Proposal; Detecting Mining Script on Web Browser

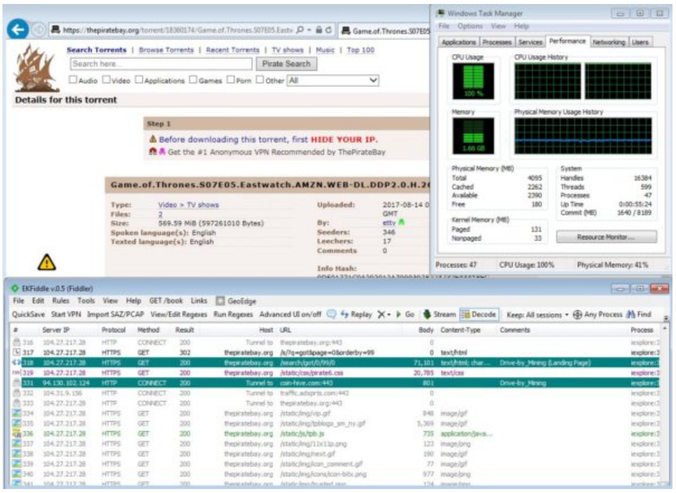
Hyunki Kim, Junghwan Park, Juhyung Song, Seonyong Jeong

Graduate School of Information Security
Korea Advanced Institute of Science and Technology
Yuseong, Daejeon
{ $saykim0727$, $ahnmo$, $sjh8563$, $s.jeong$ } @ $kaist.ac.kr$

I. Introduction

Traditionally, attackers got a profit by selling personal informations through data outflow. Recognized the seriousness of information leakage, people installed security solutions like firewalls. After the personal data outflow, the attacker infected computers by spreading ransomware, which extorts money by ransoming the user's data. However, this has also become difficult due to the introduction of a proprietary solution of Ransomware. Instead of spreading ransomware, the attacker forces to execute open source cryptocurrency minor and get profits from using people's resources without permissions. So, the attacker injects coin-mining-script into vulnerable websites and it becomes more serious.

Site administrator monetizes their website by putting advertisement through Ads agency like Google AdSense. This is a common web ecosystem.However, a excessive advertisement makes visitors unpleasant and reduce a chance of visitors revisiting. So from the end of 2017, site administrator involved a javascript mining code to mine a cryptocurrency on their website instead of advertisement. One of site that include these mining script is The Pirate Bay, Torrent Search Engine. Without user's seeking consent, users easily do not know the behavior. And it becomes more serious.


https://thepiratebay.org/torrent/18360174/Game.of.Thrones.S07E05.Eastv
Game.of.Thrones.S07E05
Search Torrents | Browse Torrents | Recent Torrents | TV shows | Music | Top 100
Search here...
Pirate Search
□Audio □Video □Applications □Games □Porn □Other All
Windows Task Manager
File Options View Help
Applications Processes Services Performance Networking Users
CPU Usage
100 %
CPU Usage History
Memory
1.66 GB
Physical Memory Usage History
Resource Monitor...
EKFiddle v.0.5 (Fiddler)
File Edit Rules Tools View Help GET /book Links GeoEdge
QuickSave Start VPN Import SAZ/PCAP View/Edit Regexes Run Regexes Advanced UI on/off Replay Go Stream Decode Keep: All sessions Any Process Find

Details for this torrent

Step 1

Before downloading this torrent, first HIDE YOUR IP.

Get the #1 Anonymous VPN Recommended by ThePirateBay

Game.of.Thrones.S07E05.Eastwatch.AMZN.WEB-DL.DDP2.0.H.26

Type: Video > TV shows
Files: 2
Size: 569.59 MiB (597261010 Bytes)
Spoken language(s): English
Texted language(s): English

Uploaded: 2017-08-14 0
GMT
By: ettv
Seeders: 346
Leechers: 17
Comments 0

Info Hash:

Physical Memory (MB)	
Total	4095
Cached	2262
Available	2390
Free	180
Kernel Memory (MB)	
Paged	131
Nonpaged	33

System	
Handles	16384
Threads	599
Processes	47
Up Time	0:00:55:24
Commit (MB)	1640 / 8189

Processes: 47 CPU Usage: 100% Physical Memory: 41%

#	Server IP	Protocol	Method	Result	Host	URL	Body	Content-Type	Comments	Process
316	104.27.217.28	HTTP	CONNECT	200	Tunnel to	thepiratebay.org:443	0			iexplore:3
317	104.27.217.28	HTTPS	GET	302	thepiratebay.org	/s/?q=got&page=0&orderby=99	0	text/html		iexplore:3
318	104.27.217.28	HTTPS	GET	200	thepiratebay.org	/search/got/0/99/0	71,101	text/html; char...	Drive-by_Mining (Landing Page)	iexplore:3
319	104.27.217.28	HTTPS	GET	200	thepiratebay.org	/static/css/pirate6.css	20,785	text/css		iexplore:3
331	94.130.102.124	HTTP	CONNECT	200	Tunnel to	coin-hive.com:443	801		Drive-by_Mining	iexplore:3
332	104.31.9.156	HTTP	CONNECT	200	Tunnel to	traffic.adxprts.com:443	0			iexplore:3
333	104.27.217.28	HTTP	CONNECT	200	Tunnel to	thepiratebay.org:443	0			iexplore:3
334	104.27.217.28	HTTPS	GET	200	thepiratebay.org	/static/img/vip.gif	848	image/gif		iexplore:3
335	104.27.217.28	HTTPS	GET	200	thepiratebay.org	/static/img/tpblogo_sm_ny.gif	5,369	image/gif		iexplore:3
336	104.27.217.28	HTTPS	GET	200	thepiratebay.org	/static/js/tpb.js	735	application/java...		iexplore:3
337	104.27.217.28	HTTPS	GET	200	thepiratebay.org	/static/img/11x11p.png	123	image/png		iexplore:3
338	104.27.217.28	HTTPS	GET	200	thepiratebay.org	/static/img/next.gif	190	image/gif		iexplore:3
339	104.27.217.28	HTTPS	GET	200	thepiratebay.org	/static/img/icon_comment.gif	77	image/gif		iexplore:3
340	104.27.217.28	HTTPS	GET	200	thepiratebay.org	/static/img/icons/icon-bitx.png	977	image/png		iexplore:3

Fig. 1. The Pirate Bay Case[1]

II. Motivation

As a cryptocurrency comes in, a lot of people started a cryptocurrency mining in their computers using mining program. Moreover, in recent years, cryptojacking has become popular ways that an attacker make a malicious mining program and send the program to victims to mine a cryptocurrency in others computer on the quiet like ¡Fig 2¿. Among them, a famous cryptojacking way is to use web-based javascript code on web server. A javascript mining code based on web browser is extremely dangerous because malicious code works on the user's computer even if the user only accesses the web site[2]. Currently, the malicious javascript mining code is included on personal sites, blogs, and even normal advertising banners in web site. To detect and To defend the malicious javascript mining code on our computer, a lot of plugin and solution is developed and is released. but still some solution and plugin have several problem. So, we will develop a plugin to detect a malicious javascript mining code based web browser and to defend user's computer from malicious code and will give users a warning.

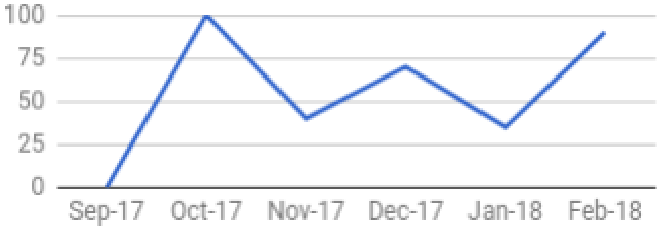


Fig. 2. Month by month percentage change in browser based mining activity[3]

III. Previous works

Chrome extension that detect javascript mining code already existed. However, these have several limitations and problems.

A. Domain-based Black List

'Miner Detector'[4], developed by Alino, blocks 4 well-known Javascript coin miner hostings, such as *Coinhive*. *'NoCoin'*[5], implemented by Keraf, blocks specific domains using blacklist which is updated by users. However, attackers can bypass the extension by using self-hosted coin mining script, instead of using well-known Javascript miner hosting.

B. DOM Element Monitoring

'MinerBlock'[6], developed by xd4rker, blocks specific domains by using domain-based black list as we mentioned before. In addition, it blocks mining scripts by checking DOM Elements name. The script based on CoinHive has *isRunning*, *stop*, *_siteKey* methods. And the script based on Mineralt miner has *db*, *getIf*, *stop*, *hps* methods. This way looks efficient, but it can make false positives. Also, the attacker can bypass this extension by element name substitution.

IV. Scope

A. What is in the scope of this project?

In this project, we will implement Chrome add-on plugin detecting malicious mining script on web browser. Recently, as malicious mining script detecting tools are introduced, Cryptojacking script becomes obfuscated[7] and disguised as a well-known javascript library[8] to deceive user. With this project, we will implement an add-on program detecting lurking scripts with following methods.

1) Normal cryptojacking Script
2) Obfuscated cryptojacking Script
3) Cryptojacking Script disguised as a well-known Javascript library

We will detect cryptojacking by pattern-based scanning and monitoring side channel properties.

B. What is **not** in the scope of this project?

We will only focus on coin mining scripts based on web-browser. We do not consider about the local execution miner as a binary form.

V. Procedure

We will implement the extension by following this procedure:

1) Investigate browser-based cryptocurrency mining paper.
2) Analyze browser-based cryptocurrency mining script: *Coinhive*, *Crypto-Loot*.
3) Learn Chrome Extension Development.
4) Design and make the Chrome Extention.
5) Test our model whether it prevents Cryptojacking.
6) Put together our data and write the mid-paper.
7) Run the model with new strategies.
8) Write final paper and prepare presentation.

VI. Resource

A. Reading materials

1) Jiawei Zhu Pe, Mining Information on Bitcoin Network Data, IEEE CPSCom, 2017[9].: In this report, we will study the Mining network data of Bitcoin or One major virtual currency on Network Data. They resolve the block chain data to analyze Bitcoin from the point of Bitcoin of IP address. Through this report, we will learn how to capture the network data on Block chain and utilize it to our project with current trends.

2) Cryptojacking detecting chrome extension: We talk about some of the new challenges with blocking the cryptojacking (E.g Miner Block) It is an efficient browser extension that focuses on blocking browser-based cryptocurrency miners all over the web. The extension uses two different approaches to block miners. The first one is based on blocking requests/scripts loaded from a blacklist, this is the traditional approach adopted by most ad-blockers and other mining blockersHowever, most of the cryptojacking ad-on is designed to track untrusted URL.We will re-design the ad-on to check a specific function acting miner-blocker and comparing with CPU resource, power consumption by side channel.

3) Google Chrome extension Developer's guide: Contains the way that make the basic ad-on using javascript, HTML,json code. We tend to study this site's some examples along guide line and research one to complete our project.

VII. Distributed

A. Hyunki Kim

: Wrote Motivation, References

B. Junghwan Park

: Wrote Introduction, Previous work, Procedure

C. Juhyung Song

: Wrote Resource, Procedure

D. Seonyong Jeong

: Wrote Introduction, Scope

Acknowledgment

This work is proposed for *Introduction to Information Security(IS 521)* , 2018 Spring Semester, at *Korea Advanced Institute of Science and Technology*.

References

[1] https://blog.malwarebytes.com/security-world/2017/10/why-is-malwarebytes-blocking-coinhive/, Malwarebytes Labs
[2] http://www.boannews.com/media/view.asp?idx=58181, 보안뉴스
[3] https://www.symantec.com/blogs/threat-intelligence/coin-mining-without-browser
[4] https://github.com/Alino/MinerDetector
[5] https://github.com/keraf/NoCoin
[6] https://github.com/xd4rker/MinerBlock
[7] http://www.thewindowsclub.com/cryptojacking-browser-mining-threat, The Windows Club
[8] https://blog.avast.com/wordpress-and-joomla-users-get-hacked-be-aware-of-fake-jquery
[9] Jiawei Zhu Pe, Mining Information on Bitcoin Network Data, IEEE CPSCom 2017