SoK: Cryptojacking Malware

Ege Tekiner[1] Abbas Acar[1] Engin Kirda[2],
Ali Aydin Selcuk[3], A. Selcuk Uluagac[1]

[1]Florida International University, USA
[2] Northeastern University, USA
[3]TOBB University of Economics and Technology, Turkey

6th IEEE European Symposium on Security and Privacy
September 6-10, 2021

Outline

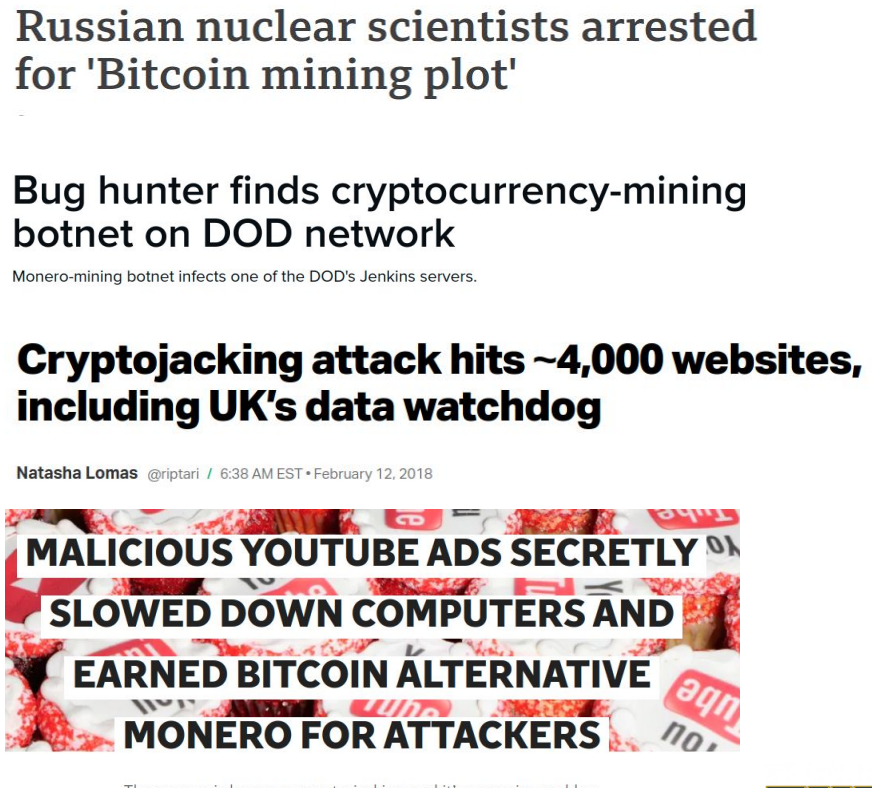
- Introduction
- SoK Methodology
- Cryptojacking Malware Types
- Cryptojacking Malware Techniques
- Literature Review
- Lessons Learned and Future Research Directions
- Conclusion

Introduction

- Since Bitcoin was launched in 2009, blockchain and cryptocurrencies have attracted ever-increasing interest from both legitimate users and attackers.

- Cryptojacking is the act of using the victim's computational power without consent to mine cryptocurrency.

- It has been found on:
  - Critical infrastructures such as US DOD [1], UK Governmental Services [2], and Russian Nuclear Science Labs [3],
  - Well-known streaming platforms like YouTube [4],
  - Mikrotik Routers and Nintendo game consoles [5-6].



SoK Methodology

We cover multiple resources to systemize knowledge.

- **Papers:** After the price surge of cryptocurrencies and distribution of ready-to-use mining scripts, cryptojacking malware become popular among researchers. We covered 43 cryptojacking-related papers.
  - 28 detection papers
  - 15 analysis papers

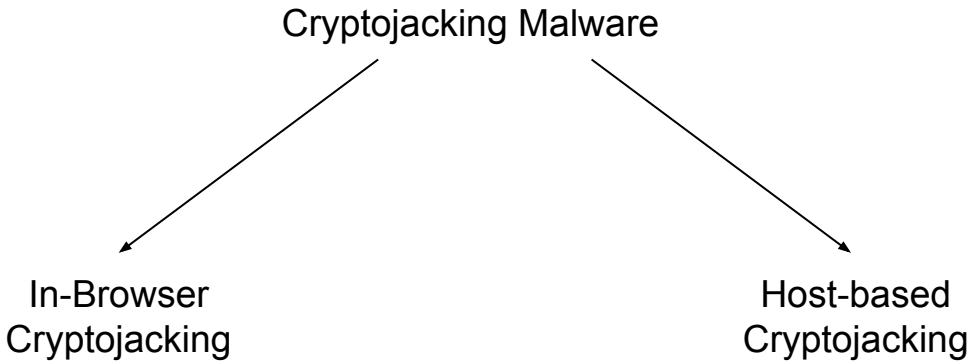
- **Samples:** For a comprehensive understanding of the cryptojacking malware, we also benefited from the real cryptojacking malware samples. We used 2 main sources to collect cryptojacking malware samples in the wild;

  - VirusTotal [7] (20200 cryptojacking samples)
  - PublicWWW [8] (6269 in-browser cryptojacking samples)
  - Both of our sample dataset are publicly available in the following link below. https://github.com/sokcryptojacking/SoK

- **Major Attack Instances:** We also use security reports released by the security companies such as Kaspersky, Trend Micro, IBM, and others.
  a. 5 annual security reports from well-known security companies such as IBM [9], Trend Micro [10], Palo-Alto Networks [11], and Cado-Security [12].

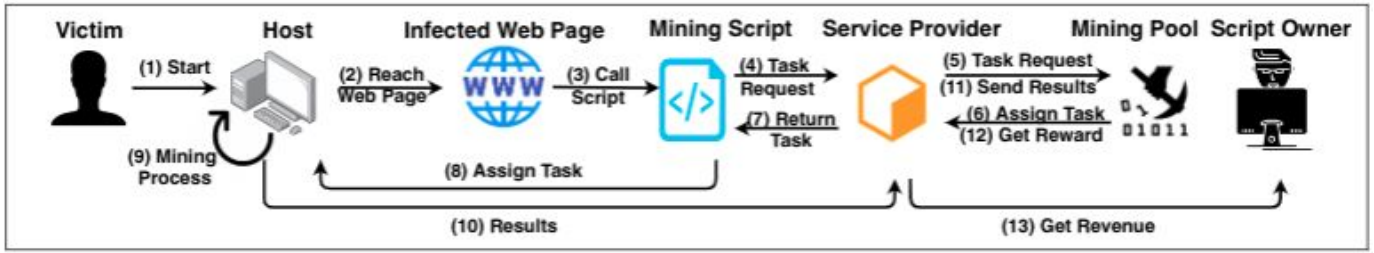
Cryptojacking Malware Types

In the literature, we identify two main types of cryptojacking malware using by the attackers.



In-browser Cryptojacking

- In-browser cryptojacking takes advantage of interactive web content technologies
- It connects to victims' host devices to access the computational resources of the victim (e.g., CPU).
- It performs mining as long as the victim keeps the webpage open.

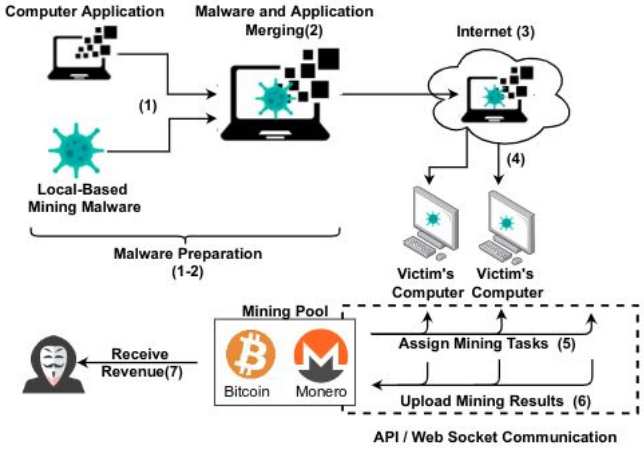


The lifecycle of a in-browser cryptojacking malware

Host-based Cryptojacking

- Host-based cryptojacking is a silent malware that attackers employ to access the victim host's resources.

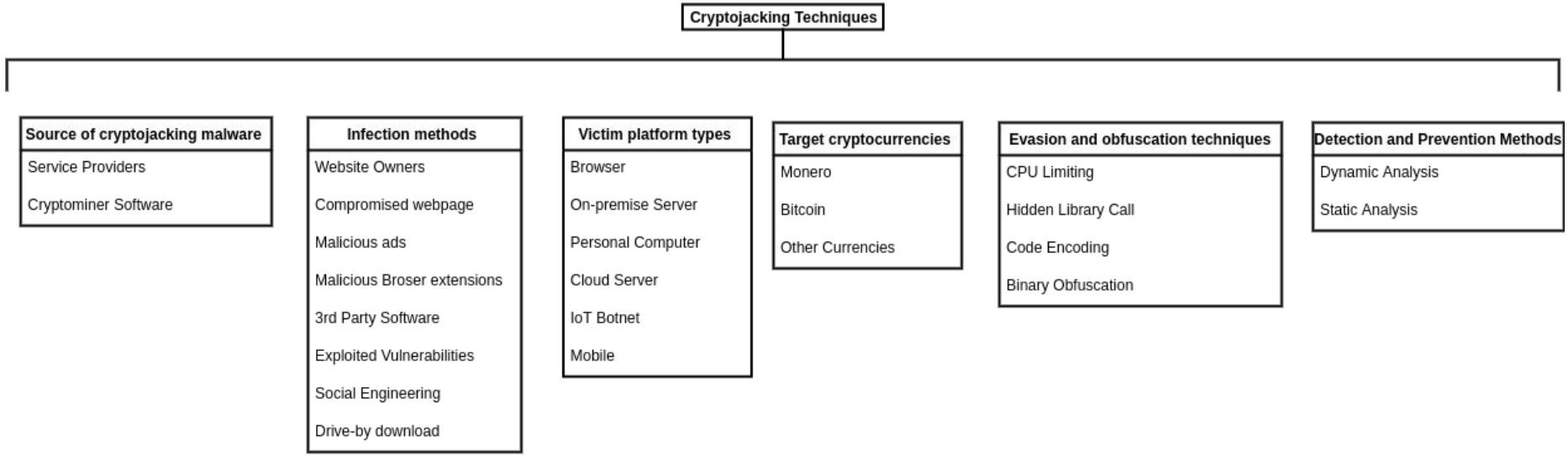
- It turns victims' host devices into a miner for the malware owner.



The lifecycle of a host-based cryptojacking malware

Cryptojacking Malware Techniques

In our research, we found several techniques used by attackers to hide and develop the model of cryptojacking malware. Particularly, we articulate as follows:



Source of Cryptojacking Malware

- Cryptojacking malware can be created and distributed by different parties and sources. In our research, we identified 2 main sources of cryptojacking malware.

- Service Providers
  - Coinhive[13], Authedmine [13], Browsermine [14], Coinhave [15], Coinimp [16], Coin nebula [17], Cryptoloot [18], DeepMiner [19], JSECoin [20], Monerise [21], Nerohut [22], Webmine [23], WebminerPool [24], and Webminepool [25].

- Regular Cryptomining Software
  - XMRig [26]

Coinimp

Webminepool

BTCminer

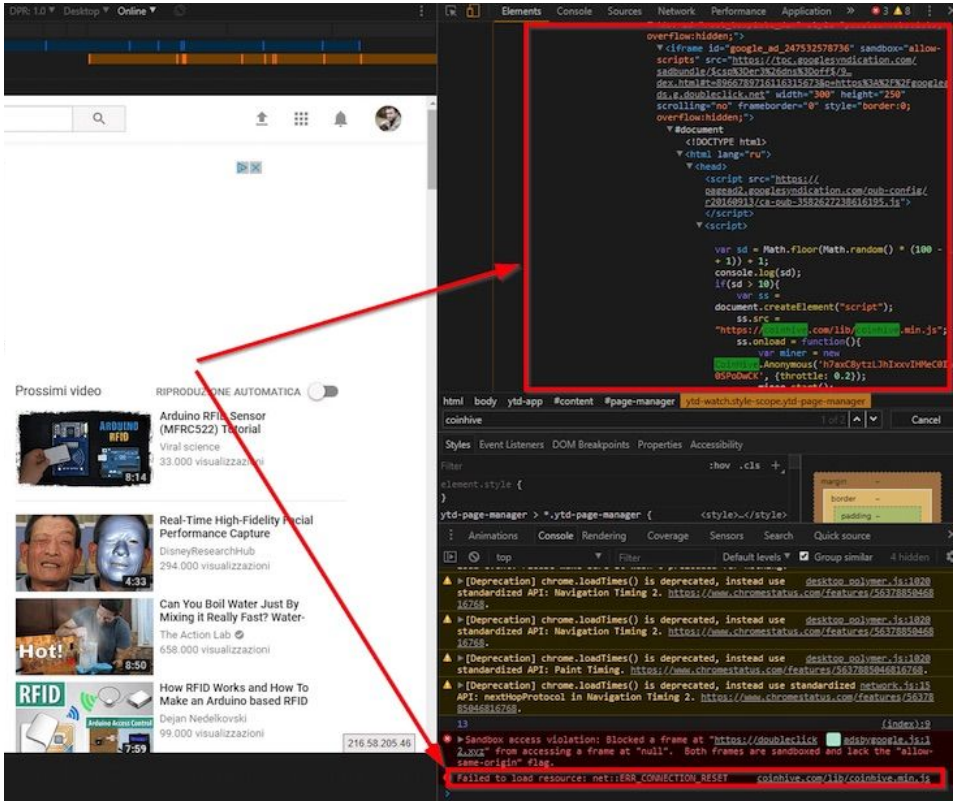
ANTmining pool

Coinhive

Infection Methods

Attackers use several techniques to inject and hide their malware inside systems and code blocks.

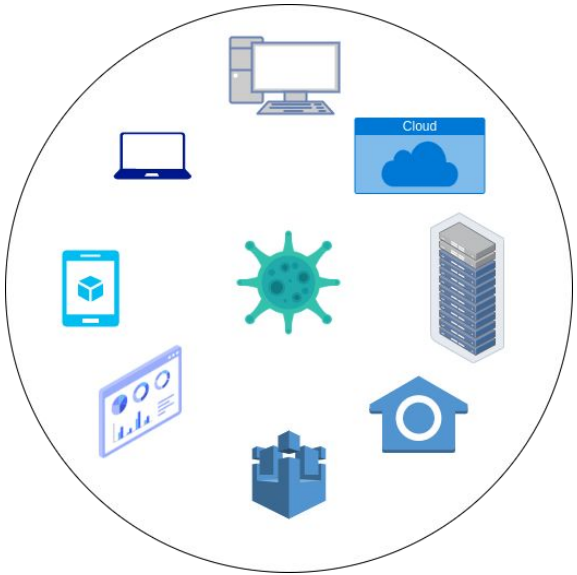
- Website owners
- Compromised websites
- Malicious ads
- Malicious browser extensions
- Third-party software
- Exploited vulnerabilities
- Social engineering attacks
- Drive-by download



Victim Platform Types

Attackers differentiate their target device domain for several reasons. Platform types can be categorized under;

- Browser
- Personal computers
- On-premise server
- Cloud server
- IoT botnet
- Mobile devices



Target Currencies

We analyzed the samples'
- cryptomining scripts
- service providers' documentation.

With this analysis, we saw that 91% of the samples in the PublicWWW [8] dataset use Monero to mine.

We also found that 7111 of 20200 samples taken from VirusTotal [7] are marked with a label containing the keyword "bitcoin".

Evasion and Obfuscation Techniques

The purpose of the cryptojacking malware is to exploit the resources of the victim as long as possible; therefore, staying on the system without being detected is of paramount importance.

- CPU Limiting
- Hidden Library Calls
- Code Encoding
- Binary Obfuscation

```
1 <script>
2       var miner=new CoinHive.Anonymous('Key', {
3           Threads:4, autoThreads:false, throttle:0.8);
4       if (!miner.isMobile()) &&!miner.didOptOut(14400)
5           { miner.start(); } }
6 </script>
```

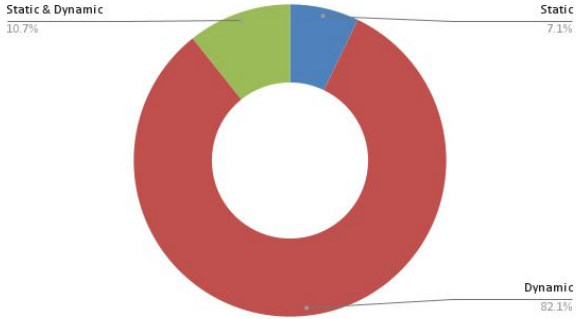
Detection and Prevention Methods

In the traditional malware detection literature, there are two main analysis methods:

- Static Analysis: Static analysis tools generally seek specific keywords, malware signatures, and hash values. In the cryptojacking domain, *2 proposed detection mechanisms* used only static analysis.

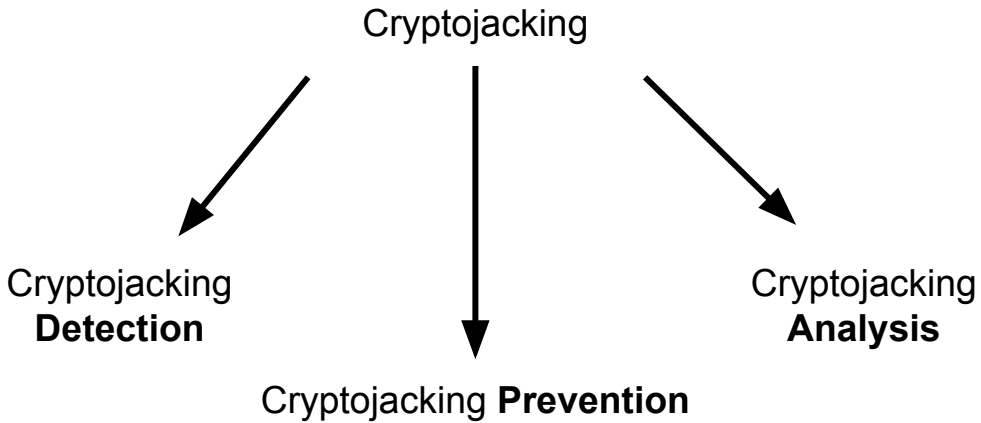
- Dynamic Analysis: In dynamic analysis, the malware sample is executed in a controlled environment, and the analysts observe the behavioral features of those malware samples. In the cryptojacking domain, *23 proposed detection mechanisms* used only static analysis.

Finally, *3 of the proposed detection mechanisms* used both static and dynamic analysis methods to detect the cryptojacking malware.



Literature Review

After the surge of the cryptojacking malware, drew the attention of academia and many publications published in a very small time frame. The papers mainly focusing on three topics;



Cryptojacking Detection Studies

We found and covered *28 cryptojacking detection studies* in the literature. We classify these studies in terms of their,

- Dataset: While 23 of the proposed detection mechanism uses dynamic analysis, we can measure the effectiveness of the proposed detection method with their dataset. However, only 3 of the proposed detection mechanism provide their dataset.

- Type (In-browser or Host-based): 82% of the proposed mechanism dedicated to detect in-browser cryptojacking malware. There are only few studies proposed a solution for host-based cryptojacking malware.

- Method (Static or Dynamic analysis): Except 2 proposed detection methods, all of the proposed detection methods are using dynamic analysis due to repetitive and predefined steps of the mining process.

Ref	Dataset	Type	Method	Features	Classifier	Performance

Cryptojacking Detection Studies

- Features: many detection mechanisms have been proposed using dynamics features. The most commonly used dynamic features in these studies are as follows:
  - CPU events
  - Memory activities
  - Network package
  - JS compilation and execution time
  - Hardware Performance Counters (HPC)
  - System Calls

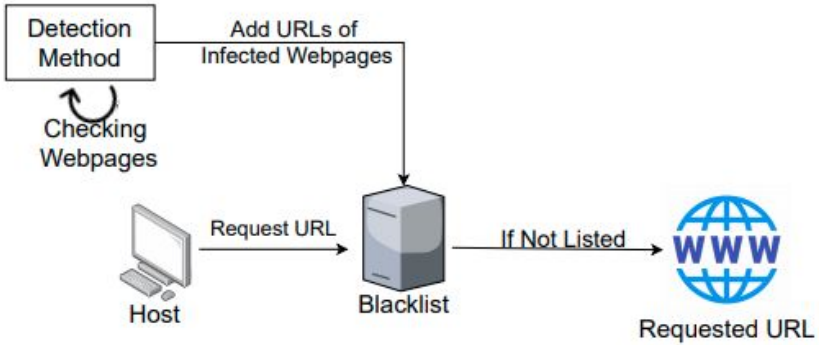
- Classifiers and Performance: The collected features used to train different ML classifiers such as;
  - Support Vector Machine
  - Random Forest
  - Neural Network
  - Decision Tree

Cryptojacking Prevention Studies

Three of the studies in the literature both focusing to detect and prevent or interrupt the cryptojacking malware. These studies prevent the mining malware with the following methods,

- Raise a notification for the user
- Sleep the mining process
- Kill the related process

Blacklists are also a handful way to prevent cryptojacking malware as long as their admin keep them updated.



Cryptojacking Analysis Studies

Finally, there are 15 analysis studies focusing on analysis of the cryptojacking studies. These studies performed empirical measurement studies to understand the cryptojacking threat landscape better. The authors of these studies focused on,

- Characterize the scope of cryptojacking malware
- Operations
- Revenue

Cryptojacking Dataset	Sample Type	Focus of the Study
2000 executable	binary	the practice of using compromised PCs to mine Bitcoin
33282 websites	script	prevalence analysis
-	-	how cybercriminals are exploiting cryptomining
5190 websites	script	campaign and domain analysis
XMR-stak, cpuminer-multi	binary	attack impact on consumer devices and user annoyance
5700 websites	script	static, dynamics and economic analysis
CoinHive cryptominer	script	sample characteristics and network traffic analysis
1.2 million miners	binary	currencies, actors , campaign and earning analysis, underground markets
107511 websites	script	profitability and the imposed overheads
3.2 TB historical scan results	script	investigation of a new type of attack that exploits Internet infrastructure for cryptomining
-	-	business model, threat sources, implications, mitigations, legality and ethics
53 websites	script	sample characteristics
2770 websites	script	activeness analysis
XMRig miner	binary	sample characteristics
156 domains, 25892 proxies	script	impact on the web users

Lessons Learned and Research Directions

- Attackers now target the devices with more processing power rather than the personal computers as in the in-browser cryptojacking attacks.

- In almost all of the attack instances we have seen during our research, the attackers use Monero as a target cryptocurrency instead of Bitcoin or other cryptocurrencies.

- We identified three issues regarding to the evaluation of the proposed solutions in the literature:
  - Dataset dates are not reported,
  - Not clear if it is online or offline detection,
  - Overhead analysis is not given.

- There is a need for more effort by researchers to work on the usage of legitimate cryptomining with user consent and knowledge as a funding model.

Conclusion

- In this paper we presented the cryptojacking malware types, their lifecycle and working logic in a systematic fashion.

- We also presented the techniques used by cryptojacking malware based on the previous research papers, cryptojacking samples, and major attack instances.

- We examined if cryptojacking is an essential tool for hackers to raise pseudonym or fully anonymized revenue.

- Even though there are a lot of important studies achieved to detect cryptojacking malware, the applicability and overhead analysis of these detection systems are not clear.

- This SoK study will facilitate not only a deep understanding of the emerging cryptojacking malware and the pertinent detection and prevention mechanisms but also a substantial additional research work needed to provide adequate mitigations in the community.

Acknowledgements

We would like to thank the US National Science Foundation and the Cyber Florida Capacity Building Program for supporting our work under the awards:

NSF-CAREER-CNS-1453647, NSF-1663051, NSF-CNS-1718116, NSF-CNS-1703454

Questions?

Ege Tekiner
Email: eteki001@fiu.edu
LinkedIn:
https://www.linkedin.com/in/ege-tekiner-72854b111/

For more information, please see:

- Our lab website: https://csl.fiu.edu/
- Dataset: https://github.com/sokcryptojacking/SoK
- Our other papers:
  - F. Naseem, A. Aris, L. Babun, E. Tekiner, and S. Uluagac, “MINOS: A lightweight real-time cryptojacking detection system,” in 28th Annual Network and Distributed System Security Symposium, NDSS, February 21-25, 2021, 2021.
  - H. Oz, A. Aris, A. Levi, and A. S. Uluagac, “A survey on ransomware: Evolution, taxonomy, and defense solutions,” arXiv preprint arXiv:2102.06249, 2021.

FIU

References

[1] - C. Cimpanu, “Miner found at USA department of defense,” https: //www.zdnet.com/article/bug-hunter-finds-cryptocurrency-mini ng-botnet-on-dod-network/, accessed: 2020-04-13.
[2] - K. Parrish, “Uk government plugin based mining,” https://www. digitaltrends.com/computing/government-websites-plugin-coinh ive-monero-miner/, accessed: 2020-04-13.
[3] - A. Milano, “Russian scientists arrested crypto mining nuclear lab,” https://www.coindesk.com/russian- scientists-arrested-crypto-mining-nuclear-lab, accessed: 2021-2-23.
[4] - D. Goodin, “Miners in youtube ads,” https://arstechnica.com/in formation-technology/2018/01/now-even-youtube-serves-ads-wit h-cpu-draining-cryptocurrency-miners/, accessed: 2020-04-13.
[5] -C. Cimpanu, “Mikrotik router hack affect 200k routers in the world,” https://www.bleepingcomputer.com/news/security/massi ve-coinhive-cryptojacking-campaign-touches-over-200-000-mi krotik-routers/, accessed: 2021-2-23.
[6] - T. Smith, “Miner found at nintendo switch console,” https://bitc oinist.com/nintendo-switch-game-pulled-over-cryptojacking-co ncerns/, accessed: 2020-04-13.
[7] - “Virus total payload scanning and ranking platform,” https://ww w.virustotal.com/, accessed: 2020-02-26.
[8] - “Source code search engine,” https://publicwww.com/, accessed: 2020-10-16.
[9] - IBM-Security, “X-force threat intelligence index 2020,” https: //securityintelligence.com/series/ibm-x-force-threat-intelligenceindex-2020, accessed: 2021-02-16.
[10] - J. M. Augusto Remillano II, “Coinminer, ddos bot attack docker daemon ports,” https://www.trendmicro.com/vinfo/hk-en/securit y/news/virtualization-and-cloud/coinminer-ddos-bot-attack-dock er-daemon-ports, accessed: 2021-2-14.
[11] - Unit42, “Watchdog: Exposing a cryptojacking campaign that’s operated for two years,” https://unit42.paloaltonetworks.com/wa tchdog-cryptojacking/, accessed: 2021-02-23.
[12] - Cado-Security, “Aws cloud-based cryptojacking report,” https:// www.cadosecurity.com/post/team-tnt-the-first-crypto-mining-w orm-to-steal-aws-credentials, accessed: 2020-02-16.
[13] - “The official webpage of both coinhive and authedmine,” http: //web.archive.org/web/20190130232758/https://coinhive.com/doc umentation, accessed: 2020-10-19.
[14] - “The official webpage of browsermine,” https://browsermine.co m/faq, accessed: 2020-10-19.
[15] - “The official webpage of coinhave,” http://web.archive.org/web/ 20180102115842/https://coin-have.com/, accessed: 2020-10-19.
[16] - “The official webpage of coinimp,” https://www.coinimp.com/do cumentation, accessed: 2020-10-19.
[17] - “Coinnebula official webpage,” https://web.archive.org/web/2018 0818144049/https://coinnebula.com/, accessed: 2020-10-19.
[18] - “Cryptoloot,” https://crypto-loot.org/, accessed: 2020-06-20
[19] - “The official github page of deep miner,” https://github.com/dee pwn/deepMiner, accessed: 2020-10-19.
[20] - “Jsecoin,” https://jsecoin.com/, accessed: 2020-10-19.
[21] - “The official webpage of monerise,” http://web.archive.org/web/ 20200813110918/http://monerise.com/, accessed: 2020-10-19.
[22] - “The official webpage of nerohut,” https://web.archive.org/web/20 190131001253/https://nerohut.com/documentation.php, accessed: 2020-10-19.
[23] - “Webmine official webpage,” webmine.cz/, accessed: 2020-10-19.
[24] - “The official webpage of webminerpool,” https://github.com/not given688/webminerpool, accessed: 2020-10-19.
[25] - “The official webpage of webmine pool,” https://www.webminep ool.com/page/documentation, accessed: 2020-10-19.
[26] - “Xmrrig,” https://github.com/xmrig/xmrig, accessed: 2021-2-23
[27] - G. Hong, Z. Yang, S. Yang, L. Zhang, Y. Nan, Z. Zhang, M. Yang,Y. Zhang, Z. Qian, and H. Duan, “How you get shot in the back:A systematical study about cryptojacking in the real world,” inProceedings of the 2018 ACM SIGSAC Conference on Computerand Communications Security (CCS), 2018, pp. 1701–1713.
[28] - R. K. Konoth, E. Vineti, V. Moonsamy, M. Lindorfer, C. Kruegel,H. Bos, and G. Vigna, “Minesweeper: An in-depth look into drive-by cryptocurrency mining and its defense,” inProceedings of the2018 ACM SIGSAC Conference on Computer and Communica-tions Security (CCS), 2018, pp. 1714–1730
[29] - A. Kharraz, Z. Ma, P. Murley, C. Lever, J. Mason, A. Miller,N. Borisov, M. Antonakakis, and M. Bailey, “Outguard: Detectingin-browser covert cryptocurrency mining in the wild,” inTheWorld Wide Web Conference (WWW), 2019, pp. 840–852
[29] - Minerblock: An efficient browser extension to block browser-based cryptocurrency miners all over the web.” https://github.com/xd4rker/MinerBlock/blob/master/assets/filters.txt, accessed:2020-04-08
[30] - W. Wang, B. Ferrell, X. Xu, K. W. Hamlen, and S. Hao, “Seismic:Secure in-lined script monitors for interrupting cryptojacks,” inEuropean Symposium on Research in Computer Security (ES-ORICS). Springer, 2018, pp. 122–142
[31] - R. Holz, D. Perino, M. Varvello, J. Amann, A. Continella,N. Evans, I. Leontiadis, C. Natoli, and Q. Scheitle, “A retrospec-tive analysis of user exposure to (illicit) cryptocurrency miningon the web,”arXiv:2004.13239, 2020.