



Το FBI προειδοποιεί για το κακόβουλο λογισμικό DNS Changer

Περίπου 360.000 υπολογιστές Windows σε όλο τον κόσμο κινδυνεύουν να μείνουν χωρίς πρόσβαση στο Διαδίκτυο τη Δευτέρα 9 Ιουλίου λόγω μόλυνσης με το κακόβουλο λογισμικό DNS Changer, προειδοποιεί ξανά το FBI.

Για πολλούς μήνες, τα μολυσμένα συστήματα χρησιμοποιούνταν από απατεώνες του Διαδικτύου προκειμένου να βομβαρδίζουν τους χρήστες με παράνομες διαφημίσεις, μέχρι που η σπείρα εξαρθρώθηκε τον Νοέμβριο του 2011.

Το πρόβλημα είναι ότι τα μολυσμένα PC επικοινωνούν με διακομιστές που είχαν στήσει οι χάκερ προκειμένου να συνδεθούν σε οποιονδήποτε δικτυακό τόπο. Το FBI έθεσε εκτός λειτουργίας αυτούς τους διακομιστές και τους αντικατέστησε με «καθαρούς» σέρβερ, οι οποίοι επιτρέπουν στα μολυσμένα συστήματα να χρησιμοποιούν το Διαδίκτυο.

- Στις 9 Ιουλίου, το FBI θα θέσει εκτός λειτουργίας αυτό το εφεδρικό σύστημα, οπότε εκατοντάδες χιλιάδες χρήστες κινδυνεύουν να αποκλειστούν από τον Παγκόσμιο Ιστό. «Συνειδητοποιήσαμε ότι υπήρχε πρόβλημα, επειδή [...] αν βγάzaμε από την πρίζα τις υποδομές των εγκληματιών και τους κλείναμε όλους στη φυλακή, τα θύματα της απάτης θα έμεναν χωρίς Διαδίκτυο» αναφέρει ο **Τομ Γκράσο**, ειδικός πράκτορας του FBI. «Ο

μέσος χρήστης θα άνοιγε τον Internet Explorer και θα έβλεπε το μήνυμα "η σελίδα δεν βρέθηκε"» εξηγεί.

- Οι χρήστες υπολογιστών Windows καλούνται τώρα να επισκεφθούν τις σελίδες dcwg.org και dns-ok.us, όπου μπορούν να ελέγξουν αν είναι μολυσμένοι και πώς μπορούν να απαλλαγούν από το DNS Changer.

Πώς στήθηκε η απάτη

Η σπείρα κυβερνοεγκληματιών, της οποίας έξι μέλη συνελήφθησαν τον περασμένο Νοέμβριο στην Εσθονία, κατάφερε αρχικά να μολύνει με το DNS Changer περίπου 580.000 υπολογιστές, από τους οποίους περίπου 200.000 εκτιμάται ότι έχουν πλέον καθαριστεί.

Ο κακόβουλος κώδικας απενεργοποιεί το αντι-ϊικό λογισμικό του υπολογιστή, αφήνοντάς τον εκτεθειμένο και σε άλλες επιθέσεις.

- Το βασικό όμως είναι ότι παρεμβαίνει στον τρόπο με τον οποίο ο υπολογιστής κατανοεί τις διαδικτυακές διευθύνσεις: το DNS (Domain Name System, Σύστημα Ονομάτων Χώρου) είναι ένα διεθνές δίκτυο διακομιστών οι οποίοι αναλαμβάνουν να μετατρέψουν τις διαδικτυακές διευθύνσεις (πχ www.in.gr) στις αριθμητικές διευθύνσεις IP που καταλαβαίνουν οι υπολογιστές (πχ 164.12.653.12).

Οι μολυσμένοι υπολογιστές προγραμματίστηκαν να επικοινωνούν με διακομιστές DNS που είχαν δημιουργήσει οι ίδιοι οι απατεώνες. Με τη μέθοδο αυτή, μπορούσαν να στέλνουν τα θύματα σε πλαστά αντίγραφα οποιουδήποτε δικτυακού τόπου.

Οι χάκερ αντλούσαν έσοδα από την προβολή παράνομων διαφημίσεων στις ψεύτικες ιστοσελίδες. Σύμφωνα με το FBI, τα συνολικά κέρδη της σπείρας έφτασαν τα 14 εκατομμύρια δολάρια.

Η σπείρα τελικά εξαρθρώθηκε στο πλαίσιο διεθνούς επιχείρησης, ωστόσο τα μολυσμένα PC εξακολουθούν να βασίζονται στους στημένους διακομιστές DNS.

Για να προστατεύσει τους χρήστες από το διαδικτυακό μπλακάουτ, το FBI συνεργάστηκε με την εταιρεία Internet Systems Consortium για την εγκατάσταση δύο νέων διακομιστών DNS, μέσω των οποίων εξυπηρετούνται ακόμα και τώρα οι υπολογιστές των θυμάτων.

Ομοσπονδιακό δικαστήριο της Νέας Υόρκης ενέκρινε τη χρήση των διακομιστών αυτών μέχρι τις 9 Ιουλίου, οπότε το εφεδρικό σύστημα θα τεθεί εκτός λειτουργίας.

Λόγω της επικείμενης διακοπής, «βρισκόμαστε σε αγώνα δρόμου για να ενημερώσουμε τον κόσμο ότι πρέπει να αντιμετωπίσει το πρόβλημα» τονίζει ο Τομ Γκράσο του FBI.

Επισημαίνει επίσης ότι το FBI το σύστημα με τέτοιο τρόπο ώστε να μην δοθεί η εντύπωση κυβερνητικής παρέμβασης στη λειτουργία του Διαδικτύου και τους υπολογιστές των θυμάτων.

tovima.gr