Τμήμα Τεχνολογίας Πληροφορικής και Τηλεπικοινωνιών

Α.Τ.Ε.Ι. Καλαμάτας – Παράρτημα Σπάρτης

ΑΡΧΙΤΕΚΤΟΝΙΚΕΣ ΦΙΛΤΡΑΡΙΣΜΑΤΟΣ ΑΝΕΠΙΘΥΜΗΤΩΝ ΚΑΚΟΒΟΥΛΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΜΗΝΥΜΑΤΩΝ (SPAM FILTERING ARCHITECTURES)

Αιβαλιώτη Χρυσοβαλάντου

Ελευθερίου Γεωργία- Αγάπη

Παπαπολυχρονίου Άγγελος

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: Μακροδημήτρης Γεώργιος

-2012-

Τμήμα Τεχνολογίας Πληροφορικής και Τηλεπικοινωνιών

Α.Τ.Ε.Ι. Καλαμάτας – Παράρτημα Σπάρτης

ΑΡΧΙΤΕΚΤΟΝΙΚΕΣ ΦΙΛΤΡΑΡΙΣΜΑΤΟΣ ΑΝΕΠΙΘΥΜΗΤΩΝ ΚΑΚΟΒΟΥΛΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΜΗΝΥΜΑΤΩΝ (SPAM FILTERING ARCHITECTURES)

Αιβαλιώτη Χρυσοβαλάντου 2006245

Ελευθερίου Γεωργία- Αγάπη 2006196

Παπαπολυχρονίου Άγγελος 2006207

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: Μακροδημήτρης Γεώργιος

Περιεχόμενα

2012

ΠΕΡΙΕΧΟΜΕΝΑ ΕΙΚΟΝΩΝ

ΕΥΧΑΡΙΣΤΙΕΣ

Θα θέλαμε να ευχαριστήσουμε τον επιβλέποντα καθηγητή μας κ. Γεώργιο Μακροδημήτρη για την εμπιστοσύνη που μας έδειξε και για την αμέριστη συμπαράσταση του στις κάθε είδους δυσκολίες που συναντήσαμε καθ' όλη την διάρκεια της πτυχιακής μας εργασίας. Η διαρκής βοήθεια και η καθοδήγηση του ήταν απαραίτητη και πολύτιμη.

Τέλος θα θέλαμε να ευχαριστήσουμε τις οικογένειες μας για την οικονομική και κυρίως ηθική υποστήριξη όλα αυτά τα χρονιά.

ΠΡΟΛΟΓΟΣ

Η εργασία έχει ως στόχο τον προσδιορισμό της έννοιας spam,την ανάλυση των επιπτώσεων της στον οικονομικό τομέα, την νομική της αντιμετώπιση από τις περισσότερες χώρες, καθώς και την παρουσίαση μεθόδων για την ουσιαστική επίλυση του προβλήματος. Το spamming είναι η αποστολή μηνυμάτων . κυρίως διαφημιστικού περιεχομένου, προς αγνώστους παραλήπτες. Έχοντας ως βασικό στόχο του, την προώθηση προϊόντων, ιδεών, ή προσώπων. Μπορεί να το συναντήσει κανείς σε διάφορες μορφές όπως: email spam, messaging spam.blog spam, spamdexing, usenet spam. Οι επιπτώσεις του στην οικονομία είναι αρκετά σημαντικές και χρήζει άμεσης αντιμετώπισης. Πολλές από τις χώρες της Ευρωπαϊκής Ένωσης έχουν θεσπίσει ειδικούς νόμους τόσο για την προάσπιση των προσωπικών δεδομένων, όσο και για την τιμωρία όλων όσων σχετίζονται με την αποστολή άχρηστων μηνυμάτων μέσω διαδικτύου. Τέλος παρουσιάζονται ορισμένες χρήσιμες συμβουλές για τους απλούς χρήστες, προκειμένου να μειώσουν τον αριθμό των spam mail που δέχονται καθημερινά, όπως επίσης και οι τεχνικές που έχουν υιοθετηθεί από τις μεγάλες εταιρείες για την διασφάλιση των συμφερόντων τους.

ΕΙΣΑΓΩΓΗ

Η ραγδαία εξέλιξη της τεχνολογίας σε συνάρτηση με την ανάπτυξη της πληροφορικής καθώς και με την ταχύτητα εξάπλωσης της χρήσης του Διαδικτύου, έχουν συντελέσει στη ριζική διαφοροποίηση της παραγωγικής διαδικασίας, έχουν επιφέρει πρωτόγνωρες και ριζοσπαστικές αλλαγές όχι μόνο στις εργασιακές σχέσεις και στις συναλλαγές αλλά και σε οποιαδήποτε άλλη πτυχή της καθημερινότητας και της ανθρώπινης επαφής.

Η σημαντική συμβολή της τεχνολογίας στην απλούστευση των καθημερινών δραστηριοτήτων, τόσο στο ατομικό επίπεδο του μεμονωμένου χρήστη όσο και στο συλλογικό επίπεδο των μεγάλων εταιρειών, αποτελεί ένα αδιαμφισβήτητο γεγονός. Οι ηλεκτρονικοί υπολογιστές πλέον αποτελούν αναπόσπαστο κομμάτι της ζωής μας και έχουν μετατραπεί από είδος πολυτελείας που θεωρούνταν κάποτε σε είδος πρώτης ανάγκης, κυρίως όσον αφορά στη χρήση τους στον τομέα της εργασίας. Σταδιακά όμως τείνουν να χρησιμοποιούνται ολοένα και περισσότερο από μεμονωμένους χρήστες για την κάλυψη των προσωπικών τους αναγκών, γεγονός το οποίο είναι άκρως ενθαρρυντικό για την μετέπειτα εξέλιξη των τεχνολογικών συστημάτων έχοντας ως κύριο σκοπό την αύξηση των δυνατοτήτων τους και την βελτίωση των υπηρεσιών που παρέχουν.

Βέβαια αξίζει να σημειώσει κανείς και τον καθοριστικό ρόλο που διαδραμάτισε η δημιουργία του Παγκοσμίου Ιστού (World Wide Web) σε όλες τις εκφάνσεις της καθημερινής ζωής του ανθρώπου. Οι δυνατότητες και οι υπηρεσίες που παρέχει το Διαδίκτυο προς κάθε χρήστη είναι πλέον απεριόριστες και έχει κατορθώσει να δώσει διαφορετική διάσταση σε πολλές πατροπαράδοτες έννοιες όπως αυτής της αγοραπωλησίας, της ενημέρωσης, της ψυχαγωγίας, της επικοινωνίας, της διαφήμισης κτλ. Με άλλα λόγια, το Internet προσφέρει τη δυνατότητα πρόσβασης σε πολυάριθμες τράπεζες πληροφοριών, ανάλογα με θέμα αναζήτησης του χρήστη, άμεσα και γρήγορα και ειδικότερα σε πολύ χαμηλό κόστος.

Παράλληλα όμως με όλες αυτές τις απεριόριστες δυνατότητες που έχουν ως κύριο στόχο τους να διευκολύνουν, να προάγουν και να βοηθήσουν στη βελτίωση της ποιότητας ζωής, την ανύψωση του βιοτικού επιπέδου των ανθρώπων και στην τάχιστη εξυπηρέτηση των αναγκών που δημιουργεί η σύγχρονη κοινωνία, οι νέες τεχνολογίες και το Διαδίκτυο δημιούργησαν ιδανικές συνθήκες για την καλλιέργεια και την ανάπτυξη νέων μορφών εγκληματικότητας που συνοψίζονται στον όρο Ηλεκτρονικό Έγκλημα. Μια μορφή του σύγχρονου ηλεκτρονικού εγκλήματος είναι και το spamming ,το οποίο και θα αναλύσουμε στη συνέχεια της παρούσας μελέτης.

ΚΕΦΑΛΑΙΟ 1

ΓΕΝΙΚΑ ΓΙΑ ΤΟ SPAMMING

1.1 Ορισμός του Spamming

"Spamming είναι η σύγχρονη μάστιγα του ηλεκτρονικού ταχυδρομείου και των ομάδων πληροφόρησης του Διαδικτύου. Μπορεί να παρεμποδίσει την λειτουργία των δημοσίων υπηρεσιών και έχει τεράστια επίδραση στην ομαλή χρήση του προσωπικού ηλεκτρονικού ταχυδρομείου οποιουδήποτε χρήστη. Στην πραγματικότητα οι Spammers δεσμεύουν πόρους τόσο από τους χρήστες όσο και από τους προμηθευτές υπηρεσιών, χωρίς καμία αποζημίωση προς αυτούς και χωρίς να υπάρχει κάποια σχετική έγκριση."

Ως spamming ή αλλιώς Unsolicites Commercial Email(UCE) ορίζεται η απρόσκλητη αποστολή email σε πολλούς παραλήπτες. Ένα μήνυμα το οποίο συντάσσεται και αποστέλλεται σε κάποιον τον οποίο γνωρίζει ο αποστολέας, είναι spam. Το ίδιο ισχύει και για την απάντηση σε αυτό. Οι αποστολείς spam μηνυμάτων, με τις δικιές τους μεθόδους και της δική τους πολιτική, αποτελούν πλέον ένα ξεχωριστό κομμάτι του Internet . Πολλές δικτυακές τοποθεσίες δεν το επιτρέπουν επειδή είναι δεοντολογικό και επιπλέον άλλες τοποθεσίες μπορούν να επιλέξουν να μη δέχονται κανένα email από αυτή την προέλευση.

Είναι η πράξη της αποστολής των εκούσιων, μαζικών(και συνήθως εμπορικών) ηλεκτρονικών μηνυμάτων. Αν και αυτό μπορεί να γίνει μέσω οποιουδήποτε αριθμού μέσων, ο πιο κοινός είναι ηλεκτρονικό ταχυδρομείο και το SMS. Το Spam πλημμυρίζει το Διαδίκτυο με πολλά αντίγραφα του ίδιου μηνύματος, σε μια προσπάθεια επιβολής του μηνύματος σε ανθρώπους που, υπό άλλες συνθήκες, δεν θα επέλεγαν να το λάβουν. Ο πιο κοινός και πιο διαδεδομένος στόχος του Spamming είναι η διαφήμιση.

Τα περισσότερα από αυτά είναι εμπορικές διαφημίσεις για προϊόντα σχετικά αμφίβολης ποιότητας και προέλευσης και συνήθως περιλαμβάνουν πορνογραφικό υλικό, λογισμικό ηλεκτρονικών υπολογιστών , προϊόντα ιατρικής όπως το Viagra, λογαριασμούς πιστωτικών καρτών κτλ. Η αποστολή τέτοιων μηνυμάτων κοστίζει ελάχιστα συγκριτικά με το κόστος που επιβαρύνει είτε τους παραλήπτες είτε τους μεταφορείς προϊόντων που προωθούνται με την μέθοδο αυτή.

Θεωρείται ως μια απαράδεκτη μορφή συμπεριφοράς τόσο από του Φορείς Παροχής Υπηρεσιών Διαδικτύου (ISP's) όσο και από τους περισσότερους μεμονωμένους χρήστες. Το μεγαλύτερο ποσό των χρηστών, το θεωρεί άκρως ενοχλητικό και πολλές φορές το περιεχόμενο του είναι προσβλητικό. Επιπλέον οι ISPs δεν φαίνεται να είναι διατεθειμένοι να επωμίζονται το κόστος διαφήμισης των spammers.

Έρευνες που έχουν διεξαχθεί έχουν αποδείξει ότι το spam είναι η πιο ενοχλητική μορφή διαφήμισης στο Internet και γι αυτό το λόγο αποτελεί(για τους περισσότερους ISPs) παραβίαση της Αποδεκτής Πολιτικής του Διαδικτύου (Acceptable Use Policy) και πολλές φορές οδηγεί στην κατάργηση του ηλεκτρονικού λογαριασμού του αποστολέα.

Επιπλέον σε πολλές περιπτώσεις το spamming θεωρείται ως έγκλημα και αδικοπραξία. Η Ομοσπονδιακή Εμπορική Επιτροπή των ΗΠΑ εκτιμά ότι τα 2/3 από τα Spam mails που αποστέλλονται, περιέχουν ψευδείς προσφορές, πλαστογραφημένες επιγραφές εταιρειών που αποσκοπούν στην παραπλάνηση και την παραπληροφόρηση του αποδέχτη τους, στοιχεία που υποδηλώνουν την εγκληματική τους δραστηριότητα.

Ένας μεγάλος αριθμός spammer συμμετέχει σε μια σκόπιμη απάτη προκειμένου να πετύχουν το σκοπό τους, να στείλουν δηλαδή spam mails. Οι spammers συχνά χρησιμοποιούν ψεύτικα ονόματα, ανύπαρκτες διευθύνσεις, λανθασμένους αριθμούς τηλεφώνων και άλλες σχετικές πληροφορίες επαφής, προκειμένου να ενεργοποιήσει λογαριασμούς μιας χρήσης σε διαφορετικούς Internet Providers. Συχνά υποκλέπτουν αριθμούς πιστωτικών καρτών με σκοπό

να πληρώσουν για τους λογαριασμούς που ενεργοποίησαν. Με αυτή την τακτική έχουν την δυνατότητα να κινούνται εύκολα και γρήγορα από τον έναν λογαριασμό στον άλλον δεδομένου ότι όταν ένας τέτοιος λογαριασμός, που χρησιμοποιείται για spamming απενεργοποιείται αυτόματα από τους εκάστοτε ISP's.

Οι Spammers χρησιμοποιούν συχνά spamware, προγράμματα λογισμικού που έχουν την δυνατότητα να ανιχνεύουν το Διαδίκτυο για υπολογιστές που μπορούν να χρησιμοποιηθούν για να παραδώσουν τα Spam μηνύματα για λογαριασμό τους. Αυτό καθιστά πιο δύσκολη την εύρεση της ακριβής-πραγματικής θέσης του spammer και κατά συνέπεια διευκολύνει τις κινήσεις τους.

Πάντως σε γενικές γραμμές οι περισσότεροι αποστολείς μηνυμάτων με διαφημιστικό περιεχόμενο ισχυρίζονταν ως η πράξη τους αυτή δεν αποτελεί spamming. Για παράδειγμα πολλά από τα spam μηνύματα που μεταδίδονται καθημερινός μέσω του Διαδικτύου περιέχουν τον ισχυρισμό ότι οι παραλήπτες που επέλεξαν την παραλαβή τους κάτι που συνήθως δεν συμφωνεί με τις πραγματικές ενέργειες και τις προθέσεις των παραληπτών. Τελικά είναι δύσκολο να καθορίσει κάνεις με ακρίβεια τα είδη των ενεργειών που αποτελούν Spamming και να διατυπώσει έναν ξεκάθαρο ορισμό του.

Τέλος η τακτική αυτή απαγορεύεται από την **Οδηγία 2002.58** όπου στο άρθρο 13 αναφέρεται ότι : «χρησιμοποίηση αυτομάτων συστημάτων κλήσης χωρίς ανθρώπινη παρέμβαση (συσκευές αυτομάτων κλήσεων), τηλεομοιοτυπικών συσκευών (φαξ) ή ηλεκτρονικού ταχυδρομείου για σκοπούς απευθείας εμπορικής προώθησης επιτρέπεται μόνον στην περίπτωση συνδρομητών οι οποίοι έχουν δώσει εκ τα προτέρων τη συγκατάθεση τους» καθώς και από άλλα νομοθετήματα.[1]

[1]Gordon V.Cormack "Email Spam Filtering:A Systematic Review"
Wikipedia.org ,
[2]Wikipedia "Spam(electronic)"
http://www.colinfahey.com/spam_topics/spam_topics_el.html

Οι παρακάτω εικόνες είναι από spam μηνύματα κατά την διάρκεια των ετών 2001-2004.

Εικόνα 1 Αυτό το μήνυμα spam αντιμετωπίζει κάποιο είδος προσωπικής ανασφάλειας και παραβίασης της προσωπικής ασφάλειας

Εικόνα 2 Αυτό το μήνυμα spam προωθεί μια υπηρεσία που επιτρέπει σε ένα πρόσωπο να στέλνουν spam μηνύματα σε 27 εκατομμύρια άτομα.

1.2 Ιστορικά στοιχεία

Προφανώς η λέξη spam περιγράφει αυτό που μας συμβαίνει, το να κατακλύζεται κανείς από ανεπιθύμητα e-mails, πια είναι όμως η ιστορία που κρύβεται πίσω από τη λέξη spam.

Η ερευνά, μας έκανε να ανατρέξουμε στο 1926, όταν το εργοστάσιο κονσερβοποιημένων τροφίμων, Hormel Foods, δημιούργησε την κονσέρβα SPAM , όπου περιείχε ένα μίγμα βοδινού και χοιρινού, παρόμοιο με το "ζαμπονάκι" 'ΣΒΑΝ' που τρώγαμε μικροί. Οι περισσότεροι Αμερικανοί διαισθητικά το αντιλαμβάνονται σαν κάτι άχρηστο, άνευ θρεπτικής αξίας. Πολλοί πιστεύουν ότι ο Όρος Spam προέρχεται από μια κωμωδία των Monty Pythons " Flying Circus", κατά τη διάρκεια της οποίας, διάφοροι χαρακτήρες αναφωνούσαν επανειλημμένως: «Spam spam, spam.....»

Εικόνα 3 "Spam" είναι χοιρινό ζαμπόν τροφίμων και προϊόντων που παράγονται από Hormel Foods

Ο Όρος Spamming χρησιμοποιήθηκε για πρώτη φορά στο χώρο του Internet για να αναφερθεί στα επαναλαμβανόμενα μηνύματα κατά την διάρκεια των MUD games. Χρησιμοποιήθηκε στο USENET για να δηλώσει την έννοια του όρου excessive multiple posting, δηλαδή την επαναλαμβανόμενη αποστολή του ίδιου μηνύματος.

Σύντομα αναφέρθηκε και στον καταιγισμό των USENET newgroups από junk mail, (άχρηστο ταχυδρομείο). Μετά από ένα ζευγάρι δικηγόρων, που ξεκίνησαν την χρήση μαζικής ταχυδρόμησης USENET ως μέθοδο διαφημιστικής προώθησης των συμφερόντων τους, ο Όρος spamming ήρθε να συμπεριλάβει και την έννοια του email spamming και η χρήση του όρου ακλούθησε αρκετά σύντομα.

Ωστόσο το Spamming είχε πολλές μορφές μέσα στα χρόνια. Το πρώτο spam χρονολογείται το 1864.Στις ΗΠΑ η Western Union επέτρεπε να στέλνονται τηλεγραφικά μηνύματα σε πολλαπλούς προορισμούς. Τα πρώτα εμπορικά τηλεγραφήματα χρονολογούνται τον Μάιο του 1864 Από τότε κι ως το κραχ του 1929 οι πλούσιοι Βορειοαμερικάνοι κατακλύζονταν τηλεγραφικά με επενδυτικές προσφορές. Στην Ευρώπη δεν συνέβη κάτι τέτοιο, γιατί τα τηλεγραφήματα ρυθμίζονταν απ' τους κατά χώρα εθνικούς οργανισμούς τηλεπικοινωνιών. Το πρώτο μικρής έκτασης διαφημιστικό Spam στην εποχή των ηλεκτρονικών Υπολογιστών πια , ήταν το 1978 και αφορούσε ένα μοντέλο πληροφορικής της εταιρείας Digital Equipment Corporation και απεστάλη σε 393 παραλήπτες.

Μέχρι το 2009 η πλειοψηφία των Spam μηνυμάτων που εστάλησαν ανά τον κόσμο ήταν στην Αγγλική γλώσσα. Από εκεί κι έπειτα οι Spammers άρχισαν να χρησιμοποιούν αυτόματα μεταφραστικά προγράμματα για να στέλνουν spam σε όλες τις γλώσσες, ανάλογα την χώρα που προορίζονται τα Spam μηνύματα.[2]

[2] Wikipedia "Spam(electronic)"
http://www.colinfahey.com/spam_topics/spam_topics_el.html

Εικόνα 4 "Spam" παρωδία από "Monty Pythons Flying Circus"

1.3 Είδη Spamming

1.3.1 E- mail Spamming

Με τον όρο email spam, χαρακτηρίζεται η μαζική αποστολή ηλεκτρονικών μηνυμάτων προς διαφόρους, αγνώστους παραλήπτες, προκειμένου να εξυπηρετηθούν εμπορικοί και διαφημιστικοί σκοποί. Δεν είναι λίγες οι φορείς που κάποιος από εμάς, κατά τη διάρκεια του ελέγχου της ηλεκτρονικής του ταχυδρομικής θυρίδας, διαπίστωσε πως έχει γίνει αποδέκτης μηνυμάτων άγνωστης προέλευσης. Το περιεχόμενο των μηνυμάτων αυτών είναι συνήθως ανούσιο και πολλές φορές προσβλητικό προς τον ίδιο τον παραλήπτη.

Οι περισσότεροι spammers ηλεκτρονικού ταχυδρομείου αποστέλλουν τα μηνύματα τους διαμέσου ανοιχτών ηλεκτρονόμων (open mail relays). Το σύστημα SMTP που χρησιμοποιείται για την προώθηση των ηλεκτρονικών μηνυμάτων από τον έναν κεντρικό υπολογιστή στον

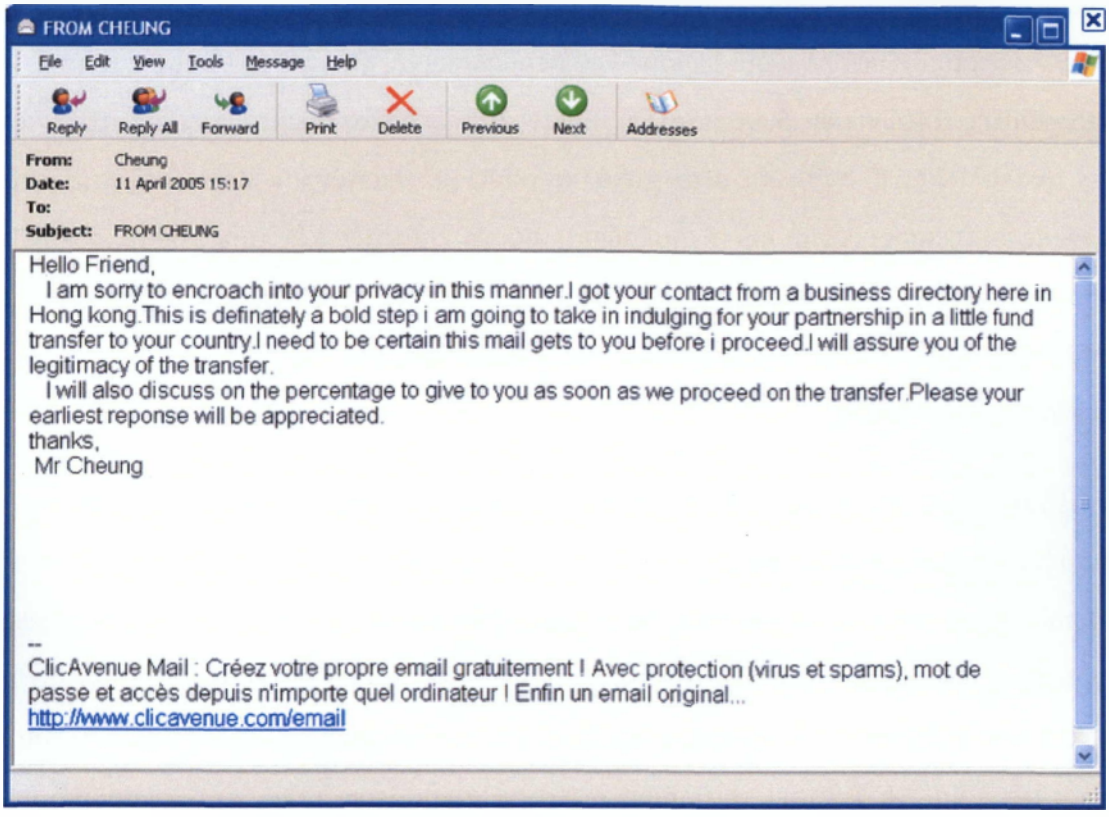
άλλον είναι έτσι δομημένο ώστε να απαιτεί ένα είδος εξουσιοδότησης, ότι δηλαδή ο αποστολέας του email είναι πελάτης του συγκεκριμένου Internet Provider. Οι ανοιχτοί ηλεκτρονόμοι όμως δεν ελέγχουν σχολαστικά το ποιος χρησιμοποιεί τον κεντρικό υπολογιστή επιτρέπουν την προώθηση όλου του ηλεκτρονικού ταχυδρομείου προς τη διεύθυνση προορισμού, ένα γεγονός που καθιστά ακόμα πιο δύσκολο τον εντοπισμό των spam μηνυμάτων.

Οι επιπτώσεις του φαινομένου είναι αρκετά μεγάλες και δεν περιορίζονται μόνο σε ατομικό επίπεδο. Είναι εύκολο να διαπιστώσει κανείς το μέγεθος των οικονομικών ζημιών που προκαλεί σε όλες τις εταιρείες Παροχής Διαδικτυακών Υπηρεσιών, αν λάβει υπ' όψιν του το γεγονός ότι περίπου το ένα με δυο τρίτα της δυνατότητας των κεντρικών τους υπολογιστών καταναλώνονται από την χρήση των Spam μηνυμάτων και το μεταφράσει σε χρηματικές μονάδες. Από νομικής απόψεως, αν αναλογιστεί κανείς πως το κόστος αυτό επιβάλλεται χωρίς την συγκατάθεση ούτε των ιδιοκτητών των δικτυακών υπηρεσιών ούτε των εξουσιοδοτημένων χρηστών, μπορεί εύκολα να οδηγηθεί στο συμπέρασμα ότι πρόκειται για μια σύγχρονη μορφή ηλεκτρονικού εγκλήματος που σχετίζεται με την κλοπή υπηρεσιών και δικαιωμάτων.

Σε μια πρόσφατη ερεύνα που διεξήχθη το Μάιο του 2003 διαπιστώθηκε ότι από το συνολικό αριθμό μηνυμάτων που εστάλησαν μέσω τα Διαδικτύου, το μεγαλύτερο ποσοστό καταλάμβαναν τα μηνύματα spam, ένα αποτέλεσμα που επιβεβαιώνει τους ισχυρισμούς των ISPs και επισφραγίζει την σημαντικότητα της κατάστασης. Ο Steve Linford , από το πρόγραμμα καταπολέμησης του spam "Spamhaus", δήλωσε χαρακτηριστικά ότι με τους ήδη αυξανόμενους ρυθμούς εξάπλωσης του φαινομένου είναι δυνατό να καταρρεύσει ολόκληρο το σύστημα μετάδοσης ηλεκτρονικών μηνυμάτων μέσα σε πολύ σύντομο χρονικό διάστημα.

Συνεπώς πρόκειται για ένα φαινόμενο του όποιου οι διαστάσεις έχουν λάβει ανησυχητική έκταση και χρήζει άμεσης αντιμετώπισης τόσο από τους μεμονωμένους χρήστες των υπηρεσιών που απλόχερα μας προσφέρει το Internet όσο και από τους ιδίους τους φορείς παροχής αυτών των υπηρεσιών προκειμένου να διατηρηθεί αναλλοίωτη η δομή και ο

χαρακτήρας όλων των επιμέρους στοιχείων που απαρτίζουν το μαγευτικό κόσμο του Παγκόσμιου Ιστού.



Εικόνα 5 Παράδειγμα email spam στο Outlook Express

1.3.2 Μηνύματα Spam

Από τα τέλη της δεκαετίας του 90, οι υπεύθυνοι των ταχυδρομικών συστημάτων έχουν λάβει αρκετά μέτρα για την καταπολέμηση του email spamming. Τα περισσότερα από αυτά είχαν θετικά και άμεσα αποτελέσματα. Συνεπώς όλοι όσοι επιθυμούν τη αποστολή εκούσιων

διαφημιστικών μηνυμάτων μέσω του Διαδικτύου επιβαρύνοντας οικονομικά κάποιους τρίτους στράφηκαν στην χρήση άλλων τέτοιων μέσων.

Τα συστήματα Instant Messaging(IM) είναι ένας ακόμη δημοφιλής στόχος των spammer. Η ευρέως διαδεδομένη χρήση τους καθώς και η ευκολία που προσφέρουν στην άμεση επικοινωνία μεταξύ των ενδιαφερόμενων μερών δεν άφησε αδιάφορους και τους επίδοξους καταχραστές αυτών των δυνατοτήτων. Είναι καθολικά παραδεκτό πως σε οτιδήποτε και αν έχει ανακαλύψει η ανθρωπότητα κατά καιρούς με σκοπό την βελτίωση της καθημερινής ανάγκης για επικοινωνία και ενημέρωση, πάντα υπάρχει και μια μικρή, ευτυχώς μερίδα ανθρώπων που επιδίδεται στην αρνητική χρησιμοποίηση τους, έχοντας ως απώτερο σκοπό την προώθηση προσωπικών συμφερόντων, αδιαφορώντας για τις επιπτώσεις που μπορούν να επιφέρουν στο σύνολο.

Τα περισσότερα συστήματα IM προσφέρουν έναν κατάλογο χρηστών όπου παρουσιάζονται ορισμένα χαρακτηριστικά τους στοιχειά, όπως το φύλλο, η ηλικία , τα ενδιαφέροντα τους κ.α. Συνεπώς είναι πιο εύκολο για τους διαφημιστές να συγκεντρώσουν τέτοιες πληροφορίες , να εγγραφούν ως χρήστες του εκάστοτε συστήματος και να στείλουν ανενόχλητοι τα μηνύματα τους. Ένας γρήγορος και εύκολος τρόπος για να απαλλαγεί κανείς από τέτοιου είδους μηνύματα είναι να επιλύει την λήψη άμεσων μηνυμάτων μόνο από ανθρώπους που ήδη γνωρίζει.

Το 2002, ένας μεγάλος αριθμός spammer άρχισε να κάνει χρήση του Microsoft Windows Messenger, προκειμένου να αποστέλλει να μηνύματα του. Αυτή η εφαρμογή της Microsoft δεν είναι η δια με το σύστημα άμεσης ανταλλαγής μηνυμάτων MSN Messenger . Αντιθέτως είναι μια λειτουργία των Windows σχεδιασμένη με τέτοιο τρόπο ώστε να επιτρέπει στους κεντρικούς υπολογιστές να στέλνουν προειδοποιητικά μηνύματα στους διαχειριστές τους. Το Windows messaging spam εμφανίζεται σαν κανονικό παράθυρο διαλόγου, το οποίο όμως περιέχει το μήνυμα του Spammer. Τα μηνύματα αυτά μπορούν να μεταδοθούν κάνοντας χρήση οποιαδήποτε πύλης του NetBIOS. Για να γίνει δυνατός ο αποκλεισμός τους από τα

προγράμματα προστασίας (firewall) πρέπει να «κλείσουν» τις πύλες 135 έως 139 καθώς επίσης και την πύλη 445.[3]

1.3.3 Spamdexing

Το Spamdexing, η αλλιώς το Search Engine Spamming είναι η διαχείριση των στοιχείων που πρόκειται να εισαχθούν σε διάφορες μηχανές αναζήτησης με τέτοιο τρόπο ώστε να δίνουν τη δυνατότητα σε ένα Web Site να ταξινομηθεί σε υψηλότερη θέση στη λίστα των αποτελεσμάτων αναζήτησης, αγνοώντας την πραγματική αξία και τη σχετικότητα του περιεχομένου του. Οι υπεύθυνοι των Search Engines θεωρούν τη τακτική αυτή καταχρηστική και σε μερικές περιπτώσεις προσαρμόζουν τις μεθόδους εύρεσης στοιχείων στον Παγκόσμιο Ιστό, με τέτοιο τρόπο ώστε οι Spamdexed σελίδες να εμφανίζονται στο τέλος, σε μία προσπάθεια περιορισμού της έκτασης του φαινομένου. Επιπλέον πολλές από τις μηχανές αναζήτησης διαθέτουν αυτόματα συστήματα εντοπισμού του spamdexing και οι σχετικές σελίδες είτε τιμωρούνται είτε αφαιρούνται παντελώς από τις λίστες των αποτελεσμάτων.

Το spamming των μηχανών αναζήτησης, σε αντίθεση με τις υπόλοιπες μορφές του φαινομένου, δε σχετίζεται με την άμεση και μαζική αποστολή εκούσιων εμπορικών μηνυμάτων σε διάφορους χρήστες. Παρ. όλα αυτά όμως επειδή περιλαμβάνει σκόπιμη εξαπάτηση και αθέμιτη εκμετάλλευση μιας δημόσιας υπηρεσίας . εφαρμογής που προσφέρει το Διαδίκτυο έχοντας ως απώτερο σκοπό την αισχροκέρδεια θεωρείται και αυτή ως μια συγκρίσιμη και ανάλογη των υπόλοιπων περιπτώσεων κατάχρηση.

Μερικές τεχνικές spamdexing είναι η εξής:

- Πολλαπλή επανάληψη σημαντικών λέξεων κλειδιών στο σώμα της σελίδας, ώστε να δοθεί ψευδής εικόνα συσχέτισης της με ένα συγκεκριμένο θέμα.

[3] http://conta.uom.gr/conta/ekpaideysh/Ptyxiaka/EidikaI/Ergasies/03-2004/Tzouflas-Spamming.pdf
Wikipedia "Email Spam"

Αρκετές μηχανές αναζήτησης έχουν πλέον την ικανότητα να προσδιορίζουν αν η συχνότητα εμφάνισης μιας λέξης είναι πάνω από ένα «κανονικό» επίπεδο.

- Κρυμμένο η αόρατο κείμενο, δηλαδή λέξεις ή φράσεις μπορούν να κρυφθούν δίνοντας τους το ίδιο χρώμα η φόντο ή χρησιμοποιώντας πολύ μικρού μεγέθους γραμματοσειρά. Σκοπός είναι να τις διαβάσουν οι μηχανές αναζήτησης και με βάση τα κριτήρια τους να κατατάξουν τις ιστοσελίδες κατά τον καλύτερο δυνατό τρόπο.

- Τοποθέτηση κρυμμένων υπερσυνδέσεων, για να αυξηθεί το λεγόμενο link popularity.

- Δημιουργία ιστοσελίδων χαμηλής ποιότητας σε μικρό περιεχόμενο αλλά με πολλές παρόμοιες φράσεις και λέξεις-κλειδιά.

- Κατεύθυνση του χρήστη σε άλλη ιστοσελίδα χωρίς τη δική του παρέμβαση, π.χ. χρησιμοποιώντας Java, JavaScript

Το πιο ενδεικτικό παράδειγμα έναντι του spamdexing είναι αυτό της Google, η οποία δημιούργησε τον αλγόριθμο PageRank. Ο εν λόγω αλγόριθμος είναι στην ουσία ένας τρόπος ταυτόχρονης μέτρησης της ποιότητας και της συνάφειας.

Γενικότερα, οι μηχανές αναζήτησης στην προσπάθεια τους να καταπολεμήσουν και να περιορίσουν την εξάπλωση τέτοιων τεχνασμάτων, εφαρμόζουν πολιτικές που περιλαμβάνουν τιμωρία των ιστοσελίδων που χρησιμοποιούν αυτού του είδους τα τεχνάσματα. Ενδεικτικά, η Google το Φεβρουάριο του 2006 αφαίρεσε τις ιστοσελίδες των εταιρειών BMW και RIHOC της Γερμανίας από το ευρετήριο της εξαιτίας της χρήσης αυτών των τεχνικών. Παρόλα αυτά, το spamdexing δεν μπορεί να θεωρηθεί ότι έρχεται σε αντίθεση με αυτό που ορίζουν οι νόμοι, αφού κύρια εργαλεία του είναι οι μηχανισμοί των υπερσυνδέσεων

και των λέξεων-κλειδιών, οι οποίοι βοήθησαν στην εδραίωση του Web ως ισχυρού μέσου.

1.3.4 Usenet Spam

Το Usenet spamming είναι μια ακόμη μορφή παραποίησης και κατάχρησης των δυνατοτήτων που παρέχει το Διαδίκτυο. Χρονικά προηγείται του email spamming και στις μέρες μας χρησιμοποιείται περισσότερο για την προώθηση μηνυμάτων κυρίως πορνογραφικού περιεχομένου. Παρ. όλα αυτά όμως, η ύπαρξή του καθώς και η χρησιμοποίηση του για την κάλυψη διαφημιστικών αναγκών έγινε γνωστή στο ευρύ κοινό για την προώθηση νομικών υπηρεσιών.

Ο αρχικός ορισμός του USENET spamming ήταν το excessive multiple posting, δηλαδή η επαναλαμβανόμενη ταχυδρόμηση του ίδιου ή περίπου του ίδιου μηνύματος. Στην αρχή της δεκαετίας του 90 υπήρξε ουσιαστική διαμάχη μεταξύ των διαχειριστών των συστημάτων USENET όσον αφορά στη χρήση της εντολής Cancel messages, προκειμένου να μμειωθεί η μμετάδοση των spam μηνυμάτων. Η εντολή Ακύρωσης μηνύματος είναι μια οδηγία προς τους κεντρικούς υπολογιστές για άμεση διαγραφή μιας ταχυδρόμησης έτσι ώστε να μην είναι εφικτή η ανάγνωσή της. Για πολλούς, η χρήση αυτής της εντολής θεωρήθηκε ως μια μορφή λογοκρισίας, ενώ για άλλους ως η σωτήρια λύση που θα βοηθούσε στη καταστολή του spamming.

Κατά τη διάρκεια εκείνης της χρονικής περιόδου ο όρος Usenet spam αναφερόταν ειδικά στην επαναλαμβανόμενη ταχυδρόμηση του ίδιου μηνύματος, ενώ για την περιγραφή ανάλογων περιστατικών είχαν αποδοθεί και οι αντίστοιχοι ορισμοί τους. Πρόσφατα όλες αυτές περιπτώσεις χαρακτηρίζονται με τον όρο spam.

1.3.5 E-mail Bomb

Ο Όρος email bomb στην επιστήμη υπολογιστών αναφέρεται σε ένα είδος επίθεσης κατά την οποία ο επιτιθέμενος στέλνει μια τεράστια ποσότητα ηλεκτρονικών μηνυμάτων σε μια διεύθυνση ηλεκτρονικού ταχυδρομείου με σκοπό να γεμίσει τον διαθέσιμο χώρο στον δίσκο και να προκαλέσει δυσλειτουργία στον mail server.

Μια μορφή email bomb που είναι αρκετά συνηθισμένη ονομάζεται ZIP bomb και βασίζεται στο γεγονός ότι πολλοί από τους σύγχρονους mail servers διαθέτουν προγράμματα ελέγχου των email για τον εντοπισμό ιων. Εάν για παράδειγμα κάποιο email περιλαμβάνει ως επισύναψη ένα συμπιεσμένο αρχείο (.zip, .rar κ.α.), τότε πολλοί από τους σύγχρονους mail servers θα αποσυμπιέσουν το αρχείο και θα ελέγξουν το περιεχόμενο του για ιούς ή δούρειους ίππους.

Μια ZIP bomb είναι ένα mail που περιέχει ένα συμπιεσμένο αρχείο ως ασυναπτόμενο. Αυτό το συμπιεσμένο αρχείο περιλαμβάνει ένα τεράστιο αρχείο κειμένου αρκετών GB , το οποίο αποτελεί ουσιαστικά συνεχή επανάληψη ενός γράμματος (π.χ. α). Ένα τέτοιο αρχείο έχει το εξής χαρακτηριστικό: Όταν είναι συμπιεσμένο καταλαμβάνει ελάχιστο χώρο, αλλά όταν αποσυμπιεστεί ο χώρος που δεσμεύει είναι τεράστιος. Άρα λοιπόν, όταν ο mail server προσπαθήσει να αποσυμπιέσει το αρχείο για να ελέγξει το περιεχόμενο του, τότε το αποσυμπιεσμένο αρχείο θα δεσμεύσει μια τεράστια ποσότητα υπολογιστικής ισχύος, μνήμης RAM, και σκληρού δίσκου. Αυτό έχει πολλές φόρες ως συνέπεια το πάγωμα του υπολογιστή.

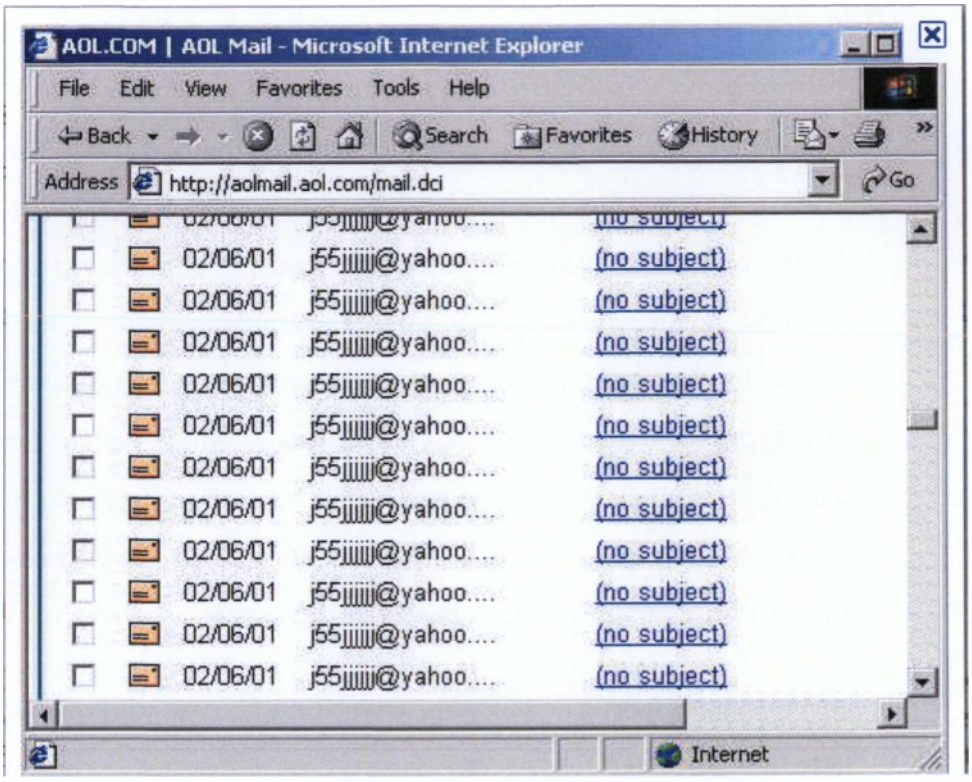
Παρόλα αυτά οι σύγχρονοι mail servers είναι η πλειοψηφία τους άτρωτοι σε ZIP bombs διότι αφενός είναι σε θέση να τις αναγνωρίζουν και αφετέρου διαθέτουν αρκετά υψηλές δυνατότητες (μεγάλη ταχύτητα επεξεργαστή, αρκετή μνήμη κ.α.) για μπορέσουν να συνεχίσουν ομαλά την λειτουργία τους ακόμη και όταν λάβουν μια τέτοια βόμβα.

Ωστόσο υπάρχουν 2 τρόποι διακίνησης των email bombs:

- Ο πρώτος τρόπος συνίσταται στην μαζική αποστολή ηλεκτρονικών μηνυμάτων στον ίδιο τον παραλήπτη. Ο σχεδιασμός προγραμμάτων που θα επιτελούν αυτή την λειτουργία είναι αρκετά απλός, αλλά τέτοιου είδους βόμβες εντοπίζονται εύκολα από φίλτρα spam και τελικά δεν πετυχαίνουν τον στόχο τους. Πολλές φορές οι hackers χρησιμοποιούν υπολογιστές zombie για να ξεκινήσουν μια επίθεση άρνησης υπηρεσιών. Κατά την επίθεση αυτή, ο hacker δίνει εντολή στους υπολογιστές zombie να στείλουν δισεκατομμύρια emails προς έναν συγκεκριμένο στόχο με σκοπό να γεμίσουν με emails και να παρεμποδίσουν την σωστή λειτουργία του. Η επίθεση αυτή είναι πιο δύσκολο να αντιμετωπιστεί σε σχέση με ένα απλό email bombing διότι αυτήν την φορά τα emails προέρχονται από δεκάδες διαφορετικούς υπολογιστές zombie.

- Ο δεύτερος τρόπος διακίνησης email bombs περιλαμβάνει την εγγραφή της ηλεκτρονικής διεύθυνσης του θύματος σε διάφορες διαδικτυακές υπηρεσίες. Εάν ο επιτιθέμενος καταφέρει να εγγράψει το θύμα σε πολλές τέτοιες υπηρεσίες τότε το θύμα θα παραλαμβάνει δεκάδες email από κάθε υπηρεσία, γεμίζοντας με τον τρόπο αυτό τον σκληρό δίσκο του mail server. Για την αποφυγή τέτοιων επιθέσεων έχει καθιερωθεί πλέον η τακτική της αποστολής ενός email επιβεβαίωσης πριν οριστικοποιηθεί η εγγραφή του χρήστη σε μια διαδικτυακή υπηρεσία. [4]

[4] Wikipedia "Email Spam"
Wikipedia "Spamdexing"
http://www.webspam.co.uk/serp-spam-definition-spamdexing/



Εικόνα 6 Παράδειγμα email bomb

1.3.6 SMS Spam

Οι διαφημιστικές στην προσπάθεια τους να προωθήσουν προϊόντα και ιδέες με όσο το δυνατόν μεγαλύτερη μερίδα ανθρώπων καταφεύγουν στην χρήση οποιοδήποτε μέσου τους προσφέρει τη δυνατότητα άμεσης επικοινωνίας με το σύνολο. Όπως είναι λογικό τα κινητά τηλέφωνα εξαιτίας των πολλαπλών δυνατοτήτων που μπορούν να προσφέρουν και λόγω της μεγάλης εξάπλωσης τους σε όλο το κοινωνικό σύνολο, ανεξαρτήτου ηλικίας και φύλλου δεν θα μπορούσαν να παραμείνουν απαρατήρητα και αδιάφορα στους επίδοξους κερδοσκόπους.

Στις μέρες μας αρκετοί χρήστες των κινητών τηλεφώνων διαπίστωσαν μια θεαματική αύξηση των ανεπιθύμητων, εμπορικών διαφημίσεων που αποστέλλονται στις συσκευές τους ,με την μορφή μηνύματος. Αυτή η μορφή spamming, που είναι γνωστή ως "sms spam", θεωρείται ως

ανάλογη το internet spam, μιας και έχουν πολλά κοινά, χαρακτηριστικά γνωρίσματα. Βασική τους όμως διαφορά είναι πως ενώ τα email spam δεν μας επιβαρύνουν οικονομικά παρά μόνο στην περίπτωση που παραγγέλλουμε κάποιο σχετικό προϊόν, το sms spamming εκτός του ότι είναι κατά πολύ πιο ενοχλητικό μιας και έχουμε πάντα μαζί μας το κινητό τηλέφωνο, επιπροσθέτως μας επιβαρύνει οικονομικά.

Το sms spam είναι λιγότερο έντονο από το email spam όπου το 2010 περίπου το 90% των email είναι spam. Το ποσοστό των sms spam ποικίλλει σημαντικά από περιοχή σε περιοχή. Στην Βόρεια Αμερική, πολύ λιγότερο από 1% των μηνυμάτων sms ήταν spam το 2010, ενώ σε τμήματα της Ασίας μέχρι και το 30% των μηνυμάτων είναι spam.

Στην προσπάθεια τους οι κατασκευαστές των κινητών τηλεφώνων να αριστοποιήσουν τις επιδόσεις και τις δυνατότητες των μοντέλων που παράγουν λόγω του έντονου ανταγωνισμού της αγοράς, έχουν καταφέρει να δημιουργήσουν μια γέφυρα επικοινωνίας μεταξύ ηλεκτρονικών υπολογιστών και κινητών συσκευών. Χαρακτηριστικό παράδειγμα αποτελεί η παροχή της δυνατότητας αποστολής email προς κινητά τηλέφωνα. Ενώ είναι μια αρκετά σημαντική καινοτομία που αποσκοπεί στην απλούστερη των καθημερινών μας αναγκών για επικοινωνία με άλλους ανθρώπους, ταυτόχρονα διογκώνει το προβλήματος spamming δημιουργώντας κατάλληλες προϋποθέσεις για περαιτέρω ανάπτυξη του.

1.3.7 Phishing

Το phishing (αγγλικός νεολογισμός βασιζόμενος στη λέξη (fishing=ψάρεμα) είναι ένας τρόπος οικονομικής εξαπάτησης ανυποψίαστων πελατών, οι οποίοι λαμβάνουν μηνύματα από «αξιόπιστες» πηγές (τράπεζες, εταιρείες κ.λπ.) που τους ζητούν προσωπικά τους στοιχεία (συνήθως αριθμούς πιστωτικών καρτών, αριθμούς λογαριασμών τραπέζης, κωδικούς πρόσβασης κ.α.), προκειμένου να διεκπεραιώσουν μία συναλλαγή.

Η πλειοψηφία των Phishing μηνυμάτων επικαλείται κάποιο επείγον πρόβλημα ή κάποια «μοναδική ευκαιρία» και ζητά από τον ανυποψίαστο παραλήπτη να απαντήσει άμεσα, είτε για να αποκατασταθεί το πρόβλημα είτε για να επωφεληθεί της ευκαιρίας.

Οι τεχνικές εξαπάτησης που χρησιμοποιούνται είναι ποικίλες. Είτε υπάρχει μια παραποιημένη διεύθυνση url μέσα στο περιεχόμενο του μηνύματος, η οποία, εκ πρώτης όψεως, φαίνεται σωστή, όταν όμως επιλεγεί από τον χρήστη οδηγεί σε σελίδες ακατάλληλου περιεχομένου. Είτε χρησιμοποιούνται εντολές JavaScript ώστε να μπερδευτεί η γραμμή διευθύνσεων και να οδηγήσει σε διαφορετικό ιστόχωρο , είτε χρησιμοποιούνται τα ίδια τα scripts των τραπεζών ή των εταιρειών και σε αυτήν την περίπτωση οι χρήστες λαμβάνουν ένα μήνυμα που φαίνεται γνήσιο και τους ζητά να επιβεβαιώσουν το λογαριασμό τους ακολουθώντας ένα σύνδεσμο που δείχνει να αντιστοιχεί σε αυθεντικό δικτυακό τόπο.

Παρόλο που οι περισσότεροι browsers έχουν ήδη αναπτύξει τεχνολογία anti-phishing προκειμένου να ανιχνεύουν τις σελίδες που ανοίγει ο χρήστης και να τον ειδοποιούν για το αν βρίσκεται σε σελίδα phishing, τα θύματα από τέτοιες επιθέσεις αυξάνονται ανησυχητικά σε όλον τον κόσμο. Ο χρήστης πρέπει να είναι ιδιαίτερα καχύποπτος απέναντι σε τέτοια μηνύματα και να επαληθεύει το περιεχόμενό τους επικοινωνώντας με την εταιρεία ή την τράπεζα που το έστειλε, όχι μέσω του μηνύματος, αλλά με τον τρόπο που χρησιμοποιούσε ως τώρα. Γενικά, οι αξιόπιστες εταιρείες και τράπεζες δεν καταφεύγουν σε γενικόλογα μηνύματα προκειμένου να εξυπηρετήσουν τους πελάτες τους, ούτε τους ζητούν να αποκαλύψουν τους κωδικούς τους.

Σήμερα κυκλοφορούν αρκετά προγράμματα anti-phishing, τα οποία είτε ελέγχουν το περιεχόμενο των ιστοσελίδων που διατρέχει ο χρήστης, είτε το περιεχόμενο των e-mail που λαμβάνει, προκειμένου να διαπιστώσουν αν πρόκειται για phishing, ενώ αποκαλύπτουν και το πραγματικό όνομα του ιστοχώρου που επισκέπτεται ο χρήστης. Τέλος, τα γνωστά

προγράμματα anti-spam μπορούν να μειώσουν τον αριθμό των απατηλών μηνυμάτων που λαμβάνει ο χρήστης.[5]

1.4 Υλοποίηση των τεχνικών από τους Spammers

Δεν υπάρχει καμία τεχνική που να μην ανακαλύψει ή χρησιμοποιήσει οι spammers.Αυτή τη φορά στόχο έχουν γίνει οι εφαρμογές **android** που αναπτύσσονται σε java και έτσι είναι εύκολο να τις αντιγράψει κανείς. Ένας ειδικός ασφάλειας από την **F – secure** υποστηρίζει ότι έχουν ανακαλύψει πολλές ανασκευασμένες εφαρμογές στη επίσημη ιστοσελίδα του **Android Market** . Οι εφαρμογές περιέχουν τα ίδια χαρακτηριστικά με τις αρχικές αλλά και μια ρύθμιση για την προβολή διαφημίσεων.
Όπως τονίζει ο ειδικός , οι περισσότερες εφαρμογές δεν περιέχουν κακόβουλο λογισμικό και μπορεί ο χρήστης να τις κατεβάσει δωρεάν. Το ζήτημα εδώ είναι ότι οι προγραμματιστές μπορούν να τις χρησιμοποιήσουν για την πώληση διαφημίσεων με σκοπό την απόκτηση κερδών. Τις περισσότερες φορές όμως οι προγραμματιστές δεν έχουν την άδεια του δημιουργού της αρχικής εφαρμογής με αποτέλεσμα η πράξη αυτή να αποτελεί κλοπή της πνευματικής ιδιοκτησίας.

Η δουλειά των spammers χωρίζεται σε διαφορετικές κατηγορίες:

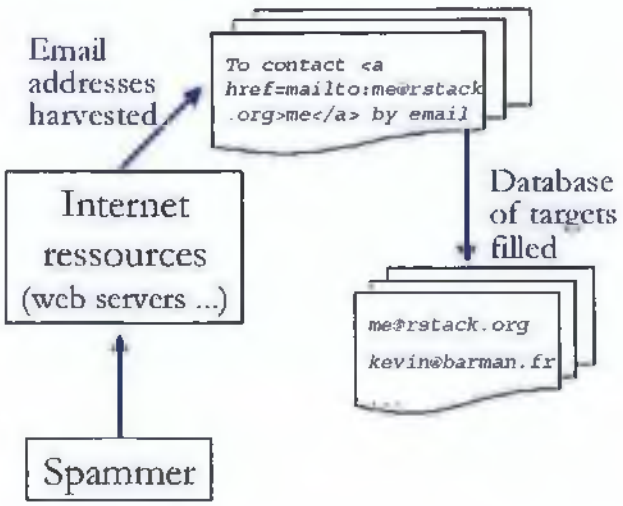
- ***Harvest*** : βρίσκουν έγκυρες email διευθύνσεις και φτιάχνουν βάσεις δεδομένων με τους στόχους
- ***Εύρεση open proxies*** : μέσω αυτών στέλνουν τα email και παραμένουν ανώνυμοι.
- ***Εύρεση open mail relay servers*** : ώστε να μπορούν να στέλνουν τα email, μέσω των open relay servers που τα προωθούν παντού.

[5]Wikipedia.org "Phishing"
http://www.spamfight.org/

1.4.1 Harvest

Για να αποσπάσουν έγκυρες email διευθύνσεις οι spammers συνεργάζονται με διάφορα άτομα που κάνουν αυτή τη δουλειά. Μάλιστα, στο internet χρησιμοποιείται ο όρος spaker, για να περιγράψει τους hacker οι οποίοι κάνουν hacking ώστε να

προμηθεύσουν τους spammers με έγκυρες διευθύνσεις, επί πληρωμής φυσικά. Ο όρος spaker είναι πολύ απαξιωτικός και τα άτομα που κάνουν αυτή τη δουλειά δεν το περηφανεύονται.



Εικόνα 7 Harvest

Οι spakers εισβάλουν σε e-commerce web sites και γενικά σε ιστοσελίδες οι οποίες περιέχουν βάσεις δεδομένων με πολλές χιλιάδες ή και εκατομμύρια άτομα ανά τον κόσμο που έχουν

κάνει αγορές. Όσο πιο συγκεκριμένο είναι το target group που θα αποσπάσει ο spaker τόσο καλύτερη θα είναι και η αμοιβή του.

Εκτός όμως από εμπορικά sites, οι spammers βρίσκουν έγκυρες email διευθύνσεις σε πολλά σημεία στο internet-public lists, forums, κοινότητες όπως τα hotmail.com, aol.com κα.

Μια ακόμα τεχνική για να αποσπάσουν email διευθύνσεις βασίζεται σε προγράμματα που ψάχνουν ιστοσελίδες στο internet και ελέγχουν για τη σύνταξη mailto:username@site.com. Όταν βρίσκουν τη σύνταξη αυτή, αποθηκεύουν τη διεύθυνση email και η αναζήτηση συνεχίζεται. Σαν προστασία σε αυτή την τεχνική προτείνεται να μην υπάρχει πουθενά email με την παραπάνω σύνταξη, αλλά να γράφεται mailto: username at site dot com. Βέβαια τα πιο προχωρημένα εργαλεία για αναζήτηση μπορούν να το καταλάβουν αυτό. Το Google.com, η μεγαλύτερη μηχανή αναζήτησης στο internet είναι σύμμαχος για τους spammers και συνήθως τα προγράμματα που χρησιμοποιούν για αναζήτηση email βρίσκουν τις ιστοσελίδες μέσα από το Google.

1.4.2 Open Proxy

Οι spammers μπορούν είτε να συνδεθούν απευθείας στον απομακρυσμένο mail relay server που θα στείλει το spam τους, είτε να συνδεθούν μέσω open proxies και έτσι να μην μπορούν να εντοπιστούν εύκολα, πετυχαίνοντας να μένουν συνέχεια ανώνυμοι. Ένας open proxy είναι μια υπηρεσία ανοικτή στον κόσμο που προωθεί οποιαδήποτε σχεδόν αίτηση, επιτρέποντας έτσι σε κάποιον να παραμένει ανώνυμος. Οι proxy servers χρησιμοποιούνται ιδιαίτερα από τους spammers και γενικότερα από το internet underground. Συνήθως οι spammers θα χρησιμοποιήσουν περισσότερους από ένα proxy servers για να καλύψουν τα ίχνη τους. Όσο περισσότερα ενδιάμεσα σημεία υπάρχουν, τόσο πιο δύσκολη θα είναι η ανίχνευσή τους. Οι spammers φοβούνται την πιθανότητα να εντοπιστούν, καθώς ξέρουν ότι οι δραστηριότητες τους είναι παράνομες και μπορούν να καταδικαστούν σε μεγάλα πρόστιμα και ποινές . Όσο πιο μεγάλη είναι η αλυσίδα των proxies στους οποίους συνδέονται τόσο καλύτερη ανωνυμία

θα έχουν, αν και η ταχύτητα μειώνεται, αφού τα δεδομένα ταξιδεύουν περισσότερο. Σε γενικές γραμμές, Open Proxy είναι ένα πρόγραμμα που επιτρέπει σε απομακρυσμένα pc να συνδέονται στο internet με την ip του μηχανήματος που τρέχει.

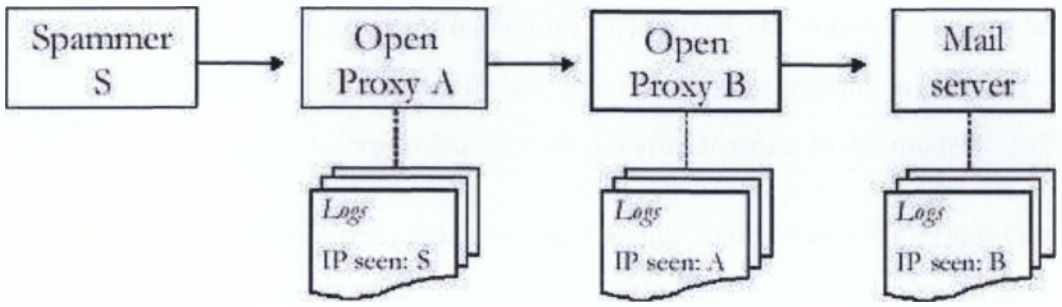
Αν ο proxy δεν είναι ρυθμισμένος σωστά, μπορεί να αποτελέσει εργαλείο επίθεσης στο IRC. Οι περισσότερες επιθέσεις με χρήση Open Proxy γίνονται ως εξής: Συλλέγει κάποιος μεγάλη λίστα με ανοιχτούς Proxy Servers και ταυτόχρονα συνδέει μεγάλο αριθμό κλώνων απ' όλους τους proxies προς το irc. Αυτοί οι κλώνοι συνήθως μπαίνουν σε ένα συγκεκριμένο κανάλι, το οποίο floodάρουν με άσχετο κείμενο, συνεχή joins/parts, notices, ή στοχεύουν σε χρήστες με notices, msgs ή CTCP responses ώστε να τους αποσυνδέσουν με flooding.

Στην περίπτωση που ανακαλυφθεί open proxy, δε σας επιτρέπεται η σύνδεση και μπαίνει K-Line (αποκλεισμός από το server). Αν είστε banned λόγω open proxy και ο proxy server είναι στο τοπικό σας δίκτυο, επικοινωνήστε με τον administrator του δικτύου σας ώστε να τον ρυθμίσει. Και επίσης σου προτείνει να επικοινωνήσεις με τους administrators για να τους παραθέσεις το αίτημα σου να συνδεθείς στο Phorum, και το μήνυμα σου να περιλαμβάνει το username/nickname και το IP σου. Τέλος, σου λέει ότι έχουν το δικαίωμα να σου αρνηθούν την πρόσβαση.

1.4.3 OPEN mail relays servers

Οι open relays είναι mail transfer agents (MTA's) που δέχονται να προωθήσουν email μηνύματα ακόμα και αν δεν προορίζονται για το δικό τους domain. Οι spammers χρησιμοποιούν open relays για να προωθήσουν τα email τους σε οποιαδήποτε διεύθυνση θέλουν. Οι MTA's είναι συνήθως mail servers που έχουν ρυθμιστεί λάθος, γι' αυτό και επιτρέπουν την προώθηση μηνυμάτων από οποιονδήποτε host επικοινωνεί.[6]

[6] support.inf.uth.gr
,oswinds.csd.auth.gr



Εικόνα 8 OPEN mail relays servers

1.5 Ποιοι είναι οι Spammers

Το 90% του spam που παράγεται σε παγκόσμιο επίπεδο, προέρχεται από 200 περίπου ομάδες spammers (κυρίως από τις ΗΠΑ, την Κίνα και την Νότιο Κορέα). Οι ομάδες αυτές διαθέτουν άριστη τεχνογνωσία και χρησιμοποιούν προηγμένο λογισμικό για την υλοποίηση των στόχων τους. Το υπόλοιπο 10% (που και πάλι μεταφράζεται σε δισεκατομμύρια spam-mails) δημιουργείται από μικρές επιχειρήσεις που δεν εφαρμόζουν τους κανόνες του email marketing, εκμεταλλευόμενοι την αφέλεια ή την άγνοια των χρηστών, από κάθε λογής και διαμετρήματος απατεώνες. Αυτό το 10% των συνολικών ποσοτήτων spam έχει υπολογιστεί ότι προέρχεται από 100.000 περίπου spammers.

Οι 200 οργανωμένες ομάδες spammer και ένα ποσοστό από τους υπόλοιπους, για να αποφύγουν τις νομικές και οικονομικές συνέπειες των πράξεων τους, πλαστογραφούν τις email διευθύνσεις τους ώστε να μην είναι δυνατό (ή να καθίσταται εξαιρετικά δυσχερής) ο εντοπισμός τους. Τις περισσότερες φορές το e-mail και το όνομα παρουσιάζεται ως ο αποστολέας των ποσοτήτων spam-mail είναι κάποιος, εντελώς αθώος, χρήστης του διαδικτύου, του οποίου χρησιμοποιήθηκε εν άγνοια του, η e-mail διεύθυνση του. Αυτό έχει σαν συνέπεια να μπλοκάρει ο λογαριασμός του από τις επιστροφές των ανεπίδοτων spam-mail(κάθε αποστολή spam, περιλαμβάνει χιλιάδες ή και εκατομμύρια διευθύνσεις, πολλές από τις οποίες έχουν καταργηθεί) ή/και από τις εκατοντάδες/χιλιάδες διαμαρτυρίες των

παραληπτών του spam. Με λίγα λόγια, μπορεί κάποιος spammer να χρησιμοποιήσει το email ενός χρήστη με πλήρη άγνοια του και να εμφανίζετε ως ο αποστολέας μιας τεράστιας ποσότητας spam. Αυτό αποτελεί την πιο συνηθισμένη τακτική Spammers.

Οι Spammers συλλέγουν διευθύνσεις ηλεκτρονικού ταχυδρομείου από τα chat rooms, από ιστοσελίδες, από καταλόγους πελατών, από newsgroups και από ιούς που «ψαρεύουν» emails και τα πουλούν στους spammers.

Αυτή είναι μια λίστα αξιόλογων ατόμων οι οποίοι έστειλαν μαζικά ηλεκτρονικά ανεπιθύμητα μηνύματα, είτε για δικό τους λογαριασμό, είτε για τρίτους. Δεν είναι μια λίστα όλων των Spammers, μόνο εκείνων των οποίων οι δράσεις έχουν προσελκύσει σημαντική και ενδιαφέρουσα προσοχή.

- **Serdar Argic** ο οποίος διατάραξε το USENET στέλνοντας μέχρι και 100 μηνύματα την ημέρα σε διαφορετικές ομάδες συζήτησης σε μια προσπάθεια να παρεμποδίσει την Γενοκτονία των Αρμενίων

- **Canter and Siegel** 2 σύζυγοι οι οποίοι δημοσίευσαν μια από τις πρώτες εμπορικές Spam διαφημίσεις, σε χιλιάδες ομάδες συζητήσεων οι οποίες ήταν προκλητικές.

- **David D' Amato** πρώην βοηθός του διευθυντή ενός λυκείου στον οποίο επιβλήθηκε πρόστιμο 500 δολαρίων και πέρασε ένα χρόνο στην φυλακή αφού καταδικάστηκε το 2001 για online εγκλήματα συμπεριλαμβάνοντας email bombs τα οποία απευθύνονταν σε άτομα και ιδρύματα.

- **Peter Francis-Macrae** καταδικάστηκε για απάτη συναλλαγών για εκβιασμούς και βίαιες απειλές, αφού έστειλε εκατοντάδες emails σε επιχειρήσεις.

- **Wayne Mansifield** ήταν ο πρώτος Αυστραλός ο οποίος καταδικάστηκε το 2005 για email spamming.

- **Oleg Nikolaenko** ο οποίος θεωρείται ο *« Βασιλιάς του Spam»* ο οποίος συνελήφθει από τον Federal Bureau γνωστός πράκτορας, τον Νοέμβριο του 2010.

- **Alan Ralsky, Scott Bradley, John Bown, Wiliam Neil and James** Fite οι οποίοι ομολόγησαν την ενοχή τους για μια συνομωσία στην οποία χρησιμοποιούσαν μηνύματα spam.

- **Gary Thuerk** , ο οποίος θεωρήθηκε ως ο *«Πατέρας του Spam»* που έστειλε την πρώτη έκρηξη ανεπιθύμητων email σε 600 άτομα το 1978.[7]

[7] wikipedia.org
http://dide.ilei.sch.gr/keplinet/tech/spam.php

ΚΕΦΑΛΑΙΟ 2
ΑΝΑΛΥΣΗ ΤΟΥ SPAMMING

2.1 Νομικά ζητήματα του Spamming

Το Spamming συνιστά πρακτική που απαγορεύεται από τη Δεοντολογία του Internet και από τη νομοθεσία των περισσότερων ευρωπαϊκών κρατών, καθώς αντιτίθεται σε μεγάλο βαθμό στην προστασία των καταναλωτών και των προσωπικών τους δεδομένων και ενέχει κινδύνους όσον αφορά στην ασφάλεια των δικτύων.

Ο νόμος 2251 του 1994 αποτελεί τον πιο σημαντικό νόμο που ρυθμίζει ζητήματα προστασίας του καταναλωτή. Περιέχει ορισμούς των εννοιών του καταναλωτή, του προμηθευτή, της σύμβασης από απόσταση και άλλων. Για την περίπτωση του spam

ενδιαφέρον παρουσιάζει το *άρθρο 9* και πιο συγκεκριμένα οι παράγραφοι *11, 12* και *13.*

Άρθρο 9(Διαφήμιση)

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

Παράγραφος 11*. «Ανεξάρτητα από τον περιορισμό της προηγούμενης παραγράφου, η μετάδοση διαφημιστικού μηνύματος απευθείας στον καταναλωτή με οποιονδήποτε τρόπο άμεσης επικοινωνίας 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 τις προηγούμενες συναλλακτικές σχέσεις του με τον καταναλωτή, από γενικά προσιτές πηγές, όπως κατάλογο η άλλα δημοσιευμένα στοιχειά, ή από άλλο φυσικό ή νομικό πρόσωπο,*

εφόσον ο καταναλωτής εγκρίνει ρητά την μεταβίβαση των προσωπικών στοιχείων για τον σκοπό της άμεσης διαφήμισης. Ο διαφημιστής είναι υποχρεωμένος να αναφέρει στον καταναλωτή τον τρόπο με τον οποίο περιήλθαν σε γνώση του τα προσωπικά του καταναλωτή.»

Παράγραφος 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.»*

Παράγραφος 13. *«Η άμεση διαφήμιση θα πρέπει να γίνεται με τρόπο που να μην προσβάλλει την ιδιωτική ζωή του καταναλωτή.»*

Η προσοχή του νομοθέτη στις αυτόκλητες κλήσεις για την προώθηση της πώλησης προϊόντων ή υπηρεσιών κατά τη διάρκεια του 2002-2003 σηματοδοτήθηκε στην Ευρωπαϊκή Ένωση με την *Οδηγία 2002/58/ΕΚ* (οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες) για την οποία, μάλιστα, ορίστηκε προθεσμία εναρμόνισής της στο εσωτερικό δίκαιο των Κρατών-Μελών η 31^{η} Οκτωβρίου 2003. Σε αρκετά Κράτη-Μέλη της Ευρωπαϊκής Ένωσης υφίσταται νομοθεσία για την αντιμετώπιση της απρόσκλητης εμπορικής επικοινωνίας. Αξιοσημείωτο είναι, επίσης, το γεγονός ότι την ίδια, περίπου περίοδο, στις Ηνωμένες Πολιτείες της Αμερικής υιοθετήθηκε η CAN SPAM Act 2003.

Η πρώτη κοινή Ευρωπαϊκή και Αμερικανική πρωτοβουλία για την αντιμετώπιση του φαινομένου της εγκληματικής δράσης στο Internet με την αποστολή spam ήταν η συνεργασία του Συμβουλίου Προστασίας Καταναλωτών της Γαλλίας με φορείς των Ηνωμένων Πολιτειών όπως η Ομοσπονδιακή Επιτροπή Εμπορίου. Σε αντίθεση με την αδικαιολόγητη βραδύτητα της Ελλάδας για την εσωτερίκευση της *Οδηγίας 2002/58/ΕΚ* στο δικαστικό της σύστημα και για την αναποτελεσματικότητα της χώρας και των αρμοδίων αρχών αυτής για την αντιμετώπιση και καταπολέμηση του φαινομένου spam, σε διεθνές επίπεδο υπάρχει έντονη κινητικότητα για τη λήψη αποτελεσματικών μέτρων.

Έτσι, για παράδειγμα, από τον Φεβρουάριο του 2004, ο Οργανισμός για την Οικονομική Συνεργασία και Ανάπτυξη (ΟΟΣΑ) έχει αρχίσει το Project Spam για να ενισχύσει τη διεθνή συνεργασία στον τομέα της καταπολέμησης της αυτόκλητης εμπορικής επικοινωνίας, ενώ ο Οργανισμός Ηνωμένων Εθνών (ΟΗΕ) έχει εκφράσει τη διάθεσή του να καταπολεμήσει την απρόσκλητη εμπορική επικοινωνία και τους κινδύνους που ελλοχεύουν από την ανεξέλεγκτη διακίνηση μηνυμάτων spam. Η International Telecommunications Union, στα πλαίσια του Παγκοσμίου Συνεδρίου για την Κοινωνία της Πληροφορίας (World Summit on the Information Society), συγκάλεσε στην Γενεύη, 7-9 Ιουλίου 2004, διεθνή διάσκεψη για την αντιμετώπιση του spam.

Η σημαντικότερη διάταξη της *Οδηγίας 2002/58/ΕΚ* για την αντιμετώπιση των αυτόκλητων εμπορικών κλήσεων, είναι αυτή του *άρθρου 13.* Ωστόσο, το εν λόγω άρθρο δεν περιέχει κάποιον ορισμό του spam. Ο τρόπος, όμως, προσδιορισμού του Spam στο άρθρο αυτό φαίνεται ότι προσεγγίζει τον ορισμό του spam όπως έχει περιγραφεί από τη Γαλλική CNIL—Commission National de l' Informatique et des Libertés. Σύμφωνα με τον ορισμό της CNIL τα κυριότερα χαρακτηριστικά γνωρίσματα του spam συνίστανται στο ότι πρόκειται για α) μαζική επικοινωνία— bulk mail, β) με σκοπό ή περιεχόμενο την εμπορική προώθηση προϊόντων ή υπηρεσιών—commercial nature, γ) που αποστέλλεται χωρίς προηγούμενη πρόσκλησή της από τον παραλήπτη της—unsolicited.

Όπως φαίνεται η Ευρωπαϊκή Επιτροπή παρουσίασε μετρά για την αντιμετώπιση του πολλαπλασιασμού των αυτόκλητων ηλεκτρονικών εμπορικών μηνυμάτων ενώ ο αρμόδιος επίτροπος δήλωνε τότε ότι οι επιχειρήσεις και οι ιδιώτες καταναλώνουν ολοένα περισσότερο χρόνο και χρήμα για να ξεκαθαρίσουν το ηλεκτρονικό τους ταχυδρομείο, αντιλαμβανόμενοι το μέγεθος του προβλήματος.

Τον Ιούλιο του 2003 η Ευρωπαϊκή Επιτροπή παρουσίασε χρονοδιαγράμματα σύμφωνα με το οποίο, μέχρι το τέλος Οκτωβρίου του 2003 τα κράτη-μέλη οφείλουν να έχουν ενσωματώσει στην εθνική τους νομοθεσία διατάξεις για την απαγόρευση του spamming, με βάση την οδηγία της επιτροπής για την προστασία της ιδιωτικής ζωής στο τομέα των ηλεκτρονικών

επικοινωνιών, που υιοθετήθηκε το 2000. Η Οδηγία προβλέπει την κινητοποίηση των αρμόδιων για το ιδιωτικό απόρρητο αρχών, την σύνταξη κατευθυντήριων γραμμών για την βιομηχανία(φιλτράρισμα μηνυμάτων, κώδικες δεοντολογίας), προγράμματα για την ευαισθητοποίηση των καταναλωτών καθώς και πλαίσιο συνεργασίας σε διεθνές επίπεδο για την αντιμετώπιση του φαινομένου.[8]

Όσον αφορά στο επίπεδο των μεγάλων επιχειρήσεων, ο πολλαπλασιασμός των αυτόκλητων εμπορικών ηλεκτρονικών μηνυμάτων δημιουργεί μείζον πρόβλημα για την ανάπτυξη του ηλεκτρονικού εμπορίου και την κοινωνία της πληροφορίας. Οι εταιρείες είναι αναγκασμένες να δαπανούν σε καθημερινή βάση αρκετό χρόνο προκειμένου να διαχωρίσουν τα εισερχόμενα μηνύματα της ηλεκτρονικής τους αλληλογραφίας, μιας και τις περισσότερες φορές τα περισσότερα από τα μηνύματα που δέχονται είναι αυτόκλητα.

Αντίστοιχη ευαισθητοποίηση για το spamming έχουν επιδείξει και οι ΗΠΑ, όπου το πρόβλημα έχει εντοπιστεί αρκετά πιο νωρίς και επιφέρει σοβαρότατα οικονομικά προβλήματα σε πολλές μεγάλες εταιρείες. Η Αμερικανική Γερουσία με σχετικό της νομοσχέδιο προβλέπει αποζημιώσεις ύψους 500 δολαρίων για κάθε μήνυμα spam, όσον αφορά στους μεμονωμένους χρήστες, και 1.000 δολαρίων για τους Φορείς Παροχής διαδικτυακών Υπηρεσιών. Το ίδιο νομοσχέδιο καθιστά παράνομη και την πώληση καταλόγων διευθύνσεων e-mail στους spammers.

Χαρακτηριστικά αναφέρεται ότι το Μάιο του 2003 επιβλήθηκε σε Αμερικανό καταβολή αποζημίωσης ύψους 16,4 εκατομμυρίων δολαρίων στην EarthLink, επειδή είχε αποστείλει στην ενάγουσα εταιρία δεκάδες εκατομμύρια αυτόκλητα μηνύματα. Την ίδια πολιτική ακολούθησε και η Microsoft, η οποία υπέβαλλε μηνύσεις εναντίον 15 νομικών προσώπων, με την κατηγορία ότι "πλημμύρισαν" το δίκτυό της με δύο δισεκατομμύρια ανεπιθύμητα e-mail. Πλέον οι αγωγές κατά αποστολέων spam mail αποτελούν καθημερινή πραγματικότητα τόσο στις ΗΠΑ όσο και σε πολλές από τις υπόλοιπες χώρες του κόσμου.[9]

---

[8] "Το πρώτο βήμα για πολλά ηλεκτρονικά εγκλήματα. Η αυτόκλητη εμπορική επικοινωνία (spam) υπό το πρίσμα της οδηγίας 2002/58/ΕΚ" του δικηγόρου Μ. ΠΑΠΑΔΟΠΟΥΛΟΥ στο 2ο πανελλήνιο συνέδριο ηλεκτρονικού εγκλήματος (2004)
[9] Wikipedia.org

2.2 Οικονομική ανάλυση του Spamming

Οι επιπτώσεις που επιφέρει το spamming στον οικονομικό τομέα όλων των ανεπτυγμένων χωρών είναι αρκετά σημαντικές. Αυτός είναι και ο κύριος λόγος για τον οποίο η Ευρωπαϊκή Ένωση, οι ΗΠΑ και μεμονωμένες ευρωπαϊκές χώρες έχουν αρχίσει να ευαισθητοποιούνται απέναντι στο συγκεκριμένο ζήτημα.

Χαρακτηριστικά αναφέρονται ορισμένα στατιστικά στοιχεία που σχετίζονται με τις οικονομικές ζημιές που έχει επιφέρει η μετάδοση spam μηνυμάτων:

Το 2001 η διακίνηση spam μηνυμάτων αντιστοιχούσε στο 8% του συνόλου της ηλεκτρονικής αλληλογραφίας μέσω Internet. Το αντίστοιχο ποσοστό του 2002 έφθασε στο 40%. Η απώλεια παραγωγικότητας των επιχειρήσεων της Ευρωπαϊκής Ένωσης υπολογίζεται σε 2,5 δισ. ευρώ για το 2002 (περισσότερα από 10 δισ. ευρώ συνυπολογίζοντας και το κόστος στους ιδιώτες). Ειδικά για τις μικρομεσαίες

επιχειρήσεις, οι οποίες συχνά αμελούν να επενδύσουν σε ειδικά συστήματα φιλτραρίσματος αλληλογραφίας και εξακολουθούν να δέχονται ανεξέλεγκτα μεγάλες ποσότητες spam mail, το κόστος υπολογίζεται μεγάλο (χωρίς προς το παρόν να υπάρχουν συγκεκριμένα στοιχεία).

Πρόσφατη έρευνα της αμερικανικής Ferris Research επιβεβαιώνει την απώλεια:

- 2,5 δισ. ευρώ στις επιχειρήσεις της Ευρωπαϊκής Ένωσης αλλά δίνει και επιπλέον στοιχεία:
- περίπου 8,9 δισ. δολάρια απώλειες για τις αμερικανικές επιχειρήσεις, και από περίπου 500 εκατ. δολάρια για εταιρίες παροχής υπηρεσιών Internet και στις δύο πλευρές του Ατλαντικού.

Τα ποσά αυτά αντιστοιχούν κυρίως σε χαμένο χρόνο. Στην έρευνα αυτή υπολογίζεται ότι, μολονότι συνήθως τα αυτόκλητα μηνύματα διαγράφονται από τον εργαζόμενο σε μια

επιχείρηση μέσα σε λίγα δευτερόλεπτα, πολλοί υπάλληλοι ρίχνουν μια γρήγορη έστω ματιά σε κάποια από αυτά. Ο περισσότερος χαμένος χρόνος υπολογίζεται ότι αφιερώνεται στο διαχωρισμό των χρήσιμων email από τα άχρηστα και στην εξακρίβωση των πραγματικά άχρηστων: δεν είναι σπάνιο το φαινόμενο να χαρακτηρίζεται ως spam ένα χρήσιμο μήνυμα, λόγω σφάλματος στο φιλτράρισμα της αλληλογραφίας από το σύστημα.

Ακόμη πιο πρόσφατη έρευνα (Ιούνιος - Ιούλιος 2003) της αμερικανικής Nucleus Research δείχνει ότι:

- τα μηνύματα spam κοστίζουν στις επιχειρήσεις των ΗΠΑ 874 δολάρια ετησίως ανά εργαζόμενο, κάτι που αντιστοιχεί σε μείωση της παραγωγικότητας κατά 1,4% σε ετήσια βάση. Το ποσό των 874 δολαρίων βασίζεται σε ωριαίες απολαβές 30 δολαρίων σε μια χρονιά 2.080 ωρών.
- ο μέσος εργαζόμενος λαμβάνει 13,3 αυτόκλητα μηνύματα την ημέρα.
- οι εργαζόμενοι αφιερώνουν 6,5 λεπτά κάθε μέρα, ελέγχοντας, διαγράφοντας ή διαβάζοντας spam mail.

Τέλος, η επίσης αμερικανική Network Associates δημοσίευσε έρευνά της, που διεξήχθη online με 1.500 συμμετέχοντες, και έδειξε ότι οι εργαζόμενοι σπαταλούν περίπου 40 λεπτά την εβδομάδα ασχολούμενοι με μηνύματα spam.

Συνεπώς μπορεί εύκολα να γίνει αντιληπτό πως δεν πρόκειται για μεμονωμένα περιστατικά, αλλά αντιθέτως για μια καλοστημένη ΄επιχείρηση[8] που αποβλέπει στη δημιουργία προσωπικού κέρδους εις βάρους του συλλογικού συμφέροντος και είναι αναγκαίο να αντιμετωπιστεί άμεσα με κάθε δυνατό μέσο.

Για να καταλάβουμε πόσο καταστροφικό είναι το φαινόμενο του spamming για την οικονομία μπορούμε να το αναλύσουμε και να διαπιστώσουμε πως επηρεάζει μια επιχείρηση πόσο και πώς της στοιχίζει.

Καταρχήν σκεπτόμενοι εντελώς απλοϊκά θα μπορούσαμε να πούμε πως για την διαγραφή ενός spam χρειάζονται μόνο μερικά δευτερόλεπτα, σαν ζήτημα δευτερολέπτων λοιπόν δεν μπορεί να βλάψει ή να επηρεάσει την επιχείρηση σε μεγάλο βαθμό. Δυστυχώς όμως με αυτή τη λογική υποτιμούμε την ζημιά που μπορεί να προκληθεί. Ενώ οι επιπτώσεις μιας χούφτας spams μπορεί να είναι αμελητέα, οι επιπτώσεις δεκάδων ή εκατοντάδων χιλιάδων spams είναι αναπόφευκτα μεγάλες. Να ορίσουμε το ακριβές ποσό της οικονομικής ζημίας είναι από πάρα πολύ δύσκολο έως και αδύνατον καθώς ορισμένες δαπάνες σχετίζονται με το εάν υπάρχει από μεριάς της επιχείρησης κάποια λύση antispam, άλλες δαπάνες σχετίζονται με το επιχειρηματικό περιβάλλον και άλλες απλά δεν είναι δυνατόν να υπολογιστούν. Ωστόσο δεν υπάρχει αμφιβολία πως το spamming κοστίζει, καθώς ορισμένες δαπάνες είναι αρκετά προφανείς όπως για παράδειγμα αν ένας χρήστης χρειάζεται x δευτερόλεπτα για να διαγράψει ένα spam, πολλαπλασιάζουμε τον αριθμό αυτό με τα ψ spams που δέχεται ημερησίως και έχουμε έναν αριθμό z που είναι οι χαμένες εργασιακές ώρες οι ώρες παραγωγικότητας δηλαδή, ένας ακόμα προφανής λόγος της συσχέτισης του spamming με την οικονομία έχει να κάνει με την αποθήκευση αχρήστων πληροφοριών και με το εύρος ζώνης των συνδέσεων που εξαιτίας του spamming δεσμεύεται. Όπως είπαμε όμως αυτά είναι τα προφανή, υπάρχει όμως και ένα άλλο εξίσου σημαντικό κόστος που δεν είναι εξαρχής τόσο ευδιάκριτο και για κανέναν λόγο ν πρέπει να παραβλεφθεί.

Εδώ γίνεται λόγος για το κόστος εσφαλμένης ταυτοποίησης. Το κόστος αυτό αποτελείται από δυο «παρακλάδια». Το πρώτο «παρακλάδι» αφορά τα μηνύματα που χαρακτηρίζονται ως ψευδώς θετικά. Τα μηνύματα αυτά στην ουσία ενώ δεν αποτελούν spasm ωστόσο χαρακτηρίζονται εσφαλμένα ως τέτοια με αποτέλεσμα να αποκλείονται. Η δεύτερη κατηγορία αφορά ακριβώς το αντίστροφο, τα ψευδώς αρνητικά. Όπως γίνεται εύκολα αντιληπτό εδώ

μιλάμε για ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου τα όποια έχουν λανθασμένα έχουν χαρακτηριστεί ως μη spasm και έτσι δεν έχουν αποκλειστεί όπως θα έπρεπε. αυτοί οι λανθασμένοι χαρακτηρισμοί μηνυμάτων μειώνουν την αποδοτικότητα των antis am λύσεων-φίλτρων των επιχειρήσεων. Αν και ορισμένα antispam φίλτρα δίνουν στους διαχειριστές την δυνατότητα να ρυθμίσουν οι ίδιοι την ευαισθησία του φίλτρου, πρόκειται για ιδιαίτερη διαδικασία με αμφίβολα αποτελέσματα καθώς με την αύξηση της ευαισθησίας του φίλτρου θα πτυχή (ο διαχειριστής) να μειώσει τα μηνύματα που κακώς χαρακτηρίστηκαν ως μη spam (μείωση ψευδώς αρνητικών) αλλά ταυτόχρονα είναι σχεδόν σίγουρο πως «πτυχή» αύξηση των μηνυμάτων που οσφραμένα χαρακτηρίστηκαν ως spam και αποκλείστηκαν (αύξηση ψευδώς θετικών), και μια τέτοια κατάσταση μπορεί να εξαιρετικά δαπανηρή για μια επιχείρηση.

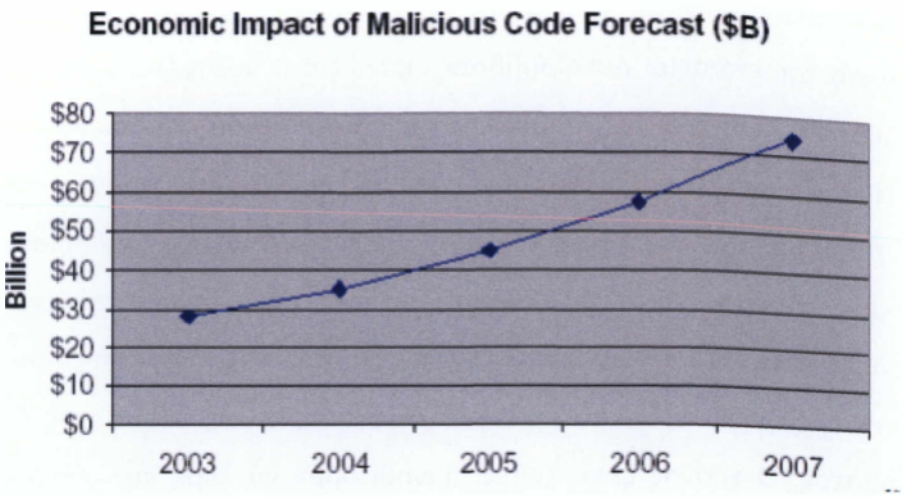
Αυτό το ρίσκο της αύξησης της ευαισθησίας ενός antispam φίλτρου το καταδεικνύει ένα συμβάν με μια εταιρεία νομικής στο Colorado των Η.Π.Α. η όποια δεν παρευρέθηκε σε μια ακροαματική διαδικασία και ορίστηκε να πληρώσει τα έξοδα του νομικού σύμβουλου της αντίπαλης μεριάς. Το συμβάν αυτό έγινε επειδή η εταιρία αποφάσισε να αυξήσει την ευαισθησία του BARRACUDA SPAM FIREWALL 200 προκειμένου να εμποδίσει τα spasm που έφταναν ακόμα στους υπολογιστές των τελικών χρηστών. Αυτό είχε ως αποτέλεσμα να μην εμποδίζεται μόνο η ανεπιθύμητη αλληλογραφία αλλά και τα ηλεκτρονικά μηνύματα του επαρχιακού δικαστηρίου των Η.Π.Α. για την περιοχή του Colorado, συμπεριλαμβανομένης και της κοινοποίησης για την ημερομηνία της ακρόασης. Έτσι η νομική εταιρία είχε να αντιμετωπίσει ένα τσουχτερό πρόστιμο αρκετών χιλιάδων δολαρίων. Τέτοια συμβάντα αποτελούν για τις επιχειρήσεις «χαμένες ευκαιρίες», και το κόστος των οποίων είναι δύσκολο να υπολογιστεί. Για παράδειγμα εάν μια παραγγελία ενός πελάτη χαρακτηριστεί εσφαλμένε ως spam τότε η εταιρεία-επιχείρηση δεν θα χάσει μόνο τη συγκεκριμένη παραγγελία αλλά πιθανόν και ης επόμενες που ο ίδιος πελάτης θα έκανε, καθώς κάνεις δεν θέλει να ενασχοληθεί να αγοράσει κάτι από μια επιχείρηση που φαίνεται να μην ανταποκρίνεται στο email-παραγγελία του.

Επιπλέον ένα μεγάλο ποσοστό «ψευδώς θετικών» αποτελεσμάτων επηρεάζει και την ιδία την παραγωγικότητα της εταιρεία. Αυτό συμβαίνει καθώς ένα αυξημένο ποσοστό θα υποχρεώνει το προσωπικό να θυσιάζει εργασιακό χρόνο προκειμένου να ελέγξει προσεκτικά στα διαγραμμένα μηνύματα ή σε όσα έχουν τεθεί σε κατάσταση καραντίνας μήπως υπάρχει κάποιο μήνυμα που δεν είναι σημαντικό και δεν θα έπρεπε κανονικά να βρίσκεται σε αυτές τις δυο κατηγορίες. Ακόμα και η επανάκτηση ενός τέτοιου μηνύματος μπορεί να αποβεί χρονοβόρα διαδικασία ιδιαίτερα αφού μερικές antispam λύσεις απαιτούν προσωπικό να επανεξετάσει όσα αρχεία τέθηκαν σε κατάσταση καραντίνας, μέσω ενός δυσκίνητου web-based συστήματος. Ο χρόνος είναι χρήμα συνηθίζουμε να λέμε και συμφώνα με όλα όσα είδαμε για το spamming και πως επηρεάζει μια εταιρεία επιβεβαιώνεται για μια ακόμα φορά η ρήση του λάου μας.

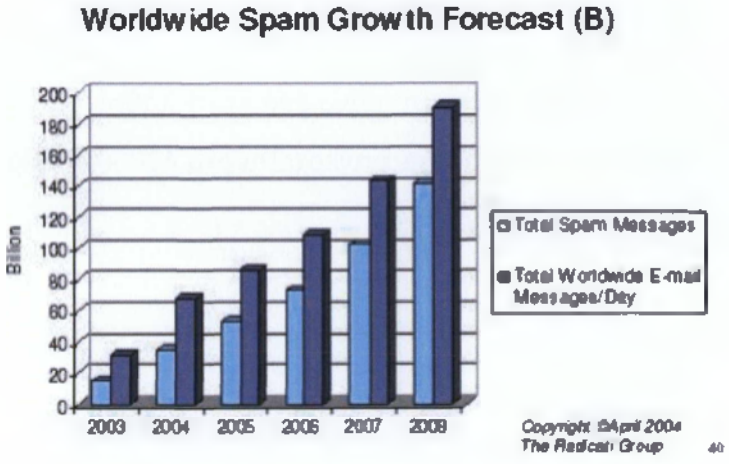
Ένα ακόμα στοιχειό προκύπτει από την ερευνά της Ferris Research, συμφώνα με την όποια κοστίζει 3,5 δολάρια η επαναφορά ενός μηνύματος που διαγράφηκε από λάθος. Αυτό μπορεί να μοιάζει με ασήμαντο ποσό και άνευ σημασίας αλλά αν σκεφτούμε πως μια εταιρεία απασχολεί 1000 άτομα προσωπικό, τότε με μόνο ένα κατά λάθος διαγραμμένο μήνυμα ανά άτομο το μηνά, το ετήσιο κόστος επαναφοράς ανέρχεται στα 42000 δολάρια.[10]

Παρατίθεται παρακάτω απεικονίσεις πινάκων πρόσφατων υπολογισμών των οικονομικών μεγεθών του spam.

[10] Industry statistics – ferris research http://www.ferris.com/research-library/industry-statistics
Spam cost report 2005 (ferris research) http://www.ferris.com/2005/02/24/the-global-economic-impact-of-spam-2005
Blacklist statistics center http://www.stats.dnsbl.com
Spam filter costs lawyers their day in court http://washingtonpost.com/wp-dyn/content/article/2007/07/13/AR2007071300606.html
www.sunbeltsoftware.com



Εικόνα 9 Στο σχήμα αυτό βλέπουμε τα οικονομικά μεγέθη που έχει το spam από το έτος 2003 έως και το 2007



Εικόνα 10 Στο σχήμα αυτό παρουσιάζονται τα μεγέθη των spam μηνυμάτων και των email για τα έτη 2003 έως 2008

2.3 Ποιο είναι το ισχύον θεσμικό πλαίσιο για το spam στην Ελλάδα

Στην Ελλάδα το spam ρυθμίζεται από το *άρθρο 11* του *Νόμου 3471/2006*, οποίος ενσωματώνεται στο εθνικό δίκαιο τη *Οδηγία 2002/58/ΕΚ* για την προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών.

Σύμφωνα με την *παράγραφο 1* του *άρθρου 11 «Μη ζητηθείσα επικοινωνία»: « Η χρησιμοποίηση αυτόκλητων συστημάτων κλήσης, ιδίως με χρήση συσκευών τηλεομοιοτυπίας (φαξ) ή ηλεκτρονικού ταχυδρομείου και γενικότερα η πραγματοποίηση μη ζητηθεισών επικοινωνιών με οποιοδήποτε μέσο ηλεκτρονικής επικοινωνίας, η με χωρίς ανθρώπινη παρέμβαση, για σκοπούς απευθείας εμπορικής προώθησης προϊόντων ή υπηρεσιών για κάθε είδους διαφημιστικούς σκοπούς, επιτρέπεται μόνο αν ο συνδρομητής συγκατατεθεί εκ των προτέρων ρητός»*

Με άλλα λόγια, κάθε ηλεκτρονικό μήνυμα που σας αποστέλλεται χωρίς την πρότερη ρητή συγκατάθεση σας, δηλαδή κάθε μήνυμα spam, είναι παράνομο. Το σύστημα αυτό είναι γνωστό στη διεθνή ορολογία ως σύστημα «opt-in».

Ειδικά γι αυτά μηνύματα ηλεκτρονικού ταχυδρομείου, εξαιρέσει αποτελεί, σύμφωνα με την *παράγραφο 3 του άρθρου 11*, η περίπτωση στην οποία η ηλεκτρονική διεύθυνση του χρήστη αποκτήθηκε από τον αποστολέα νομίμως, στο πλαίσιο της πώλησης προϊόντων ή υπηρεσιών του προμηθευτή ή για την εξυπηρέτηση παρόμοιων σκοπών, ακόμη και όταν ο αποδέκτης του μηνύματος δεν έχει δώσει εκ των προτέρων την συγκατάθεση 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 στοιχείων, και αυτό σε κάθε μήνυμα σε περίπτωση που ο χρήστης αρχικά δεν είχε διαφωνήσει σε αυτή τη χρήση.

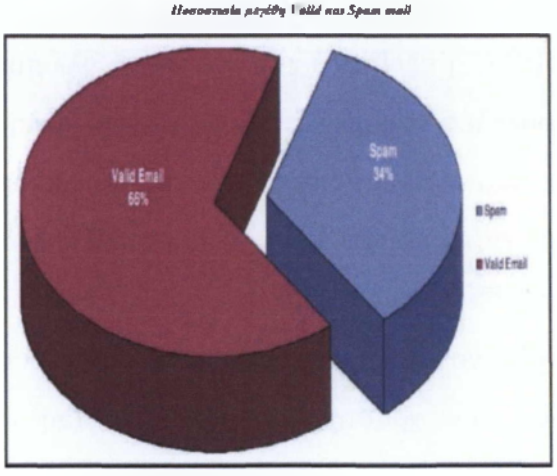
Επίσης, ως προς την αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου που έχουν σκοπό την άμεση εμπορική προώθηση προϊόντων και υπηρεσιών, ορίζεται ότι θα πρέπει να αναφέρεται ευδιάκριτα και σαφώς η ταυτότητα του αποστολέα ή του προσώπου προς όφελος του οποίου

αποστέλλεται το μήνυμα, καθώς επίσης και η διεύθυνση στην οποία ο αποδέκτης του μηνύματος μπορεί να ζητά τον τερματισμό της επικοινωνίας. Η εφαρμογή των παραπάνω ρυθμίσεων επεκτείνεται, πέρα από τα φυσικά , και τα νομικά πρόσωπα.

2.4 Στατιστικά στοιχεία

Στην ενότητα αυτή θα παρουσιάσουμε ορισμένα στατιστικά στοιχεία, σχετικά με την εξέλιξη του Spamming, σε μια προσπάθεια για καλύτερη κατανόηση του μεγέθους του φαινομένου και των πολλαπλών επιπτώσεων που επιφέρει σε διάφορους τομείς της καθημερινής δραστηριότητας, τόσο σε Ευρωπαϊκό όσο και σε Παγκόσμιο επίπεδο.

Στην Εικόνα 11 που ακολουθεί παρουσιάζεται το ποσοστιαίο μέγεθος που αντιστοιχεί στα έγκυρα μηνύματα ηλεκτρονικού ταχυδρομείου (valid mail) και στα μηνύματα spam (spam mail). Τα στοιχεία προέρχονται από μια σχετική έρευνα που πραγματοποιήθηκε τον Ιούνιο του 2003 από την εταιρεία Brightmail.

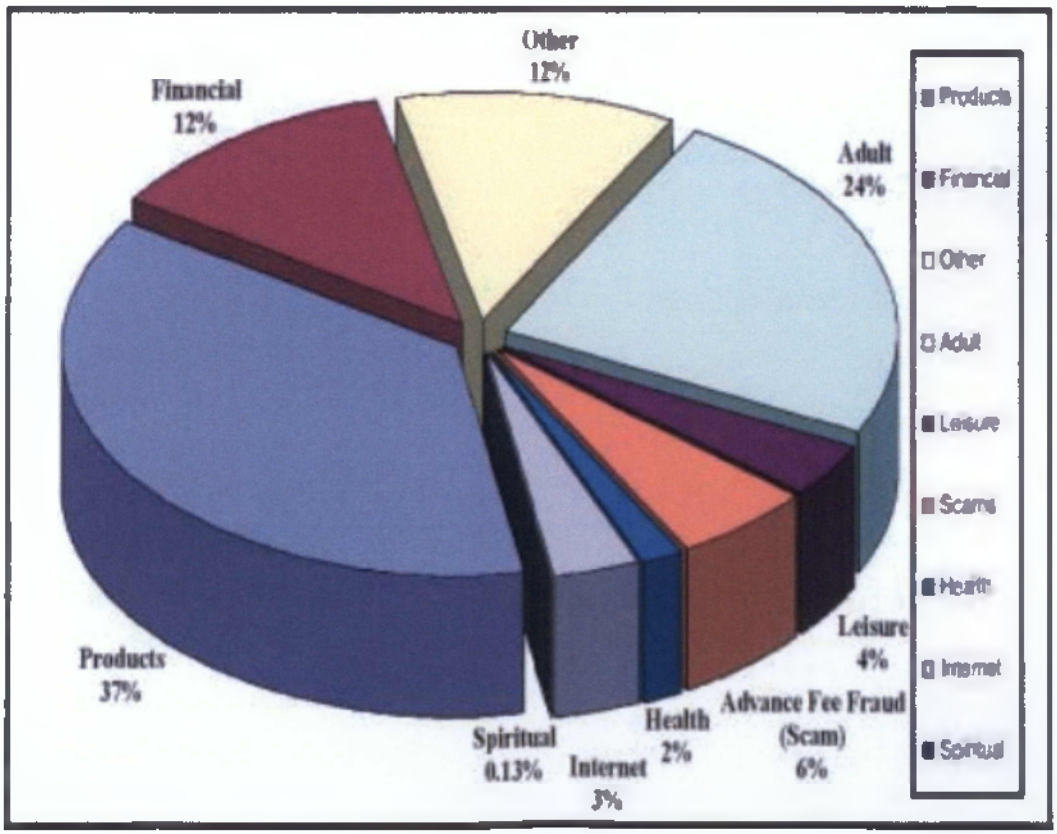


Εικόνα *11* Ποσοστιαία μεγέθη ***Valid*** και ***Spam mail***

Όπως μπορεί εύκολα να παρατηρήσει κανείς το ποσοστό που καταλαμβάνουν τα spam mail στο συνολικό μέγεθος των μηνυμάτων που διακινούνται μέσω του διαδικτύου δεν είναι σε καμία περίπτωση αμελητέο. Ειδικά δε αν αναλογιστεί κανείς και τον ταχύτατο ρυθμό ανάπτυξής του, τότε θα διαπιστώσει τις πραγματικές διαστάσεις του προβλήματος.

Στην παρακάτω Εικόνα 12 παρουσιάζονται οι τομείς της καθημερινής δραστηριότητας που αποτελούν στόχο και ταυτόχρονα περιεχόμενο των spam μηνυμάτων, μαζί με τα αντίστοιχα ποσοστά τους. Τα μεγέθη προκύπτουν από σχετική έρευνα της εταιρείας Brightmail.

Τομείς καθημερινής δραστηριότητας που αποτελούν στόχο των spam mails



Εικόνα 12 Τομείς καθημερινής δραστηριότητας που αποτελούν στόχο των spam mails

Γίνεται εύκολα αντιληπτό ότι το μεγαλύτερο μερίδιο καταλαμβάνουν τα προϊόντα, τα οποία αποτελούν και βασικό στόχο προώθησης των spam mail. Ακολουθούν τα, ακατάλληλα για ανηλίκους, προϊόντα, τα οποία συνήθως περιέχουν πορνογραφικό υλικό ή διάφορα άλλα στοιχεία σεξουαλικού ενδιαφέροντος. Αξιοσημείωτο ποσοστό κατέχουν και τα μηνύματα που σχετίζονται με οικονομικές αναφορές, τα οποία συνήθως περιέχουν τρόπους για να κερδίσει κανείς εύκολα και γρήγορα χρήματα (easy money).

Τα υπόλοιπα ποσοστά μοιράζονται στις εξής κατηγορίες:

1. Ελεύθερος Χρόνος 4%

2. Scam (Ψευδή επιχειρησιακά σχέδια ή απάτες) 6%

3. Υγεία 2%

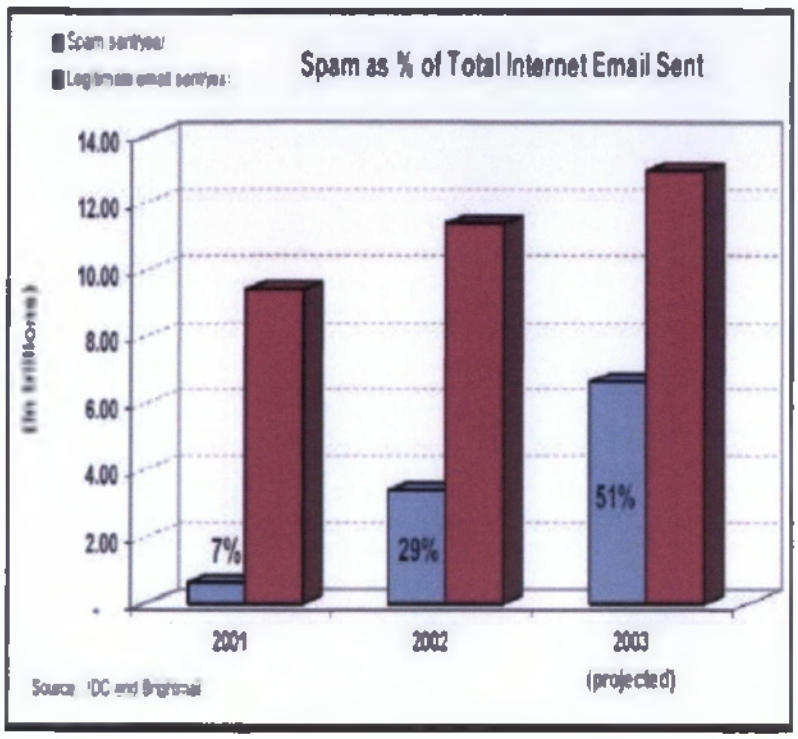
4. Διαδίκτυο 3%

5. Πνευματικά / Θρησκευτικά 0.13%

6. Άλλα θέματα 12%

Στην Εικόνα 13 παρατίθεται μια γενική εικόνα της αυξητικής τάσης του φαινομένου σε Παγκόσμιο επίπεδο. Τα στοιχεία προέρχονται από σχετική έρευνα των εταιρειών IDC και Brighmail και αναφέρονται στην τριετία 2001-2003.

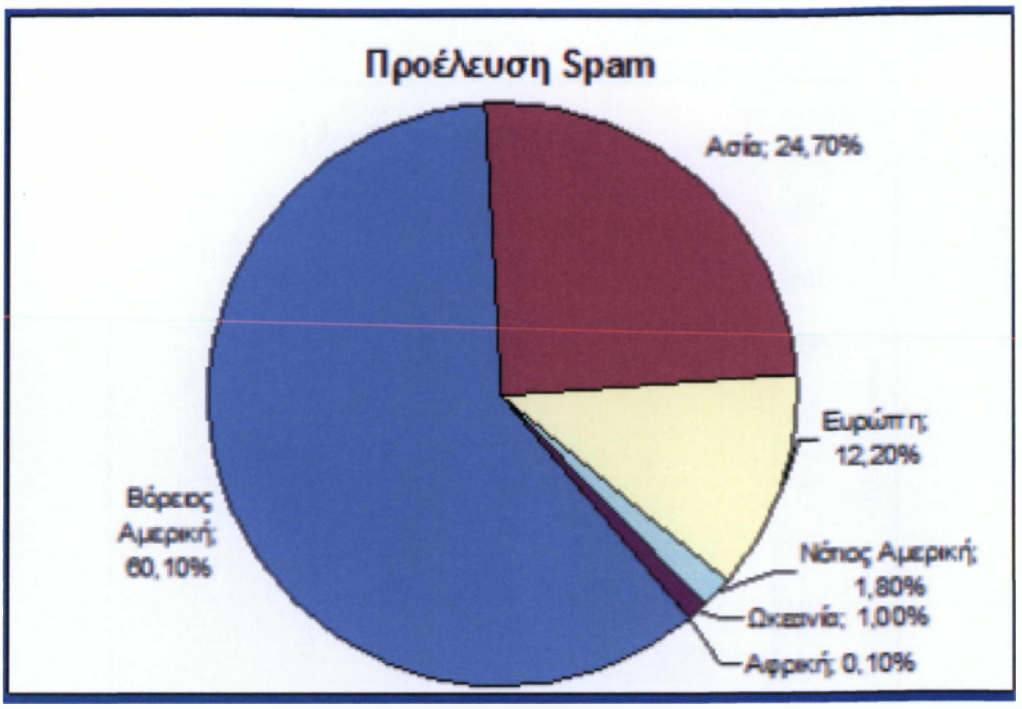
Γενική Εικόνα του Spamming από το 2001 έως το 2003



Εικόνα 13 Γενική εικόνα του Spamming από το 2001 έως το 2003

Η αυξητική πορεία του προβλήματος είναι εμφανής. Από το 2001 έως σήμερα το ποσοστό των spam mail που μεταδίδονται μέσω Internet έχει αυξηθεί κατά εφτά φορές περίπου. Η πιο εύλογη ανησυχία που μπορεί να διατυπώσει κανείς, είναι που θα καταλήξει το spamming αν συνεχίσει να αυξάνεται και να πολλαπλασιάζεται με αυτόν το ρυθμό και με ποιον τρόπο θα αντιμετωπιστεί άμεσα και ριζικά .

Στην Εικόνα 14 παρουσιάζεται το ποσοστό προέλευσης του Spam. Τα μεγέθη προκύπτουν από την έρευνα που σημειώθηκε το 2005



Εικόνα 14 Ποσοστά προέλευσης του spam από την έρευνα του 2005

Όπως βλέπουμε στο σχήμα το μεγαλύτερο πρόβλημα ήταν στην Βόρειο Αμερική με ποσοστό 60,10%. Ακολουθεί η Ασία με 24,70%, η Ευρώπη με 12.20% η Νότιο Αμερική με 1.80%, η Ωκεανία με 1,00% και τέλος η Αφρική με το ποσοστό 0,10%.

Στη συνεχεία μπορούμε να δούμε πιο αναλυτικά για τα 2 τελευταία έτη τα στατιστικά που αφορούν τα spam (πηγή εταιρεία commtouch)

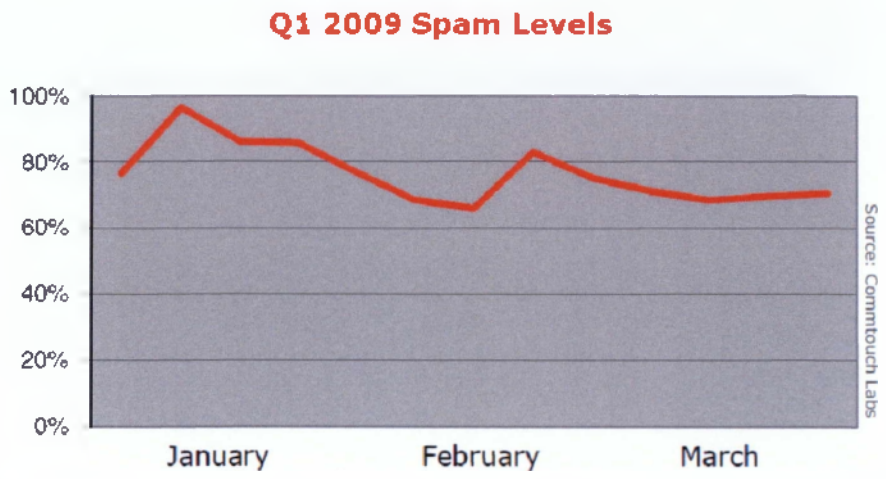
1^{ο} τρίμηνο του 2009

Topics of Spam Email Q1 2009	
Loans – 28%	Dating – 6%
Replicas – 20%	Degrees – 4%
Pharmacy – 19%	Software – 1%
Enhancers – 11%	Other – 4.6%
Weight Loss – 7%	

Source: Commtouch Labs

Εικόνα 15 Στατιστικά στοιχεία του spam για το πρώτο τρίμηνο του 2009

Στην παραπάνω εικόνα παρατηρούμε πως τα spams που έχουν ως θέμα τους τα δάνεια καταλαμβάνουν το μεγαλύτερο ποσοστό



Εικόνα 16 Μέσος όρος του Spam για το πρώτο τρίμηνο του 2009

Στο ανωτέρω γράφημα παρατηρούμε πως ο μέσος Όρος των spam για το συγκεκριμένο τρίμηνο άγγιζε το 72% την συνολικής κίνησης email, με αποκορύφωμα το 96% στις αρχές Ιανουαρίου και χαμηλότερο ποσοστό το 65% κατά τη διάρκεια του Φεβρουαρίου.[11]

2° τρίμηνο 2009

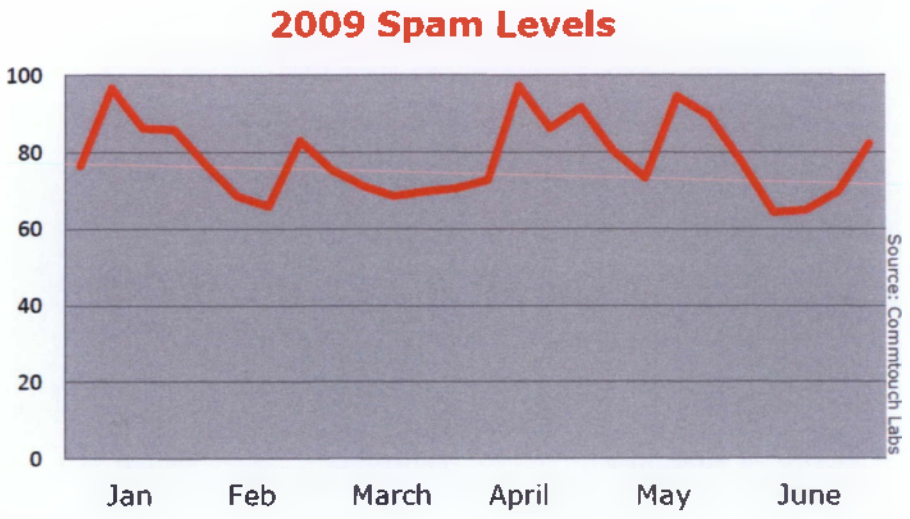
Topics of Spam Email Q1 2009			
Enhancers	46.2%	Software	1.3%
Pharmacy	33%	Degrees	0.8%
Replica	10.6%	Other	6.1%
Scams	2%		

Source: Commtouch Labs

Εικόνα 17 Στατιστικά στοιχεία για το δεύτερο τρίμηνο του 2009

[11] http://www.commtouch.com/download/1348

Παρατηρούμε πως πλέον στην πρώτη θέση των spam αφορούν τα θέματα με βελτιωτικά φάρμακα καταλαμβάνοντας μάλιστα το 46% του συνολικού μεγέθους



Εικόνα 18 Μέσος όρος του spam για το δεύτερο τρίμηνο του 2009

Στο προηγούμενο γράφημα παρατηρούμε πως ο μέσος όρος των spam για το συγκεκριμένο τρίμηνο άγγιζε το 80% της συνολικής κίνησης email, με αποκορύφωμα το 97% κατά την περίοδο του Απριλίου και χαμηλότερο ποσοστό το 64% κατά τη διάρκεια του Ιουνίου.[12]

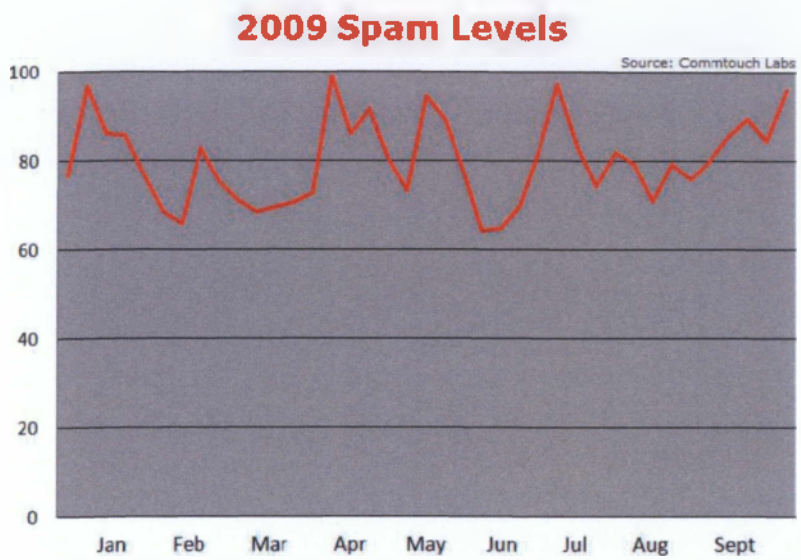
3ο τρίμηνο 2009

Topics of Spam Email Q3 2009	
Pharmacy	68%
Replicas	19%
Enhancers	11%
Degrees	1%
Other	1%

Εικόνα 19 Στατιστικά στοιχεία για το τρίτο τρίμηνο του 2009

[12] http://www.commtouch.com/download/1491

Την πρώτη θέση καταλαμβάνουν πλέον τα spam που αφορούν σε φαρμακευτικά προϊόντα με εξαιρετικά μεγάλο ποσοστό μάλιστα 68%.



Εικόνα *20* Μέσος όρος του ***spam*** για το τρίτο τρίμηνο του ***2009***

Στο ανωτέρω γράφημα παρατηρούμε πως ο μέσος όρος των spam για το συγκεκριμένο τρίμηνο έφτασε 83% της συνολικής κίνησης email, με αποκορύφωμα το 97% το μηνά Ιούλιο και χαμηλότερο ποσοστό το 71% κατά τη διάρκεια του Αύγουστου.[13]

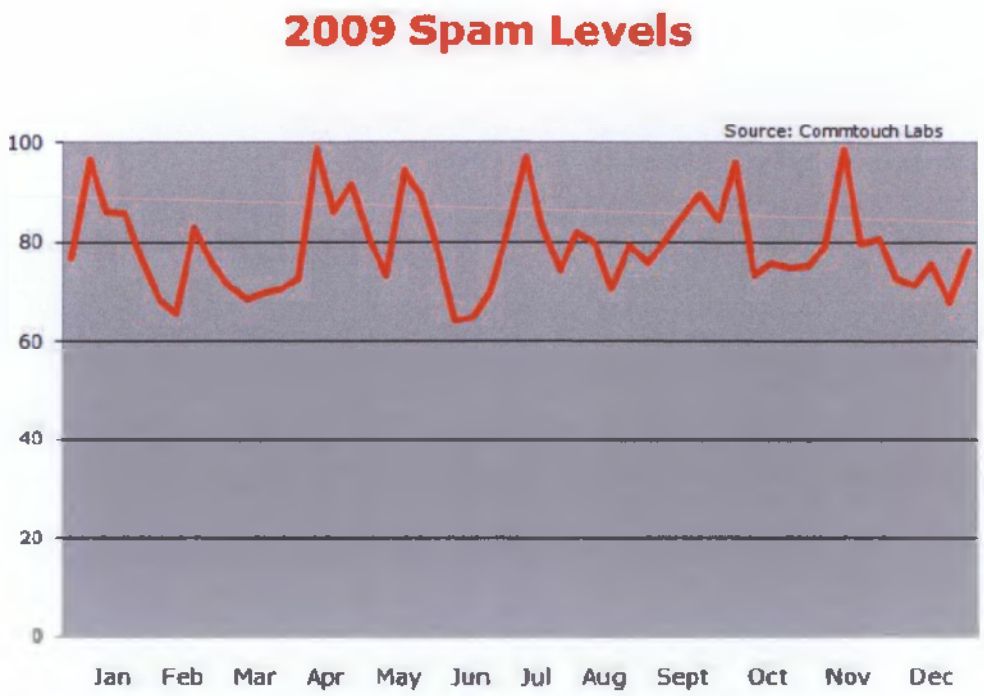
4^{ο} τρίμηνο 2009

Topics of Spam Email Q4 2009			
Pharmacy	81%	Degrees	1.3%
Replica	5.4%	Casino	1%
Enhancers	2.3%	Weight Loss	0.4%
Phishing	2.3%	Other	6.3%

Εικόνα 21 Στατιστικά στοιχεία του spam για το τέταρτο τρίμηνο του 2009

Τα spam με κεντρικό περιεχόμενο φαρμακευτικά προϊόντα παραμένουν στην πρώτη θέση

[13] http://www.commtouch.com/download/1548

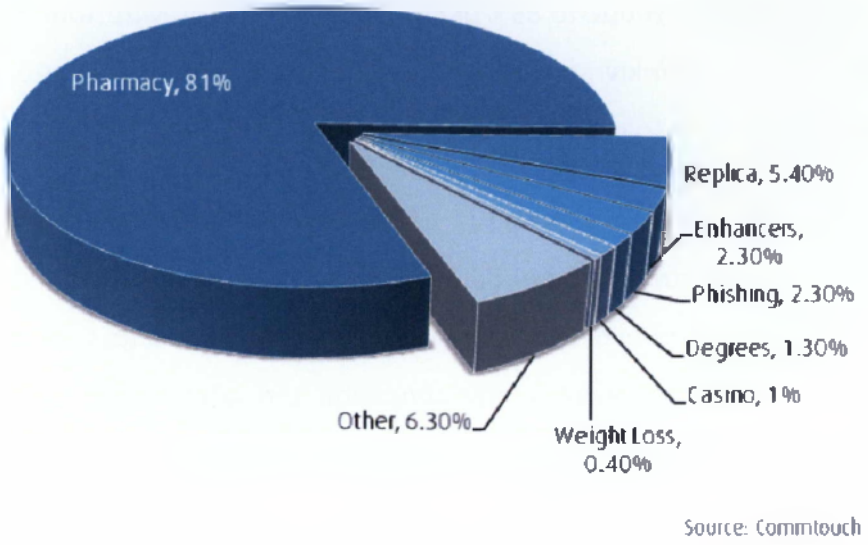


Εικόνα 22 Μέσος όρος του spam για το τέταρτο τρίμηνο του 2009

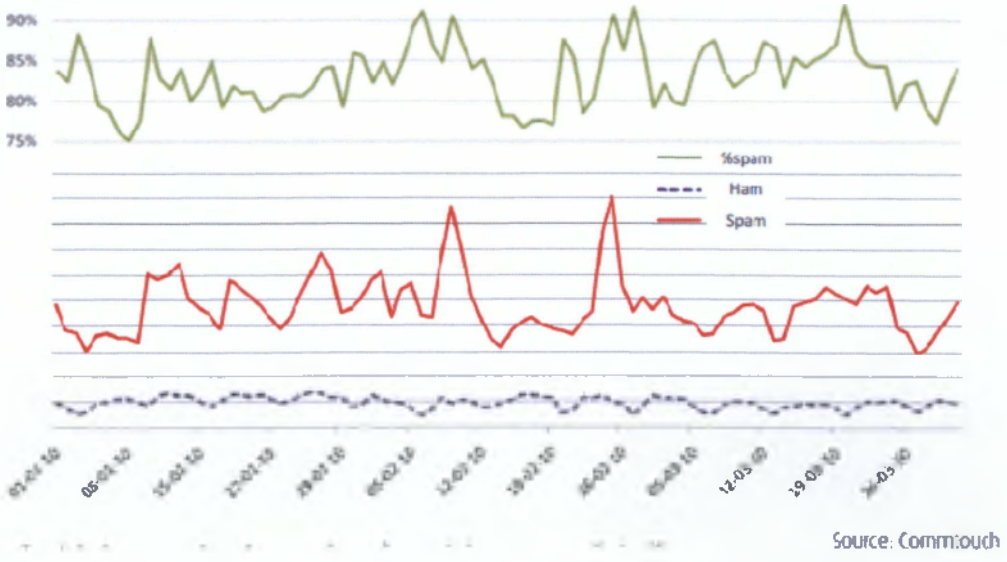
Στο ανωτέρω γράφημα παρατηρούμε πως ο μέσος όρος των spam για το συγκεκριμένο τρίμηνο άγγιζε το 97% της συνολικής κίνησης email, με αποκορύφωμα το 98% το νοερή του 2009 και χαμηλότερο ποσοστό το 68% κατά το τέλος Δεκεμβρίου.[14]

1° τρίμηνο 2010

[14] http://www.commtouch.com/download/1629



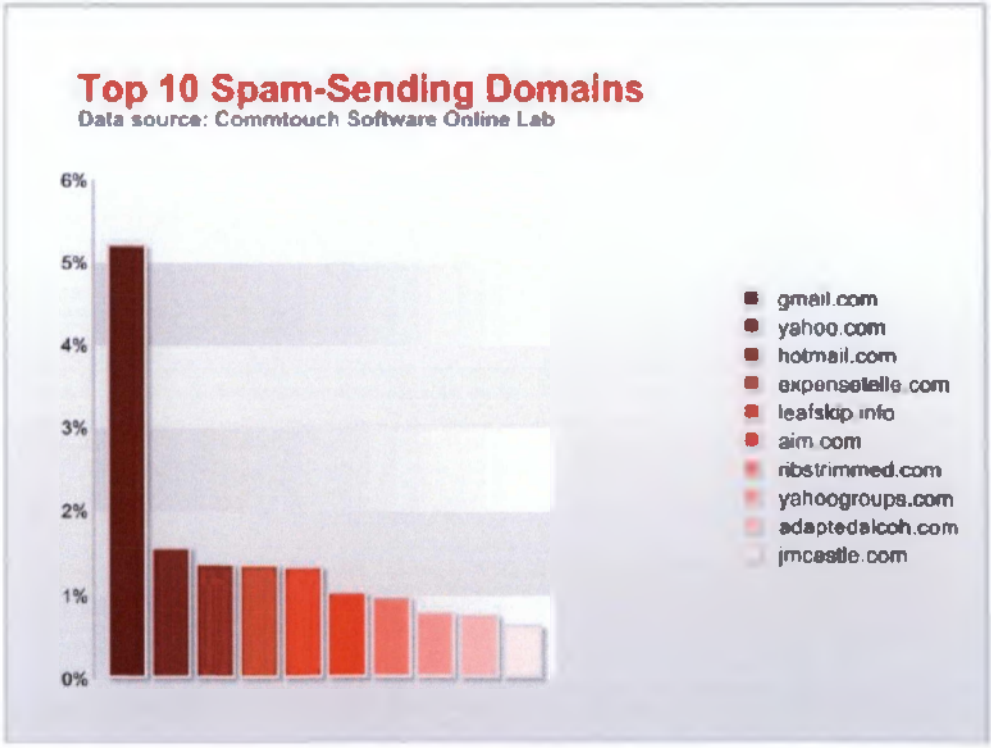
Εικόνα 23 Στατιστικά στοιχεία του spam για το πρώτο τρίμηνο του 2010



Εικόνα 24 Μέσος όρος του spam για το πρώτο τρίμηνο του 2010

Στα παραπάνω γραφήματα έχουμε το 83% μέσος Όρος, 92% τέλος Μαρτίου 75% αρχή χρονιάς, υποθέτοντας πως η συνολική κίνηση των email είναι 220 δις την ημέρα αυτό αντιστοιχεί και σημαίνει πως ανά ημέρα κυκλοφορούσαν 183 δις spam

Στο πλαίσιο της ανάλυσης της Commtouch για την ανεπιθύμητη αλληλογραφία η εταιρεία παρακολουθεί τα domains που χρησιμοποιούνται από τους spammers στο πεδίο "Από" των το spam emails. Φυσικά οι διευθύνσεις είναι συνήθως πλάστες, προκειμένου να ξεγελάσουν τα anti-spam συστήματα και να δώσουν την εντύπωση μια αξιόπιστης, πραγματικής πηγής. Περιστασιακά οι spammers θα χρησιμοποιήσουν ένα όνομα εταιρείας, για παράδειγμα, UPS – ιδιαίτερα κατά την αποστολή κακόβουλου λογισμικού που μεταμφιέζεται ως «UPS delivery information ». Το domain που είναι πιο συχνά φαλκιδεύεται είναι το Gmail.com. (όπως παρουσιάζεται και στο ακόλουθο γράφημα)



Εικόνα 25 Οι εταιρείες που "φαίνονται" ως αποστολής κακόβουλων spam

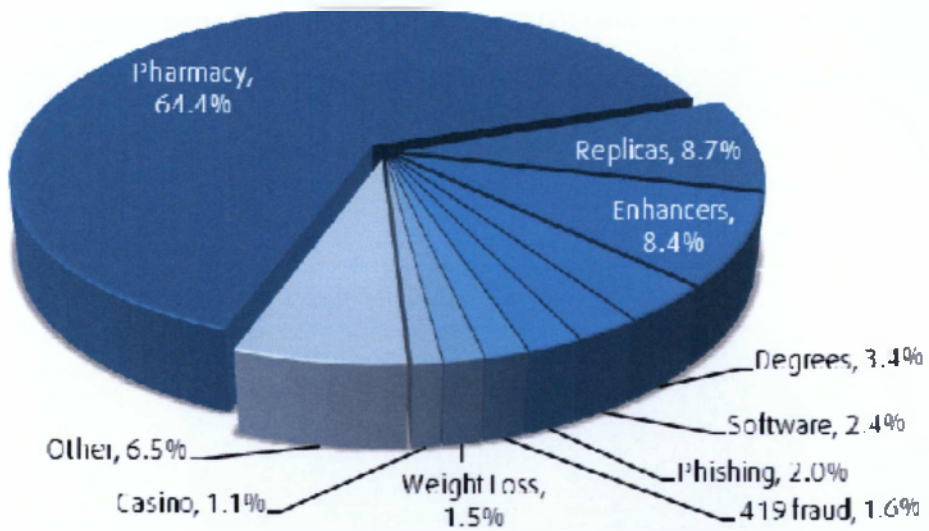
The results for all emails in the analysis period from gmail.com are presented below.

- % of genuine Gmail senders 59%
- % of fake Gmail senders 41%
- % of emails classified as spam 42%
- % of spam emails sent by genuine Gmail accounts 1%

Εικόνα 26 Στατιστικά στοιχεία για το πρώτο τρίμηνο του 2010

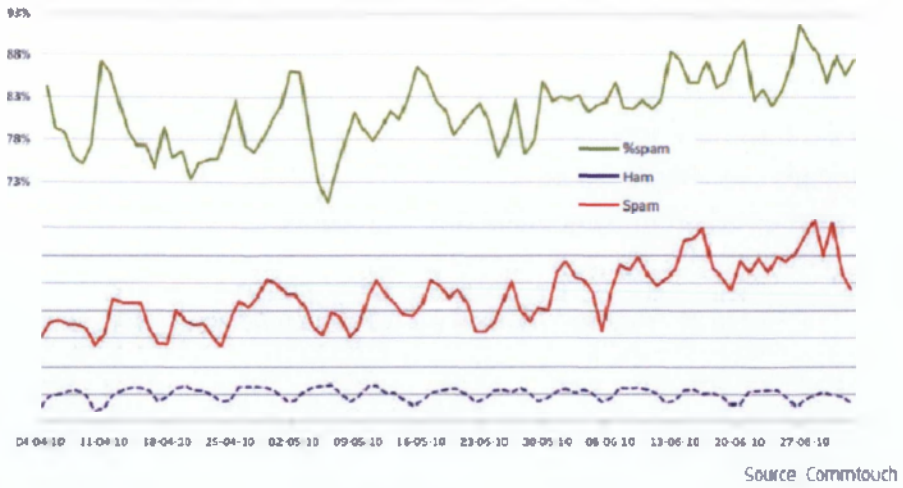
Επιπλέον από τα στατιστικά που παρουσιάζονται στο προηγούμενο γράφημα παρατηρούμε πως μόλις το 1% των spam που φαίνεται να προέρχονται από το Gmail.com είναι όντως από γνησίους λογαριασμούς του Gmail.com. [15]

2° τρίμηνο 2010



Εικόνα 27 Στατιστικά στοιχεία για το δεύτερο τρίμηνο του 2010

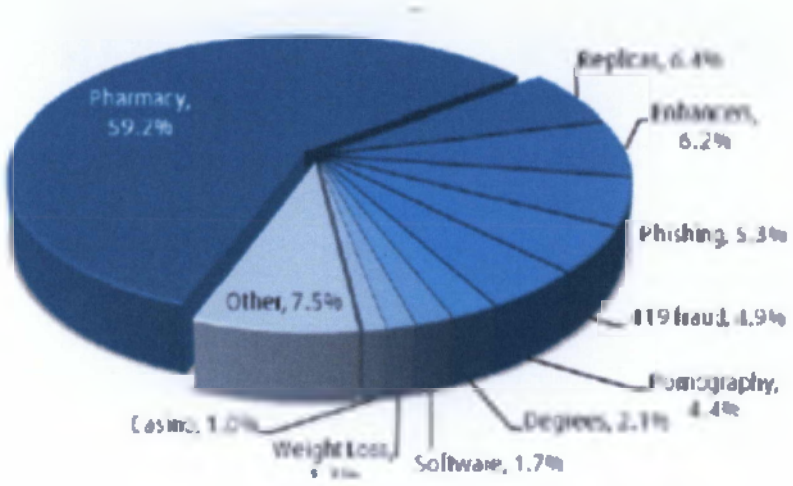
[15] http://www.commtouch.com/download/1679



Εικόνα *28* Μέσος όρος του ***spam*** για το δεύτερο τρίμηνο του ***2010***

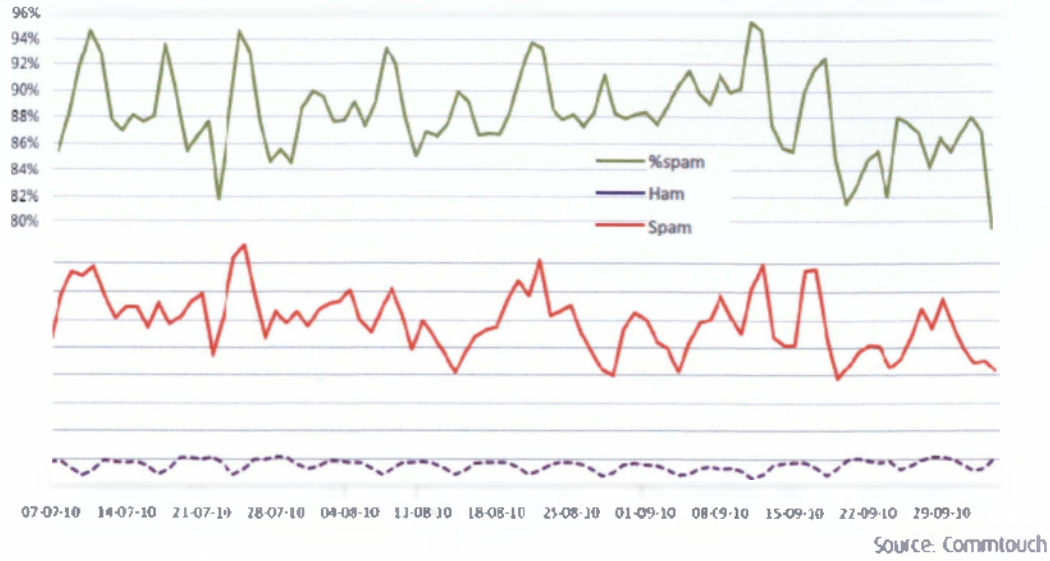
Στο ανωτέρω γράφημα παρατηρούμε πως ο μέσος Όρος των spam για το συγκεκριμένο τρίμηνο άγγιζε το 32% την συνολικής κίνησης email, με αποκορύφωμα το 92% στο τέλος Ιουνίου και χαμηλότερο ποσοστό το 71% στις αρχές Μαΐου.[16]

3° τρίμηνο 2010



Εικόνα *29* Στατιστικά στοιχεία του ***spam*** για το τρίτο τρίμηνο ***2010***

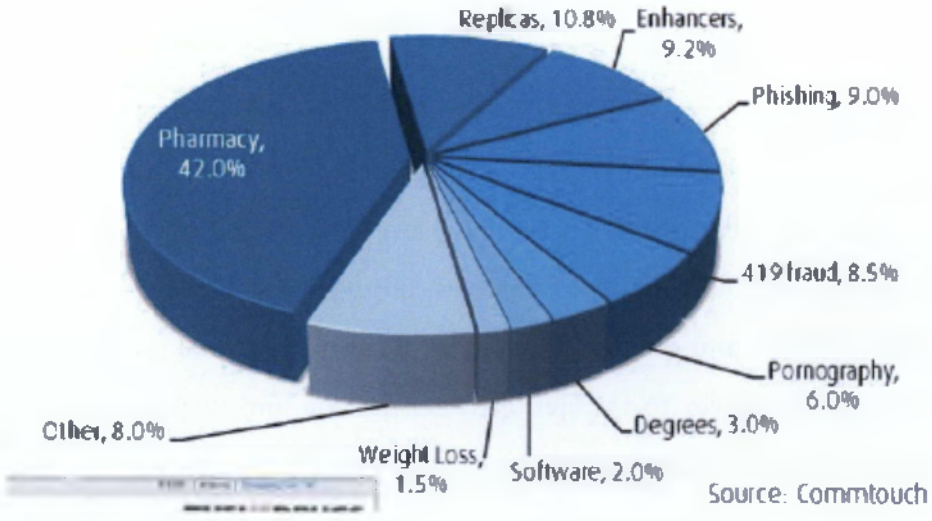
[16] http://www.commtouch.com/download/1753



Εικόνα 30 Μέσος όρος του spam για το τρίτο τρίμηνο του 2010

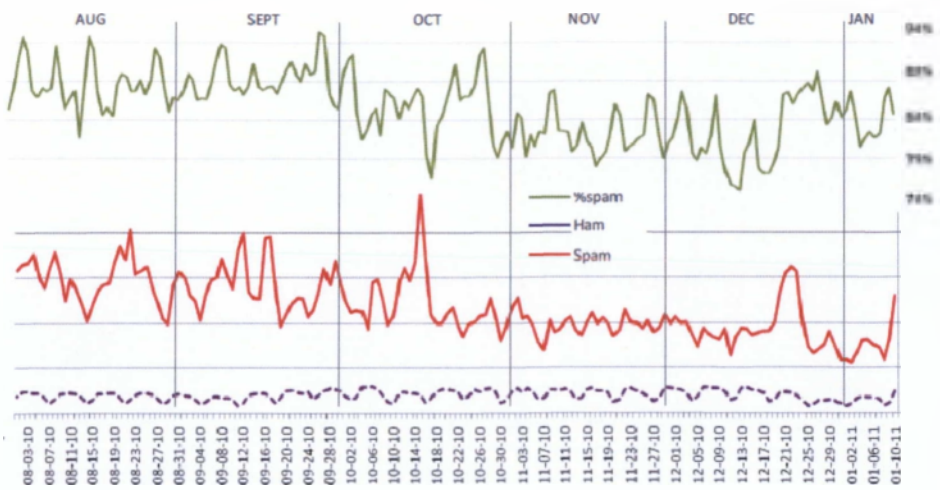
Στο ανωτέρω γράφημα παρατηρούμε πως ο μέσος όρος των spam για το συγκεκριμένο τρίμηνο άγγιζε το 88% της συνολικής κίνησης email, με αποκορύφωμα το 95% στα μέσα Σεπτεμβρίου και χαμηλότερο ποσοστό το 80% κατά το τέλος του τρίμηνου.[17]

4° τρίμηνο 2010



Εικόνα 31 Στατιστικά στοιχεία του spam για το τέταρτο τρίμηνο του 2010

[17] http://www.commtouch.com/download/1850



Εικόνα 32 Μέσος όρος του spam για το τέταρτο τρίμηνο του 2010

Μια πτώση σε επίπεδα spam παρατηρήθηκε στο τέλος του τρίτου τριμήνου όμως κατά τη χρονική στιγμή δεν ήταν σαφές αν η μείωση ήταν μια βραχυπρόθεσμη πτώση ή θα ήταν πιο παρατεταμένη.

Η μείωση του spam είναι πιθανότατα οφείλεται στο κλείσιμο του Spamit γύρω στα τέλη του Σεπτεμβρίου. Spamit είναι η οργάνωση που φέρεται να είναι πίσω από ένα μεγάλο ποσοστό φαρμακευτικών spam. Σύμφωνα με πληροφορίες, τον Οκτώβριο, οι λόγοι για το αιφνίδιο κλείσιμο του Spamit είχαν σχέση με καταγγελίες κατά των ατόμων πίσω από την οργάνωση.

Η ανάλυση των δεδομένων ανεπιθύμητης αλληλογραφίας για το τέταρτο τρίμηνο αποκαλύπτει ότι η μείωση της ανεπιθύμητης αλληλογραφίας διατηρήθηκε σε όλο το 4^{ο} τρίμηνο του 2010 εκτός από μια σύντομη προ-Χριστουγέννων περίοδο. Ο Ημερήσιος μέσος όρος του Δεκεμβρίου ήταν περίπου 30% λιγότερο από ότι τον Σεπτέμβριο. Ο μέσο ποσό των spam ως ποσοστό του συνολικού ποσού των e-mail για το τρίμηνο ήταν 83%, κάτω από 88% του 3^{ου} τρίμηνου του 2010. Στις αρχές Δεκεμβρίου παρατηρήθηκε ένα χαμηλό επίπεδο του σχεδόν 74%. Ο μέσος όρος ανά ημέρα των μηνυμάτων spam για το τρίμηνο ήταν περίπου 142 δισεκατομμύρια (από 198 δισεκατομμύρια το 3ο τρίμηνο του 2010). Στις αρχές του Ιανουαρίου 2011 καθώς η περίοδος των διακοπών τελείωνε, σημειώνεται μια ξαφνική αύξηση του επιπέδου της

ανεπιθύμητης αλληλογραφίας. Η συνολική ημερήσια ποσότητα αυξήθηκε κατά 45% σε σύγκριση με τον μέσο όρο των προηγούμενων 2 εβδομάδων.[18]

[18] http://www.commtouch.com/download/1934

ΚΕΦΑΛΑΙΟ 3

ΤΡΟΠΟΙ ΑΝΤΙΜΕΤΩΠΙΣΗΣ

3.1 Αντιμετώπιση του spamming από μεμονωμένους χρήστες

Συνήθως ο παραλήπτης ενός spam μηνύματος από ένα συγκεκριμένο δικτυακό τόπο, έχει την δυνατότητα να διαγραφεί από την σχετική λίστα παραληπτών, αρκεί να στείλει ένα μήνυμα σε συγκεκριμένη μορφή σε κάποια ηλεκτρονική διεύθυνση που αναγράφεται στο τέλος του μηνύματος. Σε καμία όμως περίπτωση δεν πρέπει να δίνεται απάντηση σε τέτοιου είδους μηνύματα για τους εξής λόγους :

- Ενημερώνει τον spammer ότι πρόκειται για ενεργό λογαριασμό, γεγονός που τον ενθαρρύνει για αποστολή περισσότερων ενοχλητικών μηνυμάτων.
- Είναι πολύ πιθανό να εκγλυφθεί σαν πράξη αποδοχής λήψης τέτοιου είδους μηνυμάτων, στοιχειό που διευκολύνει τη δράση του εκάστοτε spammer και ταυτόχρονα δυσχεραίνει την αντιμετώπιση και τον αποκλεισμό του.

Στην περίπτωση, όμως που δεν προσφέρεται η δυνατότητα διαγραφής από την λίστα παραληπτών, τότε ο χρήστης μπορεί να καταφύγει στην χρήση της επιλογής φιλτραρίσματος του προγράμματος ηλεκτρονικής αλληλογραφίας που χρησιμοποίει. Επίσης υπάρχουν διαδικτυακή τόποι στους οποίους ο χρήστης μπορεί να απευθυνθεί για την δίωξη των υπαιτίων ενοχλητικών μηνυμάτων. Ο πιο γνωστός και διαδεδομένος οργανισμός ενάντια στο spamming είναι ο Coalition Against Unsolicited Commercial Email και βρίσκεται στην ηλεκτρονική διεύθυνση `www.cause.org`.

Μια πιο αποτελεσματική αντίδραση, παρόλο που προϋποθέτει αναζήτηση για την εύρεση της σχετικής πληροφορίας, είναι η αναφορά του spammer στην εταιρεία παροχής υπηρεσιών Internet που χρησιμοποιεί. Τα προγράμματα αντιμετώπισης του φαινομένου, τα οποία μπορεί να βρει εύκολα κανείς σε ανάλογες δικτυακές τοποθεσίες όπως `www.tucows.com` , `www.download.com` κτλ., αποτελούν μια εύκολη και γρήγορη λύση τις περισσότερες φορές όμως δεν αναχαιτίζουν πλήρως την δράση των spammers.Αξίζει να σημειωθεί ότι ορισμένα προγράμματα αλληλογραφίας(mailers) παρέχουν τη δυνατότητα αποκλεισμού ορισμένων ηλεκτρονικών διευθύνσεων (block address).

Με αυτόν τον τρόπο ο χρήστης μπορεί να διαχειριστεί από τον server ορισμένα spam mails και να περιορίσει τον αριθμό των spam εισερχόμενων μηνυμάτων, με απαραίτητη προϋπόθεση να γνωρίζει την ηλεκτρονική διεύθυνση του αποστολέα τους. Η λύση αυτή δεν είναι ριζική, γιατί είναι σχεδόν πάγια τακτική ενός spammer η χρήση πλαστής ηλεκτρονικής διεύθυνσης αποστολέα και συχνά διαφορετικής για κάθε αποστολή. Η αναφορά των περιστατικών αυτών στον παροχέα του αποστολέα, συμβάλλει σημαντικά στην καταπολέμηση τέτοιων ενεργειών και περιορίζει την επανάληψη τους. [19]

3.1.1 Τακτικές για την αποφυγή των ανεπιθύμητων μηνυμάτων ηλεκτρονικού ταχυδρομείου(spam) από μεμονωμένους χρήστες

1.Χρηση διαφορετικού screen name στις δικτυακές συνομιλίες, το οποίο να μην σχετίζεται με την ηλεκτρονική διεύθυνση.

2.Χρηση ηλεκτρονικών διευθύνσεων μιας χρήσης.

Τα περισσότερα συστήματα διαχείρισης ηλεκτρονικού ταχυδρομείου, έχουν την δυνατότητα να δημιουργούν τέτοιου είδους διευθύνσεις και να προωθούν την ανεπιθύμητη αλληλογραφία

[19] Wikipedia.org

στο πραγματικό σας λογαριασμό. Στην περίπτωση που η διεύθυνση μιας χρήσης γίνει στόχος των spammers , είναι εύκολο να καταργηθεί και να δημιουργηθεί μια νέα.

3.Χρήση δυο ταχυδρομικών λογαριασμών.

Ο ένας για κοινή χρήση, όπως on line συμπλήρωση εντύπων, αγορές μέσω Internet και ο δεύτερος για ιδιωτική ή εταιρική όπως επαγγελματικές επικοινωνίες.

4.Χρηση μιας μοναδικής διεύθυνσης email , που θα περιέχει όχι μόνο αριθμούς αλλά και γράμματα.

Η σωστή επιλογή μιας ταχυδρομικής διεύθυνσης μπορεί να έχει δραστικά αποτελέσματα όσον αφορά στη μείωση των ενοχλητικών μηνυμάτων, γιατί δεν θα μπορεί να εντοπιστεί εύκολα από τους spammers που αποστέλλουν μηνύματα προς κοινότυπους λογαριασμούς.

5.Δεν πρέπει να δημοσιεύονται οι διευθύνσεις ηλεκτρονικού ταχυδρομείου.

Βάζοντας τη διεύθυνση ηλεκτρονικού ταχυδρομείου σε μια ιστοσελίδα είναι σχεδόν σίγουρο ότι σύντομα θα σταλούν στον χρήστη μηνύματα Spam στο γραμματοκιβώτιο.

6.Δεν πρέπει να δίνεται η διεύθυνση ηλεκτρονικού ταχυδρομείου, σε οργανισμούς που δεν είναι εμπιστοσύνης.

Οι χρηστές πρέπει να είναι προσεκτικοί όταν επισκέπτονται διάφορους δικτυακούς τόπους και ζητείται η συμπλήρωση προσωπικών στοιχείων και στοιχείων επικοινωνίας, όπως το email . Αν είναι αναγκαστικό να δοθεί η διεύθυνση ηλεκτρονικού ταχυδρομείου, πρέπει να διαβαστούν προσεκτικά οι όροι χρήσης και η πολιτική εχεμύθειας με την οποία δεσμεύεται ο συγκεκριμένος οργανισμός.

7.Δεν πρέπει να δίνεται απάντηση στο spam.

Οι χρηστές δεν πρέπει να απατάνε στους spammers ακόμα και στην ένδειξη για διαγραφή από τις mail λίστες τους. Είναι μια παγίδα με τελικό αποτέλεσμα:

- Να διαπιστωθεί η εγκυρότητα της mail διεύθυνσης του χρήστη και επομένως να γίνει στόχος αποστολής επιπλέον μηνυμάτων.

- Να χαθεί χρόνος του χρήστη και να σπαταλήσει πόρους χωρίς λόγο, ενώ δεν υπάρχει πρόβλημα.

8.Ελεγχος των συστημάτων του χρήστη, ώστε να είναι σωστά διαμορφωμένα και ασφαλή.

Ένα μεγάλο ποσοστό Spam διαδίδεται από mail servers που δεν είναι σωστά διαμορφωμένοι, αλλά ακόμα και από συστήματα χρηστών.

9.Διαδοση της γνώσης και της εμπειρίας σε σχέση με το Spam.

Ενημέρωση των χρηστών του δικτύου του κάθε χρήστη, μαθητές, εκπαιδευτικούς, διοικητικό προσωπικό, την οικογένεια του και τους φίλους του, για το θέμα του Spam και την αντιμετώπιση του. Είναι αρκετά συνηθισμένο οι spammers να συγκεντρώνουν e-mail διευθύνσεις από τις απαντήσεις χρηστών του Διαδικτύου.

3.2 Αντιμετώπιση του Spamming από μεγάλες εταιρείες

Το πρόβλημα του Spamming δεν έχει αφήσει καθόλου αδιάφορες τις εταιρείες που ασχολούνται με την παραγωγή λογισμικού ηλεκτρονικών συστημάτων και όχι μόνο. Ο προβληματισμός γι'αυτές είναι διπλός. Από την μια πλευρά προσπαθούν να αναπτύξουν

μεθόδους και αποτελεσματικά συστήματα για να απαλλαγούν οι ίδιες, κατά κύριο λόγο, από αυτό το πρόβλημα και από την άλλη για να προμηθεύσουν στην αγορά εφαρμογές που θα προσφέρουν τις ίδιες δυνατότητες σε οποιονδήποτε άλλο ενδιαφερόμενο, είτε από απλό χρήστη είτε εταιρεία.

Οι πιο σημαντικές επιπτώσεις, όμως, που έχει επιφέρει το spam και γενικότερα η αρκετά διαδεδομένη χρήση του αφορούν περισσότερο στους φορείς παροχής υπηρεσιών Διαδικτύου και αυτό συμβαίνει γιατί όλα τα μηνύματα που διακινούνται, είτε είναι έγκυρα είτε είναι μηνύματα spam, περνούν πρώτα μέσα από τους κεντρικούς υπολογιστές τους. Γι' αυτό το λόγο οι εταιρείες αυτές έχουν λάβει δραστικά μέτρα τόσο για την κάλυψη των οικονομικών τους συμφερόντων όσο και για την πλήρη κάλυψη της ασφάλειας των πελατών τους.

Οι ISPs έχουν δημιουργήσει «μαύρες λίστες» που περιέχουν ηλεκτρονικές διευθύνσεις και ονόματα δικτυακών τόπων που αναγνωρίζουν ότι ανήκουν σε spammers. Τις λίστες αυτές τις ανταλλάσσουν μεταξύ τους, έτσι ώστε να επιτυχαίνουν την καλύτερη δυνατή ενημέρωση τους. Οι περισσότεροι από αυτούς έχουν ήδη αναπτύξει μια σειρά από τεχνικά μέτρα για τον εντοπισμό και αποκλεισμό των άχρηστων μηνυμάτων. Παρόλα αυτά όμως κανένας ISP δεν είναι ακόμα σε θέση που να μπορεί να προσδιορίσει την αποτελεσματικότητα των μεθόδων που χρησιμοποίει για την καταπολέμηση του προβλήματος.

Οι συσκευές φιλτραρίσματος που χρησιμοποιούνται εντείνουν την απορία για το πόσο νόμιμο και θεμιτό είναι για έναν ιδιωτικό φορέα παροχής υπηρεσιών, να αποφασίζει και να κρίνει για λογαριασμό άλλων, ποια μηνύματα θα παραδώσει και ποια όχι. Επιπλέον είναι πολύ πιθανό να μην λειτουργήσουν αυτές οι συσκευές στην περίπτωση που έχει χρησιμοποιηθεί πλαστή ταυτότητα του αποστολέα των μηνυμάτων. Σε κάθε περίπτωση όμως πρέπει να τονιστεί ότι όλα αυτά τα μέτρα που έχουν ληφθεί από τους ISPs συμβάλλουν δραστικά στην μείωση των spam μηνυμάτων που κατορθώνουν να φτάσουν στον τελικό προορισμό τους.[20]

[20] Wikipedia.org

3.3 Αρχιτεκτονικές Φιλτραρίσματος του Spamming

Στη ενότητα αυτή εξετάζονται οι εναλλακτικές προσεγγίσεις που κατά καιρούς εμφανίστηκαν στο χώρο του φιλτραρίσματος μη αιτηθείσας ηλεκτρονικής αλληλογραφίας και συναντώνται σε σύγχρονες εμπορικές και μη εφαρμογές και υπηρεσίες. Για τη καλύτερη παρακολούθηση του περιεχομένου του η ενότητα αυτή διαρθρώνεται σε 8 ξεχωριστές ενότητες κάθε μια από τις οποίες αφιερώνεται στην παρουσίαση ενός από τους υπάρχοντες μηχανισμούς αναγνώρισης Spam μηνυμάτων και συμπληρώνεται από μια σύντομη περιγραφή των εφαρμογών φιλτραρίσματος που τις υλοποιούν.

3.3.1 Σύστημα Φιλτραρίσματος βασισμένα σε κανόνες

Μια από τις πρώτες χρονολογικά εμφανισθείσες κατηγορίες μεθόδων φιλτραρίσματος η οποία παραμένει στο προσκήνιο ακόμα και σήμερα λόγω της απλότητας που τη χαρακτηρίζει, είναι η κατασκευή εριστικών κανόνων για τον εντοπισμό γνωστών προτύπων spam μηνυμάτων. Ο έλεγχος δεν περιορίζεται μόνο στην αναζήτηση συνηθισμένων λέξεων-κλειδιών ή φράσεων που συναντώνται συχνά στο πεδίο του θέματος ή στο σώμα spam μηνυμάτων, άλλα σε πολλές υλοποιήσεις επεκτείνεται και στην μελέτη της δομής των επικεφαλίδων πέραν του περιεχομένου τους, για τον εντοπισμό στοιχείων που παρατηρούνται σπανιότερα σε θεμιτά μηνύματα. Ως παραδείγματα μπορούν να αναφερθούν: η ύπαρξη ενός μεγάλου αριθμού παραληπτών στο πεδίο CC ή η πολλαπλή παράθεση πεδίων CC με το καθένα να φέρει μια μόνο τιμή, ειδικευμένα πεδία που εισάγονται από προγράμματα μαζικής αποστολής μηνυμάτων παραποιημένες MIME επικεφαλίδες που στην πλειοψηφία των περιπτώσεων υποδηλώνουν ότι το αντίστοιχο συνημμένο αρχείο είναι μολυσμένο από κάποιον ιό , κ.α.

---

http://www.noc.ntua.gr/index.php?module=ContentExpress&func=display&ceid=104
http://www.dpa.gr/portal/page?_pageid=33%2c20920&_dad=portal&_schema=PORTAL#3

Ο παραπάνω μηχανισμός ανίχνευσης μη αιτηθείσας αλληλογραφίας χαίρει ευρείας αποδοχής από τους κατασκευαστές λογισμικού για το ηλεκτρονικό ταχυδρομείο, γεγονός που αποδεικνύεται από την πληθώρα των εφαρμογών διαχείρισης (όπως το Microsoft Outlook 98 και οι επόμενες εκδόσεις του) και εξειδικευμένων εφαρμογών φιλτραρίσματος που τον ενσωματώνουν.

Παρά την απλότητα του ωστόσο, δε χαρακτηρίζεται από ιδιαίτερα υψηλές επιδόσεις, όπως μπορεί αν διαπιστωθεί από τα αποτελέσματα των συγκριτικών δοκιμών του φίλτρου spam μηνυμάτων του Microsoft Outlook 2002. Η βασικότερη αιτία της χαμηλής του απόδοσης εντοπίζεται στην προσπάθεια του να καλύψει ένα ευρύτατο φάσμα χρηστών, που αντιστοιχίζεται σε ένα ευρύτατο φάσμα θεμιτών μηνυμάτων, μέρος των οποίων ενδέχεται να επαληθεύει κάποιους από τους κανόνες αναγνώρισης spam μηνυμάτων

3.3.2 Συστήματα Φιλτραρίσματος βασισμένα σε Μαύρες Λίστες

Επίσης δημοφιλής προσέγγιση είναι και εκείνη της χρήσης εκτεταμένων λιστών με ηλεκτρονικές διευθύνσεις γνωστών spammers στην απλούστερη τους μορφή, ή ακόμα και DNS-based IP διευθύνσεις γνωστών συμμοριών spammers, δικτυακών υπηρεσιών μαζικής αποστολής μηνυμάτων (spam-for-hire sites), πρακτόρων μεταφοράς ταχυδρομείου(MTAs) και αναμεταδοτών (mail relays) που υποστηρίζουν τα συμφέροντα ή έχουν πέσει θύματα εκμετάλλευσης των προαναφερθέντων ομάδων. Όσον αφορά στους μηχανισμούς ελέγχου που κάνουν χρήση των Μαύρων λιστών, οι πιο απλοϊκές υλοποιήσεις αρκούνται στη διασταύρωση του πεδίου του αποστολέα του μηνύματος με τις διευθύνσεις που περιέχονται στις λίστες, ενώ άλλες ελέγχουν για ύποπτες IP διευθύνσεις κατά μήκος ολόκληρης της διαδρομής των διακομιστών που ακλούθησε το μήνυμα για να φθάσει στον προορισμό του, προς αναζήτηση μη ασφαλών mail relays.

Η βιωσιμότητα της συγκεκριμένης μεθόδου φιλτραρίσματος βασίζεται σε μεγάλο βαθμό στην ουσιαστική συμβολή κάποιων ευαισθητοποιημένων ομάδων χρηστών που συγκεντρώνουν τα

απαραίτητα στοιχεία για τη δημιουργία των λιστών αυτών από τα spam μηνύματα που λαμβάνουν, καθώς και στην ύπαρξη spam «παγίδων» (Spam Traps), ηλεκτρονικών δηλαδή διευθύνσεων, που τοποθετούνται από φορείς ανάπτυξης anti-spam φίλτρων και από μη κερδοσκοπικούς οργανισμούς σε διάφορα στρατηγικά σημεία στο διαδίκτυο, με μοναδικό σκοπό να αποτελούν πόλο έλξης spam μηνυμάτων. Αναφορικά δε με την αποτελεσματικότητα της, αυτή εξαρτάται σχεδόν αποκλειστικά από την εγκυρότητα των διευθύνσεων που έχουν συλλεχθεί, χαρακτηριστικό το οποίο αποδεικνύεται πολύ δύσκολο να επιτευχθεί στην πράξη. Ο λόγος έγκειται τόσο στην πάγια τακτική των spammers να χρησιμοποιούν βραχύβιες ή πλασματικές ηλεκτρονικές διευθύνσεις, παραποιώντας τις επικεφαλίδες των μηνυμάτων που αποστέλλουν, όσο και στη συχνή αλλαγή διακομιστών ηλεκτρονικού ταχυδρομείου που χρησιμοποιούν, προσπαθώντας να καλύψουν κατά το δυνατόν τα ίχνη τους, με αποτέλεσμα σε πολύ σύντομο χρονικό διάστημα οι λίστες να περιέχουν παρωχημένες πληροφορίες. Προς αντιμετώπιση του προβλήματος αυτού, οι χρήστες τέτοιων συστημάτων απαιτείται να ανανεώνουν τακτικά τις Μαύρες Λίστες που έχουν στην διάθεση τους με ενημερώσεις που παρέχονται από τον κατασκευαστή. Εναλλακτικά, κάποια από αυτά τα συστήματα, προκειμένου να απαλλάξουν τον χρήστη από τη διαδικασία των διαρκών ενημερώσεων, δεν διατηρούν τοπικά αντίγραφα των λιστών αλλά κατά το φιλτράρισμα κάθε εισερχόμενου μηνύματος συνδέονται με on-line βάσεις δεδομένων στις οποίες φυλάσσονται όλες οι απαραίτητες πληροφορίες.

Να αναφέρουμε τέλος ότι, εξ αιτίας της απλότητας κα της ταχύτητας η οποία χαρακτηρίζει τη διαδικασία της κατηγοριοποίησης ενός αγνώστου μηνύματος, η εν λόγω τεχνική συναντάται σε μια μεγάλη ποικιλία συστημάτων που φιλτράρουν spam μηνύματα τόσο στην πλευρά το εξυπηρετούμενου όσο και του εξυπηρετητή ηλεκτρονικού ταχυδρομείου, καθώς και σε γενικότερες κατηγορίες εφαρμογών προστασίας υπολογιστικών συστημάτων όπως firewalls, αντιβιοτικά, ή ακόμα και σε SMTP διακομιστές.[21]

[21] Wikipedia.org,
Alistair McDonald "SpamAssassing"
"Anti-spam Technology Overview", Network and Technology Working Group Telecommunication Engineering and Certification, May 2005

3.3.3 Συστήματα Φιλτραρίσματος βασισμένα σε Υπογραφές

Εξαιρετικό ενδιαφέρον παρουσιάζει η τεχνική των υπογραφών, καθώς έχει κοινά στοιχειά με την προσέγγιση της Μηχανικής Μάθησης αλλά βασίζεται κυρίως σε τεχνικές ανίχνευσης ιων. Ο βασικός μηχανισμός αναγνώρισης μη αιτηθείσας αλληλογραφίας ,επικεντρώνεται στην εξέταση του περιεχομένου των εισερχόμενων μηνυμάτων, μέσω μιας βάσης στατικών και τυχαίων υπογράφων που εντοπίζουν αποδοτικά διάφορα χαρακτηριστικά τμήματα spam μηνυμάτων.

Ένας από τους σημαντικότερους εκπροσώπους αυτής της κατηγορίας συστημάτων είναι το Vipul's Razor , ένα κατανεμημένο δίκτυο ανίχνευσης spam περιεχομένου, το οποίο διαθέτει προς τα συνεργαζόμενα με αυτό φίλτρα έναν κατάλογο με χαρακτηριστικά γνωστών spam μηνυμάτων, που ενημερώνεται τακτικά με τη συμβολή των χρηστών του. Η αρχιτεκτονική του συστήματος ακολουθεί το μοντέλο εξυπηρετούμενου-εξυπηρετητή. Αναλυτικότερα, η κατηγοριοποίηση ενός αγνώστου μηνύματος επιτυγχάνεται μέσω της εκτέλεσης μιας μικρής εφαρμογής(του εξυπηρετούμενου), η οποία αναλαμβάνει να συνδεθεί με κάποιον από τους διαθέσιμους στο δίκτυο εξυπηρετητές Razor και να τον τροφοδοτήσει σε ένα σύνολο από υπογραφές που εξήχθησαν από το περιεχόμενο του μηνύματος για περαιτέρω επεξεργασία. Ο εξυπηρετητής αποφαίνεται για το είδος του μηνύματος και ενημερώνει σχετικά τον εξυπηρετούμενο, ο οποίος επιστρέφει το αποτέλεσμα στο καλόν πρόγραμμα.

Η αρχή λειτουργιάς του συστήματος αναγνώρισης βασίζεται στην δημιουργία υπογραφών για κάθε τύπο spam περιεχομένου, υλοποιώντας ένα σύνολο από αλγορίθμους, καθένας από τους οποίους επιδιώκει την αντιμετώπιση ενός διαφορετικού προβλήματος της αναγνώρισης προτύπων. Ως παράδειγμα θα μπορούσαμε να αναφέρουμε τον αλγόριθμο παραγωγής ασαφών (fuzzy) υπογραφών (n-grams) σε ένα τμήμα κειμένου , όντας ανθεκτικός σε μικρές παραλλαγές ανάμεσα στις συγκρινόμενες ακολουθίες. Ένα άλλο παράδειγμα είναι ο αλγόριθμος Εφήμερων υπογραφών, ο οποίος δημιουργεί βραχύβιες υπογραφές από τυχαία

επιλεγμένα τμήματα ενός spam μηνύματος. Με τον τρόπο αυτό, το σχήμα κατακερματισμού που υλοποιείται καθίσταται «κινούμενος στόχος » για τους spammers, οι οποίοι δεν είναι πλέον σε θέση να το εκμεταλλευτούν, αγνοώντας το τμήμα του μηνύματος που πρόκειται τελικά να χρησιμοποιηθεί.

Ανάμεσα στα υπόλοιπα χαρακτηριστικά του συστήματος συγκαταλέγονται:

- Η αποκωδικοποίηση μηνυμάτων που έχουν εσκεμμένα αποσταλεί με κωδικοποίηση Base64 ή Quoted-Printable, καθώς και η αφαίρεση των ετικετών html προς της αναγνώρισης τους.

- Η ταξινόμηση των spam μηνυμάτων που έχουν αναφερθεί σ' αυτό σε κλάσεις, ανάλογα με το περιεχόμενο τους, προκειμένου να διευκολύνει τη διαδικασία της αναγνώρισης, αλλά και ανάλογα με το είδος της MIME επικεφαλίδας του κάθε συνημμένου αρχείου που συνιστάται, για τον αποτελεσματικότερο εντοπισμό ιων.

- Η δυνατότητα αποστολής από τους χρήστες spam μηνυμάτων, που αναγνωρίσθηκαν λανθασμένα ως θεμιτά, επιτρέποντας στο σύστημα να ενημερώνει τη βάση των υπογραφών του αρκετές φορές εντός του εικοσιτετραώρου.

- Η υλοποίηση ενός υποσυστήματος αξιολόγησης της αλήθειας(Truth Evaluation System-TeS) των αναφορών εσφαλμένης ταξινόμησης spam μηνυμάτων που αποστέλλουν οι χρήστες, το οποίο αναθέτει σε κάθε παραγόμενη υπογραφή ένα επίπεδο εμπιστοσύνης που αυξάνεται ανάλογα με το χρόνο ζωής της και με την φήμη που έχει σχηματίσει ο χρήστης- αποστολέας της αναφοράς σφάλματος, σχετικά με την αξιοπιστία των αναφορών του. Το υποσύστημα αυτό αποσκοπεί στην εξάλειψη του προβλήματος της εσφαλμένης ταξινόμησης θεμιτών μηνυμάτων ως spam.

- Η δυνατότητα ανάκλασης ενός μηνύματος από τους χρήστες του συστήματος, εφόσον πιστεύεται ότι αποτελεί θεμιτό μήνυμα, διαδικασία η οποία έχει ως αποτέλεσμα τη διαγραφή όλων των υπογραφών που δημιουργήθηκαν από αυτό.

Ολοκληρώνοντας τη σύντομη αναφορά μας στην πολλά υποσχόμενη αυτή προσέγγιση φιλτραρίσματος, θα πρέπει να τονίσουμε για μια ακόμη φορά τον ουσιαστικό ρόλο που επιτελεί η ανταπόκριση της κοινότητας των χρηστών της για τη διατήρηση μιας βάσης υπογραφών που να ενημερώνεται σε συνεχή βάση. Πραγματική ώθηση στην αποτελεσματικότητα του Razor μπορεί αν εγγυηθεί η συνεργασία του με φορείς που συντηρούν διευθύνσεις- παγίδες spam μηνυμάτων, καθώς μέσω αυτής δύναται να εξασφαλιστεί η άμεση ανανέωση της βάσης του με υπογραφές, προερχόμενες από μηνύματα που μόλις κυκλοφόρησαν στο διαδίκτυο, πριν προλάβουν να παραδοθούν στα γραμματοκιβώτια των χρηστών του.[22]

3.3.4 Συστήματα Φιλτραρίσματος βασισμένα σε Αλγόριθμους Μηχανικής Μάθησης

Από τις πρώτες υλοποιήσεις συστημάτων κατηγοριοποίησης και φιλτραρίσματος μηνυμάτων ηλεκτρονικού ταχυδρομείου στην περιοχή αυτή αποτελεί το πρόγραμμα μάθησης RIPPER[Cohen 1995~1196], με κύριο αντικείμενο του την αυτόματη εξαγωγή κανόνων με λέξεις- κλειδιά από το σώμα ή από το θέμα ενός μηνύματος. Εφόσον όλες οι λέξεις του σώματος ενός κανόνα εντοπιστούν στο υπό εξέταση μήνυμα, τότε η απόφαση κατηγοριοποίησης του συμπεράσματος τίθεται σε ισχύ.

Παρόμοια δραστηριότητα ανέπτυξαν και οι Nottelmann και Fuhr[2001], με την υλοποίηση της μηχανής συμπερασμού HySpirit. Η προσέγγιση που διερεύνησαν συνίσταται στην εκμάθηση πιθανοτικών κανόνων Datalog , στην αυτόματη δηλαδή εξαγωγή προτάσεων Horn κατηγορηματικής λογικής. Παράλληλα η μηχανή υιοθετεί ένα σύστημα αποτίμησης της ισχύος

[22] Wikipedia.org,
Alistair McDonald "SpamAssassing"

των κανόνων, με την ανάθεση βαρών τόσο στο σώμα όσο και στο συμπέρασμα τους, που υπολογίζονται κατά τη διαδικασία της εκπαίδευσης. Το αποτέλεσμα των δυο προαναφερθέντων εφαρμογών, αλλά και των υπολοίπων ερευνητικών προσπαθειών που εντάσσονται στο χώρο του Επαγωγικού Λογικού Προγραμματισμού(Inductive Logic Programming- ILP), συγκεντρώνουν το ενδιαφέρον της επιστημονικής κοινότητας καθώς υπόσχονται να ενισχύσουν την αξιοπιστία και την ευχρηστία των συστημάτων φιλτραρίσματος που βασίζονται σε κανόνες, επιτρέποντας τη δημιουργία προτύπων που να προσανατολίζονται στις ιδιαιτερότητες του γραμματοκιβωτίου του χρήστη, χωρίς να απαιτούν την παρέμβαση του τελευταίου στην όλη διαδικασία.

Άλλες υλοποιήσεις περιλαμβάνουν τη χρήση Bayesian ταξινομητών που δρουν ως αυτόνομα φίλτρα, είτε ως αθρώματα υπαρχόντων εφαρμογών διαχείρισης ηλεκτρονικού ταχυδρομείου (π.χ. το φίλτρο iFile [Rennie 2000] που είναι γραμμένο για τον EXMH mail client), μάθησης βασισμένης σε στιγμιότυπα (π.χ. το σύστημα κατηγοριοποίησης μηνυμάτων του Mock [2001] για το Microsoft Outlook), νευρωνικών δικτύων και perceptrons (π.χ. Re: Agent,[Boone 1998]), κ.α.

Για το τέλος της ενότητας αυτής επιλέχτηκε η αναλυτική παρουσίαση ενός ολοκληρωμένου συστήματος φιλτραρίσματος spam μηνυμάτων, το οποίο εμφανίζει πολλά κοινά στοιχεία με το SpamSentinel για το οποίο θα αναφερθούμε αργότερα. Πρόκειται για το Spam Buster, προϊόν του τμήματος Πληροφορικής της Ανώτατης Εθνικής Σχολής Τηλεπικοινωνιών (E.N.S.T) του Παρισιού, το οποίο αποφαίνεται για την κλάση των εισερχόμενων μηνυμάτων ενός χρήστη (spam ή θεμιτά), εξετάζοντας το περιεχόμενο του θέματος και του κυρίου σώματος τους. Επιπλέον, το σύστημα εξετάζει ορισμένα χαρακτηριστικά που σχετίζονται με τις διευθύνσεις του αποστολέα και του παραλήπτη, και με το μήκος της επικεφαλίδας.

Πυρήνας του συστήματος αποτελεί η αρχιτεκτονική Μηχανικής Μάθησης SNoW (Sparse Network of Winnows), που υποστηρίζει την επίλυση προβλημάτων κατηγοριοποίησης πολλών κλάσεων και παρουσιάζει ικανοποιητική απόδοση κατά το χειρισμό χώρων αρκετά μεγάλης διαστασιμότητας, η οποία δεν είναι πάντα γνωστή εκ των προτέρων. Η λειτουργία της

βασίζεται στην εκμάθηση ενός αραιού δικτύου γραμμικών μοντέλων, στο οποίο οι έννοιες-στόχοι αναπαριστούνται σαν γραμμικές συναρτήσεις πάνω σε ένα κοινό χώρο χαρακτηριστικών. Πιο συγκεκριμένα, η αρχιτεκτονική του δικτύου χωρίζεται σε δυο επίπεδα.

Το πρώτο εξ αυτών, το επίπεδο εισόδου, αποτελείται από κόμβους, καθένας εκ των οποίων αντιστοιχεί σε ένα χαρακτηριστικό του χώρου. Οι κομβόι του δεύτερου επιπέδου (επίπεδο εξόδου) αντιπροσωπεύουν τις κλάσεις του προβλήματος μάθησης. Η διαδικασία της εκπαίδευσης συνίσταται στην εκμάθηση των βαρών των συνδέσμων μεταξύ των κόμβων των δυο επιπέδων. Το δίκτυο χαρακτηρίζεται ως αραιό υπό την έννοια ότι κάθε κόμβος του επιπέδου εξόδου δε συνδέονται με όλους τους κόμβους εισόδου. Ανάμεσα στους ταξινομητές που υλοποιούνται στο SNoW περιλαμβάνονται: οι Naïve Bayes, νευρωνικά δίκτυα (Perceptron) και Winnow. Εξέχουσα θέση ανάμεσα τους καταλαμβάνει ο αλγόριθμος Winnow, ο οποίος εκτελείται τακτικά σε κάθε κόμβο εξόδου, με σκοπό την εκμάθηση των βαρών των συνδέσμων του τελευταίου με κάθε κόμβο εισόδου. Το σημαντικότερο χαρακτηριστικό του εντοπίζεται στο γεγονός ότι το πλήθος των παραδειγμάτων που απαιτούνται για την εκμάθηση της συνάρτησης- στόχου αυξάνει γραμμικά με τον αριθμό των σχετικών χαρακτηριστικών και λογαριθμικά με το συνολικό αριθμό των χαρακτηριστικών. Αποδεικνύεται δε ιδιαίτερα αποδοτικός για την εκμάθηση οποιασδήποτε γραμμικής συνάρτησης κατωφλίου, ακόμα και σε χώρους μεγάλης διαστασιμότητας, παρουσιάζοντας ανοχή στην ύπαρξη θορύβου στις τιμές των χαρακτηριστικών των στιγμιότυπων εκπαίδευσης.

Τέλος το Spam Buster εκτελείται στον εξυπηρετητή ηλεκτρονικού ταχυδρομείου συστημάτων UNIX, ενώ η κλήση του επιτυγχάνεται κατά τη λήψη ενός αγνώστου μηνύματος, μέσω του διαχειριστή μηνυμάτων procmail. Εφόσον το μήνυμα βρεθεί από το διακομιστή υπηρεσιών του Spam Buster ότι ανήκει στην κλάση spam, χαρακτηρίζεται κατάλληλα και εν συνέχεια αποθηκεύεται στο γραμματοκιβώτιο του χρήστη.

3.3.5 Συνδυασμοί των Παραπάνω Τεχνικών

Στις ενότητες που προηγήθηκαν αναφέραμε ένα σύνολο από τις σημαντικότερες τεχνικές που υιοθετούνται στο χώρο του φιλτραρίσματος μη αιτηθείσας αλληλογραφίας, καθώς και τις πιο χαρακτηριστικές προσπάθειες αξιοποίησής τους σε ολοκληρωμένα συστήματα που εκμεταλλεύονται τις δυνατότητές τους. Έχοντας ωστόσο ως απώτερο στόχο τη μμεγιστοποίηση της ακρίβειας αναγνώρισης των spam μηνυμάτων με την παράλληλη ελαχιστοποίηση της πιθανότητας εσφαλμένης ταξινόμησης των θεμιτών, πολύ σύντομα το ενδιαφέρον της ερευνητικής κοινότητας αλλά και της βιομηχανίας των ανωτέρω συστημάτων στράφηκε στην αναζήτηση μιας προσέγγισης που θα συγκέντρωνε τα επιθυμητά αυτά χαρακτηριστικά, όντας ταυτόχρονα απαλλαγμένη από τα μειονεκτήματα των υπαρχουσών μεθοδολογιών. Η λύση δόθηκε μέσω του συνδυασμού δύο ή περισσότερων εξ αυτών, ανάλογα με την περίπτωση, επιτυγχάνοντας την αλληλοσυμπλήρωση τους, και κατ' επέκταση τη συνολική αύξηση της αποτελεσματικότητας τους.

Η πρώτη κατηγορία φίλτρων που στράφηκε προς την κατεύθυνση αυτή, προέκυψε από τον συνδυασμό των πιο απλών προσεγγίσεων του χώρου, της αναγνώρισης δηλαδή spam μμηνυμάτων μέσω κανόνων και μέσω της χρησιμοποίησης Μαύρων Λιστών. Τα συγκεκριμένα συστήματα εκτελούνται ως αυτόνομες εφαρμογές στην πλευρά είτε του εξυπηρετούμενου είτε και του εξυπηρετητή ηλεκτρονικού ταχυδρομείου, ενώ δεν είναι σπάνιες και οι περιπτώσεις της πλήρους ενσωμάτωσης τους στα συστήματα αυτά, όπως για παράδειγμα συμβαίνει με τη δημοφιλή εφαρμογή διαχείρισης ,μηνυμάτων Microsoft Outlook. Πιο εκλεπτυσμένες υλοποιήσεις, που εκτελούνται στο περιβάλλον εργασίας του χρήστη σε λειτουργικό σύστημα Microsoft Windows και υποστηρίζουν την αυτόματη ενημέρωση των μηχανισμών αναγνώρισης spam, κατ' αντιστοιχία με τα γνωστά πακέτα προστασίας από ιούς, είναι τα SpamKiller και JunkSpy τα οποία παρεμβάλλονται μεταξύ των προγραμμάτων διαχείρισης και των εξυπηρετητών ηλεκτρονικού ταχυδρομείου σαν proxy servers, με σκοπό την αναχαίτιση και το φιλτράρισμα της εισερχομένης αλληλογραφίας.

Στα ανωτέρω συστήματα εντάσσονται και τα SpamBouncer και JunkFilter . Πρόκειται για σύνολα οδηγιών – συνταγών όπως έχει επικρατήσει να αποκαλούνται – του διαχειριστή αλληλογραφίας procmail, τα οποία διακρίνονται για την μεγάλη ποικιλία των ευριστικών κανόνων που ενσωματώνουν. Οι κανόνες αυτοί ανέρχονται σε εκατοντάδες και επιδιώκουν την αντιπροσωπευτική μμοντελοποίηση όλων των υποκατηγοριών των spam μηνυμάτων, βάσει της δομής των επικεφαλίδων και του περιεχομένου τους. Παράλληλα, ως μέτρο επαύξησης της αποτελεσματικότητας τους χρησιμοποιούνται στατικές λίστες διευθύνσεων spammers και υπηρεσιών διακίνησης μηνυμάτων αντίστοιχου περιεχομένου. Ωστόσο, η ανάγκη ενημέρωσης και των δύο μηχανισμών από το χρήστη και η εξοικείωση του τελευταίου στη λειτουργία του procmail, φέρουν σημαντικές επιπτώσεις στην ευχρηστία τους.

Μια πιο εξελιγμένη προσέγγιση χρήσης των παραπάνω μεθόδων υλοποιείται από το σύστημα φιλτραρίσματος Brightmail, το οποίο απευθύνεται σε οργανισμούς παροχής υπηρεσιών ηλεκτρονικού ταχυδρομείου, ISPs, εταιρικά δίκτυα, κ.α. Ο μηχανισμός ταξινόμησης, ο οποίος εκτελείται στον εκάστοτε εξυπηρετητή SMTP επιχειρεί την αποτελεσματική αναγνώριση των spam, στηριζόμενος σε ένα σύνολο ευριστικών κανόνων που ανανεώνονται συνεχώς από εξειδικευμένο προσωπικό της κατασκευάστριας εταιρείας. Η όλη διαδικασία διευκολύνεται από τη λειτουργιά ενός μεγάλου αριθμού διευθύνσεων «παγίδων» που έχουν τοποθετηθεί σε στρατηγικά σημεία του διαδικτύου, μέσω των οποίων τα ληφθέντα μηνύματα αξιολογούνται, προκειμένου να αναγνωριστούν εκείνα τα spam που δεν καλύπτονται από τους υπάρχοντες κανόνες και να επιτραπεί στην συνέχεια η περαιτέρω επεξεργασία τους. Μέσω της παραπάνω οργάνωσης, ο εκάστοτε πράκτορας BrightMail ενημερώνει τη βάση του με νέους κανόνες φιλτραρίσματος, τη στιγμή της δημιουργίας τους στους κεντρικούς εξυπηρετητές του συστήματος. Επίσης, υποστηρίζεται η απομόνωση των spam σε μια συγκεκριμένη περιοχή, αποφεύγοντας τη μαζική αποστολή τους στους λογαριασμούς των χρηστών του εξυπηρετητή ηλεκτρονικού ταχυδρομείου τον οποίο προστατεύει, δίνοντας παράλληλα τη δυνατότητα στους χρήστες να εξετάζουν το περιεχόμενο των απορριφθέντων μηνυμάτων, για την αποφυγή σφαλμάτων του τύπου L->S.

Παρόμοια φιλοσοφία ακλουθείτε και από το PerIMX, το οποίο δεν αναλαμβάνει απλώς το φιλτράρισμα ανεπιθύμητων μηνυμάτων, αλλά αποτελεί μα ολοκληρωμένη σουίτα προστασίας του διακομιστή SMTP οργανισμών παροχής υπηρεσιών ηλεκτρονικού ταχυδρομείου από μη αιτηθείσα ή επιβλαβή αλληλογραφία. Η σουίτα αυτή ενσωματώνει μηχανισμό ανίχνευσης ιών και βοήθα τους διαχειριστές να οργανώσουν αποτελεσματικά την πολιτική ασφάλειας των συστημάτων τους.

Αναφορικά με τις μεθόδους αναγνώρισης των spam που υλοποιεί, τα εισερχόμενα μηνύματα εξετάζονται βάση «Λευκών» και «Μαύρων» Λιστών, ευριστικών κανόνων προς αναζήτηση γνωστών προτύπων στο σώμα ή στη δομή των επικεφαλίδων τους, καθώς και βάση υπογράφων, προερχομένων από spam μηνύματα που συναντώνται συχνά (όπως μηνύματα-φάρσες ή μηνύματα-αλυσίδες που αποστέλλονται από τον ένα χρήστη στον άλλο, χωρίς το περιεχόμενο τους να τροποποιηθεί στο ενδιάμεσο).Το αποτέλεσμα των προαναφερθέντων ελέγχων αξιολογείται ανάλογα με το βαθμό εμπιστοσύνης που επιστρέφεται μαζί με κάθε απόφαση, και εφόσον κάποιο μήνυμα θεωρηθεί spam, το σύστημα μπορεί να προβεί στην απόρριψη, στην επιστροφή του στον αποστολέα ή στην αποθήκευση του σε έναν κατάλογο «καραντίνας», προκειμένου να αποφύγει την απώλεια θεμιτών που ταξινομήθηκαν ως spam.

Ολοκληρώνοντας αυτή την ενότητα με την παρουσίαση της πλέον υποσχόμενης προσέγγισης που υλοποιείται από το σύστημα SpaAssassin. Πρόκειται για ένα σύστημα φιλτραρίσματος spam μηνυμάτων που εκτελείται στον εξυπηρετητή SMTP και ενσωματώνει όλες τις προαναφερθείσης τεχνικές, με σκοπό τη μεγιστοποίηση της απόδοσης του. Αναλυτικότερα, υποστηρίζει:

- Μηχανισμούς για την ανάλυση των επικεφαλίδων των μηνυμάτων, προς εντοπισμό παραποιημένων πεδίων ή προσπαθειών κάλυψης της πραγματικής ταυτότητας των αποστολέων, που συναντώνται συχνά σε spam μηνύματα.

- Μηχανισμούς για την ανάλυση του περιεχομένου των μηνυμάτων, με την βοήθεια ευριστικών κανόνων και της χρήσης γενετικών αλγορίθμων μάθησης.

- Μαύρες λίστες, που παρέχονται στο σύστημα τόσο στατικά, υπό μορφή αρχείων, όσο και δυναμικά, μέσω της χρήσης on-line βάσεων δεδομένων, όπως mail-abuse.org και η ordb.org.

- Συνεργασία με το δίκτυο Vipul's Razor, επιτρέποντας την απευθείας προώθηση νέων spam μηνυμάτων προς αυτό.

Για την αποδοτικότερη αξιοποίηση όλων των προαναφερθέντων τεχνικών, το σύστημα αναθέτει ένα βαθμό εμπιστοσύνης σε κάθε ένα από τους επιμέρους ελέγχους. Ο τελευταίος μπορεί να είναι θετικός ή αρνητικός ανάλογα με το είδος των μηνυμάτων που συνηθέστερα επαληθεύει τον έλεγχο (spam ή θεμιτά αντίστοιχα). Το άθροισμα των βαθμών όλων των επιτυχόντων ελέγχων καθορίζει εν θέλει την απόφαση του συστήματος. Εφόσον ένα μήνυμα κριθεί ως spam, χαρακτηρίζεται ανάλογα, ενώ σε κάθε περίπτωση, στο τέλος του επισυνάπτεται μια σύντομη αιτιολόγηση της κατηγοριοποίησης, επιτρέποντας έτσι την παραμετροποίηση της μονάδας λήψης αποφάσεων του συστήματος από τον χρήστη, με την τροποποίηση των βαθμών εμπιστοσύνης.

Στα θετικά του χαρακτηριστικά συγκαταλέγεται επίσης η επεκτασιμότητα του, καθώς επιτρέπει την συγγραφή νέων κανόνων, την υλοποίηση νέων ελέγχων ή μονάδων, και την αναθεώρηση τους συστήματος βαθμολόγησης από τον χρήστη. Τέλος αποδεικνύεται ιδιαίτερα ευέλικτο εξ αιτίας της δυνατότητας ενσωμάτωσης που προσφέρει η αρχιτεκτονική του σε ένα ευρύτερο φάσμα εφαρμογών ηλεκτρονικού ταχυδρομείου, όπως το procmail, το Mail::Audit, το qmail, το Postfix κ.α, καθιστώντας το την πλέον ολοκληρωμένη πρόταση στο χώρο της αναγνώρισης spam αλληλογραφίας.[23]

[23] Wikipedia.org,
OECD Anti-Spam Toolkit of Recommended Policies and Measures

3.3.6 Υπηρεσίες Παροχής DEAs

Από τις εξωτικότερες προσεγγίσεις αντιμετώπισης του φαινομένου των spam μηνυμάτων αποτελεί η χρήση *Πλασματικών Ηλεκτρονικών Διευθύνσεων(Dispsable E-mail Address-DEAs)*. Η ιδιαιτερότητα της έγκειται στο ότι δεν επιδιώκει την αναγνώριση και κατ' επέκταση το φιλτράρισμα των spam από το γραμματοκιβώτιο του χρήστη, αλλά αντίθετα αποσκοπεί στον έμμεσο περιορισμό τους, δίνοντας την ευκαιρία στον τελευταίο να ελέγξει τον τρόπο με τον οποίο χρησιμοποιείται η ηλεκτρονική του διεύθυνση από όσους τη γνωρίζουν.

Αναλυτικότερα η αρχή λειτουργίας της εν λόγω τεχνικής βασίζεται στη δημιουργία ξεχωριστών λογαριασμών ενός χρήστη για διαφορετικούς τύπους e-mail (π.χ. έναν για τις προσωπικές του επαφές τον οποίο φροντίζει να μη δημοσιεύσει στο δίκτυο, έναν για τις επαγγελματικές του επαφές, έναν για την επικοινωνία του on-line καταστήματα και άλλες δικτυακές υπηρεσίες, λίστες ηλεκτρονικού ταχυδρομείου, κτλ.). Το πρόβλημα της συγκεκριμένης μεθόδου εντοπίζεται στην ανάγκη ελέγχου και διαχείρισης πολλαπλών λογαριασμών, το οποίο επιτείνεται όταν κάποιος από τους πλέον ευάλωτους αρχίσει να δέχεται έναν μεγάλο αριθμό spam μηνυμάτων οδηγώντας αναπόφευκτα στην κατάργηση του.

Τη λύση αυτού του προβλήματος υπόσχεται η χρήση υπηρεσιών παροχής πλασματικών διευθύνσεων. Οι υπηρεσίες αυτές προσφέρουν ένα μεγάλο αριθμό ηλεκτρονικών διευθύνσεων σε κάθε χρήστη τους, οι οποίες δεν αντιστοιχούν σε ισάριθμους λογαριασμούς e-mail , αλλά χρησιμοποιούνται μόνο για την ανακατεύθυνση των μηνυμάτων που απευθύνονται σε αυτές στην πραγματική διεύθυνση των χρηστών τους. Μέσω του εν λόγω μηχανισμού, κάθε φορά που κάποιος επιθυμεί να επικοινωνήσει με έναν φορέα που δεν εμπιστεύεται, δεν του αποκαλύπτει την πραγματική του διεύθυνση, αλλά χρησιμοποιεί μια πλασματική. Κάθε μήνυμα που προέρχεται από μια τέτοια διεύθυνση, εσωκλείει στην επικεφαλίδα του ένα επιπλέον πεδίο που πληροφορεί τον παραλήπτη του διαμέσου ποιας

πλασματικής διεύθυνσης έφθασε σε αυτόν. Ο χρήστης έχει έτσι την ευκαιρία να προχωρήσει σε προσωρινό η μόνιμο τερματισμό της ισχύος της πλασματικής διεύθυνσης, εφόσον αρχίζει να λαμβάνει μέσω αυτής μη αιτηθείσα αλληλογραφία. Επιπλέον, τα περιεχόμενα του συμπληρωματικού πεδίου πολλές φορές επαναλαμβάνονται και στο σώμα ή στο θέμα του μηνύματος εφόσον ο παροχές της υπηρεσίας το υποστηρίζει. Το πεδίο αυτό αποτελεί σε ορισμένες περιπτώσεις τη μοναδική πηγή πληροφόρησης αναφορικά με την προέλευση των Spam μηνυμάτων που λαμβάνονται μέσω της σχετικής διευθύνσεις. Με αυτό τον τρόπο μπορεί κανείς να ανακαλύψει τον φορέα από τον οποίο η ηλεκτρονική του διεύθυνση διέρρευσε σε τρίτους.

Η τεχνική αυτή ωστόσο δε στερείται μειονεκτημάτων. Όπως αναφέραμε και στην αρχή της ενότητας, η καταφυγή σε DEAs δεν απαλλάσσει το χρήστη τους από τη λήψη ανεπιθύμητης αλληλογραφίας, αλλά βοηθά στον περιορισμό της. Αρκεί ένα μόνο λάθος του χρήστη, που μεταφράζεται σε αποκάλυψη της πραγματικής του διεύθυνσης, για την κατάρρευση της μεθόδου. Είναι μάλιστα πιθανό το «λάθος» στο οποίο αναφερόμαστε να έχει γίνει πριν ακόμα ο χρήστης στραφεί στην χρήση μιας υπηρεσίας DEA, με αποτέλεσμα η πραγματική του διεύθυνση, την οποία για πολλούς λόγους δεν μπορεί να καταργήσει, να διαδίδεται στην ολοένα αυξανόμενη κοινότητα των spammers με ταχύτατους ρυθμούς.

Επίσης, η εξάρτηση του χρήστη από μια δικτυακή υπηρεσία δύναται να αποδειχθεί προβληματική, καθώς τίθεται τόσο θέματα εμπιστοσύνης αναφορικά με τον τρόπο με τον οποίο θα χρησιμοποιηθεί η πραγματική του διεύθυνση, αλλά και ασφάλειας. Ο παροχέας της υπηρεσίας θα πρέπει να μπορεί να πείθει για την ικανότητα του να προστατεύει με κάθε τρόπο το απόρρητο των προσωπικών στοιχείων των χρηστών του από κάποια επίθεση τρίτων στο σύστημα του, ή από την κακόβουλη χρησιμοποίηση τους από τον ίδιο ή από συνεργαζόμενους με αυτόν φορείς. Στην χειρότερη περίπτωση, δεν μπορεί να αποκλεισθεί το ενδεχόμενο λειτουργίας μιας τέτοιας υπηρεσίας για ένα σύντομο χρονικό διάστημα, με απώτερο στόχο τη συλλογή έγκυρων ηλεκτρονικών διευθύνσεων για την προώθηση

διαφημιστικού υλικού. Τέλος αρκετές από τις υπό εξέταση υπηρεσίες απαιτούν την καταβολή συνδρομής, το κόστος της οποίας αυξάνεται προκειμένου να άρουν περιορισμούς διαφόρων τύπων, που εντοπίζονται στο πλήθος των DEAs που μπορούν να χρησιμοποιούνται ταυτόχρονα, στη διάρκεια ζωής τους, στο μέγεθος των διακινούμενων μηνυμάτων, κ.α.

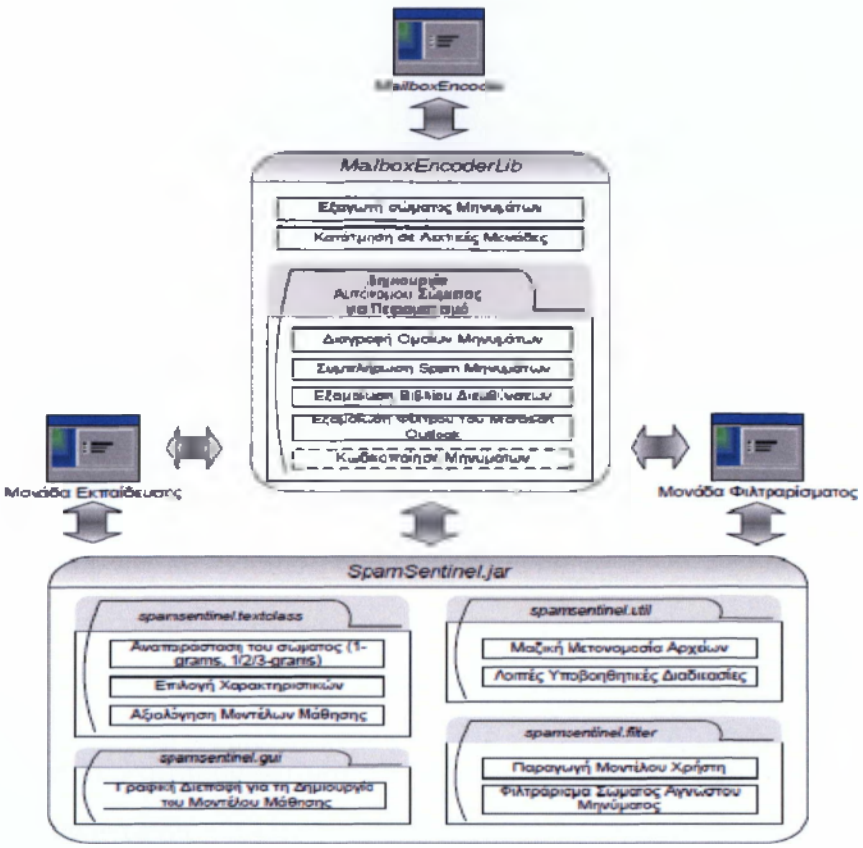
Χαρακτηριστικοί εκπρόσωποι των συστημάτων αυτών είναι οι : Spamex, Emailias, SneakeMail, κ.α.[24]

3.3.7 SpamSentinel

Το SpamSentinel αποτελεί ένα ολοκληρωμένο σύστημα φιλτραρίσματος μη αιτηθείσας εμπορικής ηλεκτρονικής αλληλογραφίας. Το σύστημα, το οποίο εκτελείται στον εξυπηρετητή ηλεκτρονικού ταχυδρομείου, αναλαμβάνει να αναγνωρίσει και να χαρακτηρίσει κατάλληλα τα εισερχόμενα μηνύματα των χρηστών του ως θεμιτά ή Spam , στηριζόμενος στο προσωπικό μοντέλο που έχει δημιουργήσει για κάθε έναν από αυτούς, κατά τη διαδικασία της εκπαίδευσης του επί του ηλεκτρονικού χρηματοκιβωτίου τους.

Η αρχιτεκτονική του SpamSentinel χωρίζεται σε δυο βασικά υποσυστήματα. Το πρώτο εξ αυτών περιλαμβάνει δυο βιβλιοθήκες χαμηλού επιπέδου, στις οποίες βρίσκονται συγκεντρωμένες οι θεμελιώδεις λειτουργίες του συστήματος , καθώς και βοηθητικές διαδικασίες, οι οποίες προσπελαύνονται από τα συστατικά του δεύτερου υποσυστήματος, από έναν αριθμό δηλαδή αυτόνομων μονάδων, που επιτρέπουν την άμεση αλληλεπίδραση με το χρήστη. Στο σημείο αυτό ακολουθεί μια σύντομη παρουσίαση της δομής και της λειτουργίας των δυο παραπάνω στρωμάτων της εφαρμογής.

[24] Wikipedia.org



Εικόνα 33 Η αρχιτεκτονική του συστήματος SpamSentinel. Με διακεκομμένες γραμμές αναπαριστάται τα (υπό)στάδια εκείνα που είναι προαιρετικά, ενώ η ύπαρξη βελών υποδηλώνει αλληλεπίδραση των διαφόρων μονάδων με τις δυο βιβλιοθήκες

3.3.7.α Μονάδες του SpamSentinel

Το SpamSentinel αποτελείται από δυο κύριες μονάδες και από ένα εργαλείο ειδικού σκοπού, τα οποία παρουσιάζονται παρακάτω:

- **Μονάδα Εκπαίδευσης:** Η μονάδα αυτή είναι επιφορτισμένη με το έργο της εκπαίδευσης του αλγορίθμου μάθησης που αξιοποιεί το σύστημα, πάνω στα χαρακτηριστικά των μηνυμάτων, θεμιτών και μη, ενός συγκεκριμένου χρήστη. Εν ολίγοις η διαδικασία που ακολουθείται διεξάγετε σε δυο φάσεις.

Στην πρώτη φάση επιχειρείται η παραγωγή του σώματος των μηνυμάτων με το οποίο θα πραγματοποιηθεί η εκπαίδευση του αλγορίθμου. Ο χρήστης καλείται να τροφοδοτήσει το

πρόγραμμα με τους ηλεκτρονικούς καταλόγους (mail folders) των θεμιτών και των spam μηνυμάτων που έχει λάβει, όπως αυτοί διατηρούνται από το πρόγραμμα διαχείρισης ταχυδρομείου που χρησιμοποιήθηκε. Στην συνέχεια, το σώμα κάθε μηνύματος αποθηκεύεται σε ξεχωριστό αρχείο, υπό μορφή κειμένου. Τυχόντα συννημένα αρχεία των μηνυμάτων δεν συμμετέχουν στη διαδικασία. Η φάση αυτή ολοκληρώνεται με την διαγραφή των πολλαπλών αντιγράφων.

Ένα από τα σημαντικότερα προβλήματα που έπρεπε το πρόγραμμα να αντιμετώπιση ήταν η δημιουργία σωμάτων εκπαίδευσης τα οποία στερούνταν παντελώς ή υστερούσαν ως προς τον αριθμό παραδειγμάτων της κλάσης spam, καθώς η πλειοψηφία των χρηστών ηλεκτρονικού ταχυδρομείου διαγράφει αυτά τα μηνύματα. Η λύση δόθηκε με την παροχή μιας συλλογής 2000 περίπου τέτοιων μηνυμάτων, μέρος των οποίων χρησιμοποιείται από το πρόγραμμα στην περίπτωση που ο χρήστης δεν έχει κρατήσει τα Spam μηνύματα που έχει λάβει.

Στην δεύτερη φάση, λαμβάνει χώρα η εκπαίδευση του ταξινομητή, από το σώμα μηνυμάτων που πρόεκυψε. Τελικό προϊόν της όλης διαδικασίας αποτελεί η παραγωγή ενός μοντέλου που αντιπροσωπεύει τη γνώση που αποκόμισε ο αλγόριθμος, όσον αφορά στα χαρακτηριστικά που διακρίνουν τα μηνύματα που λαμβάνει συνήθως ο συγκεκριμένος χρήστης.

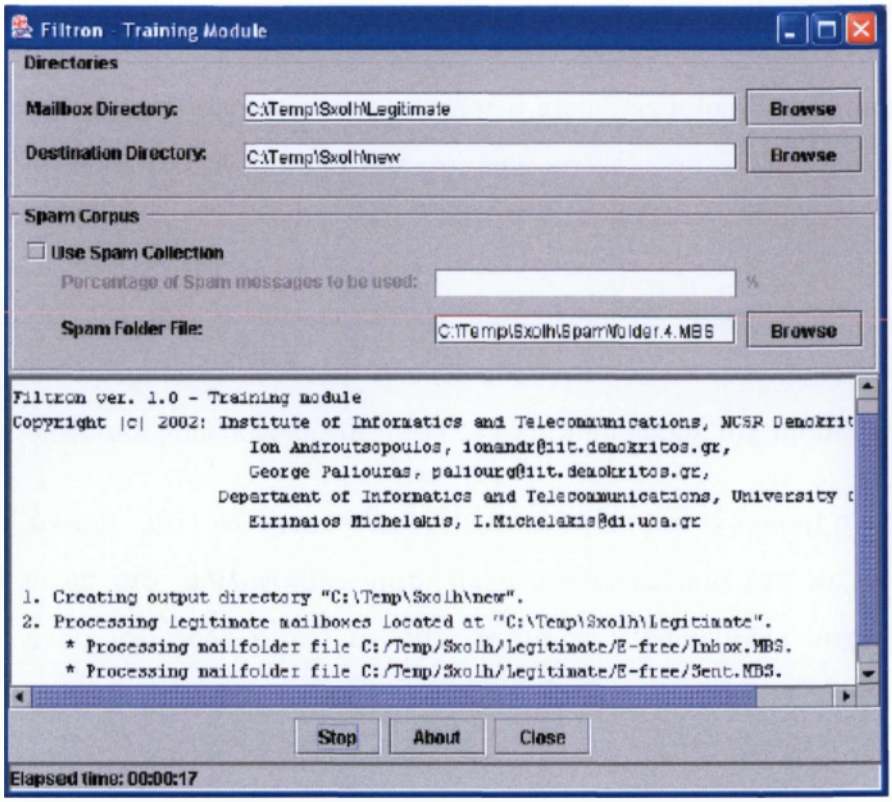
Η συγκεκριμένη μονάδα κάνει χρήση και των βιβλιοθηκών του συστήματος. Είναι δε γραμμένη σε TCL, καθιστώντας τη μεταφέρσιμη στο περιβάλλον προτίμησης του χρήστη. Εξ αιτίας του μεγάλου χρονικού διαστήματος που απαιτείται για την εκτέλεση του προγράμματος, το πρόγραμμα εξοπλίστηκε με ένα έξυπνο σύστημα ανάκαμψης , προκειμένου να διασφαλιστεί η συνέχιση της εκτέλεσης του από κάποιον απροσδόκητο τερματισμό του, αφού έχει ήδη ολοκληρώσει αρκετές ώρες συνεχούς λειτουργίας. Τέλος, η εκπαίδευση μπορεί να πραγματοποιηθεί τόσο μέσα από μια εύχρηστη και λειτουργική γραφική διεπαφή, όσο και από το περιβάλλον της κονσόλας, για τα συστήματα εκείνα που δεν παρέχουν υποστήριξη για παραθυρικές εφαρμογές.

- **Μονάδα Φιλτραρίσματος:** Η βασική μονάδα της εφαρμογής είναι αυτή του φιλτραρίσματος των εισερχόμενων μηνυμάτων ενός χρήστη, η οποία αποφαίνεται για την

κλάση στην οποία ανήκουν (legitimate η spam). Η κατηγοριοποίηση βασίζεται αποκλειστικά στις πληροφορίες από το μοντέλο του χρήστη, που δημιουργήθηκε κατά τη διαδικασία της εκπαίδευσης.

Θα πρέπει να σημειωθεί ότι το πρόγραμμα, γραμμένο και αυτό σε TCL , εκτελείται τοπικά, στον εξυπηρετητή ηλεκτρονικού ταχυδρομείου και μόνο σε συστήματα που υλοποιούν το πρότυπο μεταβίβασης και προώθησης ηλεκτρονικής αλληλογραφίας του UNIX .

Αναλυτικότερα, ο τρόπος λειτουργίας του προγράμματος έχει ως εξής : Αρχικά, το εισερχόμενο μήνυμα αναλύεται στα συστατικά του μέρη (στην επικεφαλίδα, στο σώμα και στα λοιπά αρχεία που τυχόν επισυναφθεί σε αυτό), από τα οποία κρατείται μόνο το σώμα του. Ακολουθεί η αφαίρεση των ετικετών html που ενδέχεται να υπάρχουν, καθώς και η κατάτμηση του σε λεκτικές μονάδες. Το τελικό προϊόν της επεξεργασίας αυτής αποτελεί το καθαρό περιεχόμενο του μηνύματος απαλλαγμένο από τα διάφορα λεκτικά και δομικά στοιχειά που δεν προσφέρουν στη διαδικασία της ταξινόμησης, και έτοιμο να προωθεί στο ήδη εκπαιδευμένο από τον χρήστη, μοντέλο φιλτραρίσματος. Το τελευταίο αποφαίνεται για την κλάση του μηνύματος, το μήνυμα ανασυντίθεται στην αρχική του μορφή , και το αποτέλεσμα της ταξινόμησης αναφέρεται



Εικόνα 34 Το κεντρικό παράθυρο της γραφικής επαφής της μονάδας εκπαίδευσης

σε ένα επιπλέον πεδίο στην επικεφαλίδα. Στην περίπτωση που το μήνυμα κριθεί ως spam , το πρόγραμμα επισυνάπτει στο πεδίο του θέματος το χαρακτηριστικό {SPAM?} , παρέχοντας έτσι στο χρήστη τη δυνατότητα άμεσης επόπτευσης του είδους του και αυτόματης προώθησης του σε έναν συγκεκριμένο κατάλογο, από προγράμματα διαχείρισης ηλεκτρονικού ταχυδρομείου που υποστηρίζουν την λειτουργία αυτή.

Ένα μέτρο ενίσχυσης της ακρίβειας κατηγοριοποίησης του φίλτρου, κρίθηκε σκόπιμη η εξομοίωση της λειτουργίας του Βιβλίου Διευθύνσεων(Address Book) και των Μαύρη Λίστας (Black lists), που ενσωματώνονται σε όλα τα σύγχρονα προγράμματα διαχείρισης ηλεκτρονικού ταχυδρομείου. Για το σκοπό αυτό, μαζί με το μοντέλο του ταξινομητή δημιουργούνται κατά τη διαδικασία της εκπαίδευσης δυο αρχεία κειμένου, τα οποία παρέχουν τις διευθύνσεις των αποστολέων θεμιτών

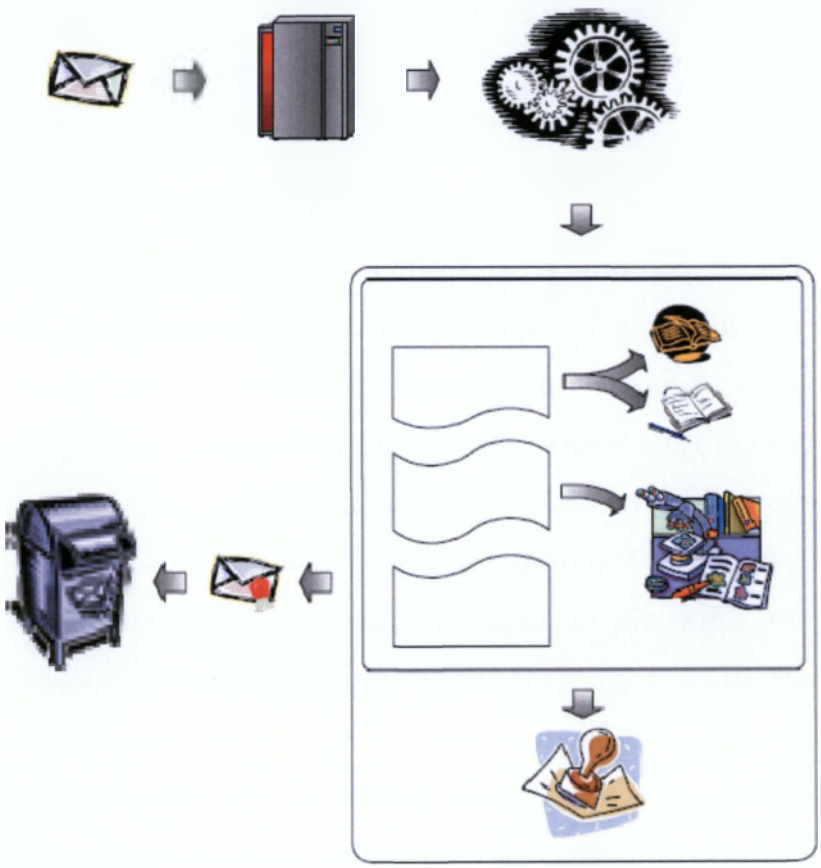
μηνυμάτων και των Spammers αντίστοιχα που διατηρούσαν συχνή αλληλογραφία με τον χρήστη. Ο ρόλος των αρχείων αυτών είναι πλέον εμφανής. Το φίλτρο, πριν από την αξιολόγηση του σώματος του μηνύματος ελέγχει αν ο αποστολέας του βρίσκεται σε κάποιο από τα δυο αρχεία. Αν βρεθεί στο Βιβλίο Διευθύνσεων, το μήνυμα θεωρείται αυτομάτως θεμιτό, ενώ αν βρεθεί στη Μαύρη Λίστα , κατηγοριοποιείται στην κλάση Spam χωρίς περαιτέρω επεξεργασία. Ωστόσο συνίσταται ιδιαίτερη προσοχή κατά τη χρήση του αρχείου της Μαύρης Λίστας, εξ αιτίας της τακτικής των Spammers να χρησιμοποιούν ως διεύθυνση αποστολέα τυχαίες διευθύνσεις ή ακόμη και την διεύθυνση του ίδιου του παραλήπτη, αυξάνοντας έτσι την πιθανότητα η τελευταία να συμπεριληφθεί στη Μαύρη Λίστα.

Η ενσωμάτωση του φίλτρου στον εξυπηρετητή ηλεκτρονικού ταχυδρομείου ενός συστήματος UNIX επιτυγχάνεται ιδιαίτερα εύκολα, απαιτεί όμως την παρέμβαση του ενδιαφερομένου χρήστη. Πιο συγκεκριμένα, αφού ο τελευταίος εκτελέσει επιτυχώς τη μονάδα εκπαίδευσης, καλείται να δηλώσει στο λειτουργικό σύστημα την πρόθεση του τα εισερχόμενα μηνύματα του να μην αποθηκεύονται στο προσωπικό του γραμματοκιβώτιο, αλλά να προωθούνται σ' έναν αυτόνομο διαχειριστή αλληλογραφίας ονόματι procmail, που συνοδεύει συνήθως όλες τις διανομές του UNIX. Βάσει της παραπάνω διαμεταγωγής, κατά την λήψη ενός μηνύματος, ο έλεγχος μεταβιβάζεται από τον εξυπηρετητή ταχυδρομείου στο πρόγραμμα procmail , το οποίο με τη σειρά του προωθεί το μήνυμα στο φίλτρο για την περαιτέρω επεξεργασία του. Το τελευταίο αποκρίνεται, επιστρέφοντας το μήνυμα με την τροποποιημένη επικεφαλίδα, το οποίο περιλαμβάνεται από το procmail και εν τέλει αποθηκεύεται στο γραμματοκιβώτιο του χρήστη.

Θα πρέπει τέλος να αναφέρουμε πως το σύστημα περιέχει αρκετές δικλείδες ασφαλείας, προκειμένου να αποφευχθεί με κάθε τρόπο η απώλεια μηνυμάτων εξ αιτίας κάποιου σφάλματος εκτέλεσης του προγράμματος ή ακόμα και ενδεχόμενης αποτυχίας κλήσης του, περιπτώσεις κατά τις οποίες αναλαμβάνει το procmail την άμεση προώθηση τους στον τελικό

τους προορισμό, είτε αυτός είναι το γραμματοκιβώτιο του χρήστη ή κάποια άλλη ηλεκτρονική διεύθυνση.[25]

Μια πιο παραστατική απεικόνιση του τρόπου λειτουργίας του φίλτρου παρέχεται στην εικόνα 35



Εικόνα 35 Απεικόνιση του τρόπου λειτουργίας της μονάδας φιλτραρίσματος κατά την λήψη ενός καινούριου μηνύματος

[25] Ειρηναίος Μιχελάκης " Αυτόματη Διάθεση Ανεπιθύμητης Ηλεκτρονικής Αλληλογραφίας με Αλγόριθμους μηχανικής Μάθησης"

ΚΕΦΑΛΑΙΟ 4

4.1 Συμπεράσματα

Η αποστολή spam μηνυμάτων αποτελεί αναμφισβήτητα ένα καρκίνωμα του Διαδικτύου, μια μορφή κατάχρησης και αλλοίωσης της δυνατότητας που μας παρέχει το Internet για άμεση και γρήγορη επικοινωνία. Πρόκειται για ένα φαινόμενο που έχει άμεσες επιδράσεις σε όλες τις κοινωνικές ομάδες και σε όλες τις στιγμές της καθημερινότητας του κάθε ανθρώπου. Απαιτείται ανάληψη δράσης σε διάφορα μέτωπα, όχι μόνο στην αποτελεσματική επιβολή των διατάξεων και στη διεθνή συνεργασία, αλλά καθώς επίσης και σε ό,τι αφορά την ευαισθητοποίηση των καταναλωτών. Ειδικότερα τα οικονομικά προβλήματα που προκαλεί κυρίως σε μεγάλες εταιρείες και στους φορείς παροχής Διαδικτυακών υπηρεσιών είναι εντονότατα και χρήζουν άμεσης αντιμετώπισης.

Υπάρχουν διάφορες απόψεις στη δικτυακή κοινότητα. Κάποιοι πιστεύουν ότι το spam δεν μπορεί να σταματήσει ποτέ, κάποιοι ότι το spam είναι ευθύνη των τελικών χρηστών και κάποιοι άλλοι ότι είναι ευθύνη των διαχειριστών mail servers. Η αλήθεια είναι ότι το spam αυξάνεται συνεχώς. Παρόλο που δημιουργούνται νέα και ανανεώνονται τα υπάρχοντα μέσα για την αντιμετώπιση του spam, οι spammers πάντα βρίσκουν νέους τρόπους για να καταφέρουν τον σκοπό τους. Οι χρήστες βλέπουν μόνο ένα μικρό ποσοστό spam στο mailbox τους, δεδομένου ότι οι κατάλογοι των Spammers περιέχουν συχνά ένα μεγάλο ποσοστό από άκυρα emails και πολλά φίλτρα spam διαγράφουν απλά η απορρίπτουν το «προφανές spam».

Μια ερευνά του 2010 για τους χρήστες του ηλεκτρονικού ταχυδρομείου σε Ευρώπη και ΗΠΑ, έδειξε ότι παρόλο που γνώριζαν τους κινδύνους των Spam mails, το 46% εξακολουθεί να τα ανοίγει και να βάζουν τους υπολογιστές τους σε κίνδυνο. Άρα από όλα αυτά βγαίνει το

συμπέρασμα πως για να περιοριστεί το Spam πρέπει όλοι οι χρήστες αλλά και οι διαχειριστές των mail servers από κοινού να συμβάλλουν σε αυτό.

Από τη σκοπιά των ατόμων, το spam συνιστά παραβίαση της ιδιωτικής ζωής. Περαιτέρω, τα μηνύματα spam είναι συχνά παραπλανητικά ή απατηλά. Σημαντικό ποσοστό spam φαίνεται ότι οφείλεται στην επιθυμία αφαίμαξης των καταναλωτών μέσω παραπλανητικών ή δόλιων δηλώσεων. Ιδιαίτερα ενοχλητικά μπορούν επίσης να είναι μηνύματα πορνογραφικού περιεχομένου. Το καθάρισμα των γραμματοθυρίδων για την απομάκρυνση των μηνυμάτων spam είναι χρονοβόρο για τον χρήστη, ενώ οι σχετικές δαπάνες του αυξάνονται όταν πρέπει να χρησιμοποιηθούν φιλτράρισμα και λοιπές δυνατότητες του λογισμικού.

Μεταξύ των πλέον ανησυχητικών συνεπειών του spam είναι ότι υποσκάπτει την εμπιστοσύνη των χρηστών, που αποτελεί προαπαιτούμενο για την επιτυχή διεξαγωγή του ηλεκτρονικού εμπορίου, αλλά και για την κοινωνία της πληροφορίας στο σύνολό της. Η εντύπωση ότι ένα μέσο λιανικών πωλήσεων επηρεάζεται από ανέντιμους εμπορευόμενους μπορεί να έχει αρνητικό αντίκτυπο στη φήμη των νομοταγών εμπορευομένων του ίδιου κλάδου. Πρόσφατα στοιχεία από τις ΗΠΑ, όπου η σχετική εμπειρία είναι μεγαλύτερη από ότι στην ΕΕ, επιβεβαιώνουν ότι πολλά άτομα αντιμετωπίζουν το ηλεκτρονικό ταχυδρομείο με λιγότερη εμπιστοσύνη λόγω του ότι παραλαμβάνουν μεγάλο αριθμό μηνυμάτων spam.

Ο κάθε χρηστής που αισθάνεται ότι απειλείται από τις τεράστιες διαστάσεις που λαμβάνει καθημερινά το φαινόμενο, αλλά και οι μεγάλες επιχειρήσεις που έχουν ήδη κληθεί να αντιμετωπίσουν τις συνέπειες του spamming πρέπει να συντονίσουν τις προσπάθειες τους ώστε να ελαχιστοποιηθούν τα κρούσματα των άχρηστων μηνυμάτων που διακινούνται καθημερινά και κατά συνέπεια να περιοριστούν οι επιπτώσεις τους.

4.2 Μελλοντική Έρευνα

Η δημιουργία του Διαδικτύου αποτέλεσε, χωρίς καμία αμφιβολία, την αρχή μιας σειράς από νέες, πρωτοφανείς υπηρεσίες και δυνατότητες που βασίζονται και οφείλουν την ύπαρξη τους αποκλειστικά και μόνο σ αυτό. Το φαινόμενο των μηνυμάτων spam συνιστά μια από τις σημαντικότερες προκλήσεις που αντιμετωπίζει σήμερα το Internet. Η έρευνα πάνω στην αντιμετώπιση του spam είναι σίγουρο ότι πρέπει να ανταποκριθεί καθώς ολοένα και περισσότερα άχρηστα email καταφθάνουν στα mailboxes των χρηστών , ενώ οι spammers συνεχώς βελτιώνουν τα εργαλεία και τις τεχνικές τους. Το πρόβλημα εντείνεται και από Worms που κυκλοφορούν κατά καιρούς και εκμεταλλεύονται τρύπες στα λειτουργικά συστήματα της Microsoft για να εγκαταστήσουν smtp proxies για αποστολή spam.

Μερικά βασικά θέματα τα οποία χρήζουν την ανάλογη μελέτη σε μελλοντικές προσπάθειες για την αντιμετώπιση του spamming είναι:

- Διεξαγωγή πειραμάτων μεγαλύτερης έκτασης, με την χρήσης περισσότερων σωμάτων μηνυμάτων προερχομένων από χρήστες διαφορετικών επιστημονικών και επαγγελματικών περιοχών.

- Ενσωμάτωση ποικίλων τεχνικών φιλτραρίσματος spam μηνυμάτων , προς ενίσχυση της αποτελεσματικότητας των συστημάτων που βασίζονται σε αλγόριθμους μάθησης, όπως το SpamSentinel .Ως παράδειγμα θα μπορούσαν να αναφερθούν η επέκταση της χρήσης Μαύρων Λιστών στην απλούστερη ή στην πιο εξελιγμένη μορφή τους, η συνεργασία με κατανεμημένα δίκτυα ανίχνευσης spam περιεχομένου.

Οι παραπάνω κατευθύνσεις, καθώς και πολλές άλλες έχουν αρχίσει να αποτελούν αντικείμενο μελέτης αρκετών ερευνητών. Οι προσπάθειες αυτές αναμένονται να συμβάλουν τόσο στην ανάπτυξη συστημάτων για την αντιμετώπιση του φαινομένου όσο και σε άλλες, συγγενικές εφαρμογές κατηγοριοποίησης κειμένου .

ΒΙΒΛΙΟΓΡΑΦΙΑ

ΔΗΜΟΣΙΕΥΣΕΙΣ

- «Anti-Spam Technology Overview», Network and Technology Working Group,
- Telecommunications Engineering and Certification, May 2005
- Μαριάς Ι. (2007), «Ανεπιθύμητη Τηλεφωνία μέσω Διαδικτύου- Μια νέα απειλή που
- αναζητά λύσεις»
- Μαρίνος Παπαδόπουλος «Ηλεκτρονικό Έγκλημα 2004»
- Ειρηναίος Μιχελάκης «Αυτόματη Διάθεση Ανεπιθύμητης Ηλεκτρονικής Αλληλογραφίας με Αλγόριθμους μηχανικής Μάθησης»
- Τζούφλας Γεώργιος «E- Spamming»

ΒΙΒΛΙΑ

- OECD Anti-Spam Toolkit of Recommended Policies and Measures
- Alistair McDonald "SpamAssassin"
- Gordon V.Cormack "Email Spam Filtering:A Systematic Review"

ΙΣΤΟΣΕΛΙΔΕΣ

- http://www.noc.ntua.gr/index.php?module=ContentExpress&func=display&ceid=104
- http://www.dpa.gr/portal/page?_pageid=33%2c20920&_dad=portal&_schema=PORTAL #3
- http://www.commtouch.com
- http://www.ferris.com/research-library/industry-statistics
- http://www.stats.dnsbl.com

- http://washingtonpost.com/wp-dvn/content/article/2007/07/13/AR2007071300606.html

- http://www.sunbeltsoftware.com
- http://dide.ilei.sch.gr/keplinet/tech/spam.php
- http://www.spamfight.org/
- http://en.wikipedia.org/wiki/Main_Page
- http://www.webspam.co.uk/serp-spam-definition-spamdexing/
- http://www.colinfahey.com/spam_topics/spam_topics_el.html
- http://www.pcw.gr/
- http://www.no-spam.gr/laws.htm
- http://www.colinfahey.com/spam_topics/spam_topics_el.html