SONICWALL

SOLUTION BRIEF: THE GROWING THREAT OF CRYPTOJACKING – AND HOW TO STOP IT

Abstract

A cryptojacker is a form of malware that mines cryptocurrencies for an attacker. It robs your business of energy, hardware, productivity and security. This paper examines trends in illegal cryptomining attacks, how to know if your organization is compromised and best practices for defense.

Introduction

Despite the apparent decline of Bitcoin and other cryptocurrencies, they are still actively traded with wild swings in price due to their activity. With the cost of mining cryptocurrencies nearing (if not above) the price of a coin, attackers have turned to mining them with other people's equipment. For some organizations, cryptomining has become a growing significant threat.

Unlike ransomware that wants to be found (to ask for payment), a cryptojacker's job is to run invisibly but noisily in the background. Cryptojacking could soon become a favorite method for malicious actors because of its concealment. Low and indirect damage to victim's devices reduces chances of exposure and extends the valuable lifespan of a successful attack.

Despite vigilance and knowledge of the warning signs, a report from the Ponemon Institute stated the average length of time for an organization to discover malware or a data breach was 191 days.

Ransomware authors have switched gears over the past two years to use cryptojacking more, because a ransomware strain's effectiveness and ROI diminish as soon as it ends up on public feeds like VirusTotal. Like anyone else running a highly profitable business, cybercriminals need to constantly find new ways to fulfill their financial targets. Cryptojacking is fulfilling part of this need, and exploit kits like CoinHive are only making it easier for new attackers to get into the game.

The Lure of Cryptomining

With such low costs and risks as compared to buying and maintaining equipment, cybercriminals have strong incentives to generate cryptocurrency with someone else's resources. According to Business Insider research, infecting one machine could net up to $10 a day, so the challenge for cryptojackers is three-fold:

1. Find targets, namely organizations with a lot of devices on the same network, especially schools or universities
2. Infect as many machines as possible
3. Stay hidden for as long as possible

Cryptojackers use similar techniques as malware to sneak on to an endpoint: drive-by downloads, phishing campaigns, in-browser vulnerabilities and browser plugins, to name a few. And, of course, they rely on the weakest link — the people — via social engineering techniques.

The Threat of Cryptojacking

In comparison to more traditional malware, cryptomining attack variants still developing, threatening four major impacts upon your organization.

The first impact is wasted electricity, the most trackable form of waste. If the research cited listed above is accurate, and your organization is paying commercial rates for electricity, you could end up paying an extra $6 or more a day per endpoint.

Secondly, the damage it can do to a system is another cost that will affect your OpEx or CapEx line. Since cryptojacking's energy use is through the video card or processor, it adds extra strain on systems, which will wear them out over time, ultimately forcing replacement. Mobile devices are additionally burdened by battery damage as well.

A third impact is the loss of productivity due to limited resources. Employees with infected laptops may not be able to use resource-heavy applications like social media monitoring suites or engineering programs. Servers may not be accessible or severely hampered, and an unaware IT administrator may ask for additional hardware to maintain service levels. System outages may eventually cost more than the wasted energy and hardware combined, namely for companies in manufacturing.

A fourth impact is that many malware strains create backdoors and other exploitable vulnerabilities to give the attacker system access to control the cryptominer, or to do other damage such as extract critical information like passwords or ransomware the device upon discovery.

SonicWall anticipates that this year, we will see a sizable surge in new cryptojacking variants and techniques. While there have been improvements in the cryptomining strains found by SonicWall, we expect attackers to use advanced evasion tactics to bypass defenses as seen in recent ransomware strains such as LockerGoga.

How to Know if You are Infected by Cryptominers

Cryptominers are interested in your processing power, and cryptojackers must trade off stealth for profit. The amount of your CPU resources they take depends on their objectives.

Siphoning less power makes it harder for unsuspecting users to notice and stealing more increases their profits. In either case, there will be a performance impact, but if the threshold is low enough, it could be a challenge to distinguish the miner from legitimate software.

Enterprise administrators may look for unknown processes in their environment. End users on Windows should spawn a Sysinternals Process Explorer to see what they are running. Linux and macOS users should investigate using System Monitor and Activity Monitor, respectively, for the same reason.

From the end user's perspective, the first warnings to look for are extra-active fans, hotter-than-normal batteries, and slower-than-normal processes.

How to Defend Against Cryptominers

The first step in defending against cryptominers is to stop this type of malware at the gateway, either through firewalls or email security (perimeter security), which is one of the best ways to scrub out known file-based threats. Since people like to reuse old code, catching cryptojackers like CoinHive can be a simple first step. Ask your vendor if they have definitions in place for perimeter defenses and to prove it with a hit count.

If the malware strain is unknown (new or updated), then it will bypass static filters in perimeter security. If the attack is initiated by a file, and that file is unknown, it will be routed to a sandbox to inspect its nature, as long as the file is decrypted by the firewall's man-in-the-middle (MitM) inspection, such as SonicWall DPI-SSL. SonicWall employs a multi-engine sandbox called Capture Advanced Threat Protection (ATP) to find evasive threats from the application, to the OS, and down to the processor.

> SonicWall recorded 57.5 million cryptojacking attacks globally between April and December of 2018.

If you have an endpoint not behind this typical set up (e.g., it's roaming at the airport or hotel), you need to deploy an endpoint security product that includes behavioral detection. Cryptominers can operate in the browser or be delivered through a fileless attack, so the legacy solutions that come free with a computer are blind to it. At the core of our Capture Client anti-malware solution is the SentinelOne engine, which is a best-in-class solution for stopping advanced attacks such as cryptojacking. Furthermore, if an administrator discovers this malware, they can easily quarantine and delete the malware or, in the case of something that does damage to system files, roll the system back to the last known good state before the malware executed.

Conclusion

By combining a mixture of perimeter defenses, sandboxing and endpoint behavioral analysis, organizations can fight the newest forms of malware no matter what the trend or intent is.

Learn more. Read our white paper, "Best Practices for Protection Against Phishing, Ransomware and Email Fraud."

About Us

SonicWall has been fighting the cybercriminal industry for over 27 years, defending small, medium-sized businesses and enterprises worldwide. Our combination of products and partners has enabled an automated real-time breach detection and prevention solution tuned to the specific needs of the more than 500,000 organizations in over 215 countries and territories, so you can do more business with less fear. For more information, visit www.sonicwall.com or follow us on Twitter, LinkedIn, Facebook and Instagram.

If you have any questions regarding your potential use of this material, contact:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Refer to our website for additional information.
www.sonicwall.com