Build Your Defense Against Cryptojacking, an Increasing Threat

Security Tips to Protect Against Cryptojacking
Almi Dumi, eMazzanti Technologies InfoSec Team

The first cryptocurrency emerged in 2009 as Bitcoin. Over the past nine years, Bitcoin and other digital currencies have gradually cemented a place on the financial playing field. While the currency has attracted attention for its growth potential and anonymity, it also opens the door to new security threats in the form of cryptojacking.

The term "cryptocurrency" combines the words cryptography and currency. And in fact, the money is based on complicated mathematical encryption. The "coins" only exist as lines of code in a centralized database, or digital ledger. Once worth only pennies, a single bitcoin is currently valued at over $6000.

Mining for Cryptocurrency

As cryptocurrency has increased exponentially in value, it has become highly desirable. There are two ways to obtain cryptocurrency. The most straightforward, and expensive, method is to buy bitcoins (or other rival currencies) on a centralized exchange such as Coinbase.

More often, individuals earn cryptocurrency through a process called mining. Miners solve the complex mathematical equations used to verify digital transactions and release new cryptocoins into circulation. In return, they are rewarded with cryptocurrency.

Over time, the complexity of the equations has increased, requiring more and more processing power. A single high-end computer might take years to solve the equations that result in a cryptocoin. But with an array of computers…a miner can turn a profit. Enter cryptojacking.

Cryptojacking: An Increasing Threat

Why buy a farm of computers and the electricity to run them when you can simply borrow the processing power from unsuspecting victims? Unscrupulous cryptominers have turned to hijacking computers, networks and even mobile devices to use the processing power to earn cryptocoins.

Alarmingly, in December 2017, cryptominers affected 55 percent of businesses across the world. And in a single quarter of this year, 2.5 million new occurrences of cryptojacking software were identified.

There are two approaches to cryptojacking:

- **Infecting an unsuspecting device with cryptomining code** – This method works like classic malware. The user clicks a malicious link that downloads cryptomining code. The mining process runs in the background, visible to the victim only as a drain on processing power.
- **In-browser mining** – This method embeds lines of JavaScript code onto a web page. While a user is visiting the web page, the code accesses the processing power of the visitor's device.

Unlike ransomware, with cryptojacking, you can be a victim and not even be aware that a bad actor has taken over your device's processing power. The most tell-tale signs are increased CPU usage, an

overheated device and higher electrical bills. For an organization, this can significantly drain both resources and budget.

Multi-faceted Defense

As the threat from cryptojacking grows, individuals and businesses need to ramp up security measures. Educate your users (again) on safe computing. Never click suspicious links and avoid downloading files from unknown sources. Make sure your antivirus software looks for cryptomining and keep it up-to-date.

Adblock includes options to block cryptomining scripts, and popular browsers now offer extensions to guard against mining. These measures provide some protection, but for organizations, a more comprehensive approach is needed.

If you suspect your business has been affected by cryptojacking, or if you want to prevent the problem before it occurs, reach out to eMazzanti. Our cyber-security experts will conduct an assessment to determine the existence of cryptomining code on your devices or even on your web site.

After an initial assessment, our team will help you implement next generation protocols and multi-layer security to guard against future attack. We will monitor your network 24/7 for threats, giving you the peace of mind you need to focus on your business.

Almi Dumi is the Chief Information Security Officer at eMazzanti Technologies. Leading a highly skilled cyber-security team, Dumi has been with eMazzanti for over eleven years. He holds numerous professional certifications and is dedicated to providing the highest quality cyber-security technology to protect customers' valuable business assets.