματος και το επηρεάζει κατά τέτοιο τρόπο που ακόμα κι αν ο χρήστης πληκτρολογεί τη σωστή διεύθυνση της ιστοσελίδας που επιθυμεί να επισκεφτεί, θεωρώντας πως βρίσκεται σε ασφαλή χώρο, ο συγκεκριμένος υπολογιστής τον καθοδηγεί μόνο σε πλαστές ιστοσελίδες.[52]

Προσωπικά στοιχειά από 6.3 εκατομμύρια πελάτες κλάπηκαν το 2007 από χάκερ όταν μπήκαν στην βάση δεδομένων της διεθνής χρηματιστηριακή εταιρείας (TDAmeritrade). Οι επιτιθέμενοι χρησιμοποιούν την μέθοδο του ηλεκτρονικού ψαρέματος όλο και περισσότερο στις ιστοσελίδες των κοινωνικών δικτύων από τα οποία μπορούν τα αποσπάσουν πιο εύκολα προσωπικά δεδομένα. [53]

Η Avalanche (χιονοστιβάδα)είναι εγκληματική συμμορία που εμπλέκετε σε επιθέσεις ηλεκτρονικού ψαρέματος (phishing). Το 2010 η ομάδα εργασίας Anti-PhishingWorkingGroup (APWG) ανέφεραν ότι η χιονοστιβάδα ήταν υπεύθυνη για τα δύο τρίτα του συνόλου των phishing επιθέσεις κατά το δεύτερο εξάμηνο του 2009, χαρακτηρίζοντάς την ως ένα από τα πιο εξελιγμένα και επιζήμια για το Διαδίκτυο και πιο παραγωγικός phishing συμμορία του κόσμου. Η Avalanche δημιουργήθηκε τον Δεκέμβριο του 2008 και ίσως να αντικαθιστά μια παλιότερη ομάδα γνωστή ως RockPhish που σταμάτησε να λειτουργεί το 2008. Ασκεί την δράση της από την Ανατολική Ευρώπη και το όνομά της δόθηκε από τους ερευνητές ασφαλείας λόγω της υψηλής έντασης των επιθέσεων της. Η Avalanche ξεκίνησε με 24% των phishing επιθέσεων κατά το πρώτο εξάμηνο του 2009 ,ενώ κατά το δεύτερο εξάμηνο του 2009 η APWG κατέγραψε 84.250 επιθέσεις από χιονοστιβάδα που αποτελούν το 66% όλων των επιθέσεων phishing. Ο αριθμός του συνόλου των επιθέσεων phishing υπερδιπλασιάστηκε, μια αύξηση που το APWG αποδίδει άμεσα στην Avalanche.Τα στατιστικά στοιχεία που προκύπτουν από τις έρευνες της APWG (Anti-Phishing Working Group) για τα τελευταία 7 χρόνια (μέχρι το 2013) δείχνουν ότι οι αναφορές επιθέσεων αυξήθηκαν ιδιαίτερα το 2009 ενώ το 2010 σημείωσαν πτώση και από τότε σταδιακά αυξάνονται. Ο αριθμός

ιστοσελίδων που παρουσίασε αυτού του είδους δραστηριότητα παρουσιάζει σχεδόν κάθε χρόνο αύξηση, με μία μικρή πτώση το 2011. Ο αριθμός των εταιριών που έπεσαν θύμα ενεργειών phishing κατά μέσο όρο αυξάνεται κάθε χρόνο.[54]

Σύμφωνα με την παγκόσμια έρευνα Global Corporate ITSecurity Risks που πραγματοποιήθηκε το 2013 διαπιστώθηκε ότι το 66% των στελεχών που συμμετείχε, ανέφερε ότι οι εταιρείες τους δέχτηκαν επιθέσεις με διάφορα είδη κακόβουλων επιθέσεων έχοντας σημειώσει αύξηση σε σχέση με το 2012 που ήταν 58%.Οι επιθέσεις phishing στοχοποίησαν το 36% των επιχειρήσεων σε παγκόσμιο επίπεδο με το phishing να παραμένει στην κορυφαία τριάδα των πιο διαδεδομένων απειλών που χρησιμοποιούνται σε εξωτερικές επιθέσεις ενάντια σε εταιρείες.[55]

Η Gartner (κορυφαία ερευνητική και συμβουλευτική εταιρεία) στις 5 Μαΐου 2004 ανακοίνωσε αποτελέσματα μιας έρευνας που δείχνει ότι τα εκατομμύρια των καταναλωτών λόγω άγνοιας έπεσαν θύματα από επιθέσεις ηλεκτρονικού ψαρέματος. Εκτιμάται ότι περίπου 19% (11 εκατομμύρια άνθρωποι) έχουν κάνει κλικ στον σύνδεσμο από πλαστογραφημένο e-mail και 3 τοις εκατό (1,78 εκατομμύρια άνθρωποι) έδωσαν στους επιτιθεμένους ευαίσθητα οικονομικά ή προσωπικά στοιχεία όπως αριθμούς πιστωτικών καρτών και διευθύνσεις χρέωσης, συμπληρώνοντας μια φόρμα σε μια πλαστή ιστοσελίδα. Η Gartner εκτιμά ότι τουλάχιστον ένα εκατομμύριο άτομα ακόμα μπορεί να έχουν πέσει θύματα από τέτοια συστήματα χωρίς καν να το συνειδητοποιούν οι ίδιοι. Η κλοπή ταυτότητας δημιούργησε άμεσες απώλειες 1.2 δισεκατομμυρίων δολαρίων το 2003. Η Gartner εκτιμά ότι κατά τους 12 μήνες έως τον Μάιο του 2005 η απάτη με χρεωστική κάρτα στις ΗΠΑ δημιούργησε απώλειες 2,75 δισεκατομμύρια δολάρια, με μέση απώλεια άνω των 900 δολαρίων. Σε άλλη μια έρευνα η Gartner εκτιμά πως οι απώλειες από επιθέσεις ηλεκτρονικού ψαρέματος το 2007 ανήλθαν σε 3,2 εκατομμύρια δολάρια. Περισσότεροι από 5 εκατομμύρια καταναλωτές των ΗΠΑ έχασαν χρήματα από επιθέσεις ηλεκτρονικού ψαρέματος σε ένα χρόνο (έως το Σεπτέμβριο του 2008), μια αύξηση 39,8% σε σχέση με τον αριθμό των θυμάτων προηγούμενου έτους σύμφωνα με την Gartner. Η ετήσια απώλεια από επιθέσεις ηλεκτρονικού ψαρέματος στις ΗΠΑ εκτιμάται σε 61 εκατομμύρια δολάρια.[56]

3.6.2 Πως λειτουργεί το ηλεκτρονικό ψάρεμα

Το ηλεκτρονικό ψάρεμα ξεκινάει με το phonephreaking, όταν οι χάκερς έκαναν επιθέσεις στα τηλεφωνικά δίκτυα επεμβαίνοντας στις γραμμές και αποσπώντας κρίσιμες πληροφορίες από προσωπικές συζητήσεις. Στην διαδικτυακή του μορφή πρωτοεμφανίστηκε το 1995 μέσω του ηλεκτρονικού ταχυδρομείου και στη συνέχεια με άμεσο μήνυμα. Ο χάκερ στέλνει ένα μήνυμα ηλεκτρονικού ταχυδρομείου ή άμεσο μήνυμα στο θύμα στο οποίο συστήνεται ως αξιόπιστο πρόσωπο και ζητά από το θύμα κάποια προσωπικά στοιχεία. Ο χρήστης βρίσκεται σε μία ιστοσελίδα, e-mail ή άμεσο μήνυμα, που τον παραπέμπουν σε έναν σύνδεσμο επιφανειακά αξιόπιστο, αλλά είναι φτιαγμένος έτσι ώστε να τον οδηγεί σε διαφορετική ιστοσελίδα από αυτή που προβλέπεται.Το βασικό εργαλείο του ηλεκτρονικού ψαρέματος είναι οι αποπλανητικοί σύνδεσμοι.

Τα Subdomain (υπο-domain) χρησιμοποιούνται και αυτά για ηλεκτρονικό ψάρεμα. Για παράδειγμα έχουμε την διεύθυνση http://www.yourbank.example.com. Φαίνεται ότι ο σύνδεσμος θα μας μεταφέρει στο τμήμα example της ιστοσελίδας yourbank αλλά στην πραγματικότητα όμως μας μεταφέρει στο τμήμα yourbank της ιστοσελίδας example. Έτσι λειτουργούν οι ψεύτικες ιστοσελίδες που μέσω παραπλανητικών συνδέσμων οδηγούν τους χρήστες σε σελίδες οπτικά πανομοιότυπες με τις αυθεντικές ιστοσελίδες αλλά ανήκουν στους χάκερ.[57]

Στο ηλεκτρονικό ψάρεμα υπάρχουν μέθοδοι ακόμα πιο δύσκολοι στην ανίχνευση τους όπως το IDN spoofing, μέσω του οποίου με κακό χειρισμό των International Domain Names (IDN) πανομοιότυπα URL μπορούν να οδηγούν σε διαφορετικές ιστοσελίδες. Για παράδειγμα στην διεύθυνση http://www.c1t1bank.com το 1 είναι το γράμμα i αλλά η διεύθυνση συγχέεται με http://www.citibank.com παραπλανώντας τους χρήστες. Η ανοιχτή ανακατεύθυνση είναι μια εφαρμογή που παίρνει μια παράμετρο και ανακατευθύνει τον χρήστη στην τιμή της παραμέτρου χωρίς επικύρωση. Αυτό το θέμα ευπάθειας χρησιμοποιείται σε επιθέσεις phishing και ωθεί τους χρήστες να επισκεφθούν κακόβουλες ιστοσελίδες χωρίς να το συνειδητοποιούν. Για παράδειγμα ο σύνδεσμος http://www.google.com/url?q=http://www.signin.com ανοίγει την ιστοσελίδα signin.com και όχι το google.com όπως φαίνεται .[58]

Στο ηλεκτρονικό ψάρεμα χρησιμοποιείτε καιη μέθοδος Cross-sites cripting η οποία αναφέρεται στην εκμετάλλευση διαφόρων ευπαθειών υπολογιστικών συστημάτων (π.χ. ιστοχώρων), όπου ο χάκερ θα μπορούσε να εισάγει κακόβουλο κώδικα και να επιτύχει κλοπή προσωπικών δεδομένων καθώς και αλλαγή όλης της δομής της ιστοσελίδας.[57]

Πρόσφατα έχει ανακαλυφθεί μια νέα μέθοδος ηλεκτρονικού ψαρέματος γνωστή και ως tabnabbing. Το όνομα της επίθεσης επινοήθηκε στις αρχές του 2010 από τον ερευνητή ασφάλειας Άζα Ράσκιν. Η επίθεση πείθει τους χρήστες να υποβάλουν τα στοιχειά της σύνδεσής τους και τους κωδικούς πρόσβασης σε δημοφιλείς ιστοσελίδες πλαστογραφώντας αυτές τις ιστοσελίδες και πείθοντας ότι είναι νόμιμες. Η επίθεση εκμεταλλεύεται την εμπιστοσύνη των χρηστών και την απροσεξία τους καθώς και στη δυνατότητα των σύγχρονων ιστοσελίδων να ξαναφορτώνουν καρτέλες μαζί με το περιεχόμενό τους μετά από ένα μεγάλο χρονικό διάστημα, αφού έχει προηγουμένως φορτωθεί η ιστοσελίδα. Το tabnabbing αντίθετα από τις περισσότερες επιθέσεις ηλεκτρονικού ψαρέματος δεν ζητάει από τους χρήστες να κάνουν κλικ σε κάποιον σύνδεσμο αλλά φορτώνει μια ψεύτικη σελίδα σε μια από τις ανοιχτές καρτέλες στον περιηγητή τους.[59]

3.6.3 Προληπτικά μέτρα αντιμετώπισης του ηλεκτρονικού ψαρέματος

Οι προσπάθειες για την αντιμετώπιση του αυξανόμενου αριθμού των περιστατικών του ηλεκτρονικού ψαρέματος περιλαμβάνουν τη νομοθεσία, την εκπαίδευση των χρηστών, την ευαισθητοποίηση του κοινού και τα τεχνικά μέτρα ασφαλείας. Η λύση στο πρόβλημα του ηλεκτρονικού ψαρέματος δεν είναι απλή. Είναι ένα πρόβλημα που συνεχώς θα υπάρχει και θα πρέπει να αντιμετωπίζεται κάθε φορά με συνεχή ενίσχυση των παραπάνω.

Οι άνθρωποι μπορούν να λάβουν μέτρα για την αποφυγή επίθεσης ηλεκτρονικού ψαρέματος τροποποιώντας τις συνήθειες της περιήγησής τους στο διαδίκτυο. Πρέπει να δείχνουν προσοχή στα παράθυρα προειδοποίησης των προγραμμάτων περιήγησης. Τα σύγχρονα προγράμματα περιήγησης εμφανίζουν αναδυόμενα παράθυρα προειδοποίησης όταν συναντούν ύποπτη δραστηριότητα. Το πρόβλημα με τα αναδυόμενα παράθυρα είναι ότι εμφανίζουν πολλές ασήμαντες προειδοποιήσεις και οι περισσότεροι άνθρωποι τα αγνοούν. Όταν έρχονται σε

επαφή για ένα λογαριασμό που πρέπει να επαληθευτεί ο σωστός τρόπος είναι να επικοινωνήσουν με την εταιρία από την όποια προέρχεται το μήνυμα ηλεκτρονικού ταχυδρομείου και να γίνει η ταυτοποίηση.

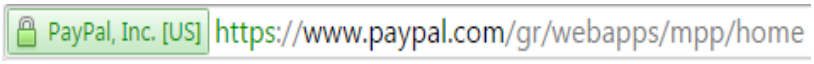
Θα ήταν χρήσιμο να αναφερθεί ότι μερικές τεχνικές αντιμετώπισης του ηλεκτρονικού ψαρέματος έχουν ενσωματωθεί στα προγράμματα περιήγησης και στις ιστοσελίδες. Οι περισσότερες ιστοσελίδες έχουν υιοθετήσει ασφαλή έλεγχο ταυτότητας μέσω του πρωτόκολλου SSL χρησιμοποιώντας μεθόδους κρυπτογράφησης των δεδομένων που ανταλλάσσονται μεταξύ δύο υπολογιστών,παρέχοντας ασφάλεια κατά την μετάδοση ευαίσθητων δεδομένων. Τοπρωτόκολλο SSL χρησιμοποιείτε για να ενημερώνει τον χρήστη εάν βρίσκετε σε νόμιμα πιστοποιημένη ιστοσελίδα και ποια Αρχή την πιστοποιεί. Τα σύγχρονα προγράμματα περιήγησης περιλαμβάνουν επεκτάσεις στη γραμμή διευθύνσεων για να προβάλλουν τέτοιες πληροφορίες.[57]

Το προγράμματα περιήγησης Google Chrome χρησιμοποίει πράσινο κουτί με εικονίδιο κλειδώματος στην αριστερή πλευρά της γραμμής διευθύνσεων(σχήμα 1)για να δείξει το πιστοποιητικό που παρέχει υψηλό επίπεδο πιστοποίησης της ταυτότητας.Το προγράμματα περιήγησης Mozilla χρησιμοποίει πράσινο κουτί στη γραμμή διευθύνσεων για να δείξει την πιστοποίηση και δείχνει άλλα πιστοποιητικά με μπλε χρώμα (σχήμα 2).Ο Internet Explorer δείχνει όλη την γραμμή διευθύνσεων με πράσινο χρώμα χρησιμοποιώντας εικονίδιο κλειδώματος στη δεξιά πλευρά (σχήμα 3) για πιστοποιητικά που επαληθεύουν την ταυτότητα.

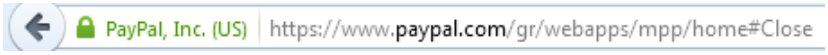
Επίσης οι χρήστες πρέπει να ξέρουν κάθε φορά σε ποιά ιστοσελίδα βρίσκονται ελέγχοντας την γραμμή διευθύνσεων. Όμως οι διευθύνσεις ιστοχώρων σε κάποιες περιπτώσεις είναι πολύπλοκες για να τα καταλάβει ο μέσος χρήστης. Έτσι τα προγράμματα περιήγησης έχουν βελτιωθεί για να βοηθάνε τους χρήστες να καταλάβουν σε ποιά ιστοσελίδα βρίσκονται. Το πρόγραμμα περιήγησης Google Chrome δείχνει όλη την διεύθυνση με γκρίζο χρώμα, τονίζοντας μόνο το όνομα χώρου με μαύρο. Για παράδειγμα στην εικόνα 4 μόνο το paypal.com έχει μαύρο χρώμα. Αυτό συμβαίνει με όλες τις ιστοσελίδες ακόμα και αν δεν έχουν ψηφιακά πιστοποιητικά. Εάν η ιστοσελίδα έχει ψηφιακά πιστοποιητικά τότε εμφανίζεται ένα πράσινο κουτί με εικονίδιο κλειδώματος στην αριστερή πλευρά της γραμμής διευθύνσεων για να δείξει ότι η ιστοσελίδα είναι νόμιμη (εικόνα 5.Το

προγράμματα περιήγησης Mozilla χρησιμοποιεί και αυτό πράσινο κουτί στη γραμμή διευθύνσεων για να δείξει τα ψηφιακά πιστοποιητικά. (εικόνα 6)

Τα προγράμματα περιήγησης υποδεικνύουν τα ψηφιακά πιστοποιητικά καθώς και την Αρχή που τα πιστοποιεί. Το πρόβλημα με τις Αρχές είναι ότι δεν παρέχουν όλες εξίσου καλές υπηρεσίες. Έτσι μια κακόβουλη ιστοσελίδα μπορεί να αποκτήσει ένα έγκυρο ψηφιακό πιστοποιητικό από μια ευάλωτη Αρχή. Τα ψηφιακά πιστοποιητικά μπορεί να τα βρει κάποιος κάνοντας κλικ στην γραμμή διευθύνσεων πάνω σε εικονίδιο κλειδώματος. Ένα παράδειγμα του προγράμματος περιήγησης του Google Chrome υπάρχει στην εικόνα 7.



Εικόνα 4 Γραμμη διευθύνσεων στο Google Chrome



Εικόνα 5 Γραμμή διευθύνσεων στο Mozilla Firefox

Εικόνα 6 Γραμμή διευθύνσεων στο Internet explorer

Εικόνα 7 Ψηφιακό πιστοποιητικό

Η προστασία από το ηλεκτρονικό ψάρεμα μπορεί να γίνει ελέγχοντας τις ιστοσελίδες που επισκέπτεται ο χρήστης μέσα από καταλόγους που έχουν δηλωμένες ιστοσελίδες με κακόβουλα λογισμικά. Όλα τα σύγχρονα προγράμματα περιήγησης περιλαμβάνουν τέτοιο είδος φίλτρου. Οι κατάλογοι μπορούν να χρησιμοποιηθούν για να φιλτράρουν τα ύποπτα ηλεκτρονικά μηνύματα πριν αυτά φτάσουν στο χρήστη. Μια άλλη τεχνική αντιμετώπισης του ηλεκτρονικού ψαρέματος είναι να μοιράζονται τα δεδομένα εισόδου σε δυο μέρη. Το πρώτο μέρος θα ανήκει στον χρήστη και το δεύτερο θα παραμένει στην υπηρεσία της ιστοσελίδας. Σε μια απλή σύνδεση η ιστοσελίδα θα ζητά από τον χρήστη να

διάλεξη μια προσωπική εικόνα και θα εμφανίζει την εικόνα με οπουδήποτε μορφή ζητώντας τον κωδικό του. Ο χρήστης θα πρέπει να εισάγει τους κωδικούς του μόνο όταν θα βλέπει την δική του προσωπική εικόνα. Έτσι εάν κάποιος επιτιθέμενος ζητήσει από τον χρήστη τους κωδικούς εισόδου του χωρίς την προσωπική εικόνα , ο χρήστης θα καταλάβει ότι το αίτημα έγινε από κάποιον άγνωστο. Σύμφωνα με μελέτες ωστόσο μερικοί δίνουν τους κωδικούς τους και χωρίς την προσωπική τους εικόνα. Ο αμοιβαίος έλεγχος ταυτότητας είναι η μέθοδος στην οποία ο πελάτης και ο εξυπηρετητής ταυτοποιούν ο ένας τον άλλο. Ο εξυπηρετητής θα πρέπει να αποδείξει την ταυτότητά του στον πελάτη πριν ο πελάτης παρουσιάσει την πιστοποίησή του. Αυτή η τεχνική μειώνει τον κίνδυνο της απρόσεκτης αποκάλυψης ιδιωτικών πληροφοριών στους χάκερ. Τα βήματα του αμοιβαίου έλεγχου ταυτότητας παρουσιάζονται παρακάτω:

1. Η πρόσβαση σε προστατευόμενο πόρο ζητείτε από τον πελάτη.
2. Το πιστοποιητικό του εξυπηρετητή παρουσιάζεται στον πελάτη.
3. Το πιστοποιητικό επαληθεύεται από τον πελάτη.
4. Εάν είναι επιτυχής το πιστοποιητικό του πελάτη στέλνεται στον εξυπηρετητή.
5. Το πιστοποιητικό του πελάτη επαληθεύεται από τον εξυπηρετητή.
6. Εάν είναι επιτυχής, η πρόσβαση χορηγείτε στον πελάτη.

Προκειμένου να αποφευχθούν οι επιθέσεις ηλεκτρονικού ψαρέματος ένα ισχυρό μοντέλο ασφαλείας πρέπει να είναι τυποποιημένο και ευρέως γνωστό. Ωστόσο ένα μοντέλο ασφαλείας περιλαμβάνει πολλούς συμμετέχοντες με διαφορετικά συμφέροντα. Χρήστες, προγραμματιστές ιστοσελίδων και η επιτροπή προτύπων δεν είναι εύκολο να καταλήξουν σε συμφωνία μεταξύ τους. Τα πρότυπα ασφαλείας χρειάζονται πολλά χρόνια για να πάρουν επικύρωση, υιοθέτηση και να εφαρμοστούν. Αφού οι επιθέσεις ηλεκτρονικού ψαρέματος εξελίσσονται γρήγορα, τα πρότυπα ασφαλείας μπορεί να γίνουν μερικώς παρωχημένα ακόμα και αν δεν έχουν επικυρωθεί. Οι χρήστες του διαδικτύου που δίνουν αρκετή προσοχή σε λεπτομέρειες όπως το πώς φαίνονται οι ιστοσελίδες και οι διευθύνσεις τους είναι λιγότεροι από εκείνους που δεν τα προσέχουν. Υπάρχουν πάρα πολλοί χρήστες

που μπορούν να εξαπατηθούν από τους χάκερ και είναι αδύνατον να αποφευχθούν πλήρως οι επιθέσεις τέτοιου είδους.[57]

3.7 Click fraud

Το Click fraud ή η απάτη με τα ψευδή κλικ είναι η πρακτική σύμφωνα με την οποία κάποιος κάνει κλικ σε μια διαφήμιση χωρίς στην πραγματικότητα να έχει την πρόθεση να επισκεφθεί την ιστοσελίδα, με σκοπό να πάρει χρήματα από την διαφήμιση με την μέθοδο CPC (κόστος ανά κλικ) ή για να δημιουργήσει ψεύτική κίνηση στην ιστοσελίδα.Με την μέθοδο CPC (κόστος ανά κλικ) ο διαφημιστής πληρώνεται ανάλογα με το πόσα κλικ έγιναν στην διαφήμιση του διαφημιζόμενου. Η αναξιοπιστία της διαφημιστικής μεθόδου CPC (κόστος ανά κλικ) οδήγησε τις διαδικτυακές διαφημιστικές εταιρείες στη δημιουργία νέων μεθόδων όπως είναι το CPA (κόστος ανά ενέργεια). Με την μέθοδο αυτή ο διαφημιζόμενος πληρώνει μόνο όταν ο χρήστης που επισκέφτηκε την ιστοσελίδα πραγματοποίησε κάποια επιθυμητή ενέργεια, π.χ. αγόρασε κάποια προϊόντα ή συμπλήρωσε κάποια στοιχεία.

Το 2004 ο Michael Bradley δημιούργησε ένα λογισμικό με το οποίο θα μπορούσε να εξαπατήσει την Google και να βγάλει εκατομμύρια δολάρια μέσα από τα ψευδή κλικ. Χρησιμοποιώντας την τεχνολογία που δημιούργησε ήταν σε θέση να αποδείξει ότι η απάτη θα μπορούσε να πραγματοποιηθεί και θα ήταν αδύνατον για την Google να την ανιχνεύσει. Απαίτησε από την Google 100.000 δολάρια για το λογισμικό του και το 2006 συνελήφθη για εκβιασμό.[60]

3.7.2 Πως λειτουργεί το Click fraud

Τα ψευδή κλικ μπορεί να διαπράττονται από ανθρώπους και από αυτοματοποιημένα προγράμματα ηλεκτρονικού υπολογιστή, τα οποία μιμούνται τους νόμιμους χρήστες κάνοντας κλικ σε διαφημίσεις χωρίς να έχουν πραγματικό ενδιαφέρον για αυτές. Οι ιδιοκτήτες των ιστοσελίδων μπορούν να κάνουν οι ίδιοι κλικ σε διαφημίσεις που φιλοξενούν. Το κίνητρο αυτού του είδους της απάτης είναι να κερδίσουν περισσότερα χρήματα από τους διαφημιζόμενους.

Ένα άλλο είδος απάτης θεωρούνται και τα ασταμάτητα κλικ από ανταγωνιστές των διαφημιζομένων. Με αυτόν τον τρόπο καταφέρνουν να εξαντλούν την διαθέσιμη επένδυση του ανταγωνιστή τους σε προβολή μέσω του διαδικτύου, καθώς εκείνος έχει προκαθορίσει το ποσό που είναι διατεθειμένος να ξοδέψει για τις εμφανίσεις των διαφημίσεών του.

Οι απάτες των ψεύτικων κλικ μπορεί να είναι πιο καταστροφικές όταν χρησιμοποιούνται ολόκληρα δίκτυα υπολογιστών (botnet). Ο επιτιθέμενος μπορεί να μολύνει με κακόβουλο λογισμικό μεγάλο δίκτυο υπολογιστών και να δώσει εντολές έτσι ώστε να επισκεφτούν ορισμένες τοποθεσίες κάνοντας κλικ σε διαφημίσεις και δημιουργώντας πολλά φαινομενικά άσχετα κλικ από διαφορετικές διευθύνσεις IP.[61]

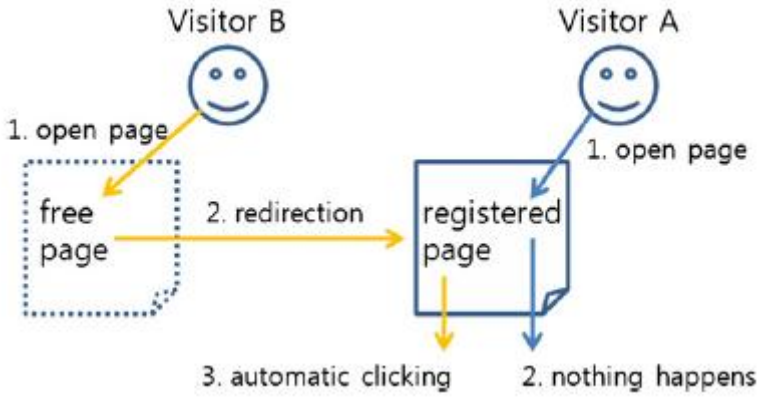
3.7.3 Μορφές και τεχνικές αντιμετώπισης των ψευδών κλικ

Τα ψευδή κλικ συχνά διαπράττονται από ιδιοκτήτες ιστοσελίδων οι οποίοι κάνουν επανειλημμένα κλικ σε διαφημίσεις που φιλοξενούν με σκοπό να κερδίσουν περισσότερα χρήματα. Παρακάτω παρουσιάζονται κάποιες μορφές και τεχνικές αντιμετώπισης των ψεύτικων κλικ.

Μια μορφή ψεύτικων κλικ είναι να διογκώνει τον αριθμό των πλαστών επισκεπτών αλλάζοντας αλλεπάλληλα τις ταυτοποιήσεις τους όπως τα cookies και την διεύθυνση IP τους. Πλέον οι πάροχοι υπηρεσιών διαδικτύου εκχωρούν μια νέα διεύθυνση IP σε έναν υπολογιστή εάν αυτός επανασυνδεθεί με το διαδίκτυο. Με αυτόν τον τρόπο οι επιτιθέμενοι μπορούν να αποκτούν νέες διευθύνσεις IP ανανεώνοντας επανειλημμένα την σύνδεσή τους στο διαδίκτυο και αλλάζοντας τα στοιχεία των πλαστών επισκεπτών.[62]

Ένα άλλο είδος απάτης των ψεύτικων κλικ χρησιμοποιεί ζεύγος σελίδων (μια καταχωρημένη και μια ελεύθερη, προκειμένου να κρύψει τα αυτόματα κλικ. Οι διαφημίσεις φιλοξενούνται στην καταχωρημένη σελίδα, ενώ η ελεύθερη δεν έχει καμία σχέση με την διαφήμιση. Η καταχωρημένη σελίδα έχει δυο τρόπους δράσης. Εάν ο χρήστης επισκέπτεται την καταχωρημένη σελίδα κατευθείαν (επισκέπτης Α στην εικόνα 8) αυτή συμπεριφέρεται ως κανονική σελίδα και δεν προκαλεί ψεύτικα κλικ. Εάν ο χρήστης επισκέπτεται την ελεύθερη σελίδα (επισκέπτης Β στο

σχήμα 1) τότε αυτόματα ανακατευθύνεται στην καταχωρημένη σελίδα. Η καταχωρημένη σελίδα αναγνωρίζει ότι ο χρήστης ανακατευθύνθηκε από την ελεύθερη σελίδα και δημιουργεί κλικ σε διαφημίσεις. Αν η επιτροπή ελέγχου διαφημίσεων ελέγξει την επίσημη ιστοσελίδα για τα ψευδή κλικ, δεν θα βρει τίποτα. Για τον εντοπισμό αυτού του είδους της απάτης τα ζεύγη σελίδων θα πρέπει να προσδιορίζονται από την ανάλυση των αρχείων καταγραφής των πάροχων υπηρεσιών διαδικτύου (ISP).[63]



Εικόνα 8 Απάτη των ψεύτικων κλικ που χρησιμοποιεί ζεύγος σελίδων

3.8 Παραβίαση ψηφιακών δικαιωμάτων ιδιοκτησίας

Στο διαδίκτυο η κοινή χρήση αρχείων ήταν το πρωταρχικό μέσο με το οποίο μπορούσε κανείς να κατεβάσει δωρεάν παράνομα ψηφιακά αρχεία τα οποία είχαν πνευματικά δικαιώματα. Η κοινή χρήση των αρχείων χρονολογείται από τη δεκαετία του 1980. Ο διαμοιρασμός των μουσικών αρχείων σε μορφή MP3 έγινε παγκόσμιο φαινόμενο μετά την κυκλοφορία του Napster το 1999. Το Napster ήταν ένα σύστημα ανταλλαγής αρχείων το οποίο επέτρεπε στους χρήστες να μοιράζονται μουσικά αρχεία χρησιμοποιώντας την τεχνολογία peer to peer (P2P). Το Napster έπαψε να λειτούργει μετά από μήνυση που κατέβαλε η Αμερικανική Ένωση Μουσικής Βιομηχανίας. Στις μέρες μας υπάρχουν ακόμα πάρα πολλοί διαμοιραστές αρχείων όπως το Bittorrent, το Bearshare και το Shareza.[64]

Ο διαμοιρασμός των αρχείων γινόταν και μέσα από τα chatrooms. Τα μέλη των chatrooms μοιράζονταν μεταξύ τους πειρατικά αντίγραφα ταινιών, παιχνιδιών,

λογισμικού και μουσικής. Με τον ερχομό στην αγορά των δίσκων CD, των ιστοσελίδων διαμοιρασμού αρχείων και την ψηφιοποίηση της μουσικής, οι άνθρωποι άρχισαν να αντιγράφουν τα αρχεία μουσικής από τους δίσκους και να τα φυλάνε στους υπολογιστές τους μοιράζοντάς τα μεταξύ τους χωρίς να πληρώνουν τίποτε στη μουσική βιομηχανία. Έχοντας δει σημαντική πτώση στις πωλήσεις η μουσική βιομηχανία επέβαλε την τεχνολογία DRM για να προστατέψει τα μουσικά αρχεία και να αποτρέψει την παράνομη λήψη και διανομή τους στο διαδίκτυο.[1]

3.8.2 Πως λειτουργεί η παραβίαση ψηφιακών δικαιωμάτων ιδιοκτησίας

Η διαχείριση ψηφιακών δικαιωμάτων (DRM) είναι ένας όρος που αναφέρεται σε οποιοδήποτε σύστημα που ελέγχει την πρόσβαση σε ψηφιακό υλικό που έχει πνευματικά δικαιώματα, χρησιμοποιώντας τεχνολογικά μέσα. Η πρώτη γενιά τεχνολογιών DRM έλεγχε μόνο την αντιγραφή. Η δεύτερη γενιά στόχευε στον έλεγχο της προβολής, της αντιγραφής και της εκτύπωσης. Ένα σύστημα διαχείρισης ψηφιακών δικαιωμάτων λειτουργεί σε τρία επίπεδα: τη θέσπιση των πνευματικών δικαιωμάτων για το περιεχόμενο, την διαχείριση της διανομής του περιεχομένου και τον έλεγχο του πελάτη σχετικά με το τι μπορεί να κάνει με το περιεχόμενο. Για να επιτευχθεί το τελευταίο επίπεδο ελέγχου ένα πρόγραμμα DRM πρέπει να καθορίσει αποτελεσματικά και να περιγράψει τρεις οντότητες: τον χρήστη, το υλικό και τα δικαιώματα χρήσης. Παρακάτω υπάρχει μια επισκόπηση των τεχνολογιών που χρησιμοποιούνται σε συστήματα DRM.[65]

Μερικά συστήματα DRM χρησιμοποιούν ψηφιακό υδατογράφημα. Το ψηφιακό υδατογράφημα είναι χαρακτηριστική πληροφορία αναγνώρισης ενός ηλεκτρονικού αρχείου που τοποθετείτε στα κυρίως δεδομένα του για την πιστοποίηση της ιδιοκτησίας του. Είναι ένα σήμα που έχει εισαχθεί μέσα σε ένα αρχείο ήχου , βίντεο ή εικόνας για να αποτρέψει την παράνομη χρήση του περιεχομένου.Τα συστήματα DRM για τα πολυμέσα συχνά κρυπτογραφούν το υλικό με τέτοιο τρόπο που μόνο μια συγκεκριμένη συσκευή μπορεί να το αναπαραγάγει. Οι δίσκοι DVD χρησιμοποιούν ένα σύστημα κρυπτογράφησης το οποίο εμποδίζει τους χρήστες να βλέπουν τους δίσκους DVD σε μη εξουσιοδοτημένες συσκευές αναπαραγωγής.[66]

3.8.3 Τεχνολογίες DRM

Η τεχνολογία DRM είναι διαφορετική ανάλογα με το είδος του περιεχομένου που έχει ως στόχο να προστατέψει και τις συσκευές στις οποίες καταγράφετε το περιεχόμενο. Παρακάτω υπάρχει μια περίληψη των τεχνολογιών DRM για πέντε τύπους περιεχομένου: τις ταινίες, τα τηλεοπτικά προγράμματα, την μουσική, τα παιχνίδια, και τα ηλεκτρονικά βιβλία. Η τεχνολογία DRM που χρησιμοποιήθηκε στους δίσκους DVD ήταν το CSS Content Scrambling System. Το CSS δημιουργήθηκε το 1996 από το DVDForum και χρησιμοποιεί αλγόριθμο κρυπτογράφησης. Το 1999 παραβιάστηκε από τον Jon Lech Johansen με χρησιμοποιώντας την εφαρμογή DeCSS με την οποία κατάφερε να αναπαράγει κρυπτογραφημένο δίσκο DVD σε σύστημα Linux.

Για την προστασία των προγραμμάτων τηλεόρασης χρησιμοποιήθηκε η CableCard, μια κάρτα ασφαλείας η οποία όταν τοποθετηθεί στην υποδοχή ενός ψηφιακού τηλεοπτικού δέκτη παρέχει ασφαλή πρόσβαση σε κρυπτογραφημένο ψηφιακό περιεχόμενο. Η CableCard παρέχετε επί πληρωμή από τους παρόχους ψηφιακής τηλεόρασης. Το CPCM είναι ένα πρότυπο διαχείρισης ψηφιακών δικαιωμάτων που αναπτύχθηκε από την DVB. Η κύρια λειτουργία της είναι να διαχειρίζεται τα δικαιώματα της ευρωπαϊκής ψηφιακής τηλεόρασης. Η DVB μια διεθνής βιομηχανία αποτελούμενη από 250 ραδιοτηλεοπτικούς φορείς, κατασκευαστές, φορείς εκμετάλλευσης δικτύων, προγραμματιστές λογισμικού, ρυθμιστικές αρχές σε πάνω από 35 χώρες δημιουργήθηκε για τον σχεδιασμό ανοιχτών τεχνικών προτύπων για την παγκόσμια διανομή ψηφιακού περιεχομένου. Το CPCM καθορίζει τον τρόπο προσθήκης πληροφοριών στο ψηφιακό περιεχόμενο, όπως τα τηλεοπτικά προγράμματα για να περιγράψει το πώς και το εάν το περιεχόμενο μπορεί να χρησιμοποιηθεί από κοινού μεταξύ άλλων συσκευών CPCM. Οι πάροχοι περιεχομένου μπορούν να χρησιμοποιούν μια σειρά από σημαίες που αποθηκεύονται μαζί με το περιεχόμενο για να περιγράψουν το πώς μπορεί να χρησιμοποιηθεί. Όλες οι συσκευές CPCM πρέπει να υπακούουν σε αυτές τις σημαίες. Οι σημαίες μπορεί να επιτρέπουν ή να απορρίπτουν περιεχόμενο εάν αυτό μετακινηθεί ή να αντιγραφεί σε άλλη συσκευή CPCM. Μπορεί επίσης να παρέχεται περιεχόμενο για καθορισμένης προθεσμίας, ή να απαγορεύουν το περιεχόμενο προς αναπαραγωγή ταυτόχρονα σε διαφορετικές συσκευές.

Το 2005 η Sony εισήγαγε μια νέα τεχνολογία DRM η οποία εγκαθιστούσε DRM λογισμικό στους υπολογιστές των χρηστών χωρίς να τους προειδοποιεί. Το FairPlay είναι η τεχνολογία DRM που δημιουργήθηκε από την Apple το 2009. Ήταν ενσωματωμένο στο λογισμικό πολυμέσων QuickTime που χρησιμοποιείτε από όλες τις συσκευές της. Στο τέλος όμως του 2009 όλη η μουσική του iTunes απαλλάχτηκε από την προστασία DRM. Αν και η τεχνολογία DRM χρησιμοποιείτε ευρέως για την μουσική στο διαδίκτυο κάποια διαδικτυακά καταστήματα όπως το Amazon, το Dogmazic το Beatport και το eMusic δεν την χρησιμοποιούν.

Τα ηλεκτρονικά παιχνίδια υπολογιστών χρησιμοποιούν και αυτά μερικές φορές την τεχνολογία DRM για να περιορίσουν τον αριθμό των υπολογιστών στα οποία μπορούν να εγκατασταθούν απαιτώντας αυθεντικοποίηση με εξυπηρετητή στο διαδίκτυο. Τα περισσότερα παιχνίδια με αυτόν τον περιορισμό επιτρέπουν τρεις ή πέντε εγκαταστάσεις, ενώ μερικά επιτρέπουν μια εγκατάσταση να ανακτηθεί εάν το παιχνίδι έχει απεγκατασταθεί. Αυτό όχι μόνο περιορίζει τους χρήστες που έχουν περισσότερους από τρεις ή πέντε υπολογιστές αλλά δημιουργεί και προβλήματα εάν ο χρήστης αναβαθμίσει το λειτουργικό του σύστημα ή επαναδιαμορφώσει το σκληρό του δίσκο. Ανάλογα με το πώς υλοποιείτε το DRM μετρά τις επόμενες επανεγκαταστάσεις ως νέες εγκαταστάσεις καθιστώντας το παιχνίδι άχρηστο μετά από ένα ορισμένο χρονικό διάστημα, ακόμα και αν χρησιμοποιείτε από ένα υπολογιστή. Οι δυο πιο σημαντικές τεχνολογίες της DRM που χρησιμοποιούνται και σήμερα είναι το SecuROM και το Steam.

Οι συσκευές ανάγνωσης των ηλεκτρονικών βιβλίων χρησιμοποιούν την τεχνολογία DRM για να περιορίσουν την αντιγραφή, την εκτύπωση και την κοινή χρήση των ηλεκτρονικών βιβλίων. Ακόμα το DRM περιορίζει το ποιες συσκευές μπορούν να ανοίξουν ένα ηλεκτρονικό βιβλίο, πόσοι διαφορετικοί χρήστες μπορούν να διαβάσουν το ίδιο ηλεκτρονικό βιβλίο και επίσης εμποδίζει την μετατροπή του ηλεκτρονικού βιβλίου σε μια άλλη μορφή. Η χρήση της τεχνολογίας DRM στα ηλεκτρονικά βιβλία δημιουργεί και κάποια προβλήματα στους χρήστες. Για παράδειγμα αγοράζοντας δύο βιβλία από δύο διαφορετικά διαδικτυακά βιβλιοπωλεία με διαφορετικά DRM θα είναι αδύνατον να αναπαραχθούν στην ίδια συσκευή ανάγνωσης γιατί το καθένα θα χρειάζεται ξεχωριστά τον δικό του. Επίσης κάποια συστήματα DRM απαιτούν πρόσβαση στο διαδίκτυο για επικοινωνία με τον κεντρικό server, με αποτέλεσμα το υλικό να μην

μπορεί να χρησιμοποιηθεί εκτός σύνδεσης. Εάν μια εταιρεία που συντηρεί την υπηρεσία ενός συγκεκριμένου DRM κλείσει τότε τα βιβλία που βασίζονται σε αυτό δεν θα μπορούν να ανοιχθούν από εκείνους που τα αγόρασαν.

Τον Ιούλιο του 2009 η Amazon το μεγαλύτερο ηλεκτρονικό βιβλιοπωλείο διέγραψε δυο ηλεκτρονικά βιβλία του συγγραφέα Τζωρτζ Όργουελ με τίτλο 1984 και η φάρμα των ζώων, πιστώνοντας τους λογαριασμούς αυτών που τα είχαν αγοράσει. Η Amazon διέγραψε αυτά τα δυο βιβλία από τις συσκευές των χρηστών μετά από αίτημα του εκδότη ώστε να μην υπάρχουν αντίγραφα σε ηλεκτρονική μορφή. Η διαγραφή των δυο βιβλίων παρομοιάστηκε με παραβίαση της ιδιωτικότητας ενός σπιτιού, την αρπαγή του βιβλίου και την απόθεση χρημάτων στα τραπέζι του σαλονιού.[67]

3.8.4 Αμφισβήτηση DRM

Η τεχνολογία DRM θέτει ένα όριο σχετικά με τον αριθμό και τον τύπο των συσκευών (υπολογιστές, λαπτοπ ,μπ3) στις οποίες ο αγοραστής μπορεί να μεταφέρει ψηφιακά αρχεία και με πόσους μπορεί να τα μοιραστεί. Αυτή η νόμιμη χρήση καθίσταται προβληματική για τον αγοραστή. Πολλοί χρήστες εξοργίστηκαν από το DRM για τους περιορισμούς στα παιχνίδια και αναζήτησαν πειρατικά αντίγραφα των παιχνιδιών και ακόμα κατέθεσαν αγωγές εναντίων των εκδοτών των παιχνιδιών.

Το 1999 ο Τζον Γιόχανσεν ένας νεαρός Νορβηγός δημιούργησε ένα πρόγραμμα (DeCSS) με το οποίο αποκτούσε πρόσβαση σε κωδικοποιημένους δίσκους DVD που είχαν προστασία CSS. Το Δεκέμβριο του 2006 η βασική διαδικασία δημοσιοποιήθηκε στο διαδίκτυο από τους χάκερ επιτρέποντας απεριόριστη πρόσβαση σε κωδικοποιημένο περιεχόμενο στους δίσκους DVD.

Το 2005 η Sony εισήγαγε μια νέα τεχνολογία DRM η οποία εγκαθιστούσε κρυφά λογισμικό DRM το οποίο περιελάμβανε ένα rootkit (κακόβουλο λογισμικό που επιτρέπει τη συνεχή πρόσβαση στον υπολογιστή με προνόμια υπερχρήστη). Όταν το λογισμικό DRM έγινε γνωστό στο κοινό η Sony αναγκάστηκε να ανακαλέσει εκατομμύρια δίσκους και να διανείμει λογισμικό για να αφαιρέσει αυτό το rootkit. Η τεχνολογία DRM της Sony θα μπορούσε να παρακαμφθεί

κρατώντας πατημένο το πλήκτρο Shift κατά την εισαγωγή του δίσκου ή απενεργοποιώντας τη λειτουργιά της αυτόματης εκτέλεσης. Με αυτόν τον τρόπο τα μουσικά κομμάτια θα μπορούσαν να αναπαραχθούν και να ξαναεγγραφθούν εκ νέου, παρακάμπτοντας έτσι το DRM εξ ολοκλήρου.[]

Το 2007 η δισκογραφική εταιρία EMI σταμάτησε την έκδοση μουσικών δίσκων που είχαν τεχνολογία DRM. Οι τέσσερεις μεγάλες δισκογραφικές εταιρείες (Universal, SonyBMG, EMI και Warner) δεν διανέμουν πια μουσικούς δίσκους με προστασία DRM. Πολλές μεγάλες εταιρείες διανομείς μουσικής έχουν επιλέξει και αυτά να διανέμουν μουσικούς δίσκους χωρίς προστασία DRM.

Τέλος υπάρχουν δυο θεμελιώδη προβλήματα από την χρήση της τεχνολογίας DRM. Το πρώτο είναι ο περιορισμός της χρήσης των ψηφιακών μέσων και των συσκευών στα όποια οι άνθρωποι μπορούν να αναπαράγουν το ψηφιακό περιεχόμενο και το δεύτερο είναι η νοοτροπία των ανθρώπων που έχουν συνηθίσει να κατεβάζουν ψηφιακό περιεχόμενο και υπηρεσίες δωρεάν από το διαδίκτυο.[67][1][68]

ΚΕΦΑΛΑΙΟ 4 Η σκοτεινή πλευρά χωρίς χρήση της τεχνολογίας

4.1. Νομοθεσία

Πολλές χώρες έχουν θεσπίσει νόμους στον αγώνα τους κατά του σπαμ, τη διάδοση του κακόβουλου λογισμικού, το hacking, τις επιθέσεις Dos, το ηλεκτρονικό ψάρεμα, τα ψευδή κλικ και κατά την παραβίαση των ψηφιακών δικαιωμάτων ιδιοκτησίας.

Στις μέρες μας οι νόμοι που έχουν σχέση με τον διαδικτυακό εκφοβισμό, τα διαδικτυακά παιχνίδια, τα ψηφιακά δικαιώματα ιδιοκτησίας και το σπαμ είναι ανεπαρκή. Ωστόσο πάρα πολλές χώρες έχουν θεσπίσει νόμους κατά του σπαμ. Για παράδειγμα η Ευρωπαϊκή Ένωση πέρασε το άρθρο 13 για την προστασία προσωπικών δεδομένων και ηλεκτρονικών επικοινωνιών το 2002. Η Αυστραλία υιοθέτησε νομοσχέδιο κατά του σπαμ το 2003. Η Αγγλία με τον νόμο για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες το 2003. Το πρόβλημα με τους νόμους κατά του σπαμ είναι ότι δεν τηρούνται από τους σπαμερς. Οι περισσότερες χώρες αυτήν την στιγμή έχουν νόμους κατά του χακινγκ. Για παράδειγμα ο νόμος περί ηλεκτρονικής απάτης και κατάχρησης που ψηφίστηκε το 1986 στην Αμερική. Ο νόμος Computer Misuse του 1990 που ψηφίστηκε από το κοινοβούλιο της Αγγλίας ποινικοποιεί το χακινγκ.[69][70][71]

4.2. Η επιβολή του νόμου

Πολλές κυβερνήσεις δεν έχουν επαρκή προϋπολογισμό ή ακόμα και αν έχουν, δεν διαθέτουν αρκετό εκπαιδευμένο ανθρώπινο δυναμικό για να ασχοληθεί με τους απατεώνες του κυβερνοχώρου. Πράγματι πολλές κυβερνήσεις δεν έχουν ακόμα νόμους για τα εγκλήματα του κυβερνοχώρου. Ωστόσο σε οποιαδήποτε χώρα η ποινική δικαιοσύνη προχωράει με αργούς ρυθμούς, ειδικά σε σύγκριση με την ταχύτητα με την οποία η σκοτεινή πλευρά του διαδικτύου εξαπλώνεται. Παρά την μη ικανοποιητική αυτή κατάσταση υπήρξαν πολλές σημαντικές συλλήψεις που έλαβαν ευρεία κάλυψη από τα μέσα μαζικής ενημέρωσης κατά την διάρκεια των τελευταίων ετών και παρουσιάζονται παρακάτω:[1]

Το 2008 η Ομοσπονδιακή Επιτροπή Εμπορίου έκλεισε μια ομάδα spam με το όνομα Herbalking, οι οποία προωθούσε αντίγραφα ρολογιών και μεγάλη ποικιλία φαρμακευτικών προϊόντων. Η ομάδα Herbalking είχε συνεργούς σε πολλές χώρες όπως Αμερική, Αυστραλία, Νέα Ζηλανδία, Ινδία και Κίνα. Χρησιμοποίησε ένα δίκτυο botnet αποτελούμενο από 35000 υπολογιστές για να στέλνουν 10 δισεκατομμύρια μηνύματα ηλεκτρονικού ταχυδρομείου ημερησίως.[72]

Το 2009 στην Αμερική εξαρθρώθηκε ένα κύκλωμα διαδικτυακών εγκληματιών που έκανε επιθέσεις ηλεκτρονικού ψαρέματος (phishing). Στο κύκλωμα εμπλέκονταν 53 μέλη από την Αμερική και την Αίγυπτο. Έστελναν από την Αίγυπτο μαζικά μηνύματα ηλεκτρονικού ταχυδρομείου για να υποκλέψουν κωδικούς πρόσβασης από τους λογαριασμούς των χρηστών. Οι άνθρωποι που άνοιγαν αυτά τα μηνύματα ηλεκτρονικού ταχυδρομείου μεταφέρονταν αυτόματα σε πλάστες ιστοσελίδες των δυο μεγαλύτερων τραπεζών της Αμερικής. Το κύκλωμα κατάφερε με αυτόν τον τρόπο σε διάστημα δυο μισή χρόνων να κλέψει δυο εκατομμύρια δολάρια.[73]

Το 2005 η αστυνομία της Βραζιλίας συνέλαβε τον Valdir Paulo de Almeida αρχηγό μιας συμμορίας που έκανε επιθέσεις ηλεκτρονικού ψαρέματος (phishing), και σε χρονικό διάστημα δυο χρόνων κατάφεραν να κλέψουν 37 εκατομμύρια δολάρια. Η συμμορία έστελνε πάνω από 3 εκατομμύρια μηνύματα ηλεκτρονικού ταχυδρομείου σε καθημερινή βάση. Τα μηνύματα ηλεκτρονικού ταχυδρομείου περιείχαν έναν δούρειο ίππο ο οποίος έκλεβε τους κωδικούς των πιστωτικών καρτών των θυμάτων. [74]

Το 2004 το FBI της Αμερικής συνέλαβε αρκετά άτομα που συνδέονταν με μέλη της μαφιόζικης συμμορίας Γκαμπίνο. Για την διενέργεια της άπατης είχαν αγοράσει μια τράπεζα και μια εταιρία τηλεφωνίας κάνοντας την μεγαλύτερη απάτη του διαδικτύου στην ιστορία με τζίρο που ξεπερνούσε τα 400 εκατομμύρια δολάρια.[75]

Τον Δεκέμβριο του 2001 η Αμερική, η Αγγλία, η Αυστραλία, η Σουηδία, η Φινλανδία, η Νορβηγία και η Γερμανία ξεκίνησαν παγκόσμιες επιδρομές με την κωδική ονομασία Operation Buccaneer με σκοπό να σταματήσουν την δράση των

ομάδων διαδικτυακών εγκληματιών εκείνης της εποχής όπως Razor1911, DrincorDie και RiSC. [76]

4.3. Δίκη

Η μουσική βιομηχανία έχει χτυπηθεί άσχημα από τον πολλαπλασιασμό των δωρεάν προγραμμάτων διαμοιρασμού αρχείων , τα οποία επιτρέπουν σε εκατομμύρια ανθρώπους να μοιράζονται ελεύθερα και χωρίς χρέωση μουσικά αρχεία μέσω του διαδικτύου. Η Αμερικανική ένωση μουσικής βιομηχανίας (RIAA) κατέφυγε σε δικαστικές διαμάχες. Μήνυσε παράνομες ιστοσελίδες διαμοιρασμού αρχείων όπως το Napster, Aimster, Grokster, και AudioGalaxy. Αυτές οι ιστοσελίδες είτε έπαψαν να λειτουργούν, είτε λειτουργούν νόμιμα πληρώνοντας για τα δικαιώματα των τραγουδιών. Η (RIAA) έχει μηνύσει ακόμα και άτομα τα οποία κατέβαζαν και διένεμαν μουσικά αρχεία στο διαδίκτυο. Ένας από αυτούς είναι ο Τζόελ Τεχενμπάουν, φοιτητής από το πανεπιστήμιο της Βοστώνης, ο οποίος έχασε την δίκη και τιμωρήθηκε με πρόστιμο 675,000 δολαρίων για κατέβασμα και διανομή 30 τραγουδιών.[77]

4.4. Διεθνή συνεργασία

Δεδομένου ότι τα εγκλήματα στον κυβερνοχώρο διασχίζουν (δεν έχουν) τα εθνικά σύνορα, οι διεθνείς συνεργασίες και οι διεθνείς συμφωνίες είναι απαραίτητες για να τα νικήσουν. Οι διεθνείς συνεργασίες έχουν πράγματι λάβει χώρα για την πάταξη των διαβόητων απατεώνων του κυβερνοχώρου. Όπως ξέρουμε πολλές ομάδες πειρατών του κυβερνοχώρου σταμάτησαν τις δράσεις τους *ως* αποτέλεσμα *των* διεθνώς συνεργασιών. Πολλές χώρες συνεργάζονται για να σταματήσουν τα κακόβουλα λογισμικά, τις επιθέσεις άρνησης εξυπηρέτησης και για να συλλάβουν εκείνους που είναι αρμόδιοι για την έναρξη και την ενίσχυση των επιθέσεων. Υπάρχουν κάποιοι θεμελιώδεις περιορισμοί στις διεθνείς συνεργασίες. Οι spammerskαι οι εγκληματίες του κυβερνοχώρο χρησιμοποιούν τυπικά ανοικτούς διακομιστές μεσολάβησης που βρίσκονται σε άλλες χώρες για να αποφύγουν την ανακάλυψη και τη δίωξη. Πολλοί από αυτούς έχουν αποφύγει την

σύλληψη για μεγάλο χρονικό διάστημα. Υπάρχουν διάφοροι λόγοι για τους περιορισμούς στις διεθνείς συνεργασίες και είναι οι παρακάτω:

1. Η κάθε χώρα έχει τους δικούς τις νόμους για τα εγκλήματα στον κυβερνοχώρο, ενώ κάποιες δεν έχουν καν νόμους. Μερικές χώρες τιμωρούν τους απατεώνες του κυβερνοχώρου με πολυετή φυλάκιση, ενώ άλλες όχι. Για παράδειγμα στις ΗΠΑ τα τυχερά παιχνίδια στο διαδίκτυο είναι παράνομα ενώ στην Αγγλία , την Γάλλια και σε κάποιες άλλες χώρες είναι νόμιμα. Άλλο ένα παράδειγμα είναι ότι ορισμένες χώρες μπλοκάρουν τις ιστοσελίδες κοινωνικών δικτύων που επιτρέπουν πορνογραφικό υλικό, ενώ κάποιες άλλες δεν το κάνουν. Κάποιες μπλοκάρουν ιστοσελίδες κοινωνικών δικτύων που χρησιμοποιούνται από ανθρώπους για οργάνωση κινητοποιήσεων ενάντια σε κυβερνήσεις ενώ κάποιες δεν το απαγορεύουν.
2. Χρειάζεται πολύς χρόνος για να αλλάξει η υπάρχουσα νομοθεσία και πιθανώς ακόμα περισσότερος χρόνος ώστε να δημιουργηθούν νέοι νόμοι προκειμένου να ισχύουν σε διεθνείς συνεργασίες.
3. Η κάθε χώρα έχει διαφορετική δυνατότητα επιβολής του νόμου. Στην πραγματικότητα οι περισσότερες αν όχι όλες οι χώρες έχουν χάσει την μάχη ενάντια σε εγκλήματα στον κυβερνοχώρο.
4. Άνθρωποι από διαφορετικές χώρες συμμορφώνονται με τον νόμο και την ηθική σε διαφορετικό βαθμό. Για παράδειγμα ο Όνελ Ντε Γκούζμαν ένας Φιλιππινέζος φοιτητής πληροφορικής που δημιούργησε και διέδωσε τον ιό «LoveByg» το 2000 και προξένησε ζημιές εκατομμυρίων δολαρίων σε όλο τον κόσμο. Αναγνωρίστηκε από τον Φιλιππινέζικο λαό ως εθνικός ήρωας, επειδή έδειξε στο κόσμο την τεχνική ικανότητα των Φιλιππινέζων.
5. Μερικές χώρες απλά δεν θέλουν ή δεν εμπιστεύονται άλλες χώρες για να συνεργαστούν για ζητήματα όπως τα διασυνοριακά εγκλήματα στον κυβερνοχώρο.
6. Μερικές χώρες δεν βλέπουν την ανάγκη να καταδιώξουν (συλλάβουν) απατεώνες του κυβερνοχώρου όταν αυτοί προκαλούν ζημιές σε ανθρώπους και υπολογιστές σε άλλες χώρες.

Οι ολοκληρωμένες διεθνείς συμφωνίες για τα εγκλήματα στον κυβερνοχώρο απέχουν πολύ ώστε να πραγματοποιηθούν. Η σύμβαση για τα εγκλήματα στον κυβερνοχώρο είναι μια διεθνής συνθήκη που υπογράφηκε από 46 χώρες το 2001. Ωστόσο αντί να προσχωρήσουν στη σύμβαση οι αναπτυσσόμενες χώρες θέλουν μια νέα συνθήκη στην οποία θα μπορούν να συμμετέχουν από την αρχική της σύνταξη. Η Ρωσία που υποστηρίζεται από αναπτυσσόμενες χώρες πρότεινε μια ενωμένη εθνική συνθήκη για τα εγκλήματα στον κυβερνοχώρο, αλλά αυτή απορρίφθηκε το 2010 λόγο αντιθέσεων από την Αμερική και τις ευρωπαϊκές χώρες. [1][78]

4.5. Εθελοντικές δράσεις

Υπάρχουν πολυάριθμες εθελοντικές ομάδες που βοηθούν στην καταπολέμηση των εγκλημάτων στον κυβερνοχώρο. Οι ομάδες αυτές μπορούν να ταξινομηθούν σε τέσσερεις κατηγορίες :

- Εκείνες οι οποίες συλλέγουν και παρέχουν πληροφορίες.
- Εκείνες οι οποίες αναπτύσσουν προϊόντα τεχνολογίας για την αντιμετώπιση των εγκλημάτων στον κυβερνοχώρο.
- Εκείνες οι οποίες υποστηρίζουν τη δημιουργία των νόμων.
- Εκείνες οι οποίες (καταδιώκουν) τους απατεώνες του κυβερνοχώρου.

Τα ακόλουθα αποτελούν παραδείγματα τέτοιων ομάδων που παρέχουν πληροφορίες στους ανθρώπους για να τους βοηθήσουν στην προστασία έναντι των εγκλημάτων του κυβερνοχώρου.

- Spamhaus Project (https://www.spamhaus.org/): είναι διεθνής μη κερδοσκοπικός οργανισμός του οποίου η αποστολή είναι:
    - Να παρακολουθεί το σπαμ και τις πηγές του στο διαδίκτυο.
    - Να παρέχει αξιόπιστα και σε πραγματικό χρόνο προστασία κατά του σπαμ στα δίκτυα.
    - Να συνεργάζεται με υπηρεσίες επιβολής του νομού για να εντοπίζουν και καταδιώκουν σπαμ συμμορίες σε όλο τον κόσμο.
    - Να ασκεί πιέσεις στις κυβερνήσεις για την αποτελεσματική νομοθεσία κατά του σπαμ.

- Anonymous Postmasters Early Warnings System (http://www.apews.org/): είναι ένας κατάλογος των περιοχών στο διαδίκτυο τον οποίο κάποιοι διαχειριστές του συστήματος και άλλοι φορείς παροχής υπηρεσιών έχουν συγκεντρώσει για την καταπολέμηση του σπαμ.
- Shadow server Fundation (https://www.shadowserver.org/wiki/): είναι μια εθελοντική ομάδα επαγγελματιών εργαζομένων πάνω στην ασφάλεια του διαδικτύου που συγκεντρώνει τραγούδια και εκθέσεις σχετικά με το κακόβουλο λογισμικό του botnet (δίκτυο υπολογιστών ζόμπι) και την ηλεκτρονική άπατη.
- Anti-Phishing Working Group (http://www.antiphishing.org/): είναι μια παγκόσμια βιομηχανική και νομοθετική ένωση που επικεντρώνεται στην καταπολέμηση της άπατης και της κλοπής ταυτότητας που προκύπτουν από το ηλεκτρονικό ψάρεμα.
- PhishTank (https://www.phishtank.com/): είναι μια υπηρεσία που έχει ως στόχο την καταπολέμηση του ηλεκτρονικού ψαρέματος.
- Millersmiles (http://www.millersmiles.co.uk/): παρουσίασε πρώτη στον κόσμο υπηρεσία ειδοποίησης απάτης χρησιμοποιώντας ροές RSS. Οι ροές ειδήσεων έχουν χρησιμοποιηθεί για την καταπολέμηση επιθέσεων ηλεκτρονικού ψαρέματος.
- Honeyports (https://www.honeynet.org/): συλλέγουν πληροφορίες σχετικά με τα κίνητρα και τις τακτικές επιθέσεων των χάκερ. Είναι ένα σύστημα που χρησιμοποιείτε για να προσελκύσει επιτιθέμενους να το επιτεθούν έτσι ώστε να αναλύσει τα στοιχεία της επίθεσης.
- StopCyberBulling.org (http://stopcyberbulling.org/): έχει ως στόχο να βοηθήσει γονείς και εκπαιδευτικούς να βοηθήσουν παιδιά και φοιτητές να αντιμετωπίσουν τον εκφοβισμό στο κυβερνοχώρο, με συμβουλές για το πώς να το σταματήσουν και ποια μέτρα πρέπει να πάρουν.

Τα ακόλουθα είναι παραδείγματα ομάδων που αναπτύσσουν τεχνολογικές λύσεις για τα εγκλήματα στον κυβερνοχώρο:

- Conficker Working Group: είναι οργανισμός που σχηματίστηκε για να κατανοήσει και να εξαλείψει τον ιό Conficker. Αποτελείτε από ερευνητές ασφαλείας, από πωλητές λογισμικού και από πανεπιστημιακούς ερευνητές.
- StopBadware (https://www.stopbadware.org/): είναι ένας μη κερδοσκοπικός οργανισμός που έχει ως στόχο την καταπολέμηση του κακόβουλου λογισμικού. Η δουλειά του είναι να κάνει το διαδίκτυο ασφαλέστερο μέσω της πρόληψης και μείωσης των κακόβουλων ιστοσελίδων.
- The National Anti-hacking Group (http://www.nag.co.in/): είναι η μεγαλύτερη μη κερδοσκοπική οργάνωση αποτελούμενη από χάκερ και από ειδικούς πάνω σε θέματα ασφαλείας από όλο τον κόσμο, που συμμετέχουν στη δημιουργία της ευαισθητοποίησης στον τομέα της ασφάλειας στον κυβερνοχώρο και για να μειώσουν τα αυξανόμενα εγκλήματα στον κυβερνοχώρο.
- The Summit Open Source Development Group (http://www.sosdg.org/): προωθεί την ανάπτυξη του λογισμικού ανοιχτού κώδικα για την καταπολέμηση των μεθόδων σπαμ.

Τα ακόλουθα είναι παραδείγματα ομάδων που υποστηρίζουν τη δημιουργία και την υιοθέτηση των νόμων κατά των εγκλημάτων στον κυβερνοχώρο:

- CAUCE (http://www.cauce.org/): είναι μια εθελοντική οργάνωση υπεράσπισης καταναλωτών κατά των επιθέσεων σπαμ.[1]

4.6. Εκπαίδευση

Κυβερνητικές υπηρεσίες, σχολεία, μέσα ενημέρωσης, επιχειρήσεις και ομάδες εθελοντών έχουν κάνει προσπάθεια για να εκπαιδεύσουν τον κόσμο σχετικά με τους τρόπους προφύλαξης από τα περισσότερα στοιχεία της σκοτεινής πλευράς του διαδικτύου, Τα μαθήματα περιλαμβάνουν ασφαλή χρήση του διαδικτύου ειδικά τις ιστοσελίδες των κοινωνικών δικτύων για εφήβους και τους γονείς τους. Προειδοποιήσεις κατά της ένταξης σε ιστοσελίδες με θέματα αυτοκτονιών, προειδοποιήσεις για διαφόρων ειδών απάτες του διαδικτύου και του ηλεκτρονικού εμπορίου. Συμβουλές για την ασφάλεια του υπολογιστή από κακόβουλα λογισμικά

και προειδοποιήσεις κατά του ηλεκτρονικού ψαρέματος. Παρακάτω υπάρχουν ομάδες και οργανισμοί που προσπαθούν να εκπαιδεύσουν τον κόσμο να προστατευτεί από τα εγκλήματα του κυβερνοχώρου.

1. Cyber Citizen Partnership (http://www.cybercitizenship.org/): εκπαιδεύει τα παιδιά και τους ενήλικες για τους κινδύνους και τις συνέπειες των εγκλημάτων στον κυβερνοχώρο.
2. Cyber Angels (http://www.cyberangels.org/): Ξεκίνησε το 1995 και είναι ένα από τα παλαιότερα και πιο σεβαστά προγράμματα εκπαίδευσης στον κόσμο.
3. GetNetWise (http://www.getnetwise.org/): Ιδρύθηκε το 1999 και παρέχει εκπαιδευτικό υλικό για την ασφάλεια στο διαδίκτυο για τους γονείς και για τους εκπαιδευτικούς ώστε να μπορούν να διδάξουν τους νέους.
4. The Internet Keep Safe Coalition (http://www.ikeepsafe.org/): Είναι ενας μη κερδοσκοπικός οργανισμός και ιδρύθηκε το 2005. Αποτελείτε πάνω από 100 μέλη ανάμεσα στους οποίους είναι πολιτικοί ηγέτες, εκπαιδευτικοί, μέλη της επιβολής του νόμου, ειδικοί της τεχνολογίας, εμπειρογνώμονες της δημόσιας υγείας και εισαγγελείς. Μέσα από το δίκτυο υποστήριξης παρακολουθεί τις παγκόσμιες τάσεις και τα ζητήματα γύρω από ψηφιακά προϊόντα και την επιρροή τους στα παιδιά. Αυτή η έρευνα οδηγεί την συνεχή δημιουργία θετικών πόρων για τους γονείς και τους εκπαιδευτικούς οι οποίοι διδάσκουν τους νέους πώς να χρησιμοποιούν νέες συσκευές πολυμέσων και πλατφόρμες με ασφαλή και υγιή τρόπο.
5. Scrambusters (http://www.scambusters.org/): Ιδρύθηκε το 1994 για να βοηθήσει τους ανθρώπους να προφυλαχθούν από τις απάτες του διαδικτύου.
6. Identity Theft Resource Centre (http://www.idtheftcenter.org/): μη κερδοσκοπικός οργανισμός που ιδρύθηκε το 1999 για να παρέχει βοήθεια προς τα θύματα και την εκπαίδευση των καταναλωτών μέσω του τηλεφωνικού κέντρου, της ιστοσελίδας της και τα μέσα κοινωνικής δικτύωσης.
7. National Cyber Security Alliance (https://www.staysafeonline.org/): Η αποστολή της είναι να εκπαιδεύσει και να ενδυναμώσει μια ψηφιακή

κοινωνία για να χρησιμοποιούν το διαδίκτυο με ασφάλεια και σιγουριά στο σπίτι, στην εργασία και στο σχολείο.[1]

4.7. Ευαισθητοποίηση και προσοχή

Όπως στον πραγματικό κόσμο έτσι και στον διαδικτυακό οι άνθρωποι πρέπει είναι ενήμεροι για τους κινδύνους του και να είναι προσεκτικοί για να αποφεύγουν τη σκοτεινή του πλευρά. Για παράδειγμα στον πραγματικό κόσμο οι άνθρωποι έχουν μάθει να μην δίνουν εύκολα ευαίσθητα προσωπικά δεδομένα, να μην μπαίνουν σε συμφωνίες που φαίνονται να είναι πάρα πολύ καλές ώστε να είναι πραγματικές, να μην εμπλέκονται σε φασαρίες και να μην πιστεύουν πάντα αυτά που διαβάζουν ή ακούνε στις ειδήσεις. Για να μην πέφτουν θύματα της σκοτεινής πλευράς του διαδικτυακού κόσμου οι άνθρωποι πρέπει να μάθουν για τους κινδύνους του και να είναι προσεκτικοί. Υπάρχουν πάρα πολλά πράγματα που πρέπει να κάνουν και είναι τα παρακάτω:

1. Οι άνθρωποι πρέπει να αγνοούν διαφημίσεις που προσφέρουν ευκαιρίες δουλειάς και πολύ μεγάλο εισόδημα δουλεύοντας με ημιαπασχόληση από το σπίτι.
2. Οι άνθρωποι πρέπει να αγνοούν τα μηνύματα ηλεκτρονικού ταχυδρομείου από άγνωστα άτομα τα όποια τους ζητάνε χρήματα για οπουδήποτε σκοπό.
3. Πρέπει να αγνοούν μηνύματα ηλεκτρονικού ταχυδρομείου που τους ζητά στοιχειά και κωδικούς πιστωτικών καρτών.
4. Πρέπει να έχουν υπόψη ότι οποιοδήποτε σχόλιο, φωτογραφία ή βίντεο που έχουν ανεβάσει στο διαδίκτυο δεν θα το δουν μόνο φίλοι αλλά θα εξετάζονται προσεκτικά από την αστυνομία, τους μελλοντικούς εργοδότες και όχι μόνο.
5. Δεν πρέπει να πιστεύουν οτιδήποτε έχουν δει ή διαβάσει στο διαδίκτυο γιατί υπάρχουν ανακρίβειες στα μπλογ, στα άρθρα και στα φόρουμ που διαδίδουν ψευδείς πληροφορίες.[1]

ΚΕΦΑΛΑΙΟ 5 Η σκοτεινή πλευρά του ελληνικού διαδικτύου

5.1 Εκφοβισμός

Ένα παράδειγμα εκφοβισμού είναι η υπόθεση του Βαγγέλη Γιακουμάκη στα Γιάννενα με την αυτοκτονία του που τον ανάγκασαν οι συμφοιτητές του, με την βίαιη και άσχημη συμπεριφορά τους μέσω διαδικτύου. Ακόμη, ένα άλλο παράδειγμα είναι σε ένα γνωστό και ιδιωτικό σχολείο των βόρειων προαστίων το 2012. Μια μαθήτρια δέχονταν πειράγματα και πονηρά αστεία από τους συμμαθητές της χωρίς να γνωρίζει το γιατί. Κάποιοι είχαν κλέψει φωτογραφίες της από το προφίλ της στο Facebook, τις παραποίησαν και στη συνέχεια τις διακίνησαν σε όλη τη τάξη της. Τέλος μία διαδικτυακή επίθεση στο Facebook είναι σε έναν γνωστό σκιτσογράφο Αρκάς για ένα σκίτσο που αφορούσε στις διαπραγματεύσεις της κυβέρνησης με τους δανειστές, διότι στο κλίμα της πολιτικής βαρβαρότητας κάποιοι παρεξήγησαν αυτή την ανάρτηση και έκαναν κακοήθη σχόλια και έτσι με εντολή του Αρκά η σελίδα αναστέλλει τις αναρτήσεις μέχρι νεοτέρας.[79]

Εικόνα 9 Το σκίτσο του Αρκάς

5.2 Hacking

Καθημερινά σχεδόν γίνονται επιθέσεις hacking στο ελληνικό διαδίκτυο. Συγκεκριμένα, στις 26/10/2014 πραγματοποιήθηκε επίθεση από χάκερ στην ελληνική τράπεζα Probank. Το χτύπημα αυτό το ανέλαβε ο χάκερ με την ονομασία «Kondor», με την χρήση εξειδικευμένων μεθόδων. Αποτέλεσμα της επίθεσης ήταν να αποκτήσει πλήρη πρόσβαση καθώς και έλεγχο της ηλεκτρονικής σελίδας της τράπεζας. Το παρακάτω αρχείο αποτελεί αρχείο μορφής UNIX/Linux που περιλαμβάνει δεδομένα χρηστών του εξυπηρετητή. Ο «Kondor» με την ικανότητα του να υπάρχει αόρατος στο σύστημα ασφαλείας της τράπεζας και τους διαχειριστές χρησιμοποίησε το παρακάτω αρχείο και με συνδυασμό της σελίδας RFI Remote File Inclusion (απομακρυσμένη εκτέλεση κώδικα) είχε σαν αποτέλεσμα να αποκτήσει πλήρη πρόσβαση στον «εσωτερικό κόσμο» της τράπεζας, αποσπώντας κωδικούς από διαχειριστές και των βάσεων δεδομένων αλλάζοντας έτσι τα αρχεία του εξυπηρετητή. [80]

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
Debian-exim:x:102:102::/var/spool/exim4:/bin/false
juantso:x:1000:1000:,,,:/home/juantso:/bin/bash
identd:x:100:65534::/var/run/identd:/bin/false
sshd:x:101:65534::/var/run/sshd:/bin/false
fetchmail:x:103:65534::/var/run/fetchmail:/bin/sh
mysql:x:104:104:MySQL Server,,,:/var/lib/mysql:/bin/false
wp:x:1001:100::/home/httpd/www:/bin/bash
awstats:x:1002:100::/home/awstats:/bin/false
amarkidis:x:1003:100::/home/amarkidis:/bin/bash
smmta:x:105:105:Mail Transfer Agent,,,:/var/lib/sendmail:/bin/false
smmsp:x:106:106:Mail Submission Program,,,:/var/lib/sendmail:/bin/false
```

Εικόνα 10 Αρχείο UNIX/LINUX

Άλλη χαρακτηριστική επίθεση ήταν στο Υπουργείο Μεταφορών, Υποδομών και Δικτύων. Επίθεση που πραγματοποιήθηκε από μέλη της Greek Hacking Scene.

Είναι μια διαφορετική μορφή επίθεσης που έχει σκοπό να τιμήσουν την μνήμη του νεαρού Αλέξη Γρηγορόπολου. Η παρακάτω εικόνα είναι το κείμενο που αναρτήθηκε και εμφανιζόταν στη σελίδα του Υπουργείου. Την επίθεση αυτή πραγματοποίησαν οι χάκερ dr0pper και Kondor. [81]

Εικόνα 11 Ανάρτηση στην ιστεσελίδα του Υπουργείο Μεταφορών

Στο επόμενο παράδειγμα επίθεσης οι χάκερ είναι μια ομάδα από την γειτονική μας χώρα, Τουρκία. Η ονομασία της ομάδας είναι 1923TURK και είναι πιθανόν η ομάδα που ευθύνεται για την επίθεση που δέχτηκαν οι ιστοσελίδες των αυτοκινητοβιομηχανιών της Dacia και της Renault στην Ελλάδα.

Ο Τούρκος χάκερ με την ονομασία fenerove, εκτός από την επίθεση στην Ελλάδα πραγματοποίησε επιθέσεις και σε άλλες ιστοσελίδες αυτοκινητοβιομηχανιών στο Ισραήλ και την Γεωργία κάνοντας deface. Το deface είναι η αλλαγή της εικόνας εισόδου της ιστοσελίδας και στις συγκεκριμένες περιπτώσεις έκανε αντικατάσταση με το σήμα της ομάδας του που είναι η χρονολογία 1923 καθώς και ο κυματισμός της τουρκικής σημαίας. Είναι φανερό ότι έχει μια αδυναμία στο χώρο των αυτοκινήτων, παρόλα αυτά άλλο ένα συμβάν επίθεσης είναι και η ιστοσελίδα του μη κερδοσκοπικού φιλανθρωπικού ιδρύματος «Το Χαμόγελο Του Παιδιού».[82]

Εικόνα 12 Σήμα ομάδας 1923TURK

5.3 Δούρειος Ίππος

Η διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος προειδοποιεί τους χρήστες του Facebook για έναν ιό (backdoor Trojan) που κάνει αισθητή την παρουσία του με αναρτήσεις πορνογραφικών βίντεων. Συγκεκριμένα, η ανάρτηση αυτή κοινοποιείται από κάποιον φίλο του χρήστη στο «Facebook» και επισημαίνεται με ετικέτα μέχρι και 20 φίλοι. Εάν ο χρήστης πατήσει το πορνογραφικό βίντεο, μεταφέρεται σε μία απατηλή ιστοσελίδα, στο βίντεο σταματάει η αναπαραγωγή του και υποχρεώνει το χρήστη να «κατεβάσει» ένα λογισμικό Adobe Flash Player. Στη συνέχεια, εάν ο χρήστης δεχτεί να «κατεβάσει»το συγκεκριμένο αρχείο, τότε μολύνεται από κακόβουλο λογισμικό (Bckdoor Trojan), το οποίο μετά μπορεί να «παρακολουθεί» κάθε κίνηση του «ποντικιού» και του πληκτρολογίου του μολυσμένου υπολογιστή, υποκλέπτοντας κωδικούς, αριθμούς πιστωτικών καρτών, κωδικούς πρόσβασης κ.α. Επιπρόσθετα, το κακόβουλο λογισμικό έχει τη δυνατότητα μετά την εγκατάσταση του και τη μόλυνση του υπολογιστή να δημοσιεύει αυτόματα στο λογαριασμό του «Facebook» του χρήστη το συγκεκριμένο βίντεο, με σκοπό την παραιτέρω αυτοδιάδοσή του.[83]

5.4 Ηλεκτρονικό ψάρεμα

Θύμα Ηλεκτρονικού ψαρέματος έπεσε ένας άνδρας από τα Γιαννιτσά, όταν ήρθε στο ηλεκτρονικό του ταχυδρομείο μήνυμα που ζητούσε τους προσωπικούς του κωδικούς πρόσβασης από δυο τραπεζικούς λογαριασμούς. Ως αποστολέας του μηνύματος εμφανιζόταν η τράπεζα. Έτσι ο άνδρας εισήγαγε τους κωδικούς του με

αποτέλεσμα οι δράστες να του αποσπάσουν το χρηματικό ποσό των 29.000 ευρώ. [84]

Συμπεράσματα

Με τη χρήση του Διαδικτύου πολλοί χρήστες του έχουν εισβάλλει στην σκοτεινή πλευρά του Διαδικτύου άλλοτε ως θύματα και άλλοτε ως θύτες. Η σκοτεινή πλευρά χωρίζεται σε δύο κατηγορίες τη τεχνολογική και τη μη-τεχνολογική. Οι τεχνολογικές περιλαμβάνουν διάφορες μορφές επίθεσης όπως: spam, malware (κακόβουλο λογισμικό), hacking, ιοί, phising κλπ. Μερικές από τις μη- τεχνολογικές είναι: cyber εκφοβισμός, online τυχερά παιχνίδια, σωματική βλάβη, παραβίαση της ιδιωτικής ζωής, και διάφορες ηλεκτρονικές απάτες.

Αυτές οι μορφές επίθεσης έχουν οικονομικό σκοπό καθώς και ψυχολογικό εις βάρος των άλλων. Μέσα από όλο αυτό τον εκφοβισμό και τις απάτες οδηγούνται πολλοί χρήστες σε σωματική βλάβη, ψυχική διαταραχή, κατάθλιψη και οικονομική απώλεια.

Υπάρχουν διάφορες τεχνικές αντιμετώπισης για την εξάλειψη της σκοτεινής πλευράς όπως διάφορα προγράμματα ελέγχου και προστασίας. Επιπλέον, νομοθεσίες που προστατεύουν τα προσωπικά δικαιώματα του χρήστη, αλλά η ποινική δικαιοσύνηπροχωράει με αργούς ρυθμούς σε αντίθεση με την ανάπτυξη της τεχνολογίας, ενώ παράλληλα είναι χρονοβόρες και δαπανήρες. Επίσης δίαφορες εθελοντικές ομάδες για την αντιμετώπισή αυτού του φαινομένου και διεθνείς συνεργασίες.

Συνοψίζοντας, θα ήταν χρήσιμο ο κάθε χρήστης να γνωρίζει για την πρόληψη για κάθε μορφή επίθεσης και να υπάρχει στοιχειώδη εκπαίδευση για την σωστή χρήση του κυβερνοχώρου, ώστε να μειωθεί σε ένα μεγάλο βαθμό η ηλεκτρονική εξαπάτηση.

Βιβλιογραφία

1. Won Kim*, Ok-Ran Jeong, Chulyun Kim, Jungmin So, The dark side of the Internet: Attacks, costs and responses, Information Systems 36 (2011) 675-705
2. http://en.wikipedia.org/wiki/Internet_fraud
3. http://www.nytimes.com/2009/02/04/technology/internet/04myspace.html
4. www.webvistas.org/topic/736-πορνογραφία στο-διαδίκτυο/
5. http://en.wikipedia.org/wiki/Cyberbullying
6. http://www.nytimes.com/2010/07/28/technology/28eurogamble.html
7. http://www.nytimes.com/2010/07/19/technology/19screen.html
8. http://www.pcworld.com/article/121381/article.html
9. https://dea.lib.unideb.hu/dea/bitstream/handle/2437/105305/Thesis_AZUAMA_titkositott.pdf?sequence=1
10. http://www.kaspersky.gr/category/for-home#tab=prod-4
11. http://www.opus1.com/www/whitepapers/antispamfeb2007.pdf
12. http://www.mcafee.com/uk/
13. http://www.kaspersky.gr/category/for-home#tab=prod-4
14. http://en.wikipedia.org/wiki/HITS_algorithm
15. http://en.wikipedia.org/wiki/Spamdexing
16. http://en.wikipedia.org/wiki/TrustRank
17. http://en.wikipedia.org/wiki/HubSpot
18. http://tech.mit.edu/author/John+Markoff/
19. http://tech.mit.edu/V130/N6/long3.html
20. https://ist.mit.edu/security/malware
21. http://en.wikipedia.org/wiki/Botnet
22. http://www.nytimes.com/2010/08/26/technology/26cyber.html?_r=0
23. http://www.naftemporiki.gr/story/836111/neo-kakoboulo-logismiko-mplokarei-upologistes
24. http://en.wikipedia.org/wiki/Trojan_horse_%28computing%29
25. http://en.wikipedia.org/wiki/Comput

26. http://el.wikipedia.org/wiki/%CE%99%CF%8C%CF%82_%CF%85%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CE%AE
27. http://en.wikipedia.org/wiki/Computer_worm
28. http://el.wikipedia.org/wiki/%CE%A3%CE%BA%CE%BF%CF%85%CE%BB%CE%AE%CE%BA%CE%B9_%CF%85%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CE%AE
29. http://en.wikipedia.org/wiki/Mydoom
30. http://el.wikipedia.org/wiki/%CE%94%CE%BF%CF%8D%CF%81%CE%B5%CE%B9%CE%BF%CF%82_%CE%8A%CF%80%CF%80%CE%BF%CF%82_(%CF%85%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CE%AD%CF%82)
31. http://coolweb.gr/virus-trojan-worm-spyware-adware-malware/
32. http://docs.dal.net/docs/exploitsgr.html#1
33. http://www.pcsteps.gr/1543-%CF%84%CE%B9-%CE%B4%CE%B9%CE%B1%CF%86%CE%BF%CF%81%CE%AC-%CE%AD%CF%87%CE%B5%CE%B9-%CE%AD%CE%BD%CE%B1%CF%82-%CE%B9%CF%8C%CF%82-%CF%85%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CE%AE-%CE%AD%CE%BD/
34. http://el.wikipedia.org/wiki/Spyware#.CE.92.CE.B9.CE.B2.CE.BB.CE.B9.CE.BF.CE.B3.CF.81.CE.B1.CF.86.CE.AF.CE.B1
35. http://windows.microsoft.com/el-gr/windows/spyware-faq#1TC=windows-7
36. http://gr.norton.com/catch-spyware-before/article
37. http://ioys.gr/adware-helpers/
38. http://ti-einai.gr/adware/
39. https://el.wikipedia.org/wiki/%CE%A7%CE%AC%CE%BA%CE%B5%CF%81
40. http://www.sptimes.com/Hackers/history.hacking.html
41. http://www.pare-dose.net/356
42. http://el.wikipedia.org/wiki/%CE%95%CE%BB%CE%BB%CE%B7%CE%BD%CE%B9%CE%BA%CE%AE_%CE%A7%CE%AC%CE%BA%CE

%B9%CE%BD%CE%B3%CE%BA_%CE%A3%CE%BA%CE%B7%CE%BD%CE%AE

43. http://www.nytimes.com/2010/01/21/technology/21password.html?_r=0
44. http://www.dikseo.teimes.gr/spoudastirio/files/%CE%97%20(AN)%CE%91%CE%A3%CE%A6%CE%91%CE%9B%CE%97%CE%A3%20%CE%9F%CE%A8%CE%97%20%CE%A4%CE%9F%CE%A5%20%CE%94%CE%99%CE%91%CE%94%CE%99%CE%9A%CE%A4%CE%A5%CE%9F%CE%A5.pdf
45. http://digilib.lib.unipi.gr/dspace/bitstream/unipi/5277/1/Ktanis.pdf
46. http://digilib.lib.unipi.gr/dspace/bitstream/unipi/4091/1/Karamanis.pdf
47. https://en.wikipedia.org/wiki/Denial-of-service_attack
48. http://cr.yp.to/syncookies.html
49. https://el.wikipedia.org/wiki/IP_spoofing
50. K. Scarfone, P. Mell, Guide to intrusion detection and prevention systems (idps), Technical Report, NIST, National Institute of Stan- dards and Technology, U.S. Department of Commerce, 2007
51. https://el.wikipedia.org/wiki/Phishing
52. https://en.wikipedia.org/wiki/Pharming
53. https://www.sophos.com/en-us/press-office/press-releases/2007/09/ameritrade.aspx
54. https://en.wikipedia.org/wiki/Avalanche_%28phishing_group%29
55. https://el.wikipedia.org/wiki/Phishing
56. https://www.gartner.com/doc/431660/phishing-attack-victims-likely-targets
57. https://el.wikipedia.org/wiki/Phishing
58. http://blog.saush.com/2006/03/11/phishing-securing-internet-banking-4/
59. http://www.azarask.in/blog/post/a-new-type-of-phishing-attack
60. https://en.wikipedia.org/wiki/Click_fraud
61. http://tech.in.gr/news/article/?aid=102318
62. A. Metwally, F. Emekci, D. Agrawal, A. El Abbadi, SLEUTH: single-publisher attack detection using correlation hunting, PVLDB, 2008
63. A. Metwally, D. Agrawal, A. El Abbadi, Using Association Rules for Fraud Detection in Web Advertising Networks, VLDB, 2005.
64. https://en.wikipedia.org/wiki/File_sharing
65. http://computer.howstuffworks.com/drm.htm

66. https://el.wikipedia.org/wiki/%CE%A8%CE%B7%CF%86%CE%B9%CE%B1%CE%BA%CF%8C_%CF%85%CE%B4%CE%B1%CF%84%CF%8C%CF%83%CE%B7%CE%BC%CE%BF
67. https://en.wikipedia.org/wiki/Digital_rights_management
68. https://en.wikipedia.org/wiki/Sony_BMG_copy_protection_rootkit_scandal
69. https://en.wikipedia.org/wiki/Email_spam_legislation_by_country
70. https://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act
71. https://en.wikipedia.org/wiki/Computer_Misuse_Act_1990
72. Brad Stone, Authorities shut down spam ring, The New York Times, October 15, 2008
73. Brad Stone, F.B.I. indicts dozens in online bank fraud, The New York Times, October 8, 2009.
74. http://content.time.com/time/business/article/0,8599,1917345,00.html
75. http://www.americanmafia.com/Feature_Articles_288.html
76. http://news.cnet.com/U.S.-plans-new-raids-on-file-swappers/2100-1023_3-276885.html
77. http://www.techworld.com.au/article/313471/tenenbaum_hit_675_000_fine_music_piracy/
78. K. Archick, Cybercrime: The Council of Europe Convention, CRS Report for Congress RS21208, Congressional Research Service, Washington, DC, 2006.
79. http://www.protothema.gr/greece/article/487917/epithesi-kai-apeiles-kata-tou-arka-gia-skitso-gia-tin-kuvernisi-sto-facebook/
80. www.alphafm.gr/archives/32464
81. https://www.secnews.gr/6607/hacking/
82. http://www.autoblog.gr/2015/04/19/tourkoi-hackers-epitethikan-sta-ellinika-sites-tis-dacia-kai-tis-renault/
83. http://news247.gr/eidiseis/koinonia/prosoxh-pornografiko-vinteo-poy-diakineitai-mesw-facebook-einai-ios.3286413.html
84. http://www.ethnos.gr/article.asp?catid=22768&subid=2&pubid=64189970