Το FBI φέρεται να κρύβεται πίσω από μαζικές επιθέσεις malware

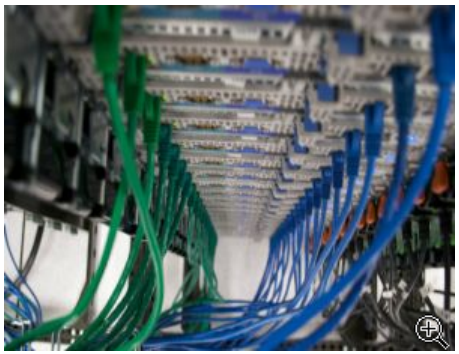
Δημοσιεύτηκε στις Τετάρτη, 09 Οκτωβρίου 2013 19:17 | Γράφτηκε από τον/την Φιλούμενος |

Αξιολόγηση Χρήστη: ○○○○○ / 0
Χειρότερο ○ ○ ○ ○ ◉ Καλύτερο **Αξιολόγηση**

Κατάφερε να ελέγξει servers που έστελναν κακόβουλο λογισμικό σε χρήστες!

Χωρίς να το έχει αμφισβητήσει ποτέ κανείς στα σοβαρά, το FBI αναγνώρισε πριν από λίγες ημέρες ότι πήρε μυστικά τον έλεγχο της Freedom Hosting τον περασμένο Ιούλιο, λίγες μέρες πριν οι servers του μεγαλύτερου παρόχου ανώνυμου hosting βρεθούν να φιλοξενούν κακόβουλο υλικό ειδικά σχεδιασμένο να αναγνωρίζει την ταυτότητα των επισκεπτών.

Ο διαχειριστής της Freedom Hosting, Eric Eoin Marques, είχε νοικιάσει τους servers από ανώνυμη υπηρεσία hosting της Γαλλίας, την οποία πλήρωσε μέσω τραπεζικού λογαριασμού του Λας Βέγκας. Δεν είναι σαφές πώς κατάφερε να FBI να υποκλέψει τους servers, το Γραφείο γνώρισε όμως τη δική του περιπέτεια: ο Marques κατάφερε προσωρινά να ανακτήσει τον έλεγχο των servers, αλλάζοντας τους κωδικούς πρόσβασης και πετώντας έξω τελικά το FBI, πριν το Γραφείο ανακτήσει για δεύτερη φορά την κυριαρχία της υπηρεσίας! Η μάχη πράγματι καλεί κρατεί…



Οι λεπτομέρειες της υπόθεσης διέρρευσαν στον τοπικό Τύπο από την ακροαματική διαδικασία που έλαβε χώρα στο Δουβλίνο της Ιρλανδίας, στην οποία ο 28χρονος Marques παλεύει να μην εκδοθεί στις ΗΠΑ για κατηγορίες που θέλουν τη Freedom Hosting να φιλοξενεί παιδική πορνογραφία σε μεγάλη κλίμακα. Ο ίδιος συνελήφθη τον Ιούλιο και του έχουν αρνηθεί την αποφυλάκιση με εγγύηση για δεύτερη πια φορά.

Η Freedom Hosting ήταν ένας από τους παρόχους ιστοσελίδων «Tor hidden service», ειδικά sites δηλαδή (με διευθύνσεις που τελειώνουν σε .onion) που κρύβουν καλά τη γεωγραφική τους θέση και είναι προσβάσιμα αποκλειστικά από την ανώνυμη κοινότητα Tor. Τα Tor hidden services χρησιμοποιούνται από ιστοσελίδες που επιδιώκουν να αποφύγουν απόπειρες παρακολούθησης και να προστατεύσουν την ανωνυμία του χρήστη σε ασύλληπτο βαθμό. Παρά το γεγονός ότι το δίκτυο Tor φιλοξενεί από sites ανθρώπινων δικαιωμάτων μέχρι και ελεύθερες και ανεξάρτητες φωνές, η εξαιρετική ανωνυμία που προσφέρει επόμενο ήταν να χρησιμοποιηθεί και για εγκληματικές ενέργειες, όπως η διακίνηση παιδικής πορνογραφίας.

Στις 4 Αυγούστου λοιπόν, όλα τα sites που φιλοξενούνται στη Freedom Hosting ξεκίνησαν να μεταδίδουν ένα μήνυμα σφάλματος με κρυμμένο κωδικό ενσωματωμένο στη σελίδα. Η κοινότητα των χρηστών κατάφερε να «σπάσει» τον κώδικα και βρήκε ότι το malware εκμεταλλευόταν ένα κενό ασφαλείας του browser Firefox για να αναγνωρίζει τους χρήστες του Tor Browser Bundle, δίνοντας κατευθείαν αναφορά σε έναν μυστηριώδη server της Βόρειας Βιρτζίνια! Το FBI ήταν ο προφανής ύποπτος, αρνήθηκε ωστόσο να σχολιάσει το γεγονός.

Η ειδική πράκτορας του FBI ωστόσο Brooke Donahue ήταν σαφώς πιο λαλίστατη όταν εμφανίστηκε στο δικαστήριο του Δουβλίνου για να σιγουρευτεί ότι ο Marques θα παραμείνει πίσω από τα κάγκελα, σύμφωνα με το δημοσίευμα που κυκλοφόρησε στην εφημερίδα Irish Independent. Κι ενώ η πράκτορας έκανε λόγο για το πόσο ύποπτος ήταν ο 28χρονος για φυγή, δεν παρέλειψε να κομπάσει για την κυβερνοεπίθεση του FBI στους νοικιασμένους servers του Marques! Ταυτόχρονα βέβαια, έγινε σαφές ότι η Freedom Hosting φιλοξενεί το 95% της παιδικής πορνογραφίας που διακινείται στο δίκτυο Tor: περισσότερες από 100 ιστοσελίδες παιδικής πορνογραφίας δηλαδή, με χιλιάδες χρήστες-μέλη.

Η φαινομενική επίθεση με κακόβουλο υλικό του FBI εντοπίστηκε στις 4 Αυγούστου, όταν όλες οι απόκρυφες υπηρεσίες της Freedom Hosting φιλοξένησαν το συγκεκριμένο malware, ακόμα και νόμιμες ιστοσελίδες, όπως ο πάροχος ηλεκτρονικού ταχυδρομείου TorMail. Οι χρήστες άρχισαν να παρατηρούν τον περίεργο κώδικα και μέχρι το μεσημέρι είχε ήδη σπάσει από τις προσπάθειες της online κοινότητας. Η ίδια η Mozilla επιβεβαίωσε ότι ο κώδικας εκμεταλλευόταν πράγματι μια κρίσιμη ευπάθεια στη διαχείριση της μνήμης του Firefox, που είχε γίνει σαφής ήδη από τις 25 Ιουνίου. Ήταν σαφές ότι το κακόβουλο υλικό έψαχνε να αναγνωρίσει τους ανώνυμους χρήστες του δικτύου Tor.

Η ισχυρότερη ένδειξη ότι η επίθεση προήλθε από κάποια μυστική υπηρεσία ή τη δαγκάνα του νόμου ήταν η περιορισμένη λειτουργικότητα του κακόβουλου υλικού και οι σαφείς διαφοροποιήσεις του από τους «παραδοσιακούς» ιούς: το μόνο που έψαχνε να κάνει είναι να αναγνωρίσει την ταυτότητα του θύματος.

Οι διευθύνσεις που έδινε την αναφορά του το malware εντοπίστηκαν στη Βιρτζίνια (τόπος όπου φιλοξενούνται και οι μυστικοί servers του Γραφείου), με τη συμπεριφορά του κώδικα και το όλο σκηνικό να «μυρίζει» το διαβόητο CIPAV, το spyware του FBI που έγινε γνωστό ήδη από το 2007 και στρεφόταν ευθέως εναντίον χάκερ, εκβιαστών, παιδόφιλων και κάθε ηλεκτρονικού εγκληματία που κρύβεται πίσω από την εκκωφαντική ανωνυμία του δικτύου Tor.

Το FBI λειτουργεί το CIPAV από το 2002, πριν ωστόσο από την επίθεση της Freedom Hosting ο κακόβουλος κώδικας είχε χρησιμοποιηθεί με εξαιρετική φειδώ, γεγονός που τον έσωσε από τη διαρροή και το «σπάσιμο»…

newsbeast