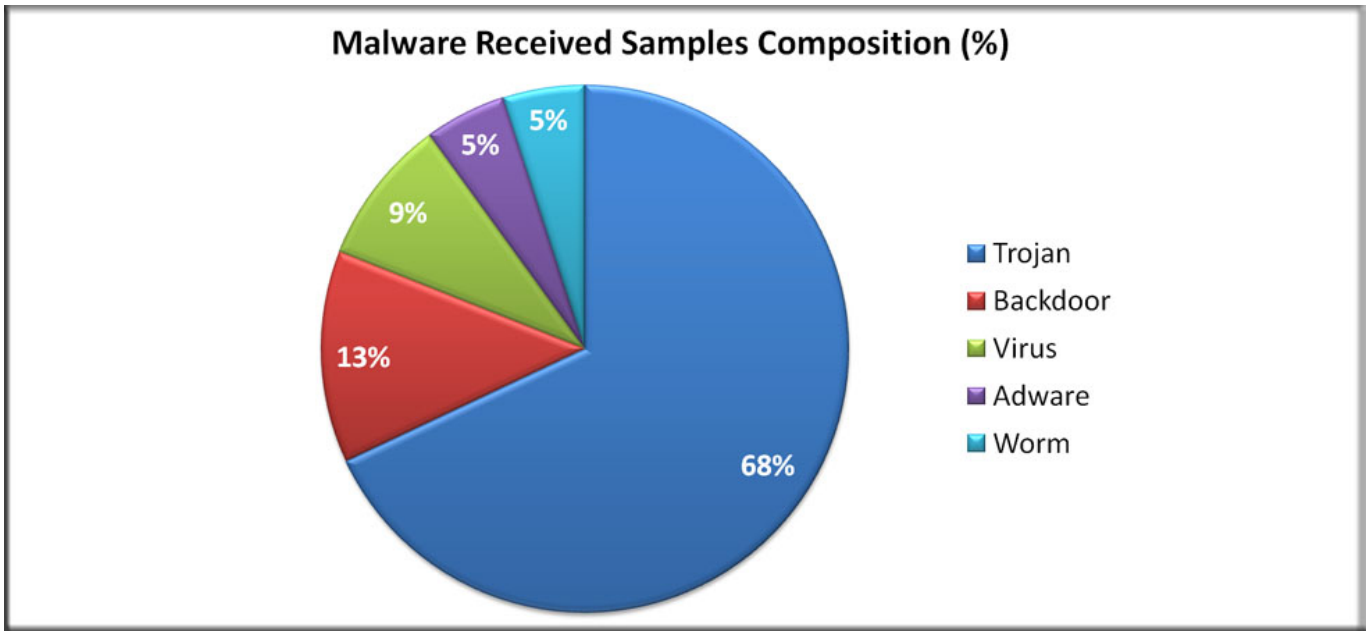
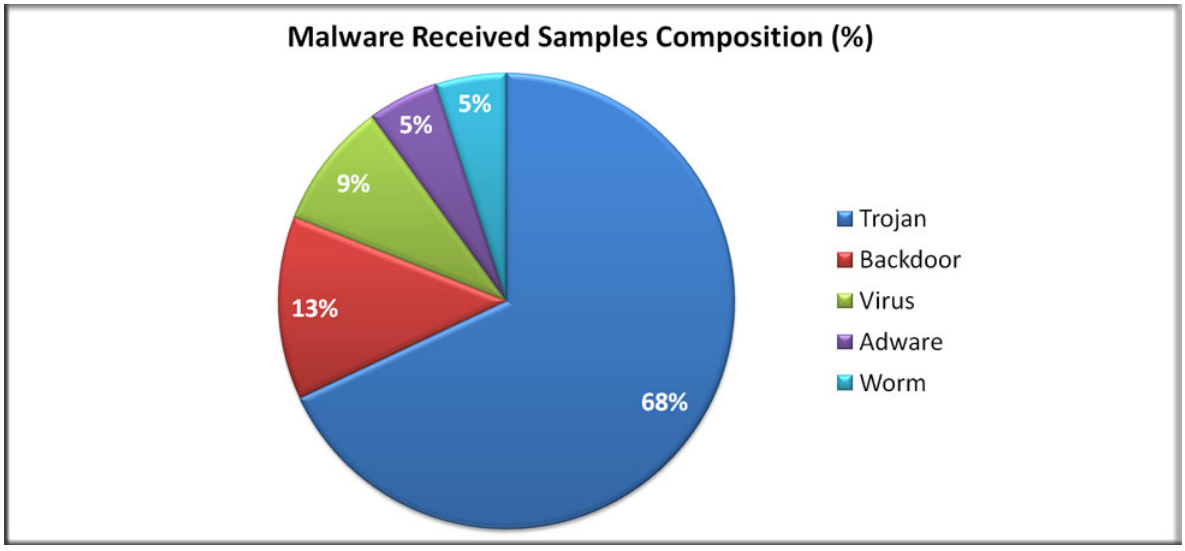
10 Ιουλίου 2014

Ένας γρήγορος οδηγός για τα malware

Επιστήμες / Πληροφορική & Internet





Νομίζετε ότι ξέρετε για τι μιλάμε όταν λέμε κακόβουλο λογισμικό; Το παρακάτω άρθρο είναι για να βεβαιωθούμε ότι ξέρουμε για τι “πράγμα” μιλάμε αλλά περιέχει και μερικές βασικές συμβουλές από το infoworld για το τι πρέπει να κάνουμε όταν έχουμε χτυπηθεί από malware.

Ιοί – Viruses

Ένας ιός υπολογιστών είναι αυτό που ο περισσότερος κόσμος αποκαλεί κάθε πρόγραμμα malware που αναφέρετε στις ειδήσεις. Ευτυχώς που τα περισσότερα προγράμματα malware δεν είναι ιοί. Ένας ιός υπολογιστών τροποποιεί νόμιμα

αρχεία υποδοχής του υπολογιστή (ή δείκτες σε αυτούς) κατά τέτοιο τρόπο, ώστε όταν ο χρήστης θελήσει να τρέξει ένα αρχείο, τρέχει αυτόματα τον ιό.

Οι απλοί ιοί υπολογιστών είναι αρκετά ασυνήθιστοι σήμερα και εκπροσωπούν το λιγότερο από το 10% του συνόλου των malware. Αυτό είναι καλό, καθώς οι ιοί είναι το μόνο είδος κακόβουλου λογισμικού που “μολύνει” άλλα αρχεία. Αυτό καθιστά ιδιαίτερα δύσκολη την απομάκρυνση τους από το σύστημα, επειδή μολύνουν αρχεία από το νόμιμο πρόγραμμα και αυτά αναπαράγουν τον ιό. Τα καλύτερα antivirus αδυνατούν να καθαρίσουν σωστά ένα σύστημα και σε πολλές περιπτώσεις απλά βάζουν σε καραντίνα τον ιό ή τον διαγράφουν. Όμως το σύστημα παραμένει μολυσμένο.

Σκουλήκια – Worms

Τα σκουλήκια υπάρχουν πολύ πριν από τους ιούς των υπολογιστών, από την εποχή mainframe. Τα e-mail τους έφεραν στη μόδα στα τέλη της δεκαετίας του 1990, και για σχεδόν μια δεκαετία, οι υπολογιστές υπέφεραν από αυτά καθώς έφταναν συνεχώς συνημμένα με τα μηνύματα ηλεκτρονικού ταχυδρομείου. Χρειάζεται ένα άτομο να ανοίξει ένα τέτοιο συνημμένο και ολόκληρη η εταιρεία θα προσβληθεί σε χρόνο μηδέν.

Το ιδιαίτερο χαρακτηριστικό τους είναι ότι τα σκουλήκια είναι αυτοαναπαραγόμενα. Πάρτε το διαβόητο worm ILOVEYOU: Χτύπησε σχεδόν σε κάθε χρήστη ηλεκτρονικού ταχυδρομείου στον κόσμο, υπερφόρτωσε τηλεφωνικά συστήματα (με την αποστολή κείμενων), έριξε τηλεοπτικά δίκτυα, και μία καθημερινή εφημερίδα καθυστέρησε την κυκλοφορία της για μισή ημέρα. Υπάρχουν πολλά άλλα σκουλήκια, συμπεριλαμβανομένων του SQL Slammer και του MS Blaster, που καθιέρωσαν και εξασφάλισαν μια πρωταγωνιστική θέση για τα Worms στην ιστορία της ασφάλειας των υπολογιστών.

Αυτό που κάνει τόσο αποτελεσματικό ένα σκουλήκι αλλά και τόσο καταστροφικό είναι η ικανότητά του να εξαπλώνετε χωρίς την άδεια του χρήστη. Οι ιοί, αντίθετα, απαιτούν κάποιο εναρκτήριο λάκτισμα από τον χρήστη, πριν να προσπαθήσουν να μολύνουν άλλα αθώα αρχεία ή άλλους χρήστες. Τα σκουλήκια εκμεταλλεύονται άλλα αρχεία και προγράμματα για να κάνουν τη βρώμικη δουλειά. Για παράδειγμα, το SQL Slammer worm χρησιμοποίησε μια (patched) ευπάθεια του Microsoft SQL για να επιβαρύνει με υπερχειλίσεις buffer σχεδόν σε κάθε unpatched διακομιστή SQL που ήταν συνδεδεμένος στο Internet σε περίπου 10 λεπτά, ένα ρεκόρ που στέκεται ακόμα και σήμερα.

Δούρειος ίππος – Trojan

Τα σκουλήκια σήμερα έχουν αντικατασταθεί από προγράμματα malware Trojansσαν νέο όπλο επίθεσης από τους hackers. Τα Trojans μεταμφιέζονται ως νόμιμα προγράμματα, αλλά περιέχουν κακόβουλες οδηγίες. Υπάρχουν σχεδόν από πάντα, ακόμα πιο πριν και από τους ιούς των υπολογιστών, αλλά έχουν επικρατήσει στους σημερινούς υπολογιστές περισσότερο από κάθε άλλο είδος κακόβουλου λογισμικού.

Ένα Trojan πρέπει να εκτελεστεί από το θύμα του για να κάνει τη δουλειά του. Τα Trojans συνήθως φτάνουν μέσω e-mail ή από ιστοσελίδες που έχουν μολυνθεί και κάποιος χρήστης τις επισκέπτεται. Το πιο δημοφιλές είδος Trojan είναι ένα ψεύτικο πρόγραμμα προστασίας από ιούς, το οποίο αναδύεται και ισχυρίζεται ότι έχετε μολυνθεί. Αν δώσετε εντολή να τρέξει το πρόγραμμα για να καθαρίσετε τον υπολογιστή σας τότε το Trojan ριζώνει.

Από τα Trojans είναι δύσκολο να προστατευτείτε για δύο λόγους: Είναι εύκολο να δημιουργηθούν (οι εγκληματίες του κυβερνοχώρου που συνήθως τα παράγουν δεν δυσκολεύονται καθώς έχουν δημιουργηθεί Trojan-building kits που διευκολύνουν το έργο τους) και εξαπλώνονται πολύ γρήγορα αφού μπορούν και εξαπατούν τον τελικό χρήστη – καθώς ένα patch, ή ένα τείχος προστασίας, ή άλλες παραδοσιακές άμυνες δεν μπορούν να τα σταματήσουν. Οι κακόβουλοι παραγωγοί των Malwares κερδίζουν από τα Trojans εκατομμύρια κάθε μήνα.

Πηγή: SecNews.gr

http://bit.ly/1m9BqbC