Defending Your Network from Cryptomining

How we defend your network from illicit cryptomining

Block cryptomining threats on the network, in the cloud and at the endpoint

Introduction

Threat actors increasingly look toward illicit cryptomining as an easy source of income. Cryptomining is the production of virtual currency, also known as cryptocurrency, such as Bitcoin and Monero. It comes at the expense of system performance and power consumption. Moreover, threat actors are infiltrating networks to use their victims' computer resources to do this work for them. In this white paper, you will learn how to defend your organization from illicit cryptomining with the Cisco® security portfolio.

Overview

Our Cisco Talos threat research team has been monitoring developments in cryptomining. Their recent research notes that the Monero cryptocurrency saw an increase in value of approximately 3000 percent in the 12 months ending in March 2018. As law enforcement continues to focus more on ransomware attacks, adversaries are looking for alternate ways to monetize their nefarious activity and, increasingly, it's leveraging malicious cryptomining. Therefore, we expect illicit cryptomining to grow in popularity.

Cryptomining is making up an increasingly large portion of the threat landscape, and it is currently growing at an exponential rate. And depending on your industry, you will want to keep the following considerations in mind:

- For financial services, cryptomining by employees, intentional or otherwise, may have securities regulation implications.
- For critical infrastructure, cryptomining is a CPU-intensive process that can adversely affect industrial control systems—resulting in service degradation or outage.
- For all enterprises, data centers and public-facing servers are the types of CPU- and GPU-rich environments that cryptominers covet. Successful intrusions result in degraded performance that may affect the user experience, particularly on public-facing websites where a brand image could also be negatively impacted.
- For all organizations, cryptomining software may be exploited by another party to launch an attack.

Unless cryptomining is a part of your organization's operations, it is advisable to block all cryptomining traffic and remove all cryptomining applications from your network.

By what means are attackers able to infect their victims' systems? By any means they can. The easy profits are worth the effort of the attackers to keep developing new infection methods and techniques. These include:

- Emails with malicious attachments
- Compromised websites that inject code by exploiting browser plug-in vulnerabilities
- Compromised trusted system processes running modified code
- Cryptomining applications using encrypted communications
- Websites that embed JavaScript that allows for cryptomining in the web browser
- Active exploitation of vulnerabilities in server-based applications
- Leveraging vulnerabilities in technologies like Adobe Flash to deliver cryptominers via exploit kits.

Because of the various targets and methods of infection, no single method of protection will address every possibility. An architecture-based approach will provide the most coverage and adaptability.

Our security portfolio detects and blocks threats present in email, network, and web traffic—whether they are within encrypted traffic, malicious files, cloud applications, or roaming endpoints. The results from our ongoing threat research are fed directly into our products. Our threat responses are automated to defend against an ever-evolving threat landscape.

This paper provides additional background on the topics related to cryptomining and how our security portfolio can protect you from these threats.

Introduction: malicious miners and cryptocurrencies

It's hard to avoid the topic of cryptocurrencies these days, particularly after the value run-up in late 2017. During this time some speculators earned millions of dollars, making illicit cryptomining highly attractive. Let's first quickly cover what cryptocurrencies are as well as the associated activities of cryptomining and illicit cryptomining.

Cryptocurrencies

Cryptocurrencies are distributed, virtual currencies that do not have the backing of any central bank or government. Cryptocurrencies use blockchain technology to create a distributed ledger, which makes tampering virtually impossible. Bitcoin is the best-known cryptocurrency, but it's far from being the only one. An attraction of virtual currencies is the ability of users to remain anonymous in financial transactions.

Mining cryptocurrency

A cryptocurrency derives its value, in part, by limiting the number of coins that may ever be created. That creation process is called mining, or cryptomining. In order to mine cryptocurrencies, a miner's computer must solve a mathematical problem so complex that it incurs a penalty in terms of computing resources. The computational effort translates into real power costs for the miner. The logic is that the overhead will limit the number of miners, and therefore, coins will slowly be released over time. But that approach has developed an unexpected flaw.

Because of the rising popularity of cryptocurrencies, the emergence of specialized hardware, and the competition among miners, the cost to mine these currencies cannot be borne by the average user. Cryptomining has now moved into the realm of those that can afford to invest in massive computing power unavailable to most would-be miners.

This development does not mean that smaller players have been dissuaded. The barrier to entry has just meant that unscrupulous miners have had to innovate. Enter pool-based mining.

Pool-based mining

Increasingly, average computers cannot mine enough coin to make it worthwhile. So technologies like pool-based mining have emerged. The idea around pool-based mining is simple: it allows an attacker to pool the resources of multiple systems into a single group for processing power. As the values of cryptocurrency have continued to increase, adversaries have realized they can have users "unknowingly" join these cryptomining pools and generate large amounts of revenue.

Malware, legitimate software, or something in between?

A complication in the hunt for unauthorized cryptomining is that it's not easy to tell when cryptomining software is being used for legitimate purposes or for illegitimate purposes. Cryptomining software does not fit neatly into the malware category. Rather, it is considered a Potentially Unwanted Application (PUA). It is advisable for businesses and government agencies who are not intentionally mining cryptocurrencies to block all such traffic.

Who benefits?

The beneficiaries of illicit cryptomining run the gamut from curious employees who may use their employer-assigned device(s) to run cryptomining software, to criminal organizations wanting to make a quick profit—and even to nation-states circumventing financial restrictions. Regardless of the actor or the actor's motives, unwanted cryptomining creates a vulnerability for its victims.

Who pays?

The victims do, of course. The cost of illicit cryptomining comes through higher energy consumption and degraded system performance for compromised devices. Cryptomining may seem more like a nuisance when compared with destructive malware attacks, but it is important to consider the potential impacts. Overburdened industrial control devices may fail and degrade service delivery, and financial services organizations may suffer regulatory implications, for example.

Think of illicit cryptomining as a parasite that sees benefits as long as its host remains healthy and unaware. Cryptominers profit from the well-being of their victims' networks and want to use as many devices as they can for as long as they can. It's not in their best interest to damage the network or any of the devices running on it. Victims should not expect to experience obvious symptoms like a data loss or system outages as they would in a ransomware attack. Rather, a symptom of cryptomining may be higher energy costs or performance degradation as miners further infiltrate their victims' devices.

How Cisco protects your resources

The network

Pool-based cryptomining relies on the speed and processing power of the network to operate efficiently and effectively. Therefore, the cornerstone to defending against unwanted cryptomining is strong, comprehensive network security.

We perform deep packet inspection, anomaly detection, and NetFlow analysis on network traffic. We utilize sandboxing and malicious file analysis. We analyze traffic in real time and continuously analyze the telemetry we collect to discover previously unknown threats, which we then retroactively remediate. We have developed extensive data models to detect anomalous and malicious behavior, including cryptomining, in encrypted traffic without the need to decrypt that traffic. We see a threat once and protect our customers everywhere.

Email continues to be a popular and effective means of communication, and as such, it's a reliable tool for attackers. Their aim: trick email recipients into visiting a malicious website, opening a malicious attachment, or giving up information.

We block email-based attacks by stripping malicious attachments and by removing malicious links from messages before they can reach the user. Our analysis engine detects advanced evasion techniques, making it that much harder for threat actors to infiltrate your network.

The power of portfolio

Motivated attackers will try every avenue available to them. Your defenses need a wide view of the threat horizon, not a patchwork of keyholes from point products. Consider this: The attacker may start with email phishing, pivot to a web exploit, and then a watering hole attack. Or use all of them simultaneously.

We see a threat once and protect everywhere. It's not enough to just block the attack. Everything we learn about a threat—files, URLs, techniques, traffic patterns, and so on—is shared across our portfolio to defend you from any angle.

The cloud

The Domain Name System (DNS) maps domain names to IP addresses and is a foundational component of the Internet. When you click a link or type a URL, a DNS request initiates the process of connecting you to your destination.

We are one of the largest recursive DNS providers, resolving 125 billion daily requests from 90 million global users. We analyze this massive, diverse telemetry to detect many types of threats and anomalies. Our customers can block outbound traffic based on cryptomining classifications of domains, IPs, URLs, and files. By blocking access to cryptomining infrastructure at the DNS layer, it doesn't matter whether the mining software is run from a browser, a non-web application, or a compromised system utility. That traffic is blocked. The same goes for mobile devices in the field and IoT devices on a network.

Additionally, real-time visibility will help you identify devices and users running cryptomining software within your environment. This ability, especially in identifying previously unknown instances of cryptomining on your network, will greatly assist in your remediation efforts.

A positive consideration for defenders is that threat actors tend to take predictable actions when, say, starting a cryptomining phishing campaign. They typically start by creating and testing their command-and-control infrastructure before launching the campaign. At Cisco, we see that activity. Those domains will be classified as "new domains" while we make a determination of the domains' status over time. Our customers can choose to block traffic to such domains until a determination is reached, which can help to protect the network before the campaign is launched.

The endpoint

All cryptomining attacks eventually make their way to the endpoint, where the prized asset resides: computing resources. Our endpoint security continuously monitors and analyzes file and command-line activity on the endpoint. We correlate disparate events and send alerts when cryptomining activity is detected. Alerts can be triggered by, for example, behavior related to propagation as an attacker tries to move through the network, establishes persistence, and makes outbound connections to the cryptominer's infrastructure.

Cloud-based collective security intelligence works across your security architecture to help contain the spread of cryptomining. We quickly propagate protection from malicious files as soon as we detect cryptomining activity.

Proactive threat hunting services

If you are not sure where to start or suspect you have cryptomining activity on your network, it is best to turn to professionals. Our proactive threat hunting services are performed by a team of incident responders. They employ threat intelligence from Talos, best practices, and a variety of tools to identify unwanted cryptomining activity in your organization.

We will work with you to design a custom hunting plan that will define the scope of the engagement to:

- Identify coverage and gaps in visibility
- Deploy the needed proprietary Cisco technology required for full visibility
- Assess the environment using the latest intelligence
- Analyze the findings
- Provide a final report of both findings and prioritized recommendations

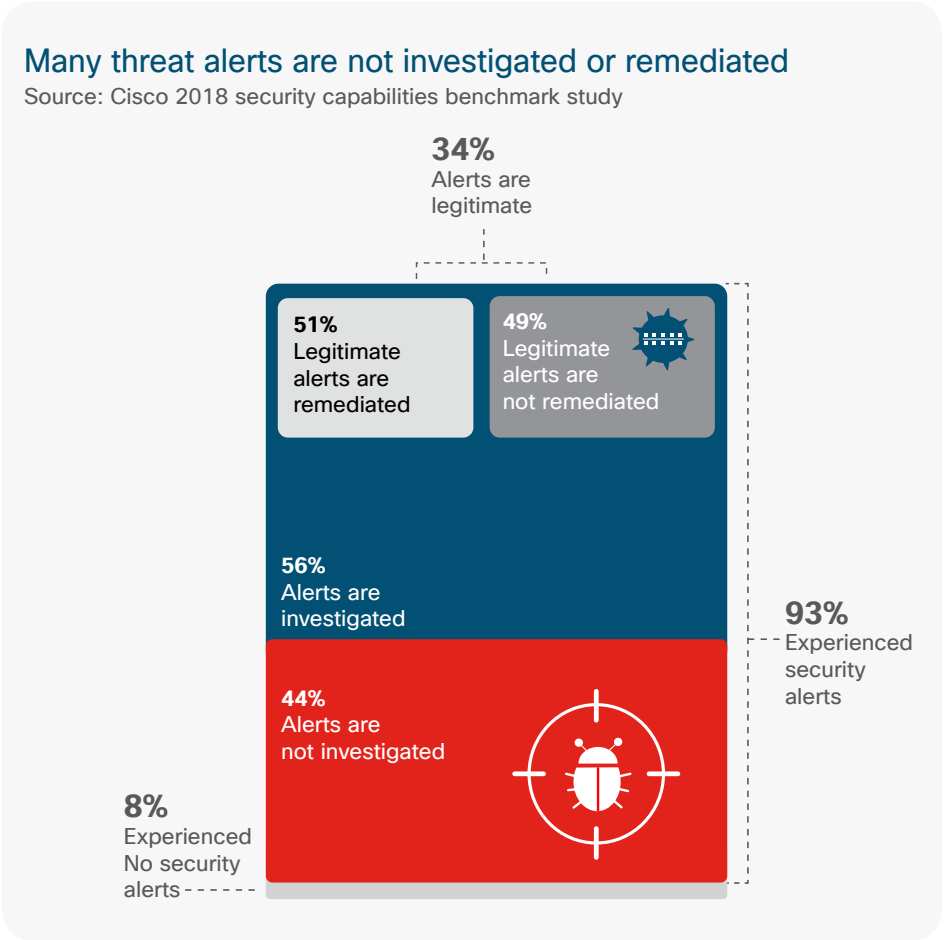
We can also lead or assist in the response to any and all findings during the course of the cryptomining assessment.

The threat intelligence advantage

That attackers continue to evolve their methods and that defenders evolve in response to new threats is a given. But how quickly and efficiently are defenders able to evolve? The root of the question is not one of the abilities of defenders, but of resources, primarily time and talent. First, there just aren't enough security professionals to meet the demand. We project a deficit of about two million security professionals worldwide in just a few years.

Second, defenders face a deluge of information, particularly by a menagerie of point products, to the extent that we found that an average of 44 percent of security alerts are not investigated (see Figure 1). This situation also means that defenders struggle to get to the more interesting or advanced work that is of greater value to their organizations.

Figure 1. Ignored and unremediated security alerts



Now what?

Sign up for a free trial of Cisco Umbrella DNS security at https://signup.umbrella.com/.

Or, just call or email us to speak further, see a demonstration of our capabilities, and learn how we can help you. Defending your organization from evolving threats like cryptomining is a vital part of managing your business, and we'd be happy to help you. Visit us at: https://www.cisco.com/cisco/web/siteassets/contacts/index.html.

We analyze and correlate telemetry across DNS and URLs, network and flow information, files, emails, and cloud applications using automated machine learning and human analysis, reverse engineering, and vulnerability research. We embed researchers with our incident response teams, which allows us to conduct first-person threat analysis and forensics on some of the most high-profile incidents around the world. The output of all of this research is available to you as content within our portfolio, and it is continuously updated and refreshed.

Automated updates and threat responses based on the latest threat intelligence means that you are protected from threats that you weren't aware even existed. Simply said: We see more, so we can do more to protect you.

C11-740602-01 05/18