Malware Analysis Crypto Miner

Static Analysis

With the rise of the cryptocurrency market the race for mining has become an industry of competitive strategy. With a preestablished limit imposed on each currency, mining for the coins is where the greatest gains and even more so, the greatest threats present themselves. In order to solve these complex problems associated to each block, a computer must crack the cryptographic hashes to receive the authentication key, and in turn is rewarded with a varying amount of value in the specified currency. This process is where we find our vulnerability, whichever device is granted the authentication key is the output gateway to financial gain. This process is reasonable for established groups and corporations who have both the access and finds to produce an environment capable of immense computing power and maintenance, such as temperature control and 24/h network connection. This environment is essential to have a competitively significant financial gain in crypto mining. Moreover, this creates a hierarchy of access to mining, and those unable to produce such an environment instead have developed other means to control the output of the coins. Crypto miner malware and its variants are an active risk and are designed to take over the power and resources from unauthorized devices around the globe to an anonymous pool where is now becomes the soul receiver of the authentication rewards.

The variant of malware being analyzed today titled "Crypto miner" was exploited on the 30th of November 2018 at 23:25:56 and was running for 60s wherein it compromised the target device via an executable file disguised as a .bin file inside the user directory.

Malicious File: eda9d4a5-9117-4b06-8d2b-7618305c7d26.bin

This variant upon analysis was targeting windows 7 professional service pack (build: 7601, 32bit), windows 10 (build 1803, 64bit) and was a multi-layer attack. The behavior when run was rapid and quiet, using both efficient logical scripting and undetectable reactions based on user interaction. On the application layer of the attack, if task manager was run the malicious executable file was renamed as a Microsoft default process called "svchost.exe", using 89.58% of the CPU recourses. Through the network layer, an IP from the Ukraine (37.1.216.8) was contacted and ".ru" domains such as "stafftest.ru". The host was sending multiple 'GET' requests from html pages

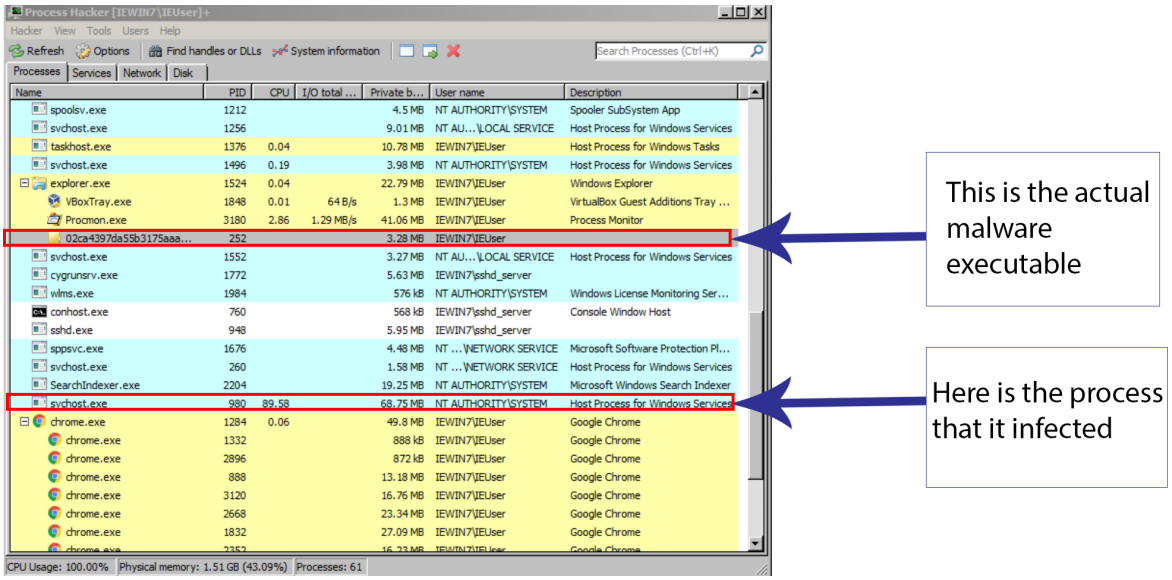
called "test.html" from the established foreign connection. All requests returned a 404 series error, where upon analysis found a common threat within the html container element. Disguised inside the <iFrame> were image src files, when requested ran the hidden executable. Only 2 out of 24 IPs were added to the hacker's pool during this attack resulting in an unknown overall monetary gain.

Dynamic Analysis

We tested this malware using two different methods. The first method we used was any.run's sandbox. The information we received from any.run was a little vague and we wanted to learn more. In order to learn more, we decided to create our own sandbox within VirtualBox. We were able to run the malware securely and watch how it reacted with our system. The information below was deduction from a culmination of our research on any.run and our own personal sandbox.

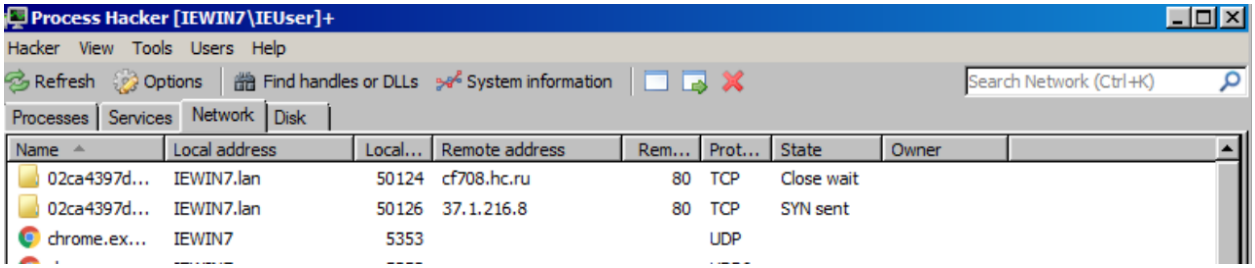
Process Environment

In the case of our crypto miner it runs as the user. Once the file is executed it it infects the svchost.exe process on the user's computer to disguise itself as a regular windows process. Shortly after your system will start to slow down due to the miner using all of your CPU's processing power. Most users will troubleshoot this by opening Windows Task Manager and seeing what process is using all of your systems resources. The user will see that it;s a regular windows process that is using the CPU and not the actual malware file. You can see in the image the executable malware file is not using any CPU but the svchost.exe is.



Network Activity

The malware did make two HTTP requests as you can see in the image below. The request was to connect the victim's system to the "crypto mining pool". A mining pool is a joint group of cryptocurrency miners who combine their computational resources over a network. Individually, participants in a mining pool contribute their processing power toward the effort of finding a block. Once a block is found the users who are part of the pool are rewarded with cryptocurrency. In this case however the group of miners are unaware that they are part of a pool. This results in the attacker receiving the complete reward for finding the block instead of splitting it between the miner.



Once the the request goes out for the domain the DNS server responds with the IP which then opens up the communication.

The following table describes the servers that the sample communicated with.

Request Type	Target Domain	Target IP Address	Reputation
HTTP	http://hrtests.ru/test.html?1	37.1.216.8	Malicious

Filesystem Modifications

There is only one filesystem modification that this particular malware creates, and it is the actual bin.exe file that infects the svchost.exe process

Summary

To summarize this particular crypto miners' goal is to mine as much cryptocurrency as it can using your systems resources. There were many signs that gave a clue to something malicious happening on the computer. The first sign being that the CPU usage went to 100% even though the system was not doing anything strenuous. The second sign was the HTTP request to a malicious web server. This malware also made several changes to the windows registry. All in all, this malware was fairly sophisticated and was very good at covering it's trace.

Containment Strategy

Scope

“CryptoMiner” as a crypto-currency mining malware has many available options for the attack surface, as can be seen by the many variation of “CryptoMiner”. This allows for “CryptoMiner” to be implemented to affect a great many systems. However, with respect to the specific versions of “CryptoMiner” that was observed it can be seen that this malware targets “Windows” operating systems. Specifically, there is a malware version that targets a “Windows 7” operating system (Windows 7 Pro Service Pack 1, Build: 7601 32 bit) and additionally there was an observed malware version that targeted a “Windows 10” operating system (Windows 10 64-bit, version 1803). “CryptoMiner”’s typical targets do not relate very much to the device instead it is more related to the user of the device and the operating system used. The reasons for that is “CryptoMiner” needs to be on one of the two previously mentioned versions of the “Windows” operating system for it to run, and additionally the start process of “CryptoMiner” needs the users input to start. Specifically, it requires the user to run an executable file that has been previously downloaded either through a phishing email file, or a website with a fake download in which the user double clicks to run the file.

Severity

“CryptoMiner”’s severity comes mainly in the form of CPU usage however this is the general aspect of “CryptoMiner”. With respect to the CPU usage this aspect of damage can vary from person to person however for a typical user device this CPU redirection is a middle to high level issue. Beyond just the CPU usage of “CryptoMiner” also gains access to a great number of various important files on the computer. Specifically, there is access to the “C: Drive” of the computer and some of the “Windows” system files in the respective “C Drive”. “CryptoMiner”, in addition to the folder and file access, modifies and changes some of the registry key settings (Internet control settings). The one bright side of “CryptoMiner” is that the initial attacker does not gain direct access to the files it is only the malware itself that holds the access to these files. The difficulty of removal has decreased over time due to the increase in the stability of the anti-viruses. However,

should the malware be installed despite that there is a reasonable amount of work with relation to additional softwires to properly clean and remove “CryptoMiner”.

As such, based on the information above we can conclude that this sample of “CryptoMiner” is of medium to high severity based on the situation, and should be patched, and removed from the system within two to three days.

Solution

For the solution to the “CryptoMiner” malware there are a few outwardly simple steps that are required to take on the computer to properly fix the computer.

1. Terminate the Program and/or Terminate the Internet Connection

The first step of clearing “CryptoMiner” and fixing the system is to stop “CryptoMiner” from running. There are two main methods of doing this the first is using either an anti-virus or an additional program to kill the process that “CryptoMiner” is running in the background. Then the other way which can be much simpler is to simple disconnect the device from the internet. Due to how “CryptoMiner” runs on a “C&C” system disconnecting the device from the network will prevent any information flow to be created and as such prevent “CryptoMiner” from functioning.

2. Scan the Device for Malware

The second step for clearing the malware is to find all of the specific changes that have been done to the system in the form of files and network changes, along with finding the specific malware function. This step can be done in parallel to step three, due to how many anti-viruses now detect “CryptoMiner” and can easily scan and remove the malware. Alternatively, the scan

can be done manually to locate the individual files.

3. Remove Malware from the Device

The third step is to remove the malware from the device similar to step one this can be done using an external program that can remove the malware or alternatively be done simple using the and anti-virus which can detect and remove the malware. This step can also be done manually, however this would increase the difficulty and time required for the malware to be clear.

4. Run Additional Tests to Confirm Removal of Malware and All Related Aspects

After removing the malware, the user should run additional tests to locate and find if there are any other traces of malware, adware, or spyware still located on the computer and then remove them. Additionally, the user should also check for any outdated software that could pose a threat to the system's security.

5. Install Anti-Virus Software to Prevent Future Attacks

Finally, the user should install an anti-virus to ensure that "CryptoMiner" does not get back on to the system. A list of anti-viruses that are known to detect "CryptoMiner" can be found below.

Anti-Virus	Detection	Anti-Virus	Detection
Acronis	Suspicious	Ad-Aware	Trojan.AgentWDCR.HWR
AegisLab	Trojan.Win32.Agentb.tn9n	AhnLab-V3	Trojan/Win32.BitCoinMiner.R230798
Alibaba	Worm:Win32/Agentb.a3d373eb	ALYac	Misc.Riskware.BitCoinMiner
SecureAge APEX	Malicious	Arcabit	Trojan.AgentWDCR.HWR
Avast	Win32:CryptoMiner-Z [Trj]	AVG	Win32:CryptoMiner-Z [Trj]
Avira (no cloud)	TR/BitCoinMiner.fra	Baidu	Win32.HackTool.CoinMiner.a
BitDefender	Trojan.AgentWDCR.HWR	BitDefenderTheta	Gen:Trojan.Heur2.PPBB.3.0.GLW@aq2CtdfiT
Bkav	W32.DotomchASAO.Trojan	CAT-QuickHeal	Risktool.BitCoinMiner.DR9
ClamAV	Win.Malware.Locky-9361	CMC	Trojan.Win32.Agentb!O
Comodo	TrojWare.Win32.CoinMiner.B@6tqin0	Cylance	Unsafe
Cyren	W32/Coinminer.DWZG-8697	DrWeb	Trojan.BtcMine.1214
Emsisoft	Trojan.AgentWDCR.HWR (B)	Endgame	Malicious (high Confidence)
eScan	Trojan.AgentWDCR.HWR	ESET-NODE32	Win32/Crytes.AA
F-Prot	W32/Coinminer.A	F-Secure	Trojan.TR/BitCoinMiner.fra

FireEye	Generic.mg.aba2d86ed17f587e	Fortinet	W32/BitCoinMiner.BXPOTENTIALLYUNSAFE!tr
GData	Win32.Trojan.Agent.ER3HBX	Ikarus	Worm.Win32.Crytes
Jiangmin	RiskTool.BitCoinMiner.ab	K7AntiVirus	Trojan (004e1d801)
K7GW	Trojan (004e1d801)	Kaspersky	Trojan.Win32.Agentb.btdr
Malwarebytes	PUP.Optional.BitCoinMiner	MAX	Malware (ai Score=100)
McAfee	Generic.zn	McAfee-GW-Edition	BehavesLike.Win32.Backdoor.tc
Microsoft	Trojan:Win32/CoinMiner.BB!bit	NANO-Antivirus	Trojan.Win32.DownLoad3.eopqgg
Palo Alto Networks	Generic.ml	Panda	Trj/WLT.C
Qihoo-360	Win32/Trojan.cb4	Rising	Trojan.CoinMiner!1.ACBA (KTSE)
SentinelOne (Static ML)	DFI - Malicious PE	Sophos AV	Troj/Miner-CZ
Sophos ML	Heuristic	SUPERAntiSpyware	Hack.Tool/Gen-BitCoinMiner
Symantec	Trojan.Coinbitminer	TACHYON	Trojan/W32.BitCoinMiner.1578496
TotalDefense	Win32/Tnega.XAUQ!suspicious	Trapmine	Malicious.moderate.ml.score
TrendMicro	WORM_COINMINE.NC	TrendMicro-HouseCall	WORM_COINMINE.NC
VBA32	Trojan.Miner	VIPRE	Trojan.Win32.Generic!BT

ViRobot	Trojan.Win32.S.CoinMiner.1578496	Webroot	W32.Bitcoinminer
Yandex	Trojan.Miner!8na/85u4hbs	Zillya	Trojan.Black.Win32.46302
ZoneAlarm by Check Point	Trojan.Win32.Agentb.btdr	Zoner	Trojan.Win32.44850

Awareness Training

When individuals encounter Cryptominer malware, one must follow the necessary steps to contain the infection. Significant things to consider are how to detect, isolate and protect data against an infection.

Symantec explains that there are three different ways malware can infect a computer network: either a worm, virus, or Trojan [4]. As shown in our behavioural analysis the Cryptominer malware utilizes CPU cycles to mine bitcoin. This mining software may run in the background on an operating system or even as JavaScript in a web browser [2]. Thus, it becomes difficult to identify an attack that is so discrete.

A crypt mining malware infection can be identified by abnormal server behaviour such as strange ads, pop-up windows, unwanted changes to one's browser and homepage [4]. In addition to this, slower server and sudden lack of storage space can be sign of malware [4]. High CPU usage is also common when a miner executable is running and is dangerous because one cannot identify performance degradation at the initial stage of an attack [4].

Once an infection is detected, it needs to be isolated and contained. This ensures that other data is protected thereby minimizing the damage to a network. Anti-virus software is common for malware protection. Some of the most efficient software come from companies such as Kaspersk Lab, Symantec and Trend Micro [4].

Furthermore, the final step when encountering a crypto mining malware infection involves quarantine and response. Certain preventative measures include keeping all systems patched and updated, keeping an inventory of hardware so one is aware of what needs to be protected against a future attack and performing continuous vulnerability assessments on infrastructure. After the necessary steps are followed to protect as much data as possible, the SOC team should be notified with an IP address, browser history and CPU usage [1].

Bibliography

Any.Run. (2018, November 30). Retrieved from Any.Run: https://app.any.run/tasks/eda9d4a5-9117-4b06-8d2b-7618305c7d26/

Bonderud, Douglas. “New Glupteba Malware Backtracks Bitcoin, Cashes in C&C Server Updates.” Security Intelligence, 2019, securityintelligence.com/news/new-glupteba-malware-backtracks-bitcoin-cashes-in-cc-server-updates/.

Belding, Greg. “Threat Hunting for URLs as an IoC.” *Infosec Resources,* https://resources.infosecinstitute.com/category/enterprise/threat-hunting/iocs-and-artifacts/threat-hunting-for-urls-as-an-ioc/#gref [3]

Channel, T. P. (2017, September 22). Bitcoin Miner Malware | Incredibly Stealthy! Youtube. Retrieved from https://www.youtube.com/watch?v=CqXA0B84Hr8

cisecurity, CIS. “Top 10 Malware June 2018.” CIS, 18 Sept. 2019, www.cisecurity.org/blog/top-10-malware-june-2018/.

Detection, VirusTotal. “Virus Total.” VirusTotal, 2018, www.virustotal.com/gui/file/807126cbae47c03c99590d081b82d5761e0b9c57a92736fc8516cf41bc564a7d/community.

Frankenfield, J. (2019, November 10). Mining Pool. Retrieved from Investopedia: https://www.investopedia.com/terms/m/mining-pool.asp

Fruhlinger, Josh. “Malware Explained: Definition, Examples, Detection and Recovery.” *CSO Online, CSO,* 17 May 2019, https://www.csoonline.com/article/3295877/what-is-malware-viruses-worms-trojans-and-beyond.html [4]

Gartner, Inc. “Best Endpoint Protection Platforms of 2018 as Reviewed by Customers.” *Gartner,* Nov. 2018, https://www.gartner.com/reviews/customers-choice/endpoint-protection-platforms [5]

Hardy, Colin, director. Adylkuzz CryptoMiner - A Quick Behavioural Analysis. YouTube, YouTube, 2017, www.youtube.com/watch?v=-T0SjvIo910.

LLC, Joe Security. “Executive Analysis.” Automated Malware Analysis Executive Report for 02ca4397da55b3175aaa1ad2c99981e792f66151.Bin - Generated by Joe Sandbox, Joe Sandbox, 2018, https://www.joesandbox.com/analysis/189339/0/executive

Sandbox, Joe. Analysis Report Photo.scr. Joe Sandbox, 2018, pp. 1–25, Analysis Report Photo.scr, https://www.joesandbox.com/analysis/189339/0/pdf

Stroud, Forrest. “Cryptomining Malware.” *What Is Cryptomining Malware? Webopedia Definition,* 2019, https://www.webopedia.com/TERM/C/cryptomining-malware.html [2]

Souppaya, Murugiah. “Guide to Malware Incident Prevention and Handling for Desktops and Laptops.” *NIST Special Publication 800-83 Revision 1*, National Institute of Standards and Technology, July 2013, nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf.

"Top 10 Cryptomining Malware." *VERSA Networks,* VERSA Networks, 2018,https://www.versa-networks.com/wp-content/uploads/2018/12/versa-sr-topcryptomining2018-final.pdf [1]

virus removal, bleepingcomputer. "Remove the Photo.scr Monero Miner." BleepingComputer, 2017, www.bleepingcomputer.com/virus-removal/remove-the-photo.scr-monero-miner.