PONDURANCE

Cryptojacking: Stop Attackers From Mining on Your Dime

Cryptojacking can lead to business costs and disruption including hardware wear and tear.

INTRODUCTION

Cryptocurrency is a digital currency used to buy goods—secured by cryptography—making it nearly impossible to counterfeit or double-spend due to the nature of its blockchain technology. Digital currencies have proven to be a dynamic market attracting more than just investor enthusiasm. With cryptocurrency hitting an all-time high in late 2017 and into 2018, threat actors quickly learned they could mine for cryptocurrency by using malicious scripts to do the job for them with minimal overhead, making 2018, at the time, the biggest year for cryptomining malware. In fact, nearly 90% of all remote code execution attacks were associated with cryptomining, stealing valuable computing resources while remaining undetected.

BASIC UNDERSTANDING OF CRYPTOCURRENCIES

Before we dive into cryptocurrency mining, let's discuss some basics about cryptocurrencies. When transactions are made with cryptocurrencies or new currencies are added they are recorded on a worldwide blockchain ledger. This ledger is part of a peer-to-peer database that is shared and maintained by a community, which is why digital currencies are decentralized.

Cryptomining is the term used to refer to the process of generating new digital currency by solving a puzzle within the blockchain, resulting in a monetary gain for the miner and new currency added to the blockchain. These complex puzzles are solved by validating previous transactions within the blockchain ledger to maintain the ledger, which results in a new block added to the chain and it is how miners earn a "reward per block". These digital rewards vary by the type of cryptocurrency being mined and are halved every four years making it harder for miners to earn more currency for their efforts.

Cryptocurrencies are becoming more difficult and resource-intensive to mine, and the reward per block is reduced by nearly 50 percent every four years. In order to gain a higher return on investment for mining cryptocurrency, many have turned to cryptojacking activities as a means to make a profit. **Cryptojacking** is a type of cyber attack that threat actors use to deploy malicious code in phishing emails or advertising malware known as "adware," to gain unauthorized access to the computing resources required to solve the complex puzzles within the blockchain.

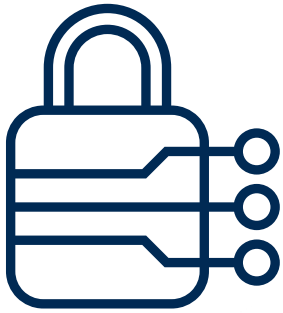
THE SKYROCKETING VALUE OF CRYPTOCURRENCY

Bitcoin is the highest valued cryptocurrency, and it has grown enormously over the years—with the exception of a significant decline in 2019—and as of March 31, 2021, it is currently trading at $59,360. As a result, there is growing market demand for cryptomining that ranges from individuals, cryptomining groups, and cybercriminals.

The surge in the market for this digital currency results in an increase in cryptomining attacks, also known as cryptojacking. While threat actors fraudulently steal computing power from cloud servers and other resources, this attack rarely sets off antivirus triggers. Cryptojacking is an attack type that doesn't require privilege escalation to gain access to resources needed to mine for cryptocurrency.

Pondurance spends a considerable amount of time analyzing these types of attacks and identifies stealth mining operations that drain bandwidth, damage hardware through wear and tear, and disrupt business operations. In doing so, we have found that some common factors associated with cryptojacking attacks are dependent on the cryptocurrency market, making it a lucrative business operation for threat actors.

Cybercrime is a profitable business for threat actors, with a cost that is growing 15 percent year-over-year, expected to reach more than $10.5 trillion by 2025.



PONDURANCE

PRICE HISTORY

To fully understand the value of cryptomining, let's take a look at the history of one of the biggest cryptocurrency players, Bitcoin. In April 2011, the Bitcoin price started to jump from $1 to $32 in June, resulting in a 3200% swing. Let's jump to 2013, Bitcoin was trading at $13.40 at the beginning of the year and quickly reached upwards of $220 by April, and by the end of the year, it was trading at $1156.10. However, by late 2017 Bitcoin had its highest streak being valued at $19,783 which was up 1,824% from January of that year.

Apart from daily volatility, cryptocurrency has seen its fair share of fraud and attackers looking to get their hands on the monetary gain associated with this digital currency. With the value of Bitcoin going back up in 2020, we expect to see a significant increase in cryptojacking scripts that compromise cloud server accounts such as Amazon Web Services, Google Cloud Platform, and Azure for the extensive raw processing power that these infrastructures offer. Malicious miners have also exploited routers, mobile devices, and unmonitored IoT devices that run these mining scripts in the background without individuals knowing it.

WHAT IS CRYPTOJACKING?

Cryptojacking involves the unauthorized access and use of computing resources to mine for cryptocurrency. Gaining access to an individual's computer or server is the easy part of the process. Mining for cryptocurrency is a detailed and costly process because of the amount of computing power needed to quickly solve mathematical equations and verify transactions to be rewarded for the "proof of work". Cryptojacking is a workaround for miners who prefer not to use their own resources to mine for cryptocurrency. Mining requires a large amount of computing power to quickly attempt to solve these mathematical puzzles in order to be the first one to complete the blockchain. Not to mention the amount of electricity to power the hardware involved, which is another reason why malicious miners prefer to use cryptojacking techniques to have others do the work for them.

HOW ARE CRYPTOJACKING ATTACKS DEPLOYED?

Threat actors often use malicious JavaScript that loads malware to an end user's computer or server to gain unauthorized access to valuable resources used to mine for cryptocurrencies. These attacks can vary in form, in fact, we were brought into a manufacturing company to help them with an investigation into a "rogue" IT administrator that was threatening to hold them hostage. The admin knew all of the passwords to the systems and was not going to share them if they terminated his employment.

Interestingly, when we activated the sensor, we immediately found two Bitcoin mining operations in progress without the manufacturer's knowledge. Attacks like this consume the processes required to mine at a low threshold and can avoid triggering anti-virus alerts or cloud providers, which is why it is important to monitor the logs, networks, and endpoints on a 24/7 basis. Manufacturing companies often have a rich level of bandwidth and system processing due to their massive supply chain systems making them an ideal target for these types of attacks.

HOW CRYPTOJACKING ATTACKS SUCCEED

In comparison to ransomware, cryptojacking is an underreported attack and remains one of the most difficult attacks to detect. In fact, the sole purpose of cryptojacking is to run in the background—with little signs of infection—often making it difficult for virus scanners to differentiate it from a benign script.

Attackers leverage common ingress techniques to gain access to devices by getting a victim to click on a malicious link in an email that leads to cryptojacking. In addition, infecting a website or online advertising with JavaScript that automatically executes once the browser is loaded is another method attackers use to gain entry to a larger network.

PONDURANCE

The best defense for cryptojacking is to first understand how it can infect and drain an organization's computing power. Some common ways that cryptojacking is deployed throughout an organization is the following tried and true methods:

- Phishing is frequently a gateway to **file-based cryptojacking**. This type of attack can lead to an end-user clicking on a malicious link that loads cryptomining scripts to a computer.
- Infected online advertising or websites with malicious JavaScript is considered **browser-based cryptojacking**. The script automatically executes and downloads the script onto the user's computer.
- Threat actors can search for credentials or API keys on GitHub as a valid reconnaissance activity to gain unauthorized access to cloud servers and other systems.

Cloud servers continue to be a more lucrative target than routers, IoT devices, and individual computers because of the computing power behind this infrastructure. Seizing on their initial access, cryptojackers can often pivot to more advanced or damaging techniques such as data exfiltration.

Let's review some ways you can identify and prevent cryptojacking attacks:

- Consistently monitor digital assets for high CPU usage, especially within your cloud infrastructure. Review your billing to ensure any costs associated with soaring CPU usage are legitimate resources being used.
- Train your organization's IT department to understand and detect cryptojacking malware. They should have a full understanding of common signs of an attack to take immediate steps to mitigate the attack.
- Educate your employees with continuous cybersecurity awareness training. Your employees can act as a human firewall by understanding common signs of cryptojacking on their local machines, especially if they experience performance issues or suspicious emails.
- Monitor your network and email for malicious links and traffic with a Managed Detection and Response (MDR) service that can provide your organization with 24/7 monitoring along with a SOC that can review alerts to ensure fast remediation.

Cryptojacking does not require escalated privileges and it rarely sets off antivirus triggers.

HOW TO PROTECT AGAINST CRYPTOJACKING ATTACKS

Even though cryptojacking does not usually damage data, it can lead to business costs and disruption — even hardware damage through wear and tear. As organizations look to manage their growing cloud computing costs, attacks that fraudulently hijack computing cycles and cloud pose an increasing threat.

- Actively manage your cloud vulnerabilities, as most vulnerabilities are found in cloud misconfigurations. The same security controls found in an organization's local network are not automatically available or configured in the cloud.
- Implement temperature-based monitoring within your data center or on-prem hosting to detect overworked hardware throughout your digital assets. Overheating is the first sign of an exhausted CPU.

CONCLUSION

As cryptojacking yields lucrative results, with minimal effort, we will continue to see an influx in cryptojacking attacks. As cryptocurrencies continue to rebound, the chaotic ups and downs will attract great actors looking to capitalize on these dynamics.

As long as their malicious scripts can run local commands on a machine, attackers can use this access to start mining cryptocurrency. Midsize and enterprise organizations will continue to be prime targets for these types of attacks, which can result in negative effects on their overhead costs.

It is important to understand the varying attack patterns, especially since attackers can run these campaigns with minimal effort. We will see more mining groups and cryptomining code injections as cryptojacking becomes more lucrative than other cybercrime techniques during these market swings. Cybercrime is a profitable business for threat actors, with a cost that is growing 15 percent year-over-year, expected to reach more than $10.5 trillion by 2025. The costs associated with cybercrime range from payouts, damages to businesses, theft of intellectual property, and the loss of personal and financial data.

By following the steps outlined in this paper, you can help reduce and detect cryptojacking malware throughout your digital landscape and reduce the cost associated with this type of attack.

ABOUT PONDURANCE

Pondurance delivers world-class Managed Detection and Response services to industries facing today's most pressing and dynamic cyber security challenges including ransomware, complex compliance requirements, and digital transformation accelerated by a distributed workforce. By combining our advanced platform with our experienced team of analysts we continuously hunt, investigate, validate and contain threats so your team can focus onwhat matters the most.

Pondurance experts include seasoned security operations analysts, digital forensics and incident response professionals, and compliance and security strategists who provide always-on services to customers seeking broader visibility, faster response and containment, and more unified risk management for their organizations. Visit Pondurance.com for more information.