ΑΣΦΑΛΕΙΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Ο **ηλεκτρονικός υπολογιστής** είναι μια μηχανή κατασκευασμένη κυρίως από ηλεκτρονικά κυκλώματα και δευτερευόντως από ηλεκτρικά και μηχανικά συστήματα, και έχει ως σκοπό να επεξεργάζεται πληροφορίες. Ο ηλεκτρονικός υπολογιστής είναι ένα αυτοματοποιημένο, ηλεκτρονικό, ψηφιακό επαναπρογραμματιζόμενο σύστημα γενικής χρήσης το οποίο μπορεί να επεξεργάζεται δεδομένα βάσει ενός συνόλου προκαθορισμένων οδηγιών, των εντολών που συνολικά ονομάζονται πρόγραμμα. Οι ηλεκτρονικοί υπολογιστές έχουν βελτιώσει κατά πολύ τη ζωή του ανθρώπου, που μπορεί να χρησιμοποιεί τις ποικίλες δυνατότητές τους αλλά δεν παύουν να αντιμετωπίζουν διάφορους κινδύνους τόσο εκείνοι όσο και οι χρήστες τους.
Το κυριότερο πρόβλημα που αντιμετωπίζουν οι υπολογιστές είναι οι ιοί. Οι ιοί μπορούν να χρησιμοποιηθούν στο οργανωμένο έγκλημα, κλέβοντας αριθμούς πιστωτικών καρτών, κωδικούς λογαριασμών, απόρρητα αρχεία και άλλα ψηφιακά μυστικά που αποκαλύπτουν οι χρήστες όταν κάνουν αγορές και παραγγελίες στο διαδίκτυο και επίσης μπορούν να χρησιμοποιηθούν στην κατασκοπεία και στο στρατό είτε για την καταστροφή αρχείων είτε για την συλλογή πληροφοριών.

ΤΙ ΣΥΜΒΑΙΝΕΙ ΣΤΗ ΧΩΡΑ ΜΑΣ
Η Ελλάδα καταλαμβάνει την 11^{η} θέση σε παγκόσμια κλίμακα στη λίστα με τις 20 χώρες που δέχθηκαν, σύμφωνα με την έγκυρη εταιρεία υπολογιστικών συστημάτων Symantec, τις περισσότερες επιθέσεις από ιούς υπολογιστών κατά το πρώτο εξάμηνο του έτους 2004, οπότε και καταγράφηκαν περίπου 5.500 επιθέσεις ανά 100 χιλιάδες χρήστες. 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.

ΟΙ ΙΟΙ ΤΟΥ ΥΠΟΛΟΓΙΣΤΗ
Ο ιός υπολογιστή είναι ένα πρόγραμμα συνήθως μικρό σε χωρητικότητα αλλά πολύ αποτελεσματικό σε δράση που έχει την ικανότητα να μεταδίδεται μεταξύ υπολογιστών και δικτύων και να δημιουργεί αντίγραφα του εαυτού του χωρίς φυσικά να το γνωρίζει ή να το εγκρίνει ο τελικός χρήστης. Αποκαλούνται ιοί επειδή έχουν μερικά κοινά γνωρίσματα με τους βιολογικούς ιούς. Ένας ιός υπολογιστή μεταφέρεται από υπολογιστή σε υπολογιστή και αναπαράγει τον εαυτό του όπως ένας πραγματικός ιός και μεταλλάσσεται για να μπορέσει να αποφύγει τα ηλεκτρονικά αντιβιοτικά .Ένας ιός υπολογιστή πρέπει να μεταφερθεί μέσω άλλων προγραμμάτων ή εγγράφων ώστε να μπορέσει να εκτελεσθεί. Αφού εκτελεσθεί μπορεί μετά να μολύνει άλλα προγράμματα ή και έγγραφα. Η ζημιά που κάνει ένας ιός μπορεί να κυμαίνεται από την απλή εμφάνιση ενός ενοχλητικού μηνύματος έως και την διαγραφή όλων των δεδομένων του σκληρού δίσκου του υπολογιστή που έχει μολυνθεί ή την αδυναμία εκτέλεσης κάποιων προγραμμάτων, την απρόσμενη επανεκκίνηση του υπολογιστή και πολλά άλλα.

ΟΙ ΠΡΩΤΟΙ ΕΚΤΕΛΕΣΙΜΟΙ ΙΟΙ
Οι πρώτοι ιοί υπολογιστών που εμφανίστηκαν ήταν κομμάτια κώδικα προσκολλημένα σε ένα κοινό πρόγραμμα όπως ένα δημοφιλές παιχνίδι ή ένας δημοφιλής επεξεργαστής κειμένου. Κάποιος ανυποψίαστος χρήστης μπορούσε να κατεβάσει ένα μολυσμένο παιχνίδι από ένα bulletin board και να το εκτελέσει. Αν κάποιο από τα μολυσμένα αυτά προγράμματα δοθεί σε άλλον χρήστη με μια δισκέτα

ή αν φορτωθεί σε ένα bulletin board θα μολυνθούν και άλλα προγράμματα. Αυτός είναι ο τρόπος που μεταδίδεται ένας ιός. Ο ιοί δεν θα ήταν τόσο ανεπιθύμητοι αν το μόνο που έκαναν ήταν να αναπαράγονται. Δυστυχώς οι περισσότεροι έχουν και μια τάση καταστροφής.

ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΠΑΡΑΔΕΙΓΜΑΤΑ ΙΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Ο πρώτος ιός υπολογιστή 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 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 My Doom , ο Jerk, ο Yamkee, ο Love Let –A, ο Nightshade (κλείδωνε με κωδικό τα αρχεία που δουλεύουμε όταν η ημερομηνία του υπολογιστή έδειχνε Παρασκευή και 13) κ.α.

Το 1988 ο φοιτητής Robert Morris δημιούργησε το πρώτο worm, που έφερε το όνομα του , και κατάφερε να μολύνει σχεδόν το 10% των συνδεδεμένων στο Iinternet υπολογιστών. Ο ιός Michelangelo έκανε την εμφάνιση του το 1922, 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. 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 μία 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 κόλπο 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 μία 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 Bbugbear 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 εταιρίες.

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 και την εμφάνιση του 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 χιλιάδες servers και αναστάτωσε αεροπορικές και σιδηροδρομικές εταιρείες.
Ο ιός MyDoom (Η καταδίκη μου) , 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 στάλθηκε με e-mail και ενός προγράμματος ηλεκτρονικής ανταλλαγής αρχείων κατάφερε να κερδίσει τον τίτλο ενός από τους πιο καταστροφικούς ιούς όλων των εποχών. Ο ιός αυτός δημιουργεί μία 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 εμφάνιση του ένας ιός ''νέας γενιάς'', ο Scob, ο οποίος λειτουργούσε ύπουλα και ο σκοπός του ήταν να συλλέγει αριθμούς πιστωτικών καρτών, 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 μεταπώληση τους.
Ανάλογη δουλειά με τον ιό Scob έκανε και ο ιός Mimail, ο οποίος εμφάνιζε μία φόρμα καταχώρησης στοιχείων, όπως αριθμούς πιστωτικών καρτών, και στη συνέχεια έστελνε αυτά τα δεδομένα με e-mail σε κάποιους χρήστες στη Ρωσία.

ΟΙ ΙΟΙ ΤΟΥ BOOT SECTOR

Καθώς οι δημιουργοί των ιών αποκτούσαν όλο και περισσότερη εμπειρία, μάθαιναν νέα κόλπα, ένα από τα οποία ήταν η δυνατότητα να φορτώνουν τους ιούς στη μνήμη του υπολογιστή έτσι ώστε να μπορούν να εκτελούνται στο παρασκήνιο για όσο καιρό παρέμενε ανοικτός ο υπολογιστής. Αυτό έδωσε στους ιούς έναν πολύ πιο αποδοτικό τρόπο για να αναπαράγουν τους εαυτούς τους.

Ένα άλλο κόλπο ήταν η δυνατότητα να μολύνουν τον boot sector (τομέα εκκίνησης) στις δισκέτες και τους σκληρούς δίσκους. Ο boot sector είναι ένα μικρό πρόγραμμα που αποτελεί το πρώτο τμήμα του λειτουργικού συστήματος που φορτώνει ο υπολογιστής και περιέχει ένα άλλο πολύ μικρό πρόγραμμα που λέει στον υπολογιστή το πώς να φορτώσει το υπόλοιπο μέρος του λειτουργικού συστήματος.

Τοποθετώντας τον κώδικά του στον boot sector, ένας ιός μπορεί να είναι σίγουρος ότι αυτός ο κώδικας θα εκτελεσθεί. Μπορεί να φορτωθεί στη μνήμη αμέσως και μπορεί να τρέξει οποτεδήποτε είναι ανοικτός ο υπολογιστής. Οι ιοί αυτοί μπορούν να μολύνουν τον boot sector όποιας δισκέτας τοποθετηθεί στο μηχάνημα. Σε γενικές γραμμές, και οι δύο ιοί, δηλαδή οι εκτελέσιμοι και οι boot sector, δεν αποτελούν και μεγάλες απειλές πλέον. Ο ένας λόγος είναι το μεγάλο μέγεθος των σημερινών προγραμμάτων καθώς όλα τα προγράμματα σήμερα βρίσκονται σε CD και τα CD's δεν μπορούν να τροποποιηθούν και συνεπώς να προσβληθούν από ιούς.

Οι boot sector ιοί έχουν ελαττωθεί επίσης καθώς τα λειτουργικά συστήματα είναι σε θέση να προστατεύσουν σήμερα τον boot sector. Οι δύο αυτοί τύποι ιών είναι πιθανό

να εμφανισθούν σήμερα αλλά είναι πιο σπάνιοι και δεν μπορούν να εξαπλωθούν τόσο γρήγορα όπως παλιά.

ΟΙ ΙΟΙ ΤΩΝ E-MAILS

Ο πιο πρόσφατος στον κόσμο των ιών των υπολογιστών είναι ο ιός που μεταδίδεται με την ηλεκτρονική αλληλογραφία (e-mails virus) και ο ιός *Melissa* που εμφανίστηκε τον Μάρτιο του 1999 ήταν εντυπωσιακός. Ο Melissa εξαπλώθηκε με έγγραφα του Microsoft Word που στάλθηκαν μέσω e-mail και δούλευε ως εξής : Κάποιος δημιούργησε τον ιό ως ένα έγγραφο του Word που φορτώθηκε σε μια ομάδα ειδήσεων του Internet.Όποιος κατέβαζε το έγγραφο και το άνοιγε θα ενεργοποιούσε τον ιό, ο οποίος θα έστελνε το έγγραφο (και συνεπώς και τον εαυτό του) με ένα μήνυμα e-mail στους πρώτους 50 χρήστες που υπήρχαν στο βιβλίο διευθύνσεων του μολυσμένου υπολογιστή. Το μήνυμα αυτό του e-mail περιείχε ένα φιλικό σημείωμα που εμφάνιζε το όνομα του ατόμου από το οποίο έφευγε και έτσι ο αποδέκτης θα άνοιγε το μήνυμα νομίζοντας ότι είναι αβλαβές. Ο ιός θα δημιουργούσε μετά 50 καινούργια μηνύματα από το μηχάνημα του παραλήπτη. Ως αποτέλεσμα, ο ιός Melissa ήταν ο πιο γρήγορα διαδεδομένος ιός που εμφανίσθηκε ποτέ και ανάγκασε μάλιστα πολλές μεγάλες εταιρίες να διακόψουν την ηλεκτρονική τους αλληλογραφία. Ο ιός *I Love You*, ο οποίος έκανε την εμφάνισή του στις 4 Μαΐου 2000, ήταν ακόμα πιο απλός καθώς περιείχε ένα κομμάτι κώδικα ως συνημμένο . Οι χρήστες που έκαναν διπλό κλικ στο συνημμένο, επέτρεπαν στον ιό να εκτελεσθεί. Ο κώδικας έστελνε αντίγραφα του εαυτού του σε όσους βρίσκονταν στο βιβλίο διευθύνσεων του θύματος και μετά άρχιζε να καταστρέφει αρχεία στον υπολογιστή του. Ο ιός Melissa εκμεταλλεύτηκε τη γλώσσα προγραμματισμού που είναι ενσωματωμένη στο Microsoft Word και αποκαλείται VBA (Visual Basic for Applications).

Οι εφαρμογές της Microsoft έχουν ενσωματωμένο ένα χαρακτηριστικό που αποκαλείται Macro Virus Protection για να εμποδίσουν την εκτέλεση τέτοιων προγραμμάτων. Όταν το Macro Virus Protection είναι ενεργό , τότε είναι απενεργοποιημένο το χαρακτηριστικό της αυτόματης εκτέλεσης και έτσι όταν ένα έγγραφο προσπαθήσει να εκτελέσει κάποιον κώδικα, εμφανίζεται ένα πλαίσιο μηνύματος για προειδοποίηση του χρήστη. Στην περίπτωση του ιού *I Love You* ήταν καθαρά ανθρώπινη ευθύνη καθώς αρκούσε να γίνει διπλό κλικ στο πρόγραμμα της Visual Basic που ερχόταν ως συνημμένο για να εκτελεσθεί και να κάνει ζημιά.

ΤΑ ΣΚΟΥΛΗΚΙΑ (WORMS)

Τα σκουλήκια είναι παρόμοια με τους ιούς, με τη μόνη διαφορά ότι δεν απαιτείται η παρουσία ενός προγράμματος-φορέα για τη διάδοσή τους. Δημιουργούν αντίγραφα του εαυτού τους και χρησιμοποιούν τις επικοινωνίες μεταξύ των υπολογιστών για να διαδοθούν. Ένα σκουλήκι (worm) είναι ένα πρόγραμμα υπολογιστή που έχει τη δυνατότητα να αντιγράφει τον εαυτό του από μηχάνημα σε μηχάνημα. Τα σκουλήκια συνήθως μετακινούνται και μολύνουν άλλα μηχανήματα μέσω των δικτύων υπολογιστών.

Χρησιμοποιώντας ένα δίκτυο, ένα σκουλήκι μπορεί να επεκταθεί απίστευτα γρήγορα, όπως για παράδειγμα το σκουλήκι *Code Red* που αναπαρήγαγε τον εαυτό του πάνω από 250.000 φορές σε εννέα ώρες στις 19 Ιουλίου 2001. Ένα σκουλήκι

εκμεταλλεύεται συνήθως κάποια τρύπα ασφαλείας σε ένα κομμάτι προγράμματος ή στο λειτουργικό σύστημα, όπως το σκουλήκι Slammer, το οποίο εκμεταλλεύθηκε μια τέτοια τρύπα στον SQL server της Microsoft και προκάλεσε καταστροφή τον Ιανουάριο του 2003, αν και το μέγεθός του ήταν μόνο 376 bytes.

Τα σκουλήκια διακρίνονται σε δύο κατηγορίες, τα Host Computer Worms και τα Network worms. Τα πρώτα είναι γνωστά και ως rabbits και λειτουργούν σε έναν και μόνο υπολογιστή, ενώ τα δεύτερα που είναι γνωστά και ως octopuses είναι χωρισμένα σε μικρά κομμάτια και απλωμένα σε ένα δίκτυο υπολογιστών και για να λειτουργήσουν θα πρέπει να επικοινωνούν την ίδια στιγμή.

⇒ ΤΟ ΣΚΟΥΛΗΚΙ CODE RED

Τα σκουλήκια εκμεταλλεύονται το χρόνο των υπολογιστών και το εύρος ζώνης των δικτύων όταν αναπαράγονται και έχουν συχνά κακές προθέσεις. Ένα σκουλήκι με το όνομα code red προκάλεσε μεγάλη δημοσιότητα το 2001 και οι ειδήμονες ανησύχησαν μήπως προκαλέσει σταμάτημα του Internet. Το σκουλήκι αυτό επιβράδυνε όντως την κυκλοφορία στο Διαδίκτυο όταν άρχισε να αναπαράγει τον εαυτό του, αλλά όχι τόσο άσχημα όσο αναμενόταν. Το κάθε αντίγραφο του σκουληκιού έψαχνε στο internet για να βρει servers με Windows NT ή Windows 2000 που να μην έχουν εγκατεστημένο το security patch της Microsoft.
Κάθε φορά που έβρισκε έναν μη ασφαλή server , το σκουλήκι αναπαρήγαγε τον εαυτό του σε εκείνον τον server και το καινούριο αντίγραφο έψαχνε μετά να βρει άλλους servers για να μολύνει. Το σκουλήκι code red ήταν σχεδιασμένο για να κάνει τα εξής τρία πράγματα :

- Να αναπαράγει τον εαυτό του κατά τις 20 πρώτες ημέρες του μήνα.
- Να αντικαθιστά τις αρχικές ιστοσελίδες στους μολυσμένους servers με μια σελίδα που εμφάνιζε το μήνυμα “Hacked by Chinese”.
- Να ξεκινά μια συντονισμένη επίθεση στον Web server του Λευκού Οίκου σε μια προσπάθεια να τον κάνει να καταρρεύσει.

❖ ΟΙ ΔΟΥΡΕΙΟΙ ΙΠΠΟΙ (TROJAN HORSES)

Ο δούρειος ίππος είναι ένα πρόγραμμα υπολογιστή που η δράση του θυμίζει τη γνωστή ιστορία της μυθολογίας με το ξύλινο άλογο που χρησιμοποιήθηκε κατά την πολιορκία της Τροίας, δηλαδή ενώ ο χρήστης εκτελεί ένα πρόγραμμα που υποτίθεται ότι κάνει κάποια χρήσιμη εργασία, στην πραγματικότητα εγκαθιστά στον υπολογιστή του ένα άλλο πρόγραμμα που μπορεί να κάνει ζημιά στον υπολογιστή ή να κατασκοπεύσει διάφορα απόρρητα αρχεία ή να προσφέρει πρόσβαση σε κάποιον άλλο στον υπολογιστή μέσω του internet.
Ένας δούρειος ίππος αποτελείται από δύο μέρη, το server και το client. Για να μπορέσει να μολυνθεί ένας υπολογιστής από ένα πρόγραμμα δούρειου ίππου, θα πρέπει με κάποιον τρόπο να εγκατασταθεί και να εκτελεσθεί σε αυτόν το μέρος server. Μετά, αφού εκτελεσθεί το μέρος client στον υπολογιστή του εισβολέα και δοθεί η IP διεύθυνση του υπολογιστή που έχει προσβληθεί, ο έλεγχός του θα είναι πλέον πολύ εύκολος. Τα προγράμματα μέσω των οποίων μεταφέρονται οι δούρειοι ίπποι στον υπολογιστή μας αποκαλούνται droppers.
Οι δούρειοι ίπποι επικοινωνούν με τον client μέσω των διαφόρων θυρών του υπολογιστή, τις οποίες μπορούμε να απενεργοποιήσουμε με τη χρήση κάποιου τείχους προστασίας.

⇒Ιστορία

Ο όρος "δούρειος ίππος" χρησιμοποιήθηκε αρχικά από τον Κεν Τόμσον στην ομιλία του το 1983 κατά την τελετή απονομής των βραβείων Turing. Ο Τόμσον παρατήρησε ότι είναι δυνατόν να προστεθεί κακόβουλος κώδικας στην εντολή login του Unix για την υποκλοπή κωδικών πρόσβασης. Αυτήν του την ανακάλυψη την ονόμασε "δούρειο ίππο". Επιπροσθέτως υποστήριξε ότι οποιοσδήποτε μεταγλωττιστής C μπορεί να μετατραπεί κατάλληλα ούτως ώστε να προσθέτει αυτόματα κακόβουλο κώδικα στα προγράμματα που δημιουργεί. Με τον τρόπο αυτό ο εντοπισμός του κακόβουλου κώδικα γίνεται ακόμη πιο δύσκολος.

⇒ Τύποι δούρειων ίππων

Υπάρχουν δύο είδη δούρειων ίππων:

- Το πρώτο είδος αποτελείται από κανονικά προγράμματα, τα οποία διάφοροι χάκερς μεταβάλλουν προσθέτοντας κακόβουλο κώδικα. Στην κατηγορία αυτή ανήκουν για παράδειγμα διάφορα ομότιμα προγράμματα ανταλλαγής αρχείων, προγράμματα ανακοίνωσης καιρικών συνθηκών κοκ.
- Το δεύτερο είδος περιλαμβάνει μεμονωμένα προγράμματα που ξεγελούν τον χρήστη και τον κάνουν να νομίζει ότι πρόκειται για κάποιο παιχνίδι ή εικόνα. Με τον τρόπο αυτό τον παρασύρουν να εκτελέσει το αρχείο, μολύνοντας έτσι τον υπολογιστή του.

Σε αντίθεση με άλλα κακόβουλα προγράμματα (σκουλήκια, ιούς κοκ), οι δούρειοι ίπποι δεν μπορούν να δράσουν αυτόνομα αλλά εξαρτώνται από τις ενέργειες που θα κάνει το υποψήφιο θύμα. Μερικές από τις επιπτώσεις εκτέλεσης ενός δούρειου ίππου είναι για παράδειγμα η διαγραφή αρχείων στον μολυσμένο υπολογιστή, η χρησιμοποίησή του για επίθεση σε άλλους υπολογιστές, το ανοιγόκλεισμα του οδηγού CD-ROM, η παρακολούθηση των κινήσεων του χρήστη για την απόκτηση των κωδικών του σε τράπεζες, απόκτηση διευθύνσεων e-mail για να χρησιμοποιηθούν για spamming, επανεκκίνηση του υπολογιστή, απενεργοποίηση προγραμμάτων firewall ή αντιϊκών και πολλά άλλα.

⇒ Τρόποι μόλυνσης

Η πλειοψηφία των μολύνσεων υπολογιστών από δούρειους ίππους συμβαίνει επειδή ο χρήστης προσπάθησε να εκτελέσει ένα μολυσμένο πρόγραμμα. Για τον λόγο αυτό οι χρήστες πάντα προτρέπονται να μην ανοίγουν ύποπτα αρχεία επισυναπτόμενα σε e-mail. Συνήθως το επισυναπτόμενο αρχείο περιλαμβάνει όμορφα γραφικά ή κινούμενη εικόνα, αλλά περιέχει επίσης ύποπτο κώδικα που μολύνει τον υπολογιστή του χρήστη. Παρόλα αυτά, το πρόγραμμα δεν είναι απαραίτητο να έχει φτάσει στον χρήστη με e-mail. Μπορεί να το έχει κατεβάσει από έναν ιστοχώρο, μέσω προγραμμάτων Instant Messaging, σε CD ή DVD.

❖ ΤΑ ΠΡΟΓΡΑΜΜΑΤΑ SPYWARE, ADWARE ΚΑΙ HIJACK

Όπως ήδη γνωρίζουμε με τα cookies ένας δικτυακός τόπος μπορεί να εξάγει χρήσιμα στατιστικά συμπεράσματα σε ό,τι έχει να κάνει μόνο με τις δικές ιστοσελίδες. Ποια

εταιρεία 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 καινούρια προϊόντα ή υπηρεσίες, να στήσουν ηλεκτρονικά καταστήματα κλπ.

Προς το σκοπό αυτό δημιουργήθηκαν διάφορα προγράμματα, τα αποκαλούμενα spyware, τα οποία εγκαθίστανται αυτόκλητα στον υπολογιστή μας, δηλαδή 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. Η βασική αποστολή τους με άλλα λόγια 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 με άλλα προγράμματα που προσφέρονται δωρεάν. Στην πράξη όμως δεν υπάρχει σαφής διαχωρισμός των προγραμμάτων αυτών. 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 μεταδίδουν προσωπικά μας δεδομένα, όπως αριθμούς τραπεζικών λογαριασμών και πιστωτικών καρτών, θα πρέπει να φροντίσουμε να απαλλαγούμε από 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. Τελευταία έχουν κάνει την εμφάνισή τους και προγράμματα που αλλάζουν την αρχική σελίδα του φυλλομετρητή internet explorer ενός υπολογιστή χωρίς φυσικά τη 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 ορισμένων ιστοσελίδων ούτως ώστε οι κάτοχοι των ιστοσελίδων αυτών να μπορούν να προσελκύσουν περισσότερες και καλύτερα αμειβόμενες διαφημίσεις.

Έλαβαν το όνομα hijack καθώς εγκαθίστανται στον υπολογιστή μας χωρίς να πάρουμε είδηση 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 απεγκατάσταση τους είναι συχνά μια χρονοβόρα διαδικασία καθώς δημιουργούν πολλές φορές καταχωρήσεις και στο Μητρώο των windows.

⇒ **Ύπαρξη του λογισμικού spyware:**

Είναι πιθανό να υπάρχει κάποιο είδος λογισμικού υποκλοπής spyware στον υπολογιστή σας:

- Εάν παρατηρήσετε νέες γραμμές εργαλείων, συνδέσεις ή αγαπημένα που δεν προσθέσατε οι ίδιοι στο πρόγραμμα περιήγησης web.
- Εάν αλλάξει η προεπιλεγμένη αρχική σελίδα, ο δείκτης του ποντικιού ή το πρόγραμμα αναζήτησης.
- Εάν πληκτρολογείτε τη διεύθυνση μιας συγκεκριμένης τοποθεσίας Web (για παράδειγμα, ενός μηχανισμού αναζήτησης), αλλά μεταφέρεστε σε άλλη τοποθεσία Web, χωρίς ειδοποίηση.
- Εάν βλέπετε αναδυόμενα διαφημιστικά μηνύματα, ακόμη και όταν δεν είστε συνδεδεμένοι στο Internet.
- Εάν ξαφνικά ο υπολογιστής σας αρχίσει να καθυστερεί κατά την εκκίνηση ή να λειτουργεί αργά.

Ίσως να υπάρχει λογισμικό υποκλοπής spyware στον υπολογιστή σας ακόμη και αν δεν παρατηρείτε συμπτώματα. Αυτός ο τύπος λογισμικού μπορεί να συλλέγει πληροφορίες σχετικά με εσάς και τον υπολογιστή σας, χωρίς να το γνωρίζετε και χωρίς τη συγκατάθεσή σας. Η εκτέλεση του Windows Defender κάθε φορά που χρησιμοποιείτε τον υπολογιστή σας μπορεί να σας βοηθήσει στην εύρεση και αφαίρεση αυτού του λογισμικού.

❖ KEYLOGGERS

Τα keyloggers είναι επιβλαβή προγράμματα που εκτελούνται σχεδόν αόρατα, καταγράφουν όλες τις πληροφορίες που πληκτρολογείτε και στη συνεχεία, στέλνουν πληροφορίες σ΄αυτόν που σας έχει μολύνει με το keylogger.

Είναι πολύ επικίνδυνα και μπορούν να χρησιμοποιηθούν για να κλέψουν τα προσωπικά σας στοιχεία όπως ο αριθμός πιστωτικής κάρτας, καθώς και τους κωδικούς σας πρόσβασης, είναι ιδιαιτέρα επικίνδυνα για όλους όσους χρησιμοποιούν ηλεκτρονικούς δικτυακούς τόπους μέσω των οποίων κάνουν χρηματικές συναλλαγές.

Αν έχετε την υποψία ότι έχετε μολυνθεί με keylogger, τότε καλό είναι να αποφύγετε να πληκτρολογείτε οποιαδήποτε προσωπική πληροφορία.

Πριν αφαιρέσετε το keylogger, θα χρειαστεί πρώτα να το ανιχνεύσετε. Η Ανίχνευση ενός keylogger δεν είναι εύκολη υπόθεση. Μπορεί να εγκατασταθεί σε πάρα πολλές θέσεις στον υπολογιστή σας και συνήθως βρίσκεται σε ένα από τα αρχεία του συστήματος.

Η ΑΠΑΤΗ ΤΩΝ DIALER

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 στη Ελλάδα εντοπίσθηκαν περισσότερες από 1.000 ύποπτες ιστοσελίδες που είναι πολύ πιθανό 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 καυτά videos on-line ή και με κάτι άλλο, οι οποίες υπηρεσίες μάλιστα διαφημίζονται έντονα και τονίζεται ότι παρέχονται δωρεάν.

Μόλις ο χρήστης κάνει κλικ σε ένα συγκεκριμένο σημείο εγκαθίσταται αυτόματα στον υπολογιστή του και χωρίς αυτός να το γνωρίζει ένα ειδικό πρόγραμμα με αποτέλεσμα αντί για αστική κλήση στον τοπικό provider (ο γνωστός ΕΠΑΚ,8962….) να γίνεται εκτροπή και διεθνής κλήση σύνδεσης και μάλιστα υπερπόντια, με πολλαπλάσιο φυσικά κόστος. Για παράδειγμα ο χρήστης αντί για 0,17 – 0,35 ευρώ την ώρα χρεώνεται με 2,50 ευρώ 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 τα χρέη τους σε δόσεις. Η μόνη αντιμετώπιση της μάστιγας αυτής που χρεώνει υπέρογκους λογαριασμούς των ανυποψίαστων χρηστών είναι η προσοχή και εγρήγορση των ίδιων των χρηστών. Η καλύτερη προστασία είναι η εγκατάσταση φραγής των διεθνών τηλεφωνικών κλήσεων ή η προμήθεια και η εγκατάσταση ειδικής συσκευής Antidialer , η οποία παρεμβάλλεται ανάμεσα στην τηλεφωνική γραμμή και τη συσκευή modem του υπολογιστή του χρήστη και επιτρέπει να γίνονται κλήσεις μόνο προς συγκεκριμένους αριθμούς ΕΠΑΚ. Για τις υπερβολικές αυτές χρεώσεις ο ΟΤΕ δεν φέρει καμία ευθύνη και συμβουλεύει τους dial –up χρήστες για τα εξής;

- Να μην κατεβάζουν προγράμματα στους υπολογιστές τους από άγνωστης και αμφίβολης προέλευσης ιστοσελίδες.
- Να αποσυνδέονται από το internet όταν δεν το χρησιμοποιούν.
- Να χρησιμοποιούν την υπηρεσία φραγής των εξερχόμενων διεθνών τηλεφωνικών κλήσεων.
- Να μην επιτρέπουν τη χρήση του υπολογιστή τους στο internet σε τρίτους, στο σπίτι ή στο χώρο εργασίας τους.

ΟΙ ΚΕΡΚΟΠΟΡΤΕΣ (BACKDOORS)

Σε πολλές περιπτώσεις επιθέσεων σε συστήματα υπολογιστών, οι επίδοξοι hachers δημιουργούν μια κρυφή είσοδο ή κερκόπορτα στον υπολογιστή στόχο από την οποία θα μπορούν να εισβάλλουν σε αυτόν χωρίς να χρειασθεί να προσπελάσουν κάποιο σύστημα ασφαλείας. Τα προγράμματα BO (Back Orifice) και Netbus είναι δύο από τα βασικότερα εργαλεία με τα οποία μπορούμε να ανοίξουμε ένα backdoor σε ένα σύστημα και να εκτελέσουμε έτσι από απόσταση ό,τι λειτουργίες θέλουμε. Οι εφαρμογές αυτές λειτουργούν παρόμοια με τους δούρειου ίππους και αποτελούνται όπως και αυτοί από δύο τμήματα, το τμήμα server που εγκαθίστανται και λειτουργεί στον υπολογιστή στόχο και το τμήμα client που εκτελείται στον υπολογιστή του επιτιθέμενου, ο οποίος θα μπορεί με αυτόν τον τρόπο να εκτελέσει από απόσταση ό,τι εντολές θέλει και να αποσπάσει ό,τι πληροφορίες θέλει.

ΟΙ ΕΠΙΘΕΣΕΙΣ DoS (DENIAL OF SERVICE)

Οι επιθέσεις του τύπου DoS, που είναι γνωστές και ως επιθέσεις άρνησης υπηρεσίας, αποτελούν μια από τις σοβαρότερες επιθέσεις που μπορούν να εκδηλωθούν σε ένα website ή σε 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 συνιστάται στη εκδήλωση χιλιάδων αιτήσεων σύνδεσης σε έναν server και σε διάστημα μερικών ημερών με απώτερο στόχο την κατάρρευση του server και την αδυναμία του να ανταποκριθεί σε έναν τόσο μεγάλο αριθμό αιτήσεων.

ΟΙ ΕΠΙΘΕΣΕΙΣ DDoS (DISTRIBUTED DENIAL OF SERVICE)

Τελευταία έχουν αρχίσει να κάνουν την εμφάνισή τους και οι λεγόμενες κατανεμημένες επιθέσεις άρνησης υπηρεσίας, γνωστές με τον όρο ddos. Σύμφωνα με το σενάριο, κάποια συγκεκριμένη ημερομηνία, τα προγράμματα τύπου worm που μέχρι τότε περίμεναν σιωπηρά στα μηχανήματα όπου φιλοξενούνταν, ξαφνικά ενεργοποιούνται και αρχίζουν όλα μαζί να στέλνουν αιτήσεις σύνδεσης σε έναν συγκεκριμένο server. Ο server δέχεται τόσες πολλές αιτήσεις που αδυνατεί να ανταποκριθεί σε 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. Αυτός που σκοπεύει να κάνει μια τέτοια επίθεση, φροντίζει αρχικά να αποκτήσει δικαιώματα administrator σε όσο το δυνατόν περισσότερα συστήματα υπολογιστών μπορεί. Η επίθεση πραγματοποιείται μέσω αυτοματοποιημένων σεναρίων για την ανακάλυψη συστημάτων που διαθέτουν χαμηλότερα στάνταρτ ασφαλείας. Από τη στιγμή που ο επιτιθέμενος αποκτήσει πρόσβαση σε έναν αριθμό συστημάτων που θεωρεί ικανοποιητικό, φορτώνει το σενάριο για να εξαπολύσει την επίθεσή του.

ΦΑΡΣΕΣ ΤΩΝ ΙΩΝ

Οι φάρσες ιών που αναφέρουν πολλοί χρήστες του internet μέσω e-mail είναι αρκετά συνηθισμένες και μπορούν να δημιουργήσουν και 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 σε όσους βρίσκονται στο βιβλίο διευθύνσεών τους θα δημιουργηθεί υπερφόρτωση του δικτύου από καταιγισμό μηνυμάτων.

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 εμφανίστηκε ως φάρσα και αργότερα και ως κανονικός ιός.

Ο καλύτερος τρόπος για να αντιμετωπιστούν οι φάρσες και όλα τα ύποπτα και άγνωστα μηνύματα email, είναι να προωθούνται στον αρμόδιο τεχνικό υπάλληλο μιας

εταιρείας, ο οποίος θα είναι και ο μόνος υπεύθυνος για να αποφασίσει τι θα πρέπει να γίνει.

ΟΙ ΑΙΤΙΕΣ ΔΗΜΙΟΥΡΓΙΑΣ ΙΩΝ

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

ΓΙΑΤΙ ΟΜΩΣ ΓΙΝΟΝΤΑΙ ΟΛΑ ΑΥΤΑ;

Υπάρχουν δυο τουλάχιστον λόγοι. Ο πρώτος είναι η ίδια η 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 αλαζονικές συμπεριφορές. Αν είστε προγραμματιστής και βρείτε μια τρύπα ασφαλείας που θα μπορούσατε να εκμεταλλευτείτε τότε θα την εκμεταλλευτείτε πριν 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.

ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ ΑΠΟ ΤΟΥΣ ΙΟΥΣ

Ο βασικός τρόπος προστασίας από τους ιούς των υπολογιστών είναι η εγκατάσταση, η σωστή ρύθμιση και η συνεχής ενημέρωση και επικαιροποίηση 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 τους ιούς τύπου spyware, adware αλλά και από dialers και από τη μάστιγα των spam e-mails.

Η χρήση ενός ψηφιακού τείχους προστασίας, 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 email 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 να κάνουμε 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 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 back-up, 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 αντιικά προγράμματα είναι το Norton Antivirus της εταιρίας Symantec, το McAfee της εταιρίας Network Associates, το Kaspersky, το Panda, το Sophos, το F-Prot της εταιρίας 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 μέσω του Internet.

Συμπτώματα ιού υπολογιστή

- Ο υπολογιστής λειτουργεί πιο αργά από ό, τι συνήθως.
- Η λειτουργία του υπολογιστή σταματάει ή κλειδώνει συχνά.
- Ο υπολογιστής παρουσιάζει σφάλματα και μετά κάνει επανεκκίνηση κάθε λίγα λεπτά.
- Ο υπολογιστής επανεκκινείται μόνος του.. Επίσης, ο υπολογιστής δεν λειτουργεί όπως συνήθως.
- Οι εφαρμογές στον υπολογιστή δεν λειτουργούν σωστά.
- Δεν είναι δυνατή η πρόσβαση στους δίσκους ή στις μονάδες δίσκου.
- Δεν είναι δυνατή η σωστή εκτύπωση..
- Βλέπετε ασυνήθιστα μηνύματα σφάλματος.
- Βλέπετε παραμορφωμένα μενού και παράθυρα διαλόγου.
- Υπάρχει διπλή επέκταση σε ένα συνημμένο που ανοίξατε πρόσφατα, όπως επέκταση .jpg, .vbs, .gif ή .exe.
- Ένα πρόγραμμα προστασίας από ιούς έχει απενεργοποιηθεί χωρίς λόγο. Επιπλέον, δεν είναι δυνατή η επανεκκίνηση του προγράμματος προστασίας από ιούς.
- Δεν μπορεί να εγκατασταθεί ένα πρόγραμμα προστασίας από ιούς στον υπολογιστή ή το πρόγραμμα προστασίας από ιούς δεν θα εκτελεστεί.
- Εμφανίζονται νέα εικονίδια στην επιφάνεια εργασίας, τα οποία δεν τοποθετήσατε εσείς εκεί ή τα εικονίδια δεν σχετίζονται με κανένα από τα προγράμματα που εγκαταστήσατε πρόσφατα.
- Παρατηρείται απροσδόκητη αναπαραγωγή περίεργων ήχων ή μουσικής από τα ηχεία.
- Κάποιο πρόγραμμα εξαφανίζεται από τον υπολογιστή, παρόλο που δεν το καταργήσατε σκόπιμα.