PONDURANCE

5 Ways to Protect Against Cryptojacking Attacks

pondurance.com

Digital currencies have proven to be a dynamic market attracting more than just investor enthusiasm. With cryptocurrency hitting an all-time high, threat actors quickly learned they could mine for cryptocurrency by using malicious scripts to do the job for them with minimal overhead. In this eBook, we will take a look at the five ways to identify and protect against cryptojacking.

PONDURANCE

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. Mining for cryptocurrency is a detailed and costly endeavor due to the amount of computing power needed to quickly solve mathematical equations and verify transactions to be rewarded for the proof of work. Cryptojacking serves as a workaround for miners who prefer not to use their own resources to mine for cryptocurrency.

PONDURANCE

How Cryptojacking Attacks Succeed

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 include the following 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 are considered **browser-based cryptojacking**. The script automatically executes and downloads the script onto the user's computer.

PONDURANCE

5 Ways To Protect Against Cryptojacking Attacks

LET'S REVIEW FIVE WAYS TO IDENTIFY AND PREVENT CRYPTOJACKING ATTACKS:

Monitor digital assets: Consistently monitor digital assets for high central processing unit (CPU) usage, especially within your cloud infrastructure. Review your billing to ensure any costs associated with soaring CPU usage are legitimate.

Train staff: 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 an attack.

Empower employees: 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.

Employ an MDR: 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 security operations center (SOC) that can review alerts to ensure fast remediation.

Monitor for overheating: Implement temperature-based monitoring within your data center or on-premises 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 bad 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. Attacks of these types can be detected by using an MDR service provider as they will be able to detect the increase in unusual activity on your networks. Learn more about cryptojacking and how to protect your organization from these types of attacks in our whitepaper: Cryptojacking: Stop Attackers From Mining on Your Dime.

PONDURANCE

About Pondurance

Pondurance delivers world-class **MDR** services to industries facing today's most pressing and dynamic cybersecurity 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 own team can focus on what matters 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 **www.pondurance.com** for more information.

pondurance.com

500 N. MERIDIAN ST., STE. 500
INDIANAPOLIS, IN 46204