WHITEPAPER

Acronis Active Protection: Combating the growing threat of illicit cryptomining

Keep criminals from hijacking system resources

Cryptojacking: Understand the Danger and Avoid Becoming a Victim

INTRODUCTION

While 2016 and the early part of 2017 were a peak period for devastating ransomware attacks, the end of 2017 saw another threat become the number one headache for home users and businesses – illicit cryptomining.

Like ransomware, cryptominers are not a new phenomenon – programs capable of using computer resources to mine bitcoin without the help of specialized or powerful hardware have been around since at least 2011. Cybercriminals only began developing malware to perform this function in the wake of the cryptocurrency boom of 2017.

At that time, thousands of different blockchain-based digital currencies appeared, many of them rocketing upward in volume and capitalization, some of them able to be mined with ordinary computer resources. That created a temptation that some cybercriminals found too hard to resist.

WHAT IS CRYPTOMINING?

Cryptomining is one of the foundations of any cryptocurrency: it provides the processing horsepower necessary to verify previous transactions in the cryptocurrency, a process that ensures the digital currency's integrity. Cryptominers use their computers' resources to solve complex mathematical problems: the first miner to solve the problem gets paid for their efforts in the same cryptocurrency.

That process can be a lucrative exercise if you are the one getting paid for the resources you have expended to verify a cryptocurrency transaction – and those resources can be substantial, since arriving at a solution gobbles CPU cycles, plus the electricity needed for computing and HVAC to keep the machine cooled properly.

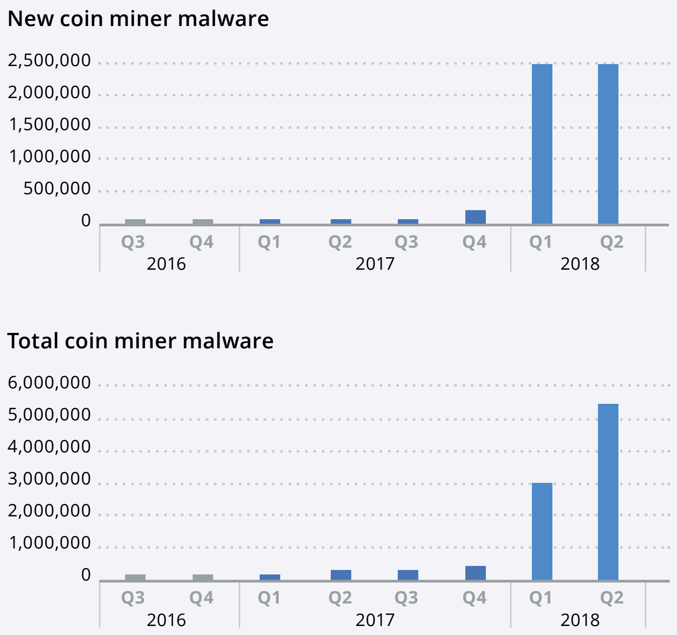
HIJACKING A COMPUTER'S POWER

What cybercriminals figured out is that if they infect your computer with cryptomining malware, you can use someone else's resources to solve the problem and collect the profits – at no cost to you. Multiply that by 1,000 or a million infected computing, and it is easy to see why cybercrooks jumped on the cryptomining malware bandwagon: it is a highly profitable racket and victims frequently have no idea their pocket is being picked.

Inventive cybercriminals decided that they could potentially multiply their profits by bundling several malware types together. If an unwary user clicked on a link or opened a malicious attachment in an email, they'd get two infections: cryptomining malware and ransomware.

The attacker would not activate both types at once – after all, a computer whose files are encrypted by ransomware cannot function as a cryptomining engine. Instead, the crook can choose which attack to launch based on the machine's hardware and software configuration, its anti-malware defenses, and which attack would prove more lucrative.

As a result, cryptomining malware suddenly became very popular with cybercriminals, and the security industry saw a huge spike in illicit coin miners.


New coin miner malware

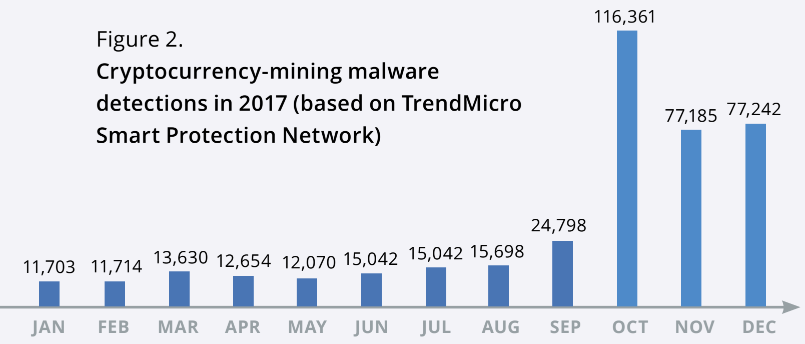
Total coin miner malware

Source: McAfee Labs Threats Report, September 2018

Anti-malware vendor McAfee detected roughly 400,000 samples of cryptomining malware in the fourth quarter of 2017, which exploded by a shocking 629 percent to more than 2.9 million samples in Q1 2018. Q2 saw an increase of 86 percent: more than 2.5 million new samples.

Anti-malware vendor TrendMicro reached similar conclusions from their research over the same period: they noted a 956 percent jump in such attacks from the start of 2017.

Figure 2.
Cryptocurrency-mining malware detections in 2017 (based on TrendMicro Smart Protection Network)



BROWSER-BASED CRYPTOJACKING

Worse, cryptomining malware has been developed not just as apps that quietly run on victims' Windows or Linux machines, but also as cryptocurrency mining services. These criminal enterprises surreptitiously install a small piece of JavaScript on websites that gets downloaded to the browser of anyone who visits the site. The pool of infected browsers works collectively on cryptomining solutions, stealing the computing and processing power without sharing the profits.

This approach caught on quickly. In November 2017, AdGuard, maker of a popular ad-blocking browser plugin, reported a 31 percent growth rate for in-browser cryptojacking. Its research found more than 30,000 websites running cryptomining scripts like Coinhive, which has affected one in five organizations worldwide. In February, Bad Packets Report found 34,474 sites running Coinhive, the most popular JavaScript miner. (It is also used for legitimate cryptomining activity.) In July 2018, Check Point Software Technologies reported that four of the top 10 malware instances it found were cryptominers.

Having affected nearly half of the world's businesses, cryptomining malware has overtaken ransomware as the biggest, most prevalent cyber threat out there today.

INTRODUCING A CRYPTOJACKING INFECTION

To infect their targets with cryptojacking malware, cybercriminals use a variety of techniques, from compromising individual user PCs and mobile devices, to infiltrating popular websites and spreading the malware to anyone that visits them.

Phishing and spearphishing emails designed to trick users into clicking on malicious links or opening malicious attachments remain an extremely effective attack vector. Some variants have worm components that allow the malware to jump from one compromised machine to others over the network. The EternalBlue exploit used in 2017 to multiply WannaCry ransomware infections into a global epidemic is still in use by cryptomining malware distributors today. But unlike ransomware targets, most cryptomining victims have no idea they're being stolen from beyond a vague sense that their system isn't performing as efficiently as it used to.

Fake software updates are another popular infiltration technique. In this instance, a malware download disguises itself as a legitimate update to Adobe Flash Player and covers its tracks by actually updating Flash while it delivers its malicious cryptomining payload.

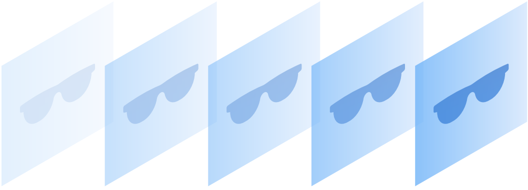
Another widespread method is to inject a malicious mining script into a legitimate website or block of online ads running on many websites. Once victims visit the website or their browsers load the online ad, the cryptomining process is initiated, stealing the resources and profits without the user's knowledge.

While infecting sites with malicious mining JavaScript that run in visitors' browsers may seem less profitable than running a native app full time, it's the large numbers that make the browser-based approach feasible. If millions of users visit an infected website and each one mines for at least 10 to 30 minutes, the final result may be more valuable than infecting 100,000 users with malware running as an application under Windows or Linux for a few hours per day.

RUNNING BELOW THE RADAR

Cryptomining malware developers have learned from their early mistakes. It is far less common today to find malware that consumes the majority of the victim's CPU capacity, which yields the kind of obvious performance slowdown that is likelier to prompt the user to notice and take remedial action. Newer editions of cryptomining malware take steps to conceal their presence, such as stealing only around 20 percent of the victim's CPU cycles, favoring idle times to perform the most resource-intensive calculations, etc. These cryptominers can thus steal resources from the victim without detection for a very long time.

Clever cryptojackers also hide themselves inside legitimate processes, e.g., using Windows PowerShell to execute hidden malicious mining scripts. This tactic fools most anti-virus programs, as they are programmed to trust Windows-signed executables like PowerShell by default.



NO EXPERTISE NEEDED

Engaging in illicit cryptomining does not require a cybercriminal to be a highly skilled software engineer. As with ransomware-as-a-service, cryptojacking-as-a-service can be purchased on the dark web for as little as half a US dollar. In addition, the high level of privacy and anonymity inherent in certain cryptocurrencies like Monero and Zcash makes it much harder to trace and catch the thieves.

For instance, Monero uses a public ledger to create and track the exchange of digital tokens, but obfuscates transactions to hide the source, destination, and actual amounts of cryptocurrency transferred. A recent academic study revealed that the embedded cryptocurrency miner, Coinhive, is generating $250,000 worth of Monero every month. This same research, released by RWTH Aachen University in Germany, concludes that Monero accounts for 75 percent of all browser-based cryptocurrency mining.

WHAT SYSTEMS ARE VULNERABLE?

In general, any internet-connected device with a CPU can be a target for cryptojackers, although Windows systems remain the most popular target given their popularity and sheer numbers.

Linux servers are next in line. Servers are particularly attractive as they usually run 24/7, so there's no downtime which provides more time for mining.

This doesn't mean cybercriminals do not mine on mobiles, tablets, printers, routers and smart TVs – they do, but it is just less effective and profitable.

CONSEQUENCES OF INFECTION

Cryptomining results in a number of adverse effects on business IT infrastructure, including:

- Degraded system and network performance
- Increased power consumption, system crashes, and potential physical damage from component failure
- Disruption of regular operations
- Financial loss due to the downtime caused by component failure, as well as the cost of restoring failed systems
- Extra cost of the increased power consumption and cooling

ACRONIS ACTIVE PROTECTION STOPS CRYPTOJACKERS

As a leading cyber protection vendor, Acronis has been tracking the cryptomining phenomenon as it has grown into a worldwide, pervasive threat. In the interest of protecting our business and consumer customers against cryptomining malware, we extended the anti-ransomware capabilities of Acronis Active Protection with technology to combat cryptomining malware as well.

The set of heuristics that are a foundation of Active Protection was expanded to detect the following scenarios on a Windows system:

- Suspiciously high CPU loads. The definition of “excessive” can be adjusted in real time and can be instantly changed by Acronis’ security experts.
- Use of Event Tracing for Windows (ETW). Cryptojackers make network requests to connect to known mining pools; Active Protection can identify and filter out such requests.
- Windowless processes. In order to stay hidden, most cryptojackers will not create a window. Acronis Active Protection monitors for windowless operations.
- Launches with specific command line arguments. Some specific command line arguments are typical of cryptomining activities, so it watches for these as well.

This enhanced version of Acronis Active Protection uses advanced machine learning to identify and terminate all known cryptojacking processes running on Windows.

Acronis’ experts also plan additional developments to further enhance the detection of cryptomining malware.

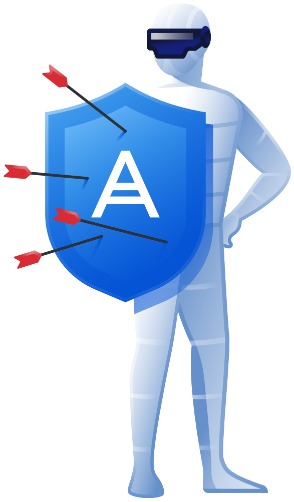
Among the refinements already in the works are:

- More heuristics addressing actual illicit cryptomining warfare
- GPU load detection, which is similar to the current CPU load monitoring
- Building machine learning models using Acronis’ Artificial Intelligence Cloud, which will simply give a verdict as to whether there is illicit cryptomining activity or not.

ADDITIONAL STEPS TO COMBAT CRYPTOJACKING

Given the continued growth in cryptojacking, businesses and consumers alike should take multiple steps to protect themselves against it. In addition to using solutions that include Acronis Active Protection, we recommend the following to combat illicit cryptomining attacks:

- Install quality anti-malware software. Good security software recognizes and protects a computer against cryptomining malware, allowing the user or admin to detect and remove an unwanted program before it can do any damage.
- Keep your software and operating systems up-to-date. Install updates and patches regularly to cover known vulnerabilities.
- Avoid downloading files from shady websites and be very careful with email attachments. Do not open attachments from any recipients you don’t know, confirm the sender’s email address, and always scan attachments using security software.
- Use strong passwords. Select passwords that will be difficult for attackers to guess, and use different passwords for different programs and devices. It is best to use long, strong passphrases that consist of at least 16 characters, and can’t be beaten by a simple dictionary attack.
- Change default usernames and passwords according to recommendations above. Default usernames and passwords are readily available to anyone on the internet.
- Apply application whitelisting, which is usually a part of an internet security suite or endpoint protection product. It will help you to prevent unknown executables from launching autonomously.



Acronis

Learn more at
www.acronis.com