Ερευνητική Εργασία:
Ασφάλεια στο Διαδίκτυο

ΔΙΑΜΟΙΡΑΣΜΟΣ ΑΡΧΕΙΩΝ ΜΕΤΑΦΟΡΤΩΣΗ ΑΡΧΕΙΩΝ

ΓΕΝΙΚΟ ΛΥΚΕΙΟ ΜΟΙΡΩΝ

Ερευνητική Ομάδα: Βασιλάκης Γεώργιος, Ξεκαρδάκης Ιωάννης, Κουτσάκης Ιωάννης, Καργάκης Στέφανος

2011-2012

ΔΙΑΜΟΙΡΑΣΜΟΣ ΑΡΧΕΙΩΝ

Το Διαδίκτυο παρέχει στους χρήστες του τη δυνατότητα να διαμοιράζονται αρχεία κάθε είδους μέσω διαφόρων προγραμμάτων που λειτουργούν έτσι ώστε να κάνουν κοινόχρηστο ένα μέρος του σκληρού δίσκου του τοπικού υπολογιστή ενός χρήστη, σε όλους τους χρήστες οι οποίοι είναι συνδεδεμένοι στο Διαδίκτυο και χρησιμοποιούν το ίδιο πρόγραμμα.

Η διάδοση της χρήσης της δυνατότητας αυτής οφείλεται στην μεγάλη ευκολία εύρεσης και τοπικής αποθήκευσης κάθε είδους αρχείων με ελάχιστο κόστος για τον χρήστη.

Οι κίνδυνοι, από την χρήση προγραμμάτων διαμοιρασμού αρχείων στο κυρίως στα εξής:

Ασφάλεια

Η χρήση των προγραμμάτων διαμοιρασμού αρχείων παραβιάζει τους κανόνες «υγιεινής» και «ασφάλειας» του υπολογιστή μας. Μοιραζόμαστε

«πράγματα» με χρήστες που δεν τους γνωρίζουμε και δεν τους εμπιστευόμαστε. Η «υγεία» του υπολογιστή μας κινδυνεύει από ιούς και άλλα καταστροφικά προγράμματα που διαχέονται στον υπολογιστή μας και τον μολύνουν. Οι ιοί μπορούν να καταστρέψουν τον υπολογιστή μας. Άλλα προγράμματα (π.χ. spyware) μπορούν να καταγράψουν τις δραστηριότητες μας στο Διαδίκτυο και να στείλουν αυτή την πληροφορία σε τρίτους ή να προκαλούν εμφάνιση διαφημιστικών μηνυμάτων ακόμη και όταν δεν είμαστε συνδεδεμένοι

Νομικά προβλήματα

Τα περισσότερα αρχεία, που είναι διαθέσιμα μέσα από τα προγράμματα διαμοιρασμού (βίντεο, μουσική, τραγούδια, βιντεοπαιχνίδια), έχουν προστατευμένα δικαιώματα. Αυτό σημαίνει ότι ο νόμος προστατεύει το δικαίωμα του ιδιοκτήτη να επιβάλλει περιορισμούς στην αντιγραφή και την διακίνηση του προϊόντος. Η απόκτηση (download) και η διάθεση (upload) προϊόντων χωρίς την άδεια του ιδιοκτήτη μπορεί να προκαλέσει νομικά προβλήματα. Η ανωνυμία δεν είναι ποτέ απόλυτα δεδομένη στο Διαδίκτυο. Σε αρκετές περιπτώσεις υπήρξαν διώξεις «πειρατών», που διακινούσαν παράνομα αρχεία μουσικής.

Προσωπικά δεδομένα

Αν, από λάθος στις ρυθμίσεις του προγράμματος διαμοιρασμού αρχείων, γίνει κοινόχρηστος ολόκληρος ο σκληρός δίσκος του τοπικού υπολογιστή, τότε προσωπικά δεδομένα, που πιθανόν έχετε στον υπολογιστή σας όπως αριθμοί πιστωτικών καρτών ή φορολογικά δεδομένα, θα εκτεθούν σε όλους τους χρήστες που χρησιμοποιούν το πρόγραμμα αυτό.

Δωρεάν Προγράμματα Διαμοιρασμού Αρχείων: Αξίζουν;

Το "Δωρεάν" συχνά έρχεται με ένα αντίτιμο.

Οι Online υπηρεσίες διαμοιρασμού αρχείων μπορεί να εκπληρώνουν μια νομική απαίτηση. Ωστόσο ορισμένες έχουν αμφισβητήσιμη χρήση.

Η υπόσχεση για δωρεάν μουσική, ταινίες και προγράμματα είναι ισχυρό δέλεαρ για πολλούς ανθρώπους. Οι συγγραφείς ιών το ξέρουν. Αυτός είναι ο λόγος που έχουν ανεβάσει τα δικά τους αρχεία μεταμφιεσμένα σε δημοφιλείς επιλογές.

Σιγουρευτείτε ότι κάνετε ασφαλή χρήση των δικτύων διαμοιρασμού αρχείων.

ΜΕΤΑΦΟΡΤΩΣΗ ΑΡΧΕΙΩΝ

Ασφαλές Download-ing!!!

Πολλά προγράμματα που προσφέρονται για μεταφόρτωση (download) είναι απολύτως νόμιμα, μερικά όμως μπορεί να περιέχουν *spyware*, ή κακόβουλο κώδικα που μπορεί να βλάψει τον φυλλομετρητή σας, ή να μολύνει το υπολογιστή σας με έναν ιό. Χρησιμοποιήστε για προστασία κάποιο *anti-spyware* και *anti-virus* πρόγραμμα. Γενικά, καλό είναι πριν από κάθε download να έλεγχετε τί λένε οι υπόλοιποι, πολλές φορές μπορεί να αποδειχτεί σωτήριο. Ανοίξτε μια μηχανή αναζήτησης, γράψτε το όνομα του προγράμματος, και δίπλα τη λέξη "spyware". Αμέσως θα δείτε αν κάποιοι είχαν προβλήματα. Πάντα να ανιχνεύετε τα προγράμματα για ιούς πριν τα εκτελέσετε. Και βέβαια, να κάνετε τακτικά *backup*.

Τι πρέπει να κάνω για να προφυλαχτώ από ιούς;

Κατ' αρχάς πρέπει να κατανοήσετε πως μεταφέρεται ένας ιός.

Ένας ιός μεταδίδεται μέσω εκτελέσιμων αρχείων, τα οποία εκτελούν δέσμες, προγράμματα ή ρουτίνες. Τέτοιοι τύποι είναι: .exe, .com, .bat, .vbs κ.α.

Αρχεία τα οποία ΔΕΝ περιέχουν ιούς είναι τα αρχεία κειμένου txt και τα αρχεία φωτογραφιών απλού τύπου .gif, .jpg, .bmp, .tif (αν και πλέον ούτε αυτά είναι απόλυτα ασφαλή).

Τα αρχεία του Word (.doc) μπορεί να εμπεριέχουν μακροεντολές που να είναι επιβλαβής. Συνήθως όμως το Word είναι ρυθμισμένο κατά τέτοιο τρόπο που μας προειδοποιεί ότι περιέχει μακροεντολές το αρχείο. Εάν δεν το εμπιστεύεστε σε αυτή την ερώτηση πρέπει να απαντήστε ΟΧΙ.

Οι ιοί εξελίσσονται, οπότε μπορεί αύριο να δημιουργηθεί ένας ιός ο οποίος για παράδειγμα να προσκολλάει σε εικόνες τύπου jpg, gif ή οτιδήποτε άλλο.

Ο καλύτερος τρόπος προφύλαξης είναι:

1) Δεν ανοίγουμε ποτέ αρχεία που έρχονται με *e-mail* και δεν γνωρίζουμε ακριβώς για τι πρόκειται και ποιος το στέλνει. Ακόμη και τον αποστολέα

να γνωρίζουμε, ΔΕΝ πρέπει να είμαστε 100% σίγουροι, γιατί μπορεί να πρόκειται για ιο που χρησιμοποιεί τον υπολογιστή του.

2) Χρησιμοποιούμε προγράμματα *antivirus* τα οποία κάνουν αυτόματη ανανέωση μέσω του Internet για νέους ιούς.
3) Ρυθμίζουμε τον υπολογιστή ώστε να μην επιτρέπει την αυτόματη εκτέλεση επιβλαβών στοιχείων.
4) Προσέχουμε πάντα τις τοποθεσίες που επισκεπτόμαστε, και δεν εκτελούμε αρχεία μέσω του Web.
5) Δεν κατεβάζουμε ανεξέλεγκτα προγράμματα που δεν γνωρίζουμε, και πάντα από πηγές που εμπιστευόμαστε.
6) Εφόσον χρησιμοποιούμε Internet, χρησιμοποιούμε προγράμματα που δεν επιτρέπουν σε άλλους χρήστες ή προγράμματα να συνδεθούν στον υπολογιστή μας, να κάνουν επιθέσεις μέσω Internet, ή να χρησιμοποιήσουν κάποιες "ανοιχτές πόρτες" και να μολύνουν τον υπολογιστή μας.

Τι είναι ένας ιός υπολογιστή;

Οι ιοί των υπολογιστών είναι μικρά προγράμματα λογισμικού που έχουν σχεδιαστεί για να εξαπλωθεί από τον έναν υπολογιστή στον άλλον και να παρεμβαίνουν στη λειτουργία του υπολογιστή.

Ένας ιός μπορεί να αλλοιώσει ή να διαγράφουν δεδομένα στον υπολογιστή σας ή ακόμα και να διαγράψει τα πάντα στον σκληρό σας δίσκο.

Οι ιοί υπολογιστών συχνά μεταδίδονται με τα συνημμένα σε μηνύματα ηλεκτρονικού ταχυδρομείου ή άμεσων μηνυμάτων. Γι 'αυτό και είναι σημαντικό ότι ποτέ δεν ανοίγετε συνημμένα ηλεκτρονικού ταχυδρομείου εάν δεν γνωρίζετε ποιος είναι και από που το περιμένουν. Έπειτα μπορεί να χρησιμοποιεί το πρόγραμμα ηλεκτρονικού ταχυδρομείου σας για να μεταδοθεί σε άλλους υπολογιστές, Οι ιοί μπορεί να είναι μεταμφιεσμένοι ως συνημμένα με αστείες εικόνες, ευχετήριες κάρτες ή αρχεία ήχου και βίντεο.

Οι ιοί υπολογιστών επίσης να μεταδοθούν μέσω downloads στο διαδίκτυο. Μπορούν να κρυφτούν σε παράνομο λογισμικό ή άλλα αρχεία ή προγράμματα που μπορείτε να κατεβάσετε.

Για να αποφύγετε τους ιούς των υπολογιστών, είναι σημαντικό να κρατάτε το αντιϊκό του υπολογιστή σας ενημερωμένο με τις πιο πρόσφατες ενημερώσεις και εργαλεία αντιμετώπισης ιών, ενημερωθείτε για τις πρόσφατες απειλές και να ακολουθείτε μερικούς βασικούς κανόνες όταν εσείς σερφάρετε στο Internet, κατεβάζετε αρχεία ή ανοίγετε συνημμένα.

Μόλις ανακαλύψετε ότι ένας ιός είναι εγκατεστημένος στον υπολογιστή σας, είναι σημαντικό να τον αφαιρέσετε άμεσα για πρόληψη περαιτέρω μόλυνσης, τόσο εσάς όσο και των γνωστών σας.

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)

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.

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.

Τρόπος 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.

ΠΗΓΕΣ:

- http://infonea.blogspot.com/
- http://www.pcproblems.gr/
- http://www.microsoft.com/
- http://el.wikipedia.org/
- http://www.e-yliko.gr