Cryptojacking: How Hackers Are Mining Cryptocurrencies Without Your Knowledge

William Zhang

October 17, 2018

Abstract

Cryptojacking, which rocketed in popularity in the fall of 2017 has an ostensibly worthy goal of using an untapped resource to generate an alternative revenue stream. Attackers do this by either sending a malicious link through email that loads crypto mining code on the computer after being clicked on or embedding a website or online ad with JavaScript code that can leverage a visiting device's processing power to mine a cryptocurrency. The crypto mining code works in the background all while the unsuspecting victim continues their everyday activities on their machine. Every visitor or victim might only do a very small bit of mining while they are there, but each user lending some processing power over time can generate real money. In theory, it can be a win-win. In practice, not so much. This article will discuss why cryptojacking is becoming more prevalent and some methods of cryptojacking. The article will also explore the ways in which cryptojacking attacks can be prevented, detected and responded to.

1 Introduction

Cryptocurrency gain monetary value based on the principle of supply and demand and the difficulty of acquiring cryptocurrency. For instance, there are only a finite number of Bitcoins that are available to mine in the world. Other variables that dictate the value of a cryptocurrency include how easy the currency is to use, and the equipment and energy required to mine it.

For these reasons and others, the value of cryptocurrency has fluctuated in the past years. For instance, in 2010, the value of a Bitcoin was less than one cent. But before the end of 2017, the value of a Bitcoin shot up to just under $20,000 US dollars. As of December 2018, the value of a Bitcoin is hovering around $3,300 US dollars. By virtue of the fact that cryptocurrencies are becoming more valuable, cryptojackers have successfully infiltrated many top companies and services that we might use on a daily basis. Some examples of recent incidents include Tesla's Amazon Web Service Container, YouTube Ads and Make-A-Wish Foundation's website.

1.1 Tesla's Amazon Web Service Container

In February 2018, cloud security intelligence firm RedLock exposed a new case of cryptojacking targeting Tesla's Amazon Web Service's (AWS) software container. Attackers accessed Tesla's AWS access credentials by penetrating a non-password protected Kubernetes software container. The attackers then used the container to mine cryptocurrencies, for an as of yet unknown amount of time. [2]

1.2 YouTube Ads

Another case of cryptojacking was discovered on YouTube late January 2018. According to the report, anonymous attackers have managed to run ads on YouTube that consumed the visitors' CPU power and electricity in order to mine cryptocurrencies for the attackers. [3]

1.3 Make-A-Wish Foundation

Even nonprofit organizations such as the Make-A-Wish Foundation are targets of cryptojacking. According to Trustwave, a cybersecurity service provider, cryptojackers managed to incorporate a JavaScript miner, CoinImp, into the domain worldwish.org in order to illicitly mine Monero late November 2018. [4]

2 To the Community

Both Google and Apple have had to remove malware-infected apps from their respective online stores. Tech behemoths like Microsoft and Tesla were also victims of this fiasco. With the heightened prices of cryptocurrencies last year, cybercriminals are evermore desperate to acquire coins by any means possible. Because of this, we are all potential victims to this practice.

2.1 Cryptojacking is on the Rise

It is impossible to know exactly how much cryptocurrency is being mined by cryptojacking, but there is no question that cryptojacking is rampant. In-browser cryptojacking is skyrocketing. Adguard reported a 31% growth rate for browser-based cryptojacking in November 2017. Adguard's research found more than 33,000 websites running crypto mining scripts and estimated that those 33,000 sites had collectively over a billion visitors monthly. [1]

In February 2018, Bad Packets Report found 34,474 sites running Coinhive, the most popular JavaScript miner. In July, Check Point Software Technologies reported that four of the top ten malware found on machines are crypto miners. [1] Earlier in January 2018, the software security firm Check Point issued a report about a sharp increase in the prevalence of crypto-mining malware, stating that 55% of businesses worldwide are affected by the attacks. [4]

2.2 More Money Less Risk

The simple reason why cryptojacking is becoming more popular with attackers is more money for less risk. "Hackers see cryptojacking as a cheaper, more profitable alternative to ransomware," says Alex Vaystikh, CTO and cofounder of SecBi. [1] With ransomware, an attacker might get three people to pay for every 100 computers infected. But with cryptojacking, all 100 of those infected machines work for the attacker to mine cryptocurrency. Although the attacker might make the same amount of money cryptojacking as those three ransomware payments in the short-term, in the long-term, crypto mining continuously generates money. [5]

Compared to that of ransomware, the risk of the attacker being caught and identified is also much lower for cryptojacking. This is because crypto mining scripts normally run surreptitiously in the background and can go undetected for a long period of time. Even once discovered, it is very hard to trace back to the source, and the victim has little incentive to do so since normally nothing of ample value was stolen or encrypted. On top of that, attackers tend to prefer the more anonymous cryptocurrencies such as Monero and Zcash over the more popular Bitcoin, which makes it even harder to trace the illegal activity back to the attacker. [1]

3 How Cryptojacking Works

A recent study from Concordia University on cryptojacking found that the JavaScript browser mining program Coinhive is currently the most popular miner for Monero mining and cryptojacking in general. [6] Using a coin miner such as Coinhive, attackers have two primary ways to get a victim's computer to secretly mine cryptocurrencies. One is to load crypto mining code onto the victim's machine, the other is to inject a script onto a website. [5]

3.1 Coinhive

Coinhive works by offering an Application Programming Interface to users, which then allows the user to use a website visitors' CPU resources to mine Monero. Coinhive markets itself to web-based companies as a substitute for online advertisement, proclaiming unabashedly on their website's main page: "Monetize Your Business With Your Users' CPU Power". [6] Coinhive itself is not an issue, but the use of Coinhive without user consent is.

3.2 Loading Crypto mining Code

The first way is to trick the victims into loading crypto mining code onto their machines. This is done through phishing-like tactics where the victims receive an email that encourages them to click on a link. The link then executes code that loads the crypto mining script on the machine. The mining script then runs in the background as the victim continues on with their activities. [1]

3.3 Inject a Script

The other way is to inject a script onto a website or an ad. When the victim visits the website, or when the infected ad pops up in their browsers, the script automatically executes. No code is stored on the victims' machines. As the script executes, the code then runs complex mathematical problems on the victims' machines and emits the solutions of those problems to a server that the attacker controls. The solutions are then transformed into cryptocurrency. [5]

4 Defenses

Cryptojacking is very prevalent and anyone can be a potential victim. The sections below illustrate how to prevent, detect and respond to cryptojacking.

4.1 Prevent Cryptojacking

Most of the effort in defending against cryptojacking should be put into preventing it. Below are a few precautions that can be taken to minimize the risk of cryptojacking.

Install an anti-crypto mining extension or ad blocker onto web browsers. Since cryptojacking scripts are normally delivered through web ads, by installing an ad blocker can be an effective way to stop cryptojacking attempts in their tracks. Some extensions like Ad Blocker Plus, No Coin and MineBlocker even have capabilities specifically designed to detect crypto mining scripts. [1]

Use end point protection that is able to detect common and known crypto miners. There are many antivirus software vendors that have added crypto miner detection to their products. If it is a known crypto miner, there's a good chance it will be detected. However, this method is not foolproof as cryptojackers are constantly changing their strategies to avoid detection at the endpoints.

Keep web filtering tools up to date. If a web page is known to be delivering cryptojacking scripts, make sure your users are blocked from accessing it. [5]

Maintain browser extensions. Since some attackers use malicious browser extensions as a vehicle to execute crypto mining scripts, by updating and maintaining browser extensions, the chance of a poisoned legitimate extensions is drastically lowered.

4.2 Detect Cryptojacking

Detecting cryptojacking can be difficult. Don't count on endpoint protection tools to stop cryptojacking as crypto mining code can a lot of times hide from signature-based detection tools. Below are a few steps that can be taken to detect cryptojacking.

Keep an eye out for signs of crypto mining. Sometimes the first sign that the machine is infected with a crypto mining script is slowed performance. Other signs to look out for include overheating systems, which could cause CPU cooling failures and can cause damage to the device.

Deploy a network monitoring solution. Cryptojacking can be easier to detect in a corporate network than it is at a home network because most consumer end-point solutions cannot detect it. Network perimeter monitoring that analyzes all web traffic has a good chance of detecting crypto miners. For example, SecBi uses an artificial intelligence solution to review network data and detect cryptojacking and other threats. [1]

Stay abreast of cryptojacking trends. Crypto mining code and methods delivery are constantly evolving. If the delivery mechanisms are understood, the particular exploit kit that is delivering crypto mining scripts can be pinpointed. Then, defenses against the exploit kit will be defenses against being infected by the cryptomining malware.

4.3 Responding to Cryptojacking

There are not many ways in which you can respond to cryptojacking. Below are some steps to take if cryptojacking is detected.

Kill and block website delivered scripts. If the detected attack is in the form of an in-browser JavaScript attack, the solution is simple. Close the browser tab that is running the script. The website that is delivering the script should then be blocked.

Update and purge browser extensions. If the browser is infected by an extension, simply closing the tab will not stop the mining script from running. Instead, locate and remove the infected extensions and make sure all the extensions are up to date.

Learn and adapt. Understand how the machine was infected and take the necessary precautions to prevent future occurrences.

5 Conclusion

It is entirely possible that many users may not realize that they are have bene infected by this malware and is potentially paying for raised electricity bills, slower computer and Internet performance, and shorter device lifespan.

Cybercriminals are following the money and cryptojacking is the way to go. Cryptojacking incidents inflicts damage that is not immediately apparent, but it is profitable. Whereas, ransomware for example, is extremely disruptive and banking Trojans are much more difficult to monetize.

Stealing has moved from using a gun to using a computer. And as long as cryptocurrencies have value, criminals will use computers to steal it. What cryptojacking shows is that someone doesn’t even need to own cryptocurrency to be a victim.

References

[1] Nadeau, Michael. “What Is Cryptojacking? How to Prevent, Detect, and Recover from It.” *CSO Online*, CSO, 29 Aug. 2018, www.csoonline.com/article/3253572/internet/what-is-cryptojacking-how-to-prevent-detect-and-recover-from-it.html.

[2] Zuckerman, Molly Jane. “Tesla Cryptojacked, Hackers Use Passwordless System To Mine Crypto.” *Cointelegraph*, Cointelegraph, 11 Dec. 2018, cointelegraph.com/news/tesla-cryptojacked-hackers-use-passwordless-system-to-mine-crypto.

[3] Partz, Helen. “Crypto-Mining Malware Epidemic: 55% of Businesses Affected Worldwide, Including YouTube.” *Cointelegraph*, Cointelegraph, 11 Dec. 2018, cointelegraph.com/news/crypto-mining-malware-epidemic-55-of-businesses-affected-worldwide-including-youtube.

[4] Partz, Helen. “Cybersecurity Firm Detects Cryptojacking Malware on Make-A-Wish Foundation Website.” *Cointelegraph*, Cointelegraph, 12 Dec. 2018, cointelegraph.com/news/cybersecurity-firm-detects-cryptojacking-malware-on-make-a-wish-foundation-website.

[5] “What Is Cryptojacking? How It Works and How to Help Prevent It.” *Norton Family Premier*, us.norton.com/internetsecurity-malware-what-is-cryptojacking.html.

[6] Zuckerman, Molly Jane. “The Ethics Of Cryptojacking: Rampant Malware Or Ad-Free Internet?” *Cointelegraph*, Cointelegraph, 12 Dec. 2018, cointelegraph.com/news/the-ethics-of-cryptojacking-rampant-malware-or-ad-free-internet.