Blocking Cryptocurrency Mining Using Cisco Security Products

PREPARED BY ALEX MCDONNELL WITH CONTRIBUTIONS FROM NICHOLAS MAVIS, SPENSER REINHARDT, JOSH REYNOLDS AND ALAN SMITH.

EDITING BY NICK BIASINI, WARREN MERCER AND JONATHAN MUNSHAW.

Updated July 20, 2018

TALOS

Blocking Cryptocurrency Mining Using Cisco Security Products

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Cisco Talos has observed a shift in malicious activity in recent months, with threat actors changing their focus from the distribution of ransomware to the far safer and more reliable deploying of cryptocurrency miners. The tactical reasons for the shift have been discussed previously on the Talos blog. In this paper, Talos' Detection Response Group will discuss the means of detection and prevention that have been established to mitigate this threat using Cisco's security solutions.

Cryptocurrency mining efforts must employ large amounts of computing resources solving the mathematical problems involved in generating cryptocurrency to be lucrative. The malicious actors we are discussing here target computing resources belonging to other people — devices in a variety of home, office, industrial or corporate settings. These efforts represent — at best — the theft of resources in the form of computing power and a potential vector for further exploitation of the network. To be successful in hijacking these resources, such actors use many of the same techniques they employed to distribute ransomware, such as spam campaigns, exploit kits, and directly via exploitation.

This paper presents how Talos is leveraging our superior visibility and the unique position and capabilities of Cisco's security solutions to identify, prevent, and remediate cryptomining infections in our customers' environments.

See the threat once, block it everywhere.

1. TALOS ASSESSMENT TEAM

1.1. Cisco's suite of security products gives our customers powerful tools to use many solutions to block threats to their networks. We can share visibility and threat intelligence across multiple products and vectors. Email vectors translate to blocks in email and endpoint products like Cisco Advanced Malware Protection (AMP) and the other solutions. Blocking cryptomining in one place translates to the blocking of mining across all of Cisco's security offerings. This reduces the overall time to detection.

Cryptocurrency mining has become one of the favorite tools of criminal actors to make money using the computational resources a large company has to offer. This whitepaper aims to explain the techniques and vectors of cryptomining and illustrate the different ways that Cisco Security and Talos can put a stop to cryptomining on your network.

2. CRYPTOCURRENCY MINING

2.1. WHAT IS CRYPTOCURRENCY?

Cryptocurrency is a digital asset designed to work as a medium of exchange that uses cryptography to secure its transactions, control the creation of additional units, and verify the transfer of assets. Some cryptocurrencies have a limit on how many coins can be produced, and

an increasing amount of work is required to produce the same number of coins. Take Bitcoin, for example. Bitcoin halves the reward for adding a block every 210,000 blocks (approximately every four years). Eventually, that limit will reach zero, and the limit of 21 million bitcoins will be hit. This limit creates an increased demand for computing resources to mine these currencies. Other currencies like Monero pride themselves on anonymity, and that makes them very attractive to cybercriminals.

2.2. WHAT IS CRYPTOCURRENCY MINING?

Cryptocurrency mining is the act of utilizing computer resources to solve complex mathematical problems to prove work performed to other users of the currency and verify transactions throughout the blockchain. In some instances, there is a block reward that a successful miner will get as a means of incentive for verifying, and thus helping secure the validity of the blockchain.

Hardware utilized to mine cryptocurrency varies greatly depending on the individual algorithms used to mine a given currency. Current algorithms focus efforts around whether they wish to be solved the fastest with the graphical processing unit (GPU) or specialized processors, or whether they attempt to restrict potential workers across hardware platforms, giving CPU miners a realistic attempt at solutions in similar time. The myriad of available cryptocurrencies results in a significant number of algorithms being utilized. The deciding factors for these algorithms can be based upon the barrier to entry for individuals to become part of the mining community for that currency. The resulting primary ideas usually begin around proof-of-work or proof-of-stake selection. Some algorithms, such as CryptoNight, used by Monero (XMR), may attempt to control the use of specialized hardware, such as ASICs.

The ever-increasing difficulty of mining cryptocurrency has led to various issues like a worldwide shortage of GPUs. It's also led to the establishment of currency mining farms to increase efficiency and outpace the cost of the electricity needed to run the hardware. The impact is evident, as the price of GPUs and other hardware used for mining will fluctuate with the valuations of the largest cryptocurrencies.

2.3. HOW DOES THIS AFFECT CUSTOMERS?

Malware is constantly evolving. Various malware families have been known to steal credentials, or turn machines into zombies to perform distributed denial of service (DDoS) attacks. More recently, malware has been used more directly to hold the machine hostage with the rise of ransomware. The high-profile outbreaks of 2017 are perfect examples of this. In addition to the success of ransomware, there was also a resurgence of worm behavior, whereby machines infect other machines in the same network segment. This uptick was due not only to zero-day exploits of Microsoft software but also use of conventional and legitimate system administration tools such as PsExec used by the Microsoft Windows operating system.

Malware authors who were successful at spreading ransomware previously took notice of the relatively large number of corporate machines that could be quickly and easily infected. Ransomware is immediately detected by its very nature since it usually adopts a scorched-earth mentality. Malware authors realized that with a potentially large pool of corporate resources (especially during non-work hours) cryptocurrency could be very lucrative. In addition, anonymous cryptocurrencies like Monero and browser-based miners like Coinhive could provide ease of access and increased anonymity for their activities. As such, we are now experiencing a wave of cryptocurrency mining malware (see figure 1 on the next page).

2.4. WHY DO WE CONSIDER IT MALICIOUS?

Mining presents a unique threat to organizations not only in resource usage but also the potential for further lateral movement and data exfiltration. At a most basic level, hardware used for mining effectively has CPU or GPU resources for other legitimate processing power stolen to mine currency. Most cryptocurrency mining in organizations will focus on CPU-bound algorithms such as CryptoNight. Current cryptocurrency mining trends fall into several categories, which range from the intended installation by legitimate users, web mining in place of ads, and malicious actors exploiting systems to mine.

Internal users may identify seemingly available systems in corporations and utilize them for mining cryptocurrency. Installing a mining program on most systems today requires little more than standard user access rights and access to pooling services to perform work.

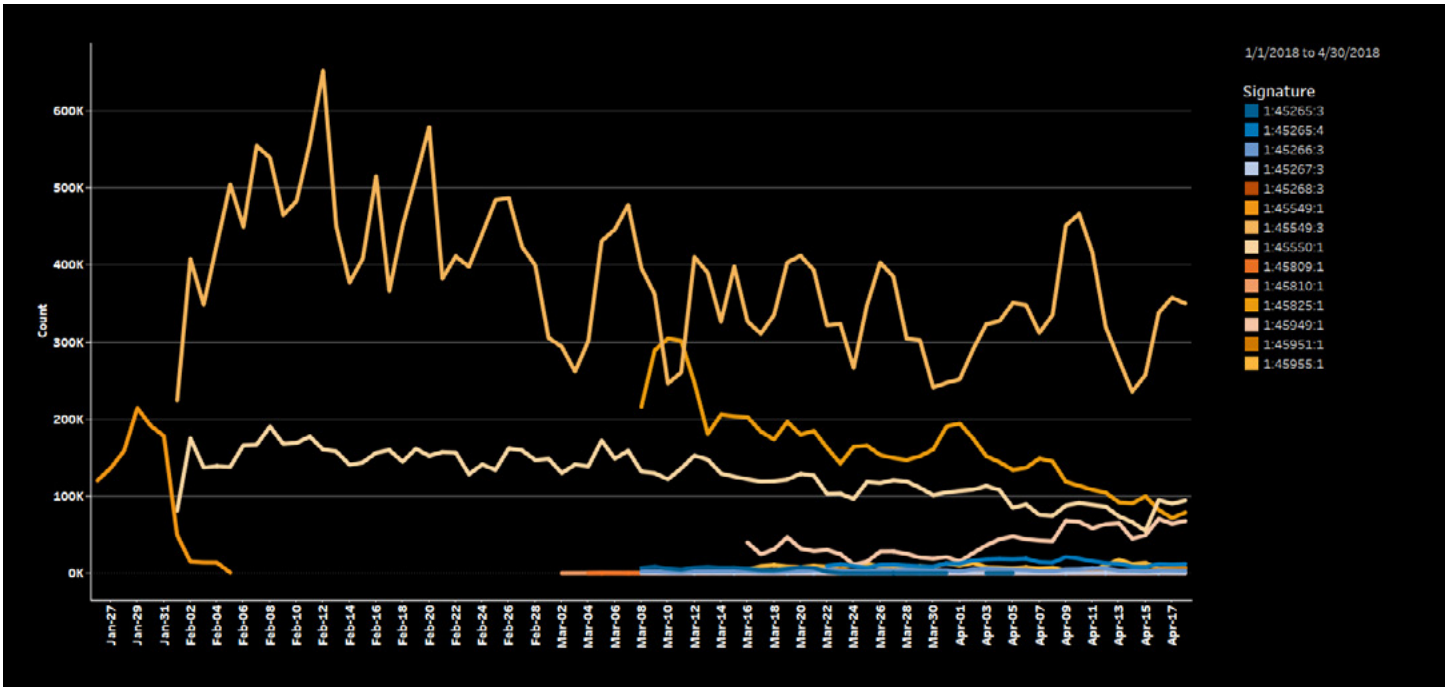

Fig 1. Cryptomining SID alerts in the past quarter.

2.5. WHY CAN'T WE TAKE THEM DOWN?

Websites looking to avoid common ad services are also turning to cryptocurrency mining through JavaScript and WebAssembly. This presents an interesting issue, as end users rarely have any knowledge of mining activities happening on their systems, yet network alerts would potentially indicate otherwise. Additionally, web mining systems are finding ways to continue mining activity well beyond the time a user has viewed their page, moving from well-meaning site funding to overtly malicious usage.

One of the standard web-based JavaScript miners, Coinhive, provides infrastructure only, taking a 30 percent commission on potential profit. Without supporting malware authors directly, they profit directly.

3. BLOCKING CRYPTOMINING ON YOUR NETWORK

Cisco Firepower devices approach mining from several network detection perspectives: downloading binary and web clients, mining stratum protocols, and blacklisting domains and SSL certificates. As we consider all mining activity suspicious, binary and web clients that may be intentionally or maliciously downloaded are also convicted.

3.1. SNORT RULES

Snort rules are quite useful in dealing with everything from preventing miners from being downloaded, to blocking mining commands and access to mining pools to the command and control infrastructure of the malware itself.

Snort rules dealing with cryptomining can be broken up into three groups (see figure 2 on the following page):

- Rules blocking incoming clients, including downloads of miners:

  SIDs: *44692-44693, 45265-45268, 45809-45810, 45949-45952, 46365-46366, 46370-46372*

- Malware variants specifically known to mine cryptocurrency on victim networks are classified separately.

  SIDs: *20035, 20057, 26395, 28399, 28410-28411, 29493-29494, 29666, 30551-30552, 31271-31273, 31531-31533, 32013, 33149, 43467-43468, 44895-44899, 45468-45473, 45548, 45826-45827, 46238-46240*

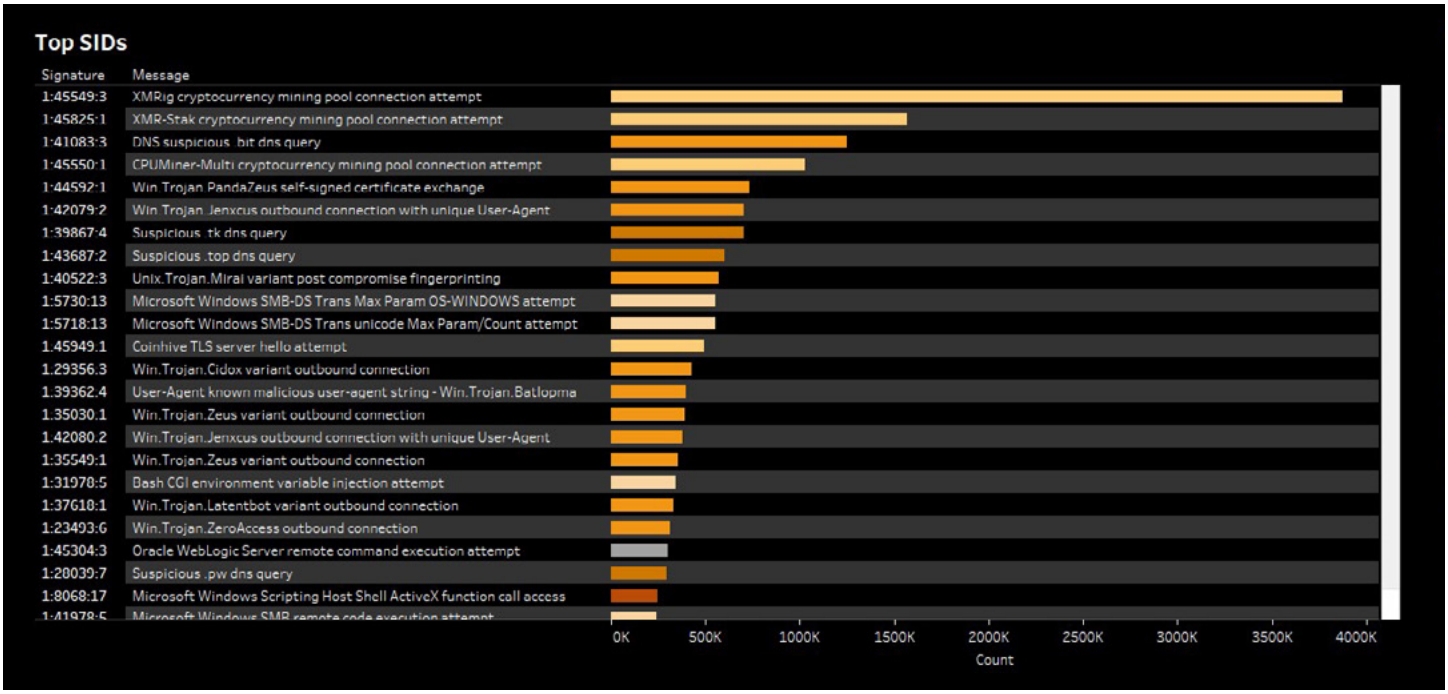

Fig 2. Top alerting Snort rules in the past two weeks.

- Finally, a category identifying common Stratum protocols focuses on identification and blocking of protocols used by cryptocurrency workers:

  ***SIDs:** 26437, 40840-40842, 45417, 45549-45550, 45825, 45955*

3.2. CLAMAV

Last year, when ransomware was extremely common, a new category was added in ClamAV and AMP for signatures to identify malware with ransomware attributes. Likewise this year, with the popularity of cryptocurrency miners in the malware world, the ClamAV "Coinminer" category is now being used by signatures that detect both miners and malware samples that drop miners on infected machines. For example, Multios.Coinminer.XMRig-6496119-0 was recently published.

3.3. ADVANCED MALWARE PROTECTION

3.3.1. Cloud IOC to detect miner

In late 2016, Talos published W32.Cryptocurrencyminer.ioc, a cloud IOC, to the field. The IOC triggers when cryptocurrency miner commands are detected, specifically for bitcoin and Monero. Unlike client-side IOCs, cloud IOCs constantly run to give the fastest results (see figure 3 on the next page for more). It has been updated several times to add more functionality.

Cisco Advanced Malware Protection (AMP) is now using the same "Cryptominer" category as ClamAV so analysts can detect malware and miners accurately for customers. We are looking into the proper labeling of samples detected through automated sandbox runs upon deployment of cryptomining IOCs in Threat Grid and sandbox environments.

The AMP for Endpoints command line capture provides an avenue for identifying miner command line arguments, which can be used to detect malicious or legitimate miners at the endpoint.

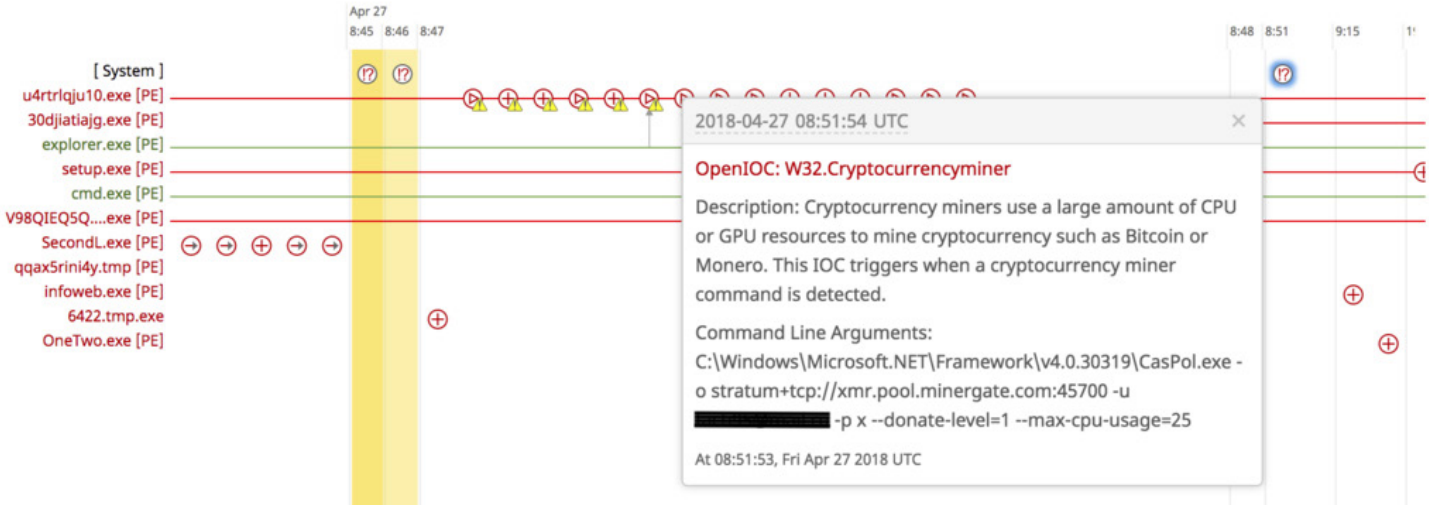

Fig 3. The Talos Cloud IOC alerting. In just the first three months of 2018, these have generated more than 8,000 events.

3.4. BLACKLISTING NETWORK TRAFFIC

We target cryptominer network traffic in two specific ways:

IP, domain. We can block IPs and domains through the use of the Talos Reputation Services, as well as Cisco Web-Based Reputation Scores (WBRS). Many mining sites now rank inside Alexa's top 1 million most popular, a standard list used in whitelisting known legitimate sites, (https://blog.netlab.360.com/file/top_web_mining_sites.txt) and thus ordinarily wouldn't be blocked.

SSL cert blocking. For SSL certificate blocking, we can use either Snort rules or the Firepower SSL certificate blocking feature.

3.4.1. New category for crypto miners in Reputation

Talos is creating a new, non-expiring, reputation category for the Reputation feed. This will be where any cryptomining-related IPs and domains will be entered.

3.4.2. Classification of miner sites/domains under "trading" in WBRS

WBRS has a level 2 category presently that is being used for cryptomining sites. It is called "Trading," and customers can enable it. WBRS is working on implementing a cryptomining-specific category soon.

3.4.3. Ingesting cryptomining to WBRS

The cryptomining Intel feed from Talos will be ingested by WBRS and mapped to a category to be determined until the WBRS cryptomining category is up and running. This means customers will get near simultaneous protection, regardless of which service they are using.

3.4.4. Populating the cryptomining category

Blog posts, open-source research and internal research is currently the best resource for finding regular mining IPs and domains. Automated feeds reporting on malware botnets using their networks will also feed into the category. The Talos Threat Intelligence and Interdiction team has been monitoring the dramatic increase in cryptominer activity since late 2017. They will continue to provide the Talos Detection Response Group (DRG) with indicators derived from multiple sources, including open-source research, telemetry hunting, partner relationships and dark web hunting.

3.4.5. SSL Certificate Blocking

Using Snort, we are blocking SSL certificates used by Monero, CryptoNight, Coinhive, AuthedMine, and other cryptocurrencies.

Blocking Cryptocurrency Mining Using Cisco Security Products

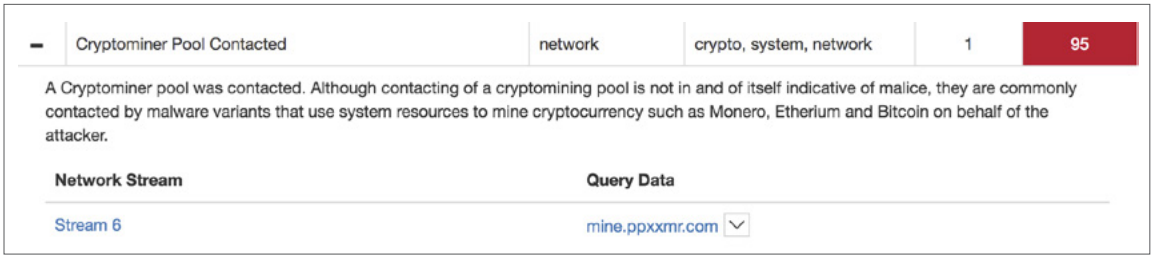

Fig 4. Here, Threat Grid has detected a sample contacting a known mining pool. Mining pools are commonly used by malicious actors to consolidate hash rates to improve chances of mining blocks and to provide funds to their wallets without needing private keys on endpoints.

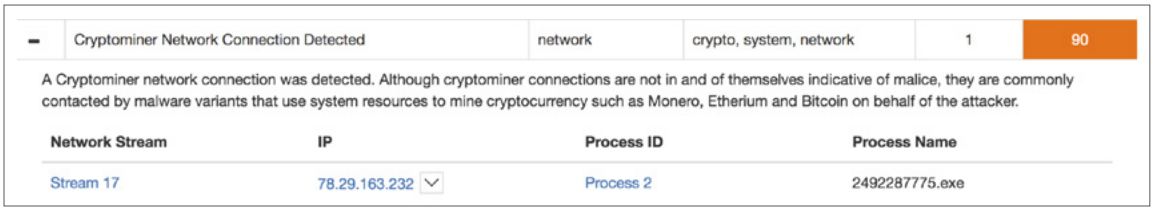

Fig 5. Miners use a common set of ports, which Threat Grid has detected here as being used here.

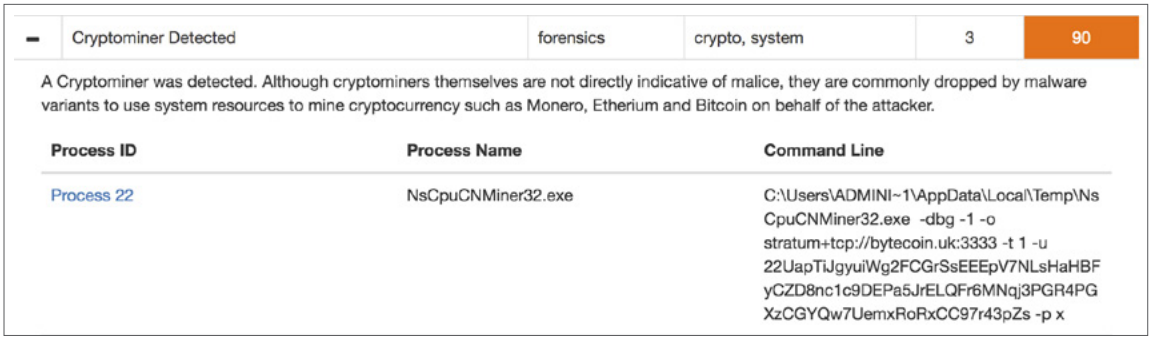

Fig 6. Threat Grid also has the capability to detect miners through their use of command line arguments. Here, you can see a pool domain, port, and cryptocurrency address being supplied as command line arguments to a CPU miner executable.

3.5. SANDBOXING

3.5.1. Threat Grid sandbox

A Cisco acquisition, Threat Grid works closely with Talos to enhance their sandbox to best suit the needs of researchers and respond to new threats and evasions we see. Three Threat Grid IOCs for cryptocurrency exist currently, one that convicts samples and two others that are indicators that will soon also convict samples, as shown in figures 4, 5 and 6 above.

3.5.2. Threat Grid IOC writing

Threat Grid continually develops IOCs to detect new malicious behavior, cryptomining and otherwise, based on research from groups like Talos within Cisco.

3.6. EMAIL REPUTATION

Cisco Email Security Appliances (ESA) products will flag known malware that drops cryptominers using the AMP/ClamAV naming conventions.

4. CURRENT RESEARCH EFFORTS

Talos has ongoing research efforts in the various aspects of cryptocurrency, focusing on tracking mining clients and worker protocols, associated malware activities, and evolutions in mining technology affecting customer systems. These efforts continually feed our threat intelligence and detection platforms through automated processes. They are enhanced as new threats are found.

Malware authors and exploit groups have turned to cryptomining recently for several reasons. Chief among them is the improbability of corporations to pay ransom for systems they can easily restore, and the likelihood that mining activities will go unnoticed outside of normal business hours. Talos is putting additional effort into tracking threat actor groups using cryptocurrency mining, and how their techniques differ from more standard usage.

As stated above, the Talos Threat Intelligence and Interdiction team has been monitoring the dramatic increase in cryptominer activity starting in late 2017. They will continue to provide DRG with indicators derived from multiple sources, including open-source research, telemetry hunting, partner relationships, dark web hunting, and their support for Cisco Security Incident Response Services. Typical aspects of the cryptocurrency miner threat uncovered via these means include malware samples, file hashes, malicious IP addresses, malicious domains, indications of new campaigns, and changes in threat actor tactics.

5. FUTURE EFFORTS

5.1. IOCS FOR SANDBOXES

5.1.1. As more miners come out, we will add IOCs for current detection in the sandboxes that Cisco uses to detect threats as they come in.

5.2. NETWORK IOC ENHANCEMENT FOR AMP

5.2.1. Similarly, we will update our OpenIOCs for AMP to keep them relevant and maintain the “seen once, blocked everywhere” methodology.

6. FURTHER READING

- https://www.investopedia.com/terms/b/bitcoin-mining.asp
- https://blog.talosintelligence.com/2018/02/coinhoarder.html
- https://blog.talosintelligence.com/2018/01/malicious-xmr-mining.html
- https://blog.talosintelligence.com/2018/04/icedid-banking-trojan.html
- https://blog.talosintelligence.com/2017/05/adylkuzz-uiwix-eternalrocks.html
- https://blog.talosintelligence.com/2016/09/tofsee-spam.html