Cryptojacking

By Noah Cunningham

Introduction

- Cryptojacking is a cybercrime in which another party's computing resources are hijacked to mine cryptocurrency. [1]
- Whether you've been cryptojacked locally on your system, or through the browser, it can be difficult to manually detect the intrusion after the fact. [2]
- Cryptojacking was the third most prevalent cybersecurity threat in 2021, according to the European Union Agency for Cybersecurity's (ENISA) annual report. In the same year, Google's Cybersecurity Action Team found that 86% of its observed compromised cloud platforms resulted from cryptojacking. In 2020, Cisco reported 69% of its customers were affected by cryptomining malware. [1]

[1] Barney, Nick. "What Is Cryptojacking? Detection and Preventions Techniques." *WhatIs.com*, TechTarget, 19 Sept. 2022, https://www.techtarget.com/whatis/definition/cryptojacking#:~:text=Cryptojacking%20is%20a%20cybercrime%20in,hardware%20and%20other%20mining%20resources.

[2] "Cryptojacking – What Is It, and How Does It Work?" Malwarebytes, https://www.malwarebytes.com/cryptojacking.

Background

- Cryptocurrency: A cryptocurrency is a digital currency, which is an alternative form of payment created using encryption algorithms.[1]
- Crypto Mining: Mining is the process that Bitcoin and several other cryptocurrencies use to generate new coins and verify new transactions [2]
- Phishing: Phishing is when criminals use fake emails, social media posts or direct messages with the goal of luring you to click on a bad link or download a malicious attachment. [3]
- Malware: Malware, or “malicious software,” is an umbrella term that describes any malicious program or code that is harmful to systems. [4]

[1] “The Basics about Cryptocurrency.” The Basics about Cryptocurrency | CTS, https://www.oswego.edu/cts/basics-about-cryptocurrency#:~:text=A%20cryptocurrency%20is%20a%20digital,you%20need%20a%20cryptocurrency%20wallet.

[2] “Crypto Basics - What Is Mining?” Coinbase, Coinbase, https://www.coinbase.com/learn/crypto-basics/what-is-mining.

[3] National Cybersecurity Alliance. “Phishing.” National Cybersecurity Alliance, 5 Oct. 2022, https://staysafeonline.org/resources/phishing/#:~:text=Phishing%20is%20when%20criminals%20use,personal%20information%20to%20the%20cybercriminals.

[4] “What Is Malware? Definition and How to Tell If You're Infected.” Malwarebytes, https://www.malwarebytes.com/malware.

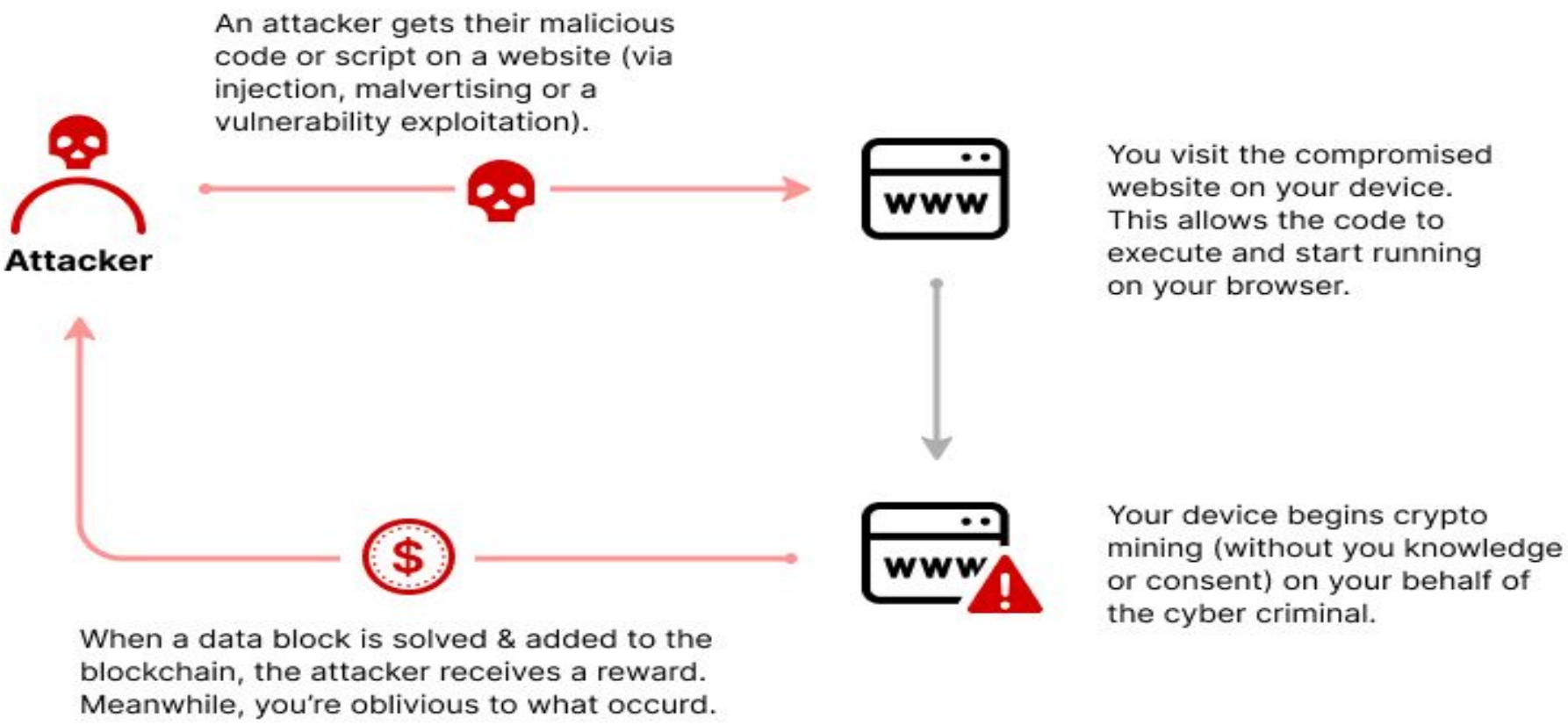
Systems Methodology

Step 1: A miner prepares a crypto mining script to infect a website or device[1]

Step 2: A website is infected or a victim's device is compromised when they click on a link and unknowingly download crypto mining software.[1]

Step 3: The crypto mining script is executed and begins using the victim's computing resources to run crypto mining software. The cybercriminal controls how much power is directed from the victim's device to the illicit mining operation.[1]

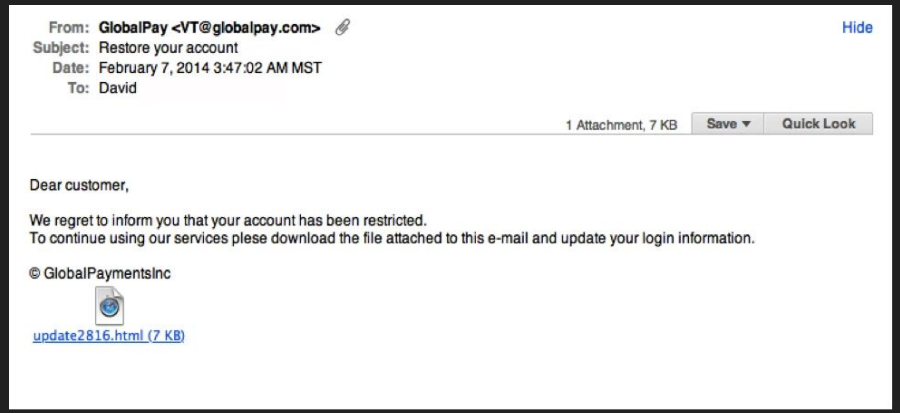
[1] Barney, Nick. “What Is Cryptojacking? Detection and Preventions Techniques.” *WhatIs.com*, TechTarget, 19 Sept. 2022, https://www.techtarget.com/whatis/definition/cryptojacking#:~:text=Cryptojacking%20is%20a%20cybercrime%20in,hardware%20and%20other%20mining%20resources.


An attacker gets their malicious code or script on a website (via injection, malvertising or a vulnerability exploitation).
Attacker
www
You visit the compromised website on your device. This allows the code to execute and start running on your browser.
www
Your device begins crypto mining (without you knowledge or consent) on your behalf of the cyber criminal.
$
When a data block is solved & added to the blockchain, the attacker receives a reward. Meanwhile, you're oblivious to what occurd.

Systems Methodology

Host Based / Classic Malware Phising

- Tricking the Victim to download Malware onto their device



Web Based / Drive-By Crypto Mining

- Embedding a piece of JavaScript code into a web page. After that, it performs cryptocurrency mining on user machines that visit the page [1]
- Existing websites can be compromised through programmatic advertising, which contains malware that automatically places ads on sites [2]

[1] “Cryptojacking – What Is It, and How Does It Work?” Malwarebytes, https://www.malwarebytes.com/cryptojacking.

[2] Barney, Nick. “What Is Cryptojacking? Detection and Preventions Techniques.” *WhatIs.com*, TechTarget, 19 Sept. 2022, https://www.techtarget.com/whatis/definition/cryptojacking#:~:text=Cryptojacking%20is%20a%20cybercrime%20in,hardware%20and%20other%20mining%20resources.

Systems Methodology

Severity

- Low Severity as there is no risk to one’s safety, identity and financial security as no one's personal information is being exposed

Protecting Against It

- Use browser extensions that are designed to block coin mining [1] (example: https://github.com/xd4rker/MinerBlock)
- Use more privacy-focused ad blockers [1] (example: https://ublockorigin.com/)
- One obvious option is to block JavaScript in the browser that you use to surf the web. [2]
- Secure servers and cloud configurations [3]

[1] “Cryptojacking.” INTERPOL, https://www.interpol.int/en/Crimes/Cybercrime/Cryptojacking.

[2] “Cryptojacking – What Is It, and How Does It Work?” Malwarebytes, https://www.malwarebytes.com/cryptojacking.

[3] Barney, Nick. “What Is Cryptojacking? Detection and Preventions Techniques.” *WhatIs.com*, TechTarget, 19 Sept. 2022, https://www.techtarget.com/whatis/definition/cryptojacking#:~:text=Cryptojacking%20is%20a%20cybercrime%20in,hardware%20and%20other%20mining%20resources.

Conclusion

- Cryptojacking may be out of the headlines, but it’s unlikely to disappear anytime soon. Where vulnerabilities exist, threat actors will continue to take advantage of the effortless monetization of access to victim endpoints or servers. [1]
- Cryptojacking is really an ingenious attack, as it’s hard to detect, and there's ‘less risk’ for the attacker because it’s not that harmful to the user besides their computer running a bit slower.
- Statistics are being collected regularly on the prevalence of crytpoajcking
- People are developing prevention and detection methods

[1] “The End of Cryptojacking?” Aon, https://www.aon.com/cyber-solutions/thinking/blog-the-end-of-cryptojacking/#:~:text=The%20Future%20Risk%3A,to%20victim%20endpoints%20or%20servers.

References

- Barney, Nick. “What Is Cryptojacking? Detection and Preventions Techniques.” *WhatIs.com*, TechTarget, 19 Sept. 2022, https://www.techtarget.com/whatis/definition/cryptojacking#:~:text=Cryptojacking%20is%20a%20cybercrime%20in,hardware%20and%20other%20mining%20resources.
- “Cryptojacking – What Is It, and How Does It Work?” Malwarebytes, https://www.malwarebytes.com/cryptojacking.
- “The Basics about Cryptocurrency.” The Basics about Cryptocurrency | CTS, https://www.oswego.edu/cts/basics-about-cryptocurrency#:~:text=A%20cryptocurrency%20is%20a%20digital,you%20need%20a%20cryptocurrency%20wallet.
- “Crypto Basics - What Is Mining?” Coinbase, Coinbase, https://www.coinbase.com/learn/crypto-basics/what-is-mining.
- National Cybersecurity Alliance. “Phishing.” National Cybersecurity Alliance, 5 Oct. 2022, https://staysafeonline.org/resources/phishing/#:~:text=Phishing%20is%20when%20criminals%20use,personal%20information%20to%20the%20cybercriminals.
- “What Is Malware? Definition and How to Tell If You're Infected.” Malwarebytes, https://www.malwarebytes.com/malware.
- “Cryptojacking.” INTERPOL, https://www.interpol.int/en/Crimes/Cybercrime/Cryptojacking.
- “The End of Cryptojacking?” Aon, https://www.aon.com/cyber-solutions/thinking/blog-the-end-of-cryptojacking/#:~:text=The%20Future%20Risk%3A,to%20victim%20endpoints%20or%20servers.
- Krishna, Ananda. “Removing Cryptojacking Coinhive Malware from Your WordPress, Magento, Drupal & Prestashop Websites.” Astra Security Blog, 19 Mar. 2018, https://www.getastra.com/blog/911/remove-crypto-mining-malware-cms-wordpress-magento-drupal/#:~:text=CoinHive%20is%20an%20online%20service,placing%20advertising%20on%20the%20website.