Security 101: The Impact of Cryptocurrency-Mining Malware

trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/security-101-the-impact-of-cryptocurrency-mining-malware

by Kevin Y. Huang (Threats Analyst)

The Australian government has just recognized digital currency as a legal payment method. Since July 1, purchases done using digital currencies such as bitcoin are exempt from the country's Goods and Services Tax to avoid double taxation. As such, traders and investors will not be levied taxes for buying and selling them through legal exchange platforms.

Japan, which legitimized bitcoin as a form of payment last April, already expects more than 20,000 merchants to accept bitcoin payments. Other countries are joining the bandwagon, albeit partially: businesses and some of the public organizations in Switzerland, Norway, and the Netherlands. In a recent study, unique, active users of cryptocurrency wallets are pegged between 2.9 and 5.8 million, most of which are in North America and Europe.

But what does the acceptance and adoption of digital currencies have to do with online threats? A lot, actually. As cryptocurrencies like bitcoin gain real-world traction, so will cybercriminal threats that abuse it. But how, exactly? What does this mean to businesses and everyday users?

What is cryptocurrency?

Cryptocurrency is an encrypted data string that denotes a unit of currency. It is monitored and organized by a peer-to-peer network also known as a blockchain, which also serves as a secure ledger of transactions, e.g., buying, selling, and transferring. Unlike physical money, cryptocurrencies are decentralized, which means they are not issued by governments or other financial institutions.

Cryptocurrencies are created (and secured) through cryptographic algorithms that are maintained and confirmed in a process called mining, where a network of computers or specialized hardware such as application-specific integrated circuits (ASICs) process and validate the transactions. The process incentivizes the miners who run the network with the cryptocurrency.

[Related: Is Bitcoin the future of cryptocurrencies?]

Bitcoin isn't the be-all and end-all

There are actually over 700 cryptocurrencies, but only some are readily traded and even less have market capitalization above $100 million. Bitcoin, for instance, was created by Satoshi Nakamoto (pseudonym) and released in 2009 as open-source code. Blockchain technology made it all work, providing a system where data structures (blocks) are broadcasted, validated, and registered in a public, distributed database through a network of communication endpoints (nodes).

While bitcoin is the most famous cryptocurrency, there are other popular alternatives. Ethereum took "smart contracts" up a notch by making the programming languages needed to code them more accessible to developers. Agreements, or conditional/if-then transactions, are written as code and executed (as long as requirements are met) in Ethereum's blockchain.

Ethereum, however, earned notoriety after a hacker exploited a vulnerability in the Digital Autonomous Organization (DAO) running on Ethereum's software, siphoning US $50 million worth of ether (Ethereum's currency). This resulted in the development of Ethereum Classic, based the original blockchain, and Ethereum, its upgraded version (via a hard fork).

[READ: Ethereum Classic's Wallet falls victim to social engineering scam]

There are also other notable cryptocurrencies: Litecoin, Dogecoin, Monero. Litecoin is a purportedly technical improvement of Bitcoin that is capable of faster turnarounds via its Scrypt mining algorithm (Bitcoin uses SHA-256). The Litecoin Network is able to produce 84 million Litecoins—four times as many cryptocurrency units issued by Bitcoin. Monero is notable for its use of ring signatures (a type of digital signature) and CryptoNote application layer protocol to protect the privacy of its transactions—amount, origin, and destination. Dogecoin, which was initially developed for educational or entertainment purposes, was intended for a broader demographic. Capable of generating uncapped dogecoins, it also uses Scrypt to drive the currency along.

[READ: Who's attacking your IoT devices and smart home, and why?]

Cryptocurrency mining also drew cybercriminal attention

Cryptocurrencies have no borders—anyone can send them anytime anywhere, without delays or additional/hidden charges from intermediaries. Given their nature, they are more secure from fraud and identity theft as cryptocurrencies cannot be counterfeited, and personal information is behind a cryptographic wall.

Unfortunately, the same apparent profitability, convenience, and pseudonymity of cryptocurrencies also made them ideal for cybercriminals, as ransomware operators showed. The increasing popularity of cryptocurrencies coincide with the incidences of malware that infect systems and devices, turning them into armies of cryptocurrency-mining machines.

Cryptocurrency mining is a computationally intensive task that requires significant resources from dedicated processors, graphics cards, and other hardware. While mining does generate money, there are many caveats. The profit is relative to a miner's investment on the hardware, not to mention the electricity costs to power them.

Cryptocurrencies are mined in blocks; in bitcoin, for instance, each time a certain number of hashes are solved, the number of bitcoins that can be awarded to the miner per block is halved. Since the bitcoin network is designed to generate the cryptocurrency every 10 minutes, the difficulty of solving another hash is adjusted. And as mining power increases, the resource requirement for mining a new block piles up. Payouts are relatively small and eventually decrease every four years—in 2016, the reward for mining a block was halved to 12.5 BTC (or $32,000 as of July 5, 2017). Consequently, many join forces into pools to make mining more efficient. Profit is divided between the group, depending on how much effort a miner exerted.

[From TrendLabs Security Intelligence Blog: How Windows OS-run machines, routers and IP cameras became bitcoin-mining zombies]

Cryptocurrency-mining malware use similar attack vectors

Bad guys turn to using malware to skirt around these challenges. There is, however a caveat for cybercriminal miners: internet-connected devices and machines, while fast enough to process network data, don't have extensive number-crunching capabilities. To offset this, cryptocurrency-mining malware are designed to zombify botnets of computers to perform these tasks. Others avoided subtlety altogether—in 2014, Harvard's supercomputer cluster Odyssey was used to illicitly mine dogecoins. During the same year, a similar incident happened to US agency National Science Foundation's own supercomputers. In early February 2017, one of the US Federal Reserve's servers was misused to mine for bitcoins.

Cryptocurrency-mining malware employ the same modus operandi as many other threats—from malware-toting spam emails and downloads from malicious URLs to junkware and potentially unwanted applications (PUAs). In January 2014, a vulnerability in Yahoo!'s Java-based advertisement network was compromised, exposing European end users to malvertisements that delivered a bitcoin-mining malware. A month before it, German law enforcement arrested hackers for purportedly using malware to mine over $954,000 worth of bitcoins.

[READ: How South Korea's largest cryptocurrency exchange was hacked]

We've seen the emergence of hacking tools and backdoors related to cybercriminal bitcoin mining as early as 2011, and we've since seen a variety of cryptocurrency-mining threats that add more capabilities, such as distributed denial-of-service and URL spoofing. Another even tried to masquerade as a component for one of Trend Micro's products. In 2014, the threat crossed over to Android devices as Kagecoin, capable of mining bitcoin, litecoin, and dogecoin. A remote access Trojan (RAT) njrat/Njw0rm readily shared in the Middle Eastern underground was modified to add bitcoin-mining functionality. The same was done to an old Java RAT that can mine litecoin.

This year's notable cryptocurrency-mining malware so far are Adylkuzz, CPUMiner/EternalMiner, and Linux.MulDrop.14. All exploit vulnerabilities. Adylkuzz leverages EternalBlue, the same security flaw that WannaCry ransomware used to destructive effect, while CPUMiner/EternalMiner used SambaCry, a vulnerability in interoperability software suite Samba. Linux.MulDrop.14, a Linux Trojan, targets Raspberry Pi devices. These threats infected devices and machines and turned them into monero-mining botnets.

[READ: What happens when your router gets compromised?]

Cryptocurrency-mining malware's impact makes them a credible threat

Cryptocurrency-mining malware steal the resources of infected machines, significantly affecting their performance and increasing their wear and tear. An infection also involves other costs, like increased power consumption.

But we've also found that their impact goes beyond performance issues. From January 1 to June 24, 2017, our sensors detected 4,894 bitcoin miners that triggered over 460,259 bitcoin-mining activities, and found that more than 20% of these miners also triggered web and network-based attacks. We even found intrusion attempts linked to a ransomware's attack vector. The most prevalent of these attacks we saw were:

- Cross-site scripting
- Exploiting a remote code execution vulnerability in Microsoft's Internet Information Server (IIS)
- Brute force and default password logins/attacks
- Command buffer overflow exploits
- Hypertext Preprocessor (PHP) arbitrary code injection

- SQL injection
- BlackNurse denial of service attack

These malware can threaten the availability, integrity, and security of a network or system, which can potentially result in disruptions to an enterprise's mission-critical operations. Information theft and system hijacking are also daunting repercussions. These attacks can also be the conduit from which additional malware are delivered.

Internet of Things (IoT) devices are also in the crosshairs of cryptocurrency-mining malware—from digital video recorders (DVRs)/surveillance cameras, set-top boxes, network-attached storage (NAS) devices, and especially routers, given their ubiquity among home and corporate environments. In April 2017, a variant of Mirai surfaced with bitcoin-mining capabilities. Mirai's notoriety sprung from the havoc it wrought in IoT devices, particularly home routers, using them to knock high-profile sites offline last year. Over the first three quarters of 2016, we detected a bitcoin-mining zombie army made up of Windows systems, home routers, and IP cameras.

From January 1 to June 24, 2017, we also observed different kinds of devices that were mining bitcoin, although our telemetry cannot verify if these activities were authorized. We also saw bitcoin mining activities surge by 40% from 1,800 triggered events daily in February to 3,000 in March, 2017.

While bitcoin mining isn't inherently illegal (at least in many countries), it can entail a compromise if it doesn't have the owner's knowledge and consent. We found that machines running Windows had the most bitcoin mining activities, but also of note are:

- Systems on Macintosh OSes, including iOS (iPhone 4 to iPhone 7)
- Devices run on Ubuntu OS, a derivative of Debian Linux OS
- Home routers
- Environment-monitoring devices, used in data centers
- Android-run smart TVs and mobile devices
- IP cameras
- Print servers
- Gaming consoles

[READ: How to secure your router against Mirai and home network attacks]

Cryptocurrency-mining malware can make victims a part of the problem

Cryptocurrency-mining malware can impair system performance and risk end users and businesses to information theft, hijacking, and a plethora of other malware. And by turning these machines into zombies, cryptocurrency malware can even inadvertently make its victims part of the problem.

Indeed, their adverse impact to the devices they infect—and ultimately a business' asset or a user's data—makes them a credible threat. There is no silver bullet for these malware, but they can be mitigated by following these best practices:

- Regularly updating your device with the latest patches helps prevent attackers from using vulnerabilities as doorways into the systems
- Changing or strengthening the device's default credentials makes the device less prone to unauthorized access
- Enabling the device's firewall (for home routers), if available, or deploying intrusion detection and prevention systems to mitigate incursion attempts
- Taking caution against known attack vectors: socially engineered links, attachments or files from suspicious websites, dubious third-party software/applications, and unsolicited emails

IT/system administrators and information security professionals can also consider application whitelisting or similar security mechanisms that prevent suspicious executables from running or installing. Proactively monitoring network traffic helps better identify red flags that may indicate malware infection. Applying the principle of least privilege, developing countermeasures against web injections, securing the email gateway, implementing best practices for corporate mobile devices, and cultivating a cybersecurity-aware workforce are part of a defense-in-depth approach to reducing an enterprise's exposure to these threats. Ultimately, however, the security of internet-connected devices against cryptocurrency-mining malware isn't just a burden for their users. Original design and equipment manufacturers also play vital roles in securing the ecosystems they run in.

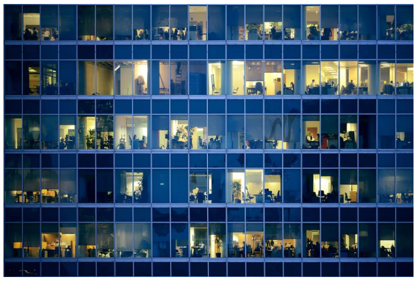
HIDE

Like it? Add this infographic to your site:
1. Click on the box below.   2. Press Ctrl+A to select all.   3. Press Ctrl+C to copy.   4. Paste the code into your page (Ctrl+V).

Image will appear the same size as you see above.

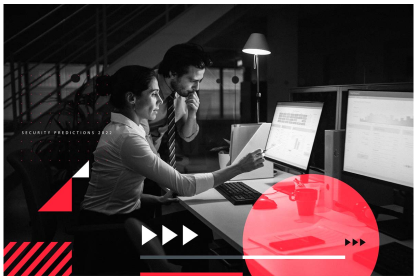
Posted in Cybercrime & Digital Threats, Cryptocurrency, Internet of Things, Bitcoin

2021 Midyear Cybersecurity Report



In the first half of this year, cybersecurity strongholds were surrounded by cybercriminals waiting to pounce at the sight of even the slightest crack in defenses to ravage valuable assets.
View the report

Trend Micro Security Predictions for 2022: Toward a New Momentum



In 2022, decision-makers will have to contend with threats old and new bearing down on the increasingly interconnected and perimeterless environments that define the postpandemic workplace.
View the 2022 Trend Micro Security Predictions