Οι Ιοί των Ηλεκτρονικών Υπολογιστών

ΟΜΑΔΑ ΕΡΓΑΣΙΑΣ:
Φιτσάκη Λιάνα (επικεφαλής ομάδας) ☺
Φραγκιαδάκη Γεωργία ☺
Φραγκιαδάκη Χρύσα ☺
Σταματάκη Αγγελική ☺

Επιβλέπων Καθηγητής: Δετοράκης Ιωάννης

ΠΕΡΙΕΧΟΜΕΝΑ

Τι είναι ιοί

Ένας ιός υπολογιστών είναι ένα κακόβουλο πρόγραμμα υπολογιστή, το οποίο μπορεί να αντιγραφεί χωρίς παρέμβαση του χρήστη και να "μολύνει" τον υπολογιστή χωρίς τη γνώση ή την άδεια του χρήστη του. Ο αρχικός ιός μπορεί να τροποποιήσει τα αντίγραφά του ή τα ίδια τα αντίγραφα μπορούν να υποστούν από μόνα τους τροποποίηση, όπως συμβαίνει σε έναν μεταμορφικό ιό. Ένας ιός μπορεί να διαδοθεί από έναν υπολογιστή σε άλλους, παραδείγματος χάριν από ένα χρήστη που στέλνει τον ιό μέσω δικτύου ή του Διαδικτύου, ή με τη μεταφορά του σε ένα φορητό μέσο αποθήκευσης, όπως δισκέτα, οπτικό δίσκο ή μνήμη flash USB. Οι ιοί ορισμένες φορές εσφαλμένα συγχέονται με τα "σκουλήκια" υπολογιστών (worms) και τους δούρειους ίππους (trojan horses). Ένα "σκουλήκι" μπορεί να διαδοθεί σε άλλους υπολογιστές χωρίς να πρέπει να μεταφερθεί ως τμήμα ενός υπολογιστή-οικοδεσπότη (host), ενώ ένας δούρειος ίππος είναι ένα αβλαβές πρόγραμμα μέχρι να εκτελεσθεί ή μέχρι να ικανοποιηθεί κάποια συνθήκη, την οποία έχει προκαθορίσει ο δημιουργός του. Πολλοί προσωπικοί υπολογιστές συνδέονται πλέον με το Διαδίκτυο και σε τοπικά δίκτυα και διευκολύνουν έτσι τη διάδοση του κακόβουλου κώδικα. Σήμερα οι ιοί μπορούν επίσης να εκμεταλλευθούν τις υπηρεσίες του Διαδικτύου, όπως το World Wide Web, το ηλεκτρονικό ταχυδρομείο και την υπηρεσία συνομιλιών (Internet Relay Chat, IRC).

Μερικοί ιοί δημιουργούνται για να προξενήσουν ζημιά στον υπολογιστή, στον οποίο εγκαθίστανται, είτε με την καταστροφή των προγραμμάτων του είτε με τη διαγραφή αρχείων ή με τη μορφοποίηση (format) του σκληρού δίσκου. Μερικές, μάλιστα, φορές, δημιουργούν σε συγκεκριμένο τομέα του σκληρού δίσκου τέτοια καταστροφή, ώστε να είναι αδύνατη η ανάκτηση ολόκληρου του περιεχομένου του. Άλλοι δεν έχουν ως σκοπό να προκαλέσουν οποιαδήποτε ζημία, αλλά απλά γνωστοποιούν την παρουσία τους με την εμφάνιση στην οθόνη κειμένου, βίντεο, ή ηχητικών μηνυμάτων, μερικές φορές αρκετά χιουμοριστικών. Όμως, ακόμη και αυτοί οι "καλοκάγαθοι" ιοί μπορούν να δημιουργήσουν προβλήματα στο χρήστη υπολογιστών: Καταλαμβάνουν τη μνήμη που χρησιμοποιείται από τα κανονικά προγράμματα και, κατά συνέπεια, προκαλούν συχνά ασταθή συμπεριφορά του συστήματος και μπορούν να οδηγήσουν σε κατάρρευσή του (system cras)

Επιπλέον, πολλοί ιοί είναι, εγγενώς, γεμάτοι προγραμματιστικά σφάλματα, τα οποία πιθανόν να οδηγήσουν στην κατάρρευση των υπολογιστικών συστημάτων και στην απώλεια δεδομένων. Τέλος, ένα μεγάλο ποσοστό των ιών δεν έχει σκοπό την καταστροφή των δεδομένων του χρήστη ή την παρενόχλησή του, αλλά την κλοπή

προσωπικών του δεδομένων ή την εισαγωγή του υπολογιστή-στόχου σε κάποιο παράνομο δίκτυο (botnet) χωρίς τη συγκατάθεση του χρήστη.

Ποιες είναι οι κατηγορίες

Υπάρχουν πολλοί τύποι υπολογιστικών ιών, όπως ιοί αρχείων, ιοί της περιοχής εκκίνησης (boot sector), ιοί σκουλήκια και προγράμματα δούρειοι ίπποι (Trojan Horse).

Ιοί περιοχής εκκίνησης - Αυτοί οι ιοί μολύνουν δισκέτες και σκληρούς δίσκους. Ο ιός φορτώνεται πριν από το λειτουργικό σύστημα. Ήταν οι πρώτοι ιοί που εμφανίστηκαν.

Ιοί αρχείων – σ' αυτή τη κατηγορία ανήκει η πλειοψηφία των ιών και η πιο εύκολα αντιμετωπίσιμη κατηγορία. Είναι μικρά εκτελέσιμα αρχεία. Προσκολλούνται σε ένα αρχείο, συνήθως αρχείο εφαρμογής. Το βασικό γνώρισμα των ιών είναι ότι δημιουργούν αντίγραφα του εαυτού τους μέσα σε άλλα αρχεία. Τα αρχεία αυτά είναι εκτελέσιμα ή αρχεία βιβλιοθηκών. Οι ιοί είτε αντικαθιστούν κάποιο τμήμα του κώδικα του αρχείου (χωρίς να μεταβάλλουν το μέγεθός του) είτε προσκολλώνται σε αυτό.

Ο πρώτος ιός που εμφανίστηκε στους προσωπικούς υπολογιστές ήταν ο ιός Brain (γνωστός και ως Ashar, (C)Brain, Clone, Nipper, Pakistani, Pakistani, Lahore, Pakistani flu, Pakistani Brain). Δημιουργήθηκε στο Πακιστάν το 1986 από τους αδελφούς Basit και Amjad Farooq Alvi. Προσέβαλε τον τομέα εκκίνησης (boot sector) του σκληρού δίσκου[3].

Ιοί σκουλήκια (Worms): Έχουν την ικανότητα αναπαραγωγής χωρίς να χρησιμοποιούν άλλα αρχεία. Ο τρόπος διάδοσης τους είναι το διαδίκτυο με τη βοήθεια των δικτυακών πρωτοκόλλων, εκμεταλλευόμενοι τα προβλήματα ασφαλείας των λειτουργικών συστημάτων ή με τη βοήθεια των μηνυμάτων του ηλεκτρονικού ταχυδρομείου. Οι ιοί σκουλήκια αποκτούν προσπέλαση στο βιβλίο διευθύνσεων του υπολογιστή (όπου κρατούνται οι διευθύνσεις ηλεκτρονικού ταχυδρομείου με τις οποίες επικοινωνεί ο χρήστης του υπολογιστή) και αποστέλλει μολυσμένα μηνύματα. Αρκετές φορές χρησιμοποιούν σαν αποστολέα ένα όνομα από το βιβλίο διευθύνσεων.

Όσοι παραλήπτες ανοίξουν το ηλεκτρονικό μήνυμα μολύνονται. Η διάδοση των ιών worm με αυτή τη μέθοδο είναι αστραπιαία. Στη συνέχεια γίνεται αναφορά σε δύο ιούς σκουλήκια τον Blaster και τον Sobig.

Η έκρηξη του Blaster έγινε την 11η Αυγούστου 2003. Το μεσημέρι της ίδιας μέρας είχαν μολυνθεί 7.000 υπολογιστές και το βράδυ 330.000. Ο ιός ήταν προγραμματισμένος να επιτεθεί στο δικτυακό τόπο της Microsoft στις 16 Αυγούστου. Οι τεχνικοί της Microsoft πρόλαβαν και άλλαξαν τις διευθύνσεις των διακομιστών της εταιρίας και η επίθεση απέτυχε. Μια εβδομάδα αργότερα έκανε την εμφάνισή του η έκτη έκδοση ενός ακόμα ιού του Sobig. Ο ιός αυτός μεταδιδόταν μέσω ηλεκτρονικού ταχυδρομείου και επιβάρυνε τα συστήματα ηλεκτρονικής αλληλογραφίας. Ο Sobig ήταν πολυμορφικός ιός. Όταν οι χρήστες άνοιγαν το μολυσμένο μήνυμα ο κώδικας του ιού ξεκινούσε την αναπαραγωγή του. Έβρισκε τις διευθύνσεις αλληλογραφίας του χρήστη και έστελνε μολυσμένα μηνύματα. Οι μολυσμένοι υπολογιστές θα επιχειρούσαν να συνδεθούν στο διαδίκτυο και Παρασκευή και Κυριακή από τις 0:00 έως τις 3:00. Τότε επικοινωνούσαν με 20 διακομιστές και θα κατέβαζαν επιπλέον λογισμικό. Η εξάπλωση του ιού ήταν τεράστια. Οι διακομιστές αλληλογραφίας κατακλύστηκαν από μηνύματα που μετέφεραν τον ιό. Η America On Line (παροχέας διαδικτύου στις ΗΠΑ) έλαβε σε μία μέρα 31 εκατομμύρια μηνύματα (τρεις φορές περισσότερα από το κανονικό). Τα 11,5 εκατομμύρια ήταν μολυσμένα μηνύματα με τον Sobig. Μέσα σε μία εβδομάδα στάλθηκαν 200 εκατομμύρια μολυσμένα μηνύματα. Η όλη δραστηριότητα του ιού σταμάτησε στις 10 Σεπτεμβρίου καθώς έτσι είχε προγραμματιστεί ο ιός.

Το Σκουλήκι Code Red

Τα σκουλήκια εκμεταλλεύονται τον χρόνο των υπολογιστών και το εύρος ζώνης των δικτύων όταν αναπαράγονται και έχουν συχνά κακές προθέσεις. Ένα σκουλήκι με 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 (Internet traffic) 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 στον εαυτό του σ' εκείνον τον server και το καινούργιο αντίγραφο έψαχνε μετά να βρει άλλους servers για να μολύνει. Το σκουλήκι Code Red ήταν σχεδιασμένο για να κάνει τα εξής τρία πράγματα :

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

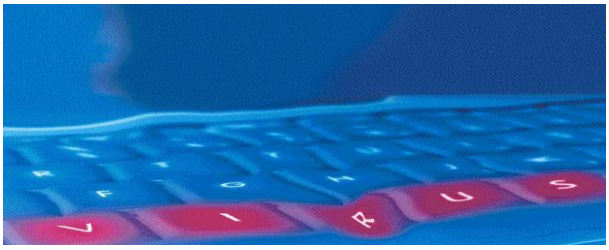
Δούρειος Ίππος

Δούρειος ίππος : Αυτοί οι ιοί δρουν αθόρυβα. Μολύνουν τον υπολογιστή και αναμένουν κάποιο γεγονός

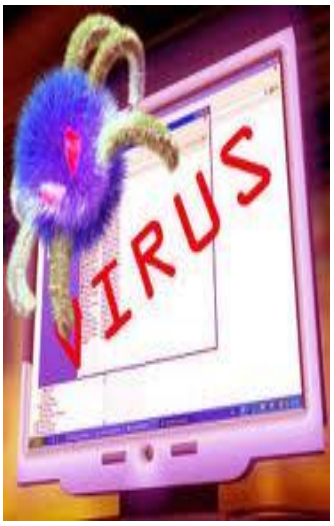
ανάλογα με το προγραμματισμό τους. Συνήθως δεν πολλαπλασιάζοντας και δεν εξαπλώνονται σε άλλους υπολογιστές. Ένας δούρειος ίππος αποτελείται από δύο μέρη, το Server και το Client. Για να μπορέσει να μολυνθεί ένας υπολογιστής από ένα πρόγραμμα δούρειου ίππου, θα πρέπει με κάποιον τρόπο να εγκατασταθεί και να εκτελεσθεί σ' 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. Επίσης είναι ένα πρόγραμμα υπολογιστή που η δράση του θυμίζει την 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 του ή να κατασκοπεύσει διάφορα απόρρητα αρχεία ή και για να αποκτήσει κάποιος άλλος πρόσβαση στον υπολογιστή του μέσω του Internet. Οι δούρειοι ίπποι επικοινωνούν με τον Client μέσω των διαφόρων θυρών (ports) του υπολογιστή, τις οποίες μπορούμε να απενεργοποιήσουμε με τη χρήση κάποιου firewall (τείχους προστασίας).

Viruses

Ιοί (Viruses): Ένας ιός (virus) είναι ένα μικρό κομμάτι προγράμματος που έχει τη δυνατότητα να μεταφέρεται μέσω των πραγματικών (κανονικών) προγραμμάτων, όπως είναι για παράδειγμα ένα πρόγραμμα λογιστικών φύλλων και έτσι κάθε φορά που εκτελείται το πρόγραμμα αυτό, εκτελείται και το πρόγραμμα του ιού και έχει επίσης τη δυνατότητα να αναπαράγεται προσκολειόμενο σ' άλλα προγράμματα ή να προκαλεί καταστροφή.Αποκαλούνται ιοί (viruses) επειδή έχουν μερικά κοινά γνωρίσματα με τους βιολογικούς ιούς. Ένας ιός υπολογιστή μεταφέρεται από υπολογιστή σε υπολογιστή όπως ακριβώς ένας βιολογικός ιός μεταφέρεται από άνθρωπο σε άνθρωπο. Επίσης, οι ιοί αναπαράγουν τον εαυτό τους όπως και οι πραγματικοί και τέλος, μεταλλάσσονται για να μπορέσουν να αποφύγουν τα ηλεκτρονικά αντιβιοτικά.Ένας ιός υπολογιστή πρέπει να μεταφερθεί μέσω άλλων προγραμμάτων ή εγγράφων ώστε να μπορέσει να εκτελεσθεί. Αφού εκτελεσθεί, μπορεί μετά να επηρεάσει (μολύνει) άλλα προγράμματα ή και έγγραφα. Μπορεί η αναλογία ανάμεσα στους ιούς των υπολογιστών και στους βιολογικούς ιούς να είναι λίγο τραβηγμένη, υπάρχουν όμως αρκετές ομοιότητες που να δικαιολογούν την αντιστοίχιση.



Ιοί των e-mail (e-mail viruses). Ένας ιός e-mail μεταφέρεται με τα μηνύματα e-mail και συνήθως αναπαράγει αυτόματα τον εαυτό του χρησιμοποιώντας το βιβλίο διευθύνσεων (address book) του χρήστη που έχει προσβληθεί ώστε να μπορέσει σταλεί αυτόματα στους παραλήπτες που βρίσκονται καταχωρημένοι εκεί.Ο πιο πρόσφατος στον κόσμο των ιών των υπολογιστών είναι ο ιός που μεταδίδεται με την ηλεκτρονική αλληλογραφία (e-mail virus) και ο ιός Melissa που εμφανίσθηκε 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 (uploaded) σε μια ομάδα ειδήσεων (newsgroup) 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) μ' ένα μήνυμα e-mail στους πρώτους 50 χρήστες που υπήρχαν στο βιβλίο διευθύνσεων (address book) του μολυσμένου υπολογιστή.



I Love You

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 (attachment). Οι χρήστες που έκαναν διπλό κλικ στο συνημμένο, επέτρεπαν στον ιό να εκτελεσθεί. Ο κώδικας έστελνε αντίγραφα του εαυτού του σ' όσους βρίσκονταν στο βιβλίο διευθύνσεων του θύματος και μετά άρχιζε να καταστρέφει αρχεία στον υπολογιστή του.

Melissa

Ο ιός Melissa: εκμεταλλεύτηκε τη γλώσσα προγραμματισμού που είναι ενσωματωμένη στο Microsoft Word και αποκαλείται VBA (Visual Basic for Applications). Είναι μια ολοκληρωμένη γλώσσα προγραμματισμού και μπορεί να προγραμματιστεί για να κάνει εργασίες όπως τροποποίηση αρχείων και αποστολή μηνυμάτων e-mail. Ένας προγραμματιστής μπορεί να εισάγει ένα πρόγραμμα μέσα σ' ένα έγγραφο, το οποίο θα εκτελεσθεί αμέσως μόλις ανοιχθεί το έγγραφο. Με τον τρόπο αυτό δημιουργήθηκε (προγραμματίσθηκε) ο ιός Melissa. Όποιος άνοιγε ένα έγγραφο που ήταν μολυσμένο με τον ιό Melissa θα ενεργοποιούσε αυτόματα τον ιό, θα έστελνε τα 50 e-mails και μετά θα μόλυνε ένα κεντρικό αρχείο με όνομα NORMAL.DOT έτσι ώστε όποιο αρχείο δημιουργείτο από δω και πέρα θα περιείχε επίσης τον ιό.

Ερυθρός κώδικας

Στο απόγειο της δόξας του στις 19/07/2001 ο code red είχε προσβάλλει 359000 Η/Υ. Εκμεταλλεύθηκε μία αδυναμία γνωστή ως buffer overflow, εμποδίζοντας τη σύνδεση στο Internet. Στα θύματά του και ο web server του Λευκού Οίκου.

NIMDA

Στις 18/9/2001 μέσα σε 22 λεπτά ο Nimda έγινε ο πιο επιτυχημένος ιός. Το κλίμα γενικευμένου πανικού από τις επιθέσεις της 11ης Σεπτεμβρίου, οδήγησε στη συσχέτιση του με την Αλ-Κάιντα. Δεν αποδείχτηκε τίποτα.

SASSER

Ο SASSER, ο συγγραφέας του οποίου ήταν ο δεκαεξάχρονος Γερμανός φοιτητής πληροφορικής Σβέν Γιάσαν, έκανε χρήση του buffer overflow. Το Γαλλικό πρακτορείο ειδήσεων έκλεισε όλες τις δορυφορικές επικοινωνίες του, η Delta Air lines ακύρωσε υπερατλαντικές πτήσεις, το Βρετανικό Λιμενικό έμεινε χωρίς ηλεκτρονικούς χάρτες, ενώ ζημιές υπέστησαν μεγάλες εταιρίες όπως η Goldman Sachs και οργανισμοί όπως το Γερμανικό ταχυδρομείο και η Κομισιόν.

Οι Ιοί 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.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 εταιρείες να διακόψουν την ηλεκτρονική τους αλληλογραφία.

Η Απάτη 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 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 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 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 (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 € 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 από την απάτη αυτή 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 για τα εξής :

1. Να μην κατεβάζουν (download) προγράμματα στους υπολογιστές τους από άγνωστης και αμφίβολης προέλευσης ιστοσελίδες.

2. Να αποσυνδέονται από το Internet όταν δεν το χρησιμοποιούν.
3. Να χρησιμοποιούν την υπηρεσία φραγής των εξερχόμενων διεθνών τηλεφωνικών κλήσεων.
4. Να μην επιτρέπουν τη χρήση του υπολογιστή για σύνδεση στο Internet από τρίτους, στο σπίτι ή τον χώρο εργασίας τους.

Οι Κερκόπορτες (Backdoors)

Σε πολλές περιπτώσεις επιθέσεων σε συστήματα υπολογιστών, οι επίδοξοι hackers φροντίζουν να δημιουργήσουν μια κρυφή είσοδο ή κερκόπορτα (backdoor) στον υπολογιστή στόχο, από την οποία θα μπορούν να εισβάλουν σ' αυτό 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 σ' ένα σύστημα και να εκτελέσουμε έτσι από απόσταση ότι λειτουργίες θέλουμε.

Οι εφαρμογές αυτές λειτουργούν παρόμοια με τους δούρειους ίππους και αποτελούνται από δύο τμήματα, το τμήμα server που εγκαθίσταται και λειτουργεί στον υπολογιστή στόχο και το τμήμα client που εκτελείται στον υπολογιστή του επιτιθέμενου, ο οποίος θα μπορεί μ' αυτόν τον τρόπο να εκτελέσει από απόσταση ότι εντολές θέλει και να αποσπάσει ότι πληροφορίες θέλει.

Οι Επιθέσεις DoS (Denial of Service)

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 στις 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 τον 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. Αυτός που σκοπεύει να κάνει μια τέτοια επίθεση, φροντίζει αρχικά να αποκτήσει δικαιώματα administrator σ' όσο το δυνατόν περισσότερα συστήματα υπολογιστών μπορεί.

Η επίθεση πραγματοποιείται μέσω αυτοματοποιημένων scripts (σεναρίων) για την ανακάλυψη συστημάτων που διαθέτουν χαμηλά στάνταρτ ασφαλείας. Από τη στιγμή που ο επιτιθέμενος αποκτήσει πρόσβαση σ' έναν αριθμό συστημάτων που θεωρεί ικανοποιητικό, φορτώνει το script για να εξαπολύσει την επίθεσή του.

Οι Φάρσες Ιών (Virus Hoaxes)

Οι φάρσες ιών που αναφέρουν πολλοί χρήστες του Internet μέσω e-mail 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.

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.

Δούρειος ίππος

Για να μολυνθεί ένας υπολογιστής ο χρήστης του πρέπει να κατεβάσει και να εκτελέσει τον ιό. Αυτό γίνεται συνήθως με ένα ηλεκτρονικό μήνυμα όπου ο ιός είναι συνημμένος και ο χρήστης πείθεται να τον εκτελέσει. Όταν ο ιός δούρειος ίππος εγκατασταθεί στέλνει μέσω διαδικτύου τις κατάλληλες πληροφορίες στο δημιουργό του ώστε αυτός να πάρει τον έλεγχο του υπολογιστή και να χρησιμοποιηθεί σε διάφορες παράνομες και επιβλαβείς ενέργειες

Επιπτώσεις διάδοσης του ίου

Τα συμπτώματα ενός μολυσμένου με ιό Η/Υ είναι:

1. Η εμφάνιση στην οθόνη ενός εκνευριστικού μηνύματος.
2. Μείωση της ελεύθερης μνήμης ή χωρητικότητας του σκληρού δίσκου.
3. Τροποποίηση δεδομένων.
4. Αντικατάσταση ή καταστροφή αρχείων.
5. Διαγραφή σκληρού δίσκου.
6. Σήμερα, οι επιπτώσεις των ιών είναι πολύ επικίνδυνες:
7. Χρήση του Η/Υ για επιθέσεις σε άλλους Η/Υ.
8. Υποκλοπή κωδικών – στοιχείων πιστωτικών καρτών.
9. Δυνατότητα παρακολούθησης του χρήστη.

Δυνατότητα κατάληψης του Η/Υ από άλλον χρήστη μέσω του Διαδικτύου

Τρόποι δράσης

Ανεξάρτητα από το τι και πώς μολύνει σε ένα σύστημα, ο ιός πρέπει να εξασφαλίσει ορισμένες βασικές συνθήκες, προκειμένου να δράσει. Συγκεκριμένα, πρέπει να μπορεί να εκτελέσει τον κώδικά του και να εξασφαλίσει πρόσβαση σε μέσα αποθήκευσης (κύρια στο σκληρό δίσκο, αλλά όχι μόνο). Γι' αυτό το λόγο πολλοί ιοί προσκολλώνται σε εκτελέσιμα (executable) αρχεία είτε του λειτουργικού συστήματος είτε του κανονικού λογισμικού ενός συστήματος.

Εξασφαλίζουν έτσι δύο πράγματα: Πρώτον, ότι θα μπορούν να αναπαραχθούν και δεύτερον ότι θα μπορέσουν να εκτελέσουν τον κώδικά τους.

Τρόποι διάδοσης

Οι ιοί διαδίδονται από τον ένα υπολογιστή στον άλλο με δύο τρόπους: Είτε μέσω φορητού μέσου αποθήκευσης είτε μέσω δικτύου. Ο δεύτερος τρόπος είναι σήμερα ο πλέον διαδεδομένος, λόγω της ευρείας διάδοσης του Διαδικτύου διεθνώς. Η βασική υπηρεσία διάδοσης ιών είναι αυτή του ηλεκτρονικού ταχυδρομείου (e-mail), μέσω του οποίου αποστέλλονται είτε ως συνημμένα είτε ως τμήμα αυτού καθαυτού του μηνύματος. Για το λόγο αυτό, πολλές υπηρεσίες e-mail προσφέρουν πρώτα σάρωση των μηνυμάτων και των συνημμένων τους με κάποιο αντιβιοτικό, πριν επιτρέψουν στο χρήστη να τα λάβει.

Τρόποι αντιμετώπισης

Οι ιοί αποτέλεσαν και αποτελούν έναν από τους πλέον διαδεδομένους τύπους κακόβουλου λογισμικού. Η ανίχνευση τους από τον απλό χρήστη είναι από δύσκολη έως αδύνατη - ορισμένοι, μάλιστα, ιοί, είναι τόσο προσεκτικά δημιουργημένοι που ακόμη και ο πλέον ειδικευμένος χρήστης αδυνατεί να τους εντοπίσει χωρίς να διαθέτει ειδικά προγραμματιστικά εργαλεία. Για την προστασία ενός συστήματος έχει δημιουργηθεί μια ειδική κατηγορία λογισμικού, γνωστή ως αντιϊκό (antivirus). Προκειμένου να εξασφαλίσουν την απρόσκοπτη και χωρίς μολύνσεις λειτουργία ενός συστήματος, τα αντιϊκά εκκινούν ταυτόχρονα με το λειτουργικό σύστημα του υπολογιστή, χωρίς εντολές από το χρήστη, και παραμένουν ως διαδικασίες στη μνήμη (memory resident), ώστε να είναι σε θέση να ανιχνεύουν τυχόν μολύνσεις σε πραγματικό χρόνο. Τα προγράμματα αυτά πρέπει να αναβαθμίζονται σε τακτική βάση, ώστε να είναι σε θέση να αντιμετωπίζουν με επιτυχία τους νεοδημιουργούμενους ιούς. Σήμερα, αρκετοί οίκοι δημιουργίας λογισμικού

ασχολούνται με τη δημιουργία τέτοιων προγραμμάτων. Τα αντιϊκά είναι σε θέση τόσο να εντοπίσουν μόλυνση τη στιγμή που αποπειράται, όσο και να "καθαρίσουν" τυχόν μολυσμένα αρχεία που εντοπίζουν. Κάθε αντιϊκό έχει το δικό του τρόπο δράσης απέναντι στους ιούς. Ωστόσο, τα περισσότερα είναι σε θέση να εργάζονται σε

πραγματικό χρόνο, εντοπίζοντας τους ιούς τη στιγμή ακριβώς που αποπειρώνται να μολύνουν το σύστημα. Ορισμένα τέτοια προγράμματα προσφέρονται δωρεάν για προσωπική χρήση (δεν καλύπτουν, ωστόσο, ούτε μικρό τοπικό δίκτυο υπολογιστών) και άλλα έναντι σχετικά χαμηλής τιμής (κανένα αντιϊκό για υπολογιστές δικτύου δεν προσφέρεται δωρεάν μέχρι σήμερα). Θα πρέπει να σημειωθεί ότι οι δημιουργοί ιών λαμβάνουν σοβαρά υπόψη τους τις μεθόδους εντοπισμού του "προϊόντος" τους και δημιουργούν ιούς, οι οποίοι προσπαθούν να αποφύγουν τον εντοπισμό, ακόμη και με απενεργοποίηση του αντιϊκού. Αυτό σημαίνει ότι ο χρήστης θα πρέπει να ενημερώνει τακτικότατα το λογισμικό του αλλά και να δημιουργεί τις ειδικές δισκέτες, που τα περισσότερα αντιβιοτικά προγράμματα προτείνουν τη δημιουργία τους, ώστε να είναι δυνατή η εκκαθάριση και η επαναφορά του συστήματος μετά από τυχόν μόλυνσή τους.

Τύποι ιών

Οι ιοί μπορούν να ταξινομηθούν σε δύο μεγάλες κατηγορίες:

Ανάλογα με το σημείο του υλικού ή του λογισμικού που μολύνουν

Τομείς σκληρού δίσκου συστήματος (system sectors)

Αρχεία

Ιοί μακροεντολών (Macros)

Ιοί πηγαίου κώδικα (Source Code Viruses)

Ιοί συμπλεγμάτων (σκληρού) δίσκου ((Hard) Disk Clusters)

Ανάλογα με τον τρόπο με τον οποίο πραγματοποιούν τη μόλυνση

Πολυμορφικοί ιοί
Αόρατοι ιοί (Stealth Viruses)
Θωρακισμένοι ιοί (Armored Viruses)
Πολυτμηματικοί ιοί (Multipartite Viruses)
Ιοί πλήρωσης κενών (Spacefiller Viruses)
Ιοί παραλλαγής (Camouflage Viruses) [5].

Σημείο Επίθεσης

Επιθέσεις άρνησης υπηρεσίας (Denial of service)

Όταν έχουμε μια επίθεση άρνησης υπηρεσίας, ένας εισβολέας εκτελεί κάποια ενέργεια η οποία είτε σταματά κάποια υπηρεσία του συστήματος είτε υποβαθμίζει την ποιότητα της. Για παράδειγμα, η εκτέλεση ενός προγράμματος το οποίο στη συνέχεια θα ξεκινήσει κάποια άλλα προγράμματα, τα οποία με τη σειρά τους θα ξεκινήσουν κάποια άλλα κ.ο.κ. θα προκαλέσει συμφόρηση στο σύστημα και συνεπώς θα εμποδίσει την παροχή των πραγματικών υπηρεσιών για τις οποίες είναι υπεύθυνο.

Μια από τις πρώτες επιθέσεις της μορφής άρνησης υπηρεσίας που εμφανίστηκαν στο Internet ήταν το διάσημο "σκουλήκι" (Worm) του Robert Morris. Ο Morris, ένας αμερικανός φοιτητής, έριξε στο Internet το συγκεκριμένο πρόγραμμα το 1988. Το "σκουλήκι" είχε φτιαχτεί με τέτοιο τρόπο ώστε αντέγραφε τον εαυτό του σε άλλους υπολογιστές στο Internet, ώστε τελικά πολλές χιλιάδες υπολογιστές είχαν μολυνθεί.

Ένα από τα προβλήματα με τις επιθέσεις άρνησης υπηρεσίας που εμφανίζονται στο Internet είναι πως αφού το λογισμικό υλοποιείται με περίπου τον ίδιο τρόπο, κάθε λειτουργικό σύστημα που χρησιμοποιεί το TCP-IP είναι ευάλωτο σε τέτοιου είδους επιθέσεις.

Οι επιθέσεις αυτές εκμεταλλεύονται τις αδυναμίες του λειτουργικού συστήματος και της ασφάλειας ενός υπολογιστή που είναι συνδεδεμένος στο Internet καθώς και τις αδυναμίες των πρωτοκόλλων επικοινωνίας που χρησιμοποιούν οι υπολογιστές. Συνολικά έχουν εμφανισθεί περί τους 90.000 ιοί τα τελευταία 15 χρόνια και ενώ οι περισσότεροι έχουν εξαφανισθεί, περίπου 400 παραμένουν ενεργοί και μπορούν να μολύνουν ανά πάσα στιγμή όποιους υπολογιστές συναντήσουν στην πορεία τους.

Πώς οι ιοί εισέρχονται σε ένα Η/Υ

Οι "ιοί" (δούρειοι ίπποι, "σκουλήκια", κ.α.), εισέρχονται συνήθως στους υπολογιστές των χρηστών, με την ηλεκτρονική αλληλογραφία, καθώς και με το λογισμικό που "κατεβάζουν" οι χρήστες από το διαδίκτυο. Η επικινδυνότητα αυτών των επιθέσεων είναι μέτρια και περιλαμβάνει παρακολούθηση ενεργειών και απώλεια δεδομένων. Η αντιμετώπιση τέτοιου τύπου επιθέσεων περιλαμβάνει την εγκατάσταση εφαρμογών "τείχους προστασίας" (firewall), καθώς και τη χρήση των λεγόμενων "αντιβιοτικών".

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 (on), τότε είναι απενεργοποιημένο το χαρακτηριστικό της αυτόματης εκτέλεσης (auto-execute feature) 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.

Ποιος κατασκευάζει τους ιούς

Υπάρχουν διάφοροι τρόποι δημιουργίας ιών. Μπορούν να δημιουργηθούν από την αρχή χρησιμοποιώντας μια γλώσσα όπως η C ή assembly. Χρησιμοποιούνται τέτοιες γλώσσες γιατί πρέπει ο κώδικας του ιού να είναι όσο το δυνατόν μικρότερος για να μπορεί να αποφεύγει τον εντοπισμό από προγράμματα anti-virus. Οι γλώσσες αυτές επίσης παρέχουν αρκετές δυνατότητες σχετικά χαμηλού επιπέδου που δεν προσφέρονται από άλλες γλώσσες όπως κάποιες λειτουργίες εισόδου / εξόδου. Υπάρχουν επίσης κάποια εργαλεία κατασκευής ιών τα οποία μπορούν να βρεθούν σε διάφορα μέρη στο internet.

Ποιοι δημιουργόυν τους ιούς

Τα πρώτα χρόνια!

Η λαϊκή φαντασία επιμένει ότι οι ιοί δημιουργούνται από τις εταιρείες κατασκευής anti-virus software, οι οποίες με τον τρόπο αυτό διατηρούν και επαυξάνουν συνεχώς την πελατεία τους. Στην πραγματικότητα, όμως, οι εταιρείες αυτές δεν έχουν κανένα λόγο να μπουν στον κόπο της δημιουργίας ιών, αφού η παγκόσμια παραγωγή είναι αρκετή για να τις κρατήσει απασχολημένες για πολλά χρόνια ακόμη.

Κατά καιρούς, διάφοροι δημοσιογράφοι και κοινωνιολόγοι έχουν προσπαθήσει να έρθουν σε επαφή με τους ανθρώπους οι οποίοι δημιουργούν ιούς, σε μια προσπάθεια να κατανοήσουν τον τρόπο σκέψης και τα κίνητρά τους.

Σύμφωνα με όλες τις ενδείξεις η πρώτη επιτυχημένη επαφή αυτής της μορφής πραγματοποιήθηκε από τη Sarah Gordon, συνεργάτιδα της IBM, η οποία κατάφερε να επικοινωνήσει με τον Dark Avenger, έναν Βούλγαρο συγγραφέα ιών, η φήμη του οποίου είχε πάρει μυθικές διαστάσεις μεταξύ των ανθρώπων του χώρου.

Σήμερα!

Η έλευση της visual basic, πριν από μερικά χρόνια, έκανε τον προγραμματισμό πολύ πιο εύκολο για εκατομμύρια ανθρώπους. Δυστυχώς με αυτό τον τρόπο έγινε ευκολότερη και η δημιουργία ιών, ενώ χάρη στο Internet η ταχύτητα διάδοσής τους μειώθηκε από μερικούς μήνες σε μερικές ημέρες ή ακόμη και ώρες. Η πλειοψηφία των συγγραφέων ιών αποτελείται σήμερα από νεαρούς με μικρές τεχνικές γνώσεις, οι οποίοι αντιγράφουν παλαιότερους ιούς και τους διαδίδουν τροποποιημένους, χωρίς πολλές φορές να καταλαβαίνουν και οι ίδιοι ακριβώς με ποιο τρόπο το επιτυγχάνουν. Χαρακτηριστικό παράδειγμα τέτοιου ιού ήταν ο I LOVE YOU, ο οποίος βασίστηκε σε παλιότερο κώδικα και διαδόθηκε τόσο γρήγορα αποκλειστικά και μόνο χάρη στην εξαιρετική ψυχολογική του προσέγγιση (ένα μήνυμα αγάπης είναι πολύ δύσκολο να παραβλεφθεί).

Πως ανακαλύπτονται οι δημιουργοί των ιών

Η λαϊκή φαντασία επιμένει ότι οι ιοί δημιουργούνται από τις εταιρείες κατασκευής anti-virus software, οι οποίες με τον τρόπο αυτό διατηρούν και επαυξάνουν συνεχώς την πελατεία τους. Στην πραγματικότητα, όμως, οι εταιρείες αυτές δεν έχουν κανένα λόγο να μπουν στον κόπο της δημιουργίας ιών, αφού η παγκόσμια παραγωγή είναι αρκετή για να τις κρατήσει απασχολημένες για πολλά χρόνια ακόμη. Κατά καιρούς, διάφοροι δημοσιογράφοι και κοινωνιολόγοι έχουν προσπαθήσει να έρθουν σε επαφή με τους ανθρώπους οι οποίοι δημιουργούν ιούς, σε μια προσπάθεια να κατανοήσουν τον τρόπο σκέψης και τα κίνητρά τους.

Σύμφωνα με όλες τις ενδείξεις η πρώτη επιτυχημένη επαφή αυτής της μορφή πραγματοποιήθηκε από τη Sarah Gordon, συνεργάτιδα της IBM, η οποία κατάφερε να επικοινωνήσει με τον Dark Avenger, έναν Βούλγαρο συγγραφέα ιών, η φήμη του οποίου είχε πάρει μυθικές διαστάσεις μεταξύ των ανθρώπων του χώρου.

Πως αντιλαμβανόμαστε την ύπαρξη τους σε ένα Η/Υ

Αν υποψιάζεστε ή είστε βέβαιοι ότι ο υπολογιστής σας έχει προσβληθεί από ιό υπολογιστή, φροντίστε να αποκτήσετε το τρέχον λογισμικό προστασίας από ιούς. Ακολουθούν ορισμένες βασικές ενδείξεις σύμφωνα με τις οποίες ένας υπολογιστής μπορεί να έχει προσβληθεί:

1. Ο υπολογιστής λειτουργεί πιο αργά από ό, τι συνήθως.
2. Η λειτουργία του υπολογιστή σταματάει ή κλειδώνει συχνά.
3. Ο υπολογιστής παρουσιάζει σφάλματα και μετά κάνει επανεκκίνηση κάθε λίγα λεπτά.
4. Ο υπολογιστής επανεκινεί μόνος του.. Επίσης, ο υπολογιστής δεν λειτουργεί όπως συνήθως.
5. Οι εφαρμογές στον υπολογιστή δεν λειτουργούν σωστά.
6. Δεν είναι δυνατή η πρόσβαση στους δίσκους ή στις μονάδες δίσκου.
7. Δεν είναι δυνατή η σωστή εκτύπωση..
8. Βλέπετε ασυνήθιστα μηνύματα σφάλματος.
9. Βλέπετε παραμορφωμένα μενού και παράθυρα διαλόγου.
10. 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.

Αυτές είναι οι συνηθισμένες ενδείξεις μόλυνσης. Ωστόσο, αυτές οι ενδείξεις μπορεί επίσης να προκληθούν από προβλήματα υλικού ή λογισμικού που δεν έχουν σχέση με ιούς υπολογιστών. Αν δεν εκτελέσετε το Εργαλείο αφαίρεσης κακόβουλου λογισμικού της Microsoft και δεν εγκαταστήσετε ενημερωμένο λογισμικό προστασίας από ιούς στον υπολογιστή σας, δεν μπορείτε να είστε βέβαιοι αν ο υπολογιστής σας έχει προσβληθεί με ιό υπολογιστή.

Συμπτώματα ιών τύπο worm και δούρειου ίππου σε μηνύματα ηλεκτρονικού ταχυδρομείου

Όταν ένας ιός υπολογιστή προσβάλλει μηνύματα ηλεκτρονικού ταχυδρομείου ή άλλα αρχεία σε έναν υπολογιστή, μπορεί
να προσέξετε τα εξής συμπτώματα:

1. Το προσβεβλημένο αρχείο ενδέχεται να παραγάγει αντίγραφα του εαυτού του. Με αυτόν τον τρόπο μπορεί να χρησιμοποιηθεί ολόκληρος ο ελεύθερος χώρος στον σκληρό δίσκο.
2. Ένα αντίγραφο του προσβεβλημένου αρχείου ενδέχεται να αποσταλεί σε όλες τις διευθύνσεις που υπάρχουν σε μια λίστα διευθύνσεων ηλεκτρονικού ταχυδρομείου.
3. Ο ιός του υπολογιστή ενδέχεται να διαμορφώσει ξανά το σκληρό δίσκο. Με αυτόν τον τρόπο θα διαγραφούν αρχεία και προγράμματα.
4. Οι ιοί υπολογιστών μπορούν να εγκαταστήσουν κρυφά προγράμματα, όπως πειρατικό λογισμικό. Αυτό το πειρατικό λογισμικό μπορεί να διανεμηθεί και να πωληθεί από τον υπολογιστή.
5. Ο ιός υπολογιστή ενδέχεται να υποβαθμίσει την ασφάλεια. Αυτό θα μπορούσε να επιτρέψει σε εισβολείς να αποκτήσουν απομακρυσμένη πρόσβαση στον υπολογιστή ή το δίκτυο.

6. Λαμβάνετε ένα μήνυμα ηλεκτρονικού ταχυδρομείου που περιέχει ένα παράξενο συνημμένο. Όταν ανοίγετε το συνημμένο αρχείο, εμφανίζονται παράθυρα διαλόγου ή σημειώνεται ξαφνική υποβάθμιση των επιδόσεων του συστήματος.
7. Κάποιος σάς λέει ότι πρόσφατα έλαβε μηνύματα ηλεκτρονικού ταχυδρομείου από εσάς που περείχαν συνημμένα αρχεία που δεν στείλατε. Τα αρχεία που είναι συνημμένα στα μηνύματα ηλεκτρονικού ταχυδρομείου έχουν επεκτάσεις όπως .exe, .bat, .scr και .vbs.

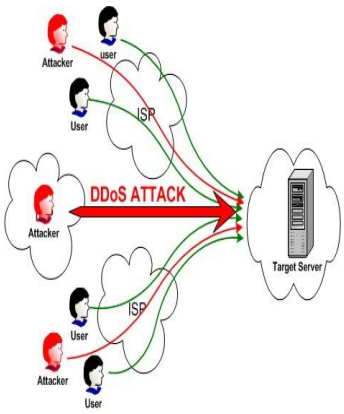
Συμπτώματα που μπορεί να οφείλονται σε συνήθεις λειτουργίες των Windows

Μια μόλυνση από ιό υπολογιστή μπορεί να προσκαλέσει τα εξής προβλήματα:

1. Τα Windows δεν ξεκινούν, παρόλο που δεν έχετε πραγματοποιήσει αλλαγές στο σύστημα ή δεν έχετε εγκαταστήσει ή καταργήσει κάποιο πρόγραμμα.
2. Υπάρχει συχνή δραστηριότητα του μόντεμ. Αν έχετε εξωτερικό μόντεμ, ενδέχεται να παρατηρήσετε ότι οι λυχνίες αναβοσβήνουν συχνά ενώ το μόντεμ δεν χρησιμοποιείται. Ενδέχεται να διανέμετε πειρατικό λογισμικό χωρίς να το γνωρίζετε.
3. Τα Windows δεν ξεκινούν επειδή λείπουν ορισμένα σημαντικά αρχεία συστήματος. Επιπλέον, εμφανίζεται ένα μήνυμα σφάλματος που αναφέρει τα αρχεία που λείπουν.
4. Ο υπολογιστής ξεκινά μερικές φορές με τον αναμενόμενο τρόπο. Ωστόσο, άλλες φορές, ο υπολογιστής σταματά να ανταποκρίνεται προτού εμφανιστούν τα εικονίδια της επιφάνειας εργασίας και η γραμμή εργασιών.
5. Ο υπολογιστής λειτουργεί πολύ αργά. Επίσης, απαιτείται περισσότερος χρόνος από τον αναμενόμενο για να γίνει εκκίνηση του υπολογιστή.
6. Εμφανίζονται μηνύματα σφάλματος που αναφέρουν ότι "Η μνήμη δεν επαρκεί" (Out-of-memory) ακόμη και αν ο υπολογιστής διαθέτει επαρκή μνήμη RAM.
7. Τα νέα προγράμματα δεν έχουν εγκατασταθεί σωστά.
8. Γίνεται απροσδόκητη επανεκκίνηση των Windows.
9. Ορισμένα προγράμματα, τα οποία λειτουργούσαν κανονικά, συχνά σταματούν να ανταποκρίνονται. Ακόμα και αν καταργήσετε και εγκαταστήσετε ξανά τα προγράμματα, το πρόβλημα εξακολουθεί να υπάρχει.
10. Ένα βοηθητικό πρόγραμμα δίσκων, όπως η Εξέταση Δίσκων (Scandisk), αναφέρει πολλά σοβαρά σφάλματα δίσκου.
11. Ένα διαμέρισμα δίσκου εξαφανίζεται.

12. Ο υπολογιστής σταματά πάντα να ανταποκρίνεται όταν προσπαθείτε να χρησιμοποιήσετε προϊόντα του Microsoft Office. Δεν είναι δυνατή η εκκίνηση της Διαχείρισης Εργασιών (Task Manager) των Windows.
13. Το πρόγραμμα προστασίας από ιούς υποδεικνύει ότι υπάρχει ιός υπολογιστή.

Αυτά τα προβλήματα μπορεί επίσης να συμβαίνουν λόγω των κανονικών λειτουργιών των Windows ή προβλημάτων στα Windows που δεν προκαλούνται από ιό υπολογιστή.



ΠΗΓΕΣ

http://support.microsoft.com
http://dide.flo.sch.gr
http://pacific.jour.auth.gr
http://el.wikipedia.org/wiki/