ΤΕΙ ΠΑΤΡΑΣ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ ΔΙΟΙΚΗΣΗ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

«ΜΕΛΕΤΗ ΥΠΗΡΕΣΙΩΝ ΔΙΑΧΩΡΙΣΜΟΥ ΑΝΕΠΙΘΥΜΗΤΗΣ ΑΛΛΗΛΟΓΡΑΦΙΑΣ»

ΝΤΖΟΥΡΟΠΑΝΟΥ ΝΙΚΟΛΙΤΣΑ

ΣΜΙΞΙΩΤΗΣ ΔΗΜΗΤΡΙΟΣ

ΕΙΣΗΓΗΤΗΣ: ΚΑΝΑΒΟΣ ΑΝΔΡΕΑΣ

ΠΑΤΡΑ, 2012

ΠΕΡΙΛΗΨΗ

Από τον πρώτο καιρό της εμφάνισής του, το Διαδίκτυο (Internet) είναι συνυφασμένο με ένα στόχο: την διευκόλυνση της επικοινωνίας των ανθρώπων με την χρήση των υπολογιστών.

Αν και το ηλεκτρονικό μήνυμα (e-mail) θεωρείται το μέσο που έχει αλλάξει τον τρόπο επικοινωνίας των ανθρώπων, αφού όχι μόνο τους απελευθέρωσε από το τηλέφωνο, αλλά τους έδωσε και την δυνατότητα να επικοινωνήσουν ανεξάρτητα από τις αποστάσεις και το κόστος, η εμφάνιση της «μη ζητηθείσας» - ανεπιθύμητης – ηλεκτρονικής αλληλογραφίας (spam) έχοντας κατακλύσει τις ηλεκτρονικές θυρίδες κάνει την επικοινωνία αυτή αρκετά δύσκολη.

Σήμερα, το μεγαλύτερο ποσοστό των χρηστών κατακλύζεται από αυτά τα μηνύματα, τα οποία στην ουσία «θάβουν» την ουσιώδη αλληλογραφία. Οι περισσότεροι χρήστες πιστεύουν πως εξαιτίας των μηνυμάτων spam η χρήση του internet έχει γίνει ανυπόφορη. Σύμφωνα με έρευνες που έχουν γίνει, τα 2/3 των μηνυμάτων που δέχονται οι χρήστες είναι spam και αυτό έχει σαν αποτέλεσμα να γίνεται δύσκολη η επικοινωνία αφού μηνύματα από γνωστούς, συναδέλφους χάνονται.

Στην παρούσα εργασία θα μελετήσουμε την ανεπιθύμητη αλληλογραφία και τις απειλές που υπάρχουν για την ασφάλεια των δικτύων και του ηλεκτρονικού ταχυδρομείου.

Πιο συγκεκριμένα στο πρώτο κεφάλαιο θα μελετηθεί η έννοια του διαδικτύου γενικά καθώς και της ηλεκτρονικής αλληλογραφίας.

Στο δεύτερο κεφάλαιο θα δούμε την ανεπιθύμητη αλληλογραφία ως έννοια, τα προβλήματα που πηγάζουν από αυτή καθώς και την ελληνική νομοθεσία που προστατεύει τους χρήστες από τα ανεπιθύμητα ηλεκτρονικά μηνύματα.

Στο τρίτο κεφάλαιο αναλύεται διεξοδικά η έννοια του spam που είναι συνυφασμένη με την ανεπιθύμητη ηλεκτρονική αλληλογραφία.

Στο τέταρτο κεφάλαιο θα παρατεθούν οκτώ είδη απειλών που θέτουν σε κίνδυνο τους χρήστες του ηλεκτρονικού ταχυδρομείου.

Τέλος παρατίθενται τα συμπεράσματα που προκύπτουν από την βιβλιογραφική μας ανασκόπηση και κάποιοι κανόνες που ισχύουν για την αποφυγή των κίνδυνων που απορρέουν από τα spam μηνύματα.

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΙΣΑΓΩΓΗ

Η ανάπτυξη των νέων ηλεκτρονικών υπηρεσιών του Διαδικτύου (Internet) είναι μια πραγματικότητα που κερδίζει καθημερινά μεγαλύτερο έδαφος. Οι υπηρεσίες πλοήγησης στον παγκόσμιο ιστό (web-surfing), ηλεκτρονικής αλληλογραφίας (e-mail), μεταφοράς αρχείων (ftp), ηλεκτρονικού εμπορίου (e-Commerce) και άλλες, αποκτούν ολοένα και περισσότερους χρήστες με ποσοστά που σε κάποιες χώρες ξεπερνούν το 70% του πληθυσμού (ΗΠΑ, Σουηδία κα). Στη χώρα μας, οι χρήστες του Διαδικτύου εκτιμάται ότι έχουν υπερβεί το 15% του πληθυσμού και αυξάνονται με υψηλό ρυθμό.

Οι νέες υπηρεσίες αξιοποιούνται για ποικίλους λόγους. Είναι πιθανόν να χρησιμοποιηθούν στην αρχή για παιχνίδι ή ψυχαγωγία, κι αυτό ανεξάρτητα από την ηλικία του χρήστη. Σύντομα όμως, μπορεί να διαπιστώσει κάποιος την δυνατότητα του Διαδικτύου να παρέχει πρόσβαση σε ενημέρωση, πληροφόρηση, γνώση και να αποτελέσει ένα εξελιγμένο εργαλείο που μπορεί να υποστηρίξει τις επαγγελματικές και επιχειρηματικές δραστηριότητες.

Η ηλεκτρονική αλληλογραφία είναι από τις πιο δημοφιλείς νέες υπηρεσίες που παρέχονται μέσω του Διαδικτύου. Με πολύ χαμηλό κόστος και σε ελάχιστα δευτερόλεπτα ή έστω μερικά λεπτά, μικρά ή εκτενή κείμενα, φωτογραφίες, video, ακόμα και ηχογραφημένα (ψηφιοποιημένα) μηνύματα μπορούν να φτάσουν στον παραλήπτη αυτής της νέας μορφής αλληλογραφίας, σε όποια γωνιά της γης και αν βρίσκεται.

Η αυθαίρετη ηλεκτρονική αλληλογραφία είναι απλά το σύνολο των μηνυμάτων που στέλνονται σε ένα χρήστη χωρίς την συναίνεσή του ή την εκδήλωση της επιθυμίας του να τα λαμβάνει. Πρόκειται κατά κανόνα για μηνύματα που στέλνουν οι επιχειρήσεις για την προώθηση

των προϊόντων ή των υπηρεσιών τους. Συχνά, αυτά τα ηλεκτρονικά μηνύματα περιλαμβάνουν προτάσεις για προγράμματα, προσφορές για γραμμές τηλεφωνικού ή δικτυακού σεξ, προσκλήσεις σε δικτυακό τζόγο που προκαλούν σύγχυση, είναι πολλές φορές προσβλητικά και κοστίζουν ακριβά για να τα «κατεβάσει» κανείς, να τα διαβάσει και να τα διαγράψει.

Η μεγάλη διάδοση που γνωρίζει η αυθαίρετη ηλεκτρονική αλληλογραφία, θα κάνει το ηλεκτρονικό ταχυδρομείο όλο και πιο δύσκολο στη χρήση του, ίσως και ακόμη τελείως άχρηστο ως μέσο επικοινωνίας για καταναλωτές και επιχειρήσεις αν το πλήθος των μηνυμάτων συνεχίσει να αυξάνει αντί να μειωθεί δραστικά.

ΚΕΦΑΛΑΙΟ 1
ΔΙΑΔΙΚΤΥΟ ΚΑΙ ΑΛΛΗΛΟΓΡΑΦΙΑ

1.1 ΤΙ ΕΙΝΑΙ ΤΟ INTERNET

Το Internet (Διαδίκτυο) είναι ένα παγκόσμιο δίκτυο ηλεκτρονικών υπολογιστών, οι οποίοι επικοινωνούν μεταξύ τους χρησιμοποιώντας ένα κοινό πρωτόκολλο επικοινωνίας, το TCP/IP (Transmission Control Protocol/Internet Protocol). Οι χρήστες του Internet μπορούν εύκολα και γρήγορα να αποστείλουν και να λάβουν αρχεία, να κάνουν χρήση της ηλεκτρονικής αλληλογραφίας, και γενικά να χρησιμοποιήσουν τις πολυάριθμες υπηρεσίες που έχουν στη διάθεσή τους ως χρήστες του Διαδικτύου[8].

Η απαράλλακτη μεταφορά της πληροφορίας σε οποιαδήποτε μορφή είναι αυτή (αρχείο, μήνυμα κλπ), επιτυγχάνεται με τη χρήση ενός κατάλληλου **πρωτοκόλλου μεταφοράς (transfer protocol)**. Το πρωτόκολλο μεταφοράς λέει στους δύο υπολογιστές πώς να στείλουν και πώς να λάβουν την πληροφορία. Ανάμεσα σε αυτά που χρησιμοποιούνται περισσότερο είναι τα εξής[8]:

- **Hypertext Transfer Protocol (HTTP)**: Για το World Wide Web (WWW)
- **Simple Mail Transfer Protocol (SMTP)**: Για την υπηρεσία του ηλεκτρονικού ταχυδρομείου
- **File Transfer Protocol (FTP)**: Για την υπηρεσία της μεταφοράς αρχείων
- **Network News Transfer Protocol (NNTP)**: Για τη συμμετοχή σε ομάδες συζητήσεων

1.2 ΙΣΤΟΡΙΑ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ

Οι πρώτες απόπειρες για την δημιουργία ενός διαδικτύου ξεκίνησαν στις ΗΠΑ κατά την διάρκεια του ψυχρού πολέμου. Η Ρωσία είχε ήδη στείλει στο διάστημα τον δορυφόρο Σπούτνικ 1 κάνοντας τους Αμερικανούς να φοβούνται όλο και περισσότερο για την ασφάλεια της χώρας τους. Θέλοντας λοιπόν να προστατευτούν από μια πιθανή πυρηνική επίθεση των Ρώσων, δημιούργησαν την υπηρεσία προηγμένων αμυντικών ερευνών ARDA (Advanced Research Projects Agency) γνωστή ως DARPA (Defense Advanced Research Projects Agency) στις μέρες μας. Αποστολή της συγκεκριμένης υπηρεσίας ήταν να βοηθήσει τις στρατιωτικές δυνάμεις των ΗΠΑ να αναπτυχθούν τεχνολογικά και να δημιουργήσει ένα δίκτυο επικοινωνίας το οποίο θα μπορούσε να επιβιώσει σε μια ενδεχόμενη πυρηνική επίθεση[4].

Το αρχικό θεωρητικό υπόβαθρο δόθηκε από τον Τζ. Λικλάιντερ (J.K.R. Licklider). Η θεωρία αύτη υποστήριζε την ύπαρξη ενός δικτύου υπολογιστών που θα ήταν συνδεδεμένοι μεταξύ τους και θα μπορούσαν να ανταλλάσσουν γρήγορα πληροφορίες και προγράμματα. Το επόμενο θέμα που προέκυπτε ήταν ότι το δίκτυο αυτό θα έπρεπε να ήταν αποκεντρωμένο έτσι ώστε ακόμα κι αν κάποιος κόμβος τους δεχόταν επίθεση να υπήρχε δίοδος επικοινωνίας για τους υπόλοιπους υπολογιστές. Τη λύση σε αυτό έδωσε ο Πολ Μπάραν (Paul Baran) με τον σχεδιασμό ενός κατανεμημένου δικτύου επικοινωνίας που χρησιμοποιούσε την ψηφιακή τεχνολογία. Πολύ σημαντικό ρόλο έπαιξε και η θεωρία ανταλλαγής πακέτων του Λέοναρντ Κλάινροκ (Leonard Kleinrock), που υποστήριζε ότι πακέτα πληροφοριών που θα περιείχαν την προέλευση και τον προορισμό τους μπορούσαν να σταλούν από έναν υπολογιστή σε έναν άλλο.

Στηριζόμενο λοιπόν σε αυτές τις τρεις θεωρίες δημιουργήθηκε το πρώτο είδος διαδικτύου γνωστό ως ARPANET. Εγκαταστάθηκε και λειτούργησε για πρώτη φορά το 1969 με 4 κόμβους μέσω των οποίων συνδέονται 4 μίνι υπολογιστές του πανεπιστημίου της Καλιφόρνια στην Σάντα Μπάρμπαρα, του πανεπιστημίου της Καλιφόρνια στο Λος Άντζελες, το SRI στο Στάνφορντ και το πανεπιστήμιο της Γιούτα. Μέχρι το 1972 επικοινωνούσαν μέσω ARPANET 23 ακαδημαϊκά ιδρύματα, οπότε και εμφανίζεται για πρώτη φορά το σύστημα διαχείρισης ηλεκτρονικού ταχυδρομείου (email).

Μέχρι τα τέλη της δεκαετίας του 1970 χρησιμοποιούσαν το δίκτυο αυτό συστήματα εκτός ΗΠΑ, όπως Αγγλία και Νορβηγία. Το 1989 η Υπηρεσία Επικοινωνιών Άμυνας διακόπτει το ARPANET λόγω μη χρηματοδότησης. Το δίκτυο αυτό αντικαθίσταται από το NSFNET (National Science Foundation Net), το οποίο χρησιμοποιείται από ακαδημαϊκά ιδρύματα, κρατικούς και ιδιωτικούς οργανισμούς πολλών χωρών[2].

Τη δεκαετία του 1990 το NSFNET επεκτείνεται σε όλο το κόσμο και παράλληλα κάνει την εμφάνιση του το Internet. Στις αρχές αυτής της δεκαετίας δημιουργείται η υπηρεσία Gopher που αποτέλεσε την πρώτη εφαρμογή περιήγησης αρχείων του Internet. Τα δίκτυα κάνουν εφικτή την επικοινωνία μέσω του ηλεκτρονικού ταχυδρομείου (e-mail), της ηλεκτρονικής διάσκεψης (conferencing) και της ηλεκτρονικής συνομιλίας (IRC), των ομάδων συζήτησης (newsgroups, forums), της μεταφοράς αρχείων (FTP-File Transfer Protocol) κτλ.

Στα μέσα της δεκαετίας του 1990 εμφανίζεται ο Παγκόσμιος Ιστός (World Wide Web), ο οποίος παρέχει τη δυνατότητα πρόσβασης σε αρχεία που συνδυάζουν κείμενο, εικόνα και ήχο. Ταυτόχρονα επικρατούν οι προσωπικοί ηλεκτρονικοί υπολογιστές που χρησιμοποιούν λειτουργικά συστήματα τύπου Windows[4].

1.3 ΣΧΕΤΙΚΗ ΟΡΟΛΟΓΙΑ

Σε αυτή την ενότητα θα παρουσιαστούν ορολογίες σχετικά με το διαδίκτυο και τα εργαλεία που χρησιμοποιούνται για την περιήγηση σε αυτό[8].

Παγκόσμιος Ιστός (World Wide Web - WWW)

Δεν είναι λίγοι αυτοί που νομίζουν ότι οι όροι Διαδίκτυο και Παγκόσμιος Ιστός είναι ταυτόσημοι. Η αλήθεια είναι ότι ο Παγκόσμιος Ιστός (World Wide Web ή WWW) είναι ένα μέρος του Διαδικτύου. Αποτελεί όμως το μεγαλύτερο, το δημοφιλέστερο και το ταχύτερα αναπτυσσόμενο κομμάτι του. Συγκεκριμένα, ο Παγκόσμιος Ιστός είναι το μέσο για την εύκολη ανάκτηση του τεράστιου όγκου πληροφοριών που διατίθενται μέσω του Διαδικτύου. Χρησιμοποιεί ένα από τα πρωτόκολλα του Διαδικτύου, το Hypertext Transfer Protocol (HTTP).

Ιστοσελίδα (web page)

Οι πληροφορίες του Παγκόσμιου Ιστού εμφανίζονται μορφοποιημένες με τη γλώσσα HTML (Hypertext Markup Language) σε μορφή ιστοσελίδων (web pages) και με την κατάληξη .htm ή .html. Υπάρχουν όμως και διαφορετικές μορφοποιήσεις ιστοσελίδων, όπως για παράδειγμα .php. (π.χ. http://www.sch.gr/postings/publications.php). Η ιστοσελίδα αυτή δεν είναι παρά μια από τις 100 εκατομμύρια ιστοσελίδες που είναι διαθέσιμες σήμερα στο Internet. Οι ιστοσελίδες μπορεί να περιέχουν εκτός από στατικό κείμενο, εικόνες, video, ήχο, κινούμενες εικόνες (animation), δυναμικό κείμενο κτλ. Πού βρίσκονται όμως όλες αυτές οι ιστοσελίδες;

Διακομιστής Ιστού (web server)

Κάθε ιστοσελίδα βρίσκεται με τη μορφή αρχείου σε κάποιον διακομιστή Ιστού (web Server). Οι διακομιστές Ιστού είναι ειδικοί υπολογιστές με ειδικό λογισμικό και κατάλληλες δικτυακές συνδέσεις, οι οποίοι επιτρέπουν τη διάθεση των ιστοσελίδων σε ολόκληρο τον κόσμο. Ο χρήστης του Διαδικτύου που θέλει να δει μια ιστοσελίδα, τη ζητάει από τον διακομιστή Ιστού στον οποίο αυτή βρίσκεται, και ο διακομιστής Ιστού με τη σειρά του την στέλνει. Πώς γίνεται όμως η ζήτηση και η διάθεση των σελίδων;

Πρόγραμμα Περιήγησης (web browser)

Το πρόγραμμα περιήγησης ή αλλιώς ο web browser είναι ένα πρόγραμμα (πχ Netscape Navigator, Internet Explorer, Mozilla κτλ.), το οποίο χρησιμοποιεί ο χρήστης για να ζητήσει μια ιστοσελίδα από τον διακομιστή Ιστού που την περιέχει. Ο διακομιστής Ιστού λαμβάνει το αίτημα και εμφανίζει την ιστοσελίδα στο παράθυρο του προγράμματος περιήγησης του χρήστη. Πώς όμως καταλαβαίνει για ποιά ιστοσελίδα πρόκειται;

Διευθύνσεις Ιστού (Web Addresses)

Κάθε ιστοσελίδα χαρακτηρίζεται με μοναδικό τρόπο από τη διεύθυνσή της, ή αλλιώς το URL (Uniform Resource Locator) της. Το URL είναι αρκετό για να εντοπιστεί μια ιστοσελίδα που βρίσκεται σε έναν διακομιστή Ιστού οπουδήποτε στον κόσμο. Συνήθως αποτελείται από 5 μέρη: το πρωτόκολλο που χρησιμοποιείται για τη μεταφορά της, το όνομα περιοχής (domain name) του διακομιστή Ιστού που την περιέχει, τη διαδρομή στο αρχείο της ιστοσελίδας και το όνομα του αρχείου της ιστοσελίδας. Για παράδειγμα, η διεύθυνση:

http://www.sch.gr/postings/publications.php

αποτελείται από τα εξής μέρη:

- **http://** - χρησιμοποιείται το πρωτόκολλο μεταφοράς HTTP
- **www** - το όνομα του Web Server. Μπορεί να είναι οποιοδήποτε όνομα, αλλά το www είναι το όνομα που χρησιμοποιείται περίπου από το 90% των servers σήμερα.
- **www.sch.gr** - το όνομα περιοχής του διακομιστή Ιστού. Το τελευταίο μέρος δηλώνει το περιεχόμενο της σελίδας (πχ .com: εμπορικό, .edu: εκπαιδευτικό, .gov: κυβερνητικό, .org: μη κερδοσκοπικό) ή την χώρα (πχ .au: Αυστραλία, .gr: Ελλάδα).
- **/postings/** - το όνομα του φακέλου που περιέχει το αρχείο της ιστοσελίδας.
- **publications.php** - το όνομα του αρχείου της ιστοσελίδας.

Τοποθεσία ιστού (web site)

Μια ομάδα ιστοσελίδων που αφορούν έναν ιδιώτη, μια επιχείρηση, έναν οργανισμό ή άλλες ομάδες αποτελεί μια τοποθεσία Ιστού ή ένα Web Site. Για παράδειγμα, η τοποθεσία ιστού του ΤΕΙ της Πάτρας είναι www.teipat.gr.

Υπερσύνδεσμος (hyperlink ή link)

Ένα από τα σημαντικότερα χαρακτηριστικά που διευκολύνουν την περιήγηση στον Παγκόσμιο Ιστό είναι η χρήση της δομής του υπερκειμένου (hypertext). Η ανάγνωση των πληροφοριών και η μετακίνηση μέσα στο υπερκείμενο γίνεται με τη βοήθεια των υπερσυνδέσμων (hyperlinks), οι οποίοι βρίσκονται σε διάφορα σημεία μιας ιστοσελίδας. Συνήθως πρόκειται για υπογραμμισμένο κείμενο με διαφορετικό χρώμα από το κείμενο της ιστοσελίδας, αλλά μπορεί να

είναι και εικόνα. Αναγνωρίζεται από την μορφή που παίρνει ο δείκτης του ποντικιού όταν είναι επάνω του (γίνεται ένα «χέρι»).

1.4 Η ΧΡΗΣΗ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ ΣΤΗΝ ΕΛΛΑΔΑ

Στην νέα έκθεση του Παγκόσμιου Οικονομικού Φόρουμ, που κατατάσσει τις χώρες του πλανήτη την περίοδο 2010-11, όσον αφορά την εισαγωγή και αξιοποίηση των νέων τεχνολογιών πληροφορικής, δικτύων και τηλεπικοινωνιών, η Ελλάδα καταλαμβάνει την 64η θέση μεταξύ 138 χωρών[19].

Η έκθεση ‘’The Global Information Technology Report 2010-11’’, σύμφωνα με το BBC, επιβεβαιώνει την τάση των προηγούμενων ετών, δείχνοντας ότι οι σκανδιναβικές χώρες και οι μικρές «ασιατικές τίγρεις» έχουν σταθερά ηγετική θέση στην υιοθέτηση των νέων τεχνολογιών και αποκομίζουν τα ανάλογα οικονομικά και κοινωνικά οφέλη.

Επίσης τονίζει ότι όσο πιο «διασυνδεδεμένη» είναι μια χώρα στον ιστό των παγκοσμίων τεχνολογιών, τόσο αναπτύσσεται ταχύτερα η οικονομία της και γίνεται πιο ανταγωνιστική, ενώ επισημαίνει ότι η σημασία των νέων τεχνολογιών είναι ακόμα μεγαλύτερη εν μέσω της σοβαρότερης οικονομικής κρίσης των τελευταίων δεκαετιών.

Η βαθμολογία της πρώτης Σουηδίας είναι 5,60 μονάδες, ενώ της 64ης Ελλάδας 3,83 και της τελευταίας χώρας (Τσαντ) 2,59 μονάδες. Την πρώτη δεκάδα των πιο τεχνολογικά προηγμένων και ψηφιακά διασυνδεδεμένων χωρών συμπληρώνουν, κατά σειρά, η Συγκαπούρη, η Φινλανδία, η Ελβετία, οι ΗΠΑ, η Ταϊβάν, η Δανία, ο Καναδάς, η Νορβηγία και η Ν. Κορέα. [20]

Η χώρα μας, αν και υστερεί έναντι των υπολοίπων χωρών της Ευρώπης όσον αφορά την διείσδυση νέων τεχνολογιών, αρχίζει να παρουσιάζει σημεία ανάπτυξης. Το συμπέρασμα αυτό προκύπτει από την

πρώτη ολοκληρωμένη μέτρηση για την διείσδυση νέων τεχνολογιών στην Ελλάδα με βάση την κοινή ευρωπαϊκή προσέγγιση (δείκτες eEurope), που παρουσιάστηκε από το Παρατηρητήριο για την Κοινωνία της Πληροφορίας.

Σύμφωνα με τα στοιχεία της έρευνας, παρά το γεγονός ότι η χρήση του Ιντερνέτ παραμένει χαμηλή στη χώρα μας συγκριτικά με την Ευρώπη, σχεδόν ένας στους πέντε Έλληνες (ποσοστό 20,08%) χρησιμοποιεί πια το διαδίκτυο, ενώ το 17,9% του πληθυσμού το χρησιμοποιεί τακτικά, τουλάχιστον μια φορά την εβδομάδα. Οι νεαρότερες ηλικίες (16-24 ετών: 42%, 25-34 ετών: 30%) και οι κάτοικοι των αστικών πόλεων με ανώτερη μόρφωση, αποτελούν με σημαντική διαφορά τις ομάδες πληθυσμού με την υψηλότερη πρόσβαση.

Αναφορικά με τη διείσδυση του γρήγορου (ευρυζωνικού) Ίντερνετ στον ελληνικό πληθυσμό, σύμφωνα με τα αποτελέσματα της έρευνας, βρίσκεται ακόμα σε πολύ χαμηλό επίπεδο (1%) και αυτό οφείλεται στο ότι οι τιμές του γρήγορού Ίντερνετ στη χώρα μας παραμένουν υψηλές συγκριτικά με την υπόλοιπη Ευρώπη, δυσχεραίνοντας την ταχύτερη εξάπλωση του. Παρ’ όλα αυτά το 84% των χρηστών Διαδικτύου αναζητούν τακτικά πληροφορίες για προϊόντα και υπηρεσίες, ενώ έχει δημιουργηθεί μια κρίσιμη μάζα καταναλωτών οι οποίοι πραγματοποιούν παραγγελίες και αγοράζουν προϊόντα και υπηρεσίες για ιδιωτική χρήση μέσω του διαδικτύου. Οι ελληνικές επιχειρήσεις δεν δείχνουν να καρπώνονται το όφελος των ηλεκτρονικών αγορών, καθώς μόλις το 0,15% του κύκλου εργασιών τους προέρχεται από ηλεκτρονικό εμπόριο (επιχειρήσεις με πάνω από δέκα άτομα προσωπικό). Σε χαμηλά επίπεδα (7.6%) κινείται και το ποσοστό των επιχειρήσεων που έγιναν αποδέκτες ηλεκτρονικών παραγγελιών, οι οποίες ωστόσο ολοκληρώθηκαν με μη ηλεκτρονικό τρόπο[21].

Η έρευνα του Παρατηρητηρίου για την Κοινωνία της Πληροφορίας, μετρά για πρώτη φορά τη διείσδυση των τεχνολογιών πληροφορικής σε όλο το εύρος των ελληνικών επιχειρήσεων, συμπεριλαμβανομένων των μικρών επιχειρήσεων με προσωπικό ένα έως εννέα άτομα. Οι επιχειρήσεις με πάνω από δέκα άτομα προσωπικό, που διαθέτουν πρόσβαση στο διαδίκτυο, ανέρχονται στο πολύ υψηλό ποσοστό του 92,8%, ενώ για τις μικρές επιχειρήσεις (ένα – εννέα άτομα προσωπικό) το αντίστοιχο ποσοστό ανέρχεται σε 38%. Παρά το γεγονός ότι το ποσοστό των βασικών δημόσιων υπηρεσιών που είναι πλήρως ηλεκτρονικά διαθέσιμες (με πάνω από δέκα άτομα προσωπικό), εκτελούν συναλλαγές με φορείς του δημοσίου μέσω Ίντερνετ. Η εικόνα είναι ωστόσο διαφορετική στις πολύ μικρές επιχειρήσεις, όπου μια στις εννέα συναλλάσσεται με το δημόσιο τομέα μέσω Ίντερνετ[22].

1.5 ΗΛΕΚΤΡΟΝΙΚΗ ΑΛΛΗΛΟΓΡΑΦΙΑ

Η ηλεκτρονική αλληλογραφία είναι η πιο δημοφιλής από τις υπηρεσίες του Διαδικτύου. Είναι μια μορφή επικοινωνίας η οποία επιτρέπει στους χρήστες του Διαδικτύου που έχουν **ηλεκτρονική διεύθυνση** (**e-mail address**) να στείλουν ένα μήνυμα σε άλλους χρήστες, με τρόπο που μοιάζει με αυτόν του κλασικού ταχυδρομείου. Κάθε μήνυμα χαρακτηρίζεται από την ηλεκτρονική διεύθυνση του αποστολέα, το περιεχόμενο (που μπορεί να είναι απλό κείμενο, εικόνα, επισυναπτόμενο αρχείο κ.ά.), και την ηλεκτρονική διεύθυνση του παραλήπτη. Τα μηνύματα φυλάσσονται σε ηλεκτρονικά γραμματοκιβώτια (**mailboxes**) μέχρι την ανάκτησή τους[12].

1.6 ΠΩΣ ΓΙΝΕΤΑΙ Η ΜΕΤΑΦΟΡΑ ΤΩΝ ΜΗΝΥΜΑΤΩΝ;

Η αποστολή των μηνυμάτων γίνεται με χρήση ενός πρωτοκόλλου μεταφοράς πληροφορίας του Διαδικτύου, του **Simple Mail Transfer Protocol (SMTP)**. Το πρωτόκολλο SMTP επιτρέπει την μεταφορά μηνυμάτων από έναν **Εξυπηρετητή Ηλεκτρονικού Ταχυδρομείου (Mail Server)** του Διαδικτύου σε έναν άλλον. Κάθε μήνυμα έχει μια **επικεφαλίδα (header)** που χρησιμοποιείται για την αναγνώριση της ηλεκτρονικής διεύθυνσης του παραλήπτη, την ηλεκτρονική διεύθυνση και το όνομα του αποστολέα, και λεπτομέρειες για τους κόμβους από τους οποίους θα περάσει το μήνυμα μέσα στο δίκτυο για να φτάσει στον προορισμό του.

Η ανάκτηση των μηνυμάτων από τον Εξυπηρετητή γίνεται με χρήση του πρωτοκόλλου **Post Office Protocol (POP)**. Η έκδοση 3 του POP (POP3) χρησιμοποιείται από τα περισσότερα προγράμματα διαχείρισης της ηλεκτρονικής αλληλογραφίας, τους **e-mail Clients**. Ο e-mail Client δημιουργεί ένα γραμματοκιβώτιο (**Inbox**) στον υπολογιστή του χρήστη, και όταν αυτός συνδέεται με τον Εξυπηρετητή Ηλεκτρονικού Ταχυδρομείου, τα μηνύματά του μεταφέρονται στο γραμματοκιβώτιο[12].

ΚΕΦΑΛΑΙΟ 2
ΑΝΕΠΙΘΥΜΗΤΗ ΑΛΛΗΛΟΓΡΑΦΙΑ

2.1 ΟΡΙΣΜΟΣ ΑΝΕΠΙΘΥΜΗΤΗΣ ΑΛΛΗΛΟΓΡΑΦΙΑΣ

Ανεπιθύμητη αλληλογραφία είναι η μαζική αποστολή μεγάλου αριθμού μηνυμάτων που απευθύνονται σε ένα σύνολο παραληπτών του Διαδικτύου χωρίς αυτοί να το επιθυμούν και χωρίς να έχουν συνειδητά προκαλέσει την αλληλογραφία με τον εν λόγω αποστολέα. Η ανεπιθύμητη αλληλογραφία συχνά έχει τη μορφή ενημερωτικών ή διαφημιστικών μηνυμάτων για προϊόντα ή υπηρεσίες τα οποία φθάνουν στο γραμματοκιβώτιό μας χωρίς να έχουμε ζητήσει αυτήν την πληροφόρηση. Αυτή η αλληλογραφία, λοιπόν, μπορεί να χαρακτηριστεί ως ανεπιθύμητη[16].

Τα κυριότερα χαρακτηριστικά της μπορούν να συνοψιστούν στα ακόλουθα σημεία:

- **Απρόκλητη:** Η επικοινωνία που επιχειρείται είναι απρόκλητη, δηλαδή δεν υπάρχει κάποια σχέση μεταξύ παραλήπτη και αποστολέα που θα δικαιολογούσε ή θα προκαλούσε την επικοινωνία αυτή.
- **Εμπορική:** Πολλές φορές η ανεπιθύμητη αλληλογραφία αφορά στην αποστολή μηνυμάτων εμπορικού σκοπού για την προβολή και τη διαφήμιση προϊόντων και υπηρεσιών, με σκοπό την προσέλκυση πελατών και την πραγματοποίηση πωλήσεων.
- **Μαζική:** Η ανεπιθύμητη αλληλογραφία συνίσταται στη μαζική αποστολή μεγάλων ποσοτήτων μηνυμάτων από τον αποστολέα σε ένα μεγάλο πλήθος παραληπτών.

Η αναγκαιότητα για την αντιμετώπιση της ανεπιθύμητης αλληλογραφίας εντοπίζεται στα ακόλουθα σημεία:

- **Είναι φαινόμενο δυσάρεστο, ενοχλητικό και απαράδεκτο από τους παραλήπτες.** Πολλές φορές προβάλει αμφίβολης ποιότητας προϊόντα και υπηρεσίες, ενώ συνηθισμένη είναι η προβολή ύποπτων οικονομικών δραστηριοτήτων τύπου πυραμίδων κ.λπ. Άλλα μηνύματα περιέχουν ή διαφημίζουν σεξουαλικό περιεχόμενο.
- **Οδηγεί σε κατάχρηση πόρων του Διαδικτύου.** Η κατάχρηση αυτή επιβαρύνει τα δίκτυα με δέσμευση εύρους ζώνης, αποθηκευτικών και υπολογιστικών πόρων στους εξυπηρετητές ηλεκτρονικής αλληλογραφίας (e-mail servers). Αντίστοιχα προβλήματα προκαλεί στην πρόσβαση και στα συστήματα των χρηστών.
- **Θέτει σε κίνδυνο την ασφάλεια και την αξιοπιστία του Διαδικτύου.** Οι spammers βρίσκονται σε συνεχή αναζήτηση συστημάτων τα οποία θα μπορούσαν να χρησιμοποιήσουν για την αποστολή των μηνυμάτων τους. Πολλά μηνύματα αυτής της κατηγορίας μεταφέρουν επισυναπτόμενα τα οποία μπορεί να είναι ιοί ή δούρειοι ίπποι, οι οποίοι θέτουν σε κίνδυνο την ασφάλεια των συστημάτων. Το τελευταίο διάστημα μεγάλο ποσοστό ανεπιθύμητης και επικίνδυνης αλληλογραφίας είναι αποτέλεσμα της δράσης ιών που έχουν προσβάλει διάφορα συστήματα διασυνδεμένα στο Διαδίκτυο.

2.2 ΟΙ ΠΡΩΤΕΣ ΑΝΕΠΙΘΥΜΗΤΕΣ ΑΛΛΗΛΟΓΡΑΦΙΕΣ

Ο Einar Stefferud, ένας μακροχρόνιος χειριστής του δικτύου, αναφέρει ότι η DEC το 1978, ανακοίνωσε ένα νέο DEC-20 μηχάνημα στέλνοντας μια πρόσκληση σε όλες τις ARPANET διευθύνσεις στη δυτική ακτή, αφού χρησιμοποίησε τον κατάλογο διευθύνσεων του

δικτύου ARPANET, προσκαλώντας άτομα σε μια δεξίωση στη Καλιφόρνια. Η εταιρεία τιμωρήθηκε διότι παραβίασε την πολιτική χρήσης της ARPANET και ένα μήνυμα στάλθηκε σ' αυτήν για να υπενθυμίσει τους κανόνες. Φυσικά κανείς τότε δεν ήξερε ότι αυτό θα ονομαζόταν αργότερα spam. Ακόμα νωρίτερα μία άλλη περίπτωση ενός spam πραγματοποιήθηκε το 1371. Κάποιος ονόματι Peter Bos χρησιμοποίησε το CTSS MAIL για να στείλει σε όλους το εξής αντιπολεμικό μήνυμα : 'THERE IS NO WAY TO PEACE. PEACE IS THE WAY." Αναφέρεται ότι ο spammer υποστήριζε το spam του λέγοντας, «μα αυτό είναι σημαντικό» [3].

2.3 ΕΙΔΗ ΑΝΕΠΙΘΥΜΗΤΗΣ ΑΛΛΗΛΟΓΡΑΦΙΑΣ

Οι ***περιγραφές,*** που ακολουθούν ερμηνεύουν κάποιους, απ' τους όρους που χρησιμοποιούνται στις συζητήσεις σχετικά με την ανεπιθύμητη αλληλογραφία. Αυτές οι ερμηνείες επίσης θα διευκρινίσουν κάποιους όρους που συχνά χρησιμοποιούνται λανθασμένα όταν περιγράφονται προβλήματα με τα ηλεκτρονικά μηνύματα[7].

- **Spamming:** Είναι η διαδικασία της αποστολής ηλεκτρονικού μηνύματος σε ένα μεγάλο αριθμό ηλεκτρονικών διευθύνσεων και συχνά συγκρίνεται με τον όρο **"junk mail"** που χρησιμοποιείται για να περιγράψει παρόμοιες δραστηριότητες που πραγματοποιούνται ***μέσω*** ταχυδρομικών υπηρεσιών. Εντούτοις, υπάρχει άλλη μια δραστηριότητα που ονομάζεται Spamming. Αυτή είναι όταν ένας μονός υπολογιστής κατακλύζεται με ηλεκτρονικά μηνύματα σε μια προσπάθεια να προκαλέσει ενόχληση και έξοδα.
- **Spam:** Χρησιμοποιείται όταν αναφέρεται σε ένα ή πολλαπλά κομμάτια ηλεκτρονικών μηνυμάτων τα οποία αντιλαμβάνονται

από τον παραλήπτη ως ανεπιθύμητα και ως αποτελέσματα του Spamming.

- **Spoofing:** Είναι η διαδικασία σύνδεσης με έναν πράκτορα μεταφορών ηλεκτρονικών μηνυμάτων, και νόθευσης της πληροφορίας που απαιτείται να παρέχει, έτσι ώστε να προκαλέσεις το μήνυμα να φαίνεται ότι προέρχεται από κάποιον άλλον και όχι από σένα.
- **Mail Forwarding:** Η διαδικασία της λήψης και αποστολής μηνύματος το οποίο κατευθύνεται σε ένα mail server αλλά στην ουσία κατευθύνεται ολοκληρωτικά κάπου αλλού παρά σε εκείνη την ιστοσελίδα.
- **Host:** Ένας υπολογιστής συνδεδεμένος στο δίκτυο, ο οποίος παρέχει δυνατότητα πρόσβασης στο δίκτυο.
- **Postmaster:** Το άτομο ή τα άτομα που είναι υπεύθυνα και εξασφαλίζουν ότι το σύστημα μηνυμάτων στην ιστοσελίδα δουλεύει κανονικά. Postmaster μπορεί να είναι το άτομο που εγκαθιστά το προϊόν που χειρίζεται το μήνυμα, ή κάποιος ο οποίος έχει πολύ μικρή εμπειρία στους υπολογιστές και στα ηλεκτρονικά μηνύματα.

2.4 Η ΑΝΕΠΙΘΥΜΗΤΗ ΑΛΛΗΛΟΓΡΑΦΙΑ ΣΤΗΝ ΚΑΘΗΜΕΡΙΝΗ ΗΛΕΚΤΡΟΝΙΚΗ ΑΛΛΗΛΟΓΡΑΦΙΑ

Η ανεπιθύμητη αλληλογραφία πλημμυρίζει το Διαδίκτυο και κατ' επέκταση το κουτί μηνυμάτων μας με πολλά αντίγραφα του ίδιου μηνύματος, σε μια προσπάθεια να αναγκάσει τη λήψη ενός μηνύματος στους παραλήπτες, που σε καμία περίπτωση δεν θα επέλεγαν να το λάβουν. Η περισσότερη Ανεπιθύμητη αλληλογραφία είναι εμπορική διαφήμιση, συχνά για αμφίβολα προϊόντα. Η ανεπιθύμητη αλληλογραφία

κοστίζει στον αποστολέα πολύ λίγα, μιας και οι περισσότερες από τις δαπάνες για την αποστολή ενός τέτοιου μηνύματος πληρώνονται από τον παραλήπτη ή τους παροχείς Internet (ISPs) [1].

2.5 ΓΙΑΤΙ Η ΑΝΕΠΙΘΥΜΗΤΗ ΑΛΛΗΛΟΓΡΑΦΙΑ ΕΙΝΑΙ ΤΟΣΟ ΜΕΓΑΛΟ ΠΡΟΒΛΗΜΑ;

- **Κόστος:** Η αποστολή μαζικών ηλεκτρονικών μηνυμάτων είναι απίστευτα φτηνή. Παρ' αυτά όμως, κάθε άτομο που λαμβάνει την ανεπιθύμητη αλληλογραφία πρέπει να μπορεί να πληρώσει το κόστος της. Και το κόστος, για τους παραλήπτες είναι πολύ μεγαλύτερο από το κόστος του αποστολέα.
- **Απάτη:** Οι spammers γνωρίζουν μετά από πολλές έρευνες, ότι η πλειοψηφία (που συχνά φτάνει το 95%) των παραληπτών δεν θέλουν να λαμβάνουν τα μηνύματά τους. Ως αποτέλεσμα, πολλοί junk emailers χρησιμοποιούν τεχνικές για να σε κάνουν να ανοίξεις τα μηνύματά τους. Για παράδειγμα, κάνουν το θέμα του μηνύματος να μοιάζει σαν να είναι οτιδήποτε άλλο παρά διαφήμιση.
- **Απώλεια άλλων πόρων:** Όταν οι spammers στέλνουν ένα ηλεκτρονικό μήνυμα σε εκατομμύρια ανθρώπους, αυτό μεταφέρεται από άλλα συστήματα που βρίσκονται καθ’ οδών προς τον προορισμό τους, μετακινώντας το για άλλη μια φορά μακριά απ' την πηγή του. Οι μεταφορείς ανάμεσα τους ξαφνικά κουβαλούν: τεράστια φορτία διαφημίσεων για τον spammer. Ο αριθμός των ανεπιθύμητων μηνυμάτων που στέλνονται κάθε μέρα είναι πραγματικά απεριόριστος και κάθε ένα ξεχωριστά πρέπει να διαχειρίζεται από άλλα συστήματα.
- **Εκτόπισμα του κανονικού ηλεκτρονικού Μηνύματος:** Το ηλεκτρονικό μήνυμα γίνεται όλο ένα και περισσότερο, σημαντικό εργασιακό εργαλείο. Στα τέλη του 1980, αφού όλο και περισσότερες

επιχειρήσεις άρχισαν να χρησιμοποιούν μηχανήματα fax, οι πωλητές αποφάσισαν ότι μπορούσαν στείλουν με fax τις διαφημίσεις τους στο κοινό.

- **Ενοχλητικός παράγοντας:** Η διεύθυνση του ηλεκτρονικού μηνύματος δεν είναι δημόσιος χώρος. Είναι προσωπική, πληρώνεται κάποιο χρηματικό ποσό και θα πρέπει να υπάρχει ο πλήρης έλεγχος, για οτιδήποτε χρησιμοποιείται, από τον νόμιμο κάτοχο. Εάν επιθυμούμε να λαμβάνουμε τόνους ανεπιθύμητων διαφημίσεων, θα πρέπει να μπορούμε. Αλλά δεν θα πρέπει να αναγκαζόμαστε να υποφέρουμε αυτή τη πληθώρα μηνυμάτων εκτός και μέχρι εμείς πραγματικά να το ζητήσουμε.
- **Ηθικολογία:** Η Ανεπιθύμητη αλληλογραφία είναι βασισμένο στην κλοπή υπηρεσίας, στην απάτη και παραπλάνηση όπως συμβαίνει με τη μετακίνηση κόστους προς τον παραλήπτη. Η μεγάλη υπερίσχυση, των προϊόντων και των υπηρεσιών που πωλούνται από την UCE είναι αμφίβολης νομιμότητας. Κάθε επιχείρηση που εξαρτάται από το κλέψιμο των πελατών της, που στήνει ενέδρες στον αθώο και υβρίζει τα γνωστά πρότυπα του Internet είναι - και θα πρέπει να είναι - καταδικασμένη στην αποτυχία[1].

2.6 ΛΟΓΟΙ ΑΠΟΣΤΟΛΗΣ ΑΝΕΠΙΘΥΜΗΤΩΝ ΜΑΖΙΚΩΝ ΜΗΝΥΜΑΤΩΝ

Πρόκειται κατά κανόνα για μηνύματα που στέλνουν οι επιχειρήσεις για την προώθηση των προϊόντων ή των υπηρεσιών τους. Συχνά, αυτά τα ηλεκτρονικά μηνύματα περιλαμβάνουν προτάσεις για πυραμοειδή – προγράμματα, προσφορές για γραμμές τηλεφωνικού ή δικτυακού σεξ, προσκλήσεις σε δικτυακό τζόγο και άλλα που προκαλούν

σύγχυση, είναι πολλές φορές προσβλητικά και κοστίζουν ακριβά για να τα «κατεβάσει» κανείς, να τα διαβάσει και να τα διαγράψει[3].

2.7 ΕΛΛΗΝΙΚΗ ΝΟΜΟΘΕΣΙΑ ΚΑΤΑ ΤΗΣ ΑΝΕΠΙΘΥΜΗΤΗΣ ΑΛΛΗΛΟΓΡΑΦΙΑΣ

ΝΟΜΟΣ 2251/1994-Προστασία των καταναλωτών

Άρθρο 4 – Σύμβαση από απόσταση

«Παρ 6. Η χρησιμοποίηση των τεχνικών επικοινωνίας πρέπει να γίνεται κατά τέτοιο τρόπο, ώστε να μην προσβάλλεται η ιδιωτική ζωή του καταναλωτή. Απαγορεύεται χωρίς την συναίνεση του καταναλωτή η χρησιμοποίηση τεχνικών επικοινωνίας για την πρόταση σύναψης σύμβασης όπως τηλεφώνου αυτόματης κλήσης, τηλεομοιοτυπίας (φαξ), ηλεκτρονικού ταχυδρομείου ή άλλου ηλεκτρονικού μέσου επικοινωνίας.»

Άρθρο 9 – Διαφήμιση. Έννοια παραπλανητικής και αθέμιτης διαφήμισης.

«Παρ 10. Η μετάδοση διαφημιστικού μηνύματος απευθείας στον καταναλωτή μέσω τηλεφώνου, τηλεομοιοτυπίας (φαξ), ηλεκτρονικού ταχυδρομείου, αυτόματης κλήση ή άλλου ηλεκτρονικού μέσου επικοινωνίας επιτρέπεται μόνο αν συναινεί ρητά ο καταναλωτής.

Παρ 11. Ανεξάρτητα από τον περιορισμό της προηγούμενης παραγράφου, η μετάδοση διαφημιστικού μηνύματος απευθείας στον καταναλωτή με οποιονδήποτε τρόπο άμεσης επικοινωνίας (άμεση διαφήμιση) επιτρέπεται μόνο αν ο προμηθευτής ή άλλος για λογαριασμό του προμηθευτή κάνει χρήση στοιχείων ή πληροφοριών προσωπικού χαρακτήρα του καταναλωτή που περιήλθαν σε γνώση του από προηγούμενες συναλλακτικές σχέσεις του με τον καταναλωτή, από γενικά προσιτές πηγές, όπως κατάλογο ή άλλα δημοσιευμένα στοιχεία, ή από άλλο φυσικό ή νομικό πρόσωπο, εφόσον ο καταναλωτής εγκρίνει ρητά την μεταβίβαση των προσωπικών του στοιχείων για το σκοπό της άμεσης διαφήμισης. Ο διαφημιστής είναι

υποχρεωμένος να αναφέρει στον καταναλωτή τον τρόπο με τον οποίο περιήλθαν σε γνώση του τα προσωπικά στοιχεία του καταναλωτή.
Παρ 12. Στις περιπτώσεις των παραγράφων 10 και 11, ο προμηθευτής οφείλει να διακόψει κάθε μορφή άμεσης διαφήμισης και να διαγράψει τα προσωπικά στοιχεία του καταναλωτή, εφόσον το ζητήσει ο καταναλωτής.»

ΝΟΜΟΣ 2472/1997-Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Άρθρο 19 – Αρμοδιότητες, λειτουργία και αποφάσεις της Αρχής
«Παρ 4. Η Αρχή τηρεί τα ακόλουθα μητρώα:
α) Μητρώο Αρχείων και Επεξεργασιών, στο οποίο περιλαμβάνονται τα αρχεία και οι επεξεργασίες που γνωστοποιούνται στην Αρχή.
β) Μητρώο Αδειών, στο οποίο περιλαμβάνονται οι άδειες που εκδίδει η Αρχή για την ίδρυση και λειτουργία αρχείων που περιέχουν ευαίσθητα δεδομένα.
γ) Μητρώο Διασυνδέσεων, στο οποίο περιλαμβάνονται οι δηλώσεις και οι άδειες που εκδίδει η Αρχή για τη διασύνδεση αρχείων.
δ) Μητρώο προσώπων που δεν επιθυμούν να περιλαμβάνονται σε αρχεία, τα οποία έχουν ως σκοπό την προώθηση προμήθειας αγαθών ή την παροχή υπηρεσιών εξ αποστάσεως.
ε) Μητρώο Αδειών Διαβίβασης, στο οποίο καταχωρίζονται οι άδειες διαβίβασης δεδομένων προσωπικού χαρακτήρα.
στ) Μητρώο Απόρρητων Αρχείων, στο οποίο καταχωρίζονται, με απόφαση της Αρχής ύστερα από αίτηση του εκάστοτε υπεύθυνου επεξεργασίας, αρχεία που τηρούν τα Υπουργεία Εθνικής Άμυνας και Δημόσιας Τάξης καθώς και η Εθνική Υπηρεσία Πληροφοριών, για λόγους εθνικής ασφάλειας ή για τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων. Στο Μητρώο Απόρρητων Αρχείων καταχωρίζονται και οι διασυνδέσεις με ένα τουλάχιστον αρχείο της περίπτωσης αυτής.»

ΝΟΜΟΣ 2774/1999-Προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα.

Άρθρο 9 – Μη ζητηθείσες κλήσεις

«1. Η χρησιμοποίηση αυτόματων συστημάτων κλήσης χωρίς ανθρώπινη παρέμβαση, ιδίως με χρήση αυτόματων συσκευών κλήσεως ή συσκευών τηλεομοιοτυπίας ή η πραγματοποίηση μη ζητηθείσων κλήσεων γενικώς με οποιοδήποτε τηλεπικοινωνιακό μέσο με ή χωρίς ανθρώπινη παρέμβαση, για σκοπούς απευθείας εμπορικής προώθησης προϊόντων ή υπηρεσιών ή για κάθε είδους διαφημιστικούς σκοπούς επιτρέπεται μόνο στην περίπτωση συνδρομητών, οι οποίοι έχουν δώσει εκ των προτέρων τη ρητή συγκατάθεσή τους.

2. Δεν επιτρέπεται η πραγματοποίηση μη ζητηθείσων κλήσεων για τους παραπάνω σκοπούς, εφόσον ο συνδρομητής έχει δηλώσει ότι δεν επιθυμεί γενικώς να δέχεται τέτοιες κλήσεις. Ο φορέας παροχής διαθέσιμων στο κοινό τηλεπικοινωνιακών υπηρεσιώω, υποχρεούται να καταχωρεί τις δηλώσεις αυτές σε ειδικό κατάλογο συνδρομητών, ο οποίος είναι στη διάθεση κάθε ενδιαφερόμενου.

3. Οι ανωτέρω ρυθμίσεις δεν ισχύουν για τους συνδρομητές που είναι νομικό πρόσωπα, εκτός εάν ο νόμιμος εκπρόσωπός τους δηλώσει ότι δεν επιθυμεί τη λήψη μη ζητηθείσων κλήσεων που γίνονται για τους παραπάνω σκοπούς.

4. Οι δηλώσεις των προηγούμενων παραγράφων γίνονται χωρίς επιβάρυνση και απευθύνονται στο φορέα παροχής δημοσίου τηλεπικοινωνιακού δικτύου ή και διαθέσιμης στο κοινό τηλεπικοινωνιακής υπηρεσίας.»

ΠΡΟΕΔΡΙΚΟ ΔΙΑΤΑΓΜΑ 131/2003-Προσαρμογή στην Οδηγία 2000/31 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με

ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά (Οδηγία για το ηλεκτρονικό εμπόριο)

Άρθρο 6 – Μη ζητηθείσα εμπορική επικοινωνία

«1. Εμπορική επικοινωνία με παραλήπτη που δεν την έχει ζητήσει, αν γίνεται με ηλεκτρονικό ταχυδρομείο και εφόσον δεν απαγορεύεται, πρέπει να αναγνωρίζεται σαφώς και επακριβώς ευθύς ως περιέλθει σ'αυτόν.

2. Με την επιφύλαξη των διατάξεων της ΚΥΑ Ζ1-496/2000 (Β΄ 1545) για την προστασία των καταναλωτών για τις εξ αποστάσεως συμβάσεις, του Ν. 2472/97 (Α 50) για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και των διατάξεων του Ν. 2774/99 (Α 287) για την προστασία της ιδιωτικής ζωής στον επικοινωνιακό τομέα οι φορείς παροχής υπηρεσιών που αναλαμβάνουν δραστηριότητες μη ζητηθείσας εμπορικής επικοινωνίας μέσω ηλεκτρονικού ταχυδρομείου οφείλουν να τηρούν και να συμβουλεύονται τακτικά μητρώα «επιλογών», όπου μπορούν να εγγράφονται τα φυσικά πρόσωπα που επιλέγουν να μη λαμβάνουν τέτοιες εμπορικές επικοινωνίες.»

ΝΟΜΟΣ 3471/2006-Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του ν. 2472/1997.

Άρθρο 11- Μη ζητηθείσα επικοινωνία

«1. Η χρησιμοποίηση αυτόματων συστημάτων κλήσης, ιδίως με χρήση συσκευών τηλεομοιοτυπίας (fax) ή ηλεκτρονικού ταχυδρομείου, και γενικότερα η πραγματοποίηση μη ζητηθείσων επικοινωνιών με οποιοδήποτε μέσο ηλεκτρονικής επικοινωνίας, με ή χωρίς ανθρώπινη παρέμβαση, για σκοπούς απευθείας εμπορικής προώθησης προϊόντων ή υπηρεσιών και για κάθε είδους διαφημιστικούς σκοπούς, επιτρέπεται μόνο αν ο συνδρομητής συγκατατεθεί εκ των προτέρων ρητώς.

2. Δεν επιτρέπεται η πραγματοποίηση μη ζητηθείσων επικοινωνιών για τους ανωτέρω σκοπούς, εφόσον ο συνδρομητής έχει δηλώσει προς τον φορέα παροχής διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ότι δεν επιθυμεί γενικώς να δέχεται τέτοιες επικοινωνίες. Ο φορέας υποχρεούται να καταχωρίζει δωρεάν τις δηλώσεις αυτές σε ειδικό κατάλογο συνδρομητών, ο οποίος είναι στη διάθεση κάθε ενδιαφερόμενου.

3. Τα στοιχεία επαφής ηλεκτρονικού ταχυδρομείου που αποκτήθηκαν νομίμως, στο πλαίσιο της πώλησης προϊόντων ή υπηρεσιών ή άλλης συναλλαγής, μπορούν να χρησιμοποιούνται για την απευθείας προώθηση παρόμοιων προϊόντων ή υπηρεσιών του προμηθευτή ή για την εξυπηρέτηση παρόμοιων σκοπών, ακόμη και όταν ο αποδέκτης του μηνύματος δεν έχει δώσει εκ των προτέρων τη συγκατάθεσή του, υπό την προϋπόθεση ότι του παρέχεται κατά τρόπο σαφή και ευδιάκριτο η δυνατότητα να αντιτάσσεται, με εύκολο τρόπο και δωρεάν, στη συλλογή και χρησιμοποίηση των ηλεκτρονικών του στοιχείων, και αυτό σε κάθε μήνυμα σε περίπτωση που ο χρήστης αρχικά δεν είχε διαφωνήσει σε αυτή τη χρήση.

4. Απαγορεύεται η αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου, που έχουν σκοπό την άμεση εμπορική προώθηση προϊόντων και υπηρεσιών, όταν δεν αναφέρεται ευδιάκριτα και σαφώς η ταυτότητα του αποστολέα ή του προσώπου προς όφελος του οποίου αποστέλλεται το μήνυμα, καθώς επίσης και η έγκυρη διεύθυνση στην οποία ο αποδέκτης του μηνύματος μπορεί να ζητεί τον τερματισμό της επικοινωνίας.

5. Οι ανωτέρω ρυθμίσεις ισχύουν και για τους συνδρομητές που είναι νομικά πρόσωπα.»

Άρθρο 14- Αστική ευθύνη

«1. Φυσικό ή νομικό πρόσωπο που, κατά παράβαση του νόμου αυτού, προκαλεί περιουσιακή βλάβη υποχρεούται σε πλήρη αποζημίωση. Αν προκάλεσε ηθική βλάβη, υποχρεούται σε χρηματική ικανοποίηση.

2. Η κατά το άρθρο 932 Α.Κ. χρηματική ικανοποίηση λόγω ηθικής βλάβης για παράβαση του παρόντος νόμου ορίζεται, κατ' ελάχιστο, στο ποσό των δέκα χιλιάδων ευρώ (10.000 €), εκτός αν ζητηθεί από τον ενάγοντα μικρότερο ποσό. Η χρηματική ικανοποίηση επιδικάζεται ανεξάρτητα από την αιτούμενη αποζημίωση για περιουσιακή βλάβη.

3. Οι απαιτήσεις του παρόντος άρθρου εκδικάζονται κατά τη διαδικασία των άρθρων 664 έως 676 Κ.Πολ.Δ., ανεξάρτητα από την έκδοση ή μη απόφασης της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα ή της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών για τη διαπίστωση παρανομίας ή την άσκηση ποινικής δίωξης.»

Οι Έλληνες χρήστες του διαδικτύου δεν είναι απροστάτευτοι από την εγχώρια νομοθεσία όσον αφορά την ανεπιθύμητη αλληλογραφία. Με το προεδρικό διάταγμα 131/2003 ορίζεται πως εμπορική επικοινωνία με παραλήπτη που δεν την έχει ζητήσει, αν γίνεται με το ηλεκτρονικό ταχυδρομείο πρέπει να αναγνωρίζεται μόλις αυτή περιέλθει σε αυτόν. Δηλαδή, αυτό σημαίνει πως πρέπει να αναφέρεται το θέμα του ηλεκτρονικού μηνύματος καθώς και τα στοιχεία του αποστολέα, για να μπορεί έτσι να αναγνωριστεί η ιδιότητα του αποστολέα.

Με την τήρηση της παραπάνω προϋπόθεσης αντιμετωπίζεται μόνο το μέρος που έχει σχέση με το κόστος που έχει η ανεπιθύμητη αλληλογραφία στον παραλήπτη και δεν ασχολείται καθόλου με το κόστος διαχείρισης του δικτύου, το οποίο αυξάνεται για τους παροχείς πρόσβασης στο Διαδίκτυο. Βέβαια η παραπάνω ρύθμιση έχει σαν προϋπόθεση την μη απαγόρευση της ανεπιθύμητης αλληλογραφίας.

Η προϋπόθεση αυτή αναφέρεται στην παράγραφο 2 του προεδρικού διατάγματος, σύμφωνα με την οποία οι φορείς παροχής υπηρεσιών που αναλαμβάνουν την αποστολή μη αιτηθείσας εμπορικής επικοινωνίας μέσω του ηλεκτρονικού ταχυδρομείου, πρέπει να συμβουλεύονται μητρώα «επιλογών», τα οποία αναφέρονται στους νόμους 2472/1997 και

2774/1999. Σύμφωνα, με τον νόμο 2251/1994 που αφορά τις πωλήσεις από απόσταση, απαγορεύεται η χρήση τεχνικών (όπως το ηλεκτρονικό ταχυδρομείο) για την πρόταση σύναψης σύμβασης χωρίς την συναίνεση του καταναλωτή. Επίσης, αναφορικά με την αποστολή διαφημιστικών μηνυμάτων μέσω του ηλεκτρονικού ταχυδρομείου, ο ίδιος νόμος ορίζει πως αυτή επιτρέπεται μόνο αν συναινεί ρητά ο καταναλωτής. Αυτό σημαίνει, πως η συναίνεση πρέπει να αναφέρεται στην συγκεκριμένη μορφή διαφήμισης, έστω και αν υπάρχουν προηγούμενες συναλλακτικές σχέσεις μεταξύ του διαφημιστή και του καταναλωτή. Όμως, η αποστολή διαφημιστικών μηνυμάτων επιτρέπεται αν ο προμηθευτής κάνει χρήση στοιχείων που περιήλθαν σε γνώση του από προηγούμενες συναλλακτικές σχέσεις με τον καταναλωτή από πηγές όπως είναι κατάλογοι ή άλλα δημοσιευμένα στοιχεία, εφόσον ο καταναλωτής εγκρίνει την μεταβίβαση των στοιχείων του για τον σκοπό της άμεσης διαφήμισης.

Το νομικό πλαίσιο που αφορά την αποστολή μη αιτηθείσας εμπορικής επικοινωνίας μέσω e-mail συμπληρώνεται με τις διατάξεις του δικαίου που αφορούν την προστασία των προσωπικών δεδομένων. Σύμφωνα, με τον νόμο 2774/1999 υιοθετείται η «εκ των προτέρων ρητή συγκατάθεση» του

καταναλωτή για την αποδοχή της εμπορικής επικοινωνίας. Επίσης, προβλέπεται και η δημιουργία ενός μητρώου, όπου μπορούν να καταχωρηθούν όσοι δεν επιθυμούν την λήψη ηλεκτρονικής αλληλογραφίας διαφημιστικής μορφής.

Η τήρηση Μητρώου «προσώπων που δεν επιθυμούν να περιλαμβάνονται σε αρχεία, τα οποία έχουν σκοπό την προώθηση προμήθειας αγαθών ή την παροχή υπηρεσιών εξ αποστάσεως» αποτελεί, σύμφωνα με τον νόμο 2472/1997, αρμοδιότητα της Αρχής Δεδομένων Προσωπικού Χαρακτήρα. Ωστόσο, η Ελλάδα είναι μία από τις χώρες που έλαβαν ειδοποίηση από την Ευρωπαϊκή Επιτροπή για την έγκαιρη

ενσωμάτωση της οδηγίας 2002/58/ΕΚ έως τις 31 Οκτωβρίου 2003 με αποτέλεσμα την παραλίγο παραπομπή της στο Διεθνές Ευρωπαϊκό Κοινοβούλιο. Ο νόμος 3471/2006 αποτελεί τροποποίηση του ήδη υπάρχοντα νόμου 2472/1997, με την ενσωμάτωση της οδηγίας 2002/58/ΕΚ και αφορά την προστασία των προσωπικών δεδομένων χαρακτήρα στον τομέα των ηλεκτρονικών επικοινωνιών με την θέσπιση των προϋποθέσεων που πρέπει να υπάρχουν για την επεξεργασία τους.

Στον νόμο αυτό αναφέρεται πως η πραγματοποίηση μη ζητηθείσων επικοινωνιών με οποιοδήποτε μέσο ηλεκτρονικής επικοινωνίας για σκοπούς απευθείας εμπορικής προώθησης προϊόντων ή υπηρεσιών επιτρέπεται μόνο αν ο συνδρομητής (καταναλωτής) έχει εκ των προτέρων συμφωνήσει ρητώς καθώς και πως στην περίπτωση που ο συνδρομητής έχει δηλώσει αντίθετος στην αποδοχή των μη ζητηθεισών επικοινωνιών, ο φορέας έχει υποχρέωση να καταχωρίσει αυτές τις δηλώσεις σε ειδικό κατάλογο συνδρομητών, ο οποίος είναι διαθέσιμος στον κάθε ενδιαφερόμενο.

Η αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου απαγορεύεται αν δεν αναφέρεται ευδιάκριτα η ταυτότητα και η έγκυρη ηλεκτρονική διεύθυνση του αποστολέα και η παράβαση των προστατευτικών διατάξεων για τους χρήστες, παρέχει στους θιγόμενους αποζημίωση τόσο για την περιουσιακή όσο και τη μη περιουσιακή ζημία που μπορεί να φτάσει έως και 100.000 ευρώ[4].

ΚΕΦΑΛΑΙΟ 3

SPAM

3.1 ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΤΟΥ SPAM

Τα βασικότερα χαρακτηριστικά του spam επικεντρώνονται στα εξής τρία σημεία. Καταρχάς, το Spam χαρακτηρίζεται ως **απρόκλητο,** γιατί δεν υπάρχει κάποια σχέση ανάμεσα σε παραλήπτες και αποστολέα ώστε να δικαιολογείται ή να προκαλείται μία τέτοιου είδους επικοινωνία. Χαρακτηρίζεται ως **εμπορικό,** διότι τα μηνύματα αυτά αφορούν τις περισσότερες φορές την προβολή και την διαφήμιση προϊόντων και υπηρεσιών με σκοπό την προσέλκυση πελατών και την πραγματοποίηση πωλήσεων.

Τέλος, χαρακτηρίζεται και ως **μαζικό,** αφού τα μηνύματα στέλνονται μαζικά από τον αποστολέα σε ένα μεγάλο πλήθος παραληπτών. Συνήθως, το ίδιο μήνυμα ή κάπως διαφοροποιημένο στέλνεται σε μεγάλο πλήθος παραληπτών.

Ωστόσο, εκτός από τα παραπάνω χαρακτηριστικά υπάρχουν και κάποια επιπλέον, όπως:

- Δεν υπάρχει η δυνατότητα της διαγραφής από τις λίστες του παραληπτών που έχουν στην κατοχής τους οι αποστολείς. Σε περίπτωση βέβαια, που γίνει διαγραφή, αυτό λειτουργεί ως επιβεβαίωση ότι υπάρχει η συγκεκριμένη ηλεκτρονική διεύθυνση.
- Η αποστολή αυτών των μηνυμάτων γίνεται με την χρήση κάποιων τεχνικών, οι οποίες έχουν στόχο την απόκρυψη της πραγματικής ταυτότητας του αποστολέα.
- Δεν υπάρχει μία έγκυρη ηλεκτρονική διεύθυνση του αποστολέα του διαφημιστικού μηνύματος για την πραγματοποίηση επικοινωνίας μαζί του.

- Στέλνονται χωρίς διάκριση, με αυτοματοποιημένα μέσα.
- Περιλαμβάνει ή προωθεί, αρκετές φορές παράνομο ή δυσάρεστο περιεχόμενο.
- Το περιεχόμενο αυτών των μηνυμάτων μπορεί να είναι ψευδές ή παραπλανητικό και τέλος
- Οι διευθύνσεις των παραληπτών έχουν αποκτηθεί με λογισμικό ανίχνευσης στο Διαδίκτυο για συλλογή ηλεκτρονικών διευθύνσεων (οι λεγόμενες ‘αράχνες’) ή μπορεί να έχουν αγοραστεί από εταιρίες που παράγουν cd με τέτοιου είδους περιεχόμενο έναντι μικρού κόστους[6].

3.2 ΙΣΤΟΡΙΑ ΤΟΥ SPAM

Ενδιαφέρον παρουσιάζει η προέλευση του όρου «spam». Spam ονομάζεται μια κονσέρβα κρέατος, το οποίο αποτέλεσε το κύριο φαγητό του Βρετανικού στρατού από τον Β΄ Παγκόσμιο πόλεμο και μετά. Η ονομασία αυτή προέρχεται από τον συνδυασμό των λέξεων «Spiced» και «Ham» που σημαίνουν πικάντικο ζαμπόν.

Η υπερπροσφορά της ανεπιθύμητη αλληλογραφία σατιρίζεται σε ένα σκετς που έκαναν οι γνωστοί Βρετανοί κωμικοί ‘Monty Python’s’, παρουσιάζοντας ένα ζευγάρι που προσπαθεί να δώσει παραγγελία σε ένα εστιατόριο για να διαπιστώσει πως όλο το μενού του καταστήματος περιέχει spam, δηλαδή συσκευασμένο κρέας σε κονσέρβα από την εταιρία Hormed Foods.

Παρόλο που το σκετς είναι μικρό σε διάρκεια, η λέξη spam ακούγεται τουλάχιστον 94 φορές παράλληλα με το παίξιμο ενός τραγουδιού από μια παρέα Βίκινγκς για το αγαπημένο τους φαγητό, το spam.

Ο κορεσμός της εποχής από το spam συσχετίστηκε με το σύγχρονο φαινόμενο του spam και ο όρος αυτός υιοθετήθηκε για να δηλώσει την δυσαρέσκεια των χρηστών του Διαδικτύου για την υπερφόρτωση του ηλεκτρονικού τους ταχυδρομείου από τα ανεπιθύμητα μηνύματα.

Η συσχέτιση αυτή προκάλεσε την αντίδραση της εταιρίας Hormed Foods, που εισήγαγε την κονσέρβα με το spam στην αγορά από το 1937. Κάθε προσπάθεια που έκανε η εταιρία για να σταματήσει την χρήση του όρου αυτού δεν απέδωσε και συμβιβάστηκε στην διάκριση μεταξύ του ‘spam’ με πεζούς χαρακτήρες που δηλώνει την ανεπιθύμητη αλληλογραφία και του ‘SPAM’ με κεφαλαίους χαρακτήρες που προσδιορίζουν το συγκεκριμένο προϊόν της.

Η πρώτη εμφάνιση της ανεπιθύμητης αλληλογραφίας έγινε το 1978 αλλά παρέμεινε σχετικά ανενεργή μέχρι το 1994 όπου έχουμε τις πρώτες προσεγγίσεις ανεπιθύμητης αλληλογραφίας με σκοπό το οικονομικό κέρδος (commercial spam).

Το 1978,την εποχή που λειτουργούσε το ARPANET, η εταιρία DEC, που σήμερα αποτελεί τμήμα της Hewlett-Packard, έστειλε προσκλήσεις σε όλες τις ηλεκτρονικές διευθύνσεις της δυτικής ακτής των Ηνωμένων Πολιτειών της Αμερικής για την παρουσίαση του νέου της μοντέλου ηλεκτρονικού υπολογιστή. Ωστόσο, η πρακτική αυτή θεωρήθηκε πως παραβίαζε τους κανόνες χρήσης του ARPANET και στάλθηκε απάντηση σε όλους τους χρήστες προκειμένου να τους υπενθυμίσει την υποχρέωση που έχουν να σέβονται το Διαδίκτυο και τους υπόλοιπους χρήστες του[3].

3.3 ΒΑΣΙΚΑ ΓΝΩΡΙΣΜΑΤΑ ΤΟΥ SPAM

Τα μηνύματα spam γίνονται αντιληπτά από κάποια βασικά γνωρίσματα, τα οποία αφορούν τόσο το περιεχόμενο των μηνυμάτων αυτών όσο και την κεφαλίδα τους.

Το κείμενο περιέχει κυρίως διαφημιστικό περιεχόμενο με σκοπό την προώθηση προϊόντων ή υπηρεσιών από επιχειρήσεις με τις οποίες οι παραλήπτες δεν έχουν καμία συναλλαγή και τις περισσότερες φορές, τις αγνοούν παντελώς. Πολλές φορές, τα μηνύματα αυτά περιέχουν διάφορους συνδέσμους (links) οι οποίοι παραπέμπουν τους παραλήπτες σε κάποια άλλη ιστοσελίδα με σκοπό α) να δηλώσουν πως είναι αντίθετοι στην λήψη τέτοιων μηνυμάτων στην ηλεκτρονική τους διεύθυνση ή β) για περισσότερες πληροφορίες για το προϊόν ή την υπηρεσία που διαφημίζεται.

Στις περισσότερες περιπτώσεις όμως, η επιλογή τέτοιου είδους συνδέσμου καθώς και μία απάντηση από τους χρήστες προς αυτό το σύνδεσμο, απλώς επιβεβαιώνει τις ενεργείς ηλεκτρονικές διευθύνσεις των χρηστών και γίνονται στόχοι για την αποστολή περισσότερων spam e-mail μελλοντικά.

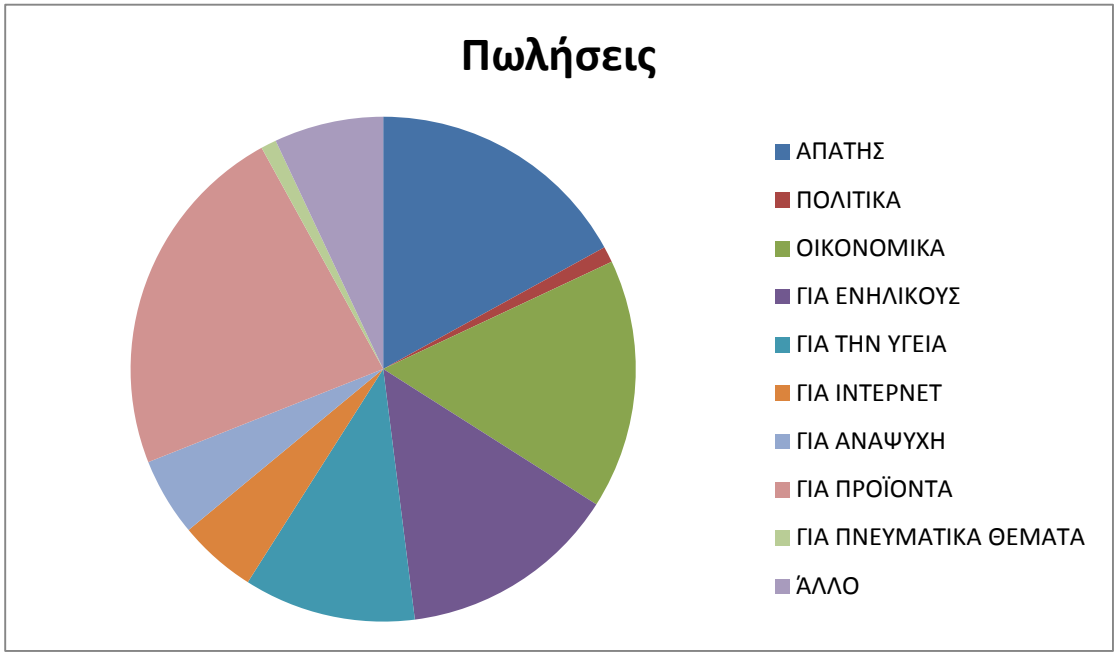
Όσο αφορά την κεφαλίδα αυτών των μηνυμάτων, δηλαδή το τμήμα που δίνει πληροφορίες σχετικά με το θέμα, τον αποστολέα, τους παραλήπτες, παρατηρείται ότι η ηλεκτρονική διεύθυνση είτε ότι δεν υπάρχει και είναι φανταστική είτε ότι έχει δημιουργηθεί μόνο για να χρησιμοποιηθεί στην αποστολή των spam.

Ενδεικτικό είναι και το θέμα του μηνύματος spam. Προκειμένου, να κεντρίσουν το ενδιαφέρον των παραληπτών, οι spammers χρησιμοποιούν φράσεις οι οποίες υπόσχονται κέρδη, προτάσεις γνωριμίας, δωρεάν πορνογραφικό υλικό κ.ο.κ. Πολλές φορές, στη γραμμή του θέματος υπάρχει και η λέξη «Re:» προκειμένου να πεισθούν οι παραλήπτες πως πρόκειται για απάντηση σε e-mail που είχαν στείλει. Φράσεις που χρησιμοποιούνται συχνά ως θέμα είναι «Επείγουσα Ανακοίνωση», «Ακύρωση συνάντησης », «Έκτακτη Ειδοποίηση» κ.λ.π. Σύμφωνα με τα παραπάνω, γίνεται φανερό πως οι spammers βασίζονται

σε πολύ μεγάλο βαθμό στην αφέλεια ορισμένων χρηστών ανάμεσα στον μεγάλο αριθμό παραληπτών ανεπιθύμητων μηνυμάτων που υπάρχει[6].

3.4 ΕΙΔΗ SPAM

Στην έννοια του spam δεν συγκαταλέγονται μόνο τα εμπορικά μηνύματα αλλά μπορεί το περιεχόμενό τους να είναι και πολιτικού, θρησκευτικού, ιδεολογικού, κοινωνικού χαρακτήρα κλπ. Το παρακάτω διάγραμμα δείχνει σε τι ποσοστό δέχονται οι χρήστες του Διαδικτύου μηνύματα spam, ως προς το περιεχόμενό τους[7].



Διάγραμμα 1

Στην συνέχεια, παρουσιάζονται τα βασικότερα είδη των μηνυμάτων spam.

3.4.1 ΑΛΥΣΙΔΩΤΑ E-MAIL

Ένα από τα είδη του spam είναι τα **αλυσιδωτά e-mail**, γνωστά ως **hoaxes**, τα οποία ποικίλλουν στο περιεχόμενό τους. Μπορεί να είναι παραδείγματος χάρη προειδοποίηση για επικίνδυνους ιούς, έκκληση βοήθειας για κάποιο κοινωνικό πρόβλημα, προτάσεις φορολόγησης των δεδομένων που διακινούνται μέσω του Διαδικτύου. Τα μηνύματα αυτά προτρέπουν τους παραλήπτες να στείλουν με την σειρά τους σε μεγάλο αριθμό ατόμων, με μοναδικό δέλεαρ κάποιο χρηματικό έπαθλο ή μια υπόσχεση καλοτυχίας.

Ο όρος hoax χρησιμοποιείται για να περιγράψει κάτι ψεύτικο ή μια απάτη. Πιο ακριβής όμως είναι ο όρος Urban Legend (Αστικός Θρύλος) αφού ένα Hoax είναι στην πραγματικότητα μια φήμη, δηλαδή ένας θρύλος ο οποίος "περιφέρεται" μέσα στο δίκτυο.

Ωστόσο, υπάρχουν τρόποι με τους οποίους μπορούμε να καταλάβουμε αν το μήνυμα που λαμβάνουμε είναι πραγματικό ή απλώς αποτελεί ένα θρύλο του Διαδικτύου. Τρόποι αναγνώρισης είναι οι εξής:

- **Τεχνική Διάλεκτος**: Για να γίνουν πιο αξιόπιστα αυτά τα μηνύματα χρησιμοποιούν επιστημονικούς ή τεχνικούς όρους, οι οποίοι με την πρώτη ανάγνωση φαίνονται σοβαροί, αλλά στην πραγματικότητα δεν σημαίνουν τίποτα.
- **Επίκληση μιας αξιόπιστης πηγής**: Για να αυξήσουν την αξιοπιστία τους, τα hoaxes υποστηρίζουν πως αποτελούν μηνύματα, τα οποία στέλνουν μεγάλοι οργανισμοί όπως είναι η Microsoft. Όμως, αυτοί οι οργανισμοί δημοσιεύουν πάντα τις ανακοινώσεις τους στον Τύπο και δεν εμπιστεύονται εύκολα το e-mail,το οποίο μπορεί και να παραποιηθεί.

- **Προτροπή προώθησης του ίδιου μηνύματος σε τρίτους:** Αυτό είναι το σήμα κατατεθέν των Αστικών Θρύλων. Όποτε κάποιο μήνυμα ζητά να προωθηθεί, είναι σίγουρα μήνυμα hoax.
- **Αδυναμία ελέγχου:** Αν το θέμα του μηνύματος είναι σημαντικό, ο αποστολέας θα έχει δημιουργήσει τουλάχιστον μια web σελίδα με περισσότερες πληροφορίες σχετικά με αυτό. Αν αυτή δεν αναφέρεται στο mail ή αν η διεύθυνσή της είναι "ύποπτη" σημαίνει πως το μήνυμα δεν ανταποκρίνεται στην πραγματικότητα.

Άλλες τεχνικές αναγνώρισης των Hoaxes είναι ο εκφοβισμός ή η χρήση συγκεκαλυμμένων απειλών, η κακή σύνταξη και ορθογραφία (κολλημένες λέξεις, πολλά κεφαλαία), κ.λπ[7].

3.4.2 ΜΗΝΥΜΑΤΑ ΜΕ ΣΚΟΠΟ ΤΟ PHISHING

Ένα είδος ανεπιθύμητου email που εμφανίζεται όλο και πιο συχνά είναι το phishing (ηλεκτρονικό ψάρεμα). Το phishing είναι ένα μήνυμα που αποστέλλεται σε όσες ηλεκτρονικές διευθύνσεις μπορεί να αποκτήσει ο εγκέφαλος της απάτης και φαίνεται ότι προέρχεται από αξιόπιστους οργανισμούς όπως τράπεζες, υπηρεσίες ηλεκτρονικών πληρωμών, ηλεκτρονικά καταστήματα, κλπ. Το μήνυμα αυτό ζητά από τον παραλήπτη να ενημερώσει ή να επαληθεύσει τα προσωπικά και οικονομικά του στοιχεία, όπως ημερομηνία γέννησης, στοιχεία σύνδεσης, στοιχεία λογαριασμού, αριθμούς πιστωτικών καρτών, PIN, κλπ. Πιο αναλυτικά θα παρουσιαστεί το phishing στο επόμενο κεφάλαιο[7].

3.4.3 ΔΙΑΔΙΚΤΥΑΚΕΣ ΑΙΤΗΣΕΙΣ

Αυτές οι αιτήσεις ζητούν από τους παραλήπτες να τις προωθήσουν και σε άλλους αποδέκτες, κρατώντας συγχρόνως τις ηλεκτρονικές τους

διευθύνσεις. Στον τελευταίο αποδέκτη που θα συμπληρώσει τις αιτήσεις, θα ζητηθεί να στείλει αυτές τις αιτήσεις στον αρχικό αποστολέα.

Με αυτόν τον τρόπο, οι αποστολείς τέτοιου είδους spam επιβεβαιώνουν όλες τις υπάρχουσες ηλεκτρονικές διευθύνσεις με ένα μόνο μήνυμα, στις οποίες μετά μπορούν να στείλουν νέα ανεπιθύμητα μηνύματα[3].

3.5 ΤΕΧΝΙΚΕΣ ΠΟΥ ΟΔΗΓΟΥΝ ΣΤΟ SPAM

Οι spammers για να αποφύγουν τις νομικές επιπτώσεις των πράξεών τους, στέλνουν τα μηνύματα spam από ενδιάμεσα συστήματα ηλεκτρονικών υπολογιστών, στα οποία έχουν αποκτήσει πρόσβαση χωρίς να το γνωρίζουν οι νόμιμοι διαχειριστές τους.

Για να καταφέρουν να αποκτήσουν πρόσβαση σε αυτά τα συστήματα, χρησιμοποιούν τεχνικές όπως είναι:

- Hacking: Οι spammers, έχοντας προχωρημένες γνώσεις για τα λειτουργικά περιβάλλοντα, εισέρχονται στα ενδότερα του υπολογιστικού συστήματος και χρησιμοποιούν τους πόρους του π.χ. για την αποστολή ηλεκτρονικών μηνυμάτων, σαν να ήταν οι νόμιμοι χρήστες.
- IP Spoofing: είναι μία τεχνική με την οποία δημιουργούνται TCP/IP πακέτα δεδομένα, τα οποία χρησιμοποιούν άλλη IP διεύθυνση αποστολέα και όχι αυτή από την οποία πραγματικά στέλνονται. Έτσι, οι routers (δρομολογητές) λαμβάνουν υπόψη μόνο την IP διεύθυνση «προορισμού» και όχι την IP διεύθυνση «προέλευσης». Η διεύθυνση προέλευσης θα αποκωδικοποιηθεί και θα παρουσιαστεί μόνο στον τελικό προορισμό ώστε αν χρειαστεί απάντηση να είναι γνωστή η διεύθυνση του αποστολέα.

- Packet sniffing: η τεχνική αυτή επιτρέπει την παρακολούθηση των πακέτων πληροφορίας που κινούνται σε ένα δίκτυο. Στα μη κωδικοποιημένα πακέτα υπάρχει ο κίνδυνος αποκάλυψης ευαίσθητων πληροφοριών των χρηστών όπως είναι διάφορα passwords, e-mails. Για την αντιμετώπιση αυτού του προβλήματος προτείνεται ως λύση η κωδικοποίηση των πληροφοριών.
- Phishing: πρόκειται για μια τεχνική κατά την οποία δημιουργείται ένας παράνομος δικτυακός τόπος, ο οποίος όμως μιμείται σε συμπεριφορά έναν νόμιμο. Έτσι, οι χρήστες επισκεπτόμενοι τον παράνομο δικτυακό τόπο και πιστεύοντας πως κάνουν συναλλαγές με τον πραγματικό δικτυακό τόπο, αποκαλύπτουν διάφορα προσωπικά δεδομένα όπως στοιχεία πιστωτικών καρτών, τραπεζικούς λογαριασμούς κ.α.
- Harassment (Παρενόχληση): έχει σχέση με την αποστολή άσεμνων, προσβλητικών ηλεκτρονικών μηνυμάτων σε πρόσωπα ή ομάδες χρηστών.
- Spam filtering: είναι λογισμικό το οποίο χρησιμοποιείται για να φιλτράρει την διάδοση των μηνυμάτων spam κατά την λήψη μηνυμάτων ηλεκτρονικού ταχυδρομείου.

Ωστόσο, οι spammers χρησιμοποιούν και τεχνικές για την συλλογή ηλεκτρονικών διευθύνσεων καθώς και για την αποστολή του εκάστοτε περιεχομένου. Για την συλλογή των ηλεκτρονικών διευθύνσεων χρησιμοποιούν πολλές μεθόδους, ορισμένες από τις οποίες είναι:

v Από μηνύματα που στέλνονται σε news group (Usenet)

Οι spammers χρησιμοποιούν ειδικά προγράμματα με τα οποία ψάχνουν σε διάφορους διαδικτυακούς τόπους για την εύρεση ηλεκτρονικών διευθύνσεων. Ορισμένα από αυτά τα προγράμματα ψάχνουν τις ηλεκτρονικές διευθύνσεις στην κεφαλίδα του e-mail, στο

σημείο δηλαδή που υπάρχουν οι φράσεις '**From:**' ή '**Reply to**' ενώ άλλα προγράμματα ψάχνουν στο κύριο μέρος των e-mail για την χρήση υπογραφών ή για οτιδήποτε περιέχει το σύμβολο '**@**'.

- **Από λίστες με ηλεκτρονικές διευθύνσεις**

Οι spammers προσπαθούν να πάρουν τις λίστες με τις διευθύνσεις από διάφορους συνδρομητές αφού γνωρίζουν πως οι περισσότερες από τις διευθύνσεις είναι έγκυρες.

Μία ακόμα μέθοδο που χρησιμοποιούν οι spammers είναι να ζητήσουν από κάποιον εξυπηρετητή (server) να τους δώσει την λίστα με τις διευθύνσεις τους (μέθοδος η οποία χρησιμοποιείται συχνά από κάποιους εξυπηρετητές για την ευκολία των νόμιμων χρηστών) και στην συνέχεια να στείλουν αυτοί τα μηνύματα spam σε αυτά τα e-mail.

- **Από Ιστοσελίδες**

Χρησιμοποιούνται αυτοματοποιημένα προγράμματα (spiders), τα οποία ανιχνεύουν τις ιστοσελίδες για διευθύνσεις π.χ. για διευθύνσεις που μπορεί να περιέχονται σε κεφαλίδα της Html.

- **Από sites** τα οποία ζητούν πολλές πληροφορίες μέσω φορμών που χρησιμοποιούν όπως για παράδειγμα σελίδες που ζητούν εγγραφή. Οι spammers μπορούν να βρουν αυτές τις διευθύνσεις είτε γιατί αυτές οι φόρμες είναι διαθέσιμες στο Παγκόσμιο Ιστό είτε γιατί το site πωλεί ή δίνει την λίστα των διευθύνσεων σε άλλους.

- **Από λογισμικά πλοήγησης (web browsers)**

Πολλές φορές, ορισμένα sites προσπαθούν να αποσπάσουν την διεύθυνση του χρήστη καθώς πλοηγείται στο Διαδίκτυο από τον web

server, χωρίς ο ίδιος ο χρήστης να το καταλαβαίνει. Ορισμένες τεχνικές που χρησιμοποιούνται για αυτό τον σκοπό είναι:

1. Η χρήση της κεφαλίδας Http_From που τα web browsers στέλνουν στους εξυπηρετητές. Ορισμένοι browsers στέλνουν και μια κεφαλίδα μαζί με την διεύθυνση του e-mail σε κάθε server (εξυπηρετητή) που επισκέπτονται οι χρήστες,
2. Κάνοντας τον browser να στείλει μια εικόνα της ιστοσελίδας σε ένα ανώνυμο FTP (ανώνυμο πρωτόκολλο μεταφοράς αρχείων) στην ίδια ιστοσελίδα. Ορισμένοι browsers θα μπορούσαν να δώσουν την ηλεκτρονική διεύθυνση του χρήστη ως κωδικό σε αυτό τον ανώνυμο FTP λογαριασμό, ότι δηλαδή έχει εγγραφεί ως μέλος με αυτούς τους κωδικούς. Ο χρήστης ο οποίος δεν είναι ενήμερος με αυτή την τεχνική, δεν θα μπορέσει να καταλάβει ότι έχει παραβιαστεί η ηλεκτρονική του διεύθυνση.

- **Από IRC και chat rooms:**

Πολλοί IRC (Διεθνής Φορέας Εκμετάλλευσης) πελάτες μπορούν να δώσουν τις ηλεκτρονικές διευθύνσεις των χρηστών σε οποιοδήποτε τις ζητήσει. Έτσι, οι spammers παίρνουν τις ηλεκτρονικές διευθύνσεις και γνωρίζοντας πως είναι νόμιμες και ισχύουν, στέλνουν τα μηνύματα spam. Οι χώροι επικοινωνίας, γνωστά και ως chat rooms, αποτελούν επίσης πηγή εύρεσης ηλεκτρονικών διευθύνσεων ειδικότερα όταν εγγράφονται νέοι χρήστες, οι οποίοι δεν έχουν μεγάλη εμπειρία στην αντιμετώπιση των spam μηνυμάτων και έτσι οι spammers μπορούν εύκολα να βρουν τις ηλεκτρονικές τους διευθύνσεις.

Τέλος, πολλές φορές οι spammers επιστρατεύουν και την **τύχη** τους, δοκιμάζοντας για κάθε domain που θέλουν να στείλουν μηνύματα spam, πιθανούς αλλά και λογικούς παραλήπτες. Στέλνουν δηλαδή κάποιο μήνυμα σε λίστα από διευθύνσεις, τις οποίες έχουν οι ίδιοι επινοήσει, και

περιμένουν να τους σταλεί μήνυμα με επιβεβαίωση για το αν ισχύουν ή όχι οι διευθύνσεις αυτές.

Για την αποστολή του περιεχομένου, χωρίς αυτό να μπορεί να εμποδιστεί από τους μηχανισμούς αντιμετώπισης του spam, χρησιμοποιούνται **ψεύτικα και συνεχώς μεταβαλλόμενα στοιχεία αποστολέα (**spoofed e-mail addresses), περιεχόμενο που έχει ενσωματωθεί σε εικόνες, περιεχόμενο ως attachment, τροποποιημένες λέξεις και πολλές άλλες τεχνικές[3].

3.6 ΠΑΡΑΛΛΑΓΕΣ ΤΟΥ SPAM

Μία παραλλαγή του spam είναι το **spim**. Ορίζεται ως «**αυτόκλητο διαφημιστικό μήνυμα**» το οποίο εμφανίζεται μέσω ενός συστήματος παραγωγής στιγμιαίων μηνυμάτων. Η ονομασία αυτή είναι αρκτικόλεξο των **SP**am **I**nstant **M**essage. Το spim προήλθε από την τάση των διαφημιστών να διεισδύουν σε κάθε μέσο που προσεγγίζει τους καταναλωτές. Τα spim παράγονται από προγράμματα, τα οποία λέγονται ‘bots’. Όταν οι χρήστες κάνουν περιήγηση στο διαδίκτυο, μεταφέρονται από τους διακομιστές (servers) που φιλοξενούν τις ιστοσελίδες, μέρη του λογισμικού που δημιουργεί τα spim στους υπολογιστές τους, σε ελκυστική μορφή δηλαδή με γραφικά, ήχο κτλ σε προκαθορισμένο ή τυχαίο «παράθυρο» της οθόνης. Το περιεχόμενο των μηνυμάτων αυτών είναι παρόμοιο με αυτό της ιστοσελίδας που τα δημιούργησε, αφού οι διαφημιστές πιστεύουν πως η περιήγηση σε μια σελίδα υποδηλώνει ενδιαφέρον για παρόμοια θέματα, με αυτά που παρουσιάζονται σε αυτήν. Επίσης, παραλλαγές του spam έχουν εμφανιστεί στις ιστοσελίδες που λειτουργούν ως forum για την καταγραφή on-line συζητήσεων. Αυτή η μορφή ονομάζεται **link spamming** και δεν έχει τον χαρακτήρα της αποστολής ομαδικών μηνυμάτων.

Το spam έχει πλέον αποκτήσει τον κλώνο του και στην **κινητή τηλεφωνία.** Οι περισσότεροι χρήστες το διαπιστώνουν στην πιο συνηθισμένη του μορφή, μέσω δηλαδή ενός σύντομου γραπτού μηνύματος SMS, MMS ή ηλεκτρονικού μηνύματος, το οποίο διαφημίζει κάποια υπηρεσία. Τα μηνύματα αυτά προέρχονται από χώρες όπου η τιμή χρέωσης είναι πολύ χαμηλότερη για προορισμούς όπως είναι η Ευρώπη. Με τα MMS δίνεται η ευκαιρία σε επιτήδειους να κάνουν χρήση απλών φωτογραφιών ή και μικρών σε διάρκεια βίντεο με ένα μήνυμα και να διαφημίζουν ένα ταξίδι σε κάποιο νησί του Ειρηνικού, ενώ ο ήχος της θάλασσας αναπαράγεται την ίδια στιγμή από το κινητό. Πολλές φορές, συνοδεύονται και από διασυνδέσεις σε ιστοσελίδες του Διαδικτύου όπου ο πελάτης μπορεί να δει με λεπτομέρειες το διαφημιζόμενο προϊόν.

Ωστόσο, υπάρχει και μια δεύτερη μορφή, η οποία είναι γνωστή ως **scam**. Μπορεί να είναι είτε για αναπάντητες κλήσεις από προορισμό με υψηλή τιμολόγηση είτε για σύντομο γραπτό μήνυμα το οποίο χρεώνει τον λήπτη με υψηλή τιμολόγηση. Πρόκειται ουσιαστικά, για μια προσπάθεια δημιουργίας παράνομου κέρδους που είναι αποτέλεσμα παραπλανητικών προσπαθειών ώθησης του χρήστη να απαντήσει σε κλήσεις ή μηνύματα που δεν γνωρίζει τον αποστολέα και οι οποίες δεν είναι κατ’ ανάγκη εμπορικού-διαφημιστικού χαρακτήρα[7].

Για παράδειγμα, η διάρκεια της εισερχόμενης κλήσης σε ένα κινητό τηλέφωνο ρυθμίζεται, έτσι ώστε ο χρήστης να μην προλάβει να απαντήσει. Εμφανίζεται έτσι μια αναπάντητη κλήση στην οθόνη του κινητού. Όταν ο χρήστης καλέσει τον αριθμό της αναπάντητης κλήσης, δεν γνωρίζει πως η κλήση του κατευθύνεται σε γραμμή αυξημένης χρέωσης. Ο απαντών θα προσπαθήσει να κρατήσει στην γραμμή τον χρήστη όση περισσότερη ώρα μπορεί, προκειμένου να μεγιστοποιήσει τα κέρδη του.

Ανάλογη είναι και η περίπτωση όπου ο χρήστης λαμβάνει ένα SMS του οποίου το περιεχόμενο περιλαμβάνει μια πρόσκληση για να πληκτρολογήσει τον αριθμό που βρίσκεται σε αυτό. Άλλες φορές, ο λήπτης του μηνύματος καλείται να απαντήσει στο περιεχόμενό του, όπου ο προορισμός του έχει υψηλή χρέωση. Επίσης, ο λήπτης του μηνύματος καλείται αν θέλει να απαλλαγεί από την λήψη παρόμοιων μηνυμάτων, να στείλει κάποιο γραπτό μήνυμα σε προορισμό αυξημένης χρέωσης[7].

ΚΕΦΑΛΑΙΟ 4

ΑΠΕΙΛΕΣ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΔΙΚΤΥΩΝ ΚΑΙ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΤΑΧΥΔΡΟΜΕΙΟΥ

4.1 SPOOFING

Το spoofing χωρίζεται σε τέσσερεις κατηγορίες: IP spoofing, ARP spoofing, DNS spoofing και SMTP spoofing. Ο όρος spoofing αναφέρεται στην αλλαγή της διεύθυνσης IP (συνήθως), έτσι ώστε ο χρήστης που λαμβάνει ένα e-mail να νομίζει ότι το λαμβάνει από έναν έγκυρο χρήστη, ενώ στη πραγματικότητα δεν είναι έτσι. Το spoofing βασίζεται στο “social engineering” και ουσιαστικά ο “Hacker” προσπαθεί να χειραγωγήσει το θύμα του, δίνοντάς του τη ψευδαίσθηση ότι είναι κάποιος άλλος στον οποίο το θύμα θα εμπιστευόταν τα προσωπικά του δεδομένα. Εκτός αυτού το spoofing χρησιμοποιείται και για επιθέσεις άρνησης υπηρεσιών (DoS – Denial of Service), όπου οι επιθέσεις αυτού του είδους έχουν ως στόχο να γεμίσουν τον υπολογιστή-θύμα με πολλά πακέτα ώστε να τον αναγκάσουν να περιέλθει σε δυσλειτουργία και να μην μπορεί να εξυπηρετήσει σωστά τους νόμιμους χρήστες του.

Τέλος, ακόμα και για το σπάσιμο των μηχανισμών ασφαλείας δικτύων υπολογιστών, όπου σε πολλά εταιρικά δίκτυα είναι συνηθισμένο η αναγνώριση των χρηστών να γίνεται μέσω των IP διευθύνσεών τους. Στη συνέχεια θα αναφέρουμε μερικά παραδείγματα Spoofing για να κατανοήσουμε ακριβώς πως δουλεύει[7].

4.1.1. IP SPOOFING

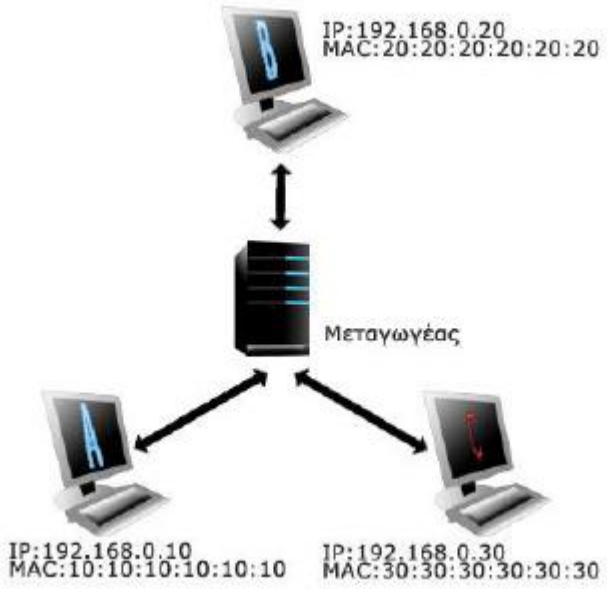
Όταν δύο υπολογιστές ανοίγουν μία σύνδεση μεταξύ τους χρησιμοποιώντας TCP/IP ακολουθείται η παρακάτω διαδικασία:

Ο πρώτος στέλνει ένα TCP πακέτο με έναν αρχικό ακέραιο αριθμό. Ο λαμβάνων υπολογιστής επιστρέφει ένα πακέτο το οποίο περιλαμβάνει έναν άλλο ακέραιο (οι αριθμοί αυτοί είναι γνωστοί ως αριθμοί ακολουθίας). Επίσης στέλνει μια επιβεβαίωση η οποία είναι ο αριθμός ακολουθίας του πρώτου συν ένα. Ο πρώτος στη συνέχεια πρέπει να επιστρέψει μια επιβεβαίωση η οποία περιλαμβάνει τον αριθμό ακολουθίας στον άλλο. Από τη στιγμή αυτή, ο πελάτης και ο διακομιστής στέλνουν πακέτα τα οποία περιέχουν αριθμούς ακολουθίας τους οποίους η άλλη πλευρά πρέπει να επιστρέψει για να πιστοποιήσει ότι είναι αυτή που ισχυρίζεται. Οι αριθμοί αυτοί προσδιορίζονται από έναν αλγόριθμο του TCP/IP. Ο εισβολέας για να πετύχει το IP spoofing πρέπει να γνωρίζει τους αριθμούς ακολουθιών που έχουν δημιουργηθεί από τους άλλους δύο υπολογιστές. Οπότε για να αποδειχθεί επιτυχημένη μία τέτοια απόπειρα IP spoofing ο εισβολέας πρέπει να ξεπεράσει τα εξής εμπόδια[2]:

- Ο πραγματικός υπολογιστής που θα προσποιηθεί ότι είναι, θα πρέπει να είναι εκτός λειτουργίας. Συνήθως αυτό το πετυχαίνει με μια επίθεση DoS (άρνησης υπηρεσιών).
- Ο υπολογιστής του εισβολέα θα πρέπει να πάρει τη διεύθυνση του υπολογιστή που θα προσποιηθεί και να συνδεθεί με τον διακομιστή για να ξεκινήσει έναν διάλογο προσποιούμενος ότι είναι κάποιος άλλος υπολογιστής.
- Ο εισβολέας πρέπει να ανακαλύψει τον αριθμό ακολουθίας που έχει δημιουργήσει ο διακομιστής. Από τη στιγμή που κάνει τα παραπάνω η συνέχεια είναι πολύ πιο εύκολη.

4.1.2. ARP SPOOFING (ADDRESS RESOLUTION PROTOCOL)

Το ARP είναι το κομμάτι του TCP-IP, που συνδέει τις φυσικές διευθύνσεις των υπολογιστών (π.χ. της κάρτας δικτύου) με τις IP διευθύνσεις. Η επίθεση ARP spoofing πραγματοποιείται μεταβάλλοντας την ARP cache (τμήμα του λειτουργικού συστήματος το οποίο αποθηκεύει τα απαραίτητα στοιχεία για να γίνεται η μετατροπή των διευθύνσεων από φυσικές σε IP), ώστε η IP διεύθυνση ενός υπολογιστή που ο διακομιστής εμπιστεύεται στην πραγματικότητα να ισοδυναμεί με τη φυσική διεύθυνση του υπολογιστή του εισβολέα. Για να πραγματοποιηθεί όμως μια τέτοια επίθεση, ο Cracker θα πρέπει να βρίσκεται στο ίδιο δίκτυο με αυτόν που θέλει να εξαπατήσει.



Στο παραπάνω παράδειγμα βλέπουμε πως ο Cracker C προσπαθεί να εξαπατήσει τους χρήστες A και B. Σκοπός του C είναι να «μπει ανάμεσα» από τον A και τον B, όπου για να το πετύχει αυτό στέλνει πακέτα ARP στον A με διεύθυνση πρωτοκόλλου 192.168.0.30 και διεύθυνση MAC 30:30:30:30:30:30. Με τον ίδιο τρόπο εξαπατά και τον B. Οπότε όταν οι A και B θα θέλουν να ανταλλάξουν αρχεία θα χρησιμοποιούν τη διεύθυνση MAC του C (παράδειγμα ανταλλαγής

μηνυμάτων μεταξύ Α και Β δηλαδή C, 192.168.0.20 à 30:30:30:30:30:30). Παρόλα αυτά για να μη γίνει αντιληπτός ο C θα πρέπει να προωθεί τα μηνύματα που δεν απευθύνονται σε αυτόν, στον νόμιμο παραλήπτη τους. Έτσι, οι δύο χρήστες δεν θα καταλάβουν ότι η επικοινωνία τους παρακολουθείται[2].

4.2 PHISHING

Η λέξη phishing είναι παραλλαγή της λέξης Fishing (ψάρεμα) και η πράξη phishing κάνει αυτό ακριβώς που υποδηλώνει η λέξη. Επίσης, το phishing είναι «υποενότητα του spam», αλλά είναι τόσο μεγάλη που αποτελεί απειλή από μόνη της.

Phishing είναι η πρακτική αποστολής ενός μηνύματος ηλεκτρονικού ταχυδρομείου ή ενός στιγμιαίου μηνύματος (εμάς μας αφορά το πρώτο κυρίως) που μοιάζει να προέρχεται από μία πραγματική εταιρία με καλή φήμη (όπως π.χ. τράπεζες, Pay pal, eBay κ.α.) αλλά δεν είναι. Σκοπό έχει να μας ξεγελάσει σαν χρήστες και να μας κάνει να αποκαλύψουμε ευαίσθητα προσωπικά στοιχεία όπως είναι ο αριθμός της πιστωτικής μας κάρτας, pin, ή οτιδήποτε άλλο μπορούν να εκμεταλλευτούν για να κάνουν στη συνέχεια συναλλαγές στις οποίες θα έχουν πρόσβαση σαν να ήταν οι νόμιμοι χρήστες. Υπάρχουν αρκετοί τρόποι για να κάνουν αυτή τη πράξη οι κακόβουλοι χρήστες. Θα παραθέσουμε ορισμένους τώρα και θα δούμε ποιοι είναι πιο αποτελεσματικοί:

- Μπορούν να μας στείλουν ένα e-mail και να φαίνεται πως το στέλνει (π.χ. η τράπεζά μας) και να μας ζητάει να επαληθεύσουμε τα στοιχεία μας για λόγους ασφαλείας.
- Επίσης με e-mail που μας στέλνει «η τράπεζά μας» πάλι μπορεί να μας λέει ότι έχουμε πρόβλημα με το λογαριασμό μας και να πρέπει

να δώσουμε άμεσα τα προσωπικά μας στοιχεία για να μη μας κλείσουν τον λογαριασμό μας. Με αυτό τον τρόπο ο κακόβουλος χρήστης προσπαθεί να μας αγχώσει ώστε να μη προλάβουμε να επαληθεύσουμε το ηλεκτρονικό μήνυμα.

- Μία άλλη ποιο έξυπνη λύση είναι, να μας στείλουν ένα e-mail το οποίο να μας προσφέρει (λέγοντάς μας πως κερδίσαμε) μία εκδρομή για παράδειγμα και να μας ζητάει τον αριθμό της πιστωτικής μας κάρτας για τα μεταφορικά και μόνο.
- Θα μπορούσε να είναι επίσης σαν χριστουγεννιάτικη προσφορά από κάποιον οργανισμό όπως το eBay και να πρέπει να βάλουμε τα προσωπικά μας στοιχεία για να μπούμε άμεσα σε αυτή τη προσφορά.

Υπάρχουν φυσικά και άλλες επιθέσεις, αλλά αυτές είναι οι πιο συχνές. Τώρα ας αναφέρουμε και ποιες μέθοδοι είναι οι πιο αποτελεσματικές.

Σε γενικές γραμμές, η δεύτερη τεχνική δεν είναι ιδιαίτερα αποτελεσματική διότι είναι δυσάρεστα νέα για εμάς ως αναγνώστες, οπότε θα το μελετήσουμε περισσότερο και πιθανό να τηλεφωνήσουμε στη τράπεζά μας για περαιτέρω πληροφορίες. Αυτό έχει ως συνέπεια να μας ενημερώσουνε ότι πρόκειται για εξαπάτηση και να το αποφύγουμε. Για να καταπολεμήσουν αυτό το πρόβλημα οι crackers μας δίνουν ένα πολύ μικρό χρονικό περιθώριο ώστε να μην μπορέσουμε να το σκεφτούμε ή να το μελετήσουμε και να προβούμε στις κινήσεις που μας ζητάνε. Η τρίτη λύση είναι η πιο έξυπνη από όλες, διότι τα ευχάριστα νέα είναι πιο εύπεπτα και άμεσα εμείς ως χρήστες για να μη χάσουμε τη προσφορά «τρέχουμε» να δώσουμε τα προσωπικά μας στοιχεία. Αυτό επίσης έχει το καλό ότι μπορούμε να το διασταυρώσουμε πιο δύσκολα και είναι πολύ πιθανό να δώσουμε τα προσωπικά μας δεδομένα. Το πρώτο και το τέταρτο δεν έχουν καμία ιδιαιτερότητα αλλά από ότι

βλέπουμε και από ότι θα δούμε από τα παραδείγματα στη συνέχεια λειτουργούν και αυτά εξ ίσου καλά.

Το phishing παλιά δεν αποτελούσε απειλή αλλά τα τελευταία χρόνια έχει αρχίσει να γίνετε μάστιγα, αυτό επιβεβαιώνεται και από μία έρευνα που διεξήχθη το 2007 και έδειξε πως ένα στα 87 e-mails είναι phishing mail. Επίσης τα τελευταία χρόνια οι crackers έχουν καταφέρει να κάνουν πολύ πιστές αντιγραφές στα web sites με τα οποία έχουν σκοπό να «ψαρέψουν» και τρανταχτό παράδειγμα είναι το eBay όπου ένας hacker έστειλε ένα υποτιθέμενο χριστουγεννιάτικο e-mail σε χρήστες και όταν ένας το έκανε προώθηση στο e-bay για να τους πει πως πρόκειται για phishing το eBay του είπε πως κάνει λάθος και όντως έστειλε στα μέλη του τέτοιο e-mail. Παρακάτω θα διαβάσετε την προσωπική εμπειρία του χρήστη:

Στα τέλη Νοεμβρίου, ο Richi Jennings, ανεξάρτητος ερευνητής που μελετά θέματα ασφαλείας και διαδικτυακής απάτης, έλαβε ένα e-mail με θέμα "Christmas is Coming on ebay.co.uk" (Τα Χριστούγεννα έρχονται στο ebay.co.uk). Το μήνυμα προσέφερε συμβουλές για επιτυχημένες χριστουγεννιάτικες αγορές και παρέπεμπε στο site ebaychristmas.net. Στο συγκεκριμένο site ο Jennings είδε ότι πρέπει να εισάγει το username και το password που χρησιμοποιεί στο eBay, καθώς και το όνομα και το password για το e-mail του.

Αντιλαμβανόμενος ότι η όλη κατάσταση φαινόταν τουλάχιστον ύποπτη, ο Jennings ανέφερε στο eBay την ύπαρξη του συγκεκριμένου e-mail στις 25 Νοεμβρίου. Η εταιρεία απάντησε τέσσερις μέρες αργότερα πως πρόκειται για πραγματικό e-mail που είχε σταλεί εκ μέρους της εταιρείας στον ίδιο. Ωστόσο, ο Jennings πεπεισμένος για την απάτη έστειλε νέο e-mail στο eBay τονίζοντας και πάλι την προσπάθεια εκμετάλλευσης αθώων χρηστών. Τη Δευτέρα 5 Δεκεμβρίου, εκπρόσωπος του eBay επιβεβαίωσε ότι πράγματι το συγκεκριμένο e-mail ήταν ψευδές,

ωστόσο δεν μπόρεσε να δώσει ξεκάθαρη απάντηση για τους λόγους που δεν εντοπίστηκε η απάτη από το πρώτο e-mail του Richi Jennings.

Είναι πολύ πιθανό η ομάδα έρευνας απάτης του eBay να ξεγελάστηκε από άλλο παρόμοιο e-mail που είχε στείλει η εταιρεία και να μην έδωσε την απαιτούμενη προσοχή στην παρατήρηση του Jennings. Μάλιστα, το eBay τόνισε πως ήδη από τις 8 Νοεμβρίου - αρκετές ημέρες πριν την πρώτη επικοινωνία του Jennings – γνώριζε για το συγκεκριμένο site και είχε κινήσει διαδικασίες για την αναστολή λειτουργίας του. Η αδυναμία του eBay να εντοπίσει μία phising απάτη, ακόμη και τη στιγμή που έλαβε στοιχεία για αυτήν, δείχνει πόσο προσεγμένες έχουν γίνει οι επιθέσεις του είδους και τη δυσκολία να τις εντοπίσει πλέον κάποιος από την πρώτη στιγμή. Όσο για τον Richi Jennings, παραθέτει την εκτεταμένη άποψή του για το θέμα στο blog του (http://richi.co.uk/blog/2005/12/ebays-anti-phishing-desk-sucks.html) και δηλώνει πρόθυμος να δώσει στο eBay μία δεύτερη ευκαιρία.

Ο λόγος που καταφέρνουν να κάνουν τόσο πιστές αντιγραφές είναι, ότι αντιγράφουν τον κώδικα της σελίδας και αλλάζουν μόνο τα σημεία τα οποία τους ενδιαφέρουν ώστε να πάρουν τα προσωπικά δεδομένα του χρήστη. Η Ελλάδα ευτυχώς, λόγο της δυσκολίας που έχει η γλώσσα της, είναι αρκετά προστατευμένη από τέτοιες επιθέσεις αλλά όχι απόλυτα. Αυτό δείχνει και η επίθεση ενός phishing mail που υποτίθεται ότι το έστελνε η City bank στους πελάτες της και ήταν το εξής:

Κλεισιματος των λογαριασμων και περιοριζοντας την προσβαση στο λογαριασμο Ο λογαριασμος σας εχει **Limited**. Εμεις που αναθεωρηθηκε προσφατα στοιχεια της πιστωτικης σας καρτας, και φαινεται οτι χρησιμοποιειτε την ιδια πιστωτικη καρτα για 2 λογαριασμους. Οπως μπορειτε να διαβασετε και μας **User Agreement** (τμημα 2.13) δημιουργια πολλαπλων λογαριασμων ειναι αυστηρα απαγορευμενη. Ειστε τωρα καλειται να παρασχει πληροφοριες σχετικα με το λογαριασμο σας. **CitiBank** θα διερευνησει το θεμα γρηγορα και αν η ερευνα ειναι υπερ σας, θα αποκαταστησει το λογαριασμο σας.
Καντε κλικ εδω για να επαναφερετε το λογαριασμο σας

Η απαράδεκτη σύνταξη του κειμένου δείχνει πως το έγραψε κάποιος που δεν γνωρίζει καλά ελληνικά ή έγινε η μετάφραση από αυτόματο μεταφραστή. Επίσης στάλθηκε και σε χρήστες που δεν διαθέτουν λογαριασμό ούτε κάρτα σε αυτή την τράπεζα. Προφανώς κάποιοι έστειλαν δεκάδες χιλιάδες e-mail ελπίζοντας πως κάποιοι θα κάνουν click στην παραπομπή ώστε να επαναφέρουν το λογαριασμό τους, δίνοντας έτσι τα προσωπικά τους στοιχεία στους πονηρούς αποστολείς του μηνύματος. Τη προηγούμενη μέρα ο ίδιος χρήστης έλαβε άλλο ένα παρόμοιο μήνυμα:

Αγαπητε πελατη

Μπορειτε εχουν βραβευθει με κουπονι για 100 eur.

Δωροεπιταγη code: 11245325932

για να συλλεξουμε παρακαλω συνδεθειτε και να εισαγετε το κωδικο κουπονιου παραπανω.

Παρακαλω επιτρεψτε 3-5 μερες για μεταποιηση.

Copyright © winbank 2008

Ευτυχώς όπως βλέπουμε ακόμα είναι εύκολο να καταλάβουμε πότε είναι απάτη κυρίως από το συντακτικό και την ορθογραφία, το θέμα είναι για πόσο ακόμα;

Ένα τελευταίο παράδειγμα phishing είναι αυτό που είχαν κάνει χρησιμοποιώντας ως πρόφαση την Alpha bank και ήταν το εξής:

"Αγαπιτέ πελάτη της Ιντερνέτ-Τράπεζας!

Επειδή η κατάσταση με Online - Τράπεζες στη χώρα μας είναι σήμερα πολύ δύσκολη, η κυβέπνιση της Ελλάδας παρακάλησέ μας να κάνουμε τον έλεγχο για όλους τους Online - λογαριασμούς της δηκής ! μας τράπεζας να μάθουμε αν υπάρχουν "λογαριασμοί μιας μέρας", τους οποίους χρησημοποιούν οι εγκληματίες για να αποπλύνονται τα κλεμμένα λεφτά. Δια ταυτα σας παρακαλούμε πολύ &sigm! a;οβαρά να συμ& pi;ληρώσετε το ερωτηματολόγιο της επιβεβαιώσεις λόγαριασμού στη επίσημη μας Ιντερμετ-σελήδα.

Οι λογαριασμοί, που δε θα επιβεβαιοθούν ως της 27.11.05, θα παγώνονται για ακαθόριστο καιρό πριν γίνει φανερό πως ακριβώς έχουν δημιουργηθεί και εκμεταλευθεί. Ο έλεγχος αυτος είν&alph! a;ι επίκαιρος οχι μόνο για ιδιωτικούς μας πελάτες, αλλα για όλους σας.

ΝΑ ΣΥΜΠΛΗΡΩΣΩ ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ

Σας ζητούμε συγνώμη για τις ενοχλήσεις που προκύπται απο τη διαταγή της παρούσες εκδήλωσης και ελπίζουμε για την κατανόηση και την βοήθειά σας.

Με σεβασμό,

Υπηρεσία ασφάλειος

Τράπεζα Alpha Bank"

Το link "ΝΑ ΣΥΜΠΛΗΡΩΣΩ ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ" οδηγεί σε δικτυακό τόπο. Και εδώ φαίνεται η πολύ κακή μετάφραση από τους αυτόματους μεταφραστές που χρησιμοποιούνε οι crackers. Αυτό που ξανά τονίζουμε είναι πως οι μεταφραστές θα βελτιωθούν οπότε δεν πρέπει να επαναπαυόμαστε και πρέπει να βρούμε τρόπους για να αποφύγουμε το phishing[1].

4.2.1 ΠΩΣ ΜΠΟΡΟΥΜΕ ΝΑ ΠΡΟΣΤΑΤΕΥΘΟΥΜΕ ΑΠΟ ΤΟ PHISHING;

Δεν είναι καθόλου εύκολη και απλή υπόθεση να προστατευθεί κανείς από το phishing και αυτό έγκειται στο ότι το phising δεν πάει να χτυπήσει Hardware, δηλαδή σύστημα του υπολογιστή μας, οπότε ένα καλό antivirus να μας προστατεύσει, αλλά χτυπάει κατευθείαν στον χρήστη και στη ψυχολογία του. Αυτό σημάνει πως το κρίσιμο σημείο ασφάλειας δεν βρίσκετε πια στον υπολογιστή αλλά βρίσκεται επάνω μας. Ότι χειρότερο και αυτό φαίνεται από τα λόγια ενός πολύ γνωστού social engineer hacker του Kevin Mitnick ο οποίος όταν βγήκε από τη φυλακή εξέδωσε ένα βιβλίο τονίζοντας την εξής φράση. *«Ο άνθρωπος είναι ο πιο αδύναμος κρίκος σε οποιοδήποτε σύστημα ασφαλείας»*. Παρόλα αυτά θα αναφέρουμε μερικούς τρόπους που μπορούν να μειώσουν τις πιθανότητες εξαπάτησής μας, αλλά σε αυτού του είδους τις απάτες το σημαντικότερο όλων είναι η σωστή ενημέρωσή μας και η αυτοσυγκράτησή μας[1].

4.2.2 ΤΡΟΠΟΙ ΑΠΟΦΥΓΗΣ ΕΞΑΠΑΤΗΣΗΣ PHISHING

- Πρέπει να είμαστε σίγουροι ότι τα λειτουργικά μας συστήματα έχουν τις τελευταίες ενημερώσεις στα προγράμματα ασφαλείας αλλά και γενικότερα στα βασικά τους προγράμματα λειτουργίας όπως π.χ. στα windows, είναι απαραίτητο το service pack 2 ή και 3, διότι εμποδίζει την εμφάνιση πλαστογραφημένων διευθύνσεων.
- Μπορούμε να ρυθμίσουμε τα φίλτρα του Outlook (αν χρησιμοποιούμε) ώστε να φιλτράρει τα phishing mails προτού φτάσουν σε εμάς. Φυσικά, όπως προείπαμε, επειδή είναι ιδιαίτερη η κατηγορία phishing ίσως τα φίλτρα να κριθούν ελαφρός αναποτελεσματικά.

- Το κυριότερο όλων να είμαστε ενήμεροι και να συνεχίζουμε να ενημερωνόμαστε, διότι με τον καιρό αλλάζει και ο τρόπος που γίνονται οι επιθέσεις.
- Να ελέγχουμε τις πηγές από όπου λαμβάνουμε τα e-mail μας και να είμαστε πάντα υποψιασμένοι. Επίσης, να κοιτάμε αν είναι secure οι διευθύνσεις στις οποίες μας πηγαίνουνε τα διάφορα links από τα e-mail και αυτό φαίνεται από το https (το τελευταίο s υποδηλώνει το secure). Άλλο ένα είναι το «λουκέτο» που εμφανίζεται πάνω δεξιά στη διεύθυνση, το οποίο δείχνει πως η ιστοσελίδα χρησιμοποιεί κάποιο πιστοποιητικό.

Τέλος, για την ασφάλεια ψάχνουν τρόπο και οι μεγάλοι οργανισμοί όπως οι τράπεζες, Microsoft, eBay κ.α. διότι πια τα πλήγματα από το phishing αρχίζουν να διευρύνονται και χρειάζεται κινητοποίηση και από τους μεγάλους οργανισμούς[1].

4.3 DNS SPOOFING

Η λιγότερο σημαντική επίθεση από όλες είναι η DNS Spoofing όπου ο Cracker μεταβάλει τα στοιχεία ενός DNS Server ώστε να αντιστοιχεί το συμβολικό όνομα κάποιου υπολογιστή που εμπιστεύονται οι χρήστες, στην IP διεύθυνση ενός υπολογιστή που χρησιμοποιείται από τον εισβολέα. Οπότε, οι υπολογιστές που προσπαθούν να συνδεθούν με τον υπολογιστή που εμπιστεύονται θα συνδέονται στην πραγματικότητα με κάποιον άλλο υπολογιστή, κατά τη διάρκεια της επικοινωνίας με τον οποίο θα μπορούσαν να αντληθούν σημαντικά δεδομένα[7].

4.3.1 SPOOFING ΜΕΣΩ SMTP

Το SMTP standard όσο παράξενο και αν φαίνεται, δεν παρέχει κάποια ασφάλεια (RFC 2821) και με αυτό τον τρόπο οποιοσδήποτε μπορεί να αλλάξει το πεδίο From: του ηλεκτρονικού μηνύματος. Τώρα θα δούμε την απλούστερη μορφή μιας τέτοιας επίθεσης σε βάθος. Για αρχή ο Cracker ανοίγει μια σύνδεση στην πόρτα επικοινωνίας του SMTP (tcp-25) server του θύματος και δίνει τις εξής εντολές:

```
[Cracker]   telnet victims.mailserver.org
[Server]    220 victims.mailserver.org
[Cracker]   hello asxeto.org
[Server]    250  victims.mailserver.org  Hello  asxeto.gr  [Crackers  IP
sender], pleased to meet you
[Cracker]   rcpt to:victim@mailserver.org
[Server]    250 victim@mailserver.org …Recipient ok
[Cracker]   data
[Server]    354 Enter mail, end with "." On a line by itself
[Cracker]   From: your.boss@mailserver.org
```

```
[Cracker]   To: victim@mailserver.org
```

```
[Cracker]   Subject: Παρακαλώ στείλε μου το password
[Cracker]   <μια κενή γραμμή>
[Cracker]   Γεια σου εργαζόμενέ μου. Έξχασα το password για το banking
application και δεν έχω πρόσβαση στο εταιρικό δίκτυο. Παρακαλώ στείλε μου
το password στο hotmail account μου που είναι boss123@hotmail.com
[Cracker]   ευχαριστώ
[Cracker]   <CR><LF>.<CR><LF>
[Server]    250 Message accepted for delivery
(η τελευταία ακολουθία είναι ένα Enter, μία τελεία και μετά πάλι ένα
Enter.)
```

Μέσα από αυτό τον κώδικα βλέπουμε πως τα στοιχεία που εμφανίζονται στον mail client μας (π.χ. Outlook 2003) είναι αυτά που καταχωρήθηκαν μετά το **DATA**. Έτσι, αφού ο Cracker άλλαξε το From: ώστε να φαίνεται το αφεντικό του θύματος προσέχοντας να βάλει το mailserver.org μιας και δεν θα μπορούσε να είναι άσχετο το e-mail του recipient (θα ήταν ανώφελο να προσπαθήσει να κάνει spoofing στον mail server της Microsoft και σαν παραλήπτη να έβαζε κάποιο χρήστη του οποίου το email τελειώνει σε @asxeto.net) και επειδή δεν είναι σίγουρο αν θα μπορεί να διαβάσει τα μηνύματα που θα στείλει το θύμα στο «αφεντικό» του, προσπαθεί να τον εξαπατήσει ζητώντας να λάβει την απάντηση στο web mail του.

Ας δούμε τώρα τις πληροφορίες που προστίθενται στο Header ενός e-mail κατά την αποστολή του και τι σημαίνουν. Πριν όμως πάμε, πρέπει να πούμε ότι αυτό είναι ένα απλουστευμένο παράδειγμα μιας και το e-mail είναι πολύ πιθανό να μη φτάσει από τον έναν υπολογιστή άμεσα στον άλλο και να πρέπει να περάσει από πολλούς mail servers μέχρι να καταλήξει στον τελικό, οπότε και θα έχει προστεθεί αρκετή παραπάνω πληροφορία. Το σημαντικό όμως είναι ότι τα σημαντικά στοιχεία που θα πούμε παραμένουν ίδια.

Ανάλυση του Internet Header:

Microsoft Mail Internet Headers Version 2.0

Αυτός ο Header μπαίνει από το Outlook του αποστολέα

Received: from mail.litwareinc.com ([10.54.108.101]) by mail.proseware.com with Microsoft SMTPSVC(6.0.3790.0);
Wed, 15 Dec 2004 13:39:22 -0800

Αυτός ο Header μας ενημερώνει πως κάποιος υπολογιστής με όνομα mail.litwareinc.com πήρε μήνυμα από τον υπολογιστή με όνομα

mail.proseware.com στις 13:39:22 την 15η Δεκεμβρίου 2004 (Λογικά αυτοί οι δύο υπολογιστές είναι mail servers).

Received: from mail ([10.54.108.23] RDNS failed) by mail.litware.com with Microsoft SMTPSVC(6.0.3790.0);

Wed, 15 Dec 2004 13:38:49 -0800

Αυτός ο header μας ενημερώνει πως με τη σειρά του, ο mail.litware.com πήρε το μήνυμα από κάποιον υπολογιστή με όνομα mail στις 13:38:49 την 15η Δεκεμβρίου 2004. Από τη στιγμή που στη συνέχεια δεν έχουμε κάποιο άλλο Header που να ξεκινάει με "Received:", θεωρούμε πως ο υπολογιστής με όνομα mail και διεύθυνση IP 10.54.108.23 είναι ο υπολογιστής από τον οποίο ξεκίνησε το μήνυμα (αν και αυτό δεν ισχύει πάντα μιας και υπάρχουν τρόποι απόκρυψης του υπολογιστή που αρχικοποιεί το μήνυμα).

From: "Kelly Weadock" kelly@litware.com

Ο συγκεκριμένος header μας ενημερώνει πως το μήνυμα φαίνεται να έχει έρθει από κάποιο χρήστη με διεύθυνση e-mail kelly@litware.com

To: <anton@proseware.com>

Εδώ βλέπουμε το όνομα του παραλήπτη του μηνύματος.

Subject: Review of staff assignments

Αυτός ο header περιέχει το subject του μηνύματος.

Date: Wed, 15 Dec 2004 13:38:31 -0800

Ο συγκεκριμένος header περιέχει την ημερομηνία που ο αποστολέας έστειλε το μήνυμα. Η ημερομηνία αυτή έγινε generate στον υπολογιστή του αποστολέα, έτσι αν ο αποστολέας είχε λανθασμένη ημερομηνία στον υπολογιστή του αυτό θα φανεί στο συγκεκριμένο header.

MIME-Version: 1.0

Αυτός ο header μπαίνει από το Outlook και περιγράφει την έκδοση του πρωτοκόλλου MIME που χρησιμοποίησε ο αποστολέας.

Content-Type: multipart/mixed;

Ο σκοπός του συγκεκριμένου header είναι να δώσει οδηγίες στον e-mail client του παραλήπτη για να μπορέσει να κάνει format το μήνυμα σωστά.

X-Mailer: Microsoft Office Outlook, Build 11.0.5510 *Αυτός ο header αναφέρει την ακριβή έκδοση του Outlook που χρησιμοποιήθηκε για να σταλεί αυτό το μήνυμα.*

X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2800.1165

Περισσότερες πληροφορίες για τον e-mail client που χρησιμοποίησε ο αποστολέας.

Thread-Index: AcON3CInEwkfLOQsQGeK8VCv3M+IPA==

Αυτός ο header χρησιμοποιείται για να γίνει λογική σύνδεση μηνυμάτων που ανήκουν στο ίδιο thread. Αυτό μπορεί να χρησιμοποιηθεί για παράδειγμα από το Outlook, όταν κάνουμε group τα μηνύματα βάση conversation (από το κεντρικό μενού του Outlook επιλέγουμε View – Arrange by – Conversation).

Return-Path: kelly@litware.com

Ο συγκεκριμένος header μας ενημερώνει για το πως μπορούμε να επικοινωνήσουμε με τον αποστολέα (π.χ. όταν επιλέγουμε να του στείλουμε ένα reply).

Message-ID: MAILbbnewS5TqCRL00000013@mail.litware.com

Κάθε μήνυμα παίρνει ένα message-ID από τον server του αποστολέα. Το μήνυμα κρατάει το ίδιο message id καθ' όλη τη διάρκεια της ζωής του. Επειδή ακριβώς το μήνυμα μπαίνει από τον originating mail server, συνήθως θα παρατηρήσουμε ότι διατηρεί και κάποιο χαρακτηριστικό γνώρισμα (πχ @mail.litware.com).

X-OriginalArrivalTime: 15 Dec 2004 21:38:50.0145 (UTC) FILETIME=[2E0D4910:01C38DDC]

Αυτός είναι ένας header που μπαίνει στο μήνυμα την πρώτη φορά που θα περάσει από έναν Microsoft Exchange Server[7].

Εδώ φαίνεται η δομή του παραπάνω Header (από ένα κανονικό e-mail)

```
1) Microsoft Mail Internet Headers Version 2.0
2) Received: from mail.litwareinc.com ([10.54.108.101]) by
mail.proseware.com with Microsoft SMTPSVC(6.0.3790.0);
Wed, 15 Dec 2004 13:39:22 -0800
3) Received: from mail ([10.54.108.23] RDNS failed) by mail.litware.com
with Microsoft SMTPSVC(6.0.3790.0);
Wed, 15 Dec 2004 13:38:49 -0800
4) From: "Kelly Weadock" kelly@litware.com
5) To: anton@proseware.com
6) Subject: Review of staff assignments
7) Date: Wed, 15 Dec 2004 13:38:31 -0800
8) MIME-Version: 1.0
9) Content-Type: multipart/mixed;
10) X-Mailer: Microsoft Office Outlook, Build 11.0.5510
11) X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2800.1165
12) Thread-Index: AcON3CInEwkfLOQsQGeK8VCv3M+IPA==
13) Return-Path: kelly@litware.com
14) Message-ID: MAILbbnews85TgCRL00000013@mail.litware.com
15) X-OriginalArrivalTime: 15 Dec 2004 21:38:50.0145 (UTC)
FILETIME=[2E0D4910:01C38DDC]
```

Και πάμε να δούμε τη δομή από ένα spoofed e-mail. Στη προκειμένη περίπτωση θα στείλουμε e-mail πάλι στον anton@proseware.com αλλά αυτή τη φορά ως ceo@proseware.com. Αυτό το οποίο θα πρέπει να ελέγξουμε είναι, αν στους Internet Headers υπάρχουν πληροφορίες οι οποίες μοιάζουν ξένες ως προς το δικό μας δίκτυο.

```
1) Microsoft Mail Internet Headers Version 2.0
2) Received: from mail.litwareinc.com ([10.54.108.101]) by
mail.spoofers.com with Microsoft SMTPSVC(6.0.3790.0);
Wed, 15 Dec 2004 13:39:22 -0800
3) Received: from spoofer ([10.10.105.123]) by mail.spoofers.com with
Microsoft SMTPSVC(6.0.3790.0);
Wed, 15 Dec 2004 13:38:49 -0800
4) From: "Company CEO" ceo@proseware.com
5) To: anton@proseware.com
6) Subject: Please send me my dialup password at ceo@niamodekaf.com
7) Date: Wed, 15 Dec 2004 13:38:31 -0800
8) MIME-Version: 1.0
9) Content-Type: multipart/mixed;
10) X-Mailer: Microsoft Office Outlook, Build 11.0.5510
11) X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2800.1165
12) Thread-Index: AcON3CInEwkfLOQsQGeK8VCv3M+IPA==
13) Message-ID: MAILbbnewS5TqCRL00000013@mail.spoofers.com
14) X-OriginalArrivalTime: 15 Dec 2004 21:38:50.0145 (UTC)
FILETIME=[2E0D4910:01C38DDC]
```

Εδώ παρατηρούμε ότι στις γραμμές δύο και τρία αναφέρουν δρομολόγηση από servers που δεν θα έπρεπε να βρίσκονται εκεί. Από τη στιγμή που το μήνυμα είναι εσωτερικό δεν θα έπρεπε να βλέπουμε

ξένους servers. Επίσης στη γραμμή 13 έχουμε περιεχόμενο που είναι και αυτό «ξένο» ως προς το δίκτυό μας. Παρόμοιο έλεγχο για spoofing μπορούμε να κάνουμε και από εξωτερική πηγή (δηλαδή από e-mails που προέρχονται από το Internet) και το Internet Header τους έχει ως εξής[7]:

```
1) Microsoft Mail Internet Headers Version 2.0
2) Received: from mail.litwareinc.com ([10.54.108.101]) by
mail.spoofers.com with Microsoft SMTPSVC(6.0.3790.0);
Wed, 15 Dec 2004 13:39:22 -0800
3) Received: from spoofer ([10.10.105.123]) by mail.spoofers.com with
Microsoft SMTPSVC(6.0.3790.0);
Wed, 15 Dec 2004 13:38:49 -0800
4) From: "Microsoft Technical Support" support@microsoft.com
5) To: anton@proseware.com
6) Subject: Change in security policy requires that you change your Hotmail
password to p@ssw0rd
7) Date: Wed, 15 Dec 2004 13:38:31 -0800
8) MIME-Version: 1.0
9) Content-Type: multipart/mixed;
10) X-Mailer: Microsoft Office Outlook, Build 11.0.5510
11) X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2800.1165
12) Thread-Index: AcON3CInEwkfLOQsQGeK8VCv3M+IPA==
13) Message-ID: MAILbbnewS5TqCRL00000013@mail.spoofers.com
14) X-OriginalArrivalTime: 15 Dec 2004 21:38:50.0145 (UTC)
FILETIME=[2E0D4910:01C38DDC]
```

4.4 DIALERS

Οι Dialers στις μέρες μας δεν αποτελούν σοβαρό κίνδυνο. Μόνο για όσους χρήστες μπαίνουν στο διαδίκτυο με modem τύπου 56k. Αλλά ως φαίνεται, σε λίγο καιρό κανένας χρήστης δεν θα αντιμετωπίζει τους Dialers ως απειλή. Παρόλα αυτά θα το αναφέρουμε διότι για αρκετά μεγάλο χρονικό διάστημα ήταν πολύ μεγάλη μάστιγα στο διαδίκτυο.

Οι Dialers είναι μικρά προγράμματα (50-80kb) τα οποία αποσυνδέουν την υπάρχουσα κλήση της τηλεφωνικής γραμμής με τον τοπικό πάροχο υπηρεσιών Internet (ISP) και καλούν αυτόματα αριθμούς υψηλής χρέωσης (π.χ. 090, 901, 00xx κ.α.), οι οποίοι είναι για πρόσβαση σε συγκεκριμένες υπηρεσίες. Φυσικά, αυτή η κίνηση γίνεται χωρίς τη συνειδητή συγκατάθεση του χρήστη. Η δημιουργία τους αρχικά ήταν για να γίνετε άμεσα η πληρωμή των συγκεκριμένων εταιριών οι οποίες χρησιμοποιούσαν τα dialers, με επίγνωση φυσικά του χρήστη. Η σωστή λειτουργία τους έχει ως εξής: αν προσπαθήσουμε να επισκεφτούμε μια ιστοσελίδα η οποία προσφέρει ειδικό περιεχόμενο με αυτό τον τρόπο, θα εμφανιστεί στην οθόνη μας ένα παράθυρο διαλόγου το οποίο μας ρωτά αν θέλουμε να κατεβάσουμε το συγκεκριμένο πρόγραμμα dialer.

Επίσης, μας ενημερώνει για το είδος της υπηρεσίας την οποία πρόκειται να χρησιμοποιήσουμε και για τη χρέωσή της. Αν επιλέξουμε «yes», το λογισμικό του dialer εγκαθιστάτε στον υπολογιστή μας. Το λογισμικό αλλάζει τον αριθμό σύνδεσης στο διαδίκτυο με αυτόν της αυξημένης χρέωσης, ενώ εμείς έχουμε τη δυνατότητα πρόσβασης στο ειδικό περιεχόμενο εφόσον χρεωνόμαστε με αυξημένη τιμολόγηση. Καθ’ όλη τη διάρκεια πρόσβασης στο ειδικό περιεχόμενο, υπάρχει στην οθόνη ένδειξη ότι χρησιμοποιείτε σύνδεση στο διαδίκτυο αυξημένης χρέωσης. Στη συνέχεια, μόλις αποσυνδεθούμε από τη συγκεκριμένη ιστοσελίδα, ο

dialer αποκαθιστάται από τον υπολογιστή μας και η σύνδεση του modem επιστρέφει στον αριθμό του παρόχου Internet που χρησιμοποιούμε. Αυτό όμως άλλαξε λόγω του «εύκολου χρήματος» και για κάποιο διάστημα αποτέλεσαν μία από τις μεγαλύτερες απειλές στο χώρο του διαδικτύου (λέω αποτέλεσαν διότι τώρα πια με τις ευρυζωνικές συνδέσεις δεν είναι δυνατό να απειληθούμε από dialers, όμως όσο η είσοδος στο διαδίκτυο γινόταν μέσο dial up και ISDN ήταν από τα ποιο επικίνδυνα προγράμματα, μιας και είχαν άμεσο αντίκτυπο στο λογαριασμό του τηλεφώνου).

Δύο είναι οι συνηθέστεροι τρόποι που δρουν οι dialers και είναι οι εξής:

1. Αλλάζουν τις ρυθμίσεις δικτύου μέσω τηλεφώνου (dial up networking) και μας υποχρεώνουν σαν χρήστη να καλέσουμε έναν συγκεκριμένο αριθμό (από αυτούς που έχουμε προαναφέρει) άγνωστο προς εμάς. Ύστερα, διαγράφουν τον αριθμό του ISP που χρησιμοποιούμε και τοποθετούν το δικό τους. Από εκεί και πέρα κάθε φορά που μπαίνουμε μέσω dial up κάνει κλήση στον δικό τους πάροχο και φυσικά έχει και τις ανάλογες χρεώσεις.

2. Ο δεύτερος τρόπος είναι να αναγκάσουν τον υπολογιστή να παρακάμψει τις ρυθμίσεις του δικτύου μέσο τηλεφώνου και να καλέσει ένα συγκεκριμένο αριθμό. Έτσι, παρόλο που μπορεί να εμφανίζονται οι προεπιλεγμένες ρυθμίσεις του χρήστη όταν συνδέεται στο Internet, θα καλείται ένας άλλος αριθμός που θα έχει οριστεί από τον dialer.

Οι dialers προέρχονται από επισκέψεις σε συγκεκριμένες ιστοσελίδες. Οι οποίες μπορεί να είναι ιστοσελίδες που παρέχουν πειρατικό λογισμικό, πορνογραφικό περιεχόμενο, ή ιστοσελίδες με αμφιλεγόμενο περιεχόμενο. Οι ιδιοκτήτες αυτών των ιστοσελίδων έχουν ενσωματώσει στο κώδικα της ιστοσελίδας τους τον dialer οπότε αυτός εγκαθίσταται αυτόματα με το που εισέρθουμε ως χρήστης στην ιστοσελίδα. Ο δεύτερος τρόπος που μας ενδιαφέρει κιόλας, είναι μέσο

ηλεκτρονικής αλληλογραφίας. Με τη μορφή συνημμένου αρχείου (συνήθως με την ετικέτα ενός δημοφιλούς προγράμματος), όπου εάν το αποθηκεύσουμε και το εκτελέσουμε στον υπολογιστή μας εγκαθιστά εν άγνοιά μας τον dialer.

Η διαφορά του μεγέθους πληρωμής γίνεται αισθητή αν υποθέσουμε πως μία κανονική κλίση είναι 0,0058 ευρώ το λεπτό σε ώρες αιχμής και 0,0029 ευρώ σε μη ώρες αιχμής, ενώ μέσο dialer μπορεί να φτάσει και τα 2 ευρώ το λεπτό δηλαδή 689 φορές ακριβότερη από τη χρέωση ΕΠΑΚ.

Υπαρκτά παραδείγματα διεθνών προορισμών από κλήσεις dialers είναι: Nauru (00674), Solomon Islands (00677) Wallis and Futuna (00 681). Για την αντιμετώπιση του συγκεκριμένου προβλήματος, οι τηλεφωνικές εταιρίες αποφάσισαν να εξυπηρετούνται αυτές οι κλήσεις μέσο ενός «operator» του ΟΤΕ, ώστε να αποφεύγονται ακούσιες κλήσεις μέσω του υπολογιστή. Τέλος, η λίστα αυτή ανανεώνεται και τροποποιείται από την ΕΕΤΤ με βάση τα στοιχεία που συλλέγονται[3].

4.4.1 ΠΩΣ ΜΠΟΡΟΥΜΕ ΝΑ ΚΑΤΑΛΑΒΑΙΝΟΥΜΕ ΟΤΙ ΕΧΕΙ ΕΓΚΑΤΑΣΤΑΘΕΙ DIALER ΣΤΟΝ Η/Υ

- Θα ακούσουμε το modem μας να αποσυνδέεται και να πραγματοποιεί νέα κλήση (βέβαια μερικοί dialers μπορούν να σιγήσουν τους ήχους κλήσης).
- Είναι πιθανό, η ταχύτητα της σύνδεσης μας στο Internet να είναι πολύ χαμηλότερη από ό, τι συνήθως. Μπορεί να υπάρχουν αρκετοί λόγοι που συμβαίνει αυτό αλλά καλό είναι να εξετάσουμε τα (dial up settings)
- Είναι πιθανό, παρά το γεγονός ότι βρισκόμαστε στο διαδίκτυο να μη μπορούμε να στείλουμε ηλεκτρονικά μηνύματα (e-mails)

- Θα λάβουμε λογαριασμό ο οποίος θα είναι απρόσμενα υψηλός και θα έχει κλήσεις σε αριθμούς εξωτερικού ή αυξημένης χρέωσης[3].

4.4.2 ΤΡΟΠΟΙ ΠΡΟΦΥΛΑΞΗΣ ΑΠΟ ΤΟΥΣ DIALERS

- Να κλείσουμε τον υπολογιστή μας όταν δεν τον χρησιμοποιούμε.
- Ποτέ να μην ανοίγουμε συνημμένα αρχεία τρίτων αν δεν γνωρίζουμε τι είναι.
- Θα πρέπει να έχουμε εγκατεστημένο ένα Antivirus (π.χ. Nod32, AGV).
- Κατά καιρούς θα πρέπει να ελέγχουμε τον υπολογιστή μας για spyware.
- Πρέπει να εξετάζουμε συχνά τις παραμέτρους σύνδεσης του Η/Υ μας με το διαδίκτυο για να βεβαιωνόμαστε ποιους αριθμούς καλεί το modem μας.
- Να είμαστε επιφυλακτικοί με τα κλικ που κάνουμε σε «pop up windows» που εμφανίζονται ξαφνικά στην οθόνη μας.
- Να είμαστε ιδιαιτέρα προσεκτικοί στη περιήγηση μας στο διαδίκτυο.
- Να έχουμε δυνατά την ένταση στο modem μας ώστε να ακούσουμε αν πάει να κάνει ανάκληση.
- Να προσέχουμε την επιφάνεια εργασίας μας μήπως μας έχει σωθεί (μόνο του) κανένα εικονίδιο που μας φαίνεται άγνωστο.
- Να ενημερώνουμε όποιον είναι να χρησιμοποιήσει τον υπολογιστή μας, για το κακόβουλο λογισμικό που κυκλοφορεί.
- Να ενεργοποιήσουμε την υπηρεσία φραγής κλήσεων για κλήσεις εξωτερικού και αυξημένων χρεώσεων[3].

4.5 E-MAIL BOMB

Ο όρος e-mail bomb, αναφέρεται σε ένα είδος επίθεσης κατά την οποία ο επιτιθέμενος «βομβαρδίζει» (δηλαδή στέλνει τεράστιες ποσότητες ηλεκτρονικών μηνυμάτων) σε μία διεύθυνση ηλεκτρονικού ταχυδρομείου με σκοπό να γεμίσει το διαθέσιμο χώρο του δίσκου ή της εικονικής μνήμης του server και να προκαλέσει δυσλειτουργία στον server και στον ηλεκτρονικό υπολογιστή. Το e-mail bomb διαφέρει από το spamming διότι όπως προείπαμε στέλνει ο “hacker” πολλά μηνύματα σε συγκεκριμένο υπολογιστή και όχι γενικός σε πληθώρα ηλεκτρονικών διευθύνσεων όπως συμβαίνει στα spam.

Υπάρχουν δύο τρόποι διακίνησης των e-mail bombs. Ο πρώτος τρόπος συνίσταται στη μαζική αποστολή μηνυμάτων από ένα πρόγραμμα που φτιάχνει ο ίδιος ο cracker (το οποίο είναι αρκετά απλό να φτιαχτεί) και το οποίο βομβαρδίζει τον εκάστοτε υπολογιστή. Αυτός ο τρόπος όμως, δεν είναι ιδιαίτερα αποτελεσματικός αφού είναι εύκολο να εντοπιστεί η διαδικασία από έναν server και να την εντάξει στα spam. Ο δεύτερος τρόπος και αποτελεσματικότερος ονομάζεται DDoS – Distributed Denial of Service. Κατά την επίθεση αυτή ο cracker δίνει εντολή σε υπολογιστές «bots» ή «ζόμπι» να στείλουν μαζικά e-mails σε μία διεύθυνση. Η διαφορά τους έγκειται στο ότι στέλνονται τα e-mails από διαφορετικά ID οπότε και είναι δυσκολότερο στους Servers να διαπιστώσουν ότι είναι spam. Αυτός ο τρόπος όμως προϋποθέτει την εγγραφή του e-mail του θύματος σε διάφορες διαδικτυακές υπηρεσίες όπως (mailing lists, Newsletters κ.α.). Αν ο cracker καταφέρει να «γράψει» το θύμα σε πολλές τέτοιες υπηρεσίες τότε το θύμα θα παραλαμβάνει δεκάδες e-mails καθημερινά, γεμίζοντας με αυτό τον τρόπο τον σκληρό δίσκο του mail server του. Για την αποφυγή τέτοιων

κρουσμάτων, είναι υποχρεωτικό πια να στέλνεται ένα e-mail επιβεβαίωσης ότι θέλουμε την εγγραφή σε μία τέτοια λίστα.

Επίσης, μια παραλλαγή των e-mail bombs (και μάλιστα πιο δραστική) είναι οι ZIP Bombs. Ο τρόπος επίθεσης είναι όπως και παραπάνω δηλαδή στέλνονται εκατοντάδες, χιλιάδες ή ακόμα και εκατομμύρια e-mails σε έναν λογαριασμό, αλλά αυτή τη φορά έχουν συνημμένο ένα αρχείο το οποίο είναι σε μορφή ZIP, RAR, 7-ZIP (δηλαδή συμπιεσμένο) και περιλαμβάνει ένα έγγραφο κειμένου το οποίο έχει επαναλαμβανόμενο αρκετές φορές το γράμμα π.χ. «a» (διαλέγουν γράμματα τα οποία να δέχονται μεγάλη συμπίεση, διότι ως γνωστόν δεν συμπιέζονται όλα τα γράμματα το ίδιο). Όταν αυτό είναι συμπιεσμένο, το αρχείο πιάνει πολύ μικρό όγκο, όταν όμως ο mail server προσπαθήσει να αποσυμπιέσει τα e-mails για να ελέγξει για ιούς, θα καταλήξει να αποσυμπιέζει έναν τεράστιο όγκο αρχείων τα οποία ενδέχεται να προκαλέσουν και το «πάγωμα» του mail server οπότε και τη γενικότερη δυσλειτουργία του συστήματος.

Αυτού του είδους οι επιθέσεις έχουν αρχίσει να μην είναι πια ιδιαίτερα απειλητικές, διότι τα φίλτρα των e-mail servers είναι σε θέση να ξεχωρίσουν αρκετά καλά πότε δεχόμαστε e-mail bombs και ακόμα και όταν αποσυμπιέζουν τα zip bombs έχουν αρκετή μνήμη και δυνατούς επεξεργαστές ώστε να μην «παγώσει» το σύστημα.

Φυσικά όμως, αν τελικά καταλήξουν στην ταχυδρομική μας θυρίδα τόσες εκατοντάδες e-mails θα μας είναι δυσάρεστο σαν χρήστες να πρέπει να δούμε ποια και πόσα emails πρέπει να διαγράψουμε από το «Inbox» μας[14].

4.6 HOAXES Ή URBAN LEGENDS

Η ονομασία Hoaxes προέρχεται από το Hocus Pocus (μία μαγική λέξη σαν το άμπρα κατάμπρα). Το Urban Legends σημαίνει αστικοί θρύλοι και δίνουν ακριβώς την ερμηνεία αυτών των e-mails, μιας και είναι φήμη ή θρύλος ο οποίος «περιφέρεται» στο διαδίκτυο. Το περιεχόμενο που έχουν συνήθως τα Hoaxes ή Urban Legends δεν διαφέρει πολύ από αυτό:

- *Διαμαρτυρία για την κακομεταχείριση των γυναικών στο Αφγανιστάν.*
- *Αποστολή χριστουγεννιάτικων καρτών σε ετοιμοθάνατα παιδιά.*
- *Προτάσεις φορολόγησης όσων δεδομένων διακινούνται μέσω Internet.*
- *Φυλακτά καλής τύχης ή κατάρες ακρωτηριασμού και καταστροφής.*

Τα hoaxes είναι e-mails που διακινούνται στο διαδίκτυο και δημοφιλέστερό τους θέμα είναι οι ιοί (*π.χ. μη διαβάσετε e-mail με subject "Good Times" διότι θα καταστραφεί ο Η/Υ σας).*

Επίσης, άλλες μεγάλες κατηγορίες τους είναι τα Συμπαράστασης τα οποία παρουσιάζουν προβλήματα κάποιου υποθετικά άρρωστου ανθρώπου και ζητούν τη μεγαλύτερη κινητοποίηση των χρηστών. Ενώ υπάρχει και η κατηγορία Εκφοβισμού τα οποία μπορεί να μας απειλεί ότι θα μας συμβεί κάτι τρομερό αν δεν το προωθήσουμε άμεσα.

Υπάρχουν αρκετοί τρόποι για να αναγνωρίσουμε τα Hoaxes και είναι οι εξής:

1. Οι συγγραφείς τους χρησιμοποιούν επιστημονικούς όρους για να γίνουν πιο πιστικοί στους αναγνώστες τους, αυτό εκ πρώτης όψεως μπορεί να δείχνει αρκετά σοβαροφανές αλλά στη συνέχεια μπορούμε να διαπιστώσουμε πως δεν έχει κανένα νόημα. Ένα παράδειγμα που μας δίνει να το καταλάβουμε είναι αυτό π.χ.

```
"...if the program is not stopped, the computer's processor will be placed
in an nth-complexity infinite binary loop which can severely damage the
processor..."
```

αν το μελετήσουμε δεν υπάρχει κάτι που να αποκαλείται nth-complexity infinite binary loop και σε τελική ανάλυση οι επεξεργαστές είναι φτιαγμένοι για να κάνουν loops εβδομάδες χωρίς να παθαίνουν τίποτε.

2. Κάτι άλλο που κάνουν για να αυξήσουν την αξιοπιστία τους ως e-mails είναι, να επικαλεσθούν οι συγγραφείς τους ότι αποτελούν e-mails που τους τα έστειλε μία επώνυμη εταιρία με κύρος όπως (π.χ. Microsoft, Yahoo, Aol). Πράγμα που είναι σχεδόν αδύνατο μιας και αυτές οι εταιρίες οτιδήποτε θέλουν να δημοσιεύσουν το δημοσιεύουν στο τύπο και δεν εμπιστεύονται τα e-mails.

3. Επόμενο και βασικότερο χαρακτηριστικό των Hoaxes είναι να ζητάει τη προώθηση του σε άλλους χρήστες. Αυτός είναι και ο σκοπός του και αν ένα email ζητάει κάτι τέτοιο είναι σχεδόν σίγουρα Hoax.

4. Επίσης πολλοί χρησιμοποιούν και τον εκφοβισμό όπως «*Ψήφισε και εσύ κατά της φορολόγησης των πακέτων του Internet διαφορετικά σύντομα θα αρχίσουν να σε χρεώνουν*». Συνήθως έχουν κακή σύνταξη και είναι ανορθόγραφα αυτού του είδους τα Hoaxes.

5. Τέλος, αν τελικά το κείμενο που έχει να σου πει στο e-mail είναι τόσο σημαντικό θα πρέπει τουλάχιστον να αναφέρει το site που έχει φτιαχτεί για αυτόν το λόγο. Και εδώ, θα πρέπει να προσέξουμε αν όντως υπάρχει το site, να μην είναι ύποπτη η διεύθυνση (π.χ. η Cisco να έχει σελίδα στο Geocities).

Τρόποι για να αποφύγουμε και να μην επεκτείνουμε τη μάστιγα των hoaxes είναι οι ακόλουθοι: ***Πρώτον*** να έχουμε σωστή ενημέρωση, σοβαρότητα και αυτοσυγκράτηση. Όταν δεχόμαστε ένα τέτοιο e-mail να

ελέγχουμε αν οι πηγές του είναι έγκυρες (δηλαδή θα πρέπει να ανατρέξουμε στην ιστοσελίδα που αναφέρεται το e-mail και να δούμε αν όντως ο συγγραφέας είναι έγκυρος). Ύστερα, δεν πρέπει να παρασυρόμαστε από συναισθηματισμούς και τέλος, δεν πρέπει να βιαζόμαστε, όσο πιο επείγον ισχυρίζεται ότι είναι το μήνυμα, τόσο πιο προσεκτικά πρέπει να ασχοληθούμε μαζί του.

Δύο είναι τα μεγάλα προβλήματα που δημιουργούν τα Hoaxes. Το πρώτο είναι ότι ανεβάζουν πολύ τη κίνηση στο διαδίκτυο και τον χώρο στο e-mail μας και το δεύτερο είναι ότι δημιουργούνται e-mails με μεγάλες λίστες λογαριασμών, τις οποίες κακόβουλοι χρήστες μπορούν να χρησιμοποιήσουν στο μέλλον για δική τους παράνομη χρήση.

Υποκατηγορία των Hoaxes είναι τα Chain Letters, τα οποία όμως δηλώνουν ξεκάθαρα ότι είναι φτιαγμένα για να διακινηθούν σε όσο περισσότερους χρήστες γίνεται, εντός διαδικτύου και συνήθως υπόσχονται καλή τύχη κ.α..

Τέλος, τα Hoaxes εκτός από το διαδίκτυο έχουν αρχίσει και διαδίδονται μέσο κινητών τηλεφώνων. Παράδειγμά τους θα αναφέρουμε στη συνέχεια. Τώρα θα δούμε μερικά παραδείγματα από Hoaxes για να είμαστε ενημερωμένοι και να ξέρουμε τι πρέπει να αποφεύγουμε:

Παράδειγμα HOAX 1:

```
A MEMBER OF AOL BY THE SCREEN NAME OF ZZ331MIGHT TRY TO SEND YOU A VIRUS
WHICH COULD CRASH YOUR COMPUTER SYSTEM.
HIS TRICK: HE INNOCENTLY IM's YOU HELLO, WAITS 30 SECONDS, THEN IM's YOU
AGAIN, WAITS ANOTHER 30 SECONDS, AND THEN WRITES...
"WHAT THE FU**, WHY AREN'T YOU ANSWERING"DO NOT REPLY TO HIS IM's, NOR READ
ANY OF HIS E-MAIL BECAUSE ONCE YOU REPLY, YOUR
COMPUTER WILL FREEZE AND THATS HOW YOU KNOW YOUR HARD DRIVE IS BEING WIPED
OUT. SO PLEASE BE VERY VERY CAREFUL!!!!
PLEASE PASS THIS ON TO EVERY ONE YOU KNOW!!!
```

Παράδειγμα HOAX 2:

```
Outbreak: I'm infecting you with t-virus, my code is <random numbers>.
Forward this to <phone number> to get your own code and chance to win
prizes.
More at <website URL>
```

Φάρσα-HOAX για το κινητό τηλέφωνο:

Μια καινούργια φάρσα που σπέρνει την αμηχανία στους χρήστες κινητών τηλεφώνων είναι η ακόλουθη:

```
"Αν σας τηλεφωνήσουν στο κινητό σας από κάποιον που θα σας πει ότι είναι
τεχνικός εταιρείας, και κάνουν έλεγχο στο τηλέφωνό σας και θα πρέπει να
πατήσετε #90 ή 09# ή οποιοδήποτε άλλο νούμερο, ΚΛΕΙΣΤΕ ΤΟ ΤΗΛΕΦΩΝΟ ΧΩΡΙΣ ΝΑ
ΠΑΤΗΣΕΤΕ ΚΑΠΟΙΟ ΑΡΙΘΜΟ. Πρόκειται για κάποια εταιρεία-απάτη που
χρησιμοποιεί κάποια συσκευή, η οποία μόλις πατήσετε τα παραπάνω νούμερα,
μπορεί να μπει στην κάρτα SIM και να παίρνουν τηλέφωνα με δική σας χρέωση.
Προωθήστε το μήνυμα σε όσους περισσότερους μπορείτε."
```

Η παραπάνω φάρσα είχε εμφανιστεί για πρώτη φορά στη Γερμανία το 1999, με ακριβώς το ίδιο κείμενο. Η γερμανική εταιρία κινητής τηλεφωνίας T-Mobil (T-D1), τότε είχε δηλώσει επίσημα ότι κάτι τέτοιο δεν είναι δυνατόν τεχνικά στο δίκτυό της γιατί:

Στη Γερμανία δεν ισχύει το reverse charging, το δίκτυο δεν υποστηρίζει πρόσβαση σε κάρτα SIM κατά τη διάρκεια κλήσης. Επίσης, υπάρχει μια λειτουργία για την πιστοποίηση του κινητού, η οποία μαζί με το κρυπτογραφικό κλειδί δεν επιτρέπει την πρόσβαση στην κάρτα με το συνδυασμό 9009. Η κάρτα SIM προστατεύεται από τον κωδικό PIN.

Έγινε ερώτηση και σε ελληνική τηλεφωνική εταιρία για τον ίδιο λόγο και η απάντηση της "Vodafone" ήταν η εξής:

«Αγαπητή κα Κοντίνη,

σε απάντηση του τελευταίου e-mail *σας θα θέλαμε να σας ενημερώσουμε ότι, και στο παρελθόν έχει αναφερθεί κάτι ανάλογο το οποίο όταν διερευνήθηκε διαπιστώθηκε ότι δεν ήταν πραγματικό γεγονός, δεν έχει καταγραφεί και διαπιστωθεί γιατί απλά δεν ισχύει κάτι τέτοιο. Ήταν μια κακόγουστη φάρσα. Τεχνικά και δικτυακά δεν υπάρχει απολύτως καμία πρόσβαση στην κάρτα* sim *του συνδρομητή με οποιαδήποτε χρήση κωδικών ή άλλων ενεργειών εξ αποστάσεως, έτσι όπως περιγράφεται. Σε καμία περίπτωση δεν ισχύει ότι αναφέρεται. Παρακαλούμε μην διστάσετε αν έχετε κάποια άλλη ερώτηση ή απορία. Στην διάθεση σας για οποιαδήποτε διευκρίνιση.*

Ευχαριστούμε που επικοινωνήσατε μαζί μας.» [2].

4.7 ΙΟΙ

Ιός πρόκειται για μία λέξη που απασχολεί έντονα όλους τους χρήστες Η/Υ. Η μορφή ηλεκτρονικού ιού έχει φυσικά διαφορά με τη μορφή ενός ιού που συναντάμε στη φύση, αλλά έχει και κοινά στοιχεία.

Η διαφορά τους είναι η προφανής, ενώ ο ένας αποτελείτε από γενετικό κομμάτι στο DNA, ο άλλος αποτελείτε από κομμάτι μέσα σε κώδικα. Το κοινό τους όμως είναι πως κάτω από ανάλογες συνθήκες και προϋποθέσεις μπορούν να διαδοθούν και να πολλαπλασιάσουν τον εαυτό τους πάρα πολλές φορές. Οι ιοί των υπολογιστών όπως και των ανθρώπων διακρίνονται σε κατηγορίες, δεν είναι όλοι το ίδιο επικίνδυνοι. Έτσι ένας ιός μπορεί να μας διαγράψει όλα τα δεδομένα από τον σκληρό μας δίσκο, μπορεί απλά να μας κάνει επανεκκινήσεις κάθε τόσο στον υπολογιστή, μπορεί να μας διαγράψει ορισμένα αρχεία ή ακόμα μπορεί απλά να μας ανοιγοκλείνει το πορτάκι του CD. Αυτό δείχνει πως οι ιοί μπορούν να είναι από φάρσα μέχρι και πολύ επικίνδυνοι, ανάλογα με το σκεπτικό που φτιάχτηκαν και το σκοπό για τον οποίο φτιάχτηκαν[1].

4.7.1 ΤΥΠΟΙ ΙΩΝ ΚΑΙ ΣΥΝΕΠΙΕΣ

Worms

Ένας ιός τύπου worm όπως και οι άλλοι ιοί, έχει σχεδιαστεί για να αντιγράφει τον εαυτό του από τον έναν υπολογιστή στον άλλο. Η διαφορά του είναι ότι αυτός ο ιός εκτελείται αυτόματα, δηλαδή δεν χρειάζεται την ενεργοποίησή του από τον χρήστη, όπως χρειάζονται άλλοι που θα δούμε στη συνέχεια. Ο μεγάλος κίνδυνος του ιού τύπου worm είναι η ικανότητά του να αναπαράγεται σε μεγάλο βαθμό. Έτσι για παράδειγμα, μπορεί να αποσταλεί μόνος του σε όλες μας τις επαφές που έχουμε στο ηλεκτρονικό μας ταχυδρομείο, προκαλώντας υπερφόρτωση της δικτυακής κυκλοφορίας, η οποία θα μπορούσε να προκαλέσει απλά επιβράδυνση στο διαδίκτυο ή και πάγωμα του διαδικτύου. Τρανταχτά παραδείγματα ιών τύπου worm είναι ο Sasses και ο Blaster. Ο δεύτερος εκ των οποίων ανακαλύφθηκε στις 11 Αυγούστου 2003 και εκμεταλλευόταν το θέμα ευπάθειας που αναφερόταν στο ενημερωτικό

δελτίο ασφάλειας MS03-026 (823980) της Microsoft για να μεταδοθεί μέσω δικτύων, χρησιμοποιώντας ανοικτές θύρες κλήσης απομακρυσμένης διαδικασίας (Remote Procedure Call) σε υπολογιστές στους οποίους εκτελούνταν κάποιο από τα προϊόντα που παρατέθηκαν από πάνω[1].

Δούρειος Ίππος (Trojan)

Όπως λέει και το όνομά του ο ιός δούρειος ίππος είναι ένας μεταμφιεσμένος ιός. Αυτό σημαίνει πως ενώ εμφανίζεται με το όνομα ενός έμπιστου αρχείου, όπως για παράδειγμα οι τελευταίες ενημερώσεις ασφαλείας της Microsoft ή ποιο απλά Nero.exe. Στη πραγματικότητα το όνομα του τελευταίου αν είναι Trojan θα είναι Nero.exe.vbs, οπότε όταν πατήσουμε να τρέξουμε το αρχείο ή να δούμε την εικόνα (γιατί μπορεί να μεταμφιεστεί ακόμα και με κατάληξη .jpg), τότε ενεργοποιείται ο ιός και μπορεί για παράδειγμα να απενεργοποιήσει τα συστήματα ασφαλείας του υπολογιστή μας. Εκτός από συνημμένα αρχεία σε ηλεκτρονικό ταχυδρομείο μπορεί να έχουν ενσωματωθεί και σε κώδικα ενός κανονικού προγράμματος, οπότε εκεί είναι ακόμα πιο δύσκολο να το καταλάβουμε και το μόνο που μπορεί να μας βοηθήσει σε αυτή τη περίπτωση είναι ένα πρόγραμμα anti virus ή το να έχουμε σωστά ενημερωμένο τον υπολογιστή μας. Σε κάθε περίπτωση δεν πρέπει να ανοίγουμε e-mails από χρήστες τους οποίους δεν γνωρίζουμε και να μην κατεβάζουμε προγράμματα από μη έγκυρες πηγές[1].

Logical Bombs

Λογική βόμβα είναι τύπος Trojan το οποίο χρησιμοποιείται για την απελευθέρωση ενός ιού ή ενός worm στο σύστημα που έχει εισβάλει. Η λογική βόμβα υπάρχει μέσα σε ένα σύστημα μέχρι κάτι να προκαλέσει την ενεργοποίησή της. Αυτό το κάτι μπορεί να είναι είτε εξωτερικός

παράγοντας, είτε εσωτερικός παράγοντας παράδειγμα του οποίου είναι ικανοποίηση μιας προεπιλεγμένης συνθήκης από τον υπολογιστή μας.
Αν και αυτός ο τρόπος δηλαδή οι Logical Bombs είναι πολύ αποτελεσματικός, δεν έχει βρεθεί έως τώρα αποτελεσματικός τρόπος για τον έλεγχό τους. Όταν αφεθεί ελεύθερος αυτός ο ιός όσο πιθανό είναι να προσβάλει ένα εχθρικό πληροφοριακό σύστημα, άλλο τόσο πιθανό είναι να προσβάλει και ένα φιλικό πληροφοριακό σύστημα. Τέλος, έχουν και μια παραλλαγή τις χρονικές βόμβες (Time Bombs), οι οποίες πυροδοτούνται κάποια συγκεκριμένη ημερομηνία με τα ίδια αποτελέσματα[1].

Mail Bugs

Αυτούς τους ιούς είναι αρκετά δύσκολο να τους καταλάβουμε, είναι σε μορφή HTML και μπορούν σε συνδυασμό με κάποιες άλλες παραμέτρους να παραβιάσουν το απόρρητο των πληροφοριών που έχουμε στον Η/Υ μας. Υπάρχουν επίσης και Micros Virus Scripts, όπου είναι ιοί που αποστέλλονται μέσω του ηλεκτρονικού ταχυδρομείου, όπου εκτός του κειμένου το μήνυμα συμπεριλαμβάνει και διάφορες εντολές ώστε ο ιός να εισβάλει στον Η/Υ. Οι εντολές αυτές είναι απλές προτάσεις όπως set DioM.JCD.exe_On.McSF. το οποίο σημαίνει, μόλις ανοίξουμε το e-mail να εκτελεστεί η εφαρμογή DioM.JCD.exe[1].

Άλλοι λιγότερο σημαντικοί ιοί:

Adware, Backdoors, Boot viruses, Bot-Net, EICAR test file, Exploit, Grayware, Honeypot, Keystroke logging, Polymorph viruses, Program viruses, Spyware, Zombie. Δεν θα κάνουμε περεταίρω αναφορά σε αυτούς τους ιούς, διότι θα ξεφύγουμε από τα πλαίσια της πτυχιακής μας

εργασίας. Κάνουμε απλά τη γενική αναφορά, διότι πιστεύουμε πως είναι απαραίτητη[1].

4.8 SNIFFING

Το sniffing εγκύπτει στα είδη των παθητικών επιθέσεων. Δηλαδή το sniffing δεν έχει σκοπό να βλάψει άμεσα τον στόχο του, αλλά έχει σαν σκοπό ο επιτιθέμενος να συλλέξει χρήσιμα στοιχεία και πληροφορίες, ώστε να τα χρησιμοποιήσει μετέπειτα στην κύρια επίθεσή του. Ένα παράδειγμα είναι υποκλοπές passwords μέσω sniffing.

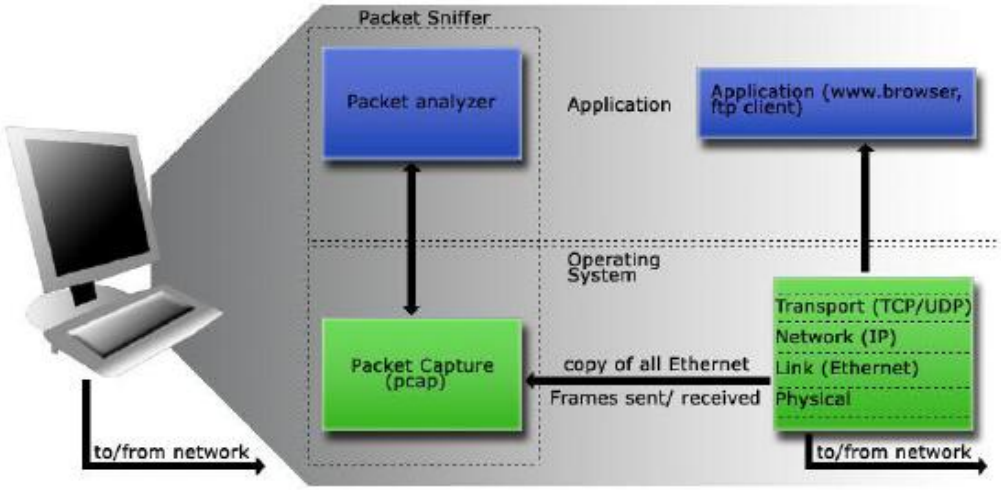
Τα προγράμματα sniffers ή network analyzers είναι νόμιμα και χρησιμοποιούνται από τους διαχειριστές του δικτύου, ώστε να διορθώσουν προβλήματα στη κίνησή του και άλλα παρόμοια, όμως δυστυχώς χρησιμοποιούνται και από τους crakers για τους παραπάνω λόγους.

Ο τρόπος λειτουργίας αυτών των προγραμμάτων είναι ο εξής. Αφού οι περισσότεροι υπολογιστές συνδέονται με Lan, δηλαδή μοιράζονται την ίδια σύνδεση με άλλους υπολογιστές, και εάν το δίκτυο δεν χρησιμοποιεί switch, η κίνηση που προορίζεται για έναν τομέα μεταδίδεται σε κάθε μηχάνημα του δικτύου. Ο κάθε υπολογιστής όμως που περνάνε τα δεδομένα από την κάρτα δικτύου, αγνοεί όλα τα δεδομένα που δεν τον αφορούν, δηλαδή που δεν προορίζονται για αυτόν. Το sniffer όμως αναγκάζει την κάρτα δικτύου του να αρχίσει να προσέχει και τα πακέτα που δεν προορίζονται για αυτόν, αλλά για τους υπόλοιπους υπολογιστές. Για να το πετύχει αυτό θέτει την κάρτα δικτύου σε ειδική λειτουργία, γνωστή ως promiscuous mode. Όταν η κάρτα δικτύου βρίσκεται σε αυτή τη λειτουργία (μία κατάσταση που απαιτεί δικαιώματα ανώτερου χρήστη, root), τότε μπορεί το μηχάνημα να βλέπει όλα τα δεδομένα που μεταδίδονται στον τομέα του.

Για να αποφύγουμε το sniffing μπορούμε να χρησιμοποιήσουμε προγράμματα anti sniffing. Θα πρέπει όμως να αναφέρουμε τη δυσκολία ελέγχου του sniffing διότι μιας και είναι παθητική επίθεση, δηλαδή συλλέγει πληροφορίες, δεν κάνει καμία αλλοίωση ή δεν αφήνει καμία υπογραφή στη συνηθισμένη κίνηση του δικτύου για να φανεί η λειτουργία του. Παρ' όλα αυτά, υπάρχουν τρόποι ώστε να γίνονται φανερές τέτοιου είδους επιθέσεις οι οποίες βρίσκονται σε promiscuous mode. Οι κύριοι μέθοδοι είναι Ping method, Arp method, local host και latency method. Πάντως, η καλύτερη όλων για την αποφυγή του είναι η κρυπτογράφηση με SSL, PGP, SSH κ.α., έτσι ώστε και να αποκτήσει πρόσβαση στα δεδομένα μας ο cracker να μην μπορεί να τα αποκωδικοποιήσει.

Για να καταλάβουμε καλύτερα πως λειτουργεί το Sniffing θα δοκιμάσουμε να κάνουμε μία επίθεση σε έναν δικτυακό τόπο με το Wireshark και να υποκλέψουμε τους κωδικούς πρόσβασης. Το Wireshark οι περισσότεροι το γνωρίζουμε ως Ethereal, όμως επειδή ο σχεδιαστής του Ethereal προχώρησε σε μια νέα εταιρία αναγκάστηκε να εγκαταλείψει το σήμα κατατεθέν Ethereal και να το μετονομάσει σε Wireshark, κατά τα άλλα δουλεύουν με τον ίδιο ακριβώς τρόπο.

Στο σχήμα που ακολουθεί φαίνεται η δομή ενός packet Sniffer



Όπου στο δεξί μέρος του Σχήματος φαίνονται τα πρωτόκολλα που τρέχουν κανονικά στον υπολογιστή μας. Μέσα στο παραλληλόγραμμο έχουμε τον packet Sniffer ο οποίος συνήθως είναι μία προσθήκη στο λογισμικό, που αποτελείται από δύο μέρη.

Το πρώτο μέρος είναι η βιβλιοθήκη σύλληψης πακέτων, η οποία λαμβάνει ένα αντίγραφο κάθε πλαισίου επιπέδου ζεύξης που στέλνεται ή λαμβάνεται από τον υπολογιστή μας. Ενώ το δεύτερο είναι ο αναλυτής πακέτων, ο οποίος απεικονίζει τα περιεχόμενα όλων των πεδίων μέσα στο μήνυμα ενός πρωτοκόλλου. Για το σκοπό αυτό, ο αναλυτής πακέτων πρέπει να «καταλαβαίνει» τη δομή όλων των μηνυμάτων που ανταλλάσσονται από τα πρωτόκολλα[5].

4.9 ΣΥΜΒΟΥΛΕΣ ΓΙΑ ΤΟΝ ΥΠΟΛΟΓΙΣΤΗ

Πρόκειται για υποτιθέμενες φιλικές συμβουλές που έχουν σκοπό την ασφάλεια του υπολογιστή από διάφορους κινδύνους, όπως είναι κάποια επικίνδυνα αρχεία που υπάρχουν ήδη τον υπολογιστή. Ενώ στην πραγματικότητα, αυτά τα αρχεία είναι ακίνδυνα και η διαγραφή τους από τον υπολογιστή θα προκαλέσει σοβαρά προβλήματα στην μετέπειτα λειτουργία του.

Έτσι πολλοί χρήστες πιστεύοντας πως αυτά τα συμβουλευτικά e-mail είναι χρήσιμα, τα προωθούν σε γνωστούς τους. Γι’ αυτό τον λόγο πρέπει όλοι οι παραλήπτες να είναι προσεκτικοί όταν δέχονται τέτοιου είδους μηνύματα[3].

ΚΕΦΑΛΑΙΟ 5

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ

5.1 ΕΙΣΑΓΩΓΗ

Η πιο κάτω μελέτη αφορά σε έκθεση της ομάδας ασφάλειας εργαστηρίων της M86 SECURITY, και αφορά στην περίοδο από Ιούλιο έως Δεκέμβριο του 2011

Πολλές ενδιαφέρουσες τάσεις προέκυψαν κατά τη διάρκεια της περιόδου, αν και μερικές ξεχώρισαν ως ιδιαίτερα αξιοσημείωτες. Οι στοχοθετημένες επιθέσεις έχουν αυξηθεί σε πολυπλοκότητα, με στοιχεία ότι τα διαδικτυακά εγκλήματα ακολουθούν όχι μόνο τους εμπορικούς οργανισμούς, αλλά και τους κυβερνητικούς οργανισμούς και οργανισμούς υποδομής επίσης. Επιπλέον, με την αυξανόμενη χρήση των ψευδών ή/και κλεμμένων ψηφιακών πιστοποιητικών, αυτές οι επιθέσεις έχουν γίνει επιτυχέστερες και αόριστες.

Μια άλλη τάση που αναφέρθηκε από την ομάδα περιέλαβε τη διάδοση του malware μέσω του spam. Αν και τα εργαστήρια M86 σημείωσαν μια πτώση στους γενικούς όγκους spam Δεκεμβρίου 2011, η ομάδα είδε μια άνοδο στην ποσότητα κακόβουλων συνδέσεων, και τις συνδέσεις μέσα στα ηλεκτρονικά ταχυδρομεία spam.

Τέλος, η ομάδα συνέχισε να βλέπει μια άνοδο στις απάτες στα κοινωνικά μέσα, με μια σημαντική αύξηση στην απάτη και τον πολλαπλασιασμό του malware χρησιμοποιώντας τα κοινωνικά δίκτυα ως αγωγό.

5.2 ΑΝΑΣΚΟΠΗΣΗ ΔΕΥΤΕΡΟΥ ΕΞΑΜΗΝΟΥ (ΙΟΥΛΙΟΣ - ΔΕΚΕΜΒΡΙΟΣ) 2011

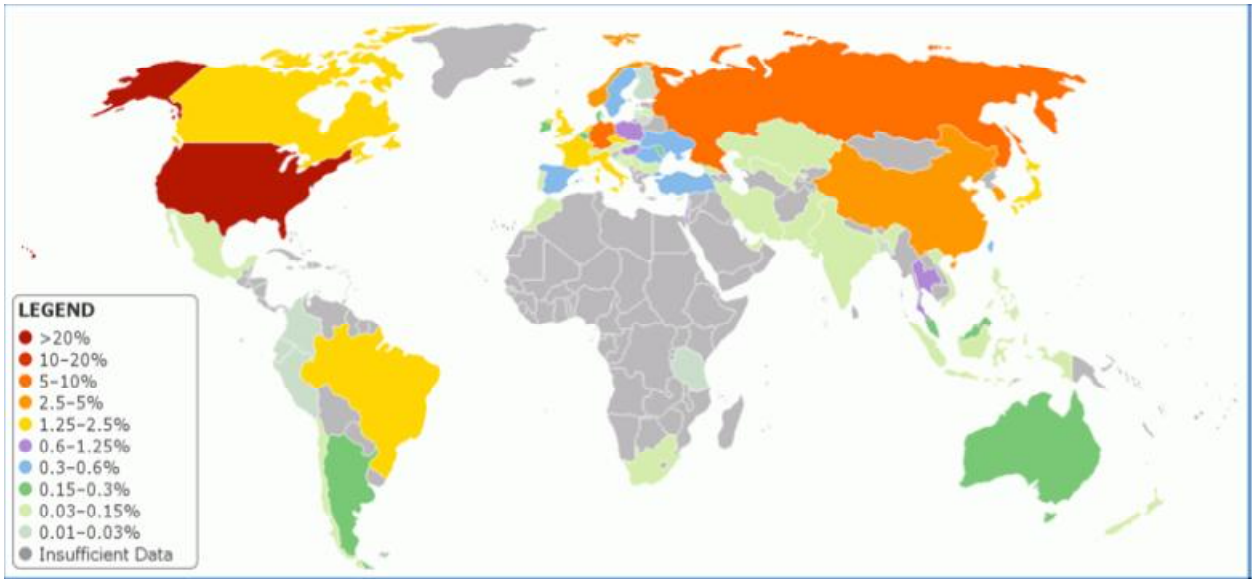
Σημεία κλειδιά

1. Οι στοχοθετημένες επιθέσεις έγιναν περίπλοκες και ακολούθησαν ένα ευρύτερο φάσμα των οργανώσεων, συμπεριλαμβανομένης της εμπορικής, εθνικής κρίσιμης υποδομής και των στρατιωτικών στόχων.
2. Η χρήση των κλεμμένων ή ψευδών ψηφιακών πιστοποιητικών έχει γίνει πιό κοινή, ειδικά ως τμήμα των στοχοθετημένων επιθέσεων.
3. Σε διάφορες στοχοθετημένες επιθέσεις, το malware κρύφτηκε με ενσωμάτωση σε διάφορα αρχεία - με μερικές περιπτώσεις του πολλαπλασίου. Αυτή η μέθοδος μπορεί να αποφύγει το λογισμικό ασφάλειας που αποτυγχάνει να ανιχνεύσει αρκετά βαθιά.
4. Το Blackhole έχει γίνει το επικρατέστερο «πακέτο» το δεύτερο εξάμηνο του 2011 με ένα τεράστιο περιθώριο από τα άλλα. Μερικές από τις εξαρτήσεις άθλου που δραστηριοποιήθηκαν στο παρελθόν χρησιμοποιούνται σπάνια τώρα ή εγκαταλείφθηκαν ουσιαστικά.
5. Οι νεώτερες εκδόσεις του Blackhole επεκτείνονται πρώτα στην Ανατολική Ευρώπη. Οι συντάκτες του αύξησαν τη συχνότητα αναπροσαρμογών του και πρόσθεσαν νέους άθλους και τεχνάσματα για να αποφύγουν την ανίχνευση, όπως ο έλεγχος της έκδοσης λογισμικού στη μηχανή πελατών πριν προσπαθήσουν να το χρησιμοποιήσουν.
6. Οι πλαστές ανακοινώσεις κοινωνικών μέσων είναι τώρα ένας επικρατών τρόπος για τους spammers χτυπώντας τις συνδέσεις των χρηστών – θυμάτων.

7. Το Facebook συνεχίζει να είναι ένας αγωγός για το spam και malware, δεδομένου ότι πολλές εκστρατείες διαδίδουν ιούς με την προσέλκυση των χρηστών για να μοιραστούν τις θέσεις που υπόσχονται, τις κάρτες δώρων ή άλλες ανταμοιβές.
8. Οι χακαρισμένοι ιστοχώροι έπαιξαν έναν κύριο ρόλο στη διανομή spam και malware με τον επαναπροσανατολισμό των μηχανών αναζήτησης στον τελευταίο προορισμό.
9. Το κακόβουλο περιεχόμενο Ιστού εκμεταλλεύεται αυτήν την περίοδο περισσότερες από 50 ευπάθειες στα διάφορα προϊόντα λογισμικού. Τα συνηθέστερα χρησιμοποιημένα προϊόντα είναι το Microsoft Internet Explorer, η Oracle Java, το Adobe Acrobat Reader, το Adobe Flash και προϊόντα του Microsoft Office.

5.3 ΣΤΑΤΙΣΤΙΚΑ ΣΤΟΙΧΕΙΑ ΤΟΥ ΕΡΓΑΣΤΗΡΙΟΥ M86 SECURITY

Χάρτης κατανομής Malware



Εικόνα 1: Παγκόσμιος χάρτης με τις ποιο κοινές τοποθεσίες διακομιστών που παρουσιάζουν malware.

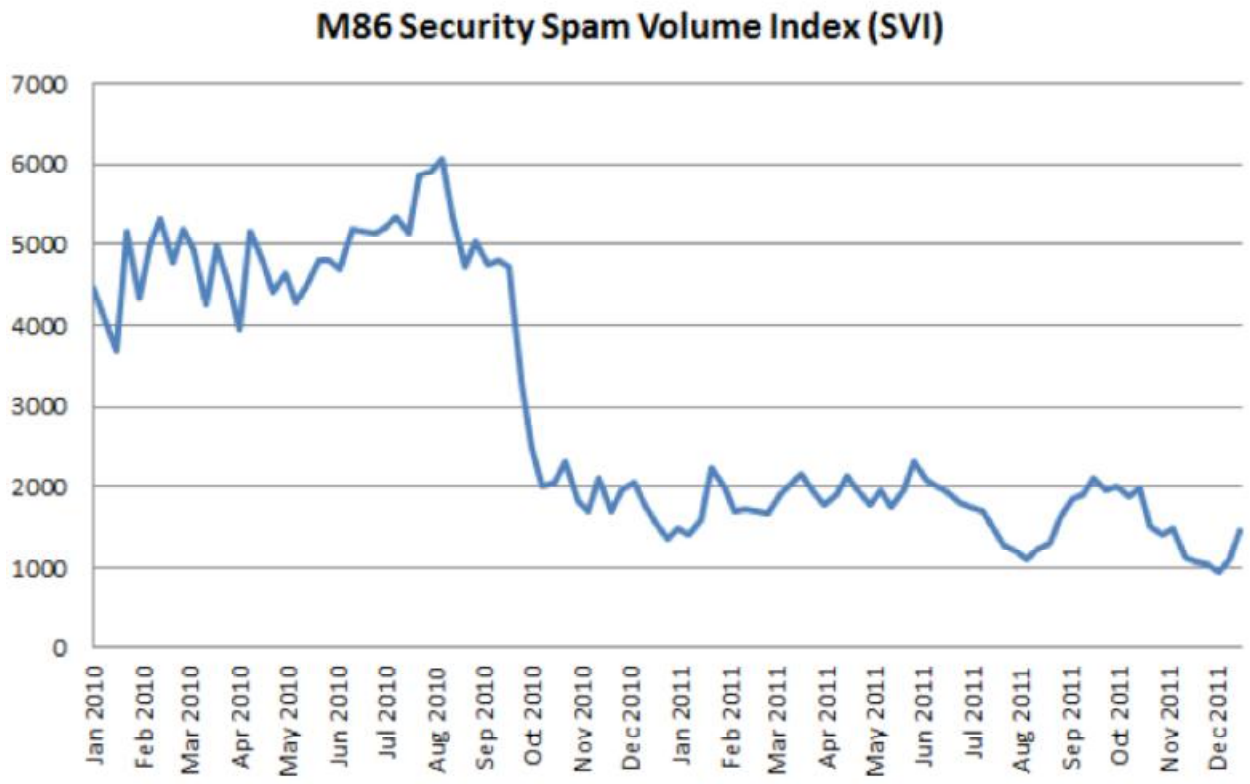
Ο χάρτης παγκόσμιου Malware παρουσιάζει τη κατανομή του κακόβουλου διαδικτυακού περιεχομένου παγκοσμίως. Επισημαίνει τη θέση του διακομιστή που φιλοξενεί το κακόβουλο περιεχόμενο, το οποίο είναι συνήθως διαφορετικό από τη θέση του συμβιβασμένου διακομιστή.
Με βάση τον παραπάνω χάρτη, οι ΗΠΑ συνεχίζουν να είναι η χώρα που οι διακομιστές περιέχουν το μεγαλύτερο μερίδιο του κακόβουλου διαδικτυακού περιεχομένου, που φιλοξενεί σχεδόν το μισό από το κακόβουλο περιεχόμενο σε ολόκληρο τον κόσμο (49.2%). Τα κράτη με τους πιο ενεργούς κακόβουλους διακομιστές είναι τα εξής: Φλόριντα, Καλιφόρνια, Τέξας και Ουάσιγκτον. Για παράδειγμα στη Φλόριντα η εταιρία διαδικτυακής ασφαλείας M86 εντόπισε 15.000 σελίδες με κακόβουλο λογισμικό όπου αποπροσανατόλιζε τις μηχανές αναζήτησης προς ένα ιστοχώρο που εμφάνιζε πλαστά αντιϊικά. Στη Καλιφόρνια και το Τέξας, διάφοροι ιστοχώροι φιλοξενούσαν προγράμματα κλοπής κωδικών πρόσβασης (stealers) όπως είναι το Sinowal. Παράλληλα στην Ουάσιγκτον αρκετοί ιστοχώροι φιλοξενούσαν malware, το οποίο παρουσιάζονταν στους χρήστες με ονομασίες κανονικών προγραμμάτων λογισμικού, όπως το πρόγραμμα αποσυμπίεσης 7Zip και το λογισμικό προβολής αρχείων πολυμέσων Xvid.
Οι διακομιστές της Ρωσίας περιέχουν το δεύτερο μεγαλύτερο αριθμό κακόβουλων σελίδων κατά 6.0%. Η υψηλή ποσότητα κακόβουλων διακομιστών που βρίσκονται σε αυτήν την χώρα δεν προκαλεί ιδιαίτερη έκπληξη, επειδή υπάρχει μεγάλος αριθμός ομάδων δημιουργίας και διανομής malware, συμπεριλαμβανομένων σε αυτή τη χώρα. Εξήντα τρία τοις εκατό του κακόβουλου περιεχομένου που φιλοξενείται στη Ρωσία βρίσκονται στη Μόσχα και τα προάστιά της.
Η Γερμανία παρουσιάζει το 5.9% του κακόβουλου διαδικτυακού περιεχομένου, και τα πιο κοινά προγράμματα εκμετάλλευσης αφορούν

τον Internet Explorer (CVE-2006-0003), Java (CVE-2010-1423) και διαδικτυακά συστατικά του Microsoft Office (CVE-2002-0727).

Μεγάλος αριθμός κακόβουλου διαδικτυακού περιεχομένου φιλοξενούνται στους διακομιστές της Κίνας, επίσης με 4.5%. Τα πιο κοινά προγράμματα εκμετάλλευσης στην Κίνα στοχεύουν στις παλαιότερες εκδόσεις του Microsoft Internet Explorer. Σύμφωνα με πληροφορίες, η έκδοση 6 του Internet Explorer, που κυκλοφόρησε πίσω το 2001, συνήθως χρησιμοποιείται ακόμα στην Κίνα, και επομένως είναι ένας άριστος στόχος για κυβερνοεπιθέσεις.

5.4 Ο ΔΕΙΚΤΗΣ ΟΓΚΟΥ SPAM ΜΕΙΩΝΕΤΑΙ

Καθ' όλη τη διάρκεια του 2011, ο όγκος του spam συνέχισε να παραμένει σε χαμηλά ιστορικά επίπεδα, γεγονός που απεικονίζει τις ουσιαστικές αλλαγές στο τρόπο δημιουργίας και διακίνησης του spam. Η M86 χρησιμοποιεί έναν ειδικό δείκτη ελέγχου της διακίνησης του spam ο οποίος ονομάζεται SVI (Spam Volume Index ή Δείκτης όγκου Spam). Μέχρι τα μέσα Δεκεμβρίου του 2011, το SVI περιορίστηκε στη τιμή 1.000, που ήταν ακριβώς η μισή τιμή από αυτή του δείκτη τον Ιούνιο του 2010, και στο χαμηλότερο επίπεδο από το 2007, όταν χρησιμοποιήθηκε αρχικά ο δείκτης.



Εικόνα 2: Δείκτης όγκου ασφάλειας Spam

Διάφοροι παράγοντες οδήγησαν στο κατρακύλισμα του όγκου του spam στο τέλος του 2010. Πιο σημαντικότερα, το Spamit.com, ένα κακόβουλο υπόγειο πρόγραμμα που αρκετά botnets χρησιμοποίησαν, διακόπηκε τον Σεπτέμβριο του 2010. Το Spamit.com συνδέθηκε στενά με το φαινόμενο του «καναδικού φαρμακείου» και άλλες μάρκες φαρμάκων που διακινούνταν από ψευδεπίγραφα φαρμακεία. Επίσης, διάφορες επιπλοκές στα botnet είχαν αρνητική επίπτωση στην παραγωγή του spam, συμπεριλαμβανομένου των mega-D, Rustock και Kelihos botnets.

Στα τέλη του 2011, ο δείκτης όγκου spam μειώθηκε ξανά γιατί η παραγωγή από το botnet Xarvester έπεσε τον Αύγουστο. Ομοίως, το spam Maazben έπεσε κατά πολύ τον Οκτώβριο. Επιπλέον, οι επιχειρήσεις των αντίπαλων ψευδεπίγραφων φαρμακευτικών προγραμμάτων στη Ρωσία μειώθηκαν όταν συλλήφθηκαν οι χειριστές τους είτε βγήκαν στην παρανομία.

Καθώς ο όγκος του spam έπεσε, το ποσοστό του spam στο συνολικό εισερχόμενο ηλεκτρονικό ταχυδρομείο μειώθηκε από περίπου 90% το Σεπτέμβριο του 2010 σε περίπου 70% τον Δεκέμβριο του 2011. Έτσι αν και η χαμηλότερη παραγωγή spam αποτελεί σίγουρα μια ευπρόσδεκτη είδηση, το spam ακόμα αποτελεί ένα σημαντικό ποσοστό του συνολικού εισερχόμενου ηλεκτρονικού ταχυδρομείου και είναι όλο και περισσότερο κακόβουλο. Υπό αυτήν τη μορφή, το spam παραμένει μια σημαντική απειλή για τους περισσότερους οργανισμούς ή επιχειρήσεις.

5.5 SPAM BOTNETS: ΕΠΙΧΕΙΡΗΣΗ ΩΣ ΣΥΝΗΘΩΣ

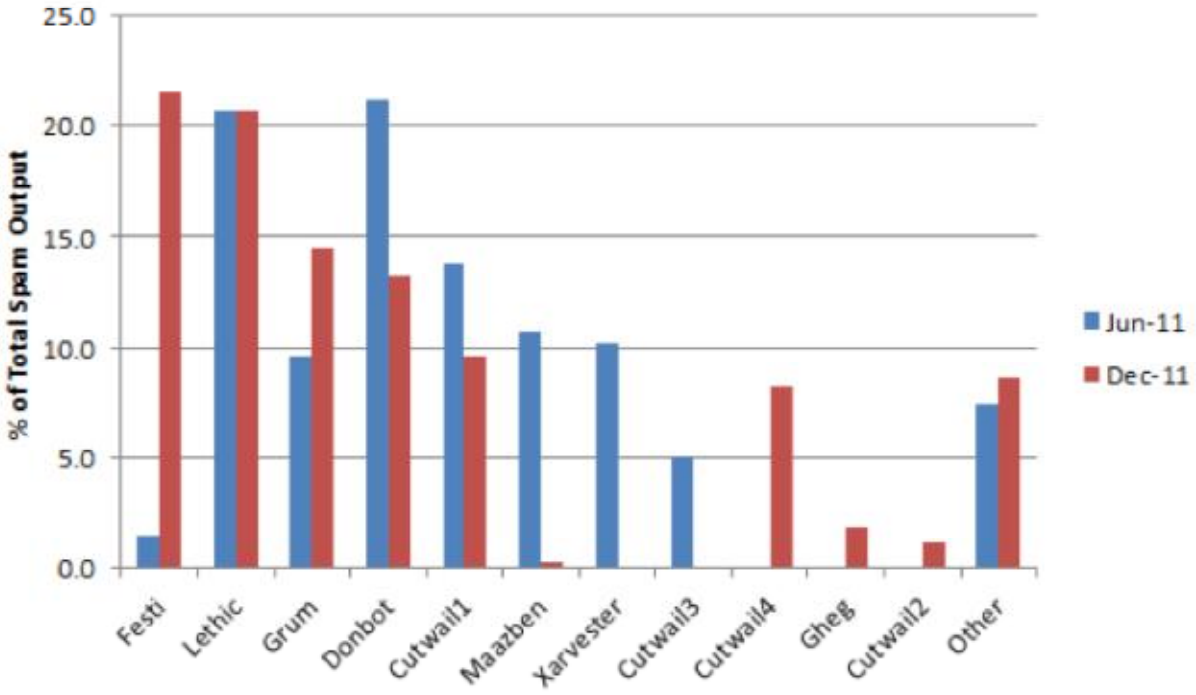
Ο όγκος του spam εκπέμπεται από τα botnets, τα οποία είναι δίκτυα υπολογιστών που συμβιβάζονται από το malware. Τα εργαστηρια ασφαλείας M86 ελέγχουν την παραγωγή spam από σημαντικά botnets με την παρατήρηση των μολυσμένων μηχανών σε ένα κλειστό περιβάλλον, και με τη σύγκριση της συμπεριφοράς με τις εισερχόμενες τροφές spam για να μετρήσουν τα επίπεδα δραστηριότητας κάθε botnet. Τα spamming Botnets είναι συνεχώς σε ροή, που απεικονίζουν τη φύση της υπόγειας αγοράς. Το Botnets morph, γίνεται ξεπερασμένο, αντικαθίσταται, αποσύρεται και αναβαθμίζεται σε απάντηση στις χρηματιστηριακές δυνάμεις, στον ανταγωνισμό και την επιβολή νόμου.

Μέχρι τον Δεκέμβριο του 2011, τα οκτώ κορυφαία spamming botnets ήταν αρμόδια για 90% του spam που ελέγχθηκε από το M86 Security. Ενώ η παραγωγή spam από τα διαφορετικά botnets κυμαινόταν καθ' όλη τη διάρκεια του 2011, το πιο αξιοπρόσεχτο είναι ότι δεν υπάρχει κανένας ουσιαστικός νεοφερμένος στο μπλοκ. Όλα τα κορυφαία spamming botnets είναι γνωστά και κυκλοφορούν για αρκετό καιρό, αν και συνεχώς αλλάζουν μορφή.

Οι δύο βασικές αλλαγές κατά τη διάρκεια των προηγούμενων έξι μηνών είναι ότι τα αυτόκλητα μηνύματα εξόδου αυξήθηκαν σημαντικά, ενώ τα spam από τα Xarvester και Maazben σημείωσαν πτώση για λόγους που είναι ασαφείς.

Αυτό συνέβαλε σε μια πτώση στους γενικούς όγκους spam. Ένα σημείο που αξίζει να αναφερθεί είναι ότι υπάρχουν διάφορες εκδόσεις αυτόκλητων μηνυμάτων, κάθε ένα με τις υπογραφές του. Αυτό συνέβαλε σε μια πτώση στους γενικούς όγκους spam. Ένα σημείο που αξίζει να αναφερθεί είναι ότι υπάρχουν διάφορες εκδόσεις κακόβουλων Cutwail, κάθε ένα με τις υπογραφές τους, όμως όλοι εκπέμπουν spam με τα χαρακτηριστικά γνωρίσματα του Cutwail. Τους ακολουθούμε χωριστά, αλλά μπορούν καλά να ελεγχθούν από την ίδια ομάδα.

ΚΟΡΥΦΑΙΑ SPAM BOTNETS: ΙΟΥΝΙΟΣ – ΔΕΚΕΜΒΡΙΟΣ 2011



Εικόνα 3: Κορυφαία Spam Botnets τον Ιούνιο του 2011 και τον Δεκέμβρη 2011

5.6 ΚΑΤΗΓΟΡΙΕΣ SPAM: ΤΟ ΠΟΣΟΣΤΟ ΤΩΝ ΚΑΚΟΒΟΥΛΩΝ SPAM ΑΥΞΑΝΕΤΑΙ

Οι κορυφαίες τέσσερις κατηγορίες spam είναι παρόμοιες με όσα είδαμε στο πρώτο εξάμηνο του έτους, ήτοι 47% φαρμακευτική (χάπια και θεραπείες), ρεπλίκες 13% (απομιμήσεις σε ρολόγια και τσάντες),12% στα τυχερά παιχνίδια (καζίνο) και σε ραντεβού το 12% (onlinedating ιστοσελίδες). Αυτές οι κατηγορίες απεικονίζουν τη διαθεσιμότητα και την ελκυστικότητα των διάφορων προγραμμάτων μάρκετινγκ που οι spammers ενώνουν για να κάνουν τα χρήματα.

Μια αξιοπρόσεχτη τάση είναι η άνοδος του malware – σχετικός με το spam στο δεύτερο εξάμηνο του 2011. Κατ' αρχάς, τα εργαστήρια ασφάλειας M86 παρατήρησαν μια μεγάλη αύξηση στο κακόβουλο spam με τις εκτελέσιμες συνδέσεις τον Αύγουστο και το Σεπτέμβριο. Συγκριτικά με τα στοιχεία νωρίτερα στο έτος, αυτό ήταν ένα ογκώδες κύμα από λιγότερο από 1% του συνολικού spam σε περισσότερο από 20% στην αιχμή του. Μετά από το Νοέμβριο, όταν αυτό το αρχικό κύμα μειώθηκε, αρχίσαμε να βλέπουμε στους αυξανόμενους όγκους των συνδυασμένων απειλών κακόβουλων spam - αυτή τη φορά με τους συνδέσμους υπερ-κειμένου που οδηγούν στο malware. Προς το τέλος του 2011, αυτές οι κακόβουλες εκστρατείες αντιπροσώπευσαν 5-10% του συνολικού spam.[23]

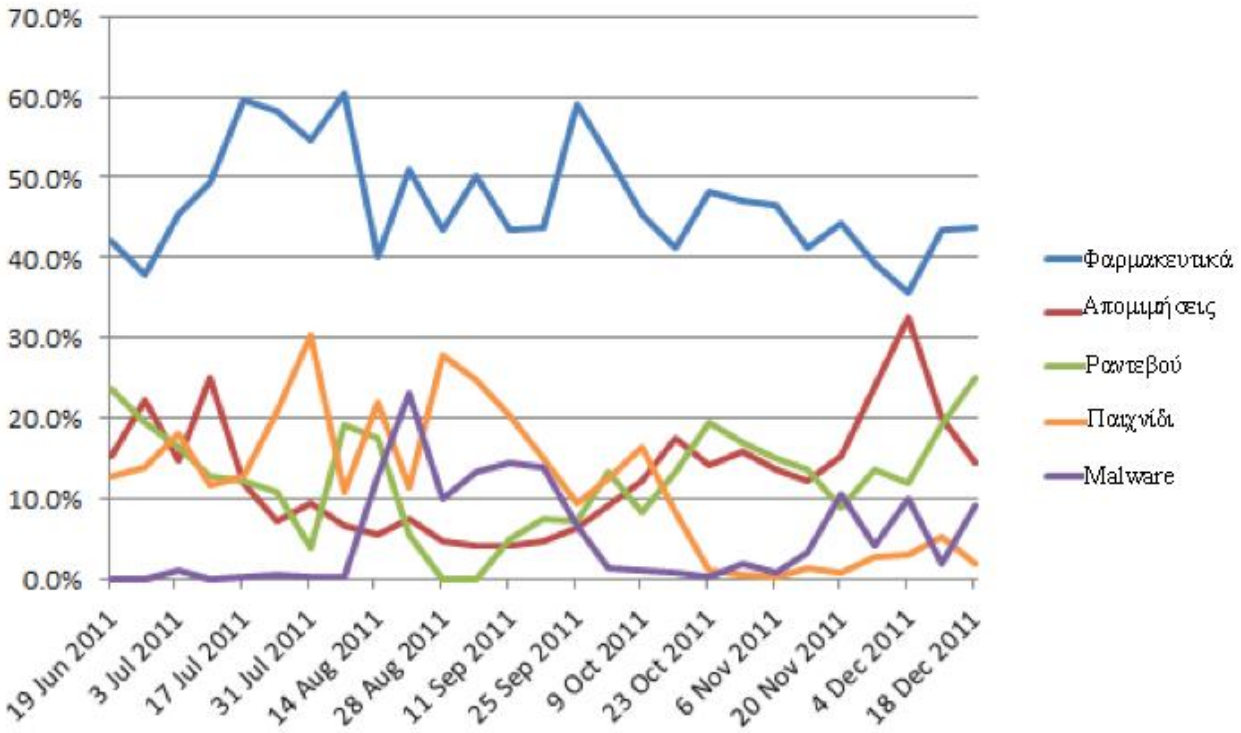
ΚΑΤΗΓΟΡΙΕΣ SPAM ΙΟΥΝΙΟΣ – ΔΕΚΕΜΒΡΙΟΣ 2011

ΠΟΣΟΣΤΟ % ΣΥΝΟΛΙΚΟΥ SPAM

Φαρμακευτικά	46,90%
Για Ενήλικους	0,30%

Απάτη	0,20%
Διπλώματα	0,70%
Malware	5,30%
Λογισμικό	7,20%
Ραντεβού	12,60%
Απομιμήσεις	13,00%
Άλλο	3,10%

Εικόνα 4: Κατηγορίες SPAM



Εικόνα 5:Κορυφαίες κατηγορίες Spam

ΣΥΜΠΕΡΑΣΜΑΤΑ

Με την συνεχή εξέλιξη του ηλεκτρονικού εμπορίου, τα θέματα ασφάλειας και η προστασία των προσωπικών δεδομένων θα αποτελούν πάντα αχίλλειο πτέρνα του συστήματος, με αποτέλεσμα οι περισσότεροι καταναλωτές – χρήστες να φοβούνται να προβούν σε τέτοιου είδους συναλλαγές.

Βέβαια, η ισχύουσα νομοθεσία για το ηλεκτρονικό εμπόριο και για την μη ζητηθείσα ηλεκτρονική αλληλογραφία δημιουργούν ένα ασφαλές περιβάλλον για τις ηλεκτρονικές συναλλαγές. Παράλληλα, έχουν αναπτυχθεί αρκετά λογισμικά για την ασφάλεια των πληροφοριών και την προστασία των προσωπικών δεδομένων σε επίπεδο χρήστη, παροχέων υπηρεσιών Διαδικτύου και όσων εμπλέκονται στις ηλεκτρονικές συναλλαγές, που κάνουν πιο εύκολη την όλη διαδικασία.

Αν και το Διαδίκτυο αποτελεί ένα πολύ σημαντικό εργαλείο για όλους μας, οι κίνδυνοι που ελλοχεύουν καθημερινά κάνουν την χρήση του όλο και πιο δύσκολη. Οι spammers βρίσκουν συνεχώς καινούργιους τρόπους για να εισβάλλουν στους υπολογιστές των χρηστών, με σκοπό την συγκομιδή πληροφοριών, όπως κωδικούς τραπεζικών λογαριασμών, αλλά και να τους παραπλανούν μέσω του ηλεκτρονικού ταχυδρομείου κλπ.

Το ηλεκτρονικό ταχυδρομείο που όπως έχουμε αναφέρει και πάλι αποτελεί μια από τις δημοφιλέστερες υπηρεσίες του Internet κρύβει κινδύνους και απειλές οι οποίες μέχρι ένα βαθμό μπορούν να καταπολεμηθούν, με την χρήση προγραμμάτων και συσκευών. Το ηλεκτρονικό ταχυδρομείο είναι μια υπηρεσία, με τάση συνεχώς να αυξάνεται η δημοτικότητά της, μιας και αποτελεί τον βασικό τρόπο ηλεκτρονικής επικοινωνίας. Άρα, συνεχώς θα εξελίσσεται και θα προστατεύεται από εταιρίες και οργανισμούς με αυτόν το σκοπό. Αλλά

αυτό που πρέπει να κάνει ο κάθε χρήστης για να προστατευθεί είναι να είναι ενήμερος και προσεκτικός στο πως την χρησιμοποιεί. Πρέπει να μπορεί να αναγνωρίζει πότε πρόκειται για αλληλογραφία η οποία είναι σημαντική για αυτόν και πότε είναι κακόβουλη ή απλά άχρηστη. Σε αυτό βοηθούν όσο μπορούν και οι ίδιοι οι πάροχοι της. Αυτό φαίνεται και από τα ποσοστά ανεπιθύμητης αλληλογραφίας που καταλήγει στα mail box των χρηστών, σήμερα σε σχέση με το παρελθόν.

Έτσι, για να μην φτάσουμε στο σημείο να πιστεύουμε πως οι υπηρεσίες του Διαδικτύου είναι επικίνδυνες για τα προσωπικά μας δεδομένα και να φοβόμαστε να τις χρησιμοποιήσουμε, πρέπει οι χρήστες να εκπαιδευτούν για να μπορούν να αντεπεξέλθουν στους κινδύνους που παρουσιάζονται. Η εκπαίδευση των χρηστών αποτελεί την βασικότερη γραμμή άμυνας εναντίον στην μη ζητηθείσα ηλεκτρονική αλληλογραφία (spam) και αυτό γιατί υπάρχουν πολλοί χρήστες, οι οποίοι δεν έχουν πολλές γνώσεις σχετικά με τις υπηρεσίες του Διαδικτύου και πολλές φορές πέφτουν θύματα απατών από τους spammers.

Πρέπει όλοι οι χρήστες να είναι σε θέση να αναγνωρίσουν την κακόβουλη και ανεπιθύμητη αλληλογραφία για να μπορούν να αμυνθούν κατάλληλα.

Τέλος, όλη η προσπάθεια που γίνεται για την αντιμετώπιση της ανεπιθύμητης αλληλογραφίας είναι μία προσπάθεια για να διατηρηθεί ο ηλεκτρονικός τρόπος επικοινωνίας, ένα σημαντικό εργαλείο στην καθημερινότητά μας.

Συμπερασματικά, αναφέρονται παρακάτω ορισμένοι «κανόνες» τους οποίους πρέπει να ακολουθήσει ένας χρήστης για την αποφυγή των ανεπιθύμητων ηλεκτρονικών μηνυμάτων, έτσι ώστε να καταφέρει να «απολαύσει» τις δυνατότητες και τα πλεονεκτήματα που σήμερα προσφέρει η ηλεκτρονική αλληλογραφία χωρίς να αντιμετωπίσει κάποιο ιδιαίτερο πρόβλημα:

1. Μην δημοσιεύετε την διεύθυνση ηλεκτρονικού ταχυδρομείου σας
2. Μην δίνετε την διεύθυνση ηλεκτρονικού ταχυδρομείου σε οργανισμούς που δεν εμπιστεύεστε.
3. Μην απαντάτε στο spam.
4. Αναφέρετε κάθε μήνυμα spam που λαμβάνετε.
5. Διαδώστε την γνώση σας και την εμπειρία σας σε σχέση με το spam.
6. Ελέγξτε τα συστήματα σας, ώστε να είναι σωστά διαμορφωμένα και ασφαλή.
7. Προμηθευτείτε τα σωστά προγράμματα για την καταπολέμηση του spam.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1]Γκρίτζαλης Σ, Κάτσικας Σ, (2003) *Ασφάλεια Δικτύων Υπολογιστών – Τεχνολογίες και υπηρεσίες σε περιβάλλοντα ηλεκτρονικού επιχειρείν και ηλεκτρονικής διακυβέρνησης*, Εκδόσεις Παπασωτηρίου.

[2]Κάτσικας Σ, Γκρίτζαλης Δ, Γκρίτζαλης Σ, (2004) *Ασφάλεια Πληροφοριακών Συστημάτων*, Εκδόσεις Νέων Τεχνολογιών.

[3]Κοζύρης Φ., Θεοδωρίδης Κ., (2006), *Διαφήμιση & Παρενόχληση: spam και τηλεόραση*, Εκδόσεις Αντ. Ν. Σάκκουλα

[4]Νομικό περιοδικό 'Αρμενόπουλος 2007/993', *Μελέτη «Διαδίκτυο και Αστικό Δίκαιο»* του Παν. Κορνηλάκη

[5]Comer D., (2007) *Δίκτυα και Διαδίκτυα Υπολογιστών – και εφαρμογές τους στο Internet*, Εκδόσεις Κλειδάριθμος.

[6]Scambray J, McClure S, Kurtz G, (2003) *Χάκερ Επίθεση και Άμυνα - Τέταρτη Έκδοση 2003*, Εκδόσεις Μ. Γκιούρδας.

[7]Stanger J, (2000) *E-mail Virus Protection Handbook*, Εκδόσεις Syngress.

ΔΙΑΔΙΚΤΥΑΚΕΣ ΠΗΓΕΣ

[8]www.cnc.uom.gr/services/pdf/seminars/INTERNET.doc

[9]http://blog.tech-spot.gr/2007/11/11/386

[10]http://blogs.in.gr/gepitidios/archive/2008/02/01/624.aspx

[11]http://blogs.technet.com/pamal/archive/2006/02/10/419211.aspx

[12] http://www.cnc.uom.gr/services/guides/email.pdf

[13]http://chtsanti.net/Firewall.html

[14]http://el.wikipedia.org/wiki/E-mail_bomb

[15]http://el.wikipedia.org/wiki/Post_Office

[16] http://dide.ilei.sch.gr/keplinet/tech/spam.php

[17]http://www.no-spam.gr/mustknow.htm

[18]http://www.spam.com

[19] http://portal.kathimerini.gr/4Dcgi/4dcgi/_w_articles_kathworld_7_13/04/2011_387432

[20] http://www.alfavita.gr

[21] http://www.i-reportergr.com/2010/03/blog-post_986.html

[22] http://www.infosoc.gr

[23]
http://www.m86security.com/documents/pdfs/security_labs/m86_security_labs_report_2h2011.pdf