Τμήμα
Μηχανικών
Πληροφορικής τ.ε.
Τεχνολογικό Εκπαιδευτικό Ίδρυμα
Δυτικής Ελλάδας

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΨΗΦΙΑΚΕΣ ΑΠΕΙΛΕΣ ΚΑΤΑ ΤΩΝ ΑΝΗΛΙΚΩΝ ΚΑΙ ΤΡΟΠΟΙ ΑΝΤΙΜΕΤΩΠΙΣΗΣ

ΚΩΝΣΤΑΝΤΙΝΑ ΛΑΖΑΡΟΠΟΥΛΟΥ **Α.Μ. 1960**
ΤΣΑΓΚΡΙΝΟΣ ΣΤΥΛΙΑΝΟΣ **Α.Μ. 1282**

Επιβλέπων Καθηγητής : Ασημακόπουλος Γεώργιος

Αντίρριο Φεβρουάριος 2017

Περιεχόμενα

Ευχαριστίες

Αρχικά θα θέλαμε να ευχαριστήσουμε όλους τους καθηγητές μας για τις πολύτιμη συμβολή τους στην ολοκλήρωση των προπτυχιακών σπουδών μας που ολοκληρώνονται με την παρούσα εργασία. Πολλές ευχαριστίες οφείλουμε στους γονείς μας που χωρίς την αμέριστη υλική και ηθική τους υποστήριξη θα ήταν αδύνατον να καταφέρουμε τον στόχους μας. Επίσης θέλουμε να ευχαριστήσουμε τον καθηγητή μας κ. Γεώργιο Ασημακόπουλο για την καθοδήγηση και την επίβλεψη της παρούσας πτυχιακής εργασίας

ΕΙΣΑΓΩΓΗ

Η ραγδαία ανάπτυξη του διαδικτύου είχε ως αποτέλεσμα την εμφάνιση μιας νέας μορφής διαφήμισης και εμπορίου καθώς και την συνεχόμενη λειτουργία επιχειρήσεων σε αυτό όπως επίσης αναμένεται να αποτελέσει μια επικοινωνιακή πρακτική του μέλλοντος (*Τσουραμάνης, 2005*). Δυστυχώς όμως για πολλούς, η ύπαρξη του διαδικτύου, δεν επιφέρει μόνο θετικά αποτελέσματα στη ζωή των ανθρώπων, αλλά και κάποιες αρνητικές επιπτώσεις μέσω της ηλεκτρονικής εγκληματικότητας ή ψηφιακής εγκληματικότητας, η οποία υπάρχει και καθιστά τις συναλλαγές και επικοινωνίες ατόμων μέσω διαδικτύου επικίνδυνες όπου σε πολλές περιπτώσεις και για ορισμένους, αναφέρονται ως άκρως απαγορευτικές (*Ζάννη, 2006*). Το διαδίκτυο είναι πλέον κυρίαρχο. Η επιρροή και η δύναμή του διαδραματίζει πρωταγωνιστικό ρολό στην ζωή μας, αφού επεκτείνεται σε κάθε πτυχή της ιδιωτικής και επαγγελματικής μας δραστηριότητας. Συνήθως χρησιμοποιείται ως σημείο αναφοράς, ως μέσο για συζήτηση και όλο και περισσότερο ως βάση για τη διεύθυνση μιας επιχείρησης. Το ηλεκτρονικό εμπόριο είναι τόσο δυνατό και χρήσιμο ιδιαίτερα στον επιχειρηματικό κόσμο. Η ηλεκτρονική επιχείρηση είναι έτοιμη να απογειωθεί. Οι αριθμοί που παρουσιάζουν το μέλλον του ηλεκτρονικού εμπορίου, είναι εντυπωσιακοί. Δυστυχώς όμως μαζί με την ανάπτυξη του διαδικτύου και των επιχειρήσεων που λειτουργούν ηλεκτρονικά, υπάρχει και η ηλεκτρονική ή ψηφιακή εγκληματικότητα την οποία μπορεί να συναντήσει κανείς σε διάφορους τομείς λειτουργίας του διαδικτύου, όπως ηλεκτρονικές συναλλαγές πληροφοριών, ανταλλαγή συγκεκριμένων πληροφοριακών στοιχείων μεταξύ χρηστών, απαγορευμένες ανταλλαγές πληροφοριών σχετικά με παιδική πορνογραφία και διάφορα άλλα σημεία. Οι διορθωτικές κινήσεις βέβαια που διεξάγονται, έχουν ως σκοπό την εξάλειψη ή τουλάχιστον την ελαχιστοποίηση του βαθμού ηλεκτρονικής εγκληματικότητας στην εποχή μας (*Τσουραμάνης, 2005*). Μιλώντας κάποιος για ηλεκτρονικό έγκλημα και ψηφιακή εγκληματικότητα, εννοεί τις επιθετικές και αμυντικές επιχειρήσεις οι οποίες μπορούν να στρέφονται εναντίον των πηγών πληροφοριών και που χαρακτηρίζονται ως τύπου «νίκης-ήττας” (*Ζάννη, 2006*). Ένας από τους λόγους για τους οποίους διεξάγεται ο συγκεκριμένος πόλεμος, συμβαίνει λόγω του γεγονότος ότι οι πηγές αυτές των πληροφοριών παρουσιάζουν ιδιαίτερη σημασία για τους απλούς ανθρώπους και στελέχη των επιχειρήσεων στις μέρες μας.

Σε κάθε φαινόμενο ηλεκτρονικής ή ψηφιακής εγκληματικότητας εντοπίζονται τρία βασικά στοιχεία, όπου αυτά είναι οι πηγές των πληροφοριών, οι επιθετικές και αμυντικές επιχειρήσεις αλλά και ο ανθρώπινος παράγοντας ο οποίος εμπλέκεται σε αυτές τις επιχειρήσεις (*Καρανικόλα, 2005*). Είναι γεγονός πως η ηλεκτρονική ή ψηφιακή εγκληματικότητας σχετίζεται άμεσα με τις επιχειρήσεις και τους ιδιώτες εκείνους, οι οποίες αποσκοπούν στην πλήρη εκμετάλλευση των πηγών των πληροφοριών. Οι πηγές αυτές μπορούν να κατηγοριοποιηθούν σε πέντε βασικές κατηγορίες ως ακολούθως :

- *Φορείς πληροφοριών*
- *Μεταφορείς πληροφοριών*
- *Αισθητήρες πληροφοριών*
- *Καταγραφείς πληροφοριών*
- *Διεκπεραιωτές πληροφοριών*

Οι κατηγορίες αυτές που αναφέρονται παραπάνω δεν σημαίνει ότι ακολουθούν πάντα την συγκεκριμένη αυτή σειρά, καθώς κάθε μια από αυτές μπορεί να επιτελεί περισσότερες από μια λειτουργία. Επιχειρώντας να γίνει μια ανάλυση στις πέντε αυτές κατηγορίες πηγών, θα μπορούσαν να αναφερθούν τα εξής. Οι φορείς πληροφοριών είναι τα μέσα εκείνα τα οποία κατέχουν τις όποιες πληροφορίες. Κάθε αντικείμενο μπορεί να χαρακτηριστεί ως κάτοχος πληροφοριών. Στα αντικείμενα αυτά μπορούν να συμπεριλαμβάνονται η μνήμη των ανθρώπων, κάθε γραπτό μέσο, οι δίσκοι και οι χώροι αποθήκευσης των υπολογιστών, η μνήμη που διαθέτουν καθώς και όποια πληροφορία βρίσκεται αποθηκευμένη σε αυτούς (Denning, 2007). Οι μεταφορείς πληροφοριών χαρακτηρίζονται ως συστήματα και αντικείμενα επικοινωνιών, τα οποία έχουν την ικανότητα να διακινούν ή να διαβιβάζουν πληροφορίες από ένα συγκεκριμένο μέρος σε κάποιο άλλο. Στα συστήματα αυτά συμπεριλαμβάνονται τα άτομα τα οποία μεταφέρουν τις πληροφορίες, τα διάφορα οχήματα και γενικά τα μέσα μεταφοράς καθώς και τα διάφορα μέσα μαζικής επικοινωνίας (Τσουραμάνης, 2005). Σχετικά με τους αισθητήρες πληροφοριών, θα μπορούσε να ειπωθεί πως αυτές είναι συσκευές οι οποίες συλλέγουν πληροφορίες από άλλα αντικείμενα, αλλά και από το περιβάλλον στο οποίο βρίσκονται. Στην κατηγορία αυτή ανήκουν οι ανθρώπινες αισθήσεις, τα scanners, τα ραντάρ και οι φωτογραφικές μηχανές. Τέλος, ως καταγραφείς των πληροφοριών χαρακτηρίζονται οι

συσκευές εκείνες οι οποίες τοποθετούν κάποιες πληροφορίες στους φορείς. Σε αυτές συγκαταλέγονται οι ανθρώπινες ενέργειες, οι οδηγοί δισκετών καθώς και οι εκτυπωτές. Οι διεκπεραιωτές πληροφοριών είναι τα αντικείμενα εκείνα που χειρίζονται τις πληροφορίες και εσωκλείουν το υλικό μέρος των υπολογιστών, τους μικροεπεξεργαστές αλλά και τα διάφορα προγράμματα (Τσουραμάνης, 2005). Ο όρος Ηλεκτρονικό έγκλημα ή Ηλεκτρονική εγκληματικότητα αποτελεί μια ευρεία έννοια στην οποία εμπίπτουν όλες εκείνες οι αξιόποινες πράξεις που τελούνται με τη χρήση ενός συστήματος ηλεκτρονικής επεξεργασίας δεδομένων. Ο όρος αυτός διακρίνεται σε στενή και σε ευρεία έννοια. Η εν στενή έννοια ηλεκτρονική εγκληματικότητα αναφέρεται στις αξιόποινες πράξεις όπως είναι η ηλεκτρονική απάτη, η χωρίς άδεια απόκτηση δεδομένων, η παραποίηση δεδομένων και η δολιοφθορά δηλαδή εγκλήματα όπου ο ηλεκτρονικός υπολογιστής αποτελεί κύριο μέσο τέλεσης των εγκλημάτων. Αντίθετα η εν ευρεία έννοια εγκληματικότητα μέσω Η/Υ περιλαμβάνει όλα εκείνα τα αδικήματα για την τέλεση των οποίων ο ηλεκτρονικός υπολογιστής χρησιμοποιείται ως βοηθητικό μέσο (*Καρανικόλα, 2005*). Ωστόσο η δίωξη του ηλεκτρονικού ή ψηφιακού εγκλήματος είναι περισσότερο δύσκολη από τη δίωξη του κοινού εγκλήματος. Τα αποδεικτικά στοιχεία και οι παντός είδους καταγραφές που δημιουργούνται σε υπολογιστικά συστήματα, υπάρχουν για τις συνήθεις ανάγκες λειτουργίας ενός δικτύου. Είναι φτιαγμένα από τεχνικούς για τεχνικούς, και συχνά δεν είναι ικανά να καλύψουν ανάγκες όπως η νομική τεκμηρίωση. Υπάρχει σοβαρή δυσκολία σύνδεσης μιας παράνομης πράξης με τον υπολογιστή από τον οποίο ξεκίνησε η παράνομη αυτή πράξη. Ακόμη μεγαλύτερη δυσκολία όμως υπάρχει στη σύνδεση της παράνομης πράξης, του υπολογιστή και του ανθρώπου που ενήργησε μέσα από αυτόν και πρέπει να έχει την ευθύνη (Denning, 2007). Η πληροφορική τεχνολογία κατέστησε δυνατή τη διάπραξη ενός ευρέως φάσματος εγκληματικών πράξεων, οι οποίες απαιτούν εξειδίκευση και αυξημένη κατάρτιση.

ΚΕΦΑΛΑΙΟ 1ο : ΨΗΦΙΑΚΗ ΕΓΚΛΗΜΑΤΙΚΟΤΗΤΑ

Ως «Ηλεκτρονικό ή Ψηφιακό Έγκλημα», θεωρούνται οι αξιόποινες εγκληματικές πράξεις που τελούνται με τη χρήση ηλεκτρονικών υπολογιστών και συστημάτων επεξεργασίας δεδομένων και τιμωρούνται με συγκεκριμένες ποινές από την ελληνική νομοθεσία. Ανάλογα με τον τρόπο τέλεσης διαχωρίζονται σε εγκλήματα τελούμενα με τη χρήση Ηλεκτρονικών Υπολογιστών (computer crime) και σε Κυβερνοεγκλήματα (cyber crime), εάν τελέσθηκε μέσω του Διαδικτύου (Ζάννη, *2006*).

1.1 Διακρίσεις Ψηφιακής Εγκληματικότητας

Τα ψηφιακά εγκλήματα, θα μπορούσαν να διαχωριστούν σε δύο μεγάλες κατηγορίες με κριτήριο τα μέσα τέλεσης και εξιχνίασης τους. Έτσι αναφέρονται,

- Τα γνήσια ψηφιακά εγκλήματα τα οποία τελούνται αλλά και εξιχνιάζονται, αποκλειστικά και μόνο με τη χρήση της ψηφιακής τεχνολογίας και
- Τα παραδοσιακά εγκλήματα τα οποία τελούνται αλλά και εξιχνιάζονται, τόσο με την υποστήριξη της ψηφιακής τεχνολογίας όσο και χωρίς τη βοήθειά της.

Με βάση τη διάκριση αυτή στην πρώτη από τις παραπάνω κατηγορίες, θεωρούνται ότι μπορεί να υπαχθούν (Τσουραμάνης, 2005):

- Η χωρίς νόμιμη εξουσιοδότηση είσοδος σε Η/Υ (hacking)
- Η κλοπή, η παραποίηση και η καταστροφή αρχείων Η/Υ
- Η προσωρινή ή οριστική διακοπή της λειτουργίας συστήματος Η/Υ που αποτελεί συνέπεια της λεγόμενης "επίθεσης άρνησης παροχής υπηρεσιών" (Denial of service attack – DoS)
- Η διασπορά κακόβουλων προγραμμάτων (όπως, ιών (virus), σκουληκιών (worms), Δούρειων Ιππων (Trojan Horses – Trojans), dialers κλπ.) και
- Η πειρατεία λογισμικού δηλ.προγραμμάτων Η/Υ που αφορά την παράνομη αντιγραφή τους και τη στη συνέχεια διάθεσή τους στην αγορά – και μέσω του Διαδικτύου - σε πολύ χαμηλότερη τιμή από εκείνη του πρωτοτύπου.

Στη δεύτερη κατηγορία των παραδοσιακών εγκλημάτων που τελούνται και με τη χρήση της ψηφιακής τεχνολογίας, μπορούν να υπαχθούν (Καρακώστας, 2003):

- Διάφορα κοινά εγκλήματα. Σαν τέτοια μπορούν να αναφερθούν π.χ. η κλοπή ενός Η/Υ ή τμημάτων του – μνήμης, μητρικής κλπ.- ή περιφερειακών του – εκτυπωτών, σκάνερς κλπ.- Στην κατηγορία αυτή ανήκουν επίσης και εγκλήματα που τελούνται με τη βοήθεια του ηλεκτρονικού ταχυδρομείου (e–mail) ή ιστοσελίδων (websites), όπως απάτες (π.χ. Νιγηριανή απάτη, "ψάρεμα ΄/phishing mail), εξυβρίσεις, εκβιασμοί, δυσφημίσεις, πωλήσεις απαγορευμένων προϊόντων (ναρκωτικών, μη εγκεκριμένων φαρμάκων), παροχή υπηρεσιών call-girls, η κυκλοφορία πορνογραφικού υλικού – που αφορά κυρίως ανηλίκους (παιδική πορνογραφία) – καθώς και η παρενόχληση χρηστών με ανεπιθύμητα διαφημιστικά μηνύματα (spamming). Εδώ υπάγονται επίσης και οι προσβολές της πνευματικής ιδιοκτησίας, οι ανταλλαγές πληροφοριών μέσω του ηλεκτρονικού ταχυδρομείου μεταξύ τρομοκρατικών οργανώσεων αλλά και συμμοριών του οργανωμένου εγκλήματος καθώς και το ηλεκτρονικό ξέπλυμα βρώμικου χρήματος.
- Η κατασκοπεία είτε αυτή χαρακτηρίζεται σαν βιομηχανική ή σαν κρατική ή σαν πολιτική και
- Οι υποκλοπές τηλεφωνικών συνομιλιών που έχουν σαν συνέπεια την προσβολή του προσωπικού απορρήτου των συνομιλούντων.

1.2 Είδη Ψηφιακής Εγκληματικότητας

Σύμφωνα με τα αποτελέσματα έρευνας που διεξήγαγε η επιχείρηση της McConnell International σε 52 χώρες με τίτλο «*Cyber Crime and Punishment*» το 2010, κατατάσσει τα αδικήματα που διαπράττονται στον Κυβερνοχώρο στις παρακάτω δέκα (10) κατηγορίες (*Ζάννη, 2006*) **:**

- Παρεμπόδιση (κυβερνο)κυκλοφορίας
- Τροποποίηση και Κλοπή δεδομένων,

- Εισβολή και Σαμποτάζ σε δίκτυο,
- Μη εξουσιοδοτημένη πρόσβαση,
- Διασπορά ιών,
- Υπόθαλψη αδικημάτων,
- Πλαστογραφία και Απάτη.

Κύριες μορφές Κυβερνοεγκλημάτων που εξιχνιάσθηκαν στην Ελλάδα από το Τμήμα Ηλεκτρονικού Εγκλήματος/ΔΑΑ, αφορούν τα παρακάτω :

- Απάτες μέσω Διαδικτύου
- Παιδική πορνογραφία
- Cracking και hacking
- Διακίνηση-πειρατεία λογισμικού
- Πιστωτικές κάρτες
- Διακίνηση ναρκωτικών
- Έγκλημα στα chat rooms
- Οικονομικά Εγκλήματα (Απάτες μέσω Διαδικτύου κ.λπ.)
- Εγκλήματα που παραβιάζουν τη νομοθεσία περί πνευματικής ιδιοκτησίας
- Διακίνηση ναρκωτικών ουσιών & φαρμακευτικών σκευασμάτων, μέσω Διαδικτύου
- Κλοπή Διαδικτυακής Ταυτότητας

Ένα πληροφοριακό σύστημα ενός οικονομικού οργανισμού ή και ενός απλού χρήστη δέχεται απειλές από :

- **Hackers – Crackers** : Αποτελούν τους «αναρχικούς» του κυβερνοχώρου με τη εισβολή τους στα πληροφοριακά συστήματα. Οι λόγοι τους, μπορεί να είναι για διασκέδαση, η να καταστρέψουν ή να επιδείξουν δύναμη καταστροφής. Οι απαγορευμένοι χώροι τους ελκύουν σχετικά. Δεν είναι λίγες οι επιχειρήσεις οι οποίες προσλαμβάνουν άτομα που είχαν εισβάλλει σε συστήματά τους με τη δικαιολογία ότι είναι καλύτερα να εργάζονται γι' αυτές και όχι εναντίον τους. Αντίστοιχα, όσοι έχουν παραβιάσει ένα σύστημα ασφαλείας γνωρίζουν πολύ καλά τα μειονεκτήματά του και μπορούν να εργαστούν να το κάνουν ασφαλέστερο (Cavoukian, Tapscott, 1997).

- **Κλέφτες** : Είναι τα άτομα που εισβάλλουν σε ένα σύστημα με στόχο να κλέψουν δεδομένα, έχοντας οικονομικά οφέλη από τη πώληση ή τη χρήση τους σε άλλους ή σε επιχειρήσεις.
- **Ανταγωνιστές** : Τις περισσότερες φορές ένας ανταγωνιστής δεν αποβλέπει σε κλοπή χρημάτων ή καταστροφής. Στόχος του είναι η απόκτηση πληροφοριών με σκοπό να έχει πλεονεκτήματα στο χώρο των επιχειρήσεων.
- **Εσωτερικοί εχθροί** : Μπορεί να είναι ορισμένοι υπάλληλοι δυσαρεστημένοι και οι οποίοι αποτελούν σημαντικό κίνδυνο για τη βάση δεδομένων της εταιρείας.
- **Ατυχήματα** : Οι όποιες καταστροφές μπορεί να συμβούν στα συστήματα των επιχειρήσεων, δεν είναι όλες αποτέλεσμα κάποιας πρόθεσης ή οργανωμένης επίθεσης. Σε ορισμένοι περιπτώσεις είναι ατυχήματα ή λάθη από αμέλειες. Πολλές φορές δε, ορισμένες εταιρείες μόνες τους καταστρέφουν τη βάση δεδομένων ή κατά λάθος τις απελευθερώνουν στο διαδίκτυο (Cavoukian, Tapscott, 1997).

1.2.1 Τύποι Ψηφιακών απειλών

Από τις πλέον διάσημες και αποτελεσματικές μεθόδους των crackers για τη διακοπή λειτουργίας δικτυωμένων υπολογιστών ενός συστήματος ασφαλείας οικονομικών συναλλαγών, είναι οι Dos επιθέσεις (Denning, 2007). Η ονομασία αυτή εξηγεί και γιατί ο υπολογιστής - θύμα δεν μπορεί να εξυπηρετήσει αιτήσεις πελατών λόγω κάποιων κίβδηλων αιτήσεων. Τα είδη αυτής της επίθεσης είναι πολλά αφού υπάρχει εκμετάλλευση και αδυναμίες ζεύγους πρωτοκόλλων TCP/IP. Είναι τα ήδη γνωστά τα μέτρα προστασίας. Οι διαχειριστές συστημάτων είναι σε θέση να εγκαταστήσουν patches στα λειτουργικά συστήματα και σε προγράμματα διακομιστές για τις εν λόγω επιθέσεις. Δεν είναι τυχαίο ότι κατά καιρούς ανακαλύπτονται και διαφορετικές παραλλαγές τέτοιων επιθέσεων (Rosenoer, 1997). Ουσιαστικά τέσσερις εν συντομία γνωστές παραλλαγές, αναφέρονται ως ακολούθως (Taylor, 1999) :

- **Ping of death** : Αίτηση PING ή, αλλιώς, αίτηση ICMP, προς τον υπολογιστή-στόχο, με άκυρο μέγεθος πακέτου στην κεφαλή (header) του τελευταίου (πάνω από 64Kb). Τέτοια «παράτυπα» πακέτα μπορούν να «κρεμάσουν» υπολογιστές που τρέχουν λειτουργικά συστήματα ανίκανα να τα μεταχειριστούν.
- **Smurf Attack** : Μέσω αιτήσεων ICMP σε κάποια διεύθυνση εκπομπής στο δίκτυο που βρίσκεται υπό επίθεση. Πλαστογραφείται η διεύθυνση επιστροφής των πακέτων για να μην είναι ίδια με εκείνη του υπολογιστή στόχου. Έτσι όλα τα μηχανήματα ενός υποδικτύου αντιστοιχεί μια διεύθυνση εκπομπής λειτουργεί ενίσχυση λόγω μιας μόνο αίτησης ICMP και με αυτό τον τρόπο προκαλεί πληροφοριακό μποτιλιάρισμα (Meinel, 1998). Πρέπει ν' αναφερθεί ότι μια διεύθυνση εκπομπής αντιστοιχεί σε 255 καταστήματα και σε μια μόνο τέτοια επίθεση μπορεί να παραχθούν 255 αιτήσεις. Είναι επομένως κατανοητός ο υπέρογκος αριθμός των πακέτων που είναι άχρηστα αφού λόγω επίθεσης στέλνονται ακόμα και χιλιάδες πακέτα
- **Sun flood attack** : Πριν την εγκαθίδρυση μιας συνεδρίας σ' ένα πελάτη και σε ένα διακομιστή, ακολουθούν τρία βήματα της γνωστής ακολουθίας χειραψίας. Σε περίπτωση που ο πελάτης αγνοήσει την τελευταία απάντηση SYN-ACK (SYNchronize ACKnowledge) του διακομιστή, ο τελευταίος θα επιμένει για ένα προκαθορισμένο χρονικό διάστημα (Taylor, 1999). Ένας cracker μπορεί να «εκμεταλλευθεί» τη συγκεκριμένη συμπεριφορά για να υπερφορτώσει το διακομιστή-θύμα ή ακόμα και για να τον «κρεμάσει». Κατά τη διάρκεια μιας τέτοιας επίθεσης, ο θύτης παραποιεί τη δικτυακή του διεύθυνση (IP address), κρύβοντας με τον τρόπο αυτό τα ίχνη του (Denning, 2007).
- **Tear Drop Attack** : Από τη «εκμετάλλευση» των αδυναμιών από τον επιτεθέμενο σε ότι αφορά τη ανασυγκρότηση πακέτων IP, προκαλείται αυτή η επίθεση. Από τη στιγμή που το πακέτο αποστέλλεται μέσω διαδικτύου, μπορεί να ταξιδέψει σε κάποια μικρότερα τμήματα. Υπάρχει ένα πεδίο στη κορυφή κάθε τμήματος όπου δίνεται η θέση του στο αρχικό πακέτο IP (Cavoukian, Tapscott, 1997). Το πρόγραμμα που χρησιμοποιείται είναι το Teardrop όπου «σπάει» τα πακέτα σε κάποια τμήματα με λάθος πληροφορίες στο υπό συζήτηση πεδίο. Έτσι όταν γίνει η προσπάθεια συναρμολόγησης από το

υπολογιστή στόχο θα επανεκκινήσει τα τμήματα αυτά εκτός αν ο διαχειριστής συστήματος έχει αναβαθμίσει το λειτουργικό με patch. Σε μια τέτοια επίθεση συμμετέχουν πολλά συστήματα με τις κατανεμημένες θέσεις Dos. Είναι δυνατό σε τέτοιου είδους επιθέσεις να συμμετέχουν και προσωπικοί υπολογιστές ή και το PC του σπιτιού (Rosenoer, 1997).

- **Απρόσκλητοι επισκέπτες** : Αποτελεί από τις πλέον παλαιές μεθόδους που χρησιμοποιούνται προκειμένου να αναλυθεί η συμπεριφορά δικτύων και να εντοπισθούν προβλήματα. Είναι το πρόγραμμα εκείνο που μπορεί να υποκλέψει δεδομένα σε ένα δίκτυο. Εάν το δίκτυο είναι βασισμένο στο TCP/IP, τότε επειδή το sniffer παρακολουθεί πακέτα IP, ονομάζεται και packet sniffer. Εξάλλου, σε ένα δίκτυο τοπολογίας αστέρα, όπως είναι πολλά τοπικά δίκτυα, τα πακέτα που φεύγουν από έναν κόμβο (μηχάνημα) εκπέμπονται προς όλους τους άλλους κόμβους του δικτύου (Rosenoer, 1997). Μόνο όμως ο κόμβος που προορίζονται τα πακέτα θα χρησιμοποιήσει και όχι οι υπόλοιποι. Αν κάποιο sniffer έχει εγκατασταθεί σε υπολογιστή με κάρτα δικτύου σε κατάσταση επιδιδόμενη το μηχάνημα μπορεί να δει όλα τα πακέτα τα οποία διακινούνται.
- **Αδιάκριτοι διαβάτες** : Η σάρωση θυρών είναι ακόμα μια άλλη τεχνική που χρησιμοποιείται. Δεν είναι παρά η αποστολή ερωτημάτων σε διακομιστές ώστε να παρθούν πληροφορίες για τις προσφερόμενες υπηρεσίες και το επίπεδο ασφαλείας. Αν ο εισβολέας πάρει κάποιες πληροφορίες του μηχανήματος στόχου, είναι σε θέση να σχεδιάσει τη επίθεσή του ξέροντας κάποιες αδυναμίες. Μια διακασία port scanning αφήνει ίχνη σε αρχεία καταστροφής και κάποιοι χρησιμοποιούν τακτικές παραλλαγής. Μια από αυτές είναι η ημι ανοικτή σάρωση SYN (Meinel, 1998). Σε αυτή τη σάρωση το πρόγραμμα συνδέεται στα port και η κάθε μια από αυτές τερματίζει τη σύνδεση πριν ολοκληρωθεί. Από τη στιγμή, λοιπόν, που οι ακολουθίες σύνδεσης δεν ολοκληρώνονται, το λειτουργικό σύστημα στο μηχάνημα-στόχος συνήθως δεν τις καταγράφει, θεωρώντας ότι δεν συνέβησαν ποτέ (Taylor, 1999). Ωστόσο, το πρόγραμμα που κάνει τη σάρωση μπορεί να καταλάβει εάν κάποιο port είναι «ανοιχτό», κρίνοντας από την απάντηση του λειτουργικού συστήματος. Υπάρχουν διάφορα εργαλεία για το μπλοκάρισμα

των port scan. Αυτό που προτείνεται στους απλούς χρήστες είναι η χρήση κάποιου προσωπικού προγράμματος firewall (Meinel, 1998).

- **Social Engineering** : Είναι πραγματικότητα πως μια επίθεση βασίζεται σε ψυχολογία. Είναι η τέχνη της απόκτησης πρόσβασης σε ένα σύστημα με εξαπάτηση των χρηστών και των διαχειριστών έχοντας τις απαραίτητες πληροφορίες. Σε ένα πείραμα που έγινε σε crackers, αυτοί ξεκίνησαν τη προσπάθειά τους να εισχωρήσουν σε ένα πληροφοριακό σύστημα μια εταιρείας. Σαν όπλο τους είχαν το τηλεφωνικό κατάλογο της εταιρείας και θέλησαν να μιλήσουν με τη γραμματέα του δικτύου. Σε 24 ώρες κατάφεραν να κάνουν τη εταιρεία να εργάζεται για εκείνους και να τους στείλει courier βράδυ το software για τη είσοδό τους (Denning, 2007).
- **Δούρειοι ίπποι** : Αποτελεί το μεγαλύτερο κίνδυνο σε πολλούς χρήστες. Είναι ένα πρόγραμμα από δυο μέρη. Ο διακομιστής φωλιάζει στον υπολογιστή κι ο πελάτης είναι στο μηχάνημα του θύτη. Αν ο χρήστης του υπολογιστή που είναι σε επίθεση συνδεθεί με το διαδίκτυο το Trojan διακομιστής στέλνει σήμα που λαμβάνεται από το Trojan πελάτη. Έτσι τοποθετείται μια συνεδρία μεταξύ τους και επιτυγχάνεται μια πρόσβαση από το cracker στο υπολογιστή. Ανάλογα με τον ιό ποικίλει και ο μακρόθεν έλεγχος του επιτεθέμενου στο άλλο μηχάνημα. Απλά αυτό που γίνεται είναι ο πρώτος να παίζει με τα νεύρα του χρήστη με το να του εμφανίζει γαργαλιστικά μηνύματα στη οθόνη του ή κι να το δημιουργήσει ζημιές στο υλικό του υπολογιστή του (Cavoukian, Tapscott, 1997). Οι Δούρειοι ίπποι έχουν ακόμα μια άλλη ύπουλη λειτουργία αυτή της παρακολούθησης κι καταγραφής πλήκτρων. Ο ιός παρακολουθεί συνεχώς τις κινήσεις του χρήστη και όταν εκείνος πληκτρολογεί το κωδικό πρόσβασής του ή κάποιους αριθμούς πιστωτικών καρτών το πρόγραμμα τις καταγράφει και τις στέλνει στο θύτη. Ο πιο συνηθισμένος τρόπος είναι να σταλεί σε κάποιο email ή να βρίσκεται σε κάποιο παιχνίδι ή freeware ή shareware. Δυο είναι οι τρόποι αποφυγής του. Αρχικά πρέπει να χρησιμοποιείται το Antivirus ή το AntiTrojαν.
- **Κουνέλια** : Τα προγράμματα αυτά έχουν την ιδιότητα όταν ξεκινήσουν να δημιουργούν αντίγραφα του εαυτού τους. Έτσι γεμίζουν τη μνήμη Ram και προκαλούν «κατάρρευση» στον υπολογιστή. Δεν προσκολλούν τους εαυτούς

τους σε υπάρχοντα αρχεία και μπορούν να καλυφθούν με το να υιοθετήσουν κάποιο όνομα ή με τη ενεργοποίηση ιδιότητας λίστας κρυφών αρχείων.

- **Σκουλήκια** : Είναι ίδια με τα «κουνέλια» απλά μπορούν να μεταδίδουν από κάποιο μηχάνημα σε ένα άλλο έπειτα από εκμετάλλευση κάποια κενά σε πρωτόκολλα διαδικτύου. Χρησιμοποιούν υπηρεσίες δικτύου όπως το ηλεκτρονικό ταχυδρομείο και πολλαπλασιάζονται. Δεν μολύνουν αρχεία του υπολογιστή. Γνωστές είναι οι περιπτώσεις Melissa και love letter είναι γνωστές όπου και εξαπλώθηκαν άμεσα στο διαδίκτυο. Μάλιστα η πρώτη έκανε ένα νέο γύρο καλυμμένο ως έγγραφο Office για Mac. Αποτελεί μια ύπουλη επίθεση από τη στιγμή που καταφέρουν να εισχωρήσουν στον υπολογιστή δίνουν καμουφλαρισμένα μηνύματα στη λίστα outlook. Ο χρήστης λοιπόν λαμβάνει τα μηνύματα από κάποιο γνωστό του και ανοίγει να το διαβάσει. Πέρα όμως από τη καταπάτηση μικρού εύρους ζώνης του modem μπορεί να δημιουργήσει πρόβλημα κι σε κεντρικούς διακομιστές αλληλογραφίας. Τα μέτρα προστασίας δεν είναι επαρκή και πάντα τα όποια προγράμματα χρησιμοποιούνται θα είναι ατελή. Είναι τα λεγόμενα exploits αδυναμίες προγραμμάτων και εφαρμογές που χρησιμοποιούνται που είναι σε θέση να αξιοποιούν με το σωστό τρόπο τη πρόσβαση μη εξουσιοδοτημένη, να προκαλούν ζημιές (Rosenoer, 1997).

Ωστόσο τα τελευταία χρόνια, παρατηρείται μια βασική στροφή και χρήση υπηρεσιών υπολογιστικού νέφους (cloud computing) και ανάπτυξη νέων μορφών εγκληματικότητας. Ο ορός "Cloud Computing" ως μία από τις τεχνολογίες αιχμής στο τομέα της παροχής υπολογιστικών υπηρεσιών. Με πολύ απλά λόγια το "cloud computing" είναι μία δομή, με την οποία μας δίνεται η δυνατότητα να έχουμε πρόσβαση και να χρησιμοποιούμε web εφαρμογές, χωρίς να τις διαθέτουμε στον υπολογιστή μας ή σε κάποια άλλη συσκευή που είναι διασυνδεδεμένη με το Διαδίκτυο. Σε αυτή τη δομή η εφαρμογή βρίσκεται σε ένα server και εμείς τη χρησιμοποιούμε χωρίς να χρειάζεται να την εγκαταστήσουμε στον υπολογιστή μας (Διεθνές και Ευρωπαϊκό νομικό καθεστώς αντιμετώπισης της παιδικής πορνογραφίας, 2008).

Τα τελευταία χρόνια τα στατιστικά στοιχεία δείχνουν μια ταχεία αύξηση της χρήσης των υπηρεσιών cloud. Για να είμαστε πιο ακριβείς άνθρωποι στρέφονται προς τις

υπηρεσίες cloud, όπως το Dropbox, το Evernote και το Box για την αποθήκευση των ψηφιακών δεδομένων τους. Από την άλλη πλευρά, οι στατιστικές δείχνουν ότι όλο και περισσότερες μεγάλες εταιρείες εκμεταλλεύονται τα οφέλη του cloud computing. Η αποθήκευση στο υπολογιστικό νέφος (cloud storage ή αλλιώς filehosting), είναι η αποθήκευση των ηλεκτρονικών δεδομένων σε απομακρυσμένες υποδομές και όχι σε τοπικά αποθηκευτικά μέσα τα οποία είναι συνδεδεμένα στον υπολογιστή (Denning, 2007). Υπάρχει ένας μεγάλος αριθμός παρόχων υπηρεσιών Cloud Storage, πολλοί από τους οποίους προσφέρουν δωρεάν υπηρεσίες αποθήκευσης: όπως το Dropbox, το SpiderOak, το Box κ.α.. Η πρόσβαση στις διάφορες αυτές υπηρεσίες μπορεί να πραγματοποιηθεί με διάφορους τρόπους, ο χρήστης μπορεί να εγκαταστήσει το λογισμικό της εφαρμογής σε έναν υπολογιστή ή να χρησιμοποιήσει ένα πρόγραμμα περιήγησης (browser). Το υπολογιστικό νέφος (Cloud Storage) μπορεί να χρησιμοποιηθεί από εγκληματίες για την αποθήκευση παράνομων δεδομένων και την παροχή ενός σημείου διανομής που να μην συνδέει τον ιδιοκτήτη ή τους χρήστες με τα παράνομα δεδομένα. Παρέχει, δηλαδή, μια δυσκολία στην απόδοση κυριότητας ή της συσχέτισης με παράνομα στοιχεία (Τσουραμάνης, 2005). Τα δεδομένα που είναι αποθηκευμένα στο Cloud μπορεί επίσης να γίνουν στόχος από εγκληματίες του κυβερνοχώρου, οι οποίοι ενδέχεται να είναι σε θέση να αποκτήσουν πρόσβαση στο λογαριασμό του θύματος και στα δεδομένα που περιέχονται σε αυτόν. Τέλος μπορούν να αποκτήσουν τον έλεγχο του λογαριασμό για να χρησιμοποιήσουν τους πόρους του για εγκληματικούς σκοπούς, όπως η διανομή παράνομων δεδομένων. Έτσι αυξάνεται η πρόκληση της διερεύνησης κυβερνο-εγκλημάτων (cybercrimes) ή των παραδοσιακών εγκλημάτων που διενεργούνται στο περιβάλλον του κυβερνοχώρου. Οι υπηρεσίες και αρχές επιβολής του νόμου και οι ερευνητές έχουν ανάγκη να έχουν πρόσβαση στα δεδομένα που αποθηκεύονται στους λογαριασμούς του Cloud Storage. Οι δυσκολίες προκύπτουν από την προσπάθεια εφαρμογής των παραδοσιακών εγκληματολογικών μεθόδων έρευνας σε ένα περιβάλλον cloud. Σε μια παραδοσιακή έρευνα ενός υπολογιστή, το φυσικό υλικό κατάσχεται, δημιουργείται ένα πιστό αντίγραφο, και η ανάλυση γίνεται στο αντίγραφο. Σε ένα περιβάλλον Cloud Storage, το υλικό φιλοξενείται σε ένα μεγάλο κέντρο δεδομένων (Data Center), το οποίο μπορεί να βρίσκεται σε άλλη χώρα και τα δεδομένα μπορούν να βρίσκονται κατανεμημένα σε πολλά τέτοια κέντρα δεδομένων σε όλο τον κόσμο. Ως εκ τούτου, η φυσική ανάλυση αποτελεί το λιγότερο μια πρόκληση (Ζάννη, 2006). Η ηλεκτρονική υποκλοπή στοιχείων από υπηρεσίες υπολογιστικού νέφους γίνεται όλο και πιο

ενδιαφέρουσα για τους εγκληματίες. Όπως προαναφέραμε, το Cloud Storage χρησιμοποιείται από εγκληματίες, και αποτελεί στόχο των κυβερνό-εγκληματιών. Αναμένεται λοιπόν ότι οι εγκληματίες θα στοχεύουν όλο και περισσότερο στην υποκλοπή τέτοιων υπηρεσιών με σκοπό την κατασκοπεία, την κλοπή προσωπικών στοιχείων και δεδομένων, την εκβίαση κ.λπ. Επιπλέον η δυσχέρεια απόδειξης και συλλογής αποδεικτικού υλικού από τους παρόχους υπηρεσιών υπολογιστικού νέφους, αποτελεί ένα υπαρκτό και δυσεπίλυτο προς το παρόν πρόβλημα για τις αρχές επιβολής του νόμου.

1.3 Αριθμητικά Στοιχεία Αναφορικά με την Ψηφιακή Εγκληματικότητα σε Ελλάδα και Διεθνώς

Το φαινόμενο της ψηφιακής εγκληματικότητας και ιδιαίτερα της παιδικής πορνογραφίας έχει λάβει πλέον ανεξέλεγκτες διαστάσεις στις μέρες μας, τόσο σε διεθνές όσο και σε τοπικό επίπεδο. Η UNESCO το 2012, πραγματοποίησε μια έρευνα μέσω της οποίας ήρθαν στην επιφάνεια τα ακόλουθα αποτελέσματα (UNESCO, 2012) :

- Ο τζίρος της βιομηχανίας της παιδικής πορνογραφίας στο διαδίκτυο ξεπερνά κάθε χρόνο τα 3-4 δισεκατομμύρια ευρώ κάθε χρόνο
- Ορισμένες ιστοσελίδες παιδικής πορνογραφίας και οι οποίες φιλοξενούν τέτοιο υλικό με πρωταγωνιστές μικρά παιδιά και σε ορισμένες περιπτώσεις και μωρά, υπολογίζεται ότι έχουν σημειώσει μια αύξηση της τάξεως του 350%
- Η έκταση της παιδικής πορνογραφίας αν και είναι δύσκολο να εκτιμηθεί, αναφέρει πως περισσότερο από ένα εκατομμύριο πορνογραφικές εικόνες ανηλίκων διακινούνται στο διαδίκτυο και 200 νέες εικόνες ταχυδρομούνται ηλεκτρονικά σε ημερήσια βάση
- Ορισμένες από τις σελίδες παιδικής πορνογραφίας, τυγχάνουν ημερήσιας επισκεψιμότητας περίπου 155.000 ατόμων, παρά το υψηλό κόστος που διαθέτουν

Σχετικά με την Ελλάδα, έχει υπολογιστεί βάσει της έρευνας του Τμήματος Δίωξης Ηλεκτρονικού Εγκλήματος της Ασφάλειας Αττικής (2014), πως από τις αρχές του έτους 2014 έως τον Οκτώβριο του 2015 αναφέρθηκαν 48 υποθέσεις διακίνησης υλικού παιδικής πορνογραφίας στις οποίες συνελήφθησαν 68 άτομα και κατηγορήθηκαν συνολικά 90 άλλοι. Σύμφωνα με τον διευθυντή του συγκεκριμένου τμήματος, η μορφή εγκλήματος της παιδικής πορνογραφίας συνεχώς αναπτύσσεται και εξελίσσεται αρνητικά για την κοινωνία μας καθώς παρουσιάζονται νέες υποθέσεις με ιστοσελίδες που φιλοξενούν παιδιά σε άσεμνες στάσεις. Παλαιότερα η συχνότητα εξιχνίασης τέτοιων υποθέσεων ήταν περίπου μια με δύο το χρόνο ενώ στις μέρες μας ξεπερνούν τις δέκα και ίσως δεκαπέντε ανά έτος (Δίωξη Ηλεκτρονικού Εγκλήματος της Ασφάλειας Αττικής (2014). Σύμφωνα με τις ίδιες αποκαλύψεις, ο ρυθμός αύξησης των εγκλημάτων αυτών από το 2011 και έπειτα κυμαίνεται με ρυθμούς αύξησης ανά 150% σε ετήσια βάση. Σημαντικό ρόλο σε όλη αυτήν την υπόθεση «*παίζει*» και το γεγονός πως η παιδική πορνογραφία έχει εξελιχθεί σε μια ιδανική «*επιχειρηματική*» ενέργεια από μέρους των επιτήδειων και οι οποίοι κάθε φορά διακυβεύουν πολλά εκατομμύρια μέσω των ειδικά διαμορφωμένων κυκλωμάτων και τους συνδέσμους ανθρώπων που χρησιμοποιούν (Δίωξης Ηλεκτρονικού Εγκλήματος της Ασφάλειας Αττικής (2014).

1.4 Deep Web

Αν και δεν είναι αποκλειστικά χτισμένο για εγκληματικούς σκοπούς το "Βαθύ Δίκτυο" (Deep Web) ή "Σκοτεινό Δίκτυο" (Dark Web) ή "Αόρατο Δίκτυο" (Invisible Web) , αποτελεί εκ της φύσεώς του πεδίο άνθισης παράνομης και εγκληματικής δραστηριότητας. Το Deep Web αναφέρεται στο περιεχόμενο του ίντερνετ που δεν ανήκει στο Επιφανειακό Web (Surface Web), το οποίο δεικτοδοτείται από μία μηχανή αναζήτησης, όπως η Google. (Mitrou, 2008). Οι μηχανές αναζήτησης εμφανίζουν αποτελέσματα χρησιμοποιώντας κάποιους αλγόριθμους που βάζουν σε λίστες της ιστοσελίδες και λέγονται crawlers ή αράχνες. Οι Web crawlers όμως δεν βρίσκουν τα πάντα. Υπάρχουν κρυφοί πόροι στο διαδίκτυο που σε γενικές γραμμές, κατατάσσονται στις παρακάτω κατηγορίες (Denning, 2007.)

- Δυναμικό περιεχόμενο: δυναμικές σελίδες στις οποίες έχει κάποιος πρόσβαση μόνο μέσα από φόρμες στις οποίες συμπληρώνει στοιχεία. Στην ίδια κατηγορία ανήκουν και οι σελίδες που δημιουργούνται με session ids και δεν έχουν σταθερό url.
- Μη συνδεδεμένο περιεχόμενο: σελίδες που δεν συνδέονται με άλλες σελίδες. Έτσι, οι αράχνες ή web crawlers που χρησιμοποιούν οι μηχανές αναζήτησης, δεν μπορούν να τις «βρουν» από άλλες σελίδες που εξετάζουν. Το ίντερνετ λειτουργεί με τους συνδέσμους (links) και οι μηχανές αναζήτησης όταν ακολουθούν έναν σύνδεσμο που παραπέμπει σε κάποια άλλη σελίδα, τότε ανακαλύπτουν και τη νέα σελίδα και την ταξινομούν.
- Private Web: ιστοσελίδες που χρειάζεται να κάνετε login με username και password
- Contextual Web: είναι οι σελίδες εκείνες το περιεχόμενο των οποίων προσαρμόζεται ανάλογα με τον τρόπο που έχει κανείς πρόσβαση σε αυτό. Για παράδειγμα, οι σελίδες εκείνες που, αν έχει κανείς πρόσβαση σε αυτές με μία διεύθυνση IP από την Ελλάδα, βλέπει διαφορετικό περιεχόμενο από το αν θα επισκεπτόσασταν την ίδια σελίδα από μία IP των ΗΠΑ.
- Περιεχόμενο περιορισμένης πρόσβασης: ιστοσελίδες που περιορίζουν την πρόσβαση στο περιεχόμενό τους με τεχνικούς τρόπους (Robots Exclusion Standards, CAPTCHAS και άλλα)
- Scripted content: σελίδες που είναι διαθέσιμες μόνο από συνδέσμους που παράγονται από JavaScript καθώς και περιεχόμενο που κατεβάζεται από Web servers μέσω Flash. Αυτός είναι και ο λόγος που τα flash sites είναι αόρατα από τη Google.
- Non-HTML/text content: περιεχόμενο κειμένου που είναι κωδικοποιημένο σε αρχεία multimedia ή συγκεκριμένα formats που δεν μπορούν να διαβάσουν οι μηχανές αναζήτησης.

Σύμφωνα με εκτιμήσεις που έγιναν σε μία μελέτη στο Πανεπιστήμιο Berkeley της Καλιφόρνια (University of California, Berkeley) το 2001, το deep Web αποτελείται περίπου από 91.000 terabytes. Αντίθετα το επιφανειακό Web, που είναι εύκολα προσπελάσιμο από τις μηχανές αναζήτησης είναι περίπου 167 terabytes. Η Βιβλιοθήκη του Αμερικάνικου Κονγκρέσου, υπολογίστηκε πως το 1997 είχε 3.000 terabytes. Το 2011, το YouTube υπολογίζεται ότι είχε αποθηκευμένα περίπου 200

εκατομμύρια βίντεο, συνολικού μεγέθους 5 petabytes ή 5000 terabytes. Ο υπολογισμός του μεγέθους του web διαφέρει από πηγή σε πηγή και έτσι υπάρχει ένα μεγάλο περιθώριο λάθους και κανένας αριθμός δε μπορεί να θεωρηθεί ως ακριβής. Ωστόσο σχετικά με τον αριθμό των πηγών του deep Web υπάρχουν πιο ακριβείς εκτιμήσεις: Το 2004, ο He ανακάλυψε 300.000 deep web sites σε ολόκληρο το Web και σύμφωνα με τον Shestakov, περίπου 14.000 deep web sites υπήρχαν στο Ρώσικο τμήμα του Web το 2006. Γενικά θα πρέπει να υπολογίσουμε ότι το βαθύ ίντερνετ είναι πολλαπλάσιο του επιφανειακού ιστού. Μοιάζει σε μεγάλο βαθμό με το SEO, όπου το SEO που φαίνεται είναι πολύ μικρό σε αναλογία με το SEO που δεν φαίνεται. Κανείς δεν μπορεί να υπολογίσει με ακρίβεια σήμερα το μέγεθος του deep web μια και αυτό είναι συνεχώς μεταβαλλόμενο και αυξανόμενο σε μέγεθος. Συνεχώς καινούριες ιστοσελίδες προστίθενται στις παλιές και επειδή ο στόχος τους είναι να μείνουν κρυφές, είναι αρκετά δύσκολο με τις υπάρχουσες μηχανές αναζήτησης να τις βρούμε. Θα πρέπει δηλαδή να υπάρξει μια μεγάλη αλλαγή στη δομή του αλγορίθμου της Google, ή να δημιουργηθεί μια νέα μηχανή αναζήτησης για να μπορέσουμε να δούμε το βαθύ ίντερνετ.

1.4.1 Πρωτόκολλα και Λογισμικά του Dark / Deep Web

Το Dark / Deep Web λειτουργεί μέσω του Tor, όπου είναι ουσιαστικά ένα δίκτυο από μηχανήματα εθελοντών που επιτρέπει την ανώνυμη περιήγηση στο διαδίκτυο εφόσον ουσιαστικά, η πληροφορία που στέλνετε ή λαμβάνετε χρησιμοποιώντας το, περνά από διάφορα στάδια κρυπτογράφησης και διάφορες διαδρομές, μέχρι τα δεδομένα να φτάσουν στον προορισμό που κάποιος επιθυμεί (Καρακώστας, 2003). Το Tor μοιάζει δηλαδή με τα torrents όπου μπορεί κάποιος να κατεβάσει προγράμματα και ταινίες δωρεάν. Η τυχαιότητα της διαδρομής που θα ακολουθήσει η πληροφορία σας, είναι εκείνη που ουσιαστικά διασφαλίζει, τόσο την ανωνυμία στην περιήγησή , όσο και την δυσκολία σε κάποιον κακόβουλο να παρακολουθήσει τη δραστηριότητά ενός ατόμου. Η ίδια τυχαιότητα όμως και η πρόσβαση στην «υποδομή» του διαδικτύου είναι εκείνη που έχει δημιουργήσει και την τεράστια πηγή πληροφοριών στο Deep Web. Το Tor είναι η πύλη για το Deep Web καθώς το δίκτυο λειτουργεί σε όλες τις πλατφόρμες. Σύμφωνα με έρευνα που δημοσιεύει το techblog, το 80% του deep web traffic αφορά

σε παιδική πορνογραφία. Οι ερευνητές εξέτασαν περίπου 40.000 διαφορετικές υπηρεσίες στο Tor και βρήκαν την τεράστια ζήτηση για παιδική πορνογραφία, αν και τα συγκεκριμένα sites βρίσκονται μόλις στο 2% των διαθέσιμων υπηρεσιών του deep web. Η έρευνα επικεντρώνεται στις κρυμμένες υπηρεσίες, τις λεγόμενες «onion addresses» που είναι διαθέσιμες μόνο από το «inside Tor» (Mitrou, 2008).

Η περιήγησή στο Deep Web δεν έχει ως εμπειρία καμία σχέση με αυτό που γνωρίζουμε στο συμβατικό διαδίκτυο. Και ο βασικός λόγος είναι γιατί δεν υπάρχει κατηγοριοποίηση στις πληροφορίες, οπότε, δεν λειτουργεί με τόσο απλοϊκό τρόπο η αναζήτηση, όπως την έχουμε συνηθίσει στο Google, ή το Bing. Επίσης, στο Deep Web το TPL (Top Level Domain) είναι συνήθως της μορφής : .onion, αντιθέτως με τα γνωστά μας .com, .gr, .gov,.org.,ενώ και οι URL's δεν έχουν καμία λεκτική συνοχή. Η περιήγηση στο Deep Web, αρχίζει συνήθως με ιστοσελίδες που περιέχουν λίστες περιεχομένων όπως το Hidden Wiki παραδείγματος χάριν : ***http://3suaolltfj2xjksb.onion/hiddenwiki/index.php/Main_Page*** . Λόγω της συνεχούς και πολύπλοκης κρυπτογράφησης που υφίστανται τα πακέτα δεδομένων που διακινούνται στο Deep Web είναι πολύ δύσκολο να ανιχνευθεί η διαδρομή και εντοπισμός τους με αποτέλεσμα να προσφέρεται εν πολλοίς ανωνυμία με αποτέλεσμα να χρησιμοποιείται ευρέως για παράνομες και εγκληματικές δραστηριότητες. Περιλαμβάνονται σε αυτές η αγορά όπλων , ναρκωτικών , παιδική πορνογραφία και παιδοφιλία , πλαστές ταυτότητες, κακόβουλο λογισμικό, κλεμμένα gadgets κ.α.

ΚΕΦΑΛΑΙΟ 2ο : ΨΗΦΙΑΚΕΣ ΑΠΕΙΛΕΣ ΚΑΤΑ ΑΝΗΛΙΚΩΝ

Στο κεφάλαιο αυτό θα εστιάσουμε στους κινδύνους που αντιμετωπίζουν τα παιδιά και εν γένει τα ανήλικα άτομα από την περιήγηση στο διαδίκτυο. Οι κίνδυνοι που είναι υπαρκτοί και σοβαροί δεν αφορούν μόνο την προσβολή της γενετήσιας αξιοπρέπειας (αν και αυτοί είναι οι πιο συνηθισμένοι) αλλά αφορούν και γενικότερα την εκμετάλλευση των ανηλίκων ψυχολογικά ακόμα και οικονομικά.

2.1 Διαδικτυακή αποπλάνηση

Το έγκλημα της παιδικής κακοποίησης έχει ανεπανόρθωτες συνέπειες στην ζωή ενός ανήλικου, τον μετατρέπει σε έναν χαρακτήρα ασταθή με σοβαρά προσωπικά προβλήματα στους φίλους, στις σχέσεις και στην εμπιστοσύνη του με νέους ανθρώπους. Δημιουργεί έφηβους με ψυχικές διαταραχές, προβλήματα προσαρμοστικότητας και κατάθλιψη. Ο όρος ‘’παιδοφιλία’’ δεν περιλαμβάνει απαραίτητα προσπάθεια σεξουαλικής επαφής με ανήλικο άτομο, ενώ ο πιο συγκεκριμένος όρος ‘’παιδεραστία’’ αναφέρεται όταν υπάρχει και σεξουαλική δραστηριότητα. Πιο αναλυτικά παιδόφιλος μπορεί να χαρακτηριστεί κάποιος που του αρέσουν και έχει ερωτικές φαντασιώσεις με ανήλικα παιδιά. Από τη στιγμή όμως που το εν λόγω άτομο ασελγήσει πάνω σε ανήλικο τότε θεωρείται και παιδεραστής και όχι απλά παιδόφιλος. Ένας παιδεραστής είναι και παιδόφιλος ενώ ένας παιδόφιλος δεν είναι απαραίτητα και παιδεραστής. Η παιδοφιλία έχει χωριστεί σε κατηγορίες :

- Η ηβηφιλία (παιδιά πρώιμης εφηβικής ηλικίας)
- Η εφηβοφιλία (παιδιά εφηβικής ηλικίας και νεαρά άτομα (15-19 ετών), η οποία δε θεωρείται διαστροφή)
- Η νηπιοφιλία (νήπια 0 - 3 ετών).

Η διαδικτυακή σεξουαλική παρενόχληση ή αποπλάνηση ανηλίκου (cyber-grooming) είναι μία από τις πιο σοβαρές εγκληματικές απειλές στο διαδίκτυο. Ονομάζεται η διαδικασία συναισθηματικής σύνδεσης με έναν ανήλικο με σκοπό την κακοποίηση και εκμετάλλευση του. Ο θύτης (ένα άτομο η μία ομάδα ατόμων) είναι ενήλικας που προσπαθεί να προσελκύσει παιδιά προσποιούμενος ότι είναι έφηβος (γιατί ένα παιδί μπορεί να εμπιστευτεί πιο εύκολα έναν τις ίδιας περίπου ηλικίας με αυτό), χρησιμοποιώντας τα δωμάτια επικοινωνίας, τις ιστοσελίδες κοινωνικής δικτύωσης και άλλους χώρους όπου υπάρχει η δυνατότητα διαδικτυακής επικοινωνίας. Πολλές είναι οι φορές όπου ο παιδόφιλος είναι άτομο μορφωμένο, οικογενειάρχης, δάσκαλος, ακόμα και συγγενικό πρόσωπο. Οι περιπτώσεις των δασκάλων ή των συγγενών είναι και εκείνες όπου το παιδί δύσκολα θα τις αναφέρει στους γονείς του, μιας και από μεριάς συγγενικού προσώπου μπορεί να δέχεται απειλές προς μέλη της οικογένειας του, ενώ ο δάσκαλος να τον απειλεί πώς αν δεν κάνει αυτό που του λέει θα ενημερώσει τους γονείς του ή θα πάρει κακούς βαθμούς. Οι αναπαραστάσεις

συμμετοχής σε σεξουαλικές πράξεις ενός ανήλικου ή οι συνθήκες υποδήλωσης του σε σεξουαλικές δραστηριότητες είναι το κοινό στοιχείο στην παιδική πορνογραφία. Τα κυκλώματα παιδοφιλίας αποτελούνται από άτομα σε διαφορετικές χώρες, που συλλέγουν και διαμοιράζουν πορνογραφικό υλικό για να ικανοποιήσουν το αρρωστημένο τους μυαλό και για προσωπικό τους όφελος. Αναμειγνύουν πορνογραφικό υλικό ενηλίκων μαζί με ανηλίκων και το αναρτούν σε καμουφλαρισμένες ιστοσελίδες ώστε να μην μπορεί να γίνει εύκολα ο εντοπισμός τους. Χρησιμοποιούν παραπλανητικές φωτογραφίες και σύμβολα σε ιστοχώρους που δεν φέρνουν καθόλου σε παράνομο περιεχόμενο, αλλά αντιθέτως μοιάζουν με κάτι αθώο και ασφαλές για εκείνους που δεν γνωρίζουν και από την πλευρά εκείνων που τα γνωρίζουν κάτι αρρωστημένο και παράνομο. Το γεγονός ότι σήμερα ένα τεράστιο ποσοστό των νέων αναζητούν γνωριμίες μέσω διαδικτύου τους καθιστά και τους πιο συνηθής στόχους παρενόχλησης. Ο θύτης με σκοπό την σεξουαλική παρενόχληση, προσπαθεί να δημιουργήσει μία σχέση φιλίας με τα θύματα του και να συλλέξει όσο περισσότερες πληροφορίες (διεύθυνση, χόμπι κλπ.) μπορεί. Συνήθως τέτοιες συζητήσεις διαρκούν αρκετό καιρό, μέχρι το παιδί να φτάσει στο σημείο να εμπιστεύεται τον άνθρωπο που συνομιλεί, παρόλο που το πιο πιθανόν είναι να μην γνωρίζει καν την αληθινή του ταυτότητα. Αφού αναπτυχθεί αυτή η σχέση μεταξύ τους ξεκινούν και οι συζητήσεις σεξουαλικής φύσεως. Πιθανόν ένας παιδόφιλος να στέλνει και υλικό πορνογραφίας στον ανήλικο, για να τον κάνει να πιστεύει πώς αυτή η δραστηριότητα και πράξη είναι κάτι καθαρά φυσιολογικό και αποδεκτό. Μία τακτική που την χρησιμοποιούν συχνά για να κάνουν τα παιδιά πιο προσιτά και πρόθυμα στην προσπάθεια σεξουαλικής επαφής μαζί τους και επιπροσθέτως, διστάζουν να μιλήσουν στους γονείς τους γιατί φτάνουν στο σημείο να νιώθουν ένοχα που έχουν κάνει τέτοιου είδους συνομιλίες και έχουν ανταλλάξει τέτοιου είδους φωτογραφίες και βίντεο. Σύμφωνα με έρευνα του Βρετανικού Οργανισμού «Stop It Now» που καταπολεμά την σεξουαλική παιδική κακοποίηση, τα ¾ των παιδιών που έχουν πέσει θύμα του φαινομένου δεν θα μιλήσουν για αυτό που τους συνέβη και λίγα ήταν τα περιστατικά εκείνα που ενημέρωσαν κατάλληλες υπηρεσίες. Επίσης έρευνες έχουν δείξει πώς η κακοποίηση των κοριτσιών φτάνει μέχρι και 3 φορές ψηλότερα από ότι τα αγόρια. Από τις πιο προσοδοφόρες εγκληματικές δραστηριότητες μετά το εμπόριο ναρκωτικών είναι εκείνη της παιδικής πορνογραφίας. Στις ΗΠΑ, τα καθημερινά νούμερα συναλλαγών αυτού του απάνθρωπου υλικού φτάνουν τις 700.000 και διακινούνται δύο τρισεκατομμύρια δολάρια. Ενώ σε παγκόσμιο επίπεδο διακινούνται

καθημερινά πέντε τρισεκατομμύρια δολάρια (κατά μέσο όρο). Το περισσότερο υλικό προέρχεται από χώρες της νοτιοανατολικής Ασίας, της Αφρικής και Λατινικής Αμερικής. Ενώ το κόστος διαφέρει ανάλογα με την ηλικία των παιδιών που συμμετέχουν (από βρέφη μέχρι και παιδιά πριν την ενηλικίωση).

Ύστερα από αρκετή έρευνα στην σκοτεινή πλευρά του διαδικτύου οι αστυνομικοί της Δίωξης Ηλεκτρονικού Εγκλήματος εντόπισαν των κώδικα επικοινωνίας των παιδόφιλων, ο οποίος αναφέρεται αναλυτικά παρακάτω :

Το συγκεκριμένο σύμβολο αναφέρεται στους παιδόφιλους που προτιμούν μικρά αγόρια.

Το συγκεκριμένο σύμβολο αναφέρεται στους παιδόφιλους που προτιμούν μικρά κορίτσια.

Το συγκεκριμένο σύμβολο αναφέρεται γενικά στους παιδόφιλους.

2.2 Προσωπικά δεδομένα

Προσωπικά δεδομένα ονομάζονται οι πληροφορίες που αναφέρονται σε ένα άτομο, όπως το ονοματεπώνυμο, το τηλέφωνο, οι φωτογραφίες, η ηλικία, το επάγγελμα, πολιτικές – θρησκευτικές απόψεις , κ.α. Πολλές είναι οι πληροφορίες που ανήκουν στην κατηγορία των ευαίσθητων δεδομένων, δηλαδή εκείνων όπου μπορεί να προκύψει ο σχηματισμός της προσωπικότητας του ατόμου. Για παράδειγμα, πληροφορίες που αφορούν την υγεία, την ερωτική ζωή, συμμετοχή σε οργανώσεις και ομάδες καθώς και το ποινικό μητρώο του είναι μερικά από τα στοιχεία όπου μπορούν να καταλήξουν σε ένα συμπέρασμα σχετικά με την ζωή και τον χαρακτήρα κάποιου, ακόμα και να οδηγήσουν στην αποκάλυψη της πραγματικής ταυτότητας του προσώπου στο οποίο αναφέρονται τα δεδομένα αν δεν είναι ήδη γνωστή. Τα προσωπικά δεδομένα αποτελούν αντικείμενο επεξεργασίας καθημερινά σε απλές δραστηριότητες, όπως :

- Στην χρήση e-mail, ο πάροχος ηλεκτρονικών επικοινωνιών καταγράφει την ώρα εισόδου στον λογαριασμό, τον αποστολέα και τους παραλήπτες του μηνύματος και την ώρα αποστολής.
- Στην αγορά τραγουδιών διαδικτυακά, η εταιρία που πουλάει το τραγούδι καταγράφει τις προσωπικές προτιμήσεις.
- Στην είσοδο σε κάποια διαφήμιση, η διαφημιστική εταιρία καταγράφει προτιμήσεις για πιο στοχευμένες μελλοντικές διαφημίσεις.

Μερικές φορές όμως μπορεί να επεξεργάζονται και να χρησιμοποιούνται από τρίτους με πιο κακόβουλο χαρακτήρα, όπως :

- Στην περίπτωση των ληστών, ενημέρωση από τα μέσα κοινωνικής δικτύωσης για τυχόν κοινοποίηση παρουσίας του ατόμου σε κάποιο μέρος εκτός της οικίας του και πληροφορίες που αφορούν ίσως συγκατοίκηση με άλλο-α πρόσωπα.
- Κλοπή διαδικτυακής ταυτότητας, κάποιος να κλέψει τις πληροφορίες ενός ατόμου και να δημιουργήσει ένα προφίλ ίδιο με το δικό του, από φωτογραφίες μέχρι και βιογραφικό.

Οτιδήποτε αναρτηθεί στο διαδίκτυο μπορεί να μείνει για πάντα και να είναι και άμεσα ορατό σε όλους, πρέπει να γίνετε έλεγχος των ρυθμίσεων ασφαλείας και απορρήτου που έχει κάθε ιστοχώρος. Σύμφωνα με στατιστικά στοιχεία της Eurobarometer, το 76% των Ευρωπαίων φοβούνται ότι τα προσωπικά τους δεδομένα δεν είναι ασφαλή όταν τα διαχειρίζονται ιδιωτικές εταιρίες , ενώ στην περίπτωση των δημόσιων αρχών είναι το 64%.

2.3 Διαδικτυακός εκφοβισμός

Παρενόχληση-Εκφοβισμός (bullying) ονομάζεται η ακραία συμπεριφορά από πρόθεση, για να έχει δύναμη και εξουσία ένα άτομο πάνω σε κάποιο άλλο. Υπάρχουν διαφορετικού τύπου εκφοβισμοί, που μπορεί να είναι :

- ο Λεκτικός (προσβολές, βρισιές, διάδοση φημών κλπ.)

- ο Ψυχολογικός (απειλές με στόχο τον φόβο , εξαναγκασμός να κάνει το θύμα πράγματα που δεν επιθυμεί)
- η Σωματική βία (καυγάδες , εσκεμμένοι τραυματισμοί), καταστροφή προσωπικών αντικειμένων και κλοπές αντικειμένων του θύματος
- η Κοινωνική απομόνωση , αγνόηση της παρουσίας του θύματος είτε ακόμα και η αποτροπή της συμμετοχής του από δραστηριότητες και παρέες.

Ο Διαδικτυακός εκφοβισμός (cyberbullying) είναι ένα από τα πιο διαδεδομένα και συνηθισμένα προβλήματα που μπορεί να συναντήσει κάποιος στο διαδίκτυο. Είναι ένα φαινόμενο επαναλαμβανόμενης επιθετικότητας, παρενόχλησης, προσβολής, ταπείνωσης, ρατσιστικής και αυταρχικής συμπεριφοράς κυρίως σε παιδιά η έφηβους, που δέχονται μέσω της χρήσης του Διαδικτύου και των διάφορων ψηφιακών συσκευών (κινητά τηλέφωνα , ηλεκτρονικοί υπολογιστές κλπ.). Ο ψηφιακός εκφοβισμός μοιάζει πολύ με τον απλό εκφοβισμό , αφού και στις δύο περιπτώσεις υπάρχει θύμα, θύτης και παρατηρητές. Οι βασικές διαφορές είναι στο γεγονός της πολύ γρήγορης εξάπλωσης σε λίγο χρονικό διάστημα σε πολλούς παραλήπτες , ο θύτης νιώθει ανώνυμος και η έλλειψη προσωπικής επαφής με το θύμα τον κάνει ακόμα πιο σκληρό απέναντι του. Μπορεί επίσης να κλέψει την ταυτότητα του θύματος ή να υποδυθεί τρίτους. Συνήθως πραγματοποιείται μεταξύ συνομήλικων. Η ανάγκη για επιβολή δύναμης, θυμός, ζήλεια, διασκέδαση είτε πάλι και αντεκδίκηση σε κάποιο συμβάν, να είναι μερικοί λόγοι όπου κάποιος μπορεί να γίνει θύτης απέναντι σε άτομα που στην πραγματική ζωή θα δίσταζε να τα αντιμετωπίσει πρόσωπο με πρόσωπο. Από την μεριά του θύματος όμως, σε τέτοια περιστατικά ασκείται κάποιος φόβος και αγανάκτηση, με αποτέλεσμα ένα ίσως όχι και τόσο αθώο παιχνίδι να έχει σοβαρές συνέπειες. Κάποιες φορές ο εκφοβισμός οδηγεί στην περιθωριοποίηση και στον αποκλεισμό του θύματος από ένα άτομο ή μία ομάδα ατόμων. Μπορεί να το οδηγήσουν σε εκπαιδευτική αποτυχία, να μην μπορεί να διαχειριστεί αυτό που του συμβαίνει με αποτέλεσμα να του δημιουργηθεί κατάθλιψη ή στις ακραίες των περιπτώσεων να μην βρίσκει κάποιο αδιέξοδο και να καταλήγει στην αυτοκτονία. Ένας ψηφιακός εκβιαστής σήμερα έχει μεγάλη πληθώρα νέων τεχνολογιών που μπορεί να επιλέξει και να χρησιμοποιήσει για τον εκφοβισμό του θύματος του. Από τις πιο γνωστές μεθόδους άσκησης του φαινομένου είναι :

- Η αποστολή μηνυμάτων (e-mail, δωμάτια συνομιλίας, sms) με προσβλητικό και απειλητικό περιεχόμενο. Τα μηνύματα αυτά συνήθως θα σταλθούν σε μία ομάδα ατόμων, με την ενθάρρυνση να πάρουν μέρος σε έναν εκφοβισμό ή αμέσως στο ίδιο το θύμα.
- Η δημοσίευση φωτογραφιών κακόβουλου σκοπού σε ιστολόγια και σε μέσα κοινωνικής δικτύωσης. Δεν λείπουν και οι φορές που δημιουργούνται ιστοσελίδες αποκλειστικά και μόνο για την κατακραυγή και την στοχοποίηση κάποιου ατόμου.
- Ανώνυμες κλήσεις
- Παραβίαση προσωπικών λογαριασμών
- Αποστολή προγραμμάτων-ιών (δούρειοι ίπποι) με σκοπό την κλοπή προσωπικών στοιχείων για την παραποίηση τους ή την κατασκοπεία.

Σε ένα τόσο σημαντικό θέμα όπως αυτό της διαδικτυακής ασφάλειας παίζει σημαντικό ρόλο και η σχολική κοινότητα. Πρέπει να δίνονται όσο στους μαθητές τόσο και στους καθηγητές οι απαραίτητες γνώσης αντιμετώπισης τέτοιων φαινομένων. Σύμφωνα με έρευνες έχει διαπιστωθεί πώς σε σχολεία που έχει γίνει κατάλληλη ενημέρωση δεν εμφανίζονται τόσο συχνά θύματα σε αντίθεση με κάποια άλλα που επικρατεί άγνοια. Στην περίπτωση που κάποιος έχει γίνει στόχος διαδικτυακού εκφοβισμού, η πιο καλή ενέργεια είναι να αποφύγει να απαντήσει σε ενοχλητικές κλήσεις και μηνύματα που πιθανόν να υπάρχουν. Ιδιαίτερη προσοχή στις ρυθμίσεις απορρήτου των λογαριασμών κοινωνικών δικτύων και σε κάθε περίπτωση σε τέτοια περιστατικά είναι αναγκαίο να διατηρούμε αποδεικτικά στοιχεία των γεγονότων που συνέβησαν (μηνύματα , email , λογαριασμοί , ημερομηνίες και ώρες).

2.4 Sexting & Ακατάλληλο περιεχόμενο

Ακατάλληλο ονομάζεται οποιοδήποτε περιεχόμενο, λεκτικό, ακουστικό και οπτικό που είναι επικίνδυνο και μη ασφαλές, μπορεί να περιλαμβάνει πορνογραφικό υλικό, ρατσιστικό περιεχόμενο, προώθηση βίας, τυχερά παιχνίδια κλπ. Ο όρος ακατάλληλο περιεχόμενο διαφέρει ανάλογα με την ηλικία ή και την ψυχική κατάσταση κάθε ατόμου. Ένα περιεχόμενο μπορεί να είναι ακατάλληλο και απαράδεκτο για ένα παιδί, μπορεί να το σοκάρει ή να του προκαλέσει ψυχικές διαταραχές και λανθασμένες

συμπεριφορές. Το ίδιο όμως περιεχόμενο για ένα άτομο μεγαλύτερης ηλικίας μπορεί να θεωρηθεί κατάλληλο και αποδεκτό. Πλέον ένα παιδί μπορεί να έρθει αντιμέτωπο με περιεχόμενο που δεν είναι κατάλληλο για την ηλικία του σε πολλές δραστηριότητες και χώρους του διαδικτύου και όχι μόνο, όπως :

- Στις διάφορες ιστοσελίδες που ίσως να μην γνωρίζει το ακριβές περιεχόμενο τους.
- Στα παιχνίδια, μερικά περιέχουν σκηνές βίας, βρισιές κλπ.
- Μέσω του ηλεκτρονικού ταχυδρομείου.
- Μέσω του κινητού τηλεφώνου.
- Στα δωμάτια επικοινωνίας.

Sexting (sex + texting) ονομάζεται η αποστολή-ανταλλαγή φωτογραφιών, βίντεο και γραπτών μηνυμάτων με σεξουαλικό περιεχόμενο. Πραγματοποιείται μέσω κινητών τηλεφώνων με SMS-MMS, σε ιστοσελίδες κοινωνικής δικτύωσης, αλλά εντοπίζεται πιο συχνά σε υπηρεσίες που παρέχεται διαδικτυακή επικοινωνία με δυνατότητα άμεσης ανταλλαγής μηνυμάτων. Ένα φαινόμενο το οποίο συνεχώς αυξάνει τα ποσοστά του στον εφηβικό πληθυσμό. Θα μπορούσε κάποιος να χαρακτηρίσει το Sexting σαν την μοντέρνα παραλλαγή του διαδικτυακού σεξ, με την μοναδική διαφορά το γεγονός ότι δεν περιορίζεται μονάχα σε διαδικτυακές συσκευές αλλά γίνεται και μέσω των κινητών τηλεφώνων. Στο Sexting μπορεί να υπάρξουν σοβαρά νομικά ζητήματα στις περιπτώσεις που εμπλέκονται ανήλικα άτομο σε μία επικοινωνία σεξουαλικής φύσεως, καθώς η διανομή και παραγωγή φωτογραφιών ή και βίντεο που αφορά ανήλικους, ως γνωστών είναι παράνομη διαδικασία. Παρόλα αυτά πολλά ήταν τα παιδιά που κατηγορήθηκαν για αυτή τους την ενέργεια και σε μερικές περιπτώσεις στις Η.Π.Α κάποια από αυτά έχουν καταδικαστεί κιόλας με την κατηγορία της διανομής παιδικής πορνογραφίας, ενώ δεν γνώριζαν καν ότι αυτό που έκαναν ήταν κάτι παράνομο. Σε σχετική επιστημονική έρευνα του τμήματος ψυχολογίας του Πανεπιστημίου του Μίσιγκαν που έγινε σε 3.447 άνδρες και γυναίκες ηλικίας 18-24 ετών, διαπιστώθηκε ότι το 57% δεν ήταν αποστολείς αλλά ούτε παραλήπτες τέτοιων μηνυμάτων, το 28.2% έστελνε και αποδεχόταν, το 12.6% ήταν μόνο παραλήπτες και το υπόλοιπο 2% του κοινού τις έρευνας ήταν μόνο αποστολείς.

2.5 Ιός Ransomware

Ένας ιός τύπου Ransomware είναι ένα είδος κακόβουλο λογισμικού και χαρακτηριστικό παράδειγμα της μεθόδου phishing. Ένας ιός απάτη με πολλαπλά ονόματα και μορφές, στην Ελλάδα κάποιος θα τον αποκαλέσει συνήθως ως «ιό των 100 ευρώ» ή «ιό της αστυνομίας». Το κακόβουλο πρόγραμμα περιορίζει την πρόσβαση στον υπολογιστή – κινητό τηλέφωνο όπου μολύνει και απαιτεί την πληρωμή κάποιου χρηματικού ποσού από το θύμα, προκειμένου να αφαιρεθεί από το μηχάνημα και να συνεχίσει ο χρήστης κανονικά. Πιο αναλυτικά, ένας ιός ransomware κλειδώνει όλες τις λειτουργίες του μηχανήματος που θα καταλάβει και ίσως να κρυπτογραφεί αρχεία του συστήματος. Προσπαθεί μέσω μίας σελίδας ή κάποιου αναδυόμενου παραθύρου που υποτίθεται ότι προέρχεται από μία επίσημη αρχή (κυρίως Ελληνική Αστυνομία ή Δίωξη Ηλεκτρονικού Εγκλήματος), να εξαπατήσει τον χρήστη πώς λόγο κάποιας παράνομης του συμπεριφοράς στο διαδίκτυο, όπως παιδική πορνογραφία, συμμετοχή σε παράνομα παιχνίδια, παράνομη κατοχή αρχείων κ.ά. είναι ένοχος και πρέπει να καταβάλει πρόστιμο, γιατί ειδάλλως προβλέπεται φυλάκιση για αυτές του τις ενέργειες.

Ο δράστης εκμεταλλεύεται τις αδυναμίες του μηχανήματος ή κάποια λάθος κίνηση του θύματος, κατά την περιήγηση του στο διαδίκτυο και του μεταφέρει κακόβουλο λογισμικό. Για παράδειγμα ο ιός μπορεί να εγκατασταθεί :

- Στο άνοιγμα συνημμένων σε μηνύματα ηλεκτρονικού ταχυδρομείου από άγνωστο κακόβουλο αποστολέα.
- Από την είσοδο σε κακόβουλες διευθύνσεις – ιστοσελίδες που μπορεί να υπάρχουν σε μηνύματα, email ή σε ιστοσελίδες κοινωνικής δικτύωσης κλπ.
- Από την επίσκεψη σε ιστοσελίδες πορνογραφικού περιεχομένου, παράνομου τζόγου κ.ά.
- Από την είσοδο σε διαφημίσεις.

Στις περιπτώσεις που τα δεδομένα κρυπτογραφούνται (το ransomware Cryptolocker είναι το πιο διαδεδομένο και οι πιο πολλές μορφές του ιού βασίζονται πάνω σε αυτό), το πρόγραμμα δημιουργεί ένα δημόσιο και ένα ιδιωτικό κλειδί αλληλεξαρτούμενα. Το δημόσιο κλειδί αποθηκεύεται στο σύστημα και μπορεί να έχει πρόσβαση ο χρήστης σε αυτό. Όμως το ιδιωτικό κλειδί αποθηκεύεται στον διακομιστή διοίκησης και ελέγχου και δίνεται από τον δράστη μετά την καταβολή του ποσού, για να πραγματοποιηθεί η αποκρυπτογράφηση των δεδομένων.

Το πρόστιμο καλείται να πληρώσει το θύμα συνήθως με προπληρωμένες κάρτες paysafe ή ucash ίσης αξίας με το χρηματικό ποσό (πχ 100 ευρώ το πρόστιμο θα πληρωθεί με 100 ευρώ κάρτα paysafe και όχι 2 των 50 ή 4 των 25 κλπ.). Μία τακτική του εγκλήματος που χρησιμοποιείται για ξέπλυμα μαύρου χρήματος, καταφέρνει οργανωμένα να διασπά το αρχικό ποσό τις προπληρωμένης κάρτας σε μικρότερα ποσά και στην συνέχεια τα διανέμει σε όλο τον κόσμο. Το κακόβουλο λογισμικό έχει κυκλοφορήσει σε αρκετές εκδόσεις με διαφορετική εμφάνιση, δυνατότητες και μέγεθος κρισιμότητας. Υπάρχουν εκδόσεις που απλά με ένα αναδυόμενο παράθυρο περιορίζουν την λειτουργικότητα και άλλες που φτάνουν μέχρι και στην κρυπτογράφηση αρχείων. Όμως το κοινό χαρακτηριστικό όλων είναι η καταβολή προστίμου. Μερικές εκδόσεις του λογισμικού είναι :

- Το «Simple locker» που δραστηριοποιείται στον χώρο των κινητών τηλεφώνων και tablets με λειτουργικό σύστημα Android. Με την εγκατάσταση του λογισμικού στη συσκευή, όλα τα αποθηκευμένα αρχεία που ανιχνεύονται σε κάποια μονάδα εξωτερικής αποθήκευσης (κάρτες μνήμης) κρυπτογραφούνται, με αποτέλεσμα να μην είναι προσβάσιμα. Επίσης στην οθόνη της συσκευής, υπάρχει κατάλληλο μήνυμα που ενημερώνει τον κάτοχο πώς το κλείδωμα των αρχείων προήρθε λόγο προβολής και διακίνησης ακατάλληλου εγκληματικού υλικού.

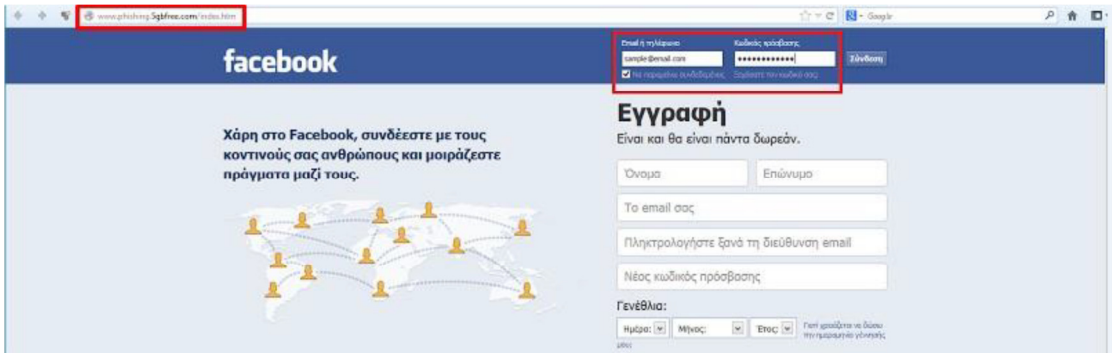
- Το CTB-Locker (Curve Tor Bitcoin Locker - Critroni), διαφέρει στον τρόπο καταβολής του χρηματικού ποσού σε σχέση με τις άλλες εκδόσεις. Πλέον για να ξεκλειδωθεί το μολυσμένο μηχάνημα πρέπει ο χρήστης να πληρώσει με ψηφιακό νόμισμα bitcoin.

- Το Teslacrypt, πέρα από τα αρχεία στοχεύει και κρυπτογραφεί κυρίως αποθηκευμένα παιχνίδια που ίσως να υπάρχουν στο μολυσμένο μηχάνημα.

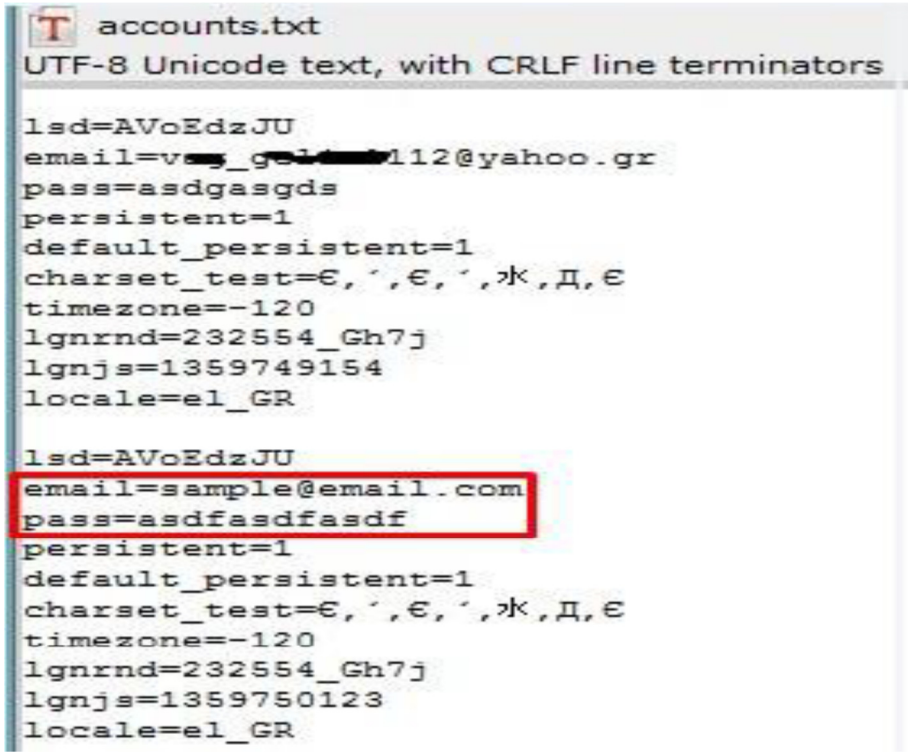
2.6 Phishing (Ηλεκτρονικό "Ψάρεμα")

Phishing (Ηλεκτρονικό Ψάρεμα) ονομάζεται η μέθοδος εξαπάτησης των χρηστών του διαδικτύου, που πραγματοποιείται κυρίως με την αποστολή μαζικών spam μηνυμάτων στο ηλεκτρονικό ταχυδρομείο, με άμεσα μηνύματα σε δωμάτια επικοινωνίας ή κοινωνικά δίκτυα και μέσω συνδέσεων που οδηγούν σε πλαστές όμοιες σελίδες εταιριών (τράπεζες, ηλεκτρονικά καταστήματα κ.λπ.). Η παραπάνω απάτη βασίζεται στην παραπλάνηση, άγνοια και απροσεξία των χρηστών. Ο θύτης υποδύεται μία αξιόπιστη πηγή, με κύριο στόχο να προσελκύσει το θύμα και να

αποσπάσει απόρρητα προσωπικά δεδομένα και οικονομικά στοιχεία. Πιο αναλυτικά, ο αποστολέας απαιτεί από τον παραλήπτη να επαληθεύσει, να ενημερώσει προσωπικά του δεδομένα ή να συνδεθεί με τα αυτά σε κάποια υπηρεσία για λόγους ασφαλείας. Στην συνέχεια το θύμα ανυποψίαστο οδηγείται στην πλαστή ιστοσελίδα και καταχωρεί τα δεδομένα που του ζητούνται.



Ο θύτης καταγράφει τα προσωπικά στοιχεία του χρήστη για μελλοντική κακόβουλη χρήση τους. Πολλές φορές προσπαθεί να εντοπίσει και άλλους λογαριασμούς που ίσως να έχει το θύμα χρησιμοποιώντας το email του και παραλλαγές του κλεμμένου κωδικού του.



Αρκετές είναι οι φορές που η απάτη είναι καλά οργανωμένη και οι phishers καλύπτουν το URL (διαδικτυακή διεύθυνση) της πλαστής ιστοσελίδας τους με ένα άλλο ψεύτικο, με αποτέλεσμα να εξαπατούν με αυτόν τον τρόπο anti-phishing προγράμματα. Όμως πέρα από την εξαπάτηση των προγραμμάτων καταπολέμησης του phishing, στόχος είναι και η εξαπάτηση του θύματος για την αυθεντικότητα και αξιοπιστία της σελίδας. Κάτι που μπορεί να πετύχει με τεχνικές οπτικής εξαπάτησης, όπως :

- Μικρές αλλαγές στην σύνταξη, στην ορθογραφία στους συνδέσμους ή αναγραμματισμούς (πχ www.fasebook.com , www.yutoube.com κλπ.).
- Χρησιμοποίηση ίδιων εικόνων και λογοτύπων με αυτά εταιριών (πχ το λογότυπο του Facebook σε ένα email).
- Με τον πηγαίο κώδικα της σελίδας και με τις παραπάνω τακτικές, μπορεί να δημιουργηθεί μία ολόκληρη σελίδα, ακριβές αντίγραφο με την αυθεντική.

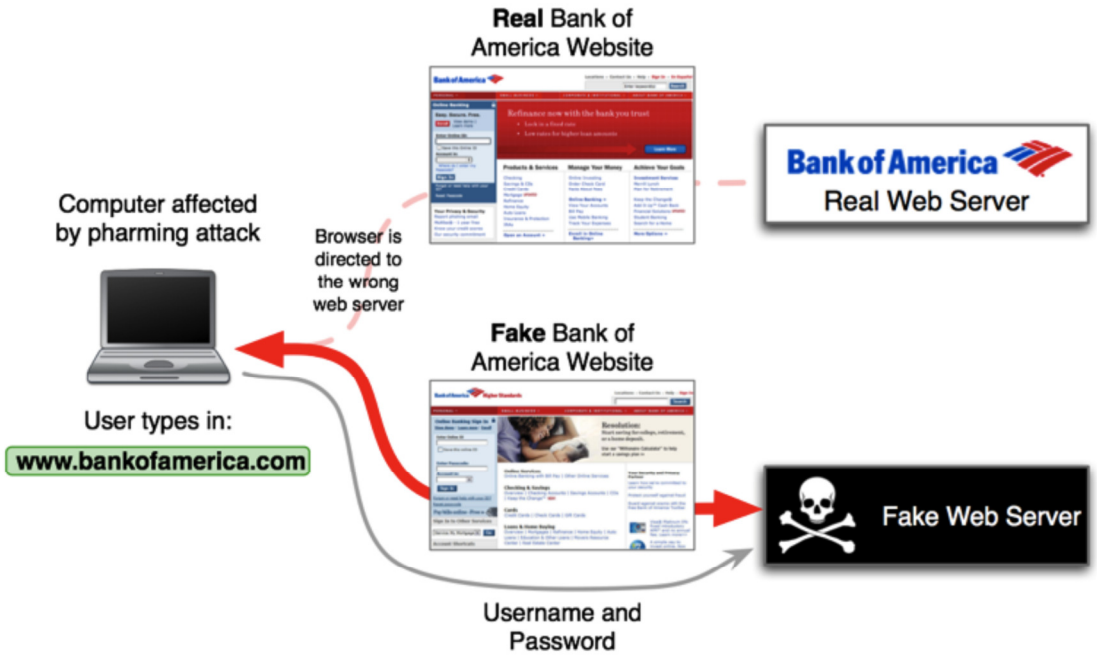
Υπάρχουν αρκετοί τύποι της μεθόδου, πιο συγκεκριμένα υπάρχει :

- Η απλή μέθοδος phishing, όπου ο θύτης παριστάνει ένα αξιόπιστο πρόσωπο και προσπαθεί να αποκτήσει προσωπικές πληροφορίες και στοιχεία πιστωτικών καρτών.
- Το Spear Phishing, που στοχοποιεί συγκεκριμένα πρόσωπά ή εταιρίες. Οι επιτιθέμενοι προσπαθούν αν συλλέξουν προσωπικά στοιχεία για το θύμα τους με στόχο να αυξήσουν την πιθανότητα επιτυχίας της επίθεσης.
- Το Clone Phishing, ένας τύπος επίθεσης που παίρνει νόμιμα μηνύματα ηλεκτρονικού ταχυδρομείου με συνημμένα αρχεία που είχαν είδη παραδοθεί παλαιότερα, δημιουργεί αντίγραφα του και αντικαθιστά το συνημμένο ή συνδέσμους που πιθανόν να υπάρχουν με κακόβουλα αρχεία και πηγές. Στην συνέχεια αποστέλλονται από μία πλαστογραφημένη διεύθυνση ηλεκτρονικού ταχυδρομείου ίδια με του αρχικού αποστολέα.
- Το Whaling, απευθύνεται σε ανώτερα στελέχη επιχειρήσεων (διευθυντές, διαχειριστές). Οι πλαστές ιστοσελίδες και μηνύματα θα αφορούν θέματα που είναι ανησυχητικά και κρίσιμα για μία εταιρία (δικαστικές υποθέσεις, παράπονα πελατών κλπ.).

- Rogue WiFi (MITM), όπου ο κακόβουλος χρήστης δημιουργεί σημεία με δωρεάν ασύρματη πρόσβαση στο διαδίκτυο και μπορεί να αναμεταδώσει, υποκλέψει στοιχεία που υπάρχουν σε μία επικοινωνία (επιθέσεις man in the middle - MTIM) ή γενικά στοιχεία περιήγησης του χρήστη στο διαδίκτυο.

2.7 Pharming

Η μέθοδος εξαπάτησης Pharming είναι η εξελιγμένη εκδοχή του Phishing, μία μορφή εγκλήματος εξαιρετικά επικίνδυνη που στοχεύει και εκείνη στην κλοπή των προσωπικών δεδομένων των χρηστών. Διαφέρει από τις τεχνικές phishing ως προς τον τρόπο που επιτυγχάνεται. Το κακόβουλο πρόγραμμα εκμεταλλεύεται κενά ασφαλείας του συστήματος και εισχωρεί στο μολυσμένα πλέον μηχάνημα του ανυποψίαστου χρήστη. Το σύστημα επηρεάζεται με τέτοιο τρόπο που το θύμα στην προσπάθεια του να επισκεφτεί διαδικτυακούς τόπους, παρόλο που πληκτρολογεί σωστά τις διευθύνσεις που επιθυμεί να επισκεφτεί στο πρόγραμμα περιήγησης του, αυτό τον ανακατευθύνει σε άλλες όμοιες σελίδες αλλά πλαστές. Οι δράστες (Pharmers), στοχεύουν στην ανακατεύθυνση ιστοσελίδων όπου οι χρήστες εισάγουν αριθμούς τραπεζικών καρτών ή άλλων οικονομικών στοιχείων για διαδικτυακές συναλλαγές. Για παράδειγμα στην προσπάθεια που το θύμα επισκεφτεί μία τράπεζα στόχο για συναλλαγές του μέσω on-line banking καταλήγει να στέλνει τα στοιχεία που εισήγαγε στους εγκληματίες.



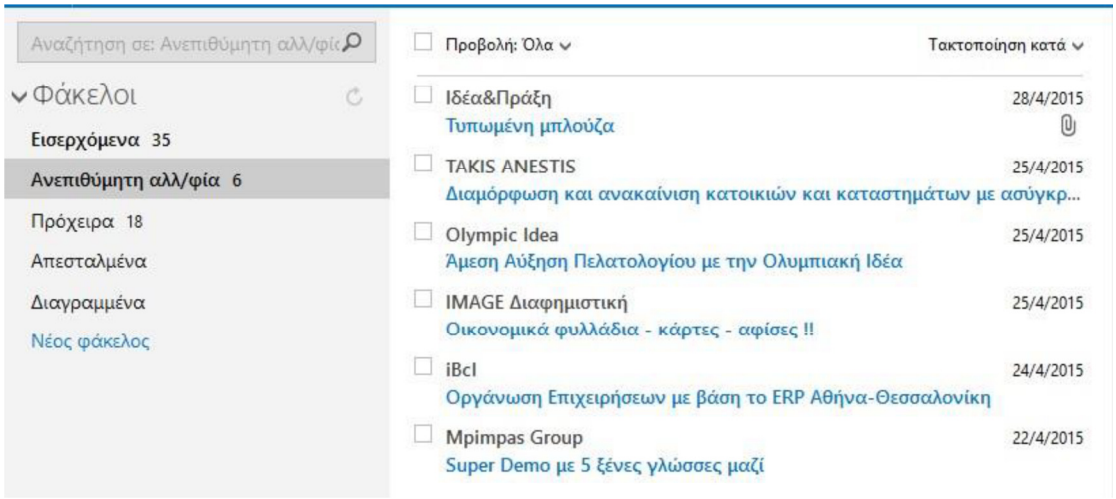
Το Pharming μπορεί να υλοποιηθεί αν το κακόβουλο πρόγραμμα που εισχωρήσει στο μηχάνημα τροποποιήσει αρχεία ή ρυθμίσεις του συστήματος , όπως :

- Την αλλαγή των ρυθμίσεων ή και του firmware (λογισμικό συσκευής) ενός router, έτσι μπορεί να επιτευχθεί η ανακατεύθυνση των διευθύνσεων για όλες τις συσκευές του δικτύου.
- Την τροποποίηση του «host» αρχείου ενός Η/Υ.
- Την πρόσβαση στον κεντρικό DNS server και αλλαγή των σωστών IP διευθύνσεων με ψεύτικων.

Αξίζει να σημειωθεί ότι, host ονομάζεται κάθε υπολογιστής δικτύου που παρέχει υπηρεσίες, αποθηκεύει αρχεία ιστοσελίδων και περιλαμβάνει και web server για τον διαμοιρασμό του περιεχομένου στο διαδίκτυο. Κάθε host και όχι μόνο, έχει μία ξεχωριστή διεύθυνση IP ή οποία τον αντιπροσωπεύει και αναπαρίσταται από αριθμούς (0-255) χωρισμένους με τελείες σε 4 μέρη (πχ 173.203.142.18). Όλες οι οντότητες που έχουν πρόσβαση στο διαδίκτυο αντιστοιχούν σε κάποια IP διεύθυνση. Κάθε πακέτο μεταφοράς δεδομένων συνοδεύεται και αυτό επίσης από δύο IP, μία του αποστολέα και μία του παραλήπτη. Επίσης σε συνδέσεις με το πρωτόκολλο επικοινωνίας Https δεν υπάρχει πρόβλημα για pharming.

2.8 Spamming – Scamming

Η μαζική αποστολή ενοχλητικών, άσχετων ή μη αποδεκτών μηνυμάτων, τα οποία έχουν σαν στόχο συνήθως την προώθηση κάποιου προϊόντος-υπηρεσίας, ονομάζεται Spamming. Το Spam βασίζεται στην κακή αντιμετώπιση και άγνοια των χρηστών, οι αποστολείς spam μηνυμάτων προσπαθούν να προσελκύσουν τον χρήστη με ένα αρκετά ενδιαφέρον περιεχόμενο στα μηνύματα, έτσι ώστε να ανταποκριθούν σε αυτά. Συνήθως οι Spammers (αποστολείς spam μηνυμάτων), χρησιμοποιούν ηλεκτρονικά μέσα για την αποστολή των μηνυμάτων, λόγο του μηδενικού λειτουργικού κόστους πέρα από αυτού τις διαχείρισης των λιστών από τα email χρηστών που χρησιμοποιούνται και του τεράστιου αριθμού αποδεκτών. Επομένως, ακόμα και αν κάποιο μικρό ποσοστό χρηστών ανταποκριθεί στο περιεχόμενο, θεωρείται επιτυχία. Τα περιεχόμενα των ενοχλητικών μηνυμάτων μπορεί να είναι προσβλητικά και επικίνδυνα πέρα από αυτά που έχουν σαν στόχο απλά την διαφήμιση. Για παράδειγμα, αρκετά spam διαφημίζουν πλαστά προϊόντα, από φάρμακα μέχρι λογισμικό υπολογιστή ως επίσημα προϊόντα ή υπηρεσίες γνωστών εταιριών, άλλα είναι εκείνα που διαδίδουν ειδήσεις παραπλανητικές και ψεύτικες και μερικά ασχολούνται με διαφημίσεις υπηρεσιών πορνογραφικού χαρακτήρα.



Επίσης τα μηνύματα spam χρησιμοποιούνται και σαν μέσα μετάδοσης κακόβουλων αρχείων και ιών. Όταν ο στόχος του αποστολέα είναι η μόλυνση του υπολογιστή του χρήστη και η εξαπάτηση του, με σκοπό να υποκλέψει δεδομένα και να τα χρησιμοποιήσει κακόβουλα, τότε πρόκειται για την διαδικασία που ονομάζεται Scamming. Για παράδειγμα ένας κακόβουλος χρήστης μπορεί να μολύνει το

μηχάνημα και να αποκτήσει πρόσβαση σε αυτό, για να το χρησιμοποιήσει σαν μέσω αποστολής μηνυμάτων spam ή και για άλλες κακόβουλες ενέργειες όπως καταγραφή πληκτρολογίου, καταγραφή των click ή και κλοπή προσωπικών δεδομένων. Αξίζει να σημειωθεί πώς μεγάλη έξαρση υπάρχει στα spam μηνύματα τύπου phishing, που στοχεύουν στην παραπλάνηση των χρηστών μέσω πλαστών ιστοσελίδων όμοιες με τις πραγματικές, για την αλίευση προσωπικών δεδομένων. Απώτερος σκοπός ή απόσπαση ευαίσθητων πληροφοριών (αριθμός πιστωτικής κάρτας, κωδικοί λογαριασμών κοινωνικών δικτύων κλπ.). Επίσης spam δημοσιεύσεις σε κοινωνικά δίκτυα όπως Facebook, που διαδικτυακοί φίλοι έχουν μολυνθεί, με αποτέλεσμα να προσθέτουν ή να κοινοποιούν σε άλλα άτομα δημοσιεύσεις που προσπαθούν να πείσουν τους χρήστες πώς το περιεχόμενο τους είναι αρκετά ενδιαφέρον και να πατήσουν τον σύνδεσμο, με αποτέλεσμα να μολυνθούν και εκείνοι. Έρευνες έχουν δείξει πώς πάνω από το 70% των μηνυμάτων ηλεκτρονικού ταχυδρομείου είναι spam και σε σχετική μελέτη που πραγματοποιήθηκε στην Μεγάλη Βρετανία το 22% των χρηστών έχουν προβεί σε αγορές προϊόντων-υπηρεσιών που διαφημίζονταν μέσω spam τουλάχιστον μία φορά.

ΚΕΦΑΛΑΙΟ 3 : SEXTING ΚΑΙ GROOMING ΑΠΟ ΚΙΝΗΤΕΣ ΣΥΣΚΕΥΕΣ

Η ραγδαία ανάπτυξη των ψηφιακών τεχνολογιών φέρνει συχνά αντιμέτωπους γονείς, εκπαιδευτικούς και εφήβους με νέα, σύνθετα, ηθικά διλήμματα αναφορικά με ζητήματα ιδιωτικότητας, ασφάλειας και δικαιωμάτων .

3.1 Sexting μέσω φορητών συσκευών

Sexting ονομάζεται η ανταλλαγή σεξουαλικών μηνυμάτων / γυμνών φωτογραφιών / βίντεο μέσω διαδικτύου ή/και κινητών τηλεφώνων και αποτελεί μια διαδεδομένη πρακτική, τόσο μεταξύ των εφήβων, όσο και μεταξύ των ενηλίκων (Sexting και έφηβοι, 2016). Ενώ το sexting στο πλαίσιο του σχολείου, παλαιότερα, εμφανίζονταν

περισσότερο μέσα από τη χρήση κινητών τηλεφώνων (sms και mms), ωστόσο, με τη διείσδυση του διαδικτύου σε κάθε σύγχρονη συσκευή (κινητά τηλέφωνα, tablet κ.τ.λ.) τα μηνύματα σεξουαλικής έκφρασης / απεικόνισης (sexts) δύναται να μεταδίδονται μέσω e-mail αλλά και μέσω ιστοτόπων κοινωνικής δικτύωσης (Τσουβέλας, Γιωτάκος & Λούβρης, 2014). Η βασική διάκριση ανάμεσα στη διακίνηση πορνογραφικού ή οιονεί πορνογραφικού υλικού και των sexts είναι ότι τα sexts σε πρώτο επίπεδο διακίνησης παράγονται και διαδίδονται με τη βούληση του απεικονιζόμενου προσώπου. Η λήψη και αποστολή σεξουαλικών μηνυμάτων - φωτογραφιών - βίντεο από τους εφήβους μπορεί να εκφράζει ένα είδος ερωτικής σχέσης μεταξύ τους που συμβαδίζει με τις σύγχρονες τεχνολογικές εξελίξεις και την διευρυμένη χρήση του υπολογιστή και των κινητών τηλεφώνων. Τα τελευταία χρόνια, πολλά νέα παιδιά επιλέγουν να φωτογραφίζονται γυμνά και να στέλνουν τις φωτογραφίες τους, χωρίς να αντιλαμβάνονται τους κινδύνους και τις συνέπειες που μπορεί να έχει αυτή -η απλή φαινομενικά- πράξη στη ζωή τους και την ψυχολογία τους. Επιπλέον, οι έφηβοι ενδέχεται να επηρεάζονται και από τα σεξουαλικά τηλεοπτικά πρότυπα, τις διαφημίσεις, τα τηλεοπτικά shows ακόμα και από τραγούδια ή διαδικτυακά βίντεο (Sexting και έφηβοι, 2016). Όπως προκύπτει από τη μελέτη των Strassberg et al. (2012), σε δείγμα εφήβων στο λύκειο στις Η.Π.Α. περίπου το 20% των συμμετεχόντων αναφέρει ότι έχει στείλει σε άλλους μια δική του φωτογραφία, σεξουαλικού περιεχομένου, ενώ αντίστοιχα το 25% που έχει λάβει αντίστοιχο υλικό, το προώθησε και σε άλλους εφήβους. Αντίστοιχα ποσοστά εντοπίζουμε και στη μελέτη National Campaign to Prevent Teen and Unplanned Pregnancy and CosmoGirl.com (2008) και στη μελέτη του Thomas (2009). Ανεξάρτητα από την συναίνεση ή όχι στη διακίνηση των sexts (σε ένα δεύτερο επίπεδο προώθησης) είναι σαφές ότι το φαινόμενο δύναται να δημιουργήσει σοβαρές επιπτώσεις στις ζωές των μαθητών σε κοινωνικό, συναισθηματικό και νομικό επίπεδο (Τσουβέλας και συν. 2015). Εξετάζοντας το ζήτημα του sexting από νομικής πλευράς, είναι σαφές ότι οι συνέπειες του δύναται να έχουν σημαντική επίδραση στην πορεία ζωής του παιδιού ή του εφήβου τόσο στο παρόν όσο και στο μέλλον. Ειδικότερα, στις περιπτώσεις που το άτομο που απεικονίζεται είναι ανήλικος, ο φωτογράφος / το άτομο που έκανε τη βιντεοσκόπηση, καθώς και όσα άτομα εμπλέκονται στη διακίνηση του υλικού δύναται να αντιμετωπίσουν σοβαρές νομικές επιπτώσεις. Ειδικότερα, η διακίνηση μιας ημίγυμνης ή γυμνής φωτογραφίας ενός μαθητή που μπορεί να γίνει στο πλαίσιο μια προσωπικής επικοινωνίας, σε νομικό επίπεδο εμπίπτει στο φάσμα της διακίνησης

παιδικής πορνογραφίας. Αντίστοιχες δικαστικές υποθέσεις εντοπίζονται στη βιβλιογραφία (DeFalco, 2009. Pawloski, 2010. National Center for Missing & Exploited Children, 2011. Park, 2010. National Conference of State Legislatures, 2011). Αναφορικά με τις νομικές συνέπειες στην Ελλάδα, η γνωστοποίηση σε τρίτους, μηνυμάτων ή φωτογραφιών σεξουαλικού περιεχομένου που αφορούν σε ανήλικους είναι μια πολύ σοβαρή συμπεριφορά που μπορεί, κατά περίπτωση, να υπαχθεί στη νομοθεσία που απαγορεύει τη συλλογή και επεξεργασία ευαίσθητων προσωπικών δεδομένων (Ν. 2472/1997) ή ακόμη και να συνιστά αδίκημα σχετικό με παιδική πορνογραφία (άρθρο 348 Α ΠΚ). Πέρα από τα όσα εν συντομία αναφέραμε για τις νομικές προεκτάσεις, είναι προφανές ότι το sexting δύναται να προκαλέσει σημαντικές αρνητικές συνέπειες στη ζωή των εφήβων τόσο σε συναισθηματικό όσο και κοινωνικό επίπεδο. Ειδικότερα στα πλαίσια του σχολείου κάποιες από τις πιθανές επιπτώσεις του sexting είναι η συναισθηματική δυσφορία, ο σχολικός ή και διαδικτυακός εκφοβισμός, η αποξένωση και η κοινωνική απομόνωση από τους συμμαθητές και τη σχολική κοινότητα, η απώλεια της ιδιωτικότητας και η διαπόμπευση (Τσουβέλας και συν. 2014). Παρά το ότι το φαινόμενο του σχολικού εκφοβισμού δεν είναι κάτι νέο, εντούτοις μέσω της ψηφιακής τεχνολογίας, όπου διευκολύνεται η ευρεία και ταχεία διάδοση των εικόνων και οπτικοακουστικού υλικού, αυξάνεται σημαντικά ο κίνδυνος και η ευπάθεια των ατόμων που απεικονίζονται στα sexts. Απόρροια των παραπάνω είναι η δυνητική διαπόμπευση των εικονιζόμενων ατόμων, η στοχοποίησή τους και η ψυχολογική τους κακοποίηση. Επιπρόσθετα, έχουν καταγραφεί περιπτώσεις αυτοκτονίας και αποπειρών αυτοκτονίας ως αποτέλεσμα κοινωνικής απομόνωσης και σχολικού εκφοβισμού ύστερα από διαρροή υλικού sexting (βλ. Kranz, 2009. Meacham, 2009. Inbar, 2009). Ως αποτέλεσμα των όσων αναφέρουμε πιο πάνω είναι προφανές ότι μέσω του sexting αυξάνεται σημαντικά η επικινδυνότητα οι έφηβοι να βιώσουν εκφοβισμό, αίσθημα του αβοήθητου, κατάθλιψη και αυτοκτονικό ιδεασμό (Τσουβέλας, 2014). Μέσα από μια αναπτυξιακή ματιά καθίσταται σαφές ότι οι εμπλεκόμενοι μαθητές στο sexting είναι μάλλον απίθανο να κατανοούν όλες τις πτυχές και τους κινδύνους που σχετίζονται με το φαινόμενο. Η αναφορά που γίνεται πιο πάνω αφορά γνωστικές διεργασίες που είναι υπό ανάπτυξη κατά την εφηβεία και αφορούν σχεδιασμό ενεργειών και λήψη αποφάσεων (Steinberg & Scott, 2003). Οι περισσότεροι εμπλεκόμενοι έφηβοι, συχνά, δεν μπορούν να διανοηθούν ότι ένα sext – π.χ. που περιέχει μια αποκαλυπτική τους φωτογραφία – μπορεί να προωθηθεί σε πολλαπλούς

αποδέκτες καθώς και ότι κάτι που προορίζονταν στα πλαίσια μιας ιδιαίτερα προσωπικής στιγμής ή/και επικοινωνίας δύναται να καταλήξει να έχει διανεμηθεί σε πολλαπλούς παραλήπτες. Στη μελέτη της Rohler (2012), το ποσοστό των εφήβων που βρέθηκε να συμφωνεί με την παραπάνω θέση ήταν μόλις 54%. Επίσης, συχνά οι έφηβοι δεν μπορούν να αντιληφθούν το γεγονός ότι όταν κάποιος/α λαμβάνει ένα αντίστοιχο μήνυμα από αυτούς είτε εικόνα, είτε βίντεο το αρχείο αυτό μπορεί να αποθηκευτεί σε χώρο εκτός του κινητού τηλεφώνου και να ανασυρθεί κάποια στιγμή στο μέλλον τόσο από τον αποδέκτη όσο και από άλλους που μπορεί να έχουν πρόσβαση στο ψηφιακό αποθηκευτικό μέσο (Τσουβέλας και συν. 2014). Τι μπορούν να κάνουν οι γονείς γι'αυτό; Παρότι είναι δεδομένο ότι οι έφηβοι επηρεάζονται από τους συνομηλίκους, εντούτοις οι γονείς θα συνεχίζουν να ασκούν σημαντική επιρροή στις ζωές τους. Όταν ένας γονέας διατηρεί θετική σχέση με το έφηβο παιδί του, το θωρακίζει ώστε να δημιουργήσει και να διατηρήσει υγιείς σχέσεις με τους φίλους του. Έφηβοι που έχουν θετικές σχέσεις με τους γονείς τους, συχνά, έχουν θετικές σχέσεις και με τους συνομηλίκους. Κάποιες προτάσεις αναφορικά με το πώς να επικοινωνήσουμε το ζήτημα του sexting με τα παιδιά είναι οι εξής:

- Ενισχύουμε την αυτοεκτίμησή τους, ώστε να είναι θωρακισμένα, να δημιουργούν θετικές σχέσεις με τους συνομηλίκους και να μπορούν να αντισταθούν στην αρνητική πίεση από τους άλλους.
- Έφηβοι με αυτοπεποίθηση και με υψηλό αίσθημα αυτοαξίας είναι λιγότερο πιθανό να υποκύψουν στην πίεση των συνομηλίκων.
- Διαμορφώνουμε μια θετική και ανοιχτή επικοινωνία με τον/την έφηβο/η
- Παροτρύνουμε το παιδί ώστε να μπορεί πάντα να έρθει σε εμάς για αναζήτηση βοήθειας ή συμβουλής σχετικά με τις σχέσεις του με τους συνομηλίκους και για θέματα που σχετίζονται με την σεξουαλικότητα του και το απασχολούν.
- Μαθαίνουμε στο παιδί πως να λαμβάνει λογικές αποφάσεις. Μαθαίνοντας στο παιδί να εξετάζει τις θετικές και τις αρνητικές όψεις, θα κατακτήσει δεξιότητες να αναλύει καταστάσεις και να λαμβάνει ορθολογικές αποφάσεις.
- Αναφορικά με το sexting μάθαινουμε το παιδί να ζυγίζει τις πιθανές επιθυμητές συνέπειες (π.χ. αποδοχή από την ομάδα, το ότι αισθάνεται ενθουσιασμό κάνοντας κάτι καινούργιο και κρυφό) με τις πιθανές μη επιθυμητές συνέπειες (π.χ. τα μηνύματα / εικόνες / βίντεο θα μπορούσαν να ποσταριστούν και ή να διαδοθούν σε όλο το σχολείο ή στο διαδίκτυο κ.α.)

- Μαθαίνουμε στο παιδί τρόπους να λέει «όχι» στην αρνητική επιρροή των άλλων.
- Συζητάμε με το παιδί πιθανά σενάρια
- Συζητάμε μαζί του αυτά τα σενάρια και σκεφτόμαστε μαζί του τρόπους με τους οποίους θα μπορούσε να χειριστεί ανάλογες καταστάσεις αν του συνέβαιναν. Είναι αποτελεσματικότερο να αφήνουμε πρώτα το παιδί να εκφραστεί και να προβληματιστεί παρά να βιαστιούμε να του δώσετε έτοιμες απαντήσεις / λύσεις.
- Συζητάμε με το παιδί το ζήτημα του μόνιμου χαρακτήρα που μπορεί να πάρουν οι φωτογραφίες που ανταλλάσσονται και ευαισθητοποιήστε το αναφορικά με το πόσο εύκολα και γρήγορα μπορούν να διανεμηθεί αυτό το υλικό σε άλλους χωρίς τη συγκατάθεση του ατόμου που απεικονίζει η φωτογραφία.
- Τέλος καλό είναι να γνωρίζουν γονείς και παιδιά ότι μια φωτογραφία που αναρτάται στο Διαδίκτυο μπορεί να μείνει εκεί για πάντα.
- Η στρατηγική «καλύτερα προλαμβάνειν παρά θεραπεύειν», αποδεικνύεται η αποτελεσματικότερη στρατηγική για το sexting. Είναι προτιμότερο οι έφηβοι να έχουν συλλογιστεί για ανάλογες καταστάσεις πριν συμβούν παρά να προσπαθούν – παιδιά, γονείς και κοινότητα - να δια-χειριστούν τις δυσμενείς συνέπειες που μπορεί να προκύψουν μετά την αποστολή και διακίνηση αντίστοιχου υλικού.

3.2 Grooming: Σεξουαλική Αποπλάνηση

Ο όρος **Grooming** αναφέρεται στην αποπλάνηση και συμβαίνει όταν άγνωστοι εκμεταλλεύονται κακόβουλα το στοιχείο της ανωνυμίας στο Διαδίκτυο για να προσεγγίσουν ανήλικους με στόχο τη σεξουαλική παρενόχληση. Γενικά, στο Διαδίκτυο ποτέ δεν μπορούμε να είμαστε σίγουροι ποιος είναι ο συνομιλητής μας στις ηλεκτρονικές μας επικοινωνίες, ακόμα και αν βλέπουμε τη φωτογραφία του ή αν χρησιμοποιούμε ψηφιακή κάμερα. Έτσι, πολλοί επιτήδειοι εκμεταλλεύονται το γεγονός αυτό, δίνουν ψεύτικα στοιχεία (π.χ., ηλικία) και ξεκινούν συζητήσεις με τα πιθανά θύματά τους με στόχο να αναπτύξουν φιλική σχέση και να αποσπάσουν όσο το δυνατό περισσότερες πληροφορίες (π.χ., τόπο διαμονής, τα ενδιαφέροντά τους, τις σεξουαλικές τους εμπειρίες κλπ). Το Grooming αποτελεί ένα είδος ψυχολογικού χειρισμού και για το λόγο αυτό είναι σημαντικό **να εξηγήσουμε στους γονείς** πως οφείλουν να είναι ενημερωμένοι για τις διαδικτυακές γνωριμίες των παιδιών τους

ώστε, όταν παρατηρήσουν κάτι ύποπτο, να μπορέσουν να τα συμβουλέψουν αποτελεσματικά και να δράσουν άμεσα.

3.2.1 Κατηγορίες Θυμάτων

Τα θύματα του Grooming είναι συνήθως έφηβοι ηλικίας 11 έως 17 ετών, ενώ σύμφωνα με έρευνες το κορίτσια είναι πιο ευάλωτα σε αυτό το φαινόμενο από τα αγόρια. Έχουν, όμως, αναφερθεί και συγκεκριμένες κατηγορίες παιδιών που τα καθιστούν ακόμα πιο ευάλωτα σε αυτήν τη διαδικασία:

1. Παιδιά με χαμηλή αυτοεκτίμηση και έλλειψη αυτοπεποίθησης.
2. Παιδιά με συναισθηματικά προβλήματα ή με προβλήματα στις σχέσεις με γονείς, σχολείο και συνομήλικους.
3. Παιδιά που δείχνουν αφελή και υπερβολική εμπιστοσύνη στους άλλους.
4. Έφηβοι, καθότι τους απασχολούν και τους ενδιαφέρουν τα σεξουαλικά ζητήματα.

Επιπλέον, οι ακόλουθες κατηγορίες παρουσιάζονται ως ιδιαίτερα ευάλωτες σε πιθανή διαδικτυακή σεξουαλική παρενόχληση:

1. Κορίτσια
2. Έφηβοι ηλικίας 14 έως 17 ετών.
3. Νέοι που έχουν βιώσει κάποιο αρνητικό γεγονός στο στενό οικογενειακό τους περιβάλλον καθώς και νέοι με καταθλιπτικό συναίσθημα.
4. Τακτικοί χρήστες του διαδικτύου (που δαπανούν πάνω από δύο ώρες ημερησίως και πάνω από τέσσερις μέρες την εβδομάδα στο διαδίκτυο ενώ αξιολογούν ότι το διαδίκτυο έχει μεγάλη σημασία για τη ζωή τους).
5. Συμμετέχοντες σε διαδικτυακά δωμάτια συνομιλιών (chat rooms) ενώ επιδεικνύουν επικίνδυνη διαδικτυακή συμπεριφορά (π.χ., παρέχουν προσωπικές και εμπιστευτικές πληροφορίες, σχολιάζουν με άκομψο και προκλητικό τρόπο, ενοχλούν άλλους χρήστες, συζητούν για σεξουαλικά ζητήματα με κάποιον που δεν γνωρίζουν, επισκέπτονται εκουσίως πορνογραφικούς διαδικτυακούς τόπους κλπ).

Σε αρκετές περιπτώσεις η παρενόχληση γίνεται από παιδιά προς παιδιά. Σε αυτή την περίπτωση, καλό είναι να αναζητήσουμε τον θύτη και να μιλήσουμε με τους γονείς

του. Αν το πρόβλημα δεν μπορεί να λυθεί με τη δική μας παρέμβαση και κρίνεται απαραίτητη η λήψη δραστικότερων μέτρων μπορούμε να καταγγείλουμε το περιστατικό στην ανοιχτή γραμμή SafeLine (http://www.safeline.gr στην ηλεκτρονική διεύθυνση report@safeline.gr) ή στο τηλέφωνο 2811 391615 από τις 9.00 έως τις 16.00 (εργάσιμες ημέρες).

3.3 Cyber-Bulling: Διαδικτυακός εκφοβισμός

Ο όρος **διαδικτυακός εκφοβισμός** (Cyber-bullying) αφορά τον εκφοβισμό που είναι δυνατό να πραγματοποιηθεί μέσω του Διαδικτύου και περιλαμβάνει εσκεμμένη, επαναλαμβανόμενη και εχθρική συμπεριφορά απέναντι σε συγκεκριμένο άτομο ή ομάδα ατόμων με σκοπό την πρόκληση συναισθηματικής και ψυχολογικής βλάβης. Ο διαδικτυακός εκφοβισμός συνήθως έχει τη μορφή ενός εκφοβιστικού, ρατσιστικού, ή προσβλητικού ηλεκτρονικού μηνύματος, φωτογραφίας ή βίντεο και ενδεχομένως μπορεί να οδηγήσει στην περιθωριοποίηση και τον κοινωνικό αποκλεισμό των θυμάτων. Γενικά, ο εκφοβισμός αυτός είναι δύσκολο να ελεγχθεί, αφού δεν υπάρχει περιορισμός των μηνυμάτων που διανέμονται ηλεκτρονικά (περίπτωση ανεπιθύμητης αλληλογραφίας[1]) καθώς και του αριθμού των παραληπτών που μπορούν να γίνουν δέκτες αυτών των μηνυμάτων.

3.3.1 Τρόποι Αντιμετώπισης

Ενδεικτικοί τρόποι αντιμετώπισης του παραπάνω διαδικτυακού κινδύνου επισημαίνονται παρακάτω:

1. Εάν πέσουμε θύμα εκφοβισμού, σταματάμε αμέσως την επικοινωνία με το θύτη.
2. Εμπιστευόμαστε στους γονείς μας ή σε κάποιο ενήλικα τον εκφοβισμό που έχουμε δεχθεί.
3. Δεν προωθούμε εκφοβιστικά μηνύματα.
4. Αν γνωρίζουμε κάποιο φίλο που είναι θύτης τον συμβουλεύουμε να σταματήσει.
5. Φιλτράρουμε ηλεκτρονικά μηνύματα από άτομα που μάς παρενοχλούν και μπλοκάρουμε την πρόσβασή τους σε προσωπικούς δικτυακούς χώρους (π.χ., ιστολόγιο).

Είναι χρήσιμο να επισημανθεί ότι στην ηλεκτρονική διεύθυνση http://www.antibullying.eu παρουσιάζεται η Ευρωπαϊκή καμπάνια κατά του σχολικού εκφοβισμού σε όλες του τις μορφές (π.χ., διαδικτυακός εκφοβισμός) που υλοποιείται στα πλαίσια του κοινοτικού προγράμματος Daphne III. Ο στόχος του συγκεκριμένου προγράμματος συνίσταται στη δημιουργία μιας ενιαίας πολιτικής στην καταγραφή και διαχείριση του σχολικού εκφοβισμού και την δημιουργία μιας Ευρωπαϊκής πλατφόρμας για την ενημέρωση των παιδιών, γονέων, εκπαιδευτικών και κάθε άμεσα ενδιαφερόμενου για το συγκεκριμένο πρόβλημα.

ΚΕΦΑΛΑΙΟ 4ο : ΜΕΤΡΑ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΨΗΦΙΑΚΩΝ ΑΠΕΙΛΩΝ

Η ασφάλεια και η προστασία ενός συστήματος από ψηφιακές απειλές περιλαμβάνει τρείς βασικούς άξονες : την πρόληψη (prevention) , την ανίχνευση (detection) και την ανάνηψη (recovery) ενός συστήματος από παραβιάσεις ασφαλείας. Στο παρόν κεφάλαιο θα αναφερθούμε στους μηχανισμούς, και τις τεχνικές πρόληψης, ανίχνευσης και αντιμετώπισης που χρησιμοποιούνται για την προστασία ενός συστήματος Η/Υ και γενικότερα συσκευών που συνδέονται στο Δικτυο. Άλλωστε σήμερα , λόγω της διείσδυσης του Internet και της άνθησης του Ηλεκτρονικού εμπορίου, οι γνωστικοί χώροι της Ασφάλειας Δικτύων και της Ασφάλειας Η/Υ τείνουν να συγκλίνουν.

4.1 Προγράμματα Antivirus

Το οπλοστάσιο για την προστασία έναντι κακόβουλου λογισμικού περιλαμβάνει εκτός των άλλων τα προγράμματα Antivirus. Η αντιμετώπιση των ιών έχει δύο σκέλη: τον *εντοπισμό* του ιού και την *απάλειψη* του. Τα προγράμματα antivirus πραγματοποιούν έλεγχο των αρχείων ενός Η/Υ για τον εντοπισμό μολυσματικού λογισμικού. Τα αρχεία αυτά μπορεί να είναι αρχεία δεδομένων, αρχεία συστήματος, ή αρχεία εφαρμογών. Επίσης, μπορεί να είναι αποθηκευμένα σε κάποια μονάδα βοηθητικής μνήμης ή να εισέρχονται στο σύστημα μέσω δικτύου (LAN, Internet). Ο κώδικας κάθε ιού έχει ορισμένα χαρακτηριστικά που τον διαφοροποιούν από τους υπόλοιπους ιούς. Το τμήμα εκείνο του κώδικα ενός ιού που χαρακτηρίζει μοναδικά τον ιό ονομάζεται υπογραφή ή αποτύπωμα του ιού. Ένα πρόγραμμα antivirus τηρεί μια *Βάση Δεδομένων* με τις υπογραφές όλων των γνωστών ιών, και ελέγχει όλα τα εκτελέσιμα αρχεία ενός Η/Υ (κατά την αποθήκευση ή εκτέλεση τους) για τον εντοπισμό μιας υπογραφής που έχει ήδη αποθηκευτεί στη Β.Δ. Εφόσον βρει κάποιο «ταίριασμα» (matching), το πρόγραμμα antivirus μπλοκάρει την εκτέλεση του κακόβουλου προγράμματος και ενημερώνει το χρήστη. Συνήθως προτρέπει το χρήστη να αποφασίσει αν επιθυμεί α) διαγραφή (delete), β) απομόνωση (isolation, quarantine) ή επιδιόρθωση (repair, clean) του μολυσμένου αρχείου. Η μέθοδος αυτή, αν και αξιόπιστη, παρουσιάζει *προβλήματα*: Το πρόγραμμα antivirus μπορεί να εντοπίσει και να απομακρύνει ιούς που είναι ήδη γνωστοί. Αυτό σημαίνει πως δεν προσφέρει προστασία έναντι ιών που δεν έχουν ανιχνευθεί ακόμα (τουλάχιστον, μέχρι να γίνει η ενημέρωση - λήψη της υπογραφής τους από τον διακομιστή Web). Επιπλέον, τα προγράμματα antivirus παραδοσιακά δυσκολεύονται στην καταπολέμηση πολυμορφικών ιών καθώς και ιών τύπου stealth/rootkits. Για το λόγο αυτό τα προγράμματα antivirus συχνά επιστρατεύουν προηγμένες τεχνικές όπως *heuristic scanning*, *behavior blocking* και *integrity checking* που θα εξετάσουμε στη συνέχεια. Οι μέθοδοι αυτές εντοπίζουν κώδικα που μπορεί να μη βρίσκεται στη ΒΔ αλλά συγκεντρώνει αρκετές πιθανότητες να είναι κακόβουλος. Αυτό έχει ως αποτέλεσμα η διάγνωση να μην είναι πάντα επιτυχημένη (π.χ. *λάθος συναγερμός* – false alarm).

Οι βασικές (Ελάχιστες) Δυνατότητες που (πρέπει να) έχει μια εφαρμογή Antivirus είναι :

- Εύχρηστο Interface & χαμηλή κατανάλωση πόρων. Το περιβάλλον της εφαρμογής πρέπει να είναι λιτό, και φιλικό προς τον χρήστη. Πολλάπαράθυρα, πολύπλοκες ρυθμίσεις και παράμετροι μπορούν να έχουν

εντελώς αντίθετα αποτελέσματα και να θέσουν σε ρίσκο την ασφάλεια του συστήματος. Επίσης, ένα πρόγραμμα antivirus θα πρέπει να προσφέρει τις υπηρεσίες του δεσμεύοντας μικρό μόνο ποσοστό από τους πόρους του υπολογιστή (μνήμη και υπολογιστική δύναμη).

- Προστασία σε πραγματικό χρόνο. Τα προγράμματα antivirus συνήθως διαθέτουν ένα υποσύστημα διάγνωσης και προστασίας σε πραγματικό χρόνο (real-timeprotection). Το antivirus φορτώνεται στην κεντρική μνήμη κατά την εκκίνηση τουΗ/Υ και λειτουργεί στο παρασκήνιο (background), ελέγχοντας τη μνήμη του συστήματος, καθώς και τα αρχεία και τις εφαρμογές που εκτελούνται ή εισέρχονται στο σύστημα για την ύπαρξη κακόβουλου λογισμικού.
- Αυτόματη ενημέρωση Σε αντίθεση με το παρελθόν, όπου τη διαδικασία ενημέρωσης την εκκινούσε ο χρήστης χειρωνακτικά, σήμερα τα προγράμματα antivirus ενημερώνουν αυτόματα τη βάση δεδομένων τους με τις πρόσφατες υπογραφές των ιών (virus definitions). Η ενημέρωση θα πρέπει να είναι τακτική (ο αποδεκτός σήμερα ρυθμός ενημέρωσης είναι της τάξης των λίγων ημερών), με δεδομένο ότι καθημερινά εμφανίζονται καινούριοι ιοί.
- Προστασία Ηλεκτρονικής Αλληλογραφίας. Το antivirus ελέγχει τα εισερχόμενα και εξερχόμενα μηνύματα ηλεκτρονικής αλληλογραφίας για την ύπαρξη ιών (στα συνημμένα έγγραφα). Για να συμβεί αυτό το πρόγραμμα θα πρέπει να συνεργάζεται με τα πλέον δημοφιλή προγράμματα ηλεκτρονικής αλληλογραφίας.
- Προγραμματισμένος Έλεγχος. Το antivirus επιτρέπει τον καθορισμό (scheduling) προγραμματισμένων ελέγχων στους δίσκους του συστήματος, σε συγκεκριμένη ημερομηνία ή ανά τακτά χρονικά χρονικά διαστήματα.
- Δισκέτα Εκκίνησης: Για την αντιμετώπιση των ιών τύπου boot sector, ή για την αντιμετώπιση περιπτώσεων όπου η εκκίνηση του Λ.Σ. είναι αδύνατη, συνήθως τα προγράμματα antivirus προσφέρουν τη δυνατότητα δημιουργίας μιας δισκέτας εκκίνησης. Η δισκέτα αυτή ενσωματώνει εφαρμογές διάγνωσης και καθαρισμού του boot sector ή/και (κρίσιμων) αρχείων συστήματος, σε περίπτωση που αυτά έχουν επικαλυφθεί (overwrite) από κακόβουλο λογισμικό.
- Καταγραφή Συμβάντων (event logging).

4.1.1 Προηγμένες Τεχνικές και Δυνατότητες Προγραμμάτων Anti-Virus

Η τεχνολογική εξέλιξη τόσο σε επίπεδο Hardware όσο και Software έχει οδηγήσει στην αντίστοιχη εξέλιξη και των αντί-υιικών προγραμμάτων με αποτέλεσμα την ανάπτυξη και διεύρυνση των δυνατοτήτων τους. Ειδικότερα μπορούμε να αναφέρουμε :

- **Ευρετικές (heuristic) μέθοδοι.** Έλεγχος κώδικα για εύρεση πιθανού (άγνωστου) Ιού. Σε αντίθεση με τους αλγόριθμους ελέγχου της υπογραφής ενός ιού, η ευρετική μέθοδος εξετάζει τον εκτελέσιμο κώδικα ενός αρχείου με σκοπό την εύρεση εντολών (ή συνόλου από εντολές) που θα μπορούσαν να αποτελούν τμήμα κακόβουλου κώδικα, με μεγάλη πιθανότητα. Παραδείγματα αποτελούν η ύπαρξη μακροεντολών σε ένα έγγραφο Office, εντολές κλήσης-τροποποίησης άλλων προγραμμάτων, ρουτίνες αποκρυπτογράφησης, εντολές διαγραφής αρχείων ή τροποποίησης του μητρώου του συστήματος, κ.λ.π. Η τεχνική αυτή είναι προενεργή (proactive), δηλαδή προσπαθεί να εντοπίσει «ύποπτο» τμήμα κώδικα πριν αυτός εκτελεστεί.
- **Έλεγχος Ακεραιότητας (integrity checks)**. Κατά την αποθήκευση ενός αρχείου, υπολογίζονται και αποθηκεύονται το μέγεθος του αρχείου, καθώς και ένα άθροισμα ελέγχου (checksum). Το άθροισμα ελέγχου είναι ένας αριθμός μοναδικός για το αρχείο αυτό: Η αλλαγή έστω και ενός bit στο αρχείο θα έχει ως αποτέλεσμα την αλλαγή του αθροίσματος ελέγχου με μεγάλη πιθανότητα. Για μεγαλύτερη ασφάλεια, μπορεί να χρησιμοποιηθεί η *κρυπτογραφική τιμή hash* του κώδικα του προγράμματος. Κάθε φορά που εκτελείται ένα αρχείο, το antivirus υπολογίζει το άθροισμα ελέγχου και το συγκρίνει την αποθηκευμένη τιμή. Αν οι δύο αριθμοί δεν είναι ίδιοι, αυτό σημαίνει πως α) ο χρήστης έχει προβεί σε μια καθ' όλα νόμιμη ενέργεια (π.χ. ενημέρωση-επιδιόρθωση του προγράμματος), ή β) ένας ιός άλλαξε τον κώδικα του αρχείου.
- **Έλεγχος Συμπεριφοράς (behaviour blocking)**. Η τεχνική αυτή μοιάζει με την τεχνική εκτέλεσης σε «προστατευμένο περιβάλλον» (sandbox) που χρησιμοποιείται κατά την εκτέλεση των προγραμμάτων Java. Δεν ελέγχεται ο κώδικας του εκτελέσιμου αρχείου καθ' αυτός, ωστόσο ελέγχεται η συμπεριφορά του προγράμματος καθώς εκτελείται. Έχοντας δηλαδή υπ' όψιν

ένα σύνολο από συμπεριφορές που θεωρούνται «ύποπτες - επικίνδυνες» (π.χ. κλήση του Μητρώου του συστήματος, προσπάθεια διαγραφής ή μετονομασίας αρχείων, κ.λ.π) το πρόγραμμα antivirus προσπαθεί να ανιχνεύσει και να αποτρέψει σε πραγματικό χρόνο τις παρενέργειες ενός (άγνωστου) ιού. Αν ανιχνευτεί «ύποπτη» συμπεριφορά, το πρόγραμμα εφαρμόζει την πολιτική ασφαλείας (την οποία διαμορφώνει ο χρήστης μέσα από τις επιλογές-ρυθμίσεις του προγράμματος). Για παράδειγμα, α) Το «ύποπτο» πρόγραμμα συνεχίζει την εκτέλεση του και ενημερώνεται το αρχείο συμβάντων, β) Αναστέλλεται η λειτουργία του «υπόπτου» προγράμματος, γ) Ερωτάται ο χρήστης. Η τεχνική αυτή είναι «*αντιδραστική*» (reactive) δηλαδή το πρόγραμμα antivirus προσπαθεί να εντοπίσει «ύποπτο» κώδικα αφού αυτός εκτελεστεί.

- **Επιπλέον προστασία**. Τα σύγχρονα προγράμματα antivirus ενσωματώνουν ορισμένες επιπλέον λειτουργίες προστασίας. Μεταξύ άλλων, προσφέρουν τη δυνατότητα ελέγχου αλληλογραφίας (εισερχόμενης/εξερχόμενης) για κακόβουλο λογισμικό, έλεγχο και παρεμπόδιση «υπόπτων» αρχείων που ανταλλάσσονται μέσω προγραμμάτων ανταλλαγής αρχείων P2P, φιλτράρισμα αρχείων που ανταλλάσσονται μέσω προγραμμάτων συνομιλίας (chat, ανταλλαγή μηνυμάτων – instant messaging), προστασία από κινητό κώδικα στο Web, κ.λ.π. Επιπλέον, αρκετά προγράμματα antivirus συχνά αποτελούν ολοκληρωμένα πακέτα εφαρμογών και ενσωματώνουν λειτουργίες firewall, ανίχνευσης εισβολών (IDS), καθώς και προστασίας από (μη μολυσματικό) λογισμικό τύπου spyware-adware.

Τα προγράμματα antivirus *δεν είναι πανάκεια.* Απλώς αποτελούν ένα ακόμη εργαλείο πρόληψης για την αντιμετώπιση κακόβουλου λογισμικού. Οι καινούριοι (και ευφυείς) ιοί θα είναι πάντα απρόβλεπτοι και θα παρακάμπτουν την προστασία που προσφέρει ένα πρόγραμμα antivirus. Επίσης, οι επιθέσεις υπερχείλισης καταχωρητών, η εκτέλεση κινητού κώδικα καθώς και οι δικτυακές επιθέσεις, αποτελούν κινδύνους τους οποίους τα προγράμματα antivirus δεν έχουν σχεδιαστεί –βελτιστοποιηθεί για να αντιμετωπίζουν. Επίσης, ένα antivirus δεν έχει τη δυνατότητα να φιλτράρει εισερχόμενη / εξερχόμενη κίνηση με βάση τα περιεχόμενα των επικεφαλίδων στα επίπεδα μεταφοράς και δικτύου, κάτι που είναι αρμοδιότητα άλλων εφαρμογών ασφάλειας (π.χ. firewalls). Για αυτούς τους λόγους η επιλογή του κατάλληλου

προγράμματος antivirus θα πρέπει να συνδυαστεί και με άλλα εργαλεία πρόληψης-αντιμετώπισης κινδύνων όπως firewalls, εργαλεία Ανίχνευσης Εισβολών (IDS), προγράμματα ανίχνευσης Spyware-Adware, εργαλεία ανίχνευσης ευπαθειών, μηχανισμοί backup κ.λ.π.

4.2 Συστήματα FIREWALL (" Τείχος Προστασίας")

Τα συστήματα firewall προστατεύουν τους πληροφοριακούς πόρους ενός Η/Υ ή ενός δικτύου Η/Υ από επιθέσεις μη εξουσιοδοτημένης πρόσβασης. Αποτελούν έναν μηχανισμό *ελέγχου πρόσβασης*, βάσει μιας πολιτικής ασφάλειας που δίνει κυρίως έμφαση στην προστασία του εσωτερικού περιβάλλοντος από επιθέσεις που προέρχονται από το εξωτερικό περιβάλλον. Λέγοντας εξωτερικό περιβάλλον εννοούμε άλλους Η/Υ ή/και άλλα δίκτυα. Στην ενότητα αυτή δίνουμε έμφαση στα προσωπικά firewall, δηλαδή σε εφαρμογές λογισμικού για την προστασία του Η/Υ από μη ανεπιθύμητες εισβολές. Τα προσωπικά firewalls λειτουργούν σε όλα τα επίπεδα του μοντέλου TCP/IP, λειτουργούν δηλαδή ως *packet filters* (φιλτράρισμα πακέτων) και ως *application gateways* (πύλες επιπέδου εφαρμογής). **Packet filter**. Σχεδόν όλα τα packet-filtering firewalls λειτουργούν ως εξής:

1. Τα κριτήρια φιλτραρίσματος αποτελούν τους κανόνες φιλτραρίσματος πακέτων (packet filter rules) και μπορούν να εφαρμοστούν τόσο στα εισερχόμενα όσο και εξερχόμενα δεδομένα.
2. Όταν ένα πακέτο αποπειραθεί να εισέλθει-εξέλθει, απομονώνονται οι επικεφαλίδες του πακέτου. Ένα packet-filter firewall εξετάζει τις επιξεφαλίδες IP, TCP, ή UDP του πακέτου :
   - Διεύθυνση IP αποστολέα, Διεύθυνση IP παραλήπτη
   - Θύρα (Port) εφαρμογής αποστολέα, Θύρα εφαρμογής παραλήπτη
   - Είδος πρωτοκόλλου (στα επίπεδα δικτύου & μεταφοράς) που δημιουργείτα πακέτα
3. Οι κανόνες φιλτραρίσματος αποθηκεύονται με αυστηρή σειρά προτεραιότητας. Κάθε κανόνας εφαρμόζεται στο πακέτο, με τη σειρά που είναι αποθηκευμένος
4. Εάν ένας κανόνας «μπλοκάρει» τη λήψη ή μετάδοση ενός πακέτου, το πακέτο απορρίπτεται.

5. Εαν ένας κανόνας επιτρέπει τη λήψη ή μετάδοση ενός πακέτου, το πακέτο γίνεται δεκτό.
6. Εαν ένα πακέτο δεν ικανοποιεί κανέναν κανόνα, τότε εφαρμόζεται μία εκ των ακόλουθων δύο πολιτικών :

- Ανοικτές: *επίτρεψε ό,τι δεν απαγορεύεται ρητά*
- Κλειστές: *απαγόρεψε ότι δεν επιτρέπεται ρητά*

Εναλλακτικά, το firewall ρωτάει το χρήστη για την ενέργεια στην οποία θα προβεί. Πρόκειται για μια διαδεδομένη τακτική στα προσωπικά firewalls, κάτι που σημαίνει πως, τουλάχιστον στην αρχή, ο χρήστης θα πρέπει να «εκπαιδεύσει» το firewall. Το firewall στη συνέχεια μπορεί να «απομνημονεύει» τις επιλογές του χρήστη και να εφαρμόζει την εκάστοτε πολιτική πρόσβασης. Επιπλέον, τα προσωπικά firewalls μπορούν να λάβουν αποφάσεις ανάλογα με το εάν τα δεδομένα που εισέρχονται (εξέρχονται), προέρχονται (προορίζονται) από (για) έναν Η/Υ του τοπικού δικτύου ή του εξωτερικού δικτύου (Internet). **Application Gateways**. Τα firewalls επιπέδου εφαρμογής ή application gateways προγραμματίζονται ώστε να «αντιλαμβάνονται» την κίνηση στο επίπεδο εφαρμογής του TCP/IP. Έτσι, παρέχουν ελέγχους προσπέλασης σε επίπεδο χρήστη (προγραμμάτα και υπηρεσίες που εκτελούνται) καθώς και σε πρωτόκολλα και υπηρεσίες επιπέδου εφαρμογής (π.χ. HTTP, DNS, SMTP, κ.λ.π). Ο ρόλος ενός application gateway διαφοροποιείται αισθητά όταν εφαρμόζεται σε ένα δίκτυο Η/Υ. Σε επίπεδο χρήστη, πολλά από τα προσωπικά firewall προσφέρουν δυνατότητες όπως:

- Φιλτράρισμα με βάση την ταυτότητα της εφαρμογής (ή του service) που λαμβάνει ή δέχεται δεδομένα
- Φιλτράρισμα με βάση το αν η εφαρμογή που επιχειρεί πρόσβαση έχει κληθεί από μια άλλη εφαρμογή (μια συνήθης πρακτική είναι ένα κακόβουλο λογισμικό να προσπαθεί να μεταμφιεστεί ως μια άλλη «νόμιμη» εφαρμογή προκειμένου να αποκτήσει πρόσβαση από και προς το σύστημα)
- Φιλτράρισμα με βάση το αν η εφαρμογή που ζητεί πρόσβαση έχει τροποποιηθεί από την τελευταία φορά που είχε πρόσβαση (μια λειτουργία παρόμοια με τον έλεγχο ακεραιότητας που εφαρμόζουν πολλά προγράμματα antivirus).

Τέλος, ένα προσωπικό firewall μπορεί να ενσωματώνει επιπλέον λειτουργίες που «ξεφεύγουν» από τις «παραδοσιακές» αρμοδιότητες λειτουργίας ενός δικτυακού firewall. Για παράδειγμα, μπορεί να ενσωματώνει ελέγχους ασφαλούς πλοήγησης στο web (π.χ. φιλτράρισμα αρχείων cookies, ανεπιθύμητων παραθύρων pop-up, προστασία από κινητό κώδικα που βρίσκεται στον κώδικα ιστοσελίδων που επισκέπτεται ο χρήστης, καθώς και λειτουργίες Ανίχνευσης Εισβολών – IDS). **Εποπτεία Κατάστασης Πακέτων - Στατικά και Δυναμικά Φίλτρα**. Ένα στατικό φίλτρο εξετάζει κάθε πακέτο που εισέρχεται-εξέρχεται και παίρνει απόφαση φιλτραρίσματος βάσει της επικεφαλίδας του πακέτου (packet header)- (π.χ. διεύθυνση πηγής και προορισμού, αριθμός πρωτόκολλων (protocol numbers) και αριθμός θυρών (port numbers). Ένα δυναμικό φίλτρο είναι πιο εξελιγμένο καθώς μπορεί να λάβει αποφάσεις φιλτραρίσματος γνωρίζοντας εαν το πακέτο είναι αναμενόμενο, με βάση την *ύπαρξη προηγούμενης επικοινωνίας*. Το φίλτρο δηλαδή απομνημονεύει την κατάσταση των πακέτων που ανταλλάσσονται (stateful packet inspection). Έτσι, π.χ. δεν επιτρέπονται πακέτα τα οποία περιέχουν ένα διαφορετικό αριθμό SYN (Sequence Number, σε μια σύνδεση TCP) από αυτόν που αναμενόταν.

4.3 Συστήματα Ανίχνευσης Εισβολών (Intrusion Detection Systems)

Εφόσον αποτύχουν οι υπηρεσίες πρόληψης, η ασφάλεια ενός συστήματος πρέπει να βασιστεί στις υπηρεσίες ανίχνευσης. Οι υπηρεσίες αυτές θεωρούνται απαραίτητες, με δεδομένο ότι ένα σύστημα δεν μπορεί να είναι ποτέ 100% ασφαλές. Καθημερινά εμφανίζονται καινούριες ευπάθειες λογισμικού ή/και (πιο σπάνια) υλικού (hardware), ενώ συχνά απρόβλεπτες επιθέσεις από εσωτερικούς χρήστες (insiders) μπορούν να καταλύσουν την ασφάλεια ενός συστήματος. Στην πιο απλή του μορφή, ένα σύστημα IDS αναλύει τα *αρχεία καταγραφής και ελέγχου* (logging and audit) του συστήματος και προσπαθεί να εντοπίσει «ίχνη» από γνωστές επιθέσεις (εισβολής). Ένα **«προσωπικό» (host-based)** λογισμικό IDS ανιχνεύει «ύποπτες» δραστηριότητες που αφορούν τον Η/Υ που προστατεύει (π.χ. εγγραφές στο Μητρώο, απόπειρες εισόδου (επιτυχημένες ή αποτυχημένες), port scans, δυσλειτουργία ή τροποποίηση προγραμμάτων, απόπειρες DOS), ενώ ένα **δικτυακό (NIDS)** λογισμικό IDS, συνήθως συνεργάζεται με ένα σύστημα firewall ή εγκαθίσταται σε καίρια σημεία εντός του

δικτύου της επιχείρησης και ανιχνεύει την κίνηση του δικτύου για γνωστές ανωμαλίες (port scans, συγχρονισμένες επιθέσεις DOS κ.λ.π). Τα συστήματα IDS κατηγοριοποιούνται ως εξής:

1. **Ανίχνευση επιθέσεων** (**Misuse Detection).** Κατά την ανίχνευση επιθέσεων, το IDS αναλύει την πληροφορία που έχει συγκεντρώσει (από τα αρχεία καταγραφής) και συγκρίνει τα αποτελέσματα της ανάλυσης με ήδη γνωστές επιθέσεις, οι «υπογραφές» των οποίων είναι αποθηκευμένες σε μια βάση δεδομένων. Η λειτουργία ενός IDS αυτού του τύπου μπορεί να παρομοιαστεί με τη λειτουργία ανίχνευσης «υπογραφών» ενός προγράμματος antivirus. Αυτό σημαίνει πως ένα τέτοιο σύστημα δεν μπορεί να ανιχνεύσει επιθέσεις που δεν είναι γνωστές.

2. **Ανίχνευση Ανωμαλιών (Anomaly Detection).** Η λειτουργία των IDS αυτού του τύπου μπορεί να παρομοιαστεί με την ευρετική (heuristic) λειτουργία ενός προγράμματος antivirus. Αρχικά ο διαχειριστής του συστήματος-δικτύου καθορίζει κάποιες παραμέτρους που αφορούν την ποσότητα και το είδος (π.χ. είδη και μέγεθος πακέτων, τύποι πρωτοκόλλων, αριθμοί θυρών) της κίνησης που επιτρέπεται σε ένα δίκτυο. Το IDS αναλύει την πληροφορία που έχει συγκεντρώσει (από τα αρχεία καταγραφής): Όταν οι στατιστικές της ανάλυσης παρεκκλίνουν-διαφοροποιούνται από το *σημείο ισορροπίας* (threshold) που έχει καθοριστεί, αυτό συνιστά ένδειξη *ανωμαλίας* και ενεργοποιεί το σύστημα IDS. Παραδείγματα ασυνήθιστων ενεργειών θα μπορούσαν να είναι:

- Αυξημένος Αριθμός αποτυχημένων αποπειρών εισόδου
- Αυξημένος αριθμός συνδέσεων ενός χρήστη στο σύστημα
- Αυξημένη κατανάλωση υπολογιστικών πόρων ή ροής πακέτων προς ένα σύστημα
- Απομακρυσμένες συνδέσεις σε μη δεσμευμένους αριθμούς θυρών προορισμού.

Τα συστήματα ανίχνευσης ανωμαλιών, λόγω του «ευρετικού» (heuristic) χαρακτήρα τους, είναι δυνατόν να προβαίνουν σε λάθος διαγνώσεις. Το ποσοστό των *εσφαλμένων θετικών* (false positives) ή των *εσφαλμένων αρνητικών* (false negatives) εξαρτάται από τις ρυθμίσεις στις οποίες προβαίνει ο διαχειριστής του συστήματος (π.χ. περισσότερη ευαισθησία = υψηλότερο ποσοστό εσφαλμένων θετικών). **Παθητικά και Ενεργητικά IDS.** Ένα παθητικό (passive) IDS, έχει κυρίως ενημερωτικό χαρακτήρα, δηλαδή «ανιχνεύει» και καταγράφει μια επίθεση ή μια «ύποπτη» ενέργεια χωρίς να την αποτρέπει ή να την αντιμετωπίζει. Το IDS μπορεί να

ενεργοποιήσει έναν συναγερμό (π.χ. αποστολή e-mail για ενημέρωση του διαχειριστή) ωστόσο δεν προβαίνει σε άλλες ενέργειες. Στην παθητική τους μορφή, τα συστήματα IDS μπορούν να παρομοιαστούν με συστήματα φυσικής ασφάλειας όπως π.χ. συστήματα παρακολούθησης και συναγερμού (alarm & monitoring systems) για την παρακολούθηση και ανίχνευση «ύποπτης» δραστηριότητας σε έναν φυσικό χώρο. Ένα ενεργητικό (reactive) σύστημα IDS μπορεί να έχει ενσωματωμένες και λειτουργίες αντιμετώπισης επιθέσεων ή/και ανωμαλιών. Για παράδειγμα, μπορεί να ενεργοποιήσει την υπηρεσία φιλτραρίσματος του firewall (με το οποίο ενδεχομένως συνεργάζεται) ώστε να εμποδιστεί η (περαιτέρω) είσοδος «ύποπτων» πακέτων στο σύστημα. Σε αυτήν την περίπτωση το λογισμικό IDS αποκαλείται και ως *Σύστημα Αποτροπής Εισβολών* (Intrusion Prevention System / IPS).

4.3 Αντίγραφα Ασφαλείας (Backup)

Η λήψη Αντιγράφων Ασφαλείας αφορά τη διαδικασία της δημιουργίας και της ασφαλούς αποθήκευσης αντιγράφων ενός ή περισσότερων πληροφοριακών πόρων του συστήματος (π.χ. δεδομένα, προγράμματα, βάσεις δεδομένων), καθώς και της ασφαλούς επαναφοράς τους σε περίπτωση επίθεσης ή λάθους. Το αποθηκευμένο αντίγραφο ονομάζεται *αντίγραφο ασφάλειας* ή εφεδρείας (backup data). Εάν οι αρχικοί (original) πόροι χαθούν ή καταστραφούν ή αλλοιωθούν, τότε επαναφέρονται τα αντίγραφα που έχουν ληφθεί. Σε επίπεδο Η/Υ, η ανάγκη για τη λήψη αντιγράφων ασφάλειας σχετίζεται με:

- Την επαναφορά ενός αντιγράφου ολόκληρου του συστήματος (Λ.Σ., δεδομένα και προγράμματα) εφόσον το σύστημα δυσλειτουργεί ή καταστραφεί, π.χ. απώλεια ή κλοπή σκληρού δίσκου, αλλοίωση αρχείων συστήματος, κακόβουλο λογισμικό με καταστρεπτικές παρενέργειες, εισβολή (hacking) και καταστροφή αρχείων, δεδομένων, ή εφαρμογών (cracking).
- Την επαναφορά συγκεκριμένων αρχείων και δεδομένων, εφόσον αυτά καταστράφηκαν, αλλοιώθηκαν, εκλάπησαν, ή δεν είναι διαθέσιμα για οποιοδήποτε άλλο λόγο (π.χ. διαγραφή δεδομένων από λάθος του χρήστη).

Ένα αντίγραφο ασφάλειας συνήθως αποθηκεύεται σε μαγνητικά μέσα (π.χ. σκληροί δίσκοι, μαγνητικές ταινίες) ή οπτικά μέσα (π.χ. CD-R, DVD-R, κ.λ.π). Η αύξηση των ρυθμών διαμεταγωγής δεδομένων στα τοπικά δίκτυα και στις

ευρυζωνικές συνδέσεις έχει επίσης καταστήσει δυνατή την *απομακρυσμένη λήψη* αντιγράφων ασφάλειας (remote backup). **Λογισμικό Αντιγράφων Ασφάλειας (backup software).** Το λογισμικό εφαρμογών που χρησιμοποιείται για τη λήψη αντιγράφων ασφάλειας. **Πολιτική Λήψης Αντιγράφων Ασφαλείας (backup policy)**. Η Πολιτική Ασφάλειας ενός οργανισμού/επιχείρησης πρέπει να ορίζει ρητώς τους κανόνες και τις διαδικασίες για το είδος των πόρων που απαιτούν λήψη αντίγραφου ασφάλειας, το είδος και την ποσότητα των αντιγράφων ασφάλειας που θα ληφθούν, καθώς και το χρόνο κατά τον οποίο πρέπει να γίνεται η λήψη τους. Η πολιτική περιλαμβάνει επίσης και τις διαδικασίες και τους κανόνες που καθορίζουν την επαναφορά των αρχικών δεδομένων από τα αντίγραφα ασφάλειας.

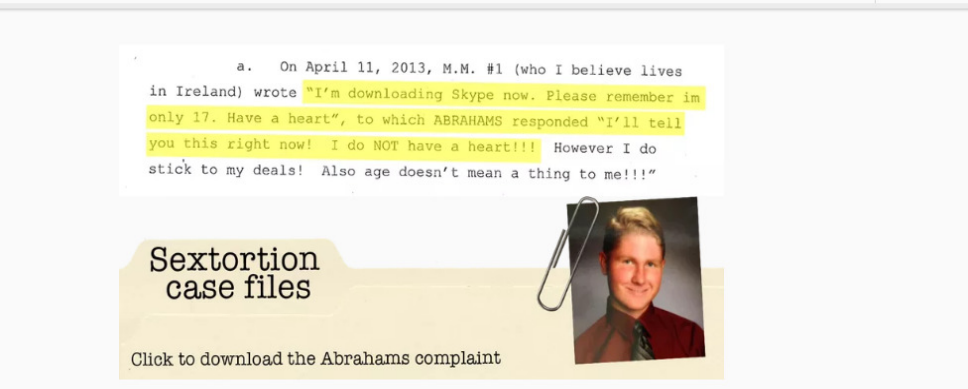
ΚΕΦΑΛΑΙΟ 5ο : ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΕΩΝ (CASE STUDIES) ΚΑΙ ΚΟΙΝΩΝΙΚΗ ΔΙΚΤΥΩΣΗ ΜΕΣΩ ΠΑΙΧΝΙΔΟΜΗΧΑΝΩΝ (SOCIAL GAMING PLATFORMS)

5.1 Case Study 1

Jared James Abrahams

Ο Jared James Abrahams, φοιτητής της Επιστήμης Υπολογιστών συνελήφθη το 2013 για τον εκβιασμό Cassidy Wolf, νικήτριας εκείνου του έτους των καλλιστείων Miss Teen USA.Ο Abrahams και η Wolf πήγαιναν μαζί στο γυμνάσιο Temecula, Καλιφόρνια. Οι πρώτες υποψίες της Wolf ξεκίνησαν όταν έλαβε ειδοποιήσεις από διάφορες παλτφόρμες κοινωνικών δικτύων ότι κάποιος προσπαθούσε να αλλαξει τους κωδικούς πρόσβασης της. Τριάντα λεπτά αργότερα, ο Abrahams της έστειλε email απαιτώντας να του στείλει γυμνές φωτογραφίες στο Snapchat ή να συνομιλήσουν στο Skype κάνοντας ο,τι της ζητήσει για 5 λεπτά. Διαφορετικά, την απείλησε ότι θα ανεβάσει γυμνές φωτογραφίες της στους λογαριασμούς κοινωνικών δικτύων της. Η Wolf δεν αναγνωρίζε τις φωτογραφίες, οι οποίες φαίνεται να έχουν ληφθεί από την κάμερα της. Οι έρευνες αργότερα έδειξαν ότι ο Abrahams είχε εκβιάσει με τον ίδιο

τρόπο 12 νεαρές κοπέλες από διάφορες χώρες του κόσμου (Ιρλανδία , Καναδάς, Μολδαβία κ.α) και είχε τον έλεγχο των συσκευών (υπολογιστών και άλλων φορητών συσκευών) παραπάνω από 100 νεαρών γυναικών. Είχε εγκαταστήσει λογισμικό Keylogger στους υπολογιστές των θυμάτων του , υποκλέπτοντας τους κωδικούς τους στα μέσα κοινωνικής δικτύωσης. Επίσης είχε εγκαταστήσει τα Malware προγράμματα Blackshades και DarkComet που του επέτρεπαν να ελέγχει τις ψηφιακές κάμερες των θυμάτων και να βγάζει φωτογραφίες εν αγνοία τους. Ερχόταν σε επαφή με τα θύματα χρησιμοποιώντας διαφορετικούς λογαριασμούς ηλεκτρονικού ταχυδρομείου που είχε υποκλέψει.

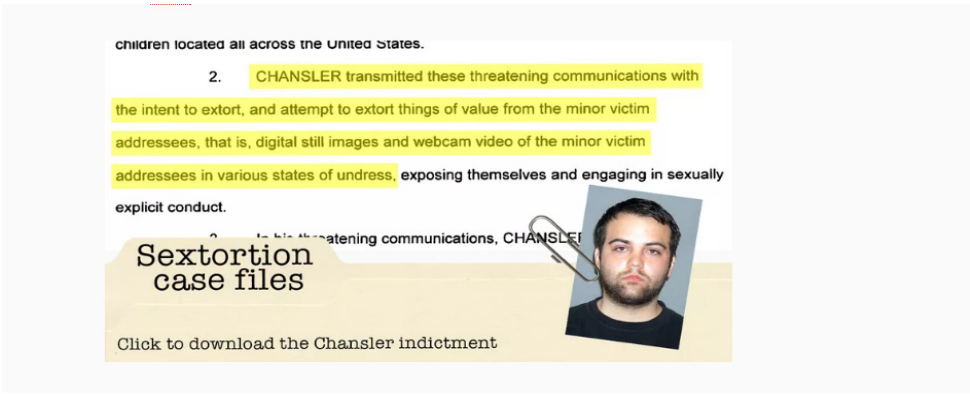


Ένα από τα θύματα του έγραψε : "Σε παρακαλώ θυμήσου είμαι μόνο 17. Δεν έχεις καρδιά? " και της απάντησε : " Στο λέω να το ξέρεις . Όχι δεν έχω καρδιά! Η ηλικία σου δεν παίζει κανένα ρόλο για μένα! " . Προκειμένου να κρύψει την IP διεύθυνση του χρησιμοποιούσε ένα VPN (Virtual Private Network) μαζί με μια DNS υπηρεσία που διατίθεται στην ιστοσελίδα NO-IP.com. Με αλαζονεία δημοσίευε σε forum hackers ότι είχε «μολύνει» τον υπολογιστή «μιας μικρής που τυγχάνει να είναι μοντέλο». Ο Abrahams συνελήφθηκε και κατηγορήθηκε για ένα πλήθος ψηφιακών υποκλοπών συμπεριλαμβανομένων και τριων περιπτώσεων σεξουαλικού εκβιασμού. Καταδικάστηκε σε δεκαοχτώ μήνες φυλάκισης.

5.2 Case Study 2

Lucas Michael Chansler

Από το 2007 έως το 2010 ο Lucas Michael Chansler στοχοποίησε περίπου 350 νεαρά κορίτσια με αποτέλεσμα μετά την καταδίκη του το FBI εξαπέλυσε μια ολόκληρη δικτυακή καμπάνια προκειμένου να ανακαλύψει και άλλα θύματά του που ενδεχομένως φοβόντουσαν να τον καταγγείλουν. Κρύβοντας την IP διεύθυνση του μέσω proxy servers , «ψάρευε» τα θύματα του μέσα στις πλατφόρμες κοινωνικών δικτύων. Προσποιούμενος έναν συνηθισμένο έφηβο , έψαχνε για θύματα αναζητώντας «φιλία και φλέρτ». Ο Chansler ζητούσε από τα θύματα του να κάνουν video chat και χρησιμοποιούσε ένα video με ένα γυμνό αγόρι ώστε να κρύψει την ταυτότητά του , ενώ συγχρόνως κατέγραφε μυστικά το θύμα.

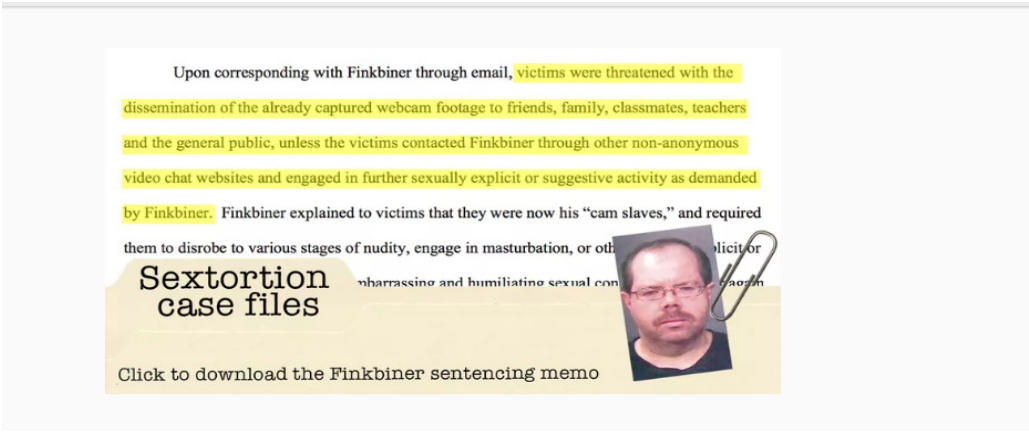


Μόλις αποκτούσε το υλικό , το χρησιμοποιούσε για να εκβιάζει τα θύματα του ζητώντας περισσότερα video και φωτογραφίες απειλώντας ότι σε διαφορετική περίπτωση θα δημοσίευε το υλικό σε φίλους και συγγενείς του θύματος. Μία νεαρή κοπέλα που έπεσε θύμα του Chansler περιέγραψε σε πράκτορες του FBI την απόγνωση και την κατάθλιψη που βίωσε με τα λόγια : "Ένιωθα σαν σκλάβα… Καθόμουν μόνη μου στο κρεβάτι σε απόλυτη ησυχία και σκεφτόμουνα ότι ο Θεός με είχε εγκαταλείψει και δεν ήξερα τι να κάνω". Στην ανάκριση που ακολούθησε τη σύλληψή του ο Chansler εξήγησε στους αστυνομικούς ότι διάλεγε ως θύματα του νεαρά ανήλικα κορίτσια γιατί ήταν πιο πιθανό να υποκύψουν στον εκβιασμό του. Κατηγορήθηκε για 4 περιπτώσεις σεξουαλικού εκβιασμού , 14 περιπτώσεις παραγωγής παιδικής πορνογραφίας και καταδικάστηκε σε 105 χρόνια φυλάκισης στις Ομοσπονδιακές Φυλακές.

5.3 Case Study 3

Richard Finkbiner

Όταν το 2012 οι πράκτορες του FBI εισέβαλαν στο εξοχικό του Richard Finkbiner ανακάλυψαν περισσότερα από 22000 αρχεία video αποθηκευμένα στον υπολογιστή του τα μισά εκ των οποίων ήταν πορνογραφικά στα οποία εμφανίζονταν ανήλικα άτομα. Κατά την ανάκριση του ο ίδιος ισχυρίστηκε ότι αδυνατούσε να αναγνωρίσει τα πρόσωπα θυμάτων του επειδή ακριβώς ήταν πολύ μεγάλος ο αριθμός τους. Ο Finkbiner προσέγγιζε τα υποψήφια θύματά του (συνήθως αγόρια στην εφηβεία τους) μέσω του Omegle ή άλλων ανώνυμων chatting προγραμμάτων. Τους ζητούσε να βγάλουν τα ρούχα τους και να προβούν σε σεξουαλικές πράξεις προσποιούμενος τον συνομήλικο τους και κρύβοντας την ταυτότητα του με ψεύτικα video , ενώ παράλληλα τα βιντεοσκοπούσε. Μετά απειλούσε τα θύματα ότι θα ανεβάσει τα video σε πορνογραφικά sites αν δε μετατρέπονταν σε "cam slaves" όπως ο ίδιος τα ονόμαζε. Πιστεύεται ότι σε τουλάχιστον τρεις περιπτώσεις χρησιμοποίησε λογισμικό επεξεργασίας εικόνων ώστε να πείσει το θύμα ότι πραγματοποίησε την απειλή του.



Ένα 17χρόνο κορίτσι του έγραψε ότι αποπειράθηκε να αυτοκτονήσει το προηγούμενο βράδυ και ότι θα το επιχειρούσε παλι αν δεν σταματούσε να την εκβιάζει και ο Finkbiner του απάντησε : " Χαίρομαι που σου φάνηκα χρήσιμος". Σε παρόμοια περίπτωση όταν ένα αγόρι του διαμαρτυρήθηκε για τον εκβιασμό εκείνος απάντησε : "Το ξέρω ότι είναι παράνομο και δεν έχω κανένα πρόβλημα με αυτό...δεν πρόκειται να με πιάσουν γιατί είμαι hacker και έχω καλύψει τα ίχνη μου". Στην δίκη του

Finkbiner ο Δημόσιος Κατήγορος δήλωσε ότι : “ (ο Finkbiner) …έχει εκβιάσει εκατοντάδες αν όχι χιλιάδες άτομα , ανήλικα και ενήλικα από όλο τον κόσμο”. Του απαγγέλθηκαν κατηγορίες για 6 περιπτώσεις παραγωγής παιδικής πορνογραφίας , 20 περιπτώσεις εκβιασμού , 8 περιπτώσεις απόπειρας εκβιασμού, 2 περιπτώσεις κατοχής πορνογραφικού υλικού παιδοφιλίας και 7 περιπτώσεις ενοχλητικής παρακολούθησης ανηλίκου. Κρίθηκε ένοχος για όλες τις κατηγορίες παρακολούθησης ανηλίκου , για 2 κατηγορίες παραγωγής παιδικής πορνογραφίας και για 15 κατηγορίες εκβιασμού και καταδικάστηκε σε 40 χρόνια φυλάκισης.

5.4 Case Study 4

“Rinat”

Το 2013 ένας 30χρονος άντρας καταδικάστηκε στο Ισραήλ για εκβιασμό , σεξουαλική παρενόχληση και δημοσιοποίηση άσεμνου πορνογραφικού υλικού. Ο άντρας αυτός εμφανιζόταν σε διάφορες πλατφόρμες κοινωνικής δικτύωσης με ψεύτικη ταυτότητα προσποιούμενος την γυναίκα (με το όνομα Rinat) , και μάλιστα ως μέλος του Ισραηλινού στρατού. (σημ. Στο Ισραήλ η στρατιωτική θητεία είναι υποχρεωτική και για τις γυναίκες). Με την ψεύτικη αυτή ταυτότητα ξεγελούσε νεαρά κορίτσια και ερχόταν σε επικοινωνία μαζί τους. Με δόλιους τρόπους και ύπο πίεση , αφού κέρδισε αρχικά την εμπιστοσύνη τους , εκβίασε τουλάχιστον 3 ανήλικα κορίτσια ζητώντας τους γυμνές φωτογραφίες και άλλο πορνογραφικό υλικό. Σε μία περίπτωση ο θύτης βιντεοσκόπησε χωρίς τη άδεια του θύματος, ένα 13χρονο κορίτσι ,μέσω Skype , αφού πρώτα το πίεσε φορτικά να προβεί σε σεξουαλική πράξη. Σε παρόμοια περίπτωση πάλι με ανήλικο κορίτσι , ο θύτης ,πίεσε το θύμα να προβεί σε σεξουαλική μέσω Skype. Όταν το θύμα του είπε ότι ήταν η μητέρα της στο δωμάτιο αυτός την εξανάγκασε να προσποιηθεί ότι άλλαζε ρούχα μπροστά στην κάμερα , ώστε να μην τραβήξει την προσοχή της μητέρας και να του επιτρέψει να την δει γυμνή. Το Ανώτατο Δικαστήριο του Ισραήλ αρνήθηκε την έφεση του θύτη ενάντια στην καταδίκη του σε δύο χρόνια φυλάκιση δηλώνοντας ότι : “… η έλλειψη σωματικής επαφής δεν αναιρεί την σοβαρότητα του αδικήματος” και κατέληξε στην απορριπτική του απόφαση με την φράση : “ η σκέψη και μόνο ότι τα παιδιά δεν είναι

ασφαλή ούτε στο ίδιο τους το σπίτι είναι άκρως ανησυχητική. Εκεί στο ίδιο τους το δωμάτιο , στο ίδιο τους το σπίτι , κάτω από το βλέμα των ίδιων των γονέων τους , ο θύτης κατάφερε να ξεγελάσει τα θύματα , να τα παγιδεύσει και να τους προκαλέσει ανείπωτη ψυχική και συναισθηματική βλάβη."

5.5 Κοινωνική Δικτύωση μέσω Παιχνιδομηχανών

Η χρήση διαδικτυακών παιχνιδιών είναι πολύ διαδεδομένη τα τελευταία χρόνια κυρίως στις νεανικές ηλικίες. Οι δυνατότητες που προσφέρουν οι σύγχρονες κονσόλες παιχνιδιών (παιχνιδομηχανές) , όπως για παράδειγμα η δυνατότητα για multigaming , αλλά και η δυνατότητα για αποστολή και λήψη μηνυμάτων μεταξύ των χρηστών, τις έχει καταστήσει ένα ακόμα πεδίο κοινωνικής δικτύωσης. Πλέον τα νεαρά άτομα που χρησιμοποιούν αυτές τις μηχανές μπορούν να ανταλλάξουν μηνύματα με φίλους τους ή και με αγνώστους ενώ παίζουν. Παράλληλα έχουν δημιουργηθεί και ειδικά chat rooms και forums που έχουν ως θέμα τα δικτυακά παιχνίδια και προσελκύουν μεγάλο τμήμα νεαρής ηλικίας χρηστών όπως π.χ το Reddit. Στο τμήμα αυτό θα κάνουμε μια συνοπτική παρουσίαση των δημοφιλέστερων παιχνιδομηχανών καθώς και στις επιλογές άμεσης επικοινωνίας που διαθέτουν.

5.5.1 Steam

Μία από τις δημοφιλέστερες πλατφόρμες παιχνιδιών η οποία προσφέρεται και για PC αλλά και για MAC Apple μηχανές είναι η Steam. Μέσω της πλατφόρμας μπορεί ο χρήστης να βρει ένα μεγάλο πλήθος παιχνιδιών τα οποία μπορεί να αγοράσει. Αρκεί να εγκατασταθεί στο desktop ή το laptop και επιτρέπει στο χρήστη να επιλέξει από μια γκάμα χιλιάδων παιχνιδιών αλλά και πολλών επιλογών άμεσης επικοινωνίας. Συγκεκριμένα η πλατφόρμα περιέχει πολλά forums όπου οι χρήστες μπορούν να ανταλλάσουν μηνύματα και να προσκαλούν άλλους χρήστες να γίνουν "φίλοι" ώστε να παίξουν είτε ως συμπαίκτες είτε ως αντίπαλοι κάποιο παιχνίδι. Τα forums εποπτεύονται από διαχειριστές της Steam. Για λόγους ασφαλείας υπάρχει ένα

κατώτερο όριο ηλικίας για τη χρήση της πλατφόρμας , τα 13 χρόνια. Επίσης υπάρχουν και ρυθμίσεις ασφαλείας που δίνουν τη δυνατότητα του αποκλεισμού οποιουδήποτε μηνύματος είτε να επιτρέπουν μηνύματα μόνο από εγκεκριμένους "φίλους".

5.5.2 Xbox Live

Η αντίστοιχη πλατφόρμα παιχνιδιών της Microsoft είναι το Xbox Live. Όταν ο χρήστης εγγραφεί στην υπηρεσία έχει τη δυνατότητα να συνομιλήσουν σε chat rooms με άλλους χρήστες καθώς και να τους προσθέσει ως "φίλους". Τα Party Chat rooms όπως ονομάζονται μπορούν να δημιουργηθούν πριν ή και κατά τη διάρκεια του παιχνιδιού ενώ παρέχεται και υπηρεσία φωνητικής επικοινωνίας μεταξύ των παικτών παράλληλα με τα γραπτά μηνύματα. Ωστόσο υπάρχουν κάποιες δικλείδες ασφαλείας που εξαρτώνται από την ηλικία του χρήστη. Όταν εγκατασταθεί για πρώτη φορά η πλατφόρμα ο χρήστης καλείται να δημιουργήσει έναν προσωπικό λογαριασμό , η ηλικία του χρήστη επί παραδείγματι αν είναι μικρότερη από 13 κλειδώνει αυτόματα την δυνατότητα να δέχεται αιτήματα φιλίας από αγνώστους.

5.5.3 Playstation Network

Όλα τα συστήματα PlayStation μπορούν να ρυθμιστούν ώστε να έχουν τον έλεγχο του λογαριασμού οι γονείς ή κηδεμόνες. Όπως και με τις κονσόλες Xbox, το προφίλ ενός παιδιού θα περιορίσει αυτόματα συγκεκριμένες ενέργειες, ανάλογα με την ημερομηνία γέννησης του χρήστη. Δίνετε η επιλογή του αποκλεισμού του chat και των μηνυμάτων αλλάζοντας τις ρυθμίσεις απορρήτου του PS4, PS3 ή PlayStation Vita. Αυτό σημαίνει ότι το voice chat, η συνομιλία κειμένου και μηνυμάτων μπορούν όλα να απενεργοποιηθούν σε έναν χρήστη με βάση τις επιλογές ασφαλείας του κηδεμόνα. Μπορείτε επίσης να αποτρέψετε τη χρήση του προγράμματος περιήγησης στο διαδίκτυο PS4.

5.5 .4 Nintendo Network

Οι κονσόλες παιχνιδιών της Nintendo φημίζονται για τους αυστηρούς κανόνες ασφαλείας που τηρούν σε σχέση με τον γονικό έλεγχο. Για παράδειγμα η υπηρεσία Miiverse όπου οι χρήστες μπορούν να μοιραστούν εικόνες που έχουν ζωγραφίσει οι ίδιοι και άμεσα μηνύματα. Ο έλεγχος από τους διαχειριστές είναι συνεχής και αυστηρός ενώ παρέχεται και η δυνατότητα στους γονείς και κηδεμόνες να απενεργοποιήσουν οποιαδήποτε διαδραστικότητα με άλλους χρήστες.

5.2 Μέτρα πρόληψης και ασφάλειας σε Παιχνιδομηχανές.

Μία από τις μεγαλύτερες ανησυχίες για τους γονείς δεν είναι η αλληλεπίδραση που έχουν οι παίκτες με εγκεκριμένους φίλους τους, αλλά η αλληλεπίδραση με αγνώστους χρήστες σε multiplayer, online παιχνίδια. Πολλά online παιχνίδια έχουν επιλογές για πολλούς παίκτες που δίνουν την δυνατότητα για άμεση επικοινωνία είτε φωνητική με ακουστικά είτε μέσω γραπτών μηνυμάτων. Αυτό μπορεί να είναι ιδιαίτερα ανησυχητικό για τους γονείς, καθώς είναι δύσκολο να παρακολουθούν τι λένε οι παίκτες, ο ένας στον άλλο. Επίσης, η αλληλεπίδραση συχνά δεν περιορίζονται σε χρήστες από την λίστα φίλων, αλλά επεκτείνεται και σε αγνώστους καθώς ένας παίκτης μπορεί να ζητήσει από το παιδί να προσθέσει ως φίλο, κατά τη διάρκεια ενός παιχνιδιού, κάποιον άγνωστο. Για τους λόγους αυτούς θα πρέπει οι γονείς ή οι κηδεμόνες των ανήλικων χρηστών παιχνιδομηχανών να :

- Είναι ρυθμισμένες οι επιλογές ασφαλείας
- Αποτρέπουν τους ανήλικους χρήστες να μοιράζονται προσωπικά δεδομένα
- Ελεγχουν τον τύπο των παιχνιδιών που αρμόζουν στην ηλικία του χρήστη
- Προειδοποιούν τους ανήλικους χρήστες για τους ενδεχόμενους κινδύνους

Βιβλιογραφία

Έντυπη Βιβλιογραφία

[1] Adams, J., 1998, The next world war, Simon and Schuster

[2[Bigelow R. (1985). The challenges of computer law. Western New England Law Review 7(3)

[3] BloomBecker, B., 1990, Spectacular Computer Crimes, Dow Jones – Irwin

[4] Ransom, A. W., 1994, Who Owns Information, Basic Books

[5] Cavoukian, A., Tapscott, D., 1997, Who Knows, McGraw-Hill

[6] Denning, D., E., 2007, Cryptography and Data Security, Addison – Wesley

[7[Diffie, W., Landau, S., 1998, Beyond Calculation, The MIT Press

[8] Edwards O.(1995). Hackersfromhell. Forbes

[9[GlickL, (1995). Criminology.Boston:Allyn and Bakon

[10] Hager, N., 1996, Secret Power, Craig Cotton Publishing, New Zealand, 1996

[11] Kesler, R., 1988, Spy vs. Spy, Pocket Books

[12] Libicki, G., M., 1995, What information is warfare?, National Defense University of USA

[13] Ludlow, P., 1996, High Noon on the Electric Frontier, The MIT Press

[14] McCarthy, L., 1997, Intranet Security, Prentice Hall

[15] Meinel, C., P., 1998, The Happy Hacker, American Eagle Publications

[16] Pfleeger, C., P., 1997, Security in Computing, Prentice Hall

[17] Mitrou, L., (2008), Cybercrime and computer crime: Lecture Notes in Postgraduate Programme Techno-economic Management & Security of Digital Systems, Department of Digital Systems, University of Piraeus.

[18] Parker, D. B. (2009). Computer Crime: Criminal Justice Resource Manual. Technical Report OJP-86-C-002, U.S. Department of Justice, National Institute of Justice, Office of Justice

[19] Rosenoer, J., 1997, CyberLaw, Springer – Verlag

[20] Schneier, B., 1996, Applied Cryptography, Prentice Hall

[21] Slade, P., 1994, Guide to Computer Viruses, Springer – Verlag

[22] Schweizer, P., 1993, Friendly Spies, The Atlantic Monthly Press

[23] Sterling, B., 1992, The Hacker Crackdown, Bantam

[24] Taylor, A., 1999, The Hackers, Routledge

[25] Thomas P. Hughes, Networks οι Power: Electrification in Western Society, 1880-1930, Baltimore: John Hopkins University Press, 1983.

[26] Volgyes M. (1980). The investigation, prosecution and prevention of computer crime: A state-of-the-art review. Computer and Law journal, 2

[27] Αλεξιάδης Στέργιος (1996). Εγχειρίδιο εγκληματολογίας Θεσσαλονίκη: Εκδόσεις Σάκκουλα

[28] Αντωνίου Δ., *(2005),* Πολυπλόκαμη η παιδική πορνογραφία, εφημερίδα «Η Καθημερινή»

[29] Αντωνίου Δ., *(2007),* Τμήματος Νομικής Πανεπιστημίου Αθηνών & Εργαστηρίου Ποινικών και Εγκληματολογικών Ερευνών, Επιμέλεια: Μπακάλη Βασιλική, Ανήλικοι και Παραβατικότητα: Πρακτικά του 1ου Φοιτητικού Συνεδρίου Εγκληματολογίας, Εκδόσεις Σάκκουλα

[30] Δήμου Γ., (2002). Η διαχείριση υποθέσεων σεξουαλικής κακοποίησης ανηλίκων,

Αθήνα

[31] Δημόπουλου Χ., (2006), *Έγκλημα της Γενετήσιας Εκμετάλλευσης Ανηλίκων,* Νομική Βιβλιοθήκη

[32] Διεθνές και Ευρωπαϊκό νομικό καθεστώς αντιμετώπισης της παιδικής πορνογραφίας σε Ιδρύματος Μαραγκοπούλου για τα Δικαιώματα του Ανθρώπου (ΙΜΔΑ), Σειρά Ομάδας Νέων, Επιστημονική εποπτεία: Κιούπης Δ., Επιμέλεια: Ιωαννίδου Α., Η παιδική πορνογραφία στο διαδίκτυο, Νομική Βιβλιοθήκη, 2007

[33] Δημόπουλου Χ., Πιτσελά Α., (2006), Κείμενα Αντεγκληματικής Πολιτικής, (Διεθνή και Ευρωπαϊκά), Τόμος Β', Δ' έκδοση, Εκδόσεις Σάκκουλα, Αθήνα

[34]Ζάννη Αν., (2006). Το διαδικτυακό έγκλημα. Αθήνα-Κομοτηνή: Εκδόσεις Αντ. Ν. Σάκκουλα

[35] Καρακώστας Ι. (2003). Δίκαιο & Internet. Νομικά ζητήματα στο Διαδίκτυο. Αθήνα : Σάκκουλα

[36] Καρανικόλα Γ., *(2005),* Παιδική πορνογραφία στο διαδίκτυο: Προβληματισμοί γύρω από τη νέα ρύθμιση του άρθρου 348Α ΠΚ, Ποιν. Δικ.

[37] Κιούπης Δ. (1999) Ποινικό δίκαιο και ίντερνετ. Αθήνα: Σάκουλας , σελ. 17-18

[38] Λάζος Γρηγόρης (2001). Πληροφορική και έγκλημα. Νομική βιβλιοθήκη

Δικτυακές Αναφορές

[1]https://www.brookings.edu/research/sextortion-cybersecurity-teenagers-and-remote-sexual-assault/

[2] https://www.internetmatters.org/hub/news-blogs/social-networking-in-gaming/

[3] https://www.fbi.gov/

[4] http://www.sch.gr/

[5]http://www.growingwireless.com/be-aware/cyberbullying/news-case-studies-on-cyberbullying

[6] http://www.blog.gr/articles/1091779/Tetarti-i-Ellada-stis-psifiakes-apeiles.html

[7] https://www.teilar.gr/dbData/ProfAnn/profann-df510a1b.pdf

[8] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2012-0353+0+DOC+XML+V0//EL

[9] https://el.wikipedia.org/wiki/

[10]http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/YOUTH/YOUTH_INTRO/YOUTH_BOOKLET.PDF