11 Ιουλίου 2014

Αντιμετωπίζοντας τα malware (spyware, adware κλπ.)

/ Πεμπτουσία

Image not found or type unknown

Ολοκληρώνουμε την «ξενάγησή» μας στον κόσμο του κακόβουλου λογισμικού με τα Υβρίδια και τις εξωτικές μορφές, καθώς επίσης και με τα Spyware και adware, ενώ παραθέτουμε και χρήσιμες πληροφορίες για την αντιμετώπιση των διαφόρων απειλών.

Υβρίδια και εξωτικές μορφές – Hybrids and exotic forms

Σήμερα, τα περισσότερα malware είναι ένας συνδυασμός των παραδοσιακών κακόβουλων προγραμμάτων, συχνά επίσης περιλαμβάνουν και μέρη των Trojans και worms και περιστασιακά έναν ιό. Συνήθως, το πρόγραμμα malware θα εμφανιστεί στον τελικό χρήστη ως ένα Trojan, αλλά μόλις εκτελεστεί, επιτίθεται σε άλλα θύματα μέσω του διαδικτύου, όπως ένα worm (σκουλήκι).

Πολλά από τα προγράμματα malware σήμερα θεωρούνται rootkits ή προγράμματα stealth. Ουσιαστικά, τα προγράμματα malware προσπαθούν να τροποποιήσουν το βασικό λειτουργικό σύστημα για να αναλάβουν τον απόλυτο έλεγχο και να κρύβονται από τα antimalware προγράμματα. Για να απαλλαγούμε από αυτά τα

είδη των προγραμμάτων, θα πρέπει να αφαιρέσετε το στοιχείο ελέγχου από τη μνήμη, αρχίζοντας με μία σάρωση από ενα antimalware.

Τα Bots είναι ουσιαστικά συνδιασμοί Trojan / worn που προσπαθούν να κάνουν ατομικούς πελάτες-θύματα ένα μέρος ενός μεγαλύτερου κακόβουλου δίκτυου. Οι Botmasters έχουν ένα ή περισσότερους “διοίκησης και ελέγχου” servers στους οποίους οι bot πελάτες ελέγχουν για να λάβετε ενημερωμένες οδηγίες τους. Τα botnet κυμαίνονται σε μέγεθος από μερικές χιλιάδες μολυσμένους υπολογιστές μέχρι τεράστια δύκτια με εκατοντάδες χιλιάδες συστημάτα υπό τον έλεγχο ενός κεντρικού botnet. Τα botnets συχνά ενοικιάζονται σε άλλους εγκληματίες που χρησιμοποιούν στη συνέχεια για τους δικούς τους φαύλους σκοπούς.

Spyware και adware

Αν είστε τυχεροί, τότε το μόνο πρόγραμμα malware που έχετε έρθει σε επαφή είναι απλά ένα adware, το οποίο επιχειρεί να εκθέσει σε κίνδυνο το τελικό χρήστη σε κάτι ανεπιθύμητο, πιθανά σε μία κακόβουλη διαφήμιση. Ένα κοινό πρόγραμμα adware μπορεί να ανακατευθύνει τις αναζητήσεις προγραμμάτων περιήγησης του χρήστη να μοιάζουν με ιστοσελίδες που περιέχουν όμως άλλες προσφορές προϊόντων.

Μια άλλη κατηγορία είναι το malware spyware, το οποίο πιο συχνά χρησιμοποιείται από τους ανθρώπους που θέλουν να ελέγχουν τις δραστηριότητες των υπολογιστών των αγαπημένων τους προσώπων. Φυσικά, σε στοχευμένες επιθέσεις, οι εγκληματίες μπορούν να χρησιμοποιήσουν λογισμικό υποκλοπής spyware για να καταγράψουν την πληκτρολόγηση των θυμάτων και να αποκτήσουν πρόσβαση σε κωδικούς πρόσβασης ή πνευματικής ιδιοκτησίας.

Τα Adware και spyware προγράμματα είναι συνήθως το πιο εύκολο να αφαιρέσετε, επειδή δεν είναι σχεδόν φαύλα ως προς τις προθέσεις τους. Βρείτε το κακόβουλο εκτελέσιμο αρχείο, αποτρέψετο να εκτελείται – τελειώσατε.

Η καταπολέμηση της απειλής

Σήμερα, πολλά προγράμματα malware ξεκινούν ως ένα Trojan ή ιός τύπου worm, αλλά στη συνέχεια προσκαλούν ένα botnet και αφήνουν στον επιτιθέμενο χρήστη τον υπολογιστή και το δίκτυο του θύματος. Πολλές προηγμένες επίμονες επιθέσειςξεκινούν με αυτόν τον τρόπο: Χρησιμοποιούν Trojans να αποκτήσουν το αρχικό προσβαση σε εκατοντάδες ή χιλιάδες επιχειρήσεις, ενώ οι ανθρώπινες επιθέσεις παραμονεύουν, σε αναζήτηση μιάς ενδιαφέρουσας πνευματικής ιδιοκτησίας. Η συντριπτική πλειοψηφία του κακόβουλου λογισμικού υπάρχει για να κλέψουν χρήματα – άμεσα από έναν τραπεζικό λογαριασμό ή έμμεσα με το να

κλέβουν τους κωδικούς πρόσβασης ή ταυτότητες.

Αν είστε τυχεροί, μπορείτε να βρείτε τα κακόβουλα εκτελέσιμα αρχεία χρησιμοποιώντας ένα πρόγραμμα όπως το Autoruns της Microsoft ή το Silent Runners. Αν το πρόγραμμα malware είναι λαθραίο, θα πρέπει να αφαιρέσετε το κομμάτι του που κρύβεται στη μνήμη πρώτα (αν είναι δυνατόν) και στη συνέχεια να εργαστείτε για να ξεριζώσετε το υπόλοιπο του προγράμματος. Συχνά εκκίνω τον υπολογιστή μου σε ασφαλή λειτουργία ή μέσω άλλης μεθόδου, αφαιρώ την ύποπτη συνιστώσα stealth (μερικές φορές κάνοντας του απλή μετονομασία), και τρέχω ένα καλό antivirus scanner μερικές φορές για να καθαρίσει τα υπολείμματα του stealth.

Δυστυχώς, η εύρεση και την αφαίρεση μεμονωμένων στοιχείων ενός προγράμματος κακόβουλου λογισμικού είναι θέλημα μόνο ενός ανόητου. Είναι εύκολο να κανετε λάθος και να χάσετε ένα στοιχείο. Πλέον, δεν ξέρετε αν το πρόγραμμα malware έχει τροποποιησεί το σύστημα με τέτοιο τρόπο ώστε να είναι αδύνατο να γίνει εντελώς αξιόπιστο και πάλι.

Όταν βρείτε κακόβουλο λογισμικό σε έναν υπολογιστή, αν δεν είστε καλά εκπαιδευμένοι στην απομάκρυνση του κακόβουλου λογισμικού, κάντε αντίγραφα ασφαλείας των δεδομένων (εάν απαιτείται), διαμόρφωστε (format) την μονάδας δίσκου, και εγκαταστήστε ξανά τα προγράμματα και τα δεδομένα. Επιδιωρθώστε σωστά την ζημιά και βεβαιωθείτε ότι οι τελικοί χρήστες θα καταλάβουν τι έκαναν λάθος. Με αυτόν τον τρόπο, μπορείτε να πάρετε ένα αξιόπιστο υπολογιστή και να προχωρήσοετε μπροστά στον αγώνα χωρίς κινδύνους ή παρατεταμένες ερωτήσεις.

Πηγή: SecNews.gr