ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ

ΤΜΗΜΑ ΕΠΙΣΤΗΜΗΣ ΥΠΟΛΟΓΙΣΤΩΝ

ΠΑΡΟΥΣΙΑΣΗ / ΕΞΕΤΑΣΗ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Τσιραντωνάκης Γεώργιος
Μεταπτυχιακός Φοιτητής

Τμήμα Επιστήμης Υπολογιστών, Πανεπιστήμιο Κρήτης
Επόπτης Μεταπτ. Εργασίας: Καθηγητής, Ευάγγελος Μαρκάτος

Τρίτη, 29/08/2017, 12:00
Αίθουσα B108 ,Τμήμα Επιστήμης Υπολογιστών, Πανεπιστήμιο Κρήτης

" Μια ανάλυση μεγάλης κλίμακας της τροποποίησης περιεχομένου από τους ανοικτούς διακομιστές μεσολάβησης πρωτόκολλου μεταφοράς υπερκειμένου "

ΠΕΡΙΛΗΨΗ

Οι ανοικτοί διακομιστές μεσολάβησης πρωτοκόλλου μεταφοράς υπερκειμένου (HTTP) προσφέρουν μια γρήγορη και βολική λύση για τη δρομολόγηση της διαδικτυακής κίνησης προς έναν προορισμό. Σε αντίθεση με πιο περίπλοκα συστήματα αναμετάδοσης, όπως δίκτυα ανωνυμίας ή υπηρεσίες εικονικών ιδιωτικών δικτύων (VPN), οι χρήστες μπορούν να συνδεθούν ελεύθερα σε ένα ανοικτό μεσολαβητή χωρίς την ανάγκη εγκατάστασης ειδικού λογισμικού. Επομένως, οι ανοιχτοί διακομιστές είναι μια ελκυστική επιλογή για την παράκαμψη φίλτρων με βάση την διεύθυνσης διαδικτυακού πρωτοκόλλου (IP)και Περιορισμούς γεωγραφικής θέσης, παρακάμπτοντας την παρεμπόδιση περιεχομένου και τη λογοκρισία και, γενικότερα, απόκρυψη της διεύθυνσης IP του πελάτη κατά την πρόσβαση σε έναν διακομιστή ιστού. Παρ΄όλα αυτά, οι συνέπειες της δρομολόγησης της κυκλοφορίας μέσω ενός μη αξιόπιστου τρίτου μέσου μπορεί να είναι σοβαρές, ενώ τα κίνητρα λειτουργίας των χιλιάδων διαθέσιμων στο κοινό HTTP διακομιστών είναι αμφισβητήσιμα.

Στην παρούσα εργασία παρουσιάζουμε τα αποτελέσματα μιας ανάλυσης μεγάλης κλίμακας των ανοιχτών διακομιστών HTTP, εστιάζοντας στον καθορισμό του βαθμού

στον οποίο χειραγωγείται η κίνηση του χρήστη ενώ αναμεταδίδονται. Έχουμε σχεδιάσει και εφαρμόσει μια μεθοδολογία που ανιχνεύει διακομιστές που αντί να μεταδίδουν παθητικά την κυκλοφορία, τροποποιούν ενεργά το αναμεταδιδόμενο περιεχόμενο. Πέρα από την απλή ανίχνευση, το πλαίσιο είναι ικανό για την απόδοση ορισμένων μικροσκοπικών αλλαγών κυκλοφορίας σε επίπεδο δικτύου σε σαφώς καθορισμένες κακόβουλες ενέργειες, όπως η τοποθέτηση διαφημίσεων, η αποτύπωση ηλεκτρονικών δακτυλικών αποτυπωμάτων των χρηστών και η ανακατεύθυνση σε σελίδες προορισμού κακόβουλου λογισμικού, για να αναφέρουμε μερικές.

Έχουμε εφαρμόσει τη μεθοδολογία μας σε ένα σύνολο σχεδόν 65,000 ανοιχτών HTTP διακομιστών, τους οποίους παρακολουθούσαμε για περίοδο δύο μηνών. Τα ευρήματά μας είναι ανησυχητικά. Ένα σημαντικό ποσοστό (5.15 %) των διακομιστών που δοκιμάσαμε βρέθηκαν να κάνουν μια αλλαγή περιεχομένου στην ανακτημένη σελίδα HTML, η οποία μπορεί να θεωρηθεί ως κακόβουλη ή ανεπιθύμητη. Συγκεκριμένα, στο 47% των περιπτώσεων η αλλαγή περιεχομένου είχε να κάνει με διαφημίσεις, 39% συγκέντρωσαν πληροφορίες χρηστών που μπορούν να χρησιμοποιηθούν για ηλεκτρονικά δακτυλικά αποτυπώματα και παρακολούθηση και το 12% προσπάθησε να ανακατευθύνει τον χρήστη σε σελίδες που περιείχαν κακόβουλο λογισμικό. Η μελέτη μας αποκαλύπτει τα αληθινά κίνητρα πολλών από των διαθέσιμών στο κοινό διαδικτυακών διακομιστών. Τα ευρήματά μας εγείρουν αρκετές ανησυχίες, καθώς καταδεικνύουμε πολλές περιπτώσεις όπου ο χρήστης μπορεί να επηρεαστεί σοβαρά από τη σύνδεση με ανοικτό διακομιστή. Επιπλέον, έχουμε δημιουργήσει μια λίστα των κακόβουλων διακομιστών που έχουν εντοπιστεί αλλά και εντοπίζονται αυτήν τη στιγμή, οι οποίοι πρέπει να αποφεύγονται και να δημοσιεύονται σε μαύρες λίστες. Τέλος, το πλαίσιο μας μπορεί να σταθεί ως ένας ανοιχτός ελεγκτής για την ανίχνευση πρόσθετων κακόβουλων διακομιστών στο μέλλον.

Tsirantonakis Georgios
M.Sc. Thesis

Computer Science Department
University of Crete
Master's Thesis Supervisor: Professor, E. Markatos

Tuesday, 29/08/2017, 12:00
Room B108, Computer Science Dept., University of Crete

“A Large-scale Analysis of Content Modification by Open HTTP Proxies”

ABSTRACT

Open HTTP proxies offer a fast and convenient solution for routing web traffic towards a destination. In contrast to more elaborate relaying systems, such as anonymity networks or VPN services, users can freely connect to an open HTTP proxy without the need to install any special software. Therefore, open HTTP proxies are an attractive option for bypassing IP-based filters and geo-location restrictions, circumventing content blocking and censorship, and in general, hiding the client's IP address when accessing a web server. Nevertheless, the consequences of routing traffic through an untrusted third party can be severe, while the operating incentives of the thousands of publicly available HTTP proxies are questionable.

In this work, we present the results of a large-scale analysis of open HTTP proxies, focusing on determining the extent to which user traffic is manipulated while being relayed. We have designed and implemented a methodology for detecting proxies that, instead of passively relaying traffic, actively modify the relayed content. Beyond simple detection, the framework is capable of macroscopically attributing certain traffic modifications at the network level to well-defined malicious actions, such as ad injection, user fingerprinting, and redirection to malware landing pages, to name a few. We have applied our methodology on a set of nearly 65,000 open HTTP proxies, which we monitored for a period of two months. Our findings are alarming. A significant fraction (5.15%) of the proxies we tested were found to perform some form of content injection in the retrieved HTML page, which can be considered as malicious or unwanted. Specifically, in 47% of the cases the injected code injected advertisements, 39% collected user information that can be used for fingerprinting and tracking and 12% attempted to redirect the user to pages that contained malware.

Our study reveals the true incentives of many of the publicly available web proxies. Our findings raise several concerns, as we demonstrate multiple cases where the user can be severely affected by connecting to an open proxy. In addition, we have generated a list of currently pinpointed malicious servers that should be strongly avoided and blacklisted. Last but not least, our framework can stand as an open monitor for detecting additional malicious proxies in the future.