19 Φεβρουαρίου 2015

Malware χρησιμοποιούν τα Windows για να μολύνουν υπολογιστές

/ Πεμπτουσία

Image not found or type unknown

Οι εγκληματίες του κυβερνοχώρου έχουν αναπτύξει ένα νέο εργαλείο για να τους βοηθήσει να διανείμουν κακόβουλο λογισμικό σε υπολογιστές κάνοντας κατάχρηση νόμιμων λειτουργιών των *Windows* και βελτιώνοντας συνεχώς τον κώδικα τους. Το πρόσφατο malware downloader ονομάστηκε"f0xy" από τους ερευνητές στο Websense, όταν το ανάλυσαν για να δουν τις δυνατότητές του.

Σύμφωνα με την ανάλυσή τους, οι developers της απειλής εργάζονται συνεχώς σε αυτό, προκειμένου να καταφέρουν μια έκδοση που να είναι συμβατή με το μεγαλύτερο αριθμό των λειτουργικών συστημάτων και που να μπορούν να τρέχουν απαρατήρητα για μεγαλύτερο χρονικό διαστήματα.

Οι ερευνητές βρήκαν ότι το f0xy στηρίζεται σε μια δυναμική λίστα C & C διακομιστών προκειμένου να προωθεί κακόβουλα αρχεία. Μια άλλη στρατηγική που υιοθετήθηκε από τους developers για να αποφύγουν την ανίχνευση του, είναι να χρησιμοποιούν την υπηρεσία μεταφοράς της Microsoft για να κατέβουν τα δεδομένα στον υπολογιστή.

Μερικά από τα δείγματα που καθόρισε το Websense, χρονολογούνται από τον Ιανουαρίου του 2015 και μπορούν να τρέξουν μόνο σε εκδόσεις Windows Vista και μεταγενέστερες. Νεότερες εκδόσεις έχουν αναπτυχθεί, εν τούτοις, συμπεριλαμβανομένης της υποστήριξης για τα Windows XP.

Το κακόβουλο λογισμικό που κατεβαίνει από το f0xy δεν υποκλέπτει ευαίσθητες πληροφορίες όπως κωδικούς πρόσβασης ή οικονομικά στοιχεία. Φαίνεται ότι οι διαχειριστές του, το χρησιμοποιούν για να βγάλουν χρήματα, όπως παρατήρησε το Websense, αφού εγκαθιστά ένα crypto-currency miner στο σύστημα που έχει επηρεαστεί.

Κατά τη στιγμή των test, μόνο πέντε από τις 57 μηχανές anti-virus που είναι διαθέσιμες στο VirusTotal, ήταν σε θέση να εντοπίσουν το malware. Ωστόσο, σε επόμενες ανιχνεύσεις που έγιναν πριν από τρεις ημέρες, έδειξαν βελτιωμένη ανίχνευση, αφού 10 software μπόρεσαν να ανιχνεύσουν το malware.

Πηγή: Secnews.gr