ΤΕΧΝΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΠΑΤΡΑΣ
ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ
ΤΜΗΜΑ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΟΙ ΙΟΙ ΥΠΟΛΟΓΙΣΤΩΝ ΚΑΙ ΟΙ ΕΠΙΔΡΑΣΗ ΤΟΥΣ ΣΤΗΝ ΕΠΙΧΕΙΡΗΜΑΤΙΚΗ ΔΡΑΣΤΗΡΙΟΤΗΤΑ

ΔΗΜΗΤΡΙΟΣ ΙΩΑΝΝΟΥ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: ΠΑΝΑΓΙΩΤΗΣ ΠΑΠΑΣΩΤΗΡΙΟΥ

ΠΑΤΡΑ 2009

1. **ΕΙΣΑΓΩΓΗ**

Ο ιός υπολογιστών είναι ένα πρόγραμμα γραμμένο αποκλειστικά για να αλλάζει τον τρόπο που λειτουργεί ο υπολογιστής σας, χωρίς την άδεια του χρήστη και χωρίς αυτός να το γνωρίζει.

Η πρώτη αναφορά στον όρο «Ιός Υπολογιστή» έγινε το 1985 όταν ο Fred Cohen, μεταπτυχιακός φοιτητής του Πανεπιστημίου της Νότιας Καλιφόρνιας, αποφάσισε να ονομάσει τα αναπαραγόμενα προγράμματα «Computer Viruses» (ιοί υπολογιστών). Ο Cohen είχε ακολουθήσει την υπόδειξη του καθηγητή του που με την σειρά του είχε επηρεαστεί από μια σειρά διηγημάτων επιστημονικής φαντασίας του David Gerrold από την δεκαετία του '70 με τον τίτλο «When HARLIE was one».

Στο διήγημα «When HARLIE was one» (όταν ο HARLIE ήταν ένας) ο Gerrold βάσισε την όλη πλοκή σε ένα ιό υπολογιστών. Ο HARLIE ήταν το ακρωνύμιο της φράσης Human Analog Robot Life Input Equivalent Computer και περιγραφόταν ως μια μορφή τεχνητής νοημοσύνης που είχε την δυνατότητα να προσομοιώνει τις εγκεφαλικές λειτουργίες. Απίστευτα προφητικό για την σημερινή εποχή δικτυακών ιών: ο τεχνητός εγκέφαλος καλούσε τυχαία τηλεφωνικά νούμερα μέχρι να πάρει απάντηση από έναν υπολογιστή. Όταν το κατάφερνε, φόρτωνε ένα αντίγραφο του εαυτού του σε αυτόν. Ο «μολυσμένος» υπολογιστής με την σειρά του άρχιζε την ίδια διαδικασία. Καλούσε και αυτός τυχαίους τηλεφωνικούς αριθμούς μέχρι να βρει άλλους υπολογιστές για να τους περάσει στο πρόγραμμα. Σε ελάχιστο χρόνο εκατοντάδες υπολογιστές ασχολούνταν αποκλειστικά με την κλήση τυχαίων αριθμών.

Ο ίδιος ο Cohen όρισε αργότερα τον ιό υπολογιστών ως «μια ακολουθία συμβόλων, τα οποία με την μετάφραση τους σε ένα δεδομένο περιβάλλον προκαλούν την μεταβολή άλλων ακολουθιών συμβόλων ούτως ώστε να περιέχουν τμήμα της αρχικής ακολουθίας».

Τελειώνοντας αυτή την εισαγωγή θα πρέπει να αναφέρω ότι σκοπός της πτυχιακής αυτής εργασίας είναι οι ιοί υπολογιστών και αν οι ιοί αυτοί επηρεάζουν τις επιχειρήσεις θετικά ή αρνητικά.

Θα ξεκινήσω με τον ορισμό των ιών, την κατηγοριοποίηση και τους τρόπους αντιμετώπισης τους. Θα αναφερθώ επίσης σε επιχειρήσεις που παράγουν αντιιοτικά προγράμματα αποκομίζοντας τεράστια κέρδη.

Συνεχίζοντας θα σημειώσω τις επιπτώσεις των ιών στις επιχειρήσεις. Θα αναφερθώ σε κάποια παραδείγματα συγκεκριμένων εταιρειών που αντιμετώπισαν αρκετά προβλήματα από ιούς υπολογιστών και ποια ήταν η στάση που κράτησαν.

2. **ΙΟΙ ΥΠΟΛΟΓΙΣΤΩΝ**

2.1. **Γενικά**

Ιοί είναι το λογισμικό που περιέχει τις απαιτούμενες εντολές για μια επίθεση σε ένα υπολογιστικό σύστημα. Διακρίνονται σε κατηγορίες ανάλογα με τον τρόπο αναπαραγωγής τους και την αυτονομία τους από αλλά προγράμματα-ξενιστές και σε επιμέρους είδη ανάλογα με τον τρόπο δράσης τους. Ο ιός είναι ένα τμήμα ηλεκτρονικού κώδικα ο οποίος προσκολλάται σε ένα πρόγραμμα ή ένα αρχείο, ώστε να μπορεί να μεταδοθεί από υπολογιστή σε υπολογιστή. Προσβάλει καθώς μετακινείται. Οι ιοί μπορούν να καταστρέψουν το λογισμικό σας, το υλικό σας και τα αρχεία σας.
Δύο πολύ σημαντικές ιδιότητες των ιών είναι η αυτονομία και η αναπαραγωγή.

- *Αυτονομία* είναι η δυνατότητα των ιών να λειτουργούν χωρίς να χρειάζεται να προσκολληθεί σε ένα λογισμικό-ξενιστή.
- *Αναπαραγωγή* είναι η δυνατότητα του ιού να αναπαράγεται από μόνος του, όταν οι συνθήκες το επιτρέπουν.

Όπως οι ιοί που προσβάλλουν τον άνθρωπο δεν έχουν τα ίδια σοβαρά αποτελέσματα από τον ιό Έμπολα μέχρι τη κοινή γρίπη, έτσι και οι ιοί των υπολογιστών ποικίλλουν, από τον ελάχιστα ενοχλητικό μέχρι τον απόλυτα καταστροφικό ιό. Τα καλά νέα είναι πως ένας πραγματικός ιός δεν μπορεί να διαδοθεί χωρίς την ανθρώπινη παρέμβαση. Κάποιος θα πρέπει να μοιραστεί ένα αρχείο ή να στείλει ένα μήνυμα ηλεκτρονικού ταχυδρομείου για να τον διαδώσει. Τα αντίμετρα κατά των ιών διακρίνονται σε τρεις κατηγορίες: αντίμετρα πρόληψης, ανίχνευσης και επανόρθωσης. Κάθε κατηγορία περιλαμβάνει διάφορα είδη αντίμετρων, εκ των οποίων το πλέον γνωστό είναι το αντιβιοτικό λογισμικό. Οι ιοί απασχολούν πλέον ιδιαίτερα τόσο την επιστημονική κοινότητα, όσο και τους υπεύθυνους διαχείρισης Πληροφοριακών Συστημάτων, λόγω της μεγάλης εξάπλωσης τους. Η μεγάλη εξάπλωση των ιών οφείλετε σε τρεις κυρίως λόγους: στην εξάπλωση των δικτύων δεδομένων μέσω των οποίων οι ιοί αναπαράγονται με γρήγορους ρυθμούς, στο γεγονός ότι δεν υπάρχει πλέον σαφής διαχωρισμός μεταξύ των εννοιών «δεδομένα» και «εκτελέσιμο πρόγραμμα» και στην έλλειψη επίγνωσης των χρηστών σχετικά με τους τρόπους αντιμετώπισης των ιών.
Παρά το γεγονός ότι οι ιοί από πολλούς επιστήμονες ονομάζονται και «κακόβουλο λογισμικό» (malicious software) η ορολογία αυτή που έχει καθιερωθεί , δεν είναι απολύτως δόκιμη . Οι λόγοι είναι οι εξής:

- Το λογισμικό, ως άψυχη οντότητα, δεν έχει βούληση . Συνεπώς, δεν πρέπει να αναφερόμαστε σε «κακόβουλο λογισμικό». (5)
- Ο χαρακτηρισμός «κακόβουλο» δεν είναι δυνατόν να αναφέρεται στους ενδεχομένως δόλιους σκοπούς του προγραμματιστή ή χρήστη ενός λογισμικού οι οποίοι δεν μας αφορούν στην προσπάθεια ταυτοποίησης ή ονοματολογίας ενός τμήματος λογισμικού. Εξάλλου, ένα τμήμα λογισμικού μπορεί να είναι επιβλαβές για ένα υπολογιστικό σύστημα, χωρίς αυτό να αποτελούσε σκοπό του προγραμματιστή ή χρήστη λογισμικού. (5)

Θα ήταν λοιπόν πλέον δόκιμο να αναφερόμαστε στο *κακόβουλο* λογισμικό ως το *λογισμικό με πιθανές επιβλαβείς συνέπειες* για ένα πληροφοριακό σύστημα. Φυσικά, μια τέτοια ονομασία δεν θα επικρατούσε στον κόσμο της πληροφορικής, όπου η συνήθης πρακτική επιβάλλει ονομασίες μίας ή δυο λέξεων, ή αρκτικόλεξα τριών γραμμάτων.
Λαμβάνοντας υπόψη τα προαναφερθέντα, ως *κακόβουλο λογισμικό* ορίζεται το λογισμικό που περιέχει τις απαιτούμενες εντολές για μια επίθεση σε ένα υπολογιστικό σύστημα.
Επίθεση σε ένα υπολογιστικό σύστημα (ή απόπειρα επίθεσης) είναι η παραβίαση (ή απόπειρα παραβίασης, αντίστοιχα) της εμπιστευτικότητας, ακεραιότητας ή διαθεσιμότητας του συστήματος.
Παλαιότερα οι ιοί διαδίδονταν με τις δισκέτες. Όταν ένας ιός εισαχθεί σε έναν υπολογιστή προσκολλάται ή αντικαθιστά ένα υπάρχον πρόγραμμα. Έτσι, όταν ο χρήστης εκτελεί το μολυσμένο πρόγραμμα, εκτελείται και ο ιός. Αυτό συνήθως συμβαίνει χωρίς να το αντιλαμβάνεται ο χρήστης.
Συνήθως ένας χρήστης δεν αντιλαμβάνεται ότι ο υπολογιστής του είναι μολυσμένος, ώσπου ο ιός εκτελέσει την ενέργειά του, όπως η εμφάνιση κάποιου ασυνήθιστου μηνύματος ή η καταστροφή ενός αρχείου. Η ανίχνευση ενός ιού πριν αυτός εκδηλωθεί είναι εξαιρετικά δύσκολη.
Η ανίχνευση και η διαγραφή των ιών γίνεται ευκολότερη με τη χρήση αντιιοτικών εργαλείων.
Υπάρχουν πολλοί τύποι αντιιοτικών προγραμμάτων που χρησιμοποιούν διαφορετική τεχνολογία. Ένας συνηθισμένος τύπος προγράμματος είναι ο "scanner".

2.2. **Η Ιστορία των Ιών**

- Ο πρώτος ιός υπολογιστών εμφανίσθηκε στα μέσα της δεκαετίας του 1980 και ήταν δημιούργημα δύο Πακιστανών ονόματι Basit και Amjad Alvi, οι οποίοι όταν ανακάλυψαν ότι το πρόγραμμα για υπολογιστή (λογισμικό) που είχαν δημιουργήσει αντιγραφόταν παράνομα από κάποιους άλλους, αποφάσισαν να δημιουργήσουν ένα μικρό

προγραμματάκι το οποίο αντέγραφε τον εαυτό του και εμφάνιζε ένα προειδοποιητικό μήνυμα copyright σε κάθε παράνομο αντίγραφο που έκαναν οι πελάτες τους. Για την ιστορία, ο ιός έμεινε γνωστός με το όνομα Brain.

- Γνωστοί ιοί υπολογιστών που άφησαν εποχή ήταν ο Melissa, ο Michelangelo (διέγραφε τον σκληρό δίσκο όταν η ημερομηνία του υπολογιστή έδειχνε 6 Μαρτίου), ο I Love You, ο Slammer, ο Chernobyl (διέγραφε το BIOS όταν η ημερομηνία του υπολογιστή έδειχνε 26 Απριλίου), ο Blaster, ο MyDoom, ο Jerk, ο Yankee, ο LoveLet-A, ο NightShade (κλείδωνε με κωδικό τα αρχεία που δουλεύουμε όταν η ημερομηνία του υπολογιστή έδειχνε Παρασκευή και 13) κ.ά.
- Το 1988 ο φοιτητής Robert Morris δημιούργησε το πρώτο worm, που έφερε το όνομά του, και κατάφερε να μολύνει σχεδόν το 10% των συνδεδεμένων στο Internet υπολογιστών. Ο ιός Michelangelo έκανε την εμφάνισή του το 1992, ήταν ο πρώτος ιός που απέκτησε μεγάλη δημοσιότητα και ανάγκασε τις εταιρείες να δημιουργήσουν προγράμματα antivirus.
- Το 2002 αμερικανικό δικαστήριο καταδίκασε σε φυλάκιση 20 μηνών τον David Smith, τον δημιουργό του ιού Melissa. Ήταν από τους πρώτους ιούς που μεταδιδόταν μέσω μηνυμάτων e-mail με τη μορφή ενός συνημμένου αρχείου Word και προξένησε ζημιές εκατομμυρίων δολαρίων. Ο ιός δημιουργήθηκε το έτος 1999. Αν ο χρήστης έκανε το λάθος να ανοίξει το επισυναπτόμενο αρχείο, ο ιός ενεργοποιείτο, αναπαρήγαγε τον εαυτό του και έστελνε ένα ανάλογο μήνυμα στους πρώτους 50 παραλήπτες που έβρισκε στο βιβλίο διευθύνσεων (address book) του θύματος. Η ποινή θεωρήθηκε ελαστική, καθώς συνεκτιμήθηκε η προσφορά του δράστη στην ανίχνευση και τον εντοπισμό άλλων ιών.
- Ο ιός I Love You εξαπλώθηκε ταχύτατα το έτος 2000 σ' όλον τον κόσμο και προκάλεσε μεγάλη αναστάτωση και κινητοποίηση. Ως δράστης συνελήφθη ένας 23χρονος από τις Φιλιππίνες, ο οποίος ισχυρίσθηκε ότι δεν δημιούργησε τον ιό αλλά ότι απλά τον βελτίωσε. Ο ιός αυτός έδειξε μια ιδιαίτερη προτίμηση σε αρχεία πολυμέσων τύπου .jpg, .mpeg και .mp3 και εκτιμάται ότι προκάλεσε ζημιές ύψους 8-10 δισ. δολαρίων σ' ολόκληρο τον κόσμο.
- Ο Ολλανδός Jan De Witt σκέφθηκε ένα πολύ έξυπνο τέχνασμα το έτος 2001 για να μπορέσει να μολύνει τους υπολογιστές ανυποψίαστων χρηστών. Δημιούργησε έναν ιό με το όνομα της διάσημης Ρωσίδας τενίστριας Άννας Κουρνίκοβα και με δόλωμα ένα συνημμένο αρχείο που περιείχε δήθεν μια γυμνή φωτογραφία της, ο ιός εγκαθίστατο στον

υπολογιστή του χρήστη με τις γνωστές συνέπειες. Ο Jan De Witt συνελήφθη και καταδικάστηκε σε 150 ώρες κοινωνικής εργασίας.

- Ο ιός Bugbear άλλαξε κάπως τα δεδομένα στον χώρο του underground των υπολογιστών καθώς ήταν ένας από τους πρώτους που δεν έκανε φανερή ζημιά στους υπολογιστές που μόλυνε αλλά είχε ως αποστολή να κλέβει αριθμούς πιστωτικών καρτών και τραπεζικά δεδομένα, χωρίς να αφήνει ίχνη και να γίνεται έτσι αντιληπτός, και έστελνε μετά αυτές τις πληροφορίες στον δημιουργό του. Από σχετικές έρευνες που έγιναν προέκυψε ότι με τη βοήθεια αυτού του ιού υποκλάπηκαν στοιχεία από 1.300 τράπεζες, οικονομικούς οργανισμούς και μεγάλες εταιρείες.
- Ο Blaster θεωρείται από τους πιο καταστροφικούς ιούς καθώς έχει τη δυνατότητα να μπλοκάρει ολόκληρα δίκτυα υπολογιστών. Δημιουργήθηκε το έτος 2003. Το ίδιο έτος έκανε την εμφάνισή του και ο ιός Slammer, που μόλυνε δεκάδες χιλιάδες υπολογιστές και servers. Το 2003 επίσης, ο ιός Sobig μόλυνε ένα εκατομμύριο υπολογιστές και δημιούργησε προβλήματα δισεκατομμυρίων δολαρίων καθώς μπλόκαρε την κίνηση στο Διαδίκτυο, απενεργοποίησε δεκάδες servers και αναστάτωσε αεροπορικές και σιδηροδρομικές εταιρείες.
- Ο ιός MyDoom που έμεινε γνωστός και ως Novarg, κατόρθωσε να μολύνει περισσότερα από 100 εκατομμύρια e-mail μέσα σε ελάχιστες ημέρες, στις αρχές του 2004. Μέσω ενός συνημμένου εγγράφου που εστέλνετο με e-mail και ενός προγράμματος ηλεκτρονικής ανταλλαγής αρχείων (peer-to-peer) κατάφερε να κερδίσει τον τίτλο ενός από τους πιο καταστροφικούς ιούς όλων των εποχών. Ο ιός αυτός δημιουργεί μια κερκόπορτα σε κάθε υπολογιστή που μολύνει και δίνει έτσι τη δυνατότητα σε επίδοξους hackers να αποκτούν πλήρη έλεγχο του μολυσμένου μηχανήματος.
- Ένας 18χρονος Γερμανός ήταν ο δημιουργός των ιών Sasser και Netski, που κατάφερε το έτος 2004 και σε διάστημα μερικών εβδομάδων να μολύνει εκατομμύρια υπολογιστές σ' όλον τον κόσμο. Ο ιός προκαλούσε συνεχείς επανεκκινήσεις των μολυσμένων υπολογιστών.
- Το 2004 έκανε την εμφάνισή του ένας ιός «νέας γενιάς», ο Scob, ο οποίος λειτουργούσε ύπουλα και σκοπός τους ήταν να συλλέγει αριθμούς πιστωτικών καρτών, απόρρητους κωδικούς και άλλα ψηφιακά μυστικά που αποκαλύπτουν οι χρήστες όταν κάνουν αγορές μέσω του Διαδικτύου. Ο ιός έστελνε μετά αυτά τα στοιχεία σε οργανωμένες συμμορίες στη Ρωσία, με στόχο ίσως την μεταπώλησή τους.
- Ανάλογη δουλειά με τον ιό Scob έκανε και ο ιός Mimail, ο οποίος εμφάνιζε μια φόρμα καταχώρησης στοιχείων, όπως αριθμούς

πιστωτικών καρτών, και στη συνέχεια έστελνε αυτά τα δεδομένα με e-mail σε κάποιους χρήστες στη Ρωσία.

2.3. **Οι Αιτίες Δημιουργίας των Ιών**

Οι άνθρωποι δημιουργούν τους ιούς και κάποιος πρέπει να γράψει τον κώδικα, να τον δοκιμάσει ώστε να διαπιστώσει ότι διαδίδεται κανονικά και μετά να μεταδώσει τον ιό. Κάποιος επίσης σχεδιάζει και αποφασίζει για το είδος της ζημιάς που θα κάνει ο ιός, αν θα εμφανίσει δηλαδή ένα αβλαβές μήνυμα ή αν θα καταστρέψει τον σκληρό δίσκο. Οι λόγοι όμως που γίνονται αυτά είναι τουλάχιστον τρεις.

- Ο πρώτος είναι η ίδια ψυχολογία που καθοδηγεί τους βάνδαλους και τους εμπρηστές. Για κάποιους αυτό προκαλεί συγκίνηση και αν αυτοί τυχαίνει να γνωρίζουν από προγραμματισμό, τότε είναι πιθανοί δημιουργοί καταστροφικών ιών.
- Ο δεύτερος λόγος έχει να κάνει με τη συγκίνηση της παρακολούθησης πραγμάτων να εκρήγνυνται. Μερικοί άνθρωποι γοητεύονται με πράγματα όπως εκρήξεις και ναυάγια. Η δημιουργία ενός ιού που απλώνεται ταχύτατα είναι κάτι παρόμοιο, δημιουργείται δηλαδή μια βόμβα μέσα σ' έναν υπολογιστή και όσο περισσότεροι υπολογιστές μολύνονται τόσο πιο διασκεδαστική γίνεται αυτή η εικονική έκρηξη.
- Ο τρίτος λόγος έχει να κάνει με αλαζονικές συμπεριφορές. Αν είστε προγραμματιστής και βρείτε μια τρύπα ασφαλείας (security hole) που θα μπορούσατε να εκμεταλλευτείτε, ίσως αναγκασθείτε να εκμεταλλευτείτε ο ίδιος την τρύπα πριν σας προλάβει κάποιος άλλος. Αυτή η λογική έχει βοηθήσει στην δημιουργία πολλών ιών.

Υπήρχε και η άποψη ότι τους ιούς τους δημιουργούσαν οι ίδιες οι εταιρείες δημιουργίας προγραμμάτων υπολογιστών, όταν διαπίστωναν ότι κυκλοφορούσαν παράνομα αντίγραφα των προγραμμάτων τους.

2.4. **Κατηγορίες Ιών**

2.4.1. **Ιομορφικό Λογισμικό**

Ιός είναι ένα τμήμα λογισμικού που ενσωματώνει τον κώδικα του σε έναν πρόγραμμα ξενιστή , αναπαράγεται με την αντιγραφή του εαυτού του σε αλλά προγράμματα ξενιστές και εκτελείται στο παρασκήνιο.
Ο κύκλος ζωής ενός ιού περιλαμβάνει τα εξής τρία στάδια:

- Φάση Επώασης: Ο ιός παραμένει ανενεργός στο υπολογιστικό σύστημα. Ενεργοποιείται από κάποιο γεγονός όπως η έλευση συγκεκριμένης

χρονικής στιγμής, ή η παρουσία κάποιου αρχείου. Η φάση της επώασης δίνει στον ιό την δυνατότητα να περιμένει μέχρι να δημιουργηθούν οι κατάλληλες συνθήκες για την αναπαραγωγή του και ταυτόχρονα παρατείνει –δυνητικά- το χρονικό διάστημα κατά το οποίο μπορεί να παραμείνει απαρατήρητος από τα προγράμματα ανίχνευσης ιών. Υπάρχουν αρκετά παραδείγματα ιών που δεν κάνουν χρήση της φάσης της επώασης , δηλαδή αναπαράγονται αμέσως μόλις βρεθεί κατάλληλος ξενιστής. (5)

- Φάση Αναπαραγωγής: Όλοι οι ιοί περνούν από την φάση αναπαραγωγής, η οποία είναι ένα από τα ιδιαίτερα χαρακτηριστικά των ιών, έναντι άλλων κατηγοριών κακόβουλου λογισμικού. Κατά την αναπαραγωγή, ο ιός δημιουργεί ένα αντίγραφο του και το ενσωματώνει σε προγράμματα ξενιστές. (5)
- Φάση Ενεργοποίησης και Εκτέλεσης: Κατά την φάση αυτή, ο ιός εκτελεί μια σειρά ενεργειών με πιθανές επιβλαβείς συνέπειες για το υπολογιστικό σύστημα που τον φιλοξενεί. Οι ενέργειες που εκτελεί ένας ιός ποικίλουν από ακίνδυνες ενέργειες, όπως η διαγραφή δεδομένων από τις μονάδες αποθήκευσης στις οποίες έχει πρόσβαση το πρόγραμμα ξενιστής.(5)

Ένας ιός αποτελείται τουλάχιστον από δυο βασικές υπορουτίνες:

- Υπορουτίνα Αναζήτησης: Αναζητά νέους ξενιστές στην περιοχή των μονάδων αποθήκευσης και δικτύου, όπου έχει πρόσβαση ο ξενιστής του ιού. (5)
- Υπορουτίνα Αντιγραφής: Δημιουργεί ένα αντίγραφο του ιού και το ενσωματώνει στον ξενιστή που έχει εντοπίσει η υπορουτίνα αναζήτησης. (5)

Ορισμένοι ιοί χρησιμοποιούν πρόσθετες υπορουτίνες, τις *υπορουτίνες κατά εντοπισμού* , που προβαίνουν στις απαιτούμενες ενέργειες για να αποφευχθεί ο εντοπισμός των ιών από το αντίστοιχο αντιβιοτικό λογισμικό που υπάρχει στο υπολογιστικό σύστημα. Οι ρουτίνες κατά του εντοπισμού ρυθμίζουν τον τρόπο και χρόνο λειτουργίας των ρουτινών αναζήτησης και αντιγραφής, με σκοπό την απόκρυψη του ιού από λογισμικό κατά των ιών. (5)

Λειτουργικό Διάγραμμα του Ιού

2.4.1.1. **Ιοί Τομέα Εκκίνησης**

Ο Τομέας Εκκίνησης (Boot Sector) είναι ο τομέας ενός δίσκου που χρησιμοποιείται για την εκκίνηση του λειτουργικού συστήματος που βρίσκεται στον δίσκο αυτό, ή για την φόρτωση του δίσκου αυτού. Ο εκτελέσιμος κώδικας που περιέχεται στον τομέα εκκίνησης εκτελείται μόλις το υπολογιστικό σύστημα εντοπίσει την ύπαρξη του δίσκου, σε κάθε εκκίνηση του υπολογιστικού συστήματος .

Οι Ιοί Τομέα Εκκίνησης εγκαθίστανται στον τομέα εκκίνησης ενός δίσκου αντικαθιστώντας τις υπάρχουσες ρουτίνες, τις οποίες τοποθετούν σε άλλο τμήμα του δίσκου και τις καλούν αφού εκτελεστούν οι ίδιοι οι ιοί πρώτα.

Λόγω του μικρού μεγέθους του τομέα εκκίνησης, οι Ιοί Τομέα Εκκίνησης εγγράφουν στον τομέα εκκίνησης μόνο μια ρουτίνα εκτέλεσης του ιού και εγγράφουν το κύριο τμήμα του ιού σε άλλη περιοχή του δίσκου.

Στις περισσότερες περιπτώσεις μετά την εκτέλεση τους παραμένουν ενεργοί στην μνήμη (Ιοί Διαμένοντες στην Κύρια Μνήμη) , με σκοπό να εκτελέσουν το στόχο τους αλλά και να διατηρήσουν τον έλεγχο του συστήματος με τέτοιο τρόπο που να αποφεύγουν την ανίχνευση από αντιβιοτικά προγράμματα. (19,5)

2.4.1.2. **Παρασιτικοί ιοί**

Οι παρασιτικοί ιοί είναι το πρώτο είδος ίων που εμφανίστηκαν και αποτελούν ακόμα την πολυπληθέστερη κατηγορία. Ένας παρασιτικός ιός προσαρτάται σε ένα εκτελέσιμο πρόγραμμα και μολύνει αλλά προγράμματα. Εντοπίζουν

εκτελέσιμα αρχεία και τα μολύνουν ενσωματώνοντας τον κώδικα του ιού στον κώδικα του εκτελέσιμου αρχείου. Η θέση του κώδικα του ιού, μέσα στον κώδικα του μολυσμένου εκτελέσιμου αρχείου μπορεί να είναι μια από τις εξής τρεις:

- Αρχή του εκτελέσιμου αρχείου: Οι ιοί αυτοί τοποθετούν τον κώδικα του ιού στην αρχή του κώδικα του εκτελέσιμου αρχείου (μη μολυσμένο και μολυσμένο εκτελέσιμο αρχείο) (5)
- Τέλος του εκτελέσιμου αρχείου: Οι ιοί αυτοί τοποθετούν τον κώδικα του ιού στο τέλος του κώδικα του εκτελέσιμου αρχείου. (5)
- Μέση του εκτελέσιμου αρχείου: Οι ιοί αυτοί τοποθετούν τον κώδικα του ιού στην μέση του κώδικα του εκτελέσιμου αρχείου, δημιουργώντας πρώτα τον κατάλληλο κενό χώρο μετατοπίζοντας τον κώδικα που έπεται. Σε οποιαδήποτε περίπτωση, το μέγεθος του εκτελέσιμου αρχείου αυξάνεται κατά το μέγεθος του κώδικα του ιού. (5)

Κεφαλίδα		**Εκτελέσιμος κώδικας και δεδομένα**

Κεφαλίδα	Virus Code	**Εκτελέσιμος κώδικας και δεδομένα**

Μη μολυσμένο και μολυσμένο εκτελέσιμο αρχείο

Όταν το μολυσμένο αρχείο εκτελεστεί, εκτελείται και ο ιός και μολύνει με τον ίδιο τρόπο άλλα αρχεία. Οι ιοί αυτού του τύπου δεν είναι ιδιαίτερα επιτυχημένοι, επειδή τα προγράμματα κατά των ιών είναι σε θέση να αντιληφθούν αλλαγές σε ένα εκτελέσιμο πρόγραμμα, οπότε ο ιός γίνεται γρήγορα αντιληπτός.

2.4.1.3. **Πολυμερείς Ιοί**

Πολυμερείς (Multipartite Viruses) είναι οι ιοί που μολύνουν είτε εκτελέσιμα αρχεία (Παρασιτικοί Ιοί) είτε τομείς εκκίνησης (Ιοί Τομέας Εκκίνησης). Αυτοί οι ιοί έχουν συνήθως δυο τμήματα. Όταν μολύνουν ένα εκτελέσιμο αρχείο, ενεργούν ως Παρασιτικοί Ιοί. Όταν μολύνουν έναν τομέα εκκίνησης, ενεργούν ως Ιοί Τομέα Εκκίνησης.

2.4.1.4. **Διαμένοντες στην Κύρια Μνήμη Ιοί**

Οι Διαμένοντες στην Κύρια Μνήμη Ιοί (Resident Viruses) παραμένουν ενεργοί στην κύρια μνήμη, ακόμα και μετά το πέρας της εκτέλεσης του ξενιστή τους.

Ο ξενιστής τους μπορεί να είναι ένα εκτελέσιμο πρόγραμμα ή ένας τομέας εκκίνησης δίσκου. Μετά το πέρας της εκτέλεσης του ξενιστή οι Διαμένοντες στην Κύρια Μνήμη Ιοί αποκολλώνται από τον ξενιστή και τοποθετούνται στην Κύρια Μνήμη όπου και παραμένουν μέχρι τον τερματισμό του συστήματος. Ο σκοπός που εξυπηρετεί η παραμονή τους στην μνήμη είναι διπλός:

- Αποκτούν έλεγχο του συστήματος σε χαμηλό επίπεδο, προσθέτοντας τον εκτελέσιμο κώδικα τους στον κώδικα συχνά εκτελουμένων διακοπών λογισμικού (interrupt requests), με αποτέλεσμα να διαφεύγουν της ανίχνευσης από αντιβιοτικό λογισμικό.
- Είναι σε θέση να μολύνουν ξενιστές, σε χρονικά σημεία που ο ελεγχόμενος έλεγχος από τον χρήστη και το εκτελούμενο αντιβιοτικό λογισμικό είναι χαλαρός.

2.4.1.5. **Κρυφοί Ιοί**

Κρυφοί (Stealth Viruses) είναι οι ιοί που αποκρύπτουν την μόλυνση των αρχείων. Ο όρος Stealth αναφέρεται στις τεχνικές που χρησιμοποιούν για να αποφύγουν την ανίχνευση της μόλυνσης των αρχείων που προσβάλλουν από αντιβιοτικά προγράμματα.

Κάθε ιός κάνει αλλαγές στα αρχεία ή τομείς εκκίνησης που προσβάλει. Αυτές οι αλλαγές γίνονται αντιληπτές από αντιβιοτικά προγράμματα που τηρούν μητρώο με αθροίσματα ελέγχου (checksums) όλων των αρχείων που περιέχονται σε ένα υπολογιστικό σύστημα.

Όταν ένα αντιβιοτικό πρόγραμμα αυτού του τύπου εκτελείται, συγκρίνει τα αθροίσματα ελέγχου των αρχείων στον δίσκο με τα αθροίσματα ελέγχου που είχε υπολογίσει στον προηγούμενο έλεγχο. Αν ορισμένα αρχεία, όπως π.χ. τα εκτελέσιμα αρχεία, έχουν μεταβληθεί, τότε είναι πιθανόν να έχουν μολυνθεί από κάποιον ιό.

Οι κρυφοί ιοί αποκτούν έλεγχο των κλήσεων συστήματος που αφορούν στην πρόσβαση σε αρχεία. Με αυτόν τον τρόπο αποκρύπτουν από τα αντιβιοτικά προγράμματα το γεγονός ότι ένα αρχείο έχει μολυνθεί. Αν ένα πρόγραμμα ζητήσει, μέσω κλήσης συστήματος, τις ιδιότητες ενός αρχείου μολυσμένου με Κρυφό Ιό, τότε ο Κρυφός Ιός επιστρέφει τις ιδιότητες του αρχείου προτού μολυνθεί. Αν ζητηθεί η ανάγνωση του αρχείου, ο Κρυφός Ιός επιστρέφει τα δεδομένα που περιέχονται στο αρχείο, όπως αυτά ήταν πριν την μόλυνση. Αν όμως ζητηθεί η εκτέλεση του αρχείου, τότε ο Κρυφός Ίος εκτελεί το μολυσμένο αρχείο.

2.4.1.6. **Κρυπτογραφημένοι Ιοί**

Ορισμένα αντιβιοτικά προγράμματα προσπαθούν να ανιχνεύσουν την ύπαρξη ιών συγκρίνοντας τον κώδικα στα αρχεία που ελέγχουν με ακολουθίες κώδικα που ανήκουν σε ήδη ταυτοποιημένους ιούς.
Οι κρυπτογραφημένοι ιοί (Encrypted Viruses) αποφεύγουν την ανίχνευση από τα προαναφερθέντα αντιβιοτικά προγράμματα κρυπτογραφώντας το μεγαλύτερο τμήμα του ιού, αφήνοντας σε μη κρυπτογραφημένη μορφή μόνο μία απλή ρουτίνα αποκρυπτογράφησης και ένα τυχαίο κλειδί κρυπτογράφησης.
Ένας ιός είναι Κρυπτογραφημένος όταν κρυπτογραφεί όλο το τμήμα του κώδικα που τον αποτελεί, εκτός από μια μικρή ρουτίνα αποκρυπτογράφησης.

2.4.1.7. **Πολυμορφικοί Ιοί**

Στην περίπτωση των Κρυπτογραφημένων Ιών, η ρουτίνα αποκρυπτογράφησης παραμένει σε μη κρυπτογραφημένη μορφή σε αντίθεση με το υπόλοιπο τμήμα του ιού που κρυπτογραφείται με τυχαίο κλειδί. Τα αντιβιοτικά προγράμματα που ανιχνεύουν ιούς με βάση τις ακολουθίες κώδικα ταυτοποιημένων ιών μπορούν να εντοπίσουν έναν κρυπτογραφημένο ιό, ανιχνεύοντας το υπολογιστικό σύστημα για τις προαναφερθείσες ρουτίνες αποκρυπτογράφησης.
Οι Πολυμορφικοί Ιοί αποτελούν μια εξέλιξη των Κρυπτογραφημένων Ιών. Πολυμορφικοί είναι οι ιοί που μεταβάλουν την μορφή τους κάθε φορά που προσβάλλουν ένα αρχείο.
Οι Πολυμορφικοί Ιοί αποτελούνται από Κρυπτογραφημένους Ιούς, οι οποίοι μεταβάλλουν την ρουτίνα αποκρυπτογράφησης μετά από κάθε προσβολή αρχείου-ξενιστή.

2.4.1.8. **Ρέτρο-Ιοί**

Πρόκειται για τους ιούς που προσπαθούν να ανιχνεύσουν την ύπαρξη αντιβιοτικών προγραμμάτων , και να τα καταστήσουν αναποτελεσματικά. Οι Ρέτρο-Ιοί εκμεταλλεύονται συγκεκριμένες στιγμές κατά τις οποίες τα αντιβιοτικά προγράμματα είναι «ευάλωτα», όπως π.χ. κατά τη διάρκεια ενημέρωσης των αντιβιοτικών προγραμμάτων στην επόμενη έκδοση τους.

2.4.1.9. **Ιοί που διαγράφουν τμήμα του ξενιστή**

Οι Ιοί διατηρούν την αρχική λειτουργικότητα των εκτελέσιμων ξενιστών που προσβάλλουν, προκειμένου να αποφύγουν τον εντοπισμό από αντιβιοτικά προγράμματα ή από τον ίδιο το χρήστη του υπολογιστικού συστήματος. Υπάρχει όμως και κατηγορία ιών που διαγράφουν τμήμα του ξενιστή (Overwriters) ή και όλα τα περιεχόμενα του ξενιστή. Αυτό τους καθιστά ιδιαίτερα ανιχνεύσιμους από το αντιβιοτικό λογισμικό.

2.4.1.10. **Μάκρο-Ιοί**

Μάκρο-Ιοί είναι οι ιοί που αποτελούνται από μια ακολουθία εντολών η οποία διερμηνεύεται αντί να εκτελείται.

Οι ιοί στους οποίους αναφερθήκαμε μέχρι αυτήν την ενότητα χρησιμοποιούν ως ξενιστές εκτελέσιμα αρχεία. Όταν το εκτελέσιμο αρχείο-ξενιστής εκτελείται, εκτελείται και ο ιός. Ορισμένα προγράμματα πλέον επιτρέπουν στον χρήστη να αποθηκεύει και εντολές (μακρο-εντολές, macros) στα αρχεία δεδομένων που χρησιμοποιούν, με σκοπό οι εντολές αυτές να διερμηνεύονται κατά την χρήση των συγκεκριμένων αρχείων δεδομένων.

Οι χρήστες χρησιμοποιούν μακροεντολές για να αυτοματοποιήσουν πολύπλοκες και επαναλαμβανόμενες εργασίες που εκτελούν σε ένα συγκεκριμένο αρχείο. Οι μακροεντολές ενεργοποιούνται είτε μετά από την παρέμβαση του χρήστη είτε με την έλευση κάποιου γεγονότος, όπως είναι το άνοιγμα ενός αρχείου δεδομένων ή η αποθήκευση ενός αρχείου δεδομένων.

Όταν ενεργοποιηθεί η μακροεντολή έχει την δυνατότητα να αντιγραφεί σε άλλα αρχεία δεδομένων του ίδιου τύπου, να διαγράψει αρχεία ή να προκαλέσει οποιαδήποτε άλλη μεταβολή στο σύστημα αρχείων.

Οι Μακρο-Ιοί προσβάλλουν πλέον τα υπολογιστικά συστήματα περισσότερο από κάθε άλλο ιό. Η διάδοση τους οφείλεται στις εξής αιτίες :

- Είναι , συνήθως , ανεξάρτητοι από το Λειτουργικό Σύστημα και το Υλικό. Ένας Μακρο-Ιός που προσβάλλει έγγραφα της εφαρμογής επεξεργασίας κειμένων Microsoft Word έχει την δυνατότητα να προσβάλλει αποιοδήποτε Λειτουργικό Σύστημα υποστηρίζει η εφαρμογή Microsoft Word. (5)
- Το πλήθος των αρχείων δεδομένων που περιέχουν και μακρο-εντολές είναι πλέον κατά μέσο όρο , μεγαλύτερο από το πλήθος των εκτελέσιμων αρχείων, στα σύγχρονα υπολογιστικά συστήματα. (5)
- Οι Μακρο-Ιοί αναπαράγονται πολύ εύκολα μέσω προγραμμάτων όπως ηλεκρονικό ταχυδρομείο , καθώς τα αρχεία δεδομένων που περιέχουν και μακρο-εντολές αποτελούν αρχεία που ανταλλάσσονται συχνά μεταξύ χρηστών. (5)

2.4.2. **Μη Ιομορφικό Κακόβουλο Λογισμικό**

2.4.2.1. **Κερκόπορτες**

Οι Κερκόπορτες (Trapdoors ή Backdoors) είναι σημεία εισόδου που επιτρέπουν την πρόσβαση σε ένα σύστημα, παρακάμπτοντας την συνηθισμένη διαδικασία πρόσβασης ασφαλείας.

Χρησιμοποιούνται από προγραμματιστές για νομότυπους σκοπούς, κατά τις διαδικασίες ελέγχου και αποσφαλμάτωσης των εφαρμογών που κατασκευάζουν. Μία Κερκόπορτα μπορεί να αποτελέσει επίσης σημείο ευπάθειας, αν γίνει γνωστή από επίδοξο εισβολέα.

Κερκόπορτες τοποθετούνται, όμως και από εισβολείς συστημάτων (hackers). Μετά από μία επιτυχημένη απόπειρα παράνομη πρόσβασης σε ένα σύστημα, τοποθετούν μία κερκόπορτα η οποία θα τους διασφαλίσει εύκολα την παράνομη είσοδο σε μελλοντικό χρόνο.

2.4.2.2. **Λογικές Βόμβες**

Μία Λογική Βόμβα (Logic Bomb) είναι ένα πρόγραμμα που εκτελεί μία ενέργεια που παραβιάζει την πολιτική ασφάλειας ενός συστήματος, όταν πληρείται κάποια λογική συνθήκη στο σύστημα.
Παρόμοιες είναι και οι Χρονικές Βόμβες, όπου οι ενέργειες που παραβιάζουν την πολιτική ασφάλειας εκτελούνται σε συγκεκριμένη χρονική στιγμή.

2.4.2.3. **Δούρειοι Ίπποι**

Οι Δούρειοι Ίπποι είναι «φαινομενικά χρήσιμα προγράμματα που περιλαμβάνουν κρυφές λειτουργίες οι οποίες μπορούν να εκμεταλλευτούν τα δικαιώματα του χρήστη που εκτελεί το πρόγραμμα , με συνέπεια μια απειλή στην ασφάλεια. Ένας Δούρειος Ίππος εκτελεί λειτουργίες που ο χρήστης του δεν σκόπευε.»(19)
Οι Δούρειοι Ίπποι δεν αναπαράγονται μόνοι τους. Πρέπει να βασιστούν στους ιδίους τους χρήστες τους για την εγκατάσταση και την εκτέλεση τους.
Για παράδειγμα, σε έναν δικτυακό χώρο όπου ο καθένας έχει αρχεία τα οποία μόνο αυτός μπορεί να επεξεργαστεί, μπορεί κάποιος να δημιουργήσει έναν Δούρειο Ίππο, ο οποίος όταν εκτελεσθεί από κάποιον χρήστη του δικτύου θα αλλάξει τα δικαιώματα των αρχείων του και να επιτρέπει στους άλλους χρήστες να τα διαχειριστούν. Αυτός ο δούρειος ίππος θα μπορούσε να έχει την μορφή ενός πολύ χρήσιμου εργαλείου το οποίο θα βρισκόταν στον κοινό δικτυακό χώρο.

Ένα άλλο παράδειγμα δούρειο ίππου είναι οι μεταλλαγμένοι μεταφραστές, οι οποίοι έχουν τροποποιηθεί κατάλληλα έτσι ώστε κατά εκτέλεση της μετάφρασης να προσθέτουν επιπλέον κώδικα (Κερκόπορτες) στα προγράμματα που ματαφράζουν.

2.4.2.4. ***Αναπαραγωγοί***

Οι Αναπαραγωγοί (Worms) είναι προγράμματα που μεταδίδονται από έναν υπολογιστή σε έναν άλλο δημιουργώντας αντίγραφα του εαυτού τους. Σε αντίθεση με τους ιούς, δεν απαιτούν ξενιστή, αλλά δημιουργούν αντίγραφα του εαυτού τους τα οποία στέλνουν μέσω δικτύου σε άλλου υπολογιστές.
Ο πρώτος γνωστός Αναπαραγωγός δημιουργήθηκε το 1988 από τον Robert Morris και είχε ως αποτέλεσμα να βγει εκτός λειτουργίας το μεγαλύτερο μέρος του Διαδικτύου. (5)

Ένας Αναπαραγωγός έχει τον ίδιο κύκλο ζωής με έναν Ιό. Κατά την διάρκεια της φάσης της αναπαραγωγής του συνήθως εκτελεί τις εξής ενέργειες :

- Αναζητά άλλα συστήματα στα οποία μπορεί να εξαπλωθεί εξετάζοντας αρχεία όπως είναι το βιβλίο διευθύνσεων ενός προγράμματος ηλεκτρικού ταχυδρομείου ή τον πίνακα των διευθύνσεων απομακρυσμένων συστημάτων. (19)
- Στην συνέχεια δημιουργεί μια σύνδεση με το απομακρυσμένο σύστημα. (19)
- Δημιουργεί ένα κλώνο του στο απομακρυσμένο σύστημα τον οποίο και εκτελεί. Ο κλώνος εκτελεί κάποια ενέργεια που παραβιάζει την πολιτική ασφάλειας του συστήματος, όπως και ένας ιός , και συνεχίζει προς αναζήτηση άλλων συστημάτων στα οποία θα μπορέσει να εξαπλωθεί. (19)

2.4.2.5. **Βακτήρια**

Τα Βακτήρια (Bacteria) αναπαράγονται όπως και οι ιοί, και δεν απαιτούν την ύπαρξη ξενιστή. Δεν αλλοιώνουν δεδομένα σκόπιμα. Μοναδικός σκοπός ενός βακτηρίου είναι να αναπαραχθεί σε ένα ή περισσότερα αντίγραφα.

Τα Βακτήρια είναι προγράμματα που καταναλώνουν έναν ή περισσότερους πόρους συστήματος σε μεγάλο βαθμό.

Ένα τυπικό βακτήριο δημιουργεί κατά την εκτέλεση του ένα ή περισσότερα αντίγραφα του εαυτού του τα οποία με την σειρά τους εκτελούνται δημιουργώντας αντίγραφα τους και ούτω καθεξής.

Παρόλο που το βακτήριο δεν εκτελεί κάποια επιζήμια ενέργεια καταναλώνει το σύνολο των πόρων του συστήματος (μνήμη, επεξεργαστική ικανότητα ή χώρο στο δίσκο) οπότε μειώνεται η διαθεσιμότητα του συστήματος. Σε αντίθεση λοιπόν με τις περισσότερες μορφές Κακόβουλου Λογισμικού, τα βακτήρια προσβάλλουν την διαθεσιμότητα και όχι την ακεραιότητα του συστήματος.

2.4.2.6. **Παραπλανητική Πληροφόρηση**

Παράλληλα με την ανάπτυξη του Κακόβουλου Λογισμικού, εμφανίστηκε και η τάση για τη διάδοση παραπλανητικής πληροφόρησης σχετικά με την ύπαρξη Κακόβουλου Λογισμικού (boaxes). Πρόκειται για τη διάδοση ψεύδους φήμης σχετικά με την ύπαρξη νέου Κακόβουλου Λογισμικού. Τυπικό παράδειγμα αποτελεί ο «ιός» Good Times (1994). (5)

Ένα email το οποίο κυκλοφόρησε στο Διαδίκτυο το 1994 και διαδόθηκε αρκετά αφορούσε στην ψευδή είδηση περί ενός νέου ιού με το όνομα Good Times. Αν και δεν υπήρξε ποτέ τέτοιος ιός, σπαταλήθηκε παγκοσμίως αρκετός χρόνος για την αποστολή αυτού του email από γνωστό σε γνωστό, την ανάγνωση του και την προσπάθεια ανεύρεσης κατάλληλης αναβάθμισης σε αντιβιοτικό λογισμικό που αντιμετωπίζει αυτόν τον ιό. (5)

Το αποτέλεσμα ήταν ότι ένα, αθώο email που γράφτηκε μέσα σε λίγα λεπτά μείωσε -έστω και λίγο- τη διαθεσιμότητα αρκετών πληροφοριακών συστημάτων σε παγκόσμιο επίπεδο.

2.5. **Μελέτες Περίπτωσης**

2.5.1. **Ιός** CIH

Ο ιός CIH είναι ένας παρασιτικός ιός που εμφανίσθηκε αρχικά στην Ταιβάν. Παραλλαγές του ιού έχουν παρουσιαστεί με τα ονόματα PE_CIH, CIHV, SPACEFILLER, VIN32, CHERNOBYL, TSHERNOBYL και TSERNOBYL. (5)
Ο ιός CIH προσβάλλει εκτελέσιμα αρχεία του Λογισμικού Συστήματος Microsoft Windows 9x. Όταν εκτελεστεί ένα προσβεβλημένο εκτελέσιμο αρχείο, ο ιός εγκαθίσταται στην μνήμη του υπολογιστικού συστήματος και προσβάλλει τα αρχεία των προγραμμάτων που βρίσκονται σε εκτέλεση. (5)
Αρχικά, όταν ενεργοποιείται ο ιός, ο CIH επανεγγράφει τα δεδομένα που περιέχονται στους τομείς του σκληρού δίσκου. Ξεκινά από τον τομέα Εκκίνησης και επανεγγράφει (με τυχαία δεδομένα) όλους τους επόμενους τομείς του σκληρού δίσκου, μέχρι το υπολογιστικό σύστημα να πάψει να λειτουργεί εξαιτίας των απολεσθέντων δεδομένων. Παράλληλα, ο CIH προσπαθεί να αλλοιώσει (επαναγγράφοντας με τυχαία δεδομένα) την περιοχή του FLASH BIOS. Στην περίπτωση που το καταφέρει, τότε οι βασικές λειτουργίες BIOS καθίστανται άχρηστες, και το υπολογιστικό σύστημα τίθεται εκτός λειτουργίας. Ο μόνος τρόπος για επανόρθωση σε αυτήν την περίπτωση είναι η μεταμόρφωση του λογισμικού του BIOS. (5)

2.5.2. **Μακρο-ιός** Melissa

Ο ιός Melissa είναι ένας Μακρο-Ιός εμφανίσθηκε αρχικά σε Ομάδες Συζητήσεων στο Διαδίκτυο τον Μάρτιο του 1999. Παραλλαγές του ιού έχουν παρουσιαστεί με τα ονόματα W97M/Melissa.o, W97M/Melissa.gen@MM, W97M/Melissa.bp@MM. (5)
Ο Μακρο-Ιός Melissa προσβάλλει αρχεία δεδομένων (έγγραφα κειμένου) της εφαρμογής Microsoft Word. Ο Μακρο-Ιός Melissa μεταδίδεται με μαζική αποστολή μέσω ηλεκτρονικού ταχυδρομείου, χρησιμοποιώντας την εφαρμογή ηλεκτρονικού ταχυδρομείου Microsoft Outlook. Ο Ιός Melissa αποτελείται από κώδικα Visual Basic Script (VBScript), ο οποίος εκτελείται από την εφαρμογή ηλεκτρονικού ταχυδρομείου Microsoft Outlook όταν ο κώδικας αυτός περιέχεται σε ένα μήνυμα ηλεκτρονικού ταχυδρομείου, την στιγμή που ο χρήστης διαβάζει το μήνυμα. (5)
Ο ιός ανακτά τις πρώτες 50 διευθύνσεις ηλεκτρονικού ταχυδρομείου, από το βιβλίο διευθύνσεων της εφαρμογής Microsoft Outlook και αποστέλλει σε αυτές τις διευθύνσεις ένα μήνυμα ηλεκτρονικού ταχυδρομείου με θέμα

"Important Message from Application. Username", και κύριο μέρος του μηνύματος: "Here is that document you asked for…don't show anyone else ;-)". (5)

Το Application Username αντικαθιστάται από το Microsoft Outlook με το κωδικό όνομα του χρήστη που χρησιμοποίει το σύστημα εκείνη τη στιγμή. Στο μήνυμα του ηλεκτρονικού ταχυδρομείου επισυνάπτεται ένα αρχείο Microsoft Word το οποίο είναι προσβεβλημένο από τον ιό, και περιέχει μια λίστα με περιοχές στο Διαδίκτυο που παρουσιάζουν υλικό ακατάλληλο για ανηλίκους.

Αν ο παραλήπτης του μηνύματος του ηλεκτρονικού ταχυδρομείου ανοίξει το επισυναπτόμενο έγγραφο, τότε ο ιός απενεργοποιεί την προστασία από μακροεντολές της εφαρμογής Microsoft Word (προκειμένου να είναι σε θέση να εκτελέσει τον κώδικα του μέσα από την εφαρμογή) και δημιουργεί αντίγραφα του εαυτού του στα έγγραφα της εφαρμογής Microsoft Word που θα ανοίξει ο χρήστης σε μελλοντικό χρόνο. Ο τρόπος με τον οποίο το επιτυγχάνει αυτό είναι με την εγκατάσταση αντιγράφου του ιού στο πρότυπο αρχείο του Microsoft Word (Normal Template), το οποίο χρησιμοποιείται ως πρότυπο σε κάθε δημιουργία νέου εγγράφου. Ο ιός Melissa δεν εκτελεί κακόβουλες ενέργειες. Απλά αναπαράγεται με την μέθοδο που περιγράψαμε στις προηγούμενες παραγράφους. Συνεπώς είναι ένας ΜακροΙός Αναπαραγωγός.

Ο ΜακροΙός Melissa δεν εκτελεί κακόβουλες ενέργειες, συνεπώς δεν διαθέτει και φάση ενεργοποίησης.

2.5.3. **Μακρο-Ιός** I Love You

Ο I Love You είναι ένας Μακρο-Ιός που εμφανίστηκε αρχικά στις Φιλιππίνες, σε μηνύματα ηλεκτρονικού ταχυδρομείου τον Απρίλιο του 2000. Παραλλαγές του ιού έχουν παρουσιαστεί με τα ονόματα VBS/Loveletter.b, VBS/Loveletter.c, VBS/Loveletter.d, VBS/Loveletter.af, VBS/Loveletter.ah, VBS/Loveletter.ag, VBS/Loveletter.ae, VBS/Loveletter.ai, VBS/Loveletter.be, LoveBug,Very Funny, Love Letter και Mothers Day. (5)

Ο Μακρο-Ιός I Love You αποτελείται από κωδικό γραμμένο σε Visual Basic Script. Χρησιμοποιεί τις εφαρμογές ηλεκτρονικού ταχυδρομείου που υποστηρίζουν VBScript για να αποστείλει ηλεκτρονικά μηνύματα (e-mails) σε όλες τις διευθύνσεις που βρίσκονται στο βιβλίο διευθύνσεων του χρήστη, επισυνάπτοντας το αρχείο "LOVE-LETTER-FOR-YOU.TXT.vbs", το οποίο περιέχει τον κώδικα του ιού. (5)

Το μήνυμα που αποστέλλεται έχει θέμα: "I LOVE YOU", ενώ στο κύριο μέρος του μηνύματος περιέχεται η φράση: "Kindly check the attached LOVELETTER coming from me". (5)

Τα επισυναπτόμενα αρχεία, το θέμα του μηνύματος και τα περιεχόμενα του κύριου μέρους του μηνύματος διαφέρουν στις προαναφερθείσας παραλλαγές του Μακρο-Ιού. Η δράση του, όμως, παραμένει ίδια.
Ο ιός αυτός επηρεάζει συστήματα με λειτουργικό συστήματα Windows 9x/NT, όπου είναι ενεργοποιημένη η δυνατότητα εκτέλεσης scripts (Windows Scripting Host – WSH). Δεν είναι κρυπτογραφημένος και το μέγεθος του είναι 10,309 bytes. Ο χρήστης πρέπει να ενεργοποιήσει τον ιό ο ίδιος, εκτελώντας τον κώδικα script που έχει επισυναφθεί στο μήνυμα ηλεκτρονικού ταχυδρομείου που παρέλαβε. (5)
Ο ιός αυτός μεταδίδεται πολύ γρήγορα. Ελέγχει όλες τις δευτερεύουσες μονάδες αποθήκευσης του συστήματος που έχει προσβάλλει και κατόπιν διασχίζει όλους τους υποκαταλόγους για να βρει πιθανούς ξενιστές. Μολύνει αρχεία με τις ακόλουθες επεκτάσεις: “vbs”, “vbe”, “js”, “jse”, “css”, “wsh”, “sct”, “hta”, “jpg”, “jpeg”, “mp3” και “mp2”. Σε όλες τις περιπτώσεις εκτός από αυτές των αρχείων τύπου “mp3” και “mp2”, ο ιός επανεγγράφει το αρχείο με τον δικό του κώδικα. (5)
Για αρχεία με επεκτάσεις “vbs” και “vbe”, ο ιός δεν αλλάζει το όνομα του αρχικού αρχείου. Στις περιπτώσεις των αρχείων με επέκταση “js”, “jse”, “css”, “wsh”, “sct”, “hta”, “jpg” και “jpeg”, αλλάζει την επέκταση του αυθεντικού αρχείου σε “vbs”. (5)
Στα αρχεία με κατάληξη “mp3” ή “mp2”, μετατρέπει το αρχείο ήχου σε κρυφό αρχείο του συστήματος και δημιουργεί ένα αντίγραφο του ιού διατηρώντας το όνομα του αυθεντικού αρχείου και επέκταση “vbs”. Συνεπώς τα αρχεία “mp3” και “mp2” μπόρουν να επαναφέρουν από ένα προσβεβλημένο σύστημα.
Επίσης ο Μακρο-Ιός δημιουργεί τα ακόλουθα αντίγραφα του εαυτού του στο σύστημα του χρήστη: το “Win32DLL.vbs” στο ριζικό κατάλογο όπου είναι εγκατεστημένα τα αρχεία του Λειτουργικού Συστήματος Windows 9x/NT, και τα αρχεία “MSKERNEL32.vbs”, LOVE-LETTER-FOR-YOU.TXT.vbs” και LOVE-LETTER-FOR-YOU.HTM” στο υποκατάλογο SYSTEM του ριζικού καταλόγου όπου είναι εγκατεστημένα τα αρχεία του Λειτουργικού Συστήματος Windows 9x/NT. (5)
Ο Μακρο-Ιός προσπαθεί να μεταφορτώσει και να εγκαταστήσει το εκτελέσιμο αρχείο WIN-BUGSFIX.EXE από το Διαδίκτυο. Αυτό το πρόγραμμα ανιχνεύει αποθηκευμένα συνθηματικά χρηστών του Λειτουργικού Συστήματος Win9x και τα αποστέλλει στην διεύθυνση ηλεκτρονικού ταχυδρομείου MAILME@SUPER.NET.PH. (5)
Ο Μακρο-Ιός I Love You τοποθετεί τη διαδρομή καταλόγου προς το εκτελέσιμο αρχείο WIN-BUGSFIX.EXE στο κλειδί HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\WIN-BUGSFIXM του Μητρώου του Λειτουργικού Συστήματος. Αυτό έχει ως αποτέλεσμα ο Μακρο-Ιός να εισέρχεται σε φάση ενεργοποίησης

(εκτελείται το αρχείο WIN-BUGSFIX.EXE) σε κάθε επανεκκίνηση του Λειτουργικού Συστήματος. (5)

2.6. **Συνήθεις Τρόποι Προσβολής από Ιούς**

Εάν χρησιμοποιείτε το Διαδίκτυο, έχετε μολυνθεί πιθανώς με έναν ιό, τρωικό ή spyware. Σύμφωνα με το κέντρο θύελλας Διαδικτύου, το μη προστατευμένο PC είναι μολυσμένο μέσα σε 20 λεπτά από την κανονική χρήση Διαδικτύου. Πολλοί άνθρωποι θέλουν να ξέρουν τι έκαναν και απόκτησαν ιό στον υπολογιστή τους. Εδώ είναι οι κορυφαίοι λόγοι που μολύνονται οι υπολογιστές με ιούς και πώς μπορούν οι άνθρωποι να αποτρέψουν αυτές τις κοινές απειλές ασφάλειας Διαδικτύου.

2.6.1. **Συνδέσεις ηλεκτρονικού ταχυδρομείου**

Οι ιοί μπορούν να σταλούν ως συνδέσεις ηλεκτρονικού ταχυδρομείου για να μολύνουν τον υπολογιστή σας. Εάν μεταφορτώνετε το ηλεκτρονικό ταχυδρομείο σας σε ένα πρόγραμμα ηλεκτρονικού ταχυδρομείου, ανιχνεύστε όλες τις συνδέσεις ηλεκτρονικού ταχυδρομείου με έναν ανιχνευτή ιών. Τα περισσότερα σημαντικά προγράμματα webmail ανιχνεύουν τις συνδέσεις προτού να τις μεταφορτώσετε, αλλά δεν πρέπει να μεταφορτώνετε τα αρχεία από άγνωστες πηγές. Το ηλεκτρονικό ταχυδρομείο "Phishing", που υποστηρίζει ότι είναι από την τράπεζά σας ή άλλο οικονομικό όργανο που σας ζητά να παρέχει προσωπικές πληροφορίες ή να μεταφορτώσει κάτι στον υπολογιστή σας.

2.6.2. ***Ανταλλαγή των αρχείων στα δωμάτια επικοινωνίας***

Δεν πρέπει ποτέ να μεταφορτώσετε τα αρχεία από τις πηγές που δεν εμπιστεύεστε. Οι ιοί και άλλες απειλές ασφάλειας Διαδικτύου μπορούν να μοιάσουν με τα έγκυρες αρχεία ή φωτογραφίες. Πάντα ανιχνεύστε τα αρχεία με έναν ανιχνευτή ιών πριν να τα ανοίγετε.

2.6.3. **Ιστοχώροι ξεφυλλίσματος**

Μερικοί ιστοχώροι χρησιμοποιούν πλαίσια διαλόγου παραπλάνησης για να εγκαταστήσουν κρυφά spyware στα προγράμματα. Μερικές φορές spyware μπορεί να εγκαταστήσει ακόμα κι αν δεν επιλέγετε "ναι" ή "να δεχτείτε". Κρατήστε τις τοποθετήσεις ασφάλειας στην προεπιλογή για να προστατευθείτε από αυτές τις μολύνσεις.

2.6.4. P2P **προγράμματα όπως** Kazaa **ή** Limewire

Εάν μοιράζεστε μουσική (ή, γενικότερα, αρχεία) χρησιμοποιώντας τα P2P δίκτυα, μπορεί να αναγκαστείτε να μεταφορτώσετε το λογισμικό διαφήμισης επάνω στον υπολογιστή σας. Αυτό το λογισμικό μπορεί να παραγάγει popups μέσα από τον υπολογιστή σας. Σε αυτές τις περιπτώσεις, μπορεί να δείτε popups ακόμα κι αν δεν είστε σε ανοικτή γραμμή.

2.6.5. **Εγκατάσταση οικονόμων οθόνης** (screen savers)

Ελέγξτε τη συμφωνία αδειών οποιουδήποτε προγράμματος που εγκαθιστάτε για να επιβεβαιώσετε ότι δεν έρχεται συσσωρευμένος με άλλα προγράμματα. Οι συμφωνίες αδειών είναι υποτιθέμενες για να εξηγήσουν εάν το λογισμικό που μεταφορτώνετε θα προκαλέσει τις διαφημίσεις ή άλλη μεταφόρτωση. Αυτά τα προγράμματα μπορούν να έχουν συμφωνίες αδειών όπου έχουν θάψει αυτές τις πληροφορίες. Πάντα να είστε προσεκτικοί και να διαβάζεται με τι συμφωνείτε προτού μεταφορτώσετε το ελεύθερο λογισμικό.

2.6.6. **Ενήλικοι-σχετικοί ιστοχώροι**

Πολλές από αυτές τις περιοχές πραγματοποιούν ένα κέρδος με τον καταναγκασμό των θεατών να μεταφορτώνουν spyware και adware για να έχουν πρόσβαση στην περιοχή τους. Μπορεί να μην είστε σε θέση να δείτε αυτές τις περιοχές εάν χρησιμοποιείτε έναν ασφαλή browser ή αν έχετε τις ρυθμίσεις ασφάλειάς σας πάρα πολύ υψηλές.

2.6.7. **Ιστοχώροι τυχερού παιχνιδιού**.

Μπορεί να φανεί ότι βλέποντας spoilers σε απευθείας σύνδεση με παιχνίδια σας αφήσουν να κερδίσετε γρηγορότερα, αλλά μπορεί να επιβραδύνει τον υπολογιστή σας με το spyware. Το Mick Lathrop, μέρος της ερευνητικής StopSign's Spyware ομάδας λέει, "παίρνω τα περισσότερα από τα δείγματα spyware μου από τους παιχνίδι-σχετικούς με την ιστοχώρους." Αποφύγετε οποιαδήποτε περιοχή που απαιτεί ότι ένα λογισμικό μεταφορτώνει στις πληροφορίες πρόσβασης.

2.7. **Αντιμετώπιση Κακόβουλου Λογισμικού**

Οι απειλές κατά υπολογιστικών συστημάτων που προέρχονται από Κακόβουλο Λογισμικό διαφέρουν από τις υπόλοιπες απειλές στα εξής σημεία:

- Γενικότητα: Το Κακόβουλο Λογισμικό δεν εκμεταλλεύεται ένα συγκεκριμένο ελάττωμα του Λειτουργικού Συστήματος το οποίο προσβάλλει, και σε πολλές περιπτώσεις δεν παραβιάζει την πολιτική ασφάλειας του συστήματος. Η πολιτική ασφάλειας (με εξαίρεση λίγα Λειτουργικά Συστήματα) δεν περιλαμβάνει συνθήκες ελέγχου για την

ακεραιότητα του συστήματος και των πόρων που το συναποτελούν, αλλά περιορίζεται σε συνθήκες ελέγχου μυστικότητας.

- Έκταση: Μια απειλή προερχόμενη από το Κακόβουλο Λογισμικό μπορεί να επεκταθεί από ένα υπολογιστικό σύστημα σε ένα άλλο.

Εφεδρικά αντίγραφα ασφάλειας: Τα εφεδρικά αντίγραφα ασφάλειας (backup) δεν λειτουργούν αποτελεσματικά εναντίον του Κακόβουλου Λογισμικού. Αυτό οφείλεται στο γεγονός ότι το αντίγραφο μπορεί να περιέχει αντίγραφο του ιού οπότε η αποκατάσταση του αντίγραφου ενδέχεται να επαναφέρει ένα αντίγραφο του ιού σε ένα σύστημα , όπου οι διαχειριστές έχουν απομακρύνει τον ιό.

2.7.1. **Τεχνικές Αντιμετώπισης Κακόβουλου Λογισμικού**

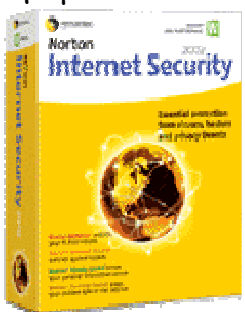
Τα κύρια αντίμετρα που χρησιμοποιούνται κατά του Κακόβουλου Λογισμικού είναι:

- Επίγνωση σε θέματα Ασφαλείας. Το λογισμικό που οι χρήστες εγκαθιστούν στα υπολογιστικά συστήματα πρέπει να προέρχεται από έμπιστες πηγές.
- Αντιβιοτικό Λογισμικό. Αυτά τα προγράμματα ανιχνεύουν τα αρχεία ενός συστήματος, προσπαθώντας να εντοπίσουν την ύπαρξη Ιών στο σύστημα.
- Αρχεία Ελέγχου του Λειτουργικού Συστήματος. Είναι ιδιαίτερα χρήσιμα στον εντοπισμό Δούρειων Ίππων που προσπαθούν να στείλουν δεδομένα σε εξωτερικό δίκτυο ή υπολογιστικό σύστημα, ή και για τον εντοπισμό Κακόβουλου Λογισμικού που προσπαθεί να διαβάσει ή να εγγράψει δεδομένα από περιοχή του πληροφοριακού συστήματος στην οποία δεν επιτρέπεται η πρόσβαση.
- Αυστηρά μέτρα ασφαλείας. Η επιβολή ελέγχου πρόσβασης και την εκτέλεση εφαρμογών παραχωρώντας τους τα ελάχιστα απαιτούμενα δικαιώματα στο σύστημα με σκοπό την ελαχιστοποίηση της ζημιάς που μπορεί να επιφέρει το Κακόβουλο Λογισμικό.
- Απαγόρευση μεταφόρτωσης εκτελεστικού κώδικα, μέσω κατάλληλων φίλτρων στους Πληρεξούσιους (Application Proxies). Εναλλακτικά, θα μπορούσε να επιτραπεί μόνο η εκτέλεση νέου, μη ελεγμένου κώδικα, που φέρει ψηφιακή υπογραφή από παροχή λογισμικού που εγκρίνεται από την πολιτική ασφαλείας του συστήματος.
- Απομόνωση. Πληροφοριακά συστήματα που περιέχουν πολύτιμη πληροφορία για έναν οργανισμό πρέπει να απομονώνονται, δικτυακά από τα συστήματα που είναι συνδεδεμένα με εξωτερικά ή άλλα μη ελεγχόμενα πληροφοριακά συστήματα.

- Αναχώματα Ασφαλείας (firewalls). Προκειμένου να αποκλεισθεί η δυνατότητα σε Κακόβουλο Λογισμικό που εκτελείται σε εξωτερικό, μη ελεγχόμενο περιβάλλον, να αποκτήσει πρόσβαση σε ένα εσωτερικό δίκτυο.
- Εργαλεία Ανίχνευσης Εισβολών. Αυτά τα εργαλεία ανιχνεύουν την κίνηση από και προς συγκεκριμένα σημεία ενός δικτύου, και εντοπίζουν πιθανές ακολουθίες ενεργειών που σηματοδοτούν ενδεχόμενη απόπειρα παραβίασης της πολιτικής ασφαλείας.

Μία διαδικασία ανάληψης από προσβολή και περιορισμού Κακόβουλου Λογισμικού πρέπει να υπάρχει ως τμήμα της πολιτικής ασφαλείας κάθε οργανισμού. Αυτή η διαδικασία πρέπει να πληροί τις ακόλουθες προδιαγραφές:

- Απομόνωση μολυσμένων συστημάτων.
- Απομάκρυνση (οριστική διαγραφή) του Κακόβουλου Λογισμικού από ένα σύστημα.
- Αποκατάσταση της ακεραιότητας ενός προσβεβλημένου συστήματος. Σε περίπτωση που έχουν αλλοιωθεί πληροφορίες που υπήρχαν στο σύστημα, η διαδικασία αυτή πρέπει να περιλαμβάνει την αποκατάσταση της αλλοιωμένης πληροφορίας με την χρήση εφεδρικών αντιγράφων ασφαλείας.
- Η διαδικασία ανάνηψης από προσβολή από Κακόβουλο Λογισμικό πρέπει να είναι τεκμηριωμένη και να ελέγχεται σε τακτικά χρονικά διαστήματα.
- Η διαδικασία ανάνηψης από προσβολή από Κακόβουλο Λογισμικό πρέπει να περιλαμβάνει την προληπτική ενημέρωση των χρηστών σχετικά τις ενέργειες που πρέπει να λάβουν, σε περίπτωση μόλυνσης από Κακόβουλο Λογισμικό. Ενημέρωση των οργανισμών που προσφέρουν προϊόντα και υπηρεσίες προστασίας από κακόβουλο λογισμικό.



2.7.2. **Ψηφιακοί Τρόποι Προστασίας από τους Ιούς**

Ο βασικός τρόπος προστασίας από τους ιούς των υπολογιστών είναι η εγκατάσταση, η σωστή ρύθμιση και η συνεχής ενημέρωση ή επικαιροποίηση (update) μέσω του Internet ενός έγκυρου προγράμματος προστασίας από ιούς, που είναι γνωστά με τον όρο Antivirus ή αντιικά προγράμματα.

Υπάρχουν ακόμη ειδικά προγράμματα για προστασία από ιούς τύπου spyware, adware αλλά και από dialers και από τη μάστιγα των spam e-mails.
Οι ενέργειες που εκτελεί ένα αντιιοτικό λογισμικό είναι οι ακόλουθες:

- Ανίχνευση του ιού από τη στιγμή που το σύστημα έχει προσβληθεί.
- Ταυτοποίηση του ιού που έχει προσβάλλει το σύστημα.
- Αφαίρεση των τμημάτων του ιού από όλα τα αρχεία που έχει μολύνει.

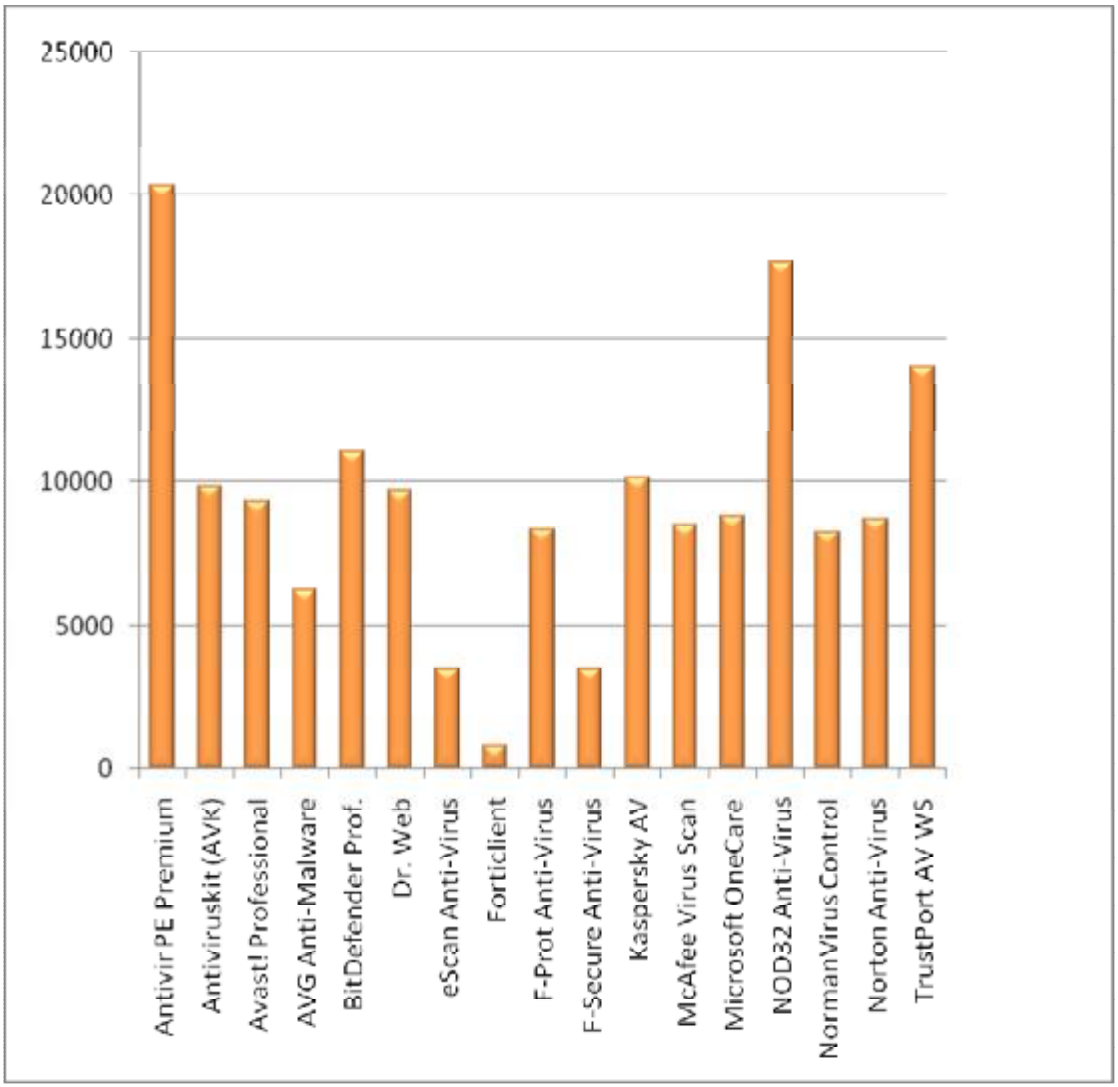
Η χρήση ενός ψηφιακού τείχους προστασίας (firewall), με τη μορφή software ή hardware, είναι χρήσιμη αλλά θα πρέπει να γίνεται με προσοχή και με την προϋπόθεση ότι υπάρχει καλή γνώση του τρόπου ρύθμισης και λειτουργίας του. Οι γενικοί κανόνες προστασίας είναι ότι θα πρέπει να προσέχουμε τι προγράμματα εκτελούμε στον υπολογιστή μας, τι αρχεία κατεβάζουμε από το Internet, ποιος μας στέλνει e-mail καθώς και ποιος έχει το δικαίωμα να χρησιμοποιήσει τον υπολογιστή μας όταν εμείς απουσιάζουμε. Προσοχή πρέπει να δίνουμε και στα προγράμματα που διαφημίζονται και διανέμονται δωρεάν καθώς και στα προγράμματα που χρησιμοποιούμε για διαδικτυακές συνομιλίες (chat).
Μια πολύ καλή λύση είναι να εγκαταστήσουμε και να εκτελέσουμε μια από τις εφαρμογές που αναλαμβάνουν να ανιχνεύσουν στο σύστημά μας τα τυχόν υπάρχοντα ευαίσθητα σημεία (vulnerabilities) και να μας τα παρουσιάσουν με παραστατικό τρόπο. Τέλος, μια πολύ καλή συμβουλή είναι να λαμβάνουμε πολύ τακτικά, ίσως και καθημερινά, εφεδρικά αντίγραφα ασφαλείας των αρχείων μας, σε CD, σε DVD ή σε εξωτερικό σκληρό δίσκο, μια διαδικασία που είναι γνωστή με τον όρο backup, έτσι ώστε ακόμα και στην ακραία περίπτωση που χάσουμε σημαντικά αρχεία από την επίθεση κάποιου ιού, να μπορέσουμε να τα ανακτήσουμε άμεσα.
Από τα πιο γνωστά αντιβιοτικά προγράμματα είναι το Symantec Antivirus της εταιρείας Symantec, το McAfee της εταιρείας Network Associates, το Kaspersky, το Panda, το Sophos, το F-Prot της εταιρείας Frisk, το F-Secure καθώς και το AntiVir και το AVG της εταιρείας Grisoft που διατίθενται δωρεάν για προσωπική χρήση. Όλα έχουν τη δυνατότητα αυτόματης ενημέρωσης (update) μέσω του Internet. (5)

2.7.3. **Αντιβιοτικά προγράμματα**

Στην ιστοσελίδα *http://www.av-comparatives.org* υπάρχουν συγκεκριμένες εταιρείες που παράγουν αντιιοτικά προγράμματα στην οποία πραγματοποιείται έρευνα για το πόσους ιούς ανιχνεύει το κάθε αντιβιοτικό πρόγραμμα. Η έρευνα αυτή γίνεται περίπου κάθε 3 μήνες.

Στον πιο κάτω πίνακα αναφέρεται το ποσοστό και ο αριθμός ιών που ανιχνεύτηκαν από το κάθε αντιιτικό πρόγραμμα από 25036 ιούς σε έρευνα που έγινε το Μάιο του 2008. Αρχικά η έρευνα αυτή έγινε χωρίς την παρέμβαση του χρήστη.

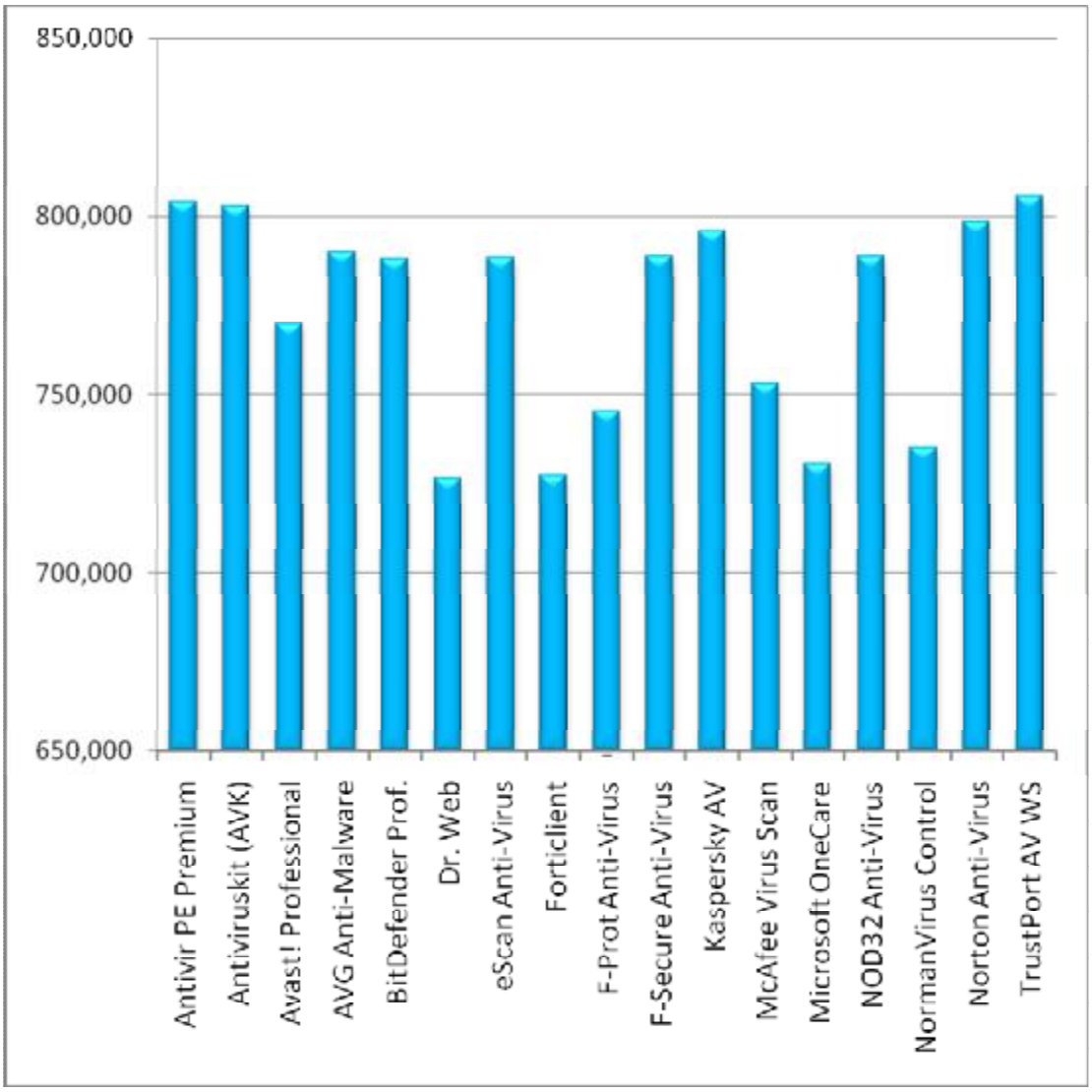
COMPANY	PRODUCT			
AVIRA	Antivir PE Premium	20378	81%	
GDATASecurity	Antiviruskit (AVK)	9857	39%	
Alwil software	Avast! Professional	9346	37%	
GriSoft	AVG Anti-Malware	6249	25%	
Softwin	BitDefender Prof.	11071	44%	
Doctor Web	Dr. Web	9695	39%	
MicroWorld	eScan Anti-Virus	3462	14%	
Fortinet	Forticlient	792	3%	
Frisk Software	F-Prot Anti-Virus	8346	33%	
F-Secure	F-Secure Anti-Virus	3473	14%	
Kaspersky Labs	Kaspersky AV	10125	40%	
McAfee	McAfee Virus Scan	8488	34%	
Microsoft	Microsoft OneCare	8807	35%	
ESET	NOD32 Anti-Virus	17687	71%	
Norman ASA	NormanVirusControl	8234	33%	
Symantec	Norton Anti-Virus	8733	35%	
AEC	TrustPort AV WS	14044	56%	(20)



Σε αυτή την περίπτωση αναφέρεται το ποσοστό και ο αριθμός ιών που ανιχνεύτηκαν από το κάθε αντιβιοτικό πρόγραμμα από ένα σύνολο 808344 ιών. Η έρευνα αυτή έγινε με την παρέμβαση του χρήστη στο αντιβιοτικό πρόγραμμα.

COMPANY	PRODUCT		
AVIRA	Antivir PE Premium	803,876	99.45%
GDATASecurity	Antiviruskit (AVK)	802,774	99.31%
Alwil software	Avast! Professional	769,862	95.24%
GriSoft	AVG Anti-Malware	790,160	97.75%
Softwin	BitDefender Prof.	788,220	97.51%
Doctor Web	Dr. Web	726,481	89.87%
MicroWorld	eScan Anti-Virus	788,370	97.53%
Fortinet	Forticlient	727,374	89.98%

Frisk Software	F-Prot Anti-Virus	745,257	92.20%	
F-Secure	F-Secure Anti-Virus	788,732	97.57%	
Kaspersky Labs	Kaspersky AV	795,924	98.46%	
McAfee	McAfee Virus Scan	752,953	93.15%	
Microsoft	Microsoft OneCare	730,485	90.37%	
ESET	NOD32 Anti-Virus	788,965	97.60%	
Norman ASA	NormanVirusControl	735,033	90.93%	
Symantec	Norton Anti-Virus	798,627	98.80%	
AEC	TrustPort AV WS	805,460	99.64%	(20)



Σημαντικό είναι να αναφέρουμε ότι από την έρευνα που έγινε κανένα αντιβιοτικό πρόγραμμα δεν ανιχνεύει 100% τους ιούς.

2.8. Cookies

Τα cookies αποτελούν μικρές συμβολοσειρές (αρχεία κειμένου) οι οποίες χρησιμοποιούνται κατά την επικοινωνία των φυλλομετρητών (web browsers) με τους διάφορους διαδικτυακούς χώρους. Όταν κάποιος φυλλομετρητής επικοινωνεί με ένα εξυπηρετητή (server) για να κατεβάσει μία ιστοσελίδα, ο εξυπηρετητής δύναται να στείλει και μία μικρή μοναδική συμβολοσείρα, το cookie. Το cookie αποθηκεύεται από τον φυλλομετρητή και αποστέλλεται στον εξυπηρετητή κάθε φορά που ζητά από τον συγκεκριμένο εξυπηρετητή μία ιστοσελίδα.
Ένας χρήστης χρησιμοποιεί τον φυλλομετρητή για να προσπελάσει ιστοσελίδες που βρίσκονται σε περισσότερους από ένα εξυπηρετητές. Για κάθε διαφορετικό εξυπηρετητή ο φυλλομετρητής αποθηκεύει τα cookies που του αποστέλλονται. Σε κάθε νέα επικοινωνία με ένα εξυπηρετητή εντοπίζει και στέλνει το cookie που του αποστάλθηκε τη προηγούμενη φορά.
Τα cookies επιτρέπουν στους εξυπηρετητές να «θυμούνται» καταστάσεις και αυτή είναι η κύρια χρήση τους. Πολλές ιστοσελίδες επιτρέπουν στους πελάτες τους να ρυθμίσουν το πως εμφανίζεται μία ιστοσελίδα, να αποθηκεύσουν το κωδικό πρόσβασης τους, να χρησιμοποιήσουν ένα νοητικό καλάθι αγορών κ.τ.λ. Αυτά τα χαρακτηριστικά δεν θα ήταν εφικτά εάν οι εξυπηρετητές δεν μπορούσαν να αποθηκεύσουν κάποια πληροφορία που να υποδηλώνει την ταυτότητα του χρήστη. Αυτή ακριβώς η διευκόλυνση παρέχεται από το cookie. Οι εξυπηρετητές αποθηκεύουν τις επιλογές του χρήστη σε συνδυασμό με το cookie. Όταν ο εξυπηρετητής λάβει από ένα φυλλομετρητή ένα cookie τότε μπορεί να επαναφέρει τις ρυθμίσεις και επιλογές που επέλεξε ο χρήστης.
Τα cookies μπορεί να προκαλέσουν δύο ζητήματα ασφαλείας. Το πρώτο πρόβλημα εντοπίζεται στην περίπτωση που μια κακόβουλη ιστοσελίδα αξιοποιήσει κάποια αδυναμία του φυλλομετρητή για να λάβει ένα cookie το οποίο κανονικά δεν θα έπρεπε να αποσταλεί στον εξυπηρετητή που φιλοξενεί την ιστοσελίδα. Στην περίπτωση που συμβεί αυτό, τότε το cookie μπορεί να χρησιμοποιηθεί για την μην εξουσιοδοτημένη πρόσβαση σε κάποια ιστοσελίδα που μόνο ο πραγματικός κάτοχος του cookie θα μπορούσε να έχει.
Το δεύτερο πρόβλημα (που αποτελεί και σύνηθες φαινόμενο) είναι ότι κάποιοι οργανισμοί(π.χ. doubleclick) χρησιμοποιούν τα cookies για να εντοπίσουν τις δραστηριότητες των χρηστών. Είναι γνωστό ότι πολλές ιστοσελίδες φιλοξενούν διαφημίσεις (banners) οι οποίες παρέχονται από άλλες εταιρείες. Οι διαφημίσεις αυτές διατηρούνται στους εξυπηρετητές των διαφημιστικών εταιρειών. Με άλλα λόγια, όταν ένα φυλλομετρητής κατεβάζει μια διαφήμιση επικοινωνεί με τον εξυπηρετητή της διαφημιστικής εταιρείας. Κατά τη διάρκεια αυτής της επικοινωνίας οι εξυπηρετητές μπορούν φυσικά να αποστέλλουν και να λαμβάνουν cookies.

Έτσι όταν ένας χρήστης χρησιμοποιεί κάποιο φυλλομετρητή για να προσπελάσει ιστοσελίδες ο οποίες ιστοσελίδες είναι πελάτες της ίδιας διαφημιστικής εταιρείας, τα cookies επιτρέπουν στην διαφημιστική εταιρεία να εντοπίσει το διαδικτυακό μονοπάτι που ακολούθησε ο χρήστης.
Προφανώς τα cookies δεν αποτελούν κακόβουλο χαρακτηριστικό. Απλά πολλές φορές χρησιμοποιούνται όχι για την προκαθορισμένη τους χρήση με αποτέλεσμα να οδηγήσει πολλούς χρήστες να απενεργοποιήσουν την υποστήριξη για cookies από τους φυλλομετρητές.

2.9. **Ιοί στη Σύγχρονη Εποχή**

Η ιοί των υπολογιστών έχουν αλλάξει χρήση τελευταία και από ένα παιχνίδι νεαρών προγραμματιστών έχουν αρχίσει να προσφέρουν τις υπηρεσίες τους στο οργανωμένο έγκλημα, κλέβοντας αριθμούς πιστωτικών καρτών, κωδικούς λογαριασμών (passwords), απόρρητα αρχεία και άλλα ψηφιακά μυστικά που αποκαλύπτουν οι χρήστες όταν κάνουν αγορές και παραγγελίες στο Διαδίκτυο. Οι νέοι ιοί έχουν ως αντικείμενο την υποκλοπή και αξιοποίηση στοιχείων και πληροφοριών για εγκληματικούς ή στρατιωτικούς σκοπούς και ήδη έχουν κάνει την εμφάνισή τους κάποιοι ιοί που θεωρούνται οι πρόδρομοι της νέας γενιάς των ιών «κατασκόπων». Οι ιοί του μέλλοντος είναι πολύ πιθανό να χρησιμοποιηθούν στην κατασκοπεία και στον στρατό είτε για την καταστροφή αρχείων είτε για την συλλογή πληροφοριών. Οι ημέρες που τους ιούς τους δημιουργούσαν έφηβοι που ήθελαν να διασκεδάσουν έχουν παρέλθει και είναι πολλοί αυτοί που θα τις αναπολήσουν. Αναλυτές θεμάτων που ασχολούνται με την ασφάλεια των συστημάτων υπολογιστών περιγράφουν τους ιούς της νέας γενιάς με τους όρους *Blended Threats*, δηλ. συνδυασμένες απειλές, και *Flash Threats*, δηλ. ακαριαίες απειλές, και εκτιμούν ότι θα τους συναντάμε όλο και συχνότερα στο άμεσο μέλλον. Υπάρχει, όμως, και η εκτίμηση ειδικών αναλυτών που ισχυρίζονται ότι εφόσον η επόμενη γενιά των ιών θα είναι στην ουσία συλλέκτες απόρρητων δεδομένων, θα μπορούν κάλλιστα να χρησιμοποιηθούν στην κατασκοπεία, είτε για την διείσδυση και την καταστροφή αρχείων είτε απλά για την συλλογή πληροφοριών. Ήδη η χρήση και η αξιοποίηση των ιών του μέλλοντος εξετάζεται σοβαρά από σχολές πολέμου και μυστικές υπηρεσίες, ενώ μια πρώτη επιτυχής εφαρμογή τους φέρεται να έλαβε χώρα σε πρόσφατες πολεμικές συγκρούσεις.
Η Ελλάδα καταλαμβάνει την 11^{η} θέση σε παγκόσμια κλίμακα στη λίστα με τις 20 χώρες που δέχθηκαν, σύμφωνα με την έγκυρη εταιρεία ασφάλειας υπολογιστικών συστημάτων Symantec, τις περισσότερες επιθέσεις από ιούς υπολογιστών κατά το πρώτο εξάμηνο του έτους 2004, οπότε και καταγράφηκαν περί τις 5.500 επιθέσεις ανά 100 χιλιάδες χρήστες. Αν λάβουμε υπόψη μας ότι οι Έλληνες χρήστες είναι περίπου 3 εκατομμύρια, οι

συνολικές επιθέσεις από ιούς υπολογιστών κατά το πρώτο εξάμηνο του έτους 2004, υπολογίζονται σε περίπου 160.000, μόνο στην Ελλάδα. Οι ιοί που προτίμησαν περισσότερο τους υπολογιστές των Ελλήνων χρηστών ήταν ο *Slammer* και ο *Gaobot*, ενώ οι περισσότερες επιθέσεις προέρχονταν από τις ΗΠΑ και την Κίνα.

Σημαντική μείωση στα προβλήματα που έχουν σχέση με την ασφάλεια των υπολογιστών και των πληροφοριακών συστημάτων παρατηρήθηκε τόσο στις επιχειρήσεις όσο και στα νοικοκυριά της Ελλάδας το 2007.

Αυτό είναι το συμπέρασμα στο οποίο καταλήγουν οι πρόσφατες έρευνες που πραγματοποιήθηκαν για λογαριασμό του Παρατηρητηρίου για την Κοινωνία της Πληροφορίας.

Συγκεκριμένα, το 79% (από 73% το 2006) των επιχειρήσεων με περισσότερους από 10 εργαζόμενους, το 80% (από 74%) των μικρότερου μεγέθους εταιρειών και το 65% (από 64%) των νοικοκυριών, δεν αντιμετώπισε κάποιο πρόβλημα ασφάλειας κατά τη διάρκεια της προηγούμενης χρονιάς. Είναι χαρακτηριστικό ότι μόλις το 20% των ελληνικών επιχειρήσεων με σύνδεση στο Διαδίκτυο αντιμετώπισε πρόβλημα από ιούς ή άλλα «κακοήθη» προγράμματα όταν το αντίστοιχο ποσοστό το 2006 ήταν στο 26% για τις μεγάλες και στο 23% για τις μικρές επιχειρήσεις, ενώ το 2005 τα ποσοστά είχαν φθάσει στο 51% και στο 42% αντίστοιχα. (14)

Στο βελτιωμένο επίπεδο ασφάλειας, σημαντικό ρόλο τα συστήματα προστασίας που έχουν εγκαταστήσει οι ελληνικές επιχειρήσεις. Για παράδειγμα, το 98% των μεγάλων επιχειρήσεων έχει λογισμικό ελέγχου από ιούς, ενώ το 82% διαθέτει και συστήματα προστασίας του δικτύου (π.χ. firewalls). Παράλληλα, αυξημένα είναι τα ποσοστά χρήσης ηλεκτρονικών ψηφιακών υπογραφών (13% στις μεγάλες επιχειρήσεις από 10% το 2005) και κρυπτογράφησης (12% από 9%). Εξαιρετικά μικρά είναι και τα ποσοστά των εταιρειών που αντιμετώπισαν προβλήματα με μη εξουσιοδοτημένη πρόσβαση ή απειλές στα δεδομένα και το λογισμικό της εταιρείας. (14)

Στις επιχειρήσεις με 10 και πλέον εργαζόμενους, οι περιπτώσεις μη εξουσιοδοτημένης πρόσβασης ήταν μόλις στο 2%, ενώ απειλές δέχτηκε μόλις το 1%. Τα αντίστοιχα ποσοστά στις εταιρείες με 1-9 εργαζόμενους ήταν 4% και1%.(14)

Στην περίπτωση των οικιακών χρηστών, η κατάσταση επίσης δείχνει σαφή βελτίωση δεδομένης της υψηλότερης χρήσης συστημάτων προστασίας. Για παράδειγμα, το 76% έχει πρόγραμμα προστασίας από ιούς, το 36% firewall και το 29% λογισμικό προστασίας από spyware. Τα ποσοστά είναι υψηλότερα σε άτομα ηλικίας 16 - 24 ετών. Το αποτέλεσμα είναι η σημαντική μείωση των προβλημάτων. Έτσι, μόλις το 25% αντιμετώπισε πρόβλημα με ιούς (έναντι 27% το 2006 και 33% το 2005), ενώ το spam email ήταν στο 14%, παρουσιάζοντας ελαφρά αύξηση σε σχέση με το 12% του 2006 αλλά σημαντική μείωση σε σχέση με το 21% του 2005. (14)

Σε πολύ χαμηλά επίπεδα κινήθηκε και το ποσοστό των νοικοκυριών με σύνδεση στο Διαδίκτυο που αντιμετώπισαν σημαντικότερα προβλήματα ασφάλειας. Συγκεκριμένα, περιπτώσεις παράνομης πρόσβασης σε προσωπικά δεδομένα, υπήρξαν μόλις στο 3% των νοικοκυριών, απώλεια χρημάτων παρατηρήθηκε στο 1%, ενώ στο 1% ήταν και οι απάτες με πιστωτικές κάρτες. (14)

3. Η ΕΠΙΔΡΑΣΗ ΤΩΝ ΙΩΝ ΣΤΙΣ ΕΠΙΧΕΙΡΗΣΕΙΣ

3.1. Επιχειρήσεις και Ιοί Υπολογιστών

Η ύπαρξη ιών υπολογιστών αποτελεί σοβαρή ανησυχία για τις περισσότερες σύγχρονες επιχειρήσεις. Η προσβολή ενός υπολογιστή σε μία επιχείρηση από ιό είναι σοβαρό περιστατικό ασφαλείας και για την πρόληψη τέτοιων περιστατικών ασφαλείας επενδύονται εκατομμύρια. Αξιοσημείωτο όμως είναι το γεγονός ότι παρά τις επενδύσεις που πραγματοποιούν οι επιχειρήσεις ουδέποτε είναι σε θέση να πιστοποιήσουν ότι είναι απόλυτα ασφαλείς από ιούς. Αυτό συμβαίνει ουσιαστικά γιατί δεν υπάρχει μέτρο που να προσφέρει απόλυτη ασφάλεια από ιούς. Για αυτό ακριβώς τον λόγο, πέρα από τις επενδύσεις που γίνονται για πρόληψη από ιούς, γίνεται προσπάθεια για τη δημιουργία ενεργειών που εφαρμόζονται σε περίπτωση που ένα περιστατικό ασφαλείας σχετικό με ιούς είναι γεγονός. Αυτές οι ενέργιες εξασφαλίζουν την ομαλή συνέχιση των λειτουργιών της επιχείρησης μετά το περιστατικό ασφαλείας και μειώνουν τις πιθανές ζημίες που προκύπτουν από αυτά τα περιστατικά.

Οι επενδύσεις για πρόληψη περιστατικών ασφαλείας που αφορούν ιούς ηλεκτρονικούς υπολογιστών ανέρχονται σε εκατομμύρια. Μία τέτοια επένδυση περιλαμβάνει αγορά κατάλληλου λογισμικού, ανθρώπινους πόρους για διαχείριση του λογισμικού και έξοδα συντήρησης. Οι καθαρά κερδισμένοι από αυτές τις επενδύσεις είναι οι εταιρείες που παρέχουν αυτού του είδους λογισμικό και τεχνική υποστήριξη.

Οι εταιρείες παροχής συστημάτων προστασίας από ηλεκτρονικούς υπολογιστές εκμεταλλεύονται την άλλοτε επιθυμία και άλλοτε υποχρέωση των επιχειρήσεων να διασφαλίσουν την ασφάλεια των συστημάτων τους και προσφέρουν διάφορες λύσεις στο πρόβλημα των ιών υπολογιστών. Συνήθως αυτές οι λύσεις είναι συνδρομητικές, διότι τα προϊόντα πρέπει να ενημερώνονται καθημερινά με τις υπογραφές των νέων ιών. Επιπλέον, τα εταιρικά πακέτα προσφέρουν υποστήριξη στις εταιρείες στην περίπτωση που κάποιος άγνωστος (ιός που δεν έχει εντοπιστεί από το προστατευτικό σύστημα της εταιρείας) έχει “εισβάλει” στα υπολογιστικά της συστήματα.

Είναι όμως γενικά αποδεκτό ότι κανένα προϊόν δεν μπορεί να προσφέρει απόλυτη ασφάλεια από τη δράση των ιών υπολογιστών.

Μία τέτοια έρευνα έχει παρουσιαστεί στο προηγούμενο κεφάλαιο: κανένα αντιβιοτικό πρόγραμμα δεν ήταν ικανό να εντοπίσει όλους τους υπό εξέταση ιούς. Αυτό έχει οδηγήσει τις επιχειρήσεις στο να σχεδιάσουν πλάνα ανάκαμψης σε περίπτωση κάποιου περιστατικού ασφαλείας.

Τα πλάνα ανάκαμψης περιλαμβάνουν άμεσες ενέργειες στη περίπτωση που κάποιο περιστατικό ασφαλείας είναι πλέον γεγονός. Τέτοια πλάνα ανάκαμψης

αποτελούν και τον σωστό τρόπο αντιμετώπισης περιστατικών ασφαλείας διότι είναι αναπόφευκτο για μία εταιρεία να μην έρθει αντιμέτωπη με ένα περιστατικό ασφαλείας όπως η προσβολή ενός υπολογιστή από ηλεκτρονικό ιό. Ακριβώς για αυτό τον λόγο είναι σύνηθες φαινόμενο οι δραστηριότητες που πρέπει να εκτελεστούν μετά από ένα τέτοιο περιστατικό να περιλαμβάνονται στα σχέδια ανάκαμψης των εταιρειών.
Παρόλα τα μέτρα προστασίας από ιούς υπολογιστών που λαμβάνουν οι επιχειρήσεις και τα εκατομμύρια που επενδύονται για το σκοπό αυτό, η προσβολή ενός εταιρικού δικτύου ηλεκτρονικών υπολογιστών από κάποιο ιό υπολογιστή δύναται να προκαλέσει ανυπολόγιστες ζημίες.
Καταρχήν πλήττεται η αξιοπιστία της επιχείρησης και κατ' επέκταση χάνεται η σχέση εμπιστοσύνης των πελατών με την εταιρεία. Προφανώς αυτό μπορεί να οδηγήσει σε μείωση του αριθμού των πελατών της εταιρείας, αφού μετά από ένα τέτοιο συμβάν οι πελάτες μπορεί να στραφούν στον ανταγωνισμό. Η σχέση εμπιστοσύνης που κτίστηκε μετά από πολύ κόπο και χρόνο μπορεί να χαλάσει σε μια μόνο στιγμή.
Άμεσο κόστος για την επιχείρηση αποτελούν οι επιπλέον πόροι που απαιτούνται για την αντιμετώπιση του περιστατικού. Μετά από ένα περιστατικό συνήθως απαιτούνται επιπλέον ώρες εργασίας για την αντιμετώπιση του γεγονότος. Για παράδειγμα, είναι απαραίτητο να διασφαλιστεί η ακεραιότητα των δεδομένων που πιθανώς να κατάστρεψε ή τροποποίησε ο ιός με την επαναφορά τους από αντίγραφα ασφαλείας. Επιπλέον υπάρχει μεγάλη πιθανότητα κάποιοι σταθμοί εργασίας να τεθούν εκτός λειτουργίας οπότε δημιουργείται άμεσα επιπρόσθετος φόρτος εργασίας στις υπόλοιπες μονάδες εργασίες. Πέραν τούτων, είναι πολύ πιθανόν να χρειαστεί να διατεθούν επιπλέον χρηματικά ποσά για εξωτερικούς συμβούλους και τεχνική υποστήριξη από τον συνεργάτη της εταιρείας στα θέματα ασφαλείας. Αυτό συμβαίνει συνήθως σε επιχειρήσεις που διαχωρίζονται κρίσιμα δεδομένα και πληροφορίες: προσωπικά δεδομένα, τραπεζικές εντολές, λογαριασμούς πελατών κ.τ.λ.

3.2. **Πειρατικό Λογισμικό και Επιχειρήσεις**

Οι μικρομεσαίες επιχειρήσεις αγνοούν τους πραγματικούς κινδύνους που κρύβει το πειρατικό λογισμικό:

- 1 στους 5 ερωτηθέντες πιστεύει ότι δεν κινδυνεύει από τη χρήση λογισμικού χωρίς νόμιμη άδεια
- Το 87% δεν συνειδητοποιεί ότι το παράνομο λογισμικό κάνει τους υπολογιστές τους πιο ευάλωτους σε ιούς. (12)

- Λιγότερο από το 50% των μικρομεσαίων επιχειρήσεων (ΜΜΕ) δήλωναν απόλυτα βέβαιοι ότι τα προγράμματα λογισμικού είχαν όλες τις νόμιμες άδειες. (12)
- Το 97% έκρινε ότι η χρήση παλαιών εκδόσεων λογισμικού δεν επιφέρει προβλήματα παρότι δεν μπορούν να πραγματοποιήσουν αναβάθμιση λόγω των παράνομων εκδόσεων. (12)

Μια ανεξάρτητη στατιστική μελέτη που πραγματοποιήθηκε από την Business Software Alliance (BSA) καταδεικνύει ότι ενώ η πλειοψηφία των ΜΜΕ αναγνωρίζει τα οφέλη που προσφέρει η τεχνολογία στην λειτουργία μιας επιχείρησης, εκείνοι που αγνοούν το γεγονός ότι το παράνομο λογισμικό μπορεί να αποτελέσει σημαντική απειλή, θέτουν σε κίνδυνο την ομαλή λειτουργία και τη φήμη της επιχείρησης τους. Το θέμα της «παραβίασης της πνευματικής ιδιοκτησίας του λογισμικού» σε συνάρτηση με τους τεχνικούς κινδύνους κρίθηκε ως το λιγότερο σημαντικό, ενώ στην ουσία το παράνομο λογισμικό αποτελεί σημαντικό κίνδυνο για την υπόσταση της επιχείρησης. Άλλα προβλήματα που κρίθηκαν πολύ σημαντικά από τη χρήση πειρατικού λογισμικού είναι η «απώλεια αρχείων ή συστημάτων», «οι ιοί, τα trojans και το κακόβουλο λογισμικό». Οι δύο πιο συχνά αναφερόμενες κατηγορίες κινδύνων είναι οι «ποινικές κυρώσεις» (23%) και τα «οικονομικά πρόστιμα» (21%). Στην ελληνική πραγματικότητα, το νομοσχέδιο (ν. 3524/07) που ψηφίστηκε φέτος προβλέπει την επιβολή διοικητικού προστίμου 1,000 € για κάθε ένα πρόγραμμα που είναι παράνομα εγκατεστημένο σε Η/Υ, το οποίο ακόμη και για μια μικρή εταιρία 5-10 υπαλλήλων, μεταφράζεται σε αρκετές χιλιάδες ευρώ.

Οι ΜΜΕ πρέπει να κατανοήσουν ότι οι κίνδυνοι που συνεπάγονται του παράνομου λογισμικού περιλαμβάνουν τεχνολογικά και λειτουργικά προβλήματα και φυσικά οικονομικές και νομικές κυρώσεις. Κατά μέσο όρο, οι ευρωπαϊκές ΜΜΕ αντιμετώπισαν πρόστιμα άνω των 15.940 € ανά επιχείρηση για τη χρήση πειρατικών προγραμμάτων, ενώ οι ελληνικές επιχειρήσεις κατέβαλαν φέτος στις εταιρίες-μέλη της BSA συνολικά 162.000 € ως αποζημίωση για χρήση παράνομου λογισμικού, έπειτα από ελέγχους που βασίστηκαν σε ανώνυμες καταγγελίες. Το πειρατικά προγράμματα που λαμβάνουν οι υπάλληλοι των επιχειρήσεων από ηλεκτρονικές δημοπρασίες ή ιστοσελίδες P2P συχνά περιέχουν ιούς και κακόβουλο λογισμικό. Σε πρόσφατη έρευνα της IDC βρέθηκε ότι οι πιθανότητες να αγοράσει κανείς νόμιμο λογισμικό από ιστοσελίδα δημοπρασιών είναι λιγότερες από 50% (1), ενώ στην τελευταία έκθεση της Symantec «Internet Security Threat Report» (2) αναφέρεται ότι κατά το 2006, το 47% του κακόβουλου λογισμικού (malicious code) διαδόθηκε μέσω δικτύων P2P. Με βάση πραγματικά παραδείγματα, τα κόστη που προκύπτουν από την παραβίαση

ασφαλείας σε ένα σύστημα ανέρχονται κατά μέσο όρο σε 3,8 εκατομμύρια €, επομένως είναι ξεκάθαρο ότι οι οικονομικές επιπτώσεις αποτελούν ένα σοβαρό πλήγμα για τα οικονομικά μιας επιχείρησης. Παρόλα αυτά, ο πανευρωπαϊκός δείκτης πειρατείας λογισμικού για το 2006 ανήλθε στο 35% (4). Τα αντίγραφα των προγραμμάτων που δεν φέρουν τις νόμιμες άδειες χρήσης, και το λογισμικό που έχει μεταφορτωθεί από μη εγκεκριμένους προμηθευτές, εκθέτουν τις επιχειρήσεις σε πολλαπλούς κινδύνους. Επίσης ανησυχητικό είναι το συμπέρασμα ότι σχεδόν το 50% των ερωτηθέντων είναι πεπεισμένοι πως το λογισμικό τους είναι νόμιμο και συνεπώς αγνοούν το ρίσκο που διατρέχουν. Το πειρατικό λογισμικό δεν δικαιούται την ίδια τεχνική υποστήριξη ή αναβαθμίσεις, όπως τα νόμιμα προγράμματα, επομένως μια επιχείρηση διακυβεύει την ασφάλεια των συστημάτων της και πιθανώς τίθεται σε μειονεκτική θέση απέναντι στους ανταγωνιστές της. Απλές διαδικασίες όπως η εφαρμογή τακτικών ελέγχων, η εφαρμογή πολιτικών χρήσης λογισμικού από τους εργαζόμενους και η διαχείριση πόρων λογισμικού μπορούν εξασφαλίζουν στον επιχειρηματία ασφάλεια, βέλτιστη απόδοση και παραγωγικότητα της εταιρείας του.

Πραγματοποιήθηκε επίσης τηλεφωνική έρευνα από την Gfk NOP εκ μέρους της BSA σε 1,800 ευρωπαϊκές μικρομεσαίες επιχειρήσεις και συγκεκριμένα στην Αγγλία, Γαλλία, Γερμανία, Ολλανδία, Ιταλία, Ισπανία, Ρωσία, Πολωνία και Ουγγαρία. Επίσης διεξήχθησαν 200 συνεντεύξεις σε κάθε χώρα. Για τους σκοπούς της έρευνας, ως ΜΜΕ θεωρήθηκαν οι επιχειρήσεις που απασχολούν από 10 έως και 250 υπαλλήλους. Τα δείγματα ελήφθησαν τυχαία από κάθε χώρα βάσει αρχείων δεδομένων.
Πραγματοποιήθηκαν 100 συνεντεύξεις σε επιχειρήσεις που απασχολούν 10-99 στελέχη και 100 σε επιχειρήσεις που απασχολούν 100-250 στελέχη, Όπου αναφέρονται στοιχεία για την Ευρώπη και την Κεντρική Ανατολική Ευρώπη (εξαιρέθηκε η Ρωσία).

3.3. **Μελέτες Περιπτώσεων**

3.3.1. **Η Απάτη των** Dialer

Μια από τις μεγαλύτερες επιχειρήσεις στην Ελλάδα, ο ΟΤΕ, βρέθηκε εκτεθειμένος ως αποτέλεσμα μιας υπόθεσης σχετικής με ιούς υπολογιστών. Σύμφωνα με τις πρώτες εκτιμήσεις του Τμήματος Δίωξης Ηλεκτρονικού Εγκλήματος της Ασφάλειας Αττικής και του ΟΤΕ, τα θύματα της απάτης των dialer ξεπερνούν τις 10.000, ενώ μόνο στην Ελλάδα εντοπίσθηκαν περισσότερες από 1.000 ύποπτες ιστοσελίδες που είναι πολύ πιθανόν να

σχετίζονται με την απάτη αυτή. Η απάτη λειτουργεί ως εξής: Μια ιστοσελίδα δελεάζει τον επισκέπτη, συνήθως με ανακοινώσεις για γυμνές φωτογραφίες επώνυμων γυναικών ή για videos on-line ή και με κάτι άλλο, οι οποίες υπηρεσίες μάλιστα διαφημίζονται έντονα και τονίζεται ότι παρέχονται δωρεάν. Μόλις ο χρήστης κάνει κλικ σ' ένα συγκεκριμένο σημείο, εγκαθίσταται αυτόματα στον υπολογιστή του και χωρίς αυτός να το γνωρίζει, ένα ειδικό πρόγραμμα («πρόγραμμα-τσούχτρα») με αποτέλεσμα αντί για αστική κλήση στον τοπικό provider να γίνεται εκτροπή και διεθνής κλήση σύνδεσης και μάλιστα υπερπόντια, με πολλαπλάσιο φυσικά κόστος. Για παράδειγμα, ο χρήστης αντί για 0,17 – 0,35 € την ώρα, χρεώνεται με 2,50 € ανά λεπτό. Οι δημιουργοί παρόμοιων ιστοσελίδων έχουν κάνει συμβάσεις με τους τηλεπικοινωνιακούς οργανισμούς των χωρών αυτών και μοιράζονται τα κέρδη από τις υπέρογκες χρεώσεις των ανυποψίαστων χρηστών.
Οι τηλεφωνικές εταιρείες ισχυρίζονται ότι δεν φέρουν καμία ευθύνη για τις υποθέσεις αυτές και ότι η μόνη παραχώρηση που μπορούν να κάνουν προς τους παθόντες είναι να αποπληρώσουν οι τελευταίοι τα χρέη τους σε δόσεις. Η μόνη αντιμετώπιση και πρόληψη της μάστιγας αυτής που χρεώνει υπέρογκα τους λογαριασμούς των ανυποψίαστων χρηστών είναι η προσοχή και η εγρήγορση των ίδιων των χρηστών. Η καλύτερη προστασία είναι η εγκατάσταση φραγής των διεθνών τηλεφωνικών κλήσεων ή η προμήθεια και εγκατάσταση ειδικής συσκευής *AntiDialer*, η οποία παρεμβάλλεται ανάμεσα στην τηλεφωνική γραμμή και την συσκευή modem του υπολογιστή του χρήστη και επιτρέπει να γίνονται κλήσεις μόνο προς συγκεκριμένο αριθμό ΕΠΑΚ.
Για τις υπερβολικές αυτές χρεώσεις, ο ΟΤΕ δεν φέρει καμία ευθύνη και συμβουλεύει τους dial up χρήστες τα εξής:

- Να μην μεταφορτώνουν (download) προγράμματα στους υπολογιστές τους από ιστοσελίδες άγνωστης ή αμφίβολης προέλευσης.
- Να αποσυνδέονται από το διαδίκτυο όταν δεν το χρησιμοποιούν.
- Να χρησιμοποιούν την υπηρεσία φραγής των εξερχόμενων διεθνών τηλεφωνικών κλήσεων.
- Να μην επιτρέπουν τη χρήση του υπολογιστή για σύνδεση στο διαδίκτυο από τρίτους, στο σπίτι ή στον χώρο εργασίας τους.

3.3.2. **Επιθέσεις** DoS & DDoS

Οι επιθέσεις του τύπου DoS (Denial of Service), που είναι γνωστές και ως επιθέσεις άρνησης υπηρεσίας, αποτελούν μια από τις σοβαρότερες επιθέσεις που μπορούν να εκδηλωθούν σ' ένα web site ή σ' ένα δίκτυο υπολογιστών. Οι επιθέσεις αυτές είναι καταστροφικές για τις εταιρείες και έχουν μεγάλο οικονομικό κόστος. Το κόστος αφορά τις χαμένες ώρες λειτουργίας μιας

επιχείρησης, αλλά και στο κόστος που απαιτείται για τον εντοπισμό και την αντιμετώπιση αυτών των επιθέσεων. Ουσιαστικά μια τέτοια επίθεση έχει ως αποτέλεσμα την αδυναμία της εταιρείας να εξυπηρετήσει τους πελάτες της. Η επίθεση συνίσταται στην εκδήλωση χιλιάδων αιτήσεων σύνδεσης σ' έναν server και σε διάστημα μερικών ημερών, με απώτερο στόχο την κατάρρευση του server από την αδυναμία του να ανταποκριθεί σ' έναν τόσο μεγάλο αριθμό αιτήσεων

Τελευταία έχουν αρχίσει να κάνουν την εμφάνισή τους και οι λεγόμενες *κατανεμημένες επιθέσεις άρνησης υπηρεσίας*, γνωστές με τον όρο *DDoS (Distributed Denial of Service).* Σύμφωνα με το σενάριο, κάποια συγκεκριμένη ημερομηνία, προγράμματα τύπου worm που μέχρι τότε περίμεναν σιωπηρά στα μηχανήματα όπου φιλοξενούνταν, ξαφνικά ενεργοποιούνται και αρχίζουν όλα μαζί να στέλνουν αιτήσεις σύνδεσης σ' έναν συγκεκριμένο server. Ο server δέχεται τόσες πολλές αιτήσεις που αδυνατεί να ανταποκριθεί σ' όλες και αναπόφευκτα καταρρέει. Πρόκειται για μια εξελιγμένη μορφή των επιθέσεων του τύπου DoS, οι οποίες είναι πιο αποτελεσματικές όσον αφορά τα καταστροφικά αποτελέσματα που επιφέρουν, καθώς η επίθεση πραγματοποιείται από πολλά σημεία ταυτόχρονα.

Ένα χαρακτηριστικό παράδειγμα είναι η περίπτωση του worm Mydoom για τον οποίο υπολογίζεται ότι το έμμεσο και άμεσο κόστος από την επίδραση του ανέρχεται σε 250 εκατομμύρια δολάρια.

Για τη διάδοση του worm Mydoom χρησιμοποιήθηκε η γνωστή σε όλους υπηρεσία ηλεκτρονικού ταχυδρομείου (e-mail). Υπολογίζεται ότι μόνο λίγες μέρες μετά την κυκλοφορία του είχαν επηρεαστεί περισσότερα από ένα εκατομμύριο υπολογιστές. Η διάδοση είχε γίνει σε τόσο γρήγορους ρυθμούς που προκάλεσε μεγάλη επιβάρυνση στο διαδίκτυο. Είναι αξιοσημείωτο ότι κατά τις μέρες αναπαραγωγής του ιού ο χρόνος φόρτωσης ιστοσελίδων είχε διπλασιαστεί. Το worm είχε προγραμματιστεί να στείλει μαζικά αιτήσεις συνδέσεις στην ιστοσελίδα www.sco.com τη 1η Φεβρουαρίου 2004. Η εταιρεία αναγκάστηκε να αλλάξει διεύθυνση πριν την μέρα ενεργοποίησης του worm για να μειώσει τις πιθανές ζημιές από την επίθεση και επικήρυξε το δημιουργό του worm για 250000 δολάρια. Ο δημιουργός του worm Mydoom παραμένει ακόμη άγνωστος. Είναι γνωστό μόνο ότι η επίθεση ξεκίνησε από τη Ρωσία.

3.3.3. ***Οι* Φάρσες Ιών** (Virus Hoaxes)

Οι φάρσες ιών, που διαδίδουν πολλοί χρήστες του διαδικτύου μέσω ηλεκτρονικού ταχυδρομείου είναι αρκετά συνηθισμένες και μπορούν να δημιουργήσουν κι αυτές πολλά προβλήματα. Πρόκειται για αναφορές σε ανύπαρκτους ιούς, όπου υποτίθεται ότι το μήνυμα το στέλνει μια μεγάλη

εταιρεία και μας προειδοποιεί για έναν νέο μη αντιμετωπίσιμο καταστροφικό ιό.
Το πρόβλημα με τις φάρσες ιών είναι ότι αν όλοι οι χρήστες που λαμβάνουν ένα τέτοιο μήνυμα το προωθήσουν σ' όσους βρίσκονται στο βιβλίο διευθύνσεών τους (address book), θα δημιουργηθεί υπερφόρτωση του δικτύου από καταιγισμό μηνυμάτων. Σημειώστε ότι η υπερφόρτωση του δικτύου πολλές φορές κοστίζει εκατομμύρια.
Ένας άλλος κίνδυνος είναι ότι αφού καταλαγιάσει ο θόρυβος για μια φάρσα ιού, υπάρχει το ενδεχόμενο να κάνει την εμφάνισή του ένας πραγματικός ιός με το ίδιο όνομα, όπως πράγματι συνέβη με τον ιό *Good Times*, που εμφανίσθηκε ως φάρσα και αργότερα και ως κανονικός ιός. Ο καλύτερος τρόπος για να αντιμετωπισθούν οι φάρσες και όλα τα ύποπτα και άγνωστα μηνύματα e-mail, είναι να προωθούνται στον αρμόδιο τεχνικό υπάλληλο μιας εταιρείας, ο οποίος θα είναι και ο μόνος υπεύθυνος για να αποφασίσει τι πρέπει να γίνει. Ενημέρωση σχετικά με τις φάρσες των ιών υπολογιστών υπάρχει στην εξής διεύθυνση : http://www.vmyths.com.

3.3.4. **Τα Προγράμματα** Spyware **και** Adware

Πολλοί συγκαταλέγουν τα προγράμματα spywares και adwares στην κατηγορία των ιών. Γι' αυτό άλλωστε τα αντιιοτικά προγράμματα εντοπίζουν τέτοια προγράμματα ως ιομορφικό λογισμικό.
Όπως ήδη γνωρίζουμε, με τα cookies ένας δικτυακός τόπος μπορεί να εξάγει χρήσιμα στατιστικά συμπεράσματα σ' ότι έχει να κάνει μόνο με τις δικές του ιστοσελίδες. Ποια εταιρεία, όμως, δεν θα ήθελε να γνωρίζει ποιους δικτυακούς τόπους προτιμούν να επισκέπτονται οι χρήστες και τι ακριβώς βλέπουν; Οι πληροφορίες αυτές είναι πολύτιμες στις εταιρείες, ώστε να μπορέσουν να προωθήσουν σωστά τα προϊόντα τους, να δημιουργήσουν καινούργια προϊόντα ή υπηρεσίες, να στήσουν ηλεκτρονικά καταστήματα (e-shops) κ.ά. Προς τον σκοπό αυτό δημιουργήθηκαν διάφορα προγράμματα, τα αποκαλούμενα *spyware,* τα οποία εγκαθίστανται αυτόκλητα στον υπολογιστή μας, δηλ. χωρίς εμείς να έχουμε ζητήσει κάτι τέτοιο, και παρακολουθούν συνεχώς και αδιαλείπτως όλες τις κινήσεις και τις προτιμήσεις μας στο Internet, ενημερώνοντας κατάλληλα τους δημιουργούς τους.
Με άλλα λόγια, η βασική αποστολή των προγραμμάτων spyware είναι να μας κατασκοπεύουν, εν αγνοία μας φυσικά. Εκτός, όμως από την κατασκοπεία μπορεί να εμφανίζουν διάφορα διαφημιστικά μηνύματα, συνήθως σε ανεξάρτητα παράθυρα, τα λεγόμενα *pop-ups,* όπου το περιεχόμενο της διαφήμισης προσαρμόζεται αυτόματα στις προτιμήσεις του χρήστη-καταναλωτή. Αυτά τα προγράμματα αποκαλούνται πιο συγκεκριμένα *adware.*
Τα προγράμματα spyware και adware εγκαθίστανται συνήθως μαζί μ' άλλα

προγράμματα που προσφέρονται δωρεάν (freeware). Στην πράξη πάντως δεν υπάρχει σαφής διαχωρισμός μεταξύ των προγραμμάτων spyware και adware. Έτσι λοιπόν, ένα πρόγραμμα spyware μπορεί να εμφανίζει και διαφημιστικά μηνύματα, ενώ ένα πρόγραμμα adware μπορεί να παρακολουθεί τις κινήσεις μας και να στέλνει προσωπικά μας στοιχεία σε τρίτους. Συνήθως, τα προγράμματα αυτού του τύπου εξυπηρετούν διαφημιστικούς σκοπούς είτε από τις ίδιες τις ενδιαφερόμενες εταιρείες είτε από εταιρείες που εξυπηρετούν άλλες εταιρείες στις οποίες πωλούν τις πληροφορίες που συγκεντρώνουν.
Επειδή δεν μπορούμε να γνωρίζουμε αν τα προγράμματα αυτά απλά καταγράφουν τις κινήσεις μας στο διαδίκτυο και αλιεύουν έτσι τις καταναλωτικές μας συνήθειες ή αν, επιπλέον, μεταδίδουν προσωπικά μας δεδομένα (όπως είναι οι αριθμοί τραπεζικών λογαριασμών και πιστωτικών καρτών) καλό θα ήταν να φροντίσουμε να απαλλαγούμε απ' αυτά.
Η Αμερικανική Επιτροπή Ομοσπονδιακού Εμπορίου επενέβη και ζήτησε από το αρμόδιο δικαστήριο να εμποδίσει την πώληση του προγράμματος με το όνομα *Spyware Assassin*, το οποίο διαφημιζόταν σε banners ιστοσελίδων και εμφάνιζε απατηλές προειδοποιήσεις για δήθεν ύπαρξη προγραμμάτων spyware στον υπολογιστή του χρήστη. Στην πραγματικότητα και τα προειδοποιητικά μηνύματα ήταν ψευδή και το πρόγραμμα ανίκανο να απαλλάξει τους χρήστες από κατασκοπευτικά προγράμματα spyware.

3.3.5. Τα **προγράμματα εξαπάτησης** Hijacks

Τελευταία έχουν κάνει την εμφάνισή τους και προγράμματα που αλλάζουν την αρχική σελίδα (Home Page) του φυλλομετρητή Internet Explorer ενός υπολογιστή, χωρίς φυσικά την συγκατάθεση του χρήστη. Τα προγράμματα αυτά είναι γνωστά με τον όρο *Hijack* και ο απώτερος στόχος τους είναι να κάνουν γνωστές συγκεκριμένες ιστοσελίδες ή να διαφημίσουν προϊόντα και υπηρεσίες.
Υπάρχει και το ενδεχόμενο με τις ενέργειές τους αυτές να αυξάνουν τον αριθμό των επισκέψεων συγκεκριμένων ιστοσελίδων, ούτως ώστε οι κάτοχοι των ιστοσελίδων αυτών να μπορούν να προσελκύσουν περισσότερες και καλύτερα αμειβόμενες διαφημίσεις. Έλαβαν το όνομα *hijack* (αεροπειρατεία) καθώς εγκαθίστανται στον υπολογιστή μας χωρίς να το αντιληφθούμε και υποχρεώνουν το πρόγραμμα πλοήγησης που χρησιμοποιούμε να μεταβεί στις ιστοσελίδες που αυτά θέλουν. Τα προγράμματα hijack συνήθως δεν προκαλούν ζημιές, απλά είναι ενοχλητικές οι ενέργειές τους. Η απεγκατάστασή τους είναι συνήθως μια χρονοβόρα διαδικασία καθώς δημιουργούν πολλές φορές καταχωρήσεις και στο Μητρώο (Registry) των Windows.

4. **ΕΠΙΛΟΓΟΣ**

Στη σύγχρονη εποχή των τεχνολογικών αλμάτων και του διαδικτύου, το λογισμικό άλλαξε την καθημερινότητα εκατομμυρίων ανθρώπων παγκοσμίως. Από το λογιστή ως το μουσικοσυνθέτη και από τον αρχιτέκτονα μέχρι τον υπάλληλο του Δημοσίου, το λογισμικό αποτελεί το σημαντικότερο εργαλείο παραγωγής έργου.

Η εποχή της πληροφορίας χαρακτηρίζεται από την εξάπλωση των πληροφοριακών συστημάτων και την αυξημένη δυνατότητα για ταχεία συλλογή, αφομοίωση, επεξεργασία και διάδοση πληροφοριών.

Σήμερα, εκείνοι οι οποίοι έχουν πρόσβαση σε συστήματα πληροφοριών ή στον έλεγχο αυτών, μπορούν άμεσα να επηρεάζουν την κοινή γνώμη, το διεθνές εμπόριο, τον πολιτικό διάλογο και άλλα θέματα τα οποία επηρεάζουν την ασφάλεια. Η επίδραση της εποχής της πληροφορίας στις στρατιωτικές επιχειρήσεις έχει προκαλέσει επαναστατικές αλλαγές στον τρόπο που οι σύγχρονοι στρατοί διεξάγουν επιχειρήσεις και στην φύση των ίδιων των εχθροπραξιών.

Οι ιοί των υπολογιστών (computer viruses) από τη μια μεριά μας δείχνουν το πόσο ευπρόσβλητοι είμαστε, καθώς ένας κατάλληλα φτιαγμένος ιός μπορεί να έχει μια τρομακτική επίδραση στο διαδίκτυο. Από την άλλη μεριά, μας δείχνουν πόσο αλληλοσυνδεόμενες έχουν γίνει οι ανθρώπινες κοινωνίες.

Αξίζει να αναφέρουμε ότι ένας στους δέκα χρήστες του διαδικτύου έχει πέσει θύμα online απάτης τον περασμένο χρόνο, χάνοντας κατά μέσο όρο σχεδόν 2000 ευρώ έκαστος. Μάλιστα, όπως αναφέρει έρευνα, ανάμεσα τους συγκαταλέγονται και αρκετά έμπειροι χρήστες του διαδικτύου. Στο σύνολο της έρευνας καταγράφεται ότι το 6% των χρηστών έχει πέσει θύμα απάτης από ηλεκτρονικές αγορές, 4% έχει πέσει θύμα γενικευμένης απάτης και το 3% έχει εξαπατηθεί από τραπεζικές συναλλαγές μέσω διαδικτύου. Ωστόσο παρατηρείται ότι, παρά τα αυξημένα ποσοστά online απάτης, οι χρήστες του διαδικτύου εξακολουθούν να αδυνατούν να λάβουν τα απαραίτητα μέτρα προστασίας όταν είναι συνδεδεμένοι, ενώ λιγότεροι από τους μισούς θεωρούν ότι φέρουν ακέραια την ευθύνη της ασφάλειας των συναλλαγών τους.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Πηγή OTENET

http://www.otenet.gr/portal/portal/info/technology/security_protection?media-type=html&user=anon&js_panename=security_protection&action=portlets.PsmlPortletAction&eventsubmit_doview=342787

2. Πηγή ΕΕΧΙ

http://www.otenet.gr/portal/portal/info/technology/security_protection;jsessionid=556C46E561067556B1ED7D4583481374.tomcat2?media-type=html&user=anon&js_panename=security_protection&action=portlets.PsmlPortletAction&eventsubmit_doview=303852&category=security_protection

3. Πηγή: UsaToday

http://www.e-pcmag.gr/modules/news/article.php?storyid=210

4. Πηγή ΕΕΧΙ

http://www.otenet.gr/portal/portal/info/technology/security_protection?media-type=html&user=anon&js_panename=security_protection&action=portlets.PsmlPortletAction&eventsubmit_doview=303851&category=security_protection

5. Βιβλίο «Ασφάλεια Πληροφοριακών Συστημάτων» - Κεφ. 8, Εκδόσεις Νέων Τεχνολογιών, Επιστημονική Επιμέλεια: Σωκρ. Κάτσικας-Δημ. Γκρίτζαλης-Στέφ. Γκρίτζαλης

Αλεξανδρής Ν.Γκρίτζαλης Δ. Κιουντούζης Ε. Μια προσέγγιση της κοινωνικά αποδεκτής αξιοποίησης της Πληροφορικής σε ΕΠΥ, Ασφάλεια Πληροφοριών Τεχνικά , Νομικά και Κοινωνικά Θέματα, Αθήνα 1995, σελίδα 381 επ.
Άνθιμου Κ. Το δικαίωμα πληροφοριακού αυτοκαθορισμού του ατόμου ως έκφανση του δικαιώματος επί της προσωπικότητας , ΚριτΕ 1998, σελ.155 επ.}

Αραβαντινός Β. Η προστασία των στοιχείων προσωπικού χαρακτήρα από την αθέμιτη επεξεργασία τους με ηλεκτρικό υπολογιστή , Αθήνα – Κομοτηνή 1997

Αραβαντινός Β. Εισαγωγή στη Νομοπληροφορική και τη Δικαιοκυβερνητική , τόμος 1ος , Νομοπληροφορική , Αθήνα – Κομοτηνή 1994

Benabou Valerie-Laure, Should there be a minimum harmonisation of the law?, International Colloqium, Internet law- European and international approaches (Paris 2001) ,

6. http://droit-internet-2001.univ.paris1.fr/ve/page004.html

7. http://www.dart.gov.gr/?q=node/17

8. Πηγή: The Register

http://www.e-pcmag.gr/modules/news/index.php?storytopic=6&start=470

anthony@itia.ntua.gr

9. http://www.microsoft.com/hellas/athome/security/viruses/intro_viruses_what.mspx

10. http://www.go-online.gr/ebusiness/specials/article.html?article_id=1107

11. http://www.microsoft.com/hellas/athome/security/spyware/software/about/productcomparisons.mspx

12. http://w3.bsa.org/hellas/press/newsreleases/greece_release_2007_06_14_01.cfm

13. http://www.tech-faq.com/ylang/el/why-computer-viruses.shtml

14. http://www.imerisia.gr/article.asp?catid=4776&subid=2&tag=4417&pubid=1295132

15. http://find.in.gr/result.asp?q=%F0%F1%EF%E2%EB%E7%EC%E1%F4%E1+%E5%F0%E9%F7%E5%E9%F1%E7%F3%E5%F9%ED+%E1%F0%EF+%E9%EF%F5%F2

16. http://money.cnn.com/2004/01/28/technology/mydoom_costs/index.htm

17.
http://www.microsoft.com/hellas/athome/security/viruses/virus101.mspx

18.
http://el.wikipedia.org/wiki/%CE%99%CF%8C%CF%82_(%CF%80%CE%BB%CE%B7%CF%81%CE%BF%CF%86%CE%BF%CF%81%CE%B9%CE%BA%CE%AE)

19. http://dide.flo.sch.gr/Plinet/Tutorials/Tutorials-Viruses.html

20. http://www.av-comparatives.org

21. http://www.ctg.gr/downloads.htm