Digital forensics

120926 Lindemann, 120912 Rudolfsson?

5. desember 2014

Sammendrag

Abstract

Innhold

1 Introduction

For our project we chose proposal number 2: Experiment or theoretical analysis of cyber crime using VPN, TOR network or proxys for anti-forensics

> Anti-forensics methods are heavily used to avoid that digital investigators to identify user committing cyber-crime, e.g., economic fraud, piracy (sharing/downloading torrents), or child pornagraphy. Digital forensics investigation is challenging when these techniques are used with regards to legal aspects and analysis techniques.

In this project we have looked at what kind of information it is possible to acquire from hosting your own TOR exit node / VPN server.

Most TOR exit nodes are hosted in a different country than your own, and some of these servers might cost a noticable ammount of money to keep up, due to the network traffic going through them. It is therefore interesting for us to know what kind of information the administrator of these servers can see and to what extent they can identify/fingerprint a user.

To summarize: we have looked at what kind of information is visible such as usernames, e-mail adresses, user-agents, websites visited and much more..

2 Survey of related material

When researching the topic of this article, we looked into several known and previously covered issues with the use of TOR and anonymity.

2.1 Tracking users through a unique signature

One particular technology that has recieved quite a bit attentio the last year is ”Canvas fingerprinting”, a technology meant to replace cookies in tracking a unique user across websites. It functions by instructing the browser of the user to draw a figure, using html5, the variations in browser, GPU, drivers and other settings and specifications. It is possible to identify a user to some degree, while the previously mentioned settings are not always unique for every user the technology has some shortcommings. [1]

Somewhat related to this is the standard way of tracking unique users, cookies. It exists many different types of cookies, but the the short summary of it is that its a very common way to track users across one or several websites. It has some shortcommings, due it usually being limited to the current browser/user/system. [2]

2.2 Altering the expected content in communication

Earlier this year it was uncovered that at least one tor exit node based in Russia was pp-atchingbinaries transmitted through it. [3] [4] It appeared that in this particular incident it was mainly used to spread malware with no particular targeted agenda other then the ”usual”malicious behaviour of malware.

3 results

if we do any practical experiments, what did we learn. Its important to keep the key elements of digital forensics in mind:

- evidence integrity
- Chain of custody
- Forensically sound

4 conclusion

yabba-dabba-doo, this is what we found:

- stuff
- more stuff

A apendix; if applicable...

Referanser

[1] Wikipedia. (2014, december) Canvas fingerprinting — wikipedia, the free encyclopedia. Wikipedia. [Online]. Available: http://en.wikipedia.org/w/index.php?title=Canvas_fingerprinting&oldid=633888278 1

[2] ——. (2014, december) Http cookie — wikipedia, the free encyclopedia. [Online]. Available: http://en.wikipedia.org/w/index.php?title=HTTP_cookie&oldid=636454636 1

[3] (2014, November) Onionduke: Apt attacks via the tor network. FSLabs. [Online]. Available: https://www.f-secure.com/weblog/archives/00002764.html 2

[4] J. Pitts. (2014, The Case of the Modified Binaries) The case of the modified binaries. leviathansecurity.com. [Online]. Available: http://www.leviathansecurity.com/blog/the-case-of-the-modified-binaries/ 2