NTT Security

GTIC Monthly Threat Report

August 2018

Contents

NTT Security Observations: Cryptojacking

In August 2018, NTT Security researchers wrapped up part of their analysis into browser-based cryptojacking events, trending events over the past three months.

In this report, researchers outline the most-observed cryptojackers/cryptominers, share data on the industries most impacted by these events, and wrap up with recommendations for protecting network environments from browser-based cryptojacking.

What variants of cryptojackers do we see most?

Nearly 40 percent of the browser-based cryptocurrency mining researchers analyzed was non-descript browser-based mining, not associated with a specific cryptocurrency mining platform. The top three cryptocurrency miners identified were CoinHive, XMRig, and Authedmine, each of which is outlined below.

1.1.1 CoinHive

Based on NTT Security data, CoinHive – or some variation of it – accounts for approximately 55 percent of the cryptominers observed from 1 May through 31 July 2018.

CoinHive is a browser-based cryptocurrency mining service, typically used to mine Monero cryptocurrency. Monero has gained popularity this year due to its virtually untraceable transactions, allowing users (or *attackers*) to maintain a high level of anonymity.

CoinHive mines Monero by leveraging unused computing power of user systems connected to the infected site. While the intention of Coinhive was to 'help' website owners generate revenue through mining, as opposed to relying on ads being published on their sites, the best elements of CoinHive have set it apart as *the* go-to cryptocurrency miner in the cybercriminal space.

1.1.2 XMRig

Data shows that XMRig accounts for approximately 5 percent of the cryptomining activity observed. XMRig is open source software which can be used to mine Monero and CryptoNote. XMRig supports cryptocurrency mining by leveraging power from systems' CPUs, NVIDIA graphics cards and AMD GPUs. These features make XMRig popular as users (both legitimate users, as well as cybercriminals) can install it on any hardware device (including systems running Windows), and easily start mining.

1.1.3 Authedmine

Authedmine (a.k.a., 'Authorized Mining'), can be defined as CoinHive 2.0 or CoinHive with explicit opt-in. Due to an increase in negative attention toward CoinHive as a result of cybercriminals (or uninformed website owners) placing the code on websites and using visitors' system resources to mine cryptocurrency without permission, developers responded by creating a miner which would only run after an explicit opt-in from the user. Data shows that approximately 2 percent of observed cryptomining activity is associated with Authedmine.

In other words, although Authedmine showed as 2 percent of crypto*jacking* detections, researchers would classify this as crypto*mining*, since the user explicitly allowed the activity, while cryptojacking is when an attacker *steals* a system's resources to mine cryptocurrency. It is a subtle, but critically important difference.

It's also important to note here that, while Authedmine events *appeared* to be from users who understood what they were clicking, there is also the distinct possibility, and even likelihood, that a significant number of the users accepted the opt-in without fully understanding what they were agreeing to by clicking.

Top Industries

While nearly every industry was impacted on some scale, data shows the top three industries – education, health care, and finance – comprised around 88 percent of all detections. (See Figure 1.)

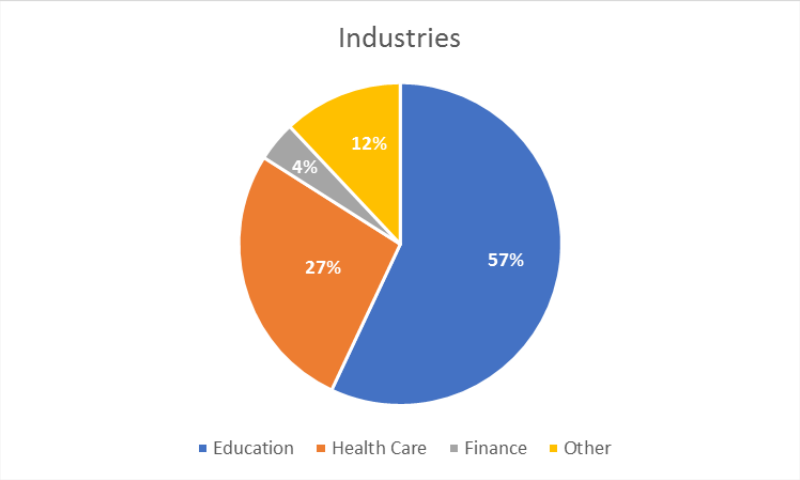


Figure 1. Most affected industries

Recommendations

While completely preventing browser-based cryptocurrency mining or cryptojacking is incredibly difficult, NTT Security recommends following the below guidelines to reduce the risk browser-based cryptojacking can have in your environment:

- Maintain an updated anti-virus (AV) solution on network endpoints. Most endpoint AV solutions will automatically detect browser-based coin mining attempts, and if configured properly, will block those attempts, or block the website altogether.
- Leverage network blocklists. Add domain and host blocklists at the network level (i.e., firewall policies) to prevent communication with known coin mining sites.
- Add browser extensions to detect and block cryptominers. These extensions use cryptominer blacklists or JavaScript executing cryptomining behavior, subsequently blocking the activity.

Rise in Cryptojacking: A Harbinger of Deeper Issues?

Lead Analyst: Danika Blessman

Cryptojacking has recently replaced ransomware as one of the most leveraged tactics of cybercriminals, and it appears these criminals are targeting corporate servers rather than individual users, to spread across a network, potentially garnering a much greater profit.

For all the recent news and increase in activity, cryptojacking malware may be overlooked as a true threat to a system, as it "just eats up a bit of processing power and memory." For the most part, that could be true; an in-browser cryptojacking malware *generally* isn't doing anything truly malicious to your system, other than using resources. In extreme situations, the cryptojacking malware can increase your power consumption (and consequently, your utility bills) and shorten the life of your affected systems.

But it *could* indicate a much greater problem on a system, or even network-wide.

The bigger issue is this: your system has been compromised. You have been breached. This, alone, is indicative of a bigger issue – you're likely vulnerable to other threats. If hackers can install this type of malware, there is a greater likelihood that your system isn't properly patched, opening up the possibility of other attackers placing keyloggers or ransomware on your system or network.

Another larger threat that could be overlooked are the threats to internet of things (IoT) devices or networks, particularly those related to industrial control systems (ICS). Sure, a laptop or Android device might just overheat as its resources are used, but this same effect could be disastrous to a system on an ICS network which controls a water treatment facility, for instance.

Frighteningly, many system users infected with cryptojacking malware aren't even aware this mining is occurring in the background on their system.

Discovering cryptojacking malware in your organization's network is a telltale sign that attackers have been present in your network. It could also mean those attackers are still present or that there may be additional vulnerable entry points.

To harden networks against this type of malware, as well as possible further attacks, take the following actions:

- Ensure your organization is leveraging a defense-in-depth strategy.
- Staying as up-to-date as possible with software patches for the systems in your environment.
- Consider monitoring CPU utilization to increase the likelihood you can successfully identify a cryptojacking infection, short of any other indicators.

References

Why Cryptojacking Malware May Be a Sign of More Serious Intrusion
Cryptojacking Displaces Ransomware As Most Popular Cyberthreat
How Cryptojacking Can Corrupt the Internet of Things

Software Supply Chain Attacks are the "New" Ransomware!

Lead Analyst: Danika Blessman

Though perhaps not as highly considered in a threat assessment as a "standard" threat such as ransomware, supply chain attacks – especially via the software supply chain – are becoming a common and effective method of gaining access to a threat actor's target.

In fact, software supply chain attacks have increased in frequency over the past 12 months, as virtually *every* organization depends on third-party software for its operations. These types of attacks present an incredible challenge to an organization's security endeavors since vulnerabilities in many of these software programs are difficult to detect. Additionally, many organizations simply *trust* their vendors are providing secure software.

Interestingly, while 90 percent of respondents in a recent survey answered that a software supply chain attack resulted in, on average, a financial cost of $1.1 million, only 71 percent of the same respondents held those in their supply chain to the same security standards as for their own company.

The U.S. government has recently said not to allow software from various vendors believed to have affiliations with nation-state actors within Russia, Iran and China. The U.S. government forbids this software from being installed or used in government networks. And, perhaps, rightly so.

Another notable – and successful – infiltration of the software supply chain was an operation dubbed Kingslayer, which targeted *sysadmin* accounts associated with U.S. firms to steal login credentials. The ultimate purpose of this campaign was to break into a targeted host and replace a legitimate application with a malicious version containing a backdoor. This backdoor could then be used to maintain persistent access, exfiltrate targeted data, or upload additional malware. Security researchers continue analyzing the total number of organizations impacted by this campaign.

And lest we forget CCleaner, which targeted 18 specific companies but infected *2.2 million* CCleaner customers worldwide, showing the targets of attackers are not the only ones who need to worry.

Attacks against an organization's software supply chain is a real threat which clearly warrants attention, perhaps more than it is receiving at this point, as attackers are using this effective method for a wide range of results – everything from cyber espionage and financial theft to the disruption of an organization's operations.

Imagine the access a threat actor could have to your environment if they were able to replace one of your common tools or office applications with their own malevolent version. Would you even know?

While this is a challenging problem, you *can* take steps to help strengthen your cybersecurity posture.

- Ensure your organization has a comprehensive, defense-in-depth security strategy in place as threats morph from one to another.
- Ensure you include your supply chain in your security strategy, holding your vendors to the same security standard your hold your own organization.
- Implement threat intelligence into to help your organization understand and mitigate a variety of threats.

References

Software supply chain attacks: preventing and mitigating "the next ransomware"
Securing the supply chain
NCSC Releases 2018 Foreign Economic Espionage in Cyberspace Report
Kingslayer – A Supply Chain Attack

Governing the Internet of Everything

Lead Analyst: Aaron Perkins

In an article titled, “Have You Updated your Toaster?”, soon to be published in the European Journal of International Law, researchers propose a set of cybersecurity standards established by international organizations, national governments, and industry.

It is no secret that the internet was not designed with security as a primary consideration, and with new IoT devices connecting to the internet every single day, there is no question that, to properly secure network environments, a global set of standards should be established.

With no security built-in to the network (internet) on which these IoT devices operate, as researchers point out, “security is left to the devices connected to the network.” Vendors have been slow to understand (and accept) their responsibility for building security *into* their devices, and as a result, the responsibility for securing these devices has fallen to the users. The catch is that a significant number of these devices are not being managed effectively by those users.

While a global set of cybersecurity standards will not prevent *all* attacks, it will go a long way to help organizations around the globe combat not only ‘lone wolf’ hackers, but also nation-state sponsored attacks.

In the article, researchers argue for “a polycentric approach to boosting IoT security.” While the U.S. has opted for a more voluntary, or industry-specific, set of standards for both cybersecurity, as well as data privacy, the European Union (EU) has taken a much more comprehensive approach, implementing the sweeping General Data Protection Regulation (GDPR), affecting organizations inside the EU, as well as firms located outside the EU, but that do business with those inside.

A key element to understand is that, for the EU, a big part of how the region will shape internet governance is through the GDPR, an extension of the EU’s long-held efforts to create a Digital Single Market (DSM). While the GDPR has received press coverage primarily for the fines associated with

organizations not complying with GDPR data privacy regulations, one of the crucial goals of the GDPR is to move toward a single EU market, with one, blanket set of cybersecurity standards.

In other words, the EU is well on its way toward providing more security to the internet in general, with IoT devices directly impacted by the GDPR.

Conceptualizing what internet security *should be* is no easy task, but one method is to consider cybersecurity policy in terms of *polycentric governance*. According to researchers, the polycentric governance framework can "be considered to be a multi-level, multi-purpose, multi-functional, and multi-sectoral model." In other words, organizations at all levels, both public and private, play key roles in solidifying this framework.

NTT Security analysts assess that blockchain technology could potentially play a critical role in next-level cybersecurity, as the polycentric governance model could be built on the blockchain, with checks and balances implemented to ensure that every device connected to the internet meets or exceeds security standards.

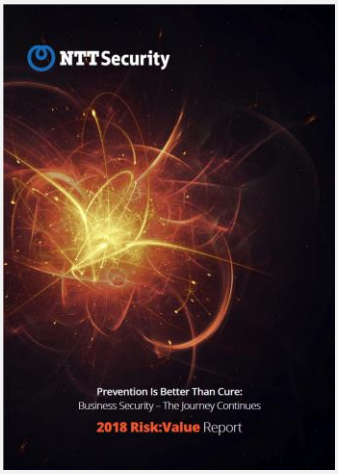
The polycentric approach to cybersecurity essentially has two "strategic paths" forward. The first path is to better refine how we view "due diligence" within cybersecurity. In other words, both public and private firms, at each step along the way – development, the supply chain, delivery, connection to the internet – are responsible for ensuring the device meets or exceeds cybersecurity standards.

The second path is to shift the public mindset surrounding cybersecurity, enabling firms to view security implementation measures as a form of corporate social responsibility. This path has the greatest potential to create a more sustainable internet environment as IoT devices connected to the internet look to outnumber the entire human population 3-to-1 by 2020.

References

Article: Have You Updated Your Toaster? Transatlantic Approaches to Governing the Internet of Everything
Report: The Zettabyte Era: Trends and Analysis

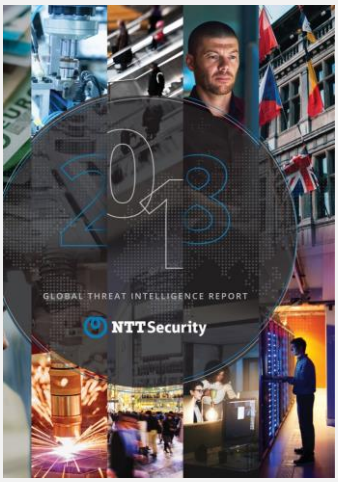
NTT Security Annual Reports



Risk:Value 2018

Many organizations are stuck in a reactive mindset when it comes to information security and would opt to pay a hacker's ransom rather than proactively invest in security. That's a key finding in this year's Risk:Value 2018 Report.

Download your copy today!



2018 Global Threat Intelligence Report

This year's report summarizes activity we detected in over 6.1 trillion+ logs and more than 150 million+ attacks, along with vulnerability scans, incident response engagements, and diverse findings from threat research and threat intelligence teams across NTT Security.

Download your copy today!

About GTIC

The NTT Security GTIC protects and informs NTT Group clients through security threat research, vulnerability analysis and the development of effective countermeasures. For more information, including vulnerability disclosures, threat reports and white papers, visit the resource page on www.nttsecurity.com or our blog.