CTPRO.IO

CRYPTOJACKING

What is Cryptojacking?

Cryptojacking refers to the unauthorized use of another person’s computing resources to mine cryptocurrency. This type of cyberattack targets a wide range of systems, including desktops, servers, and cloud infrastructure, allowing hackers to mine crypto coins without the owner’s consent. The cryptojacking code typically operates discreetly in the background, allowing users to continue their normal activities without immediate awareness of the intrusion. As a result, victims may only notice subtle signs of compromise, such as a decline in system performance, delays in application responsiveness, overheating of devices, increased power consumption, or unexpectedly high bills from cloud computing services.

These indicators can serve as crucial alerts for users to investigate further. By recognizing these symptoms early, organizations and individuals can take proactive measures to mitigate the impact of cryptojacking and protect their resources from unauthorized exploitation. Regular monitoring and security practices are essential to safeguard against such threats.

How Cryptojacking Works

Coin mining is a legitimate process that generates new cryptocurrency by rewarding miners who solve complex computational problems. These problems verify transactions and add them to the blockchain, with miners acting as auditors to ensure transaction legitimacy while introducing new coins into circulation.

However, mining requires significant processing power and energy, leading to high operational costs. As competition increases and rewards decrease, some cybercriminals exploit this by stealing computing and energy resources. They use various hacking methods to hijack systems for mining, redirecting the results to their own servers for profit. This highlights the need for strong cybersecurity measures to protect against such threats.

Attack Methods

Cryptojacking has mainly targeted desktops and laptops using methods like fileless malware, phishing, and malicious scripts. Attackers often send fake emails that install crypto mining scripts when users click links. They also inject scripts into websites or ads that run automatically without leaving code on devices. While these tactics are still a threat, criminals have developed more sophisticated methods for higher profits.

Attackers are increasing their profits from cryptojacking by targeting servers, network devices, and IoT devices. Servers are especially appealing because they are more powerful than regular desktops. In 2022, hackers looked for publicly exposed servers with vulnerabilities like Log4J. They exploit these weaknesses to secretly install crypto mining software that connects back to the hacker's servers. Often, they use the compromised server to spread their cryptojacking efforts to other devices on the network.

Cybercriminals are targeting the software supply chain by adding harmful packages to open-source repositories. These packages contain cryptojacking scripts. This allows attackers to quickly expand their operations by attacking developers' systems and networks to use them for crypto mining, and infecting the software that developers create, so it runs crypto mining scripts on end users' machines.

Cryptojacking operations are exploiting cloud resources by breaking into cloud infrastructure for larger computing power. A Google study found that 86% of compromised cloud instances are used for crypto mining. Attackers target cloud services to scale their operations, often taking over managed environments or abusing SaaS applications. They scan for exposed APIs or unsecured storage to install mining software, using automated scripts to find vulnerable servers and spread across cloud systems.

Prevention and Detection

With a well-constructed and multifaceted defense strategy these evolving attacks can be effectively prevented. Organizations should use endpoint protection and anti-malware to detect crypto miners, keep web filters updated, manage browser extensions, and extend protection to servers. Cryptojackers target servers with known vulnerabilities, so basic hardening—like patching, disabling unused services, and limiting visibility—can greatly reduce attack risks. SCA tools improve visibility into software components to prevent supply chain attacks using coin mining scripts. Organizations can stop cryptojacking in the cloud by tightening configurations, securing exposed services, and removing hardcoded credentials.

Cryptojacking is a stealthy cyberattack that can slow down devices, often indicated by increased help desk complaints. Advances in endpoint protection and detection have improved the identification of these attacks. Network monitoring tools can detect suspicious web traffic, while cloud monitoring helps spot unauthorized crypto miners. Google Cloud, for example, offers Virtual Machine Threat Detection (VMTD) for this purpose. Organizations should actively hunt for subtle signs of cryptojacking and regularly monitor their websites for mining code and file changes.

Responding to Cryptojacking

To effectively respond to a cryptojacking attack, organizations should follow a structured approach. First, containment is crucial; this involves killing any web-delivered scripts by closing the browser tab running the malicious JavaScript. It’s important to note the URL of the source and update web filters to block it. Next, during the eradication phase, compromised container instances should be shut down. Organizations must investigate the root causes of the compromise to ensure that new container images are secure and not similarly configured. Recovery involves reducing permissions for affected cloud resources and regenerating API keys to prevent attackers from re-entering the environment. Finally, learning from the incident is essential. Organizations should analyze how the attack occurred and update training for users and IT staff to enhance their ability to recognize and respond to future cryptojacking attempts. This comprehensive response not only addresses the immediate threat but also strengthens defenses against future incidents.