EN

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

From January 2019 to April 2020

Crypto-jacking

ENISA Threat Landscape

Overview

Cryptojacking (also known as cryptomining) is the unauthorized use of a device's resources to mine cryptocurrencies. Targets include any connected device, such as computers and mobile phones; however, cybercriminals have been increasingly targeting cloud infrastructures.[1] This type of attack has not attracted much attention from law enforcement agencies and its abuse is rarely reported[2], mainly because of its relatively few negative consequences. Nevertheless, organisations may notice higher IT costs, degraded computer components, increased electricity consumption and reduced employee productivity caused by slower workstations.[3]

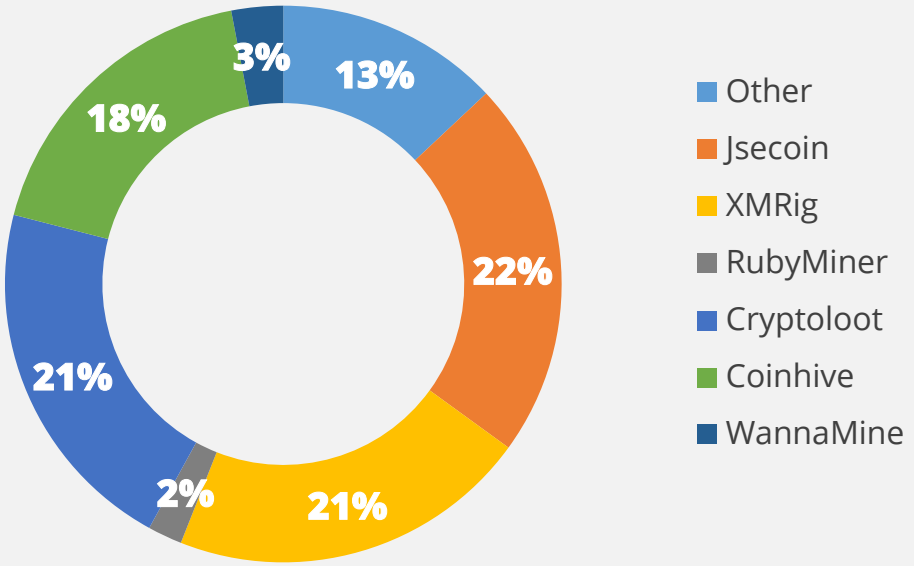


Figure 1: Top cryptomining malware globally . Source: Check Point[9]

Findings

64,1_ million cryptojacking hits by the end of 2019

78%_ decrease in cryptojacking activities in the second half of 2019 compared with the first half

Activities grew by 9% in the first half of 2019 compared with the previous 6 months of 2018.[4,5]

65%_ of the 120 most popular exchanges in Q3 2019 had weak or porous know your costumer (KYC) processes

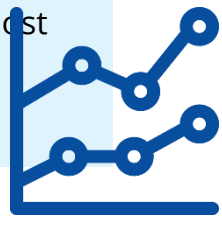
32% of the exchanges traded privacy coins.[6]

39,3%_ of 2019 crypto mining infections targeted Japan.

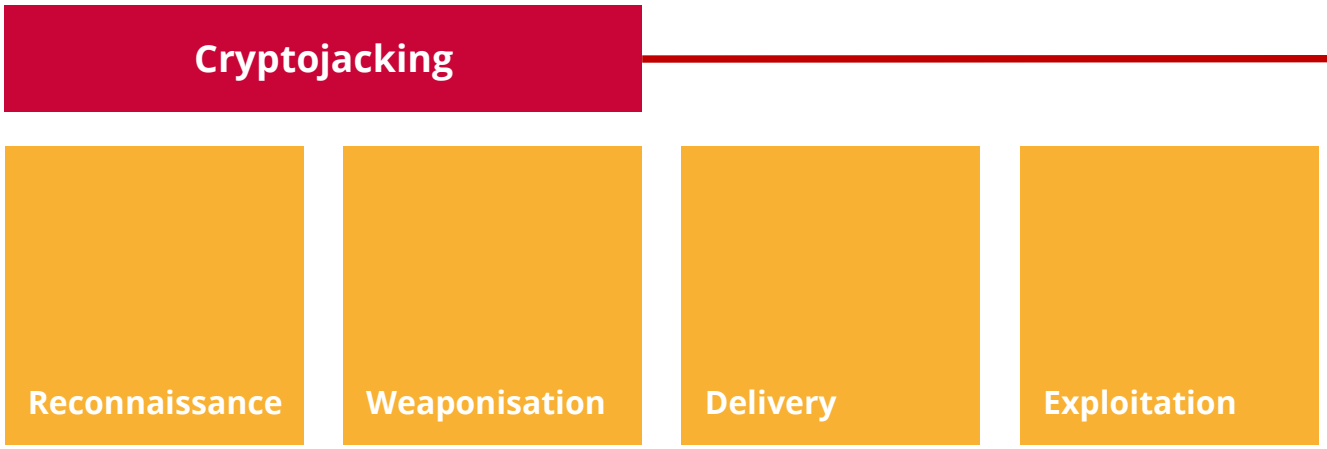
20,8% of the crypto mining infections targeted India and 14,2% Taiwan, Figure 1 depicts the five countries with the most detected cryptocurrency miner malware infection attempts for 2018 and 2019.[7]

13%_ is attributed to trojan.Win32.Miner.bbb

During the period November 2018 to October 2019, the next most active miners were Trojan.Win32.Miner.ays (11,35%), Trojan.JS.Miner.m (11,12%).[6]



Kill chain



Step of Attack Workflow

Width of Purpose

Cryptojacking

Installation	Command & Control	Actions on Objectives

The Cyber Kill Chain® framework was developed by Lockheed Martin, adapted from a military concept related with the structure of an attack. To study a particular attack vector, use this kill-chain diagram to map each step of the process and reference the tools, techniques and procedures used by the attacker.

MORE INFORMATION

Trends

Popular cryptomining service Coinhive closed down

Coinhive started in September 2017 and advertised itself as an alternative revenue stream for web developers instead of banner advertisements.[24] It used JavaScript libraries, which could be installed on websites, and the visitor's processing power to legitimately mine cryptocurrency. Until its closure, in March 2019, it had been highly abused by threat actors who injected code into hacked websites to mine the Monero cryptocurrency and divert funds to their own pockets. After its closure, the volume of web-based cryptojacking hits dropped by 78% during the second half of 2019.[4] As a result of this decrease, cybercriminals begun focusing on higher value targets, such as powerful servers[9] and cloud infrastructures.[1] Coinhive's place at the top has since been taken[9] by Jsecoin (22%), XMRig (21%) and Cryptoloot (21%). The distribution of top cryptomining malware globally is presented in Figure 1.

More attacks on cloud infrastructures

An increasing trend was visible in the first half of 2019, regarding incidents of cryptocurrency-mining attacks on the cloud.[15,25] Cloud environments usually employ mechanisms that tailor resources on-demand and are therefore lucrative targets for running mining software. However, this comes at the expense of website owners, who in turn need to pay higher bills for exceeding quotas.[15] In the first half of 2019, vulnerabilities in cloud container software increased by 46% compared with the same period in 2018.[26] Attackers have been successful in exploiting application programming interfaces (APIs) and container management platforms in order to install malicious images (e.g. Docker and Kubernetes) and mine cryptocurrencies.[25]

Incidents

April 2019_ **Cryptojacking campaign dubbed Beapy, exploited the EternalBlue vulnerability and affected enterprises in China**[3]

May 2019_ **Monero-mining malware PCASTLE mostly targeted China-based systems, by employing fileless arrival techniques**[19]

Over 50.000 servers belonging to companies in the healthcare, telecommunications, media and IT sectors were found to be infected by malware mining the TurtleCoin (TRTL) cryptocurrency.[20] A new malware family named BlackSquid, utilized eight known exploits including EternalBlue and DoublePulsar and subsequently spread to web servers across Thailand and the United States so as to deliver Monero mining scripts.[17,21]

August 2019_ **Cryptojacking malware found in 11 RubyGem language repositories, exposing thousands of users to cryptomining code**[22]

Trends

Shift towards file-based cryptomining

In 2019, a decline in browser-based cryptojacking in favour of file-based cryptomining was noticed. File-based cryptomining[27] attacks spread through malware and made use of pre-existing exploits on unpatched operating systems such as EternalBlue and other high-risk vulnerabilities. Factors contributing to this shift were the closure of the popular web-based mining provider Coinhive[1] and the decline in cryptocurrency values.[10] Another factor is that file-based cryptomining has always been more efficient than web-based mining, being 25 times more profitable.[3] Threat actors adapted their malware with additional tools, to extract sensitive information from the victim's computer.

Worldwide cryptojacking attacks are decreasing

In 2019, a downwards trend[5], in cryptojacking attacks was noticed, mainly due to the closure of Coinhive[6], the coordinated efforts of law enforcement agencies, and the depreciation of the Monero cryptocurrency . However, as cryptojacking attacks have been known to follow cryptocurrency values, a service similar to Coinhive may emerge, and fuel a new spike. Early statistics for 2020, show a 30% increase year-on-year in March.

_Monero remained the cryptocurrency of choice

Similar to previous trends, Monero (XMR) was the cryptocurrency of choice for 2019 cryptojacking activities. The reason is two-fold; first, Monero is focused on privacy and anonymity and, therefore, the transactions cannot be traced. Second, the Proof-of-Work algorithm is designed to make mining viable with a standard CPU as opposed to specialized hardware. In Q3 2019, 32% of exchanges traded privacy coins such as Monero. However, in anticipation of new anti-money laundering regulations, many exchanges opted to delist privacy coins.

_Most targeted countries

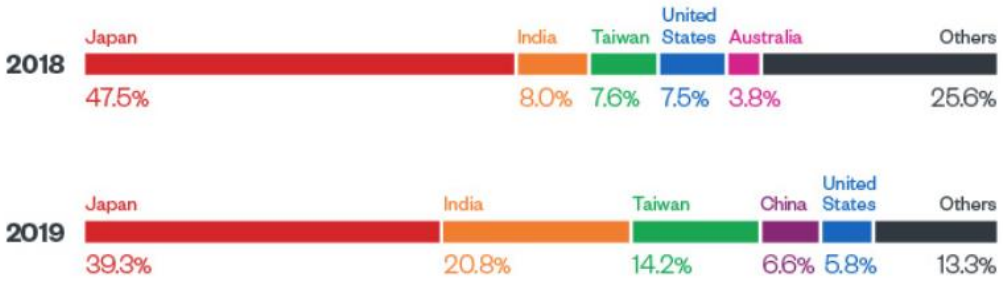


Figure 2: Most target countries by cryptojacking. Source: Trend Micro[7]

Attack Vectors

_Techniques

Cyber criminals used the following techniques to run or deliver cryptominers:

- by incorporating cryptojacking capabilities in existing malware;[10]
- by compromising websites;[11]
- by persistent drive-by attacks;[12]
- using social networks;[13]
- using mobile apps and app stores;[14]
- using exploit kits;[15]
- using advertising networks and malvertising;[16]
- using removable media;[17]
- and using wormable cryptominers.[18]

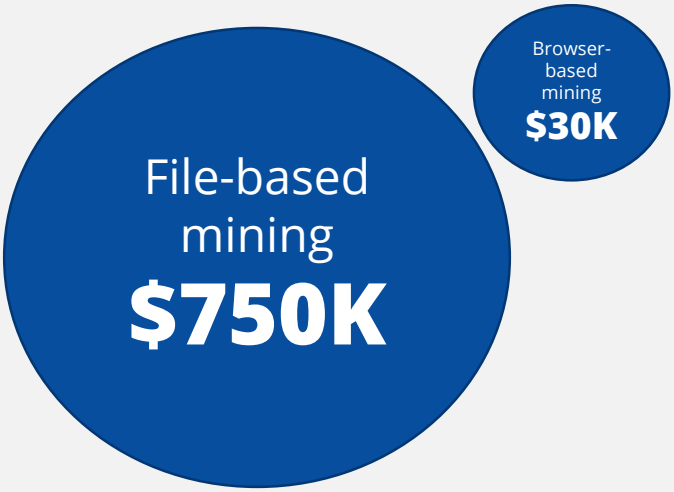


Figure 3: How much can a coin-mining botnet make in 30 days? Source: Broadcom[3]

Proposed actions

- Monitor battery usage on users' devices and, in the case of suspicious spikes in CPU usage, scan for the presence of file-based miners.
- Implement content filtering to filter out unwanted attachments, e-mails with malicious content and spam.
- Implement filtering of the stratum mining protocol as well as blacklisting the IP addresses and domains of popular mining pools.
- Install end-point protection by means of anti-virus programs or cryptominer blocking browser plug-ins.
- Conduct regular security audits to detect network anomalies.
- Implement robust vulnerability and patch management.
- Use whitelisting to prevent unknown executables from being executed at the endpoints.
- Invest in raising users' awareness of crytojacking, especially with regard to secure browsing behaviour.
- Implement patches and fixes against well-known exploits, such as Eternal Blue, on less obvious targets, such as queue management systems, POS terminals, and even vending machines.
- Monitor and blacklist common cryptomining executables.

References

1. Sergiu Gatlan. "Cryptominers Still Top Threat In March Despite Coinhive Demise." April 9, 2019. Bleeping Computer. https://www.bleepingcomputer.com/news/security/cryptominers-still-top-threat-in-march-despite-coinhive-demise/

2. "Internet Organised Crime Threat Assessment (IOCTA)." 2019. EUROPOL. https://www.europol.europa.eu/iocta-report

3. "Beapy: Cryptojacking Worm Hits Enterprises in China." 24 April, 2019. BROADCOM. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/beapy-cryptojacking-worm-china

4. Bill Conner. "SONICWALL Cyber Threat Report." 2020. SONICWALL https://www.sonicwall.com/resources/2020-cyber-threat-report-pdf/

5. Yessi Bello Perez. "Unsuspecting victims were cryptojacked 52.7 million times in the first half of 2019." July 24, 2019. TheNextWeb – HARD FORK. https://thenextweb.com/hardfork/2019/07/24/cryptojacking-cryptocurrency-million-hits-first-half-2019/

6. Ben Noble. "A Third of Cryptocurrency Exchanges Still Host Privacy Coins Despite Fears of Impending FATF Travel Rule." November 27, 2019. CIPHERTRACE https://ciphertrace.com/ciphertrace-q3-2019-caml-press-release/

7. "Defending Systems Against Cryptocurrency Miner Malware." October 28, 2019. Trend Micro. https://www.trendmicro.com/vinfo/be/security/news/cybercrime-and-digital-threats/defending-systems-against-cryptocurrency-miner-malware

8. "Kaspersky Security Bulletin '19 Statistics." 2009. Kaspersky. https://go.kaspersky.com/rs/802-IJN-240/images/KSB_2019_Statistics_EN.pdf

9. "CYBER SECURITY REPORT." 2020. Check Point Research cp<r>. https://www.checkpoint.com/downloads/resources/cyber-security-report-2020.pdf

10. Ionut Ilascu. "EternalBlue Exploit Serves Beapy Cryptojacking Campaign." April 25, 2019. Bleeping Computer. https://www.bleepingcomputer.com/news/security/eternalblue-exploit-serves-beapy-cryptojacking-campaign/

11. "New mining worm PsMiner uses multiple high-risk vulnerabilities to spread." March 12, 2019. 360 Total Security. https://blog.360totalsecurity.com/en/new-mining-worm-psminer-uses-multiple-high-risk-vulnerabilities-to-spread/

12. Dan Thorp-Lancaster. "New drive-by cryptocurrency mining scheme persists after you exit your browser window." November 9, 2017. Windows Central. https://www.windowscentral.com/new-drive-cryptocurrency-mining-scheme-persists-even-after-you-exit-your-browser-window

13. Dr. Michaeal McGuire. "Social Media Platforms and the Cybercrime Economy." 2019. Bromium. https://www.bromium.com/wp-content/uploads/2019/02/Bromium-Web-of-Profit-Social-Platforms-Report.pdf

14. Axelle Apvrille. "Abusing cryptocurrencies on Android smartphones." 2019. Fortinet. https://fortinetweb.s3.amazonaws.com/fortiguard/research/currency-insomnihack19.pdf

15. "2019 Midyear Security Roundup Evasive Treats Pervasive Effects." 2019. TrendMicro https://documents.trendmicro.com/assets/rpt/rpt-evasive-threats-pervasive-effects.pdf

16. Margi Murphy. "YouTube shuts down hidden cryptojacking adverts." January 29, 2018. The Telegraph https://www.telegraph.co.uk/technology/2018/01/29/youtube-shuts-hidden-crypto-jacking-adverts/

17. Matthew Beedham. "New cryptocurrency mining malware is spreading across Thailand and the US." June 4, 2019. TheNextWeb – HARD FORK. https://thenextweb.com/hardfork/2019/06/04/security-crypto-jacking-mining-malware/

18. Sean Lyngaas. "BlueKeep is back. For now, attackers are just using it for cryptomining." November 4, 2019. CyberScoop. https://www.cyberscoop.com/bluekeep-exploited-cryptomining/

19. Janus Agcaoili. "Monero-Mining Malware PCASTLE Zeroes Back In on China, Now Uses Multilayered Fileless Arrival Techniques." June 5, 2019. Trend Micro. https://blog.trendmicro.com/trendlabs-security-intelligence/monero-mining-malware-pcastle-zeroes-back-in-on-china-now-uses-multilayered-fileless-arrival-techniques/

20. Marie Huillet. "Researchers Say 50,000 Servers Worldwide Infected With Privacy Coin Cryptojacking Malware." May 29, 2019. Cointelegraph. https://cointelegraph.com/news/researchers-say-50-000-servers-worldwide-infected-with-privacy-coin-cryptojacking-malware

21. Johnlery Triunfante, Mark Vicente. "BlackSquid Slithers Into Servers and Drives With 8 Notorious Exploits to Drop XMRig Miner." August 27, 2019. Trend Micro. https://blog.trendmicro.com/trendlabs-security-intelligence/blacksquid-slithers-into-servers-and-drives-with-8-notorious-exploits-to-drop-xmrig-miner/

22. "Malicious cryptojacking code found in 11 Ruby libraries." August 2, 2019, Decrypt. https://decrypt.co/8602/malicious-cryptjacking-code-found-in-11-ruby-libraries

23. Brook Chelmo. "Cryptojacking in 2019: Cryptocurrency Value Keeping Attack Vector in Play ." August 6, 2019. SonicWall. https://blog.sonicwall.com/en-us/2019/08/cryptojacking-in-2019-cryptocurrency-value-keeping-attack-vector-in-play/

24. Catalin Cimpanu. "Coinhive cryptojacking service to shut down in March 2019". February 27, 2019. ZD Net. https://www.zdnet.com/article/coinhive-cryptojacking-service-to-shut-down-in-march-2019/

25. Tom Hegel. "Making it Rain - Cryptocurrency Mining Attacks in the Cloud". March 14, 2019. AT&T Business. https://cybersecurity.att.com/blogs/labs-research/making-it-rain-cryptocurrency-mining-attacks-in-the-cloud/

26. "How a Prominent Cryptomining Botnet is Paving the Way for a Lucrative and Illicit Revenue Model". August 2019. Carbon Black. https://cdn.www.carbonblack.com/wp-content/uploads/2019/08/Carbon-Black-Access-Mining.pdf

27. "Cryptojacking Attacks: Who's Mining on Your Coin?". April 5, 2019. Security Intelligence. https://securityintelligence.com/cryptojacking-attacks-whos-mining-on-your-coin/

28. "Malware Creates Cryptominer Botnet Using EternalBlue and Mimikatz'. April 12, 2019. Bleeping Computer. https://www.bleepingcomputer.com/news/security/malware-creates-cryptominer-botnet-using-eternalblue-and-mimikatz/

Related

READ THE REPORT

ENISA Threat Landscape Report
The year in review

A summary on the cybersecurity trends for the period between January 2019 and April 2020.

READ THE REPORT

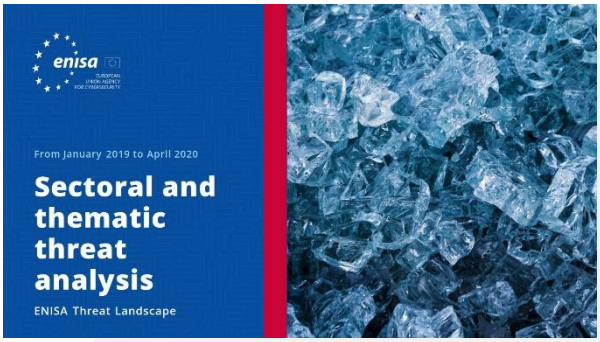
ENISA Threat Landscape Report
List of Top 15 Threats

ENISAs' list of the top 15 threats of the period between January 2019 and April 2020.

READ THE REPORT

ENISA Threat Landscape Report
Research topics

Recommendations on research topics from various quadrants in cybersecurity and cyber threat intelligence.



READ THE REPORT

ENISA Threat Landscape Report **Sectoral and thematic threat analysis**

Contextualised threat analysis between January 2019 and April 2020.

READ THE REPORT

ENISA Threat Landscape Report **Emerging trends**

Main trends in Cybersecurity observed between January 2019 and April 2020.

READ THE REPORT

ENISA Threat Landscape Report **Cyber Threat Intelligence Overview**

The current state of play of cyber threat intelligence in the EU.

About

_ The agency

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contributors

Christos Douligeris, Omid Raghimi, Marco Barros Lourenço (ENISA), Louis Marinos (ENISA) and *all members of the ENISA CTI Stakeholders Group:* Andreas Sfakianakis, Christian Doerr, Jart Armin, Marco Riccardi, Mees Wim, Neil Thaker, Pasquale Stirparo, Paul Samwel, Pierluigi Paganini, Shin Adachi, Stavros Lingris (CERT EU) and Thomas Hemker.

Editors

Marco Barros Lourenço (ENISA) and Louis Marinos (ENISA).

Contact

For queries on this paper, please use enisa.threat.information@enisa.europa.eu.

For media enquiries about this paper, please use press@enisa.europa.eu.

Legal notice

Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

© European Union Agency for Cybersecurity (ENISA), 2020
Reproduction is authorised provided the source is acknowledged.

Copyright for the image on the cover: © Wedia. For any use or reproduction of photos or other material that is not under the ENISA copyright, permission must be sought directly from the copyright holders.

ISBN: 978-92-9204-354-4
DOI: 10.2824/552242

Vasilissis Sofias Str 1, Maroussi 151 24, Attiki, Greece
Tel: +30 28 14 40 9711
info@enisa.europa.eu
www.enisa.europa.eu

All rights reserved. Copyright ENISA 2020.

https://www.enisa.europa.eu