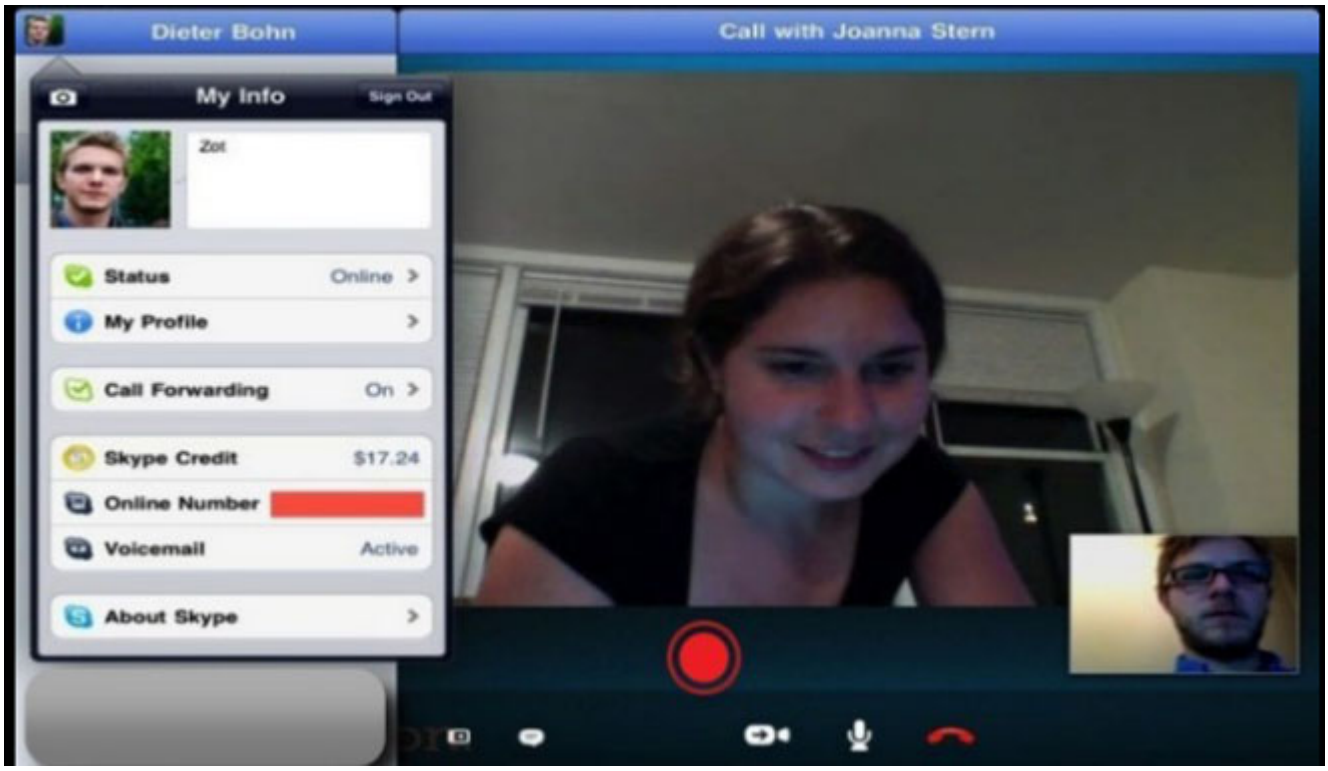
9 Φεβρουαρίου 2016

Backdoor trojan – κίνδυνος υποκλοπής συνομιλιών μέσω Skype!

/ Πεμπτουσία

Image not found or type unknown



Ερευνητές ασφάλειας προειδοποιούν για ένα νέο backdoor trojan που κάνει τον γύρο του διαδικτύου και είναι εξοπλισμένο με προηγμένες λειτουργίες υποκλοπής αρχείων, λήψης screenshots και καταγραφής συνομιλιών μέσω Skype.

Το trojan T9000, είναι μια ιβρυδική έκδοση του κακόβουλου λογισμικού T5000, το οποίο εντοπίστηκε για πρώτη φορά το 2013 και επανεμφανίστηκε το 2014, στοχοποιώντας αυτοκινητοβιομηχανίες, ακτιβιστές ανθρωπίνων δικαιωμάτων και κυβερνητικούς φορείς της περιοχής Ασίας-Ειρηνικού. Η προηγμένη παραλλαγή, η οποία εντοπίστηκε από ερευνητές της Palo Alto Networks, διανέμεται μέσω ειδικά σχεδιασμένων spear phishing emails και στοχεύει κυρίως επιχειρήσεις και οργανισμούς των ΗΠΑ.

Το T9000 είναι αρκετά ευέλικτο και έχει σχεδιαστεί ώστε να μπορεί να

χρησιμοποιηθεί ένανται οποιουδήποτε υποψήφιου στόχου. Το κακόβουλο λογισμικό υποκρύπτεται σε κακόβουλα αρχεία RTF, τα οποία αξιοποιούν γνωστές ευπάθειες (CVE-2012-1856 και CVE-2015-1641) για την παραβίαση των ευάλωτων συστημάτων. Αφού εγκατασταθεί στους ευπαθείς υπολογιστές, το κακόβουλο λογισμικό συλλέγει πληροφορίες σχετικά με το μολυσμένο σύστημα και τις αποστέλλει προς έναν C & C διακομιστή. Με βάση τις πληροφορίες αυτές, ο διακομιστής προωθεί ειδικά modules στον υπολογιστή-στόχο.

Οι ερευνητές της Palo Alto εντόπισαν τρία βασικά modules, τα οποία προκαλούν και τη μεγαλύτερη ζημιά στις πληγείσες συσκευές.

Το **tyeu.dat** αποτελεί το πιο επικίνδυνο module, και είναι υπεύθυνο για την παρακολούθηση των συνομιλιών των χρηστών του Skype. Από τη στιγμή που το module γίνει download και εκτελεστεί, κατά την εκκίνηση του Skype εμφανίζεται ένα μήνυμα στο επάνω μέρος του παραθύρου το οποίο αναφέρει ότι το «explorer.exe θέλει να χρησιμοποιήσει το Skype».

Οι χρήστες που επιτρέπουν στο «explorer.exe» να αλληλεπιδρά με το Skype, επιτρέπουν στην πραγματικότητα στο T9000 να τους κατασκοπεύει.

Το module T9000 μπορεί να καταγράφει γραπτά μηνύματα, συνομιλίες ήχου και βίντεο, ακόμη και να λαμβάνει screenshots κατά τη διάρκεια των βιντεο-κλήσεων.

Το T9000 έχει τη δυνατότητα να υποκλέπτει και άλλου είδους αρχεία, όχι μόνο δεδομένα από τις συνομιλίες του Skype. Μέσω του module **vnkd.dat** οι επιτιθέμενοι μπορούν να υποκλέπτουν δεδομένα από συσκευές αποθήκευσης με επεκτάσεις όπως doc, ppt, xls, docx, pptx, και xlsx.

Τέλος, το πιο αβλαβές module είναι το **qhnj.dat**, το οποίο επιτρέπει στον C & C server να αποστέλλει εντολές στους μολυσμένους υπολογιστές, δημιουργώντας, διαγράφοντας ή μετακινώντας αρχεία, και κρυπτογραφόντας ή αντιγράφοντας δεδομένα.

Πηγή: secnews.gr