NTT Security

GTIC Monthly Threat Report

December 2017

Contents

NTT Security

Preliminary GTIC Analysis into Coinhive

Coinhive is an organization which offers a JavaScript (JS) based miner for Monero (XMR), a cryptocurrency built on the same technology as Bitcoin. The Coinhive script is meant to be embedded into a website where site visitors directly mine for Monero from their browser for the website's owner.

On the surface, this looks promising for the user. The website leverages the user's system resources to silently mine XMR in the background for the website's owner, and in return, receives incentives such as:

- An ad-free website
- Additional video streaming time
- Free files to download, such as e-books
- Credit for in-game money or items in an online game

The last incentive, "Credit for in-game money or items in an online game" is an outstanding perk, especially for those who enjoy mobile gaming but are unwilling to spend money in-game to progress within the game.

In a sense, Coinhive seems like a great alternative to gathering users' contact information, spamming users with intrusive ads, or requesting users create an account.

The NTT Security Global Threat Intelligence Center (GTIC) took a deeper look into coin mining threats, and, although Coinhive is not currently categorized as a "threat", additional research was warranted as a natural first step.

One global organization in the food service industry is reported to be "unexpectedly" running the miners. And, although it is currently unknown as to how many websites are currently affected by the Coinhive application, GTIC research analysts continue to investigate potential other coin mining operations being leveraged on these websites.

Using the string '*coinhive.min.js*', GTIC researchers queried publicwww's API for data, in which researchers identified nearly 38,000 websites with the embedded JavaScript code.

Taking this list of domains, researchers performed *nslookups* for every domain to correlate the IP addresses on which the websites were being hosted.

Next, the GTIC performed geolocation lookups on each IP address, mapping host countries and Internet Service Providers (ISPs), then identified the top-level domains (TLDs).

This data revealed some unexpected findings. For example, Germany and the United States have the highest numbers of IPs hosting websites with the embedded Coinhive JS as shown in the heat map in Figure 1.

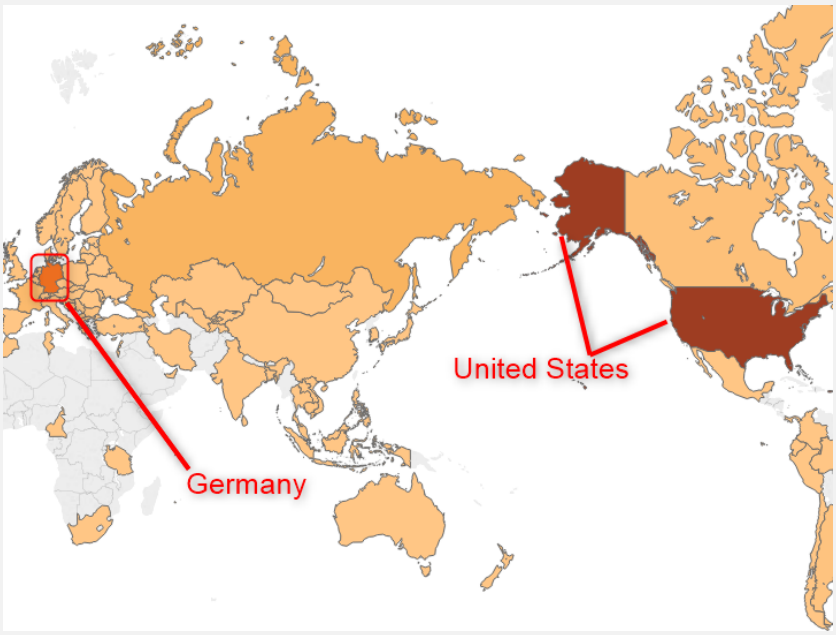

Figure 1. Coinhive website installations

The data also showed a large amount of *regex* [0-9a-Z]{5}.cn[.]com websites being hosted only by Amazon Technologies Inc. Of interest here is that all of these sites are hosted in the United States, were created in 1996, and were recently updated in 2017. Specifically, nearly 3,200 domains which matched the previously stated *regex* were hosted by Amazon and contained coinhive.min.js code in their webpages.

Although the intentions of Coinhive are not malicious, researchers assess it will likely be abused, either by ISPs or threat actors who scan the internet for a specific vulnerability or vulnerable server and inject the code into the page.

A complete list of these domains can be found at this Pastebin site. GTIC is actively researching higher-risk coin mining activities, and plans to publish this research once completed.

Continued Threat of Intellectual Property Theft from Suspected Iranian Hackers

Iranian threat actors, suspected to be affiliated with the Iranian government or military, have recently been active in targeting intellectual property (IP) theft globally. Researchers find this activity interesting, as historically, it has been more common for Iranian threat actors to target perceived adversaries in the oil and gas industry, primarily those in Saudi Arabia and Qatar.

In the wake of a recent attack on a cable network where an Iranian hacker was charged with hacking into the organization and stealing episodes of a popular show, security researchers continue to observe Iranian hackers with suspected ties to the Iranian government targeting Western IP. The Iranian hacker was subsequently indicted, potentially leading to organizations in the private sector beginning to take this threat more seriously. Iran has successfully used oblique methods to bypass current technology embargos. One of these methods, as evidenced in previous attacks, is to create and/or use front companies as a part of their acquisition chain.

Iranian threat actors are typically, and historically, known for retaliatory attacks – not only against oil and gas industry leaders like Saudi Aramco, but against perceived injustices by Western 'adversaries' – such as the attacks against a large casion and Operation Ababil. It appears that now, to bypass sanctions, Iranian actors are increasing their use of tactics, techniques and procedures (TTPs) such as ransomware to fund their operations and supplement funds lost as a result of these sanctions.

In previous threat reporting, Iranian actors suspected to be working on behalf of the Iranian government used Netherlands IP addresses as proxies. NTT Security GTIC researchers noted several Netherlands IP addresses targeting NTT Security clients over the past several months. While it is currently unclear if these Netherlands-based IP addresses are being used by Iranian actors, the GTIC continues to research this activity.

References

Iran targeting international IP for theft and extortion
Saudi Aramco Attack
Casino Attack
Operation Ababil

Iranian State-Sponsored Actors Targeting Critical Infrastructure Networks

APT34, an advanced persistent threat actor suspected to have ties with the Iranian government, is now being reported as targeting critical infrastructure networks.

Targeting critical infrastructure – particularly in the energy industry – is not new for Iranian actors. In fact, this is one of their primary objectives, especially given the sanctions impeding one of their principal means of state income – oil.

It seems that Iranian state-sponsored actors have recently opted for more proactive operations to achieve their goals than the reactionary model. Some operations appear to be driven by vengeance (e.g., Operation Ababil; recent casino attacks), and threat actors are trending toward seeking specific impacts, as opposed to selecting targets of opportunity.

Like other threat actors, Iranian actors still take advantage of recently released exploits, relying on the lack of urgency with which these vulnerabilities are patched. But security researchers have recently observed Iranian actors developing and employing homegrown malware, including the espionage-

focused MacDownloader malware targeting U.S. defense contractors running MacOS-enabled machines. This indicates a growing level of sophistication and, possibly, funding or assistance from outside sources.

These new tactics demonstrate a clear evolution of APT34's capabilities and doctrine, and although they have come to light only recently, NTT Security analysts assess that APT34 will continue to develop their capabilities, and Iran will climb the *attack source* charts in the coming months.

References

Iranian Hackers Have Been Infiltrating Critical Infrastructure Companies
APT34 Targeting Critical Infrastructure
APTs Targeting Energy Sector
APT34 Leveraging New Exploits
Iranian Hackers Build New MacOS Malware

North Korea Gains New Tool for Use in Cyberattacks

On December 21, the US-CERT released malware analysis report (MAR) MAR-10135536-B. This report detailed a joint analysis by the U.S. Department of Homeland Security (DHS) and U.S. Federal Bureau of Investigation (FBI) on a new Trojan variant titled BANKSHOT. This malware is supposedly used by the North Korean government advanced persistent threat (APT), HIDDEN COBRA.

HIDDEN COBRA (a.k.a., Lazarus Group) is a highly-sophisticated cybercriminal organization suspected to operate in the interest of the North Korean government. The group's targets of interest are organizations in the manufacturing, finance, and media sectors, with the bulk of attacks targeting organizations in the finance industry. BANKSHOT malware consists of several portable executables (PEs) which can be leveraged against Windows operating systems.

The PEs are remote access tools (RATs), which allow remote attackers to run various commands on the infected system. One of these RATs uses a cipher and the OpenSSL library to add a layer of encryption to communications between the infected system and its command and control (C2) server. Analysis indicates this RAT may have been used to install proxy servers onto compromised systems.

Mitigation and Recommended Action

- Maintain up-to-date anti-virus signatures and engines.
- Restrict users' ability (permissions) to install and run unwanted software applications; restrict admin accounts for only administrative functions.
- Enforce a strong password policy and implement regular password changes.
- Exercise caution when opening email attachments even if the attachment is expected and the sender appears to be known.
- Keep operating system patches up-to-date.
- Enable a personal firewall on agency workstations.
- Disable unnecessary services on agency workstations and servers.

- Scan for (and remove) suspicious email attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file header).
- Monitor users' web browsing habits; restrict access to sites with unfavorable content.
- Exercise caution when using removable media (e.g., USB thumb drives, external drives, CDs, etc.).
- Scan all software downloaded from the internet prior to installing and running the software.
- Maintain situational awareness of the latest threats and implement appropriate access control lists.

References

https://www.us-cert.gov/sites/default/files/publications/MAR-10135536-B_WHITE.PDF
https://www.us-cert.gov/ncas/current-activity/2017/12/21/North-Korean-Malicious-Cyber-Activity

About GTIC

The NTT Security Global Threat Intelligence Center (GTIC) protects and informs NTT Security clients through security threat research, vulnerability analysis and the development of effective countermeasures. For more information, including vulnerability disclosures and threat reports, visit the GTIC page on nttsecurity.com.