MARSH

INSIGHTS | AUGUST 2018

Mining for Virtual Gold: Understanding the Threat of Cryptojacking

Instead of stealing company data or holding it ransom, cyber criminals have mastered a new way to attack businesses. Through cryptojacking, one of the fastest growing types of cyber-attacks globally, criminals can siphon an organisation's computing power to mine cryptocurrency, opening the door to new sources of illicit revenue at the company's expense. And your organisation may already be a victim and not even know it.

What is Cryptojacking?

Thousands of cryptocurrencies or "coins" exist today, all with varying purposes. Some, such as Bitcoin and Monero, serve as a digital currency and can retain considerable monetary value. The all-time high for a single Bitcoin, for example, peaked around $20,000 in December 2017; the value fluctuates daily based on availability and currency movement. Creating certain cryptocurrencies, including Bitcoin and Monero, requires the completion of a complex cryptographic puzzle that is recorded on a blockchain, a process known as cryptomining. Performing these calculations can be expensive, requiring considerable processing and electrical power and, in some cases, specialised equipment. For their efforts, miners are rewarded with newly created units of the mined cryptocurrency, providing a potentially lucrative pay day depending on the value and quantity of the coin.

As the value of cryptocurrencies has soared, many organisations have turned to coin mining as a new source of revenue. Some companies have asked online users whether they would allow the mining of cryptocurrency on their computers in exchange for eliminating advertisements. However, a growing number of miners are now simply stealing or "hijacking" the necessary computing power from unsuspecting consumers and businesses. What was once a complicated process has become relatively easy with the advent of in-browser mining scripts that allow scammers to use the computing power of anyone who visits an infected website. Cryptomining malware can also be spread through malicious links, advertisements, email attachments, public Wi-Fi, fake apps, and system backdoors.

Infections have been rampant, affecting nearly 30% of companies monitored by cybersecurity firm Fortinet in the first quarter of 2018, doubling 2017's record numbers. In February 2018, for example, hackers compromised a screen-reading web plugin for the blind, affecting over 4,000 websites worldwide, including the UK's National Health Service.

Some companies represent particularly strong targets for cryptojacking. These include:

- Critical infrastructure companies, which consume significant amounts of power and often have vulnerable industrial control systems.
- Companies that rely heavily on cloud services, which present the opportunity for "high-powered mining."

Cryptojacking is also frequently tied to Internet of Things (IoT) devices such as mobile phones, which can allow miners to quickly amass armies of hijacked devices to mine cryptocurrency at scale.

How Cryptojacking Can Affect Businesses

The theft of company computing power through cryptojacking can have real financial consequences over time. Accurately capturing the direct costs of cryptojacking, however, may prove difficult, since most victims may not notice an infection or recognise the culprit.

But the threat is real. The performance of an infected computer system could become sluggish due to the complex and continuous operations required to perform mining calculations. Overworking computers could lead to the crashing of necessary functions and, in some cases, the overheating and ultimate failure of central processing units. This may seem like a temporary or isolated nuisance, but spread across a corporate enterprise, it could have disruptive and costly implications for companies. In addition to the potential degradation in service and resulting lost productivity and income, businesses may incur costs for higher energy consumption or cloud usage. An organisation could also incur extra expenses to replace hardware sooner or more frequently than planned, and for additional IT support to help address system performance issues.

Companies that transfer cryptomining software to unsuspecting third parties have also become the subject of litigation and regulatory scrutiny.

Of course, if miners are able to compromise a corporate network to steal company computing power, it is possible for the same individuals to access data, install malware, or exploit other vulnerabilities to cause mischief. And, just as announcing any type of major data breach can bring reputational harm, publicly disclosing a cryptojacking event may also damage a company's standing with customers and others.

Can Cyber Insurance Help?

Cyber insurance policies are designed to cover both direct loss and liability caused by a cyber event. Cyber policies can cover expenses incurred directly by policyholders for IT forensics, recreation or restoration of data assets, data breach response, loss of business income, and reputational damage. Coverage also extends to third-party liability claims for privacy breaches and security failures, such as the transfer of malware to a third party or the unauthorised disclosure of sensitive customer data.

A cryptojacking incident could result in several types of losses that are covered under cyber insurance policies. For example, a cryptojacking incident could disrupt important control systems or a company network, triggering business interruption coverage, or it could result in the loss of sensitive information, triggering data asset recovery coverage. Cyber insurance may also help cover costs for investigations to determine the cause, source, and scope of a cryptojacking event and forensic accounting services for claim preparations. Companies that unwittingly pass cryptojacking malware to third parties may also look to a cyber insurance policy for relief from any related claims for damages.

Whether cyber insurance responds will depend upon the specific terms and conditions of a given policy. Businesses should consider carefully reviewing specific coverage provisions to determine whether and how their policies will react to cryptojacking losses. Businesses should also work with their risk advisors to ensure that their cyber policies include specific claim triggers and broad definitions of loss in order to capture all possible scenarios for which an insured would expect to recover loss.

Recommendations

As long as there is big money to be made, cyber actors will likely continue to hijack computer systems to mine cryptocurrency, evolving their methods along the way. Like other cyber attacks, businesses should look to detect and prevent this growing and evolving threat and closely watch for signs of infection.

To further protect your business from cryptojacking, work with your insurance advisor to assess your potential exposures to cryptojacking and determine how your cyber policy may respond. The time to assess your cyber insurance policies for potential coverage is before your organisation is attacked.

For more information, contact your Marsh representative or:

JONO SOO
Client Executive – FINPRO Specialties
DDI: +64 9 928 3092
Mob: +64 21 071 8846
jono.soo@marsh.com