28 Αυγούστου 2016

Εισβολείς μπορούν να συλλέξουν το HTTPS Web traffic ιστορικό σας!

/ Πεμπτουσία

Image not found or type unknown

Ο Alex Chapman και ο Paul Stone από την Context, μια βρετανική συμβουλευτική εταιρεία ασφάλειας στον κυβερνοχώρο, ανακάλυψαν μια νέα μέθοδο επίθεσης χρησιμοποιώντας το πρωτόκολλο WPAD και τα PAC αρχεία για να διαρρεύσουν πληροφορίες σχετικά με τις HTTPS τοποθεσίες που επισκέπτεται ένας χρήστης.

Η ανακάλυψή τους είναι μια ακόμη σταγόνα στον ωκεανό των exploits που χρησιμοποιούν το ευρέως ανασφαλές WPAD πρωτόκολλο.

Εισβολείς μπορούν να συλλέξουν το HTTPS Web traffic ιστορικό σας! HTTPS
Image not found or type unknown

Το WPAD σημαίνει *Web Proxy Auto-Discovery* και είναι ένα πρωτόκολλο που χρησιμοποιείται για τη μετάδοσηproxy configurations σε ένα δίκτυο. Αυτή η λειτουργία “μετάδοσης” που γίνεται με τη χρήση proxy configurations ονομάζεται PAC files ή proxy auto-configs, τα οποία λαμβάνουν τα προγράμματα περιήγησης ή άλλες εφαρμογές που συνδέονται μέσω Internet, πριν σταλούν στον προορισμό τους.

Οι Chapman και Stone λένε ότι ένας εισβολέας που βρίσκεται ήδη σε εκτεθειμένο δίκτυο μπορεί να αντιληφθεί τη διέλευση PAC αρχείων και να εισάγει περιεχόμενο με κακόβουλο κώδικα. Αυτό είναι δυνατόν, όταν οι WPAD διακομιστές χρησιμοποιούν HTTP αντί για HTTPS για τη μετάδοση proxy configuration αρχείων.

Οι ερευνητές εξηγούν ότι μια από τις διαθέσιμες PAC λειτουργίες επιτρέπουν σε έναν εισβολέα να διαρρεύσει την πλήρη URL διεύθυνση ενός HTTPS ιστοτόπου, στον οποίο ενδέχεται να αποκτήσει πρόσβαση. Κανονικά, όταν κάποιος προσπαθεί να παρατηρήσει την HTTPS κυκλοφορία, συνήθως βλέπει μόνο το *https://domain-name.com* κομμάτι του URL.

Η επίθεσή τους, όμως, επιτρέπει σε έναν κακόβουλο εισβολέα να παρατηρήσει την πλήρη διεύθυνση URL, όπως το*https://domain-name.com/page/about/something.html*

.

Η επίθεση δεν είναι τόσο καταστροφική όσο το BadTunnel ή το Hot Potato, αλλά είναι ένας απλός τρόπος για να συλλέξει κανείς το Web traffic ιστορικό από ένα στόχο σπάζοντας την προστασία που παρέχεται από την HTTPS κυκλοφορία.

Το ζήτημα επηρεάζει όλα τα λειτουργικά συστήματα, δεδομένου ότι όλοι υποστηρίζουν WPAD και PAC αρχεία. Οι ερευνητές έχουν ειδοποιήσει όλους τους πωλητές και κάποιοι από αυτούς έχουν κυκλοφορήσει patches για τα προϊόντα τους, που επιδιορθώνουν τον τρόπο με τον οποίο δουλεύουν τα WPAD και PAC αρχεία. Αυτό περιλαμβάνει την Apple για τα iOS και OS X και την Google για τα Android και Chrome.

Για τους Windows χρήστες, οι δύο ερευνητές συνιστούν:

Οι χρήστες να απενεργοποιήσουν την WPAD υποστήριξη αν δεν χρησιμοποιείται στο δίκτυό τους, συνήθως χρειάζεται μόνο σε εταιρικά δίκτυα με ισχυρά firewalls.

Πηγή: www.secnews.gr