

THE ANATOMY OF SHADOW MINING

How malicious insiders abuse IT rights to mine cryptocurrency, how is it done, and what organizations can do to protect themselves

EXECUTIVE SUMMARY

Mining cryptocurrency has the potential to be very profitable, but it requires a vast number of high-speed computations run by powerful systems that often need significant amounts of electricity. Because of these infrastructure and energy requirements, malicious insiders have devised various schemes to compromise the IT resources of their organizations, covertly using them for illicit cryptocurrency mining. We call these illicit cryptomining activities “shadow mining.”

Another potential risk is that a hacker may compromise a privileged user and perform the same activity from outside the organization. Not only does shadow mining consume resources and increase utility bills, it also affects the security of an organization’s IT infrastructure.

Consider this scenario: What if system administrators or operational security staff, working for an organization having centrally managed computers, recruited a small amount of computing power from a number of users’ systems to mine cryptocurrency? Could it be achieved using simple automation? And could their effort remain relatively hidden?

The answers to these questions form the hypothesis of Exabeam’s research into the anatomy of shadow mining. In this research paper, we outline tactics insiders could use to abuse their employer’s infrastructure access for the goal of shadow mining. We also review the methods they might use to hide their illicit activities, and we outline what organizations can do to protect their infrastructure and systems from potential shadow mining.

Key findings:

- Incidents of covertly mining cryptocurrency are reported across many industries and appear to be on the rise.
- Techniques employed in shadow mining and the methods of using automation to do it are scaling upwards.
- Shadow mining negatively affects a company’s security posture by increasing its attack surface.
- There are heuristic and statistical methods for detecting shadow mining using host and network data as input data sources.

INTRODUCTION

In 2012 a phenomenon emerged to describe IT infrastructure managed and operated without the knowledge and consent of the organization's IT department. It's called shadow IT and has both positive and negative connotations.

Often, employees may try to work around an IT organization to achieve a business goal, which could be argued as a positive for shadow IT. But as it relates to information security, the connotations are largely negative because operating infrastructure without the knowledge and consent of those who are responsible for defending it creates risks for any organization.

Cryptocurrencies have become a potential money-making opportunity for those willing to experience their wild market value fluctuations. All that's required to purchase cryptocurrency is access to money and basic computer literacy. For those who mine cryptocurrency, only basic system administration skills are required. These can be developed by watching any of the thousands of instructional videos about the topic.

The term shadow mining is a portmanteau combining both shadow IT and illicit cryptocurrency mining. It's the covert, unauthorized use of an organization's computing resources to mine cryptocurrencies by a privileged user to illegally make money.

As Amazon realized when building and launching AWS, its successful web services platform, unused computing resources can be very valuable. Aware of the origins of AWS, individuals may be motivated to put such unused resources to work by covertly mining cryptocurrency. This is especially true at a time when many companies enter into property leases with utilities included, where any additional electricity cost can go unnoticed.

MINING CRYPTOCURRENCY

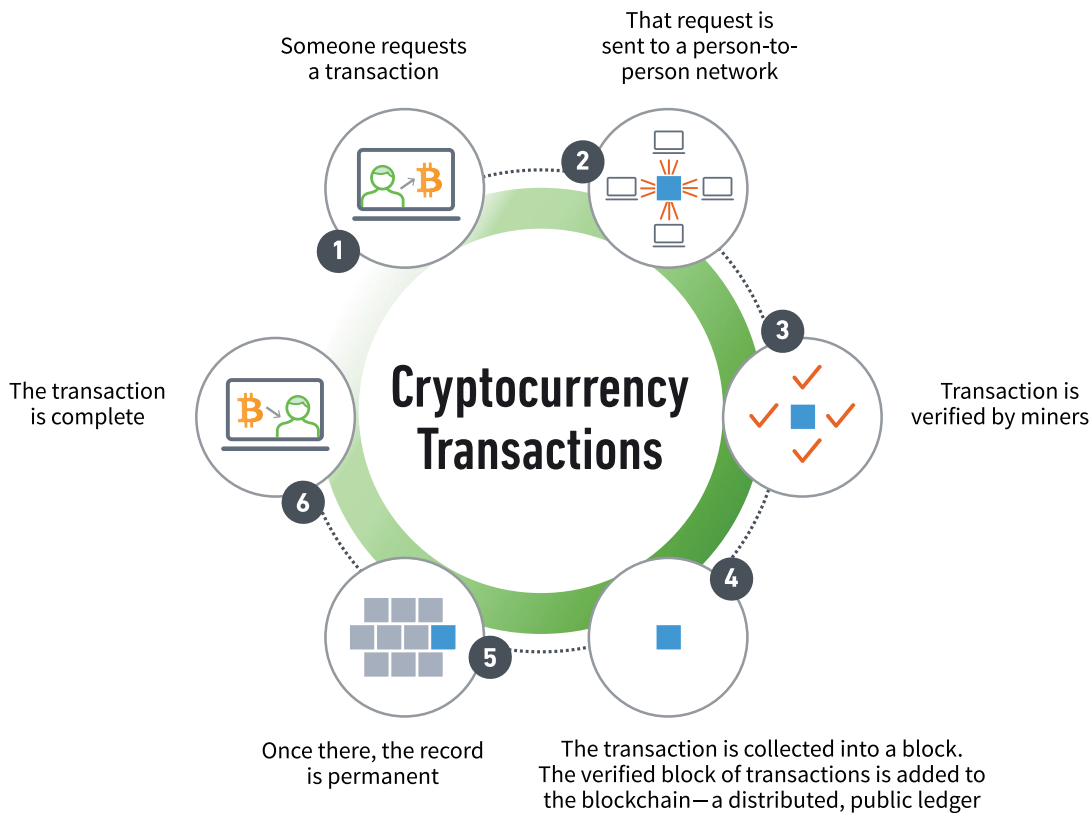
There are two ways cryptocurrencies are obtained: They can be purchased using actual fiat currency through a digital transaction on an exchange, or they can be mined.

Mining is a collaborative effort that validates such transactions in exchange for a reward of cryptocurrency. Each cryptocurrency transaction is validated to ensure it occurs only once, as well as to thwart attempts to change any transaction in the digital ledger (the blockchain). Validation involves computing a cryptographic hash¹ of all the transactions in a block (a collection of transactions), coupled with a computational task.

Blocks are made up of the underlying transaction along with a collection (a tree) of cryptographic hashes that relate to each transaction. Blocks also encompasses additional data, such as the correct hash for the previous block and a difficult target. In this way, each transaction is resilient to tampering, as manipulating any transaction affects the entire block. And altering any block affects the entire blockchain.

¹ https://en.wikipedia.org/wiki/Cryptographic_hash_function

FIGURE 1: A HIGH-LEVEL BLOCKCHAIN OVERVIEW



Typically, the computational task is to generate thousands (or millions or billions) of cryptographic hashes per second in an effort to guess the piece of input (a nonce²) that, when put through a cryptographic hash function, is the correct value for the current block of transactions.

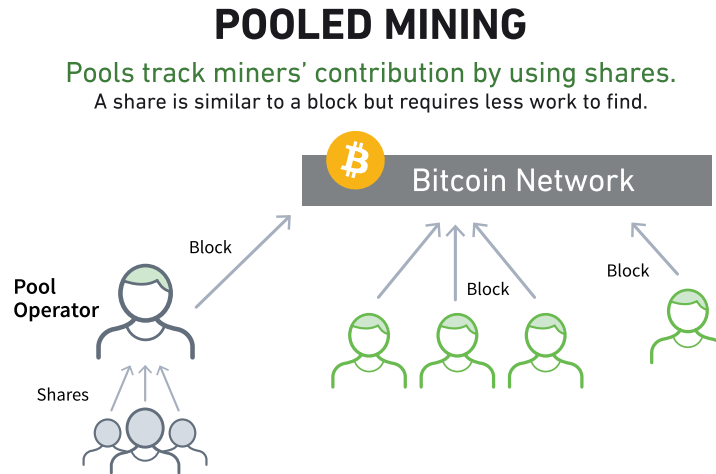
Miners are computer applications that perform the validation work through hashing, thus interacting with the blockchain for a given cryptocurrency. Because two input nonces can produce very different results, and because the correct guess can't be found using the previous answer, miners produce millions of guesses to determine the correct answer in validating a transaction block.

The number of available units, or coins, for a particular cryptocurrency is regulated and grows over time. To keep the growth rate constant, the difficulty in completing the validation task is adjusted as the number of miners and their productivity rises and falls. The net result is a consistent number of new cryptocurrency units become available every period (measured in seconds or minutes). The cryptocurrency reward is given to the first miner who successfully guesses and submits the correct nonce for a block of transactions.

While an in-depth explanation of cryptocurrencies is outside the scope of this research paper, Appendix A offers a more thorough description.

² https://en.wikipedia.org/wiki/Cryptographic_nonce

FIGURE 2: A HIGH-LEVEL VISUALIZATION OF POOLED CRYPTOCURRENCY MINING



CPU Mining

The tasks completed while processing transactions are most frequently the work of the general-purpose processors (CPU) found in all computers. All computers can theoretically participate in cryptocurrency mining, which requires intensive arithmetic computations on a large scale.

But while CPUs are capable of performing most computing tasks, they're limited in how efficiently they perform such arithmetic computations. And the faster a system—or collection of systems—can complete a cryptocurrency block, the more likely the miner will be the first to do so and win the reward. With this in mind, we move on to a technology better suited for completing validation tasks—GPU mining.

GPU Mining

To gain a competitive advantage, cryptocurrency popularity has driven thousands of interested parties worldwide to assemble dedicated computer systems more suited for solving mining tasks more efficiently. Exposure to computer gaming is how most people become familiar with a GPU, or graphics processing unit. It's what provides the requisite high-speed, high resolution graphics.

But beyond graphics, GPUs can perform the mathematical computations involved in validating cryptocurrency transactions much more efficiently due to their large number of arithmetic logic units (ALUs). In addition, virtualized systems (particularly those in cloud computing) often don't have GPU hardware, but emerging technologies allow virtualized systems to share GPU resources.

Disk Mining

Unlike CPU and GPU mining, disk mining doesn't rely on a proof-of-work regime. Rather, it relies on a proof-of-capacity (PoC) or proof-of-space (PoSpace)—where storage space takes the place of computing power in completing mining tasks.

The core concept is that solutions are randomly generated, and in a process called plotting, such solutions are typically stored on a drive dedicated to disk mining. The more storage space allotted to plotting, the more potential solutions.

Finding and matching them on disk is akin to the aforementioned CPU method. Again, the miner that solves all the transactions in a block the fastest is most likely to receive the associated reward.

Regardless of the type of mining, it's possible (though unlikely) for two miners to validate new blocks at the same time. Since only one can be added to the blockchain, the other becomes orphaned and ignored. Thus the first to guess the correct nonce may not win the reward if something prevents it from submitting its new block before another miner.

Unlike CPU and GPU mining—which requires substantial amounts of high-performance computing power and ultimately electricity to run systems—disk mining requires much less energy. Even low-power systems can participate through being connected to large storage systems.

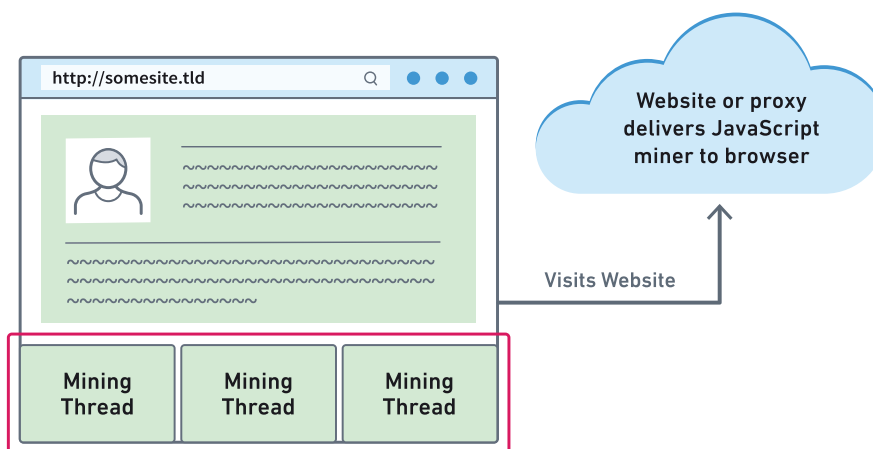
Browser Mining

While not a distinct mining category, browser mining is CPU-based and occurs without the need of a standalone executable. Requisite code being implemented in JavaScript, browsers can initiate dedicated mining processes by visiting a website without the user's knowledge or consent. Briefly employed by The Pirate Bay,³ a BitTorrent tracker site, this technology led to the development of browser extensions to block cryptocurrency mining.⁴

ASIC Mining

ASICs are application-specific integrated circuits optimized for specific tasks. Composed of thousands or millions of logic gates, they sometimes integrate all the components of a computer—a so-called system on a chip (SoC). For cryptocurrency mining, some ASICs were developed to achieve peak efficiency in hash generation, thus achieving a higher likelihood of winning a reward for any given transaction block. But because ASICs are uncommon in corporate settings, they weren't examined in Exabeam's shadow mining research.

FIGURE 3: A HIGH-LEVEL VISUALIZATION OF BROWSER MINING



While browsing websites, threads run in the background to mine cryptocurrency

³ <https://www.ccn.com/the-pirate-bay-is-using-visitors-computers-to-mine-monero-again/>

⁴ <https://chrome.google.com/webstore/search/miner?hl=en>

SHADOW MINING

Shadow IT loosely describes the unauthorized use of systems and infrastructure. Shadow mining goes a step further. Here, IT or operational security staff enrich themselves through use of shadow IT to illicitly mine cryptocurrency.

Mining cryptocurrencies at any significant scale isn't free. There is the very high cost of the computing power, which usually translates into the cost of electricity. But what if there were no material costs other than time invested in setting up the mining?

The negligible (or arguably zero) cost of mining, coupled with the chance to make money, is at the root of shadow mining. There must also be a confluence of a large enough pool of computers to participate in the mining, combined with rogue individuals who have access to the required resources.

For example, in a 2014 report to the US Congress, a National Science Foundation⁵ researcher was described as using supercomputers at two universities to mine between \$8,000 – \$10,000 in Bitcoin per month.

In the last days of 2017, more than 105,000 users were affected by a Chrome browser extension that secretly mined cryptocurrency.⁶ And briefly in September 2017, showtime.com and showtimeanytime.com were discovered delivering browser-based cryptomining code to users' browsers.⁷

In another incident, Australian Federal Police executed a search warrant in February of 2018 after discovering Bureau of Meteorology employees had used desktop systems to mine cryptocurrency.⁸

Also in February of that same year, a Russian scientist was reportedly arrested⁹ after attempting to connect a Russian supercomputer to the internet (presumably, rather than an air-gapped network¹⁰) so they could mine Bitcoin.

In March of 2018, a Florida man was arrested after it was discovered he had used state Department of Citrus computers to mine cryptocurrency, using his state-issued purchasing card to buy 24 computer graphics cards.¹¹

In November of 2018, a school principal in China¹² was fired after teachers became suspicious of noisy computers running day and night. They reportedly ran up an additional \$2,100 a month in electricity costs.

And in one of the most pervasive incidents of someone caught mining, a US Federal Reserve communications analyst was discovered covertly operating cryptomining for more than two years.¹³

⁵ <https://www.nsf.gov/pubs/2014/oig14002/oig14002.pdf>

⁶ <https://www.gearbrain.com/archive-poster-chrome-extension-mining-2520659343.html>

⁷ https://www.theregister.co.uk/2017/09/25/showtime_hit_with_coinmining_script/

⁸ <https://www.abc.net.au/news/2018-03-08/bureau-of-meteorology-staff-implicated-in-cryptocurrency-ring/9524208>

⁹ <https://www.bbc.com/news/world-europe-43003740>

¹⁰ [https://en.wikipedia.org/wiki/Air_gap_\(networking\)](https://en.wikipedia.org/wiki/Air_gap_(networking))

¹¹ https://www.tampabay.com/news/publicsafety/crime/Department-of-Citrus-employee-arrested-when-caught-mining-for-cryptocurrency-agents-say_166345974

¹² <https://www.bbc.com/news/technology-46150107>

¹³ <https://bravenewcoin.com/insights/employee-mined-bitcoins-on-federal-reserve-servers-for-two-years>

Though none of those caught in these schemes were reported as being IT or operational security staff, and the scale of their efforts appear small, cryptocurrency mining economics clearly change when the computers and electricity are essentially free.

The idea of stealing small amounts of resources from a number of sources and aggregating it might sound familiar. It's the plot of Superman III (and later Office Space), where fractional amounts of money left over from financial transactions were siphoned off, totaling \$85,789.90 at the end of the subsequent pay period.

THE RISKS AND IMPACT OF SHADOW MINING

Quis custodiet ipsos custodes?

“Who will guard the guards themselves?”

Shadow IT creates risk within an organization because it creates infrastructure that isn't monitored for security compromises. For a shadow mining operator to be successful, they must deploy mining applications, or miners, across many systems. And the miners must remain undetected by users and those responsible for IT or operational security.

Several malware families include built-in miners. As a result, a number of antivirus products detect miners as malware. While it may be partially a subjective decision, the documentation for many mining applications instruct users to first disable their antivirus software.

So to be successful and remain undetected, an insider threat such as shadow mining depends on deliberately configuring

security systems to function incorrectly. And miners are yet another piece of software, with the infosec mantra declaring all software contains bugs. Therefore, installing additional internet-connected software, even if it isn't detected as malware, increases any computer's attack surface.

This scenario not only makes an organization less secure, but by introducing software that consumes additional resources and increasing its attack surfaces, shadow mining can be said to make affected computers less reliable.

AS DAN GEER OF IN-Q-TEL WROTE:¹⁴

If a system is insecure,

It is unreliable, therefore

Security is necessary for reliability, yet

Security is insufficient for reliability, therefore

Security is a subset of reliability

¹⁴ [1] Geer D. August 2003. Patch work. ;login:. 28(4):27-28

HOW MIGHT SHADOW MINING OCCUR

In conducting the research for this paper, Exabeam built a network that loosely resembles many corporate environments. It included:

- Windows servers with DNS
- Active Directory (Kerberos/LDAP/Group Policy)
- Windows file servers
- Windows 10 users and administrative systems

We configured Windows Group Policy so that Windows Defender allowed miner applications to run and remain on disk without automatically being quarantined. From the admin system, we deployed and remotely executed mining applications and their configuration files to user systems.

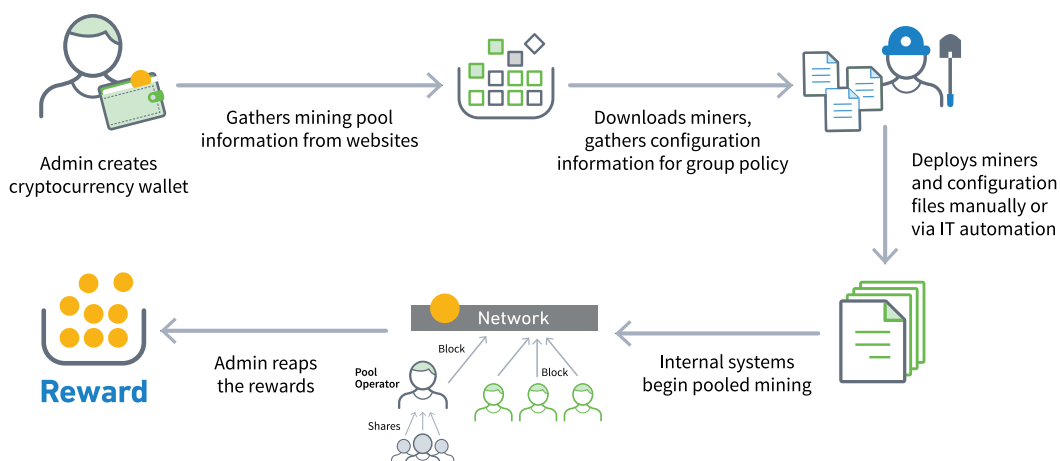
The code and related underpinnings to mine cryptocurrencies proved to be relatively easy to distribute. The applications were all standalone programs that don't require installation on a target system. Once in place, each was quickly tuned to have relatively little impact to the overall performance of the system.

When logged in as an unprivileged user, the cryptomining applications—each renamed to `svchost.exe`—were indistinguishable from legitimate processes having the same name, provided the user didn't view their file locations. (Most users never look at process details, let alone view the file location for a running process.) And when tuned to consume very little processing power (to create as little system impact as possible) the systems appeared completely normal to users.

Web-based mining proved even easier, as a web proxy can be easily configured to inject JavaScript mining code into certain pages. This becomes even more plausible when corporate entities build their own certificate authority (CA) as part of a Windows domain and generate a subordinate signing certificate deployed on the web proxy. The proxy then automatically generates TLS certificates that browsers treat as entirely valid, allowing companies to peek into TLS-encrypted traffic. By visiting any website—encrypted or not—the proxy could inject mining code at will.

SHADOW MINING ATTACK FLOW

FIGURE 4: AN OVERVIEW OF THE PHASES OF SHADOW MINING



Armed with an understanding of how Windows Defender and Google Chrome behave when downloading, then executing each mining application, Exabeam deployed at least one miner from each category to gather host and network data for further analysis.

Step 1: Preparation

CPU MINING

For CPU mining where the Monero (XMR)¹⁵ cryptocurrency was selected, we installed the standalone Monero wallet to obtain a corresponding ID for mining. Initially, we attempted to use a Cryptopia¹⁶ wallet for mining Monero, but were unable to use it for this purpose.

GPU MINING

For GPU mining where we selected the Zcash (ZEC) cryptocurrency (and unlike CPU-based Monero mining), we were ultimately able to mine to a Zcash wallet provided by Cryptopia.

DISK MINING

Using BURST for disk mining, where it takes one BURST coin to get started, we had to first find a way to get one. All publicly available BURST faucets were exhausted, but fortunately a kind soul on a Discord¹⁷ channel donated one. With our BURST donation in-hand, we were able to name a BURST wallet, then designate a pool beneficiary—a step unique to disk mining.

MINING POOLS

Since pooled resources are much more effective in cryptocurrency mining, we used a mining pool for each currency. Subsequent mining activity during all research stages occurred using pooled mining.

¹⁵ <https://www.getmonero.org/>

¹⁶ <https://www.cryptopia.co.nz/>

¹⁷ <https://discord.gg/3nkprV>

Step 2: Windows Group Policy Configuration

We created a Windows Group Policy to ensure Windows Defender didn't quarantine mining executables or prevent their execution. First, we added path exclusions¹⁸ on Windows Defender so that a `C:\Windows` subdirectory was excluded from antivirus protection. Next, we added exclusions¹⁹ to Defender that ensured it didn't scan or quarantine any files opened by the excluded processes. Next, we added a Defender firewall exception²⁰ to allow remote administration from administrative systems. Then we applied our Group Policy to user systems within the Group Policy Management Console. Finally, we forced a Group Policy update on user systems by running `gpupdate /force`²¹ in a command prompt window running with administrator privileges.

Step 3: Configuration

To efficiently make use of computer memory, some applications want to use large memory pages²² within an operating system. When this happens on a Windows system, a User Account Control (UAC) pop-up²³ appears, informing the user that a program is asking for elevated privileges. Many mining applications default to using large memory pages, so to run them remotely without any user interaction, we disabled large pages for all miners.

CPU mining applications also consume 100% of at least one CPU core by default. While this might make sense for people trying to mine using their own resources, it doesn't in a shadow mining scenario where the goal is for the illicit activity to remain hidden.

To keep them hidden, Exabeam configured each mining application to not request any additional privileges and to keep resource utilization to a minimum. We selected only miners that allowed some degree of control over CPU utilization for the persistent execution phase of our shadow mining study. We gained this control by configuring the number of threads consumed by each mining process, and in some cases its priority.

Being command-line tools, each mining application naturally generated a bunch of text as it ran. As this, too, was undesirable, we configured the miners to produce as little output as possible. And since some have built-in web servers to aid in monitoring and configuration, we disabled these features so as to keep the miners hidden.

As a last step, we configured the CPU and GPU miners to participate in the pools selected for their respective currencies.

¹⁸ <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-antivirus/configure-extension-file-exclusions-windows-defender-antivirus>

¹⁹ <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-antivirus/configure-extension-file-exclusions-windows-defender-antivirus>

²⁰ https://docs.microsoft.com/en-us/sql/analysis-services/analysis-services-powershell?view=sql-server-2014#bkmk_remote

²¹ <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/gpupdate>

²² <https://docs.microsoft.com/en-us/windows/desktop/memory/large-page-support>

²³ <https://docs.microsoft.com/en-us/windows/desktop/uxguide/winenv-uac>

Step 4: Remote Installation

Initially, we remotely created a `C:\Windows` subdirectory (excluded from Windows Defender antivirus in Step 2) on each user system by running `PsExec`²⁴ from an administrative system. Next, we used `Xcopy`²⁵ to copy files to that subdirectory on each user system.

To study disk mining (where plot files are required), we explored two scenarios. In the first, we used `PsExec` and `Xcopy` to copy the plot files from an administrative system to the aforementioned `C:\Windows` subdirectory on each user system. In the second, we placed plot files on a network share to which the user systems connect. Then, using `PsExec` and `mklink`,²⁶ within each `C:\Windows` subdirectory we created a symbolic link to the mounted network share containing the plot files.

Step 5: Execution

Since Exabeam used virtual machines (VMs) to build the entire shadow mining environment, the user systems were reset to a known good state before each round of miner execution and the gathering of associated data.

With all steps in place to deploy the miners and their configuration files, we used a Visual Basic script, `invis.vbs`,²⁷ such that a batch file could run without a command window. We copied it and simple two-line batch scripts in Step 4. We used the Windows Script Host, `wscript`,²⁸ to execute the `invis.vbs` contents, calling the batch files and running the miners in the background.

With all the files in place, we used a `PsExec` command line (similar to the one below) to start each miner:

```
PsExec \\USER-SYSTEM -w C:\Windows\mining_
subdirectory wscript.exe invis.vbs run.bat
```

²⁴ <https://docs.microsoft.com/en-us/windows/desktop/memory/large-page-support>

²⁵ <https://docs.microsoft.com/en-us/windows/desktop/uxguide/winenv-uac>

²⁶ <https://docs.microsoft.com/en-us/sysinternals/downloads/psexec>

²⁷ <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/xcopy>

²⁸ <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/mklink>

²⁹ <https://gist.github.com/jonschoning/1558919>

³⁰ <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/wscript>

Step 6: Persistent Execution

We then verified that miners could be remotely deployed and executed without revealing themselves to users. That is, no command prompt window would appear, no identified mining process appeared in Windows Task Manager's default view, and the miners weren't placing a noticeable load on the user systems. Now it was time to fully realize the shadow mining concept by engaging the miners at system startup.

Remote persistent execution relied once again on Windows Group Policy—this time using a startup script. Note that we tested each miner application one at a time, resetting virtual machines before we proceeded.

For each miner we tested, after copying the step 4 files onto each user system, we placed a version of our `run.bat` file in the `Startup Scripts` directory within the Windows Group Policy. We tailored these simple two-line `run.bat` files for each miner, specifying their unique configuration options when calling each executable, and the miner being renamed to `svchost.exe`.

We added a startup script to the Group Policy by selecting `run.bat` from the `Startup Scripts` subdirectory. Finally, we performed a Group Policy update using `gpupdate/force` on the user systems. After each reboot, the user systems ran the next mining application to be tested (as configured).

After each reboot and user login, the running `svchost.exe` task (the disguised miner) appeared no different to the unprivileged user in Windows Task Manager than any other `svchost.exe` process. After each iteration, we repeated the exercise.

Detecting Shadow Mining

While IT and operational security staff may be able to hide security exceptions to allow cryptocurrency miners, it may be more difficult for them to altogether disable the generation and/or reception of security logs. Additionally, as evidenced over the past twenty years of infosec history, not all attackers are sophisticated. Exabeam used some of the most common tools to simulate infrastructure-wide shadow mining, with this approach being reasonably representative of how it may already be deployed in unsuspecting enterprises.

To be competitive, it's likely that anyone engaged in shadow mining would participate in a mining pool to increase their earning opportunity. Because they seek to grow in size, such pools publish information about how to participate. As a result, mining pools can be enumerated to identify DNS domains, DNS hostnames, IP addresses, TCP ports, and TLS server certificates (where present).

Appendix A lists all the host and network signals we collected during our research.

Network-Based Mining Detection

Armed with up-to-date blacklists of mining pool information, it becomes relatively straightforward to detect mining activities on a network. They can be revealed by DNS requests, and even rudimentary network telemetry can reveal mining activity when matched up to blacklists.

An important question is, "What if a mining application encapsulates network communication inside TLS?" We reviewed the source code of several cryptocurrency mining applications and determined that some do not verify server TLS certificates. This may be by design, as their approach is instead to publish a certificate hash and provide a command line switch that lets a user specify the hash for comparison. Essentially, this is a simple certificate-pinning implementation.

The result is that a decapsulating web proxy can generate self-signed certificates for mining pool sites on-the-fly, with the miner simply accepting such certificates. With TLS traffic decapsulated by a proxy serving as a man-in-the-middle, the network activity of the miners can be observed without encryption (see How Might Shadow Mining Occur, page 8)

While some mining pools publish a certificate hash for miners that support certificate pinning through configuration, this too could be defeated by a seasoned IT or operational security organization. By configuring proxies to selectively change the certificate hash presented on mining pool websites, such that they match the certificates automatically generated by proxies, certificate-pinning features can also be defeated.

We also observed the Blago Burstcoin disk miner performing HTTP POST transactions containing Stratum data. This is a convenient design decision by the Blago authors that translates into an easily detectable network signal.

Host-Based Mining Detection

Host-based mining detection is more difficult because it relies on software running on the host. While an administrator can disable the generation of some host logs that might reveal shadow mining, it's nearly impossible to have a mining application communicate over a network while not also producing network packets.

If properly configured, Windows process logs reveal process startup behavior. They can provide a historical time-series of applications that spawn additional processes/threads. Once enumerated, such startup behavior can lead to rules in a detection system that uses conditional statements.

For example:

```
If process name 'A' starts
and if process 'A' starts process 'B'
and if process 'A' starts process 'C'
then generate a security event
```

Detecting Shadow Mining Deployment

A particularly savvy administrator might even configure their mining to begin as employee activity ramps up during the day and stop at the end of the business day. And an even more insidious insider might first probe for employee activity on a system before commencing mining. But for both efforts, the scripts that enable such behavior leave telltale artifacts on a system.

Thankfully, not all attackers are sophisticated, and some of the most convenient deployment technologies are very detectable. Deploying mining programs between systems using `Psexec` not only generates SMB session data, it also generates process and service logs on a target system (if it's properly configured to generate them).

Using a tool such as `xcopy` also generates SMB session data for each file copied between systems. Depending on the environment, this may or may not be a common activity. However, the potential one-to-many relationship of an administrator deploying mining applications to many user systems might reveal itself both volumetrically and by virtue of out-degree³¹ when the network conversations are graphed.

Finally, in the process of automatically starting miners at system start, one can consider a number of possibilities, including: Scheduled Tasks in Windows Group Policy, Startup

Scripts in Windows Group Policy, Windows Desired State Configuration (DSC), Azure Desired State Configuration, or even something as simple and effective as the Non-Sucking Service Manager (NSSM).³² Each approach generates detectable security data that can reveal uncommon events.

A number of technologies make it possible to audit Windows Group Policy changes; doing so is likely desirable for most organizations wanting to have comprehensive visibility into their Windows environment. Auditing for additions and changes to startup scripts or scheduled tasks can reveal a variety of undesirable activities.

What about auditing the DSC Pull or Push server role and its available LCM configuration? This can reveal the existence of automation that initiates mining once a Windows system enters a desired state. The existence of NSSM in most corporate environments is unlikely; that alone may be a strong enough signal to delve further into investigating hosts.

Indeed, various aspects of shadow mining are detectable by gathering a variety of host and network data. As surveillance methods develop for identifying it, shadow mining may prove to be more prevalent than anyone ever guessed.

See Appendix C for additional information about shadow mining detection, in addition to cryptocurrency mining in general.

³¹ [https://en.wikipedia.org/wiki/Degree_\(graph_theory\)](https://en.wikipedia.org/wiki/Degree_(graph_theory))

CONCLUSIONS AND SUMMARY

Although one may never have mined cryptocurrency, resources in the form of forum posts, how-to guides, and step-by-step videos inform even the layperson how to do it. The barrier to entry has been lowered such that almost anyone can get started.

From school principals to scientists to communications analysts, people caught covertly mining cryptocurrency using stolen employers' resources highlight the economic incentive and temptation to make money by mining cryptocurrency. As discussed in the preceding Shadow Mining section, these attempts can be lucrative and go on for years before they're discovered.

Equipped with a basic understanding of cryptocurrencies, a system administrator needs very little additional expertise to deploy miners throughout their company—using automation to start and stop miners as they see fit. Exabeam's research has laid out one of the simplest ways a shadow mining operation can be carried out.

That said, a sufficiently knowledgeable person could be much more effective in hiding their mining efforts. Several of the miners we used are open source software and could easily be customized to be installed as an ostensibly innocuous-sounding service.

It's more difficult to hide the artifacts of deploying and running a shadow mining operation. In environments where host logs are configured to send data to a SIEM for detection, absence of such logs would be noticed. Though with modification, the miners could be tweaked to start in a manner similar to other applications and, if they're also renamed, SIEM correlation rules might not detect anything of note.

Network-based detection could also be made substantially more difficult by using schemes to hide communication. Employing a few proxies having innocuous advertising network, social media, or shopping domain name lookalikes/soundalikes would add some obfuscation. All told, there are dozens, if not hundreds, of ways these efforts could be disguised or hidden.

Shadow mining is clearly possible. Given the popularity of cryptocurrencies (despite their value being highly volatile over the past year), it's entirely plausible that it's already occurring in one enterprise or another. Perhaps even yours. But without surveillance of these efforts and in the absence of public disclosures, it's difficult to know.

APPENDIX A: CRYPTOCURRENCIES

Much has been written about cryptocurrencies, particularly in an era when blockchain technology has become the ever-present hammer looking for a nail—the solution looking for a problem. That said, a brief overview is unavoidable.

Cryptocurrencies are a form of digital currency untethered to the true identity of the user. They're not backed by the full faith and credit of any sovereign nation, and every transaction is kept in perpetuity in a public, distributed electronic ledger. Records within the ledger are collected into blocks.

Each block is connected to the blocks that precede and follow it in a chain, hence the term blockchain. Blockchains are constantly growing in size and are themselves distributed. Many copies are frequently held in peer-to-peer networks.

There are different means to prove the validity of each blockchain transaction. They're typically unique to each cryptocurrency (or family of cryptocurrencies). Ultimately, they relate to independently validating each transaction—without the need for any central supervisory authority.

To ensure each transaction occurs only once, blockchains rely on disparate timestamping regimes to both prove the validity of each transaction and ensure that each is serialized.

Through a consensus method such as proof-of-work or proof-of-capacity, each participating system in the validation effort completes a task—an effort that requires some resource (e.g., computational, or input/output).

These tasks are easy for other participating systems to verify, but are difficult (and time consuming) to complete. In the most commonly used cryptocurrency, Bitcoin, a proof-of-work task must be completed for each transaction in a block for it to be submitted to the network of other verifiers. Typically the difficulty of these tasks are automatically adjusted to ensure a relatively consistent duration elapses during the generation of each block.

There are a limited number of monetary units for each cryptocurrency; the total number nominally rises at a predetermined rate. The fact that every transaction—including purchasing cryptocurrency—must be verified creates an economic incentive for validating transactions through mining. By solving a block, new cryptocurrency units are rewarded to miners (i.e., systems participating in the transaction validation process).

As the popularity of cryptocurrencies has grown, so have the resources dedicated to processing transactions. People often work together in a mining pool to have a better chance of solving a block as a result.

Additional information about cryptocurrencies can be found at sources such as Wikipedia and the Bitcoin Wiki.³³

³³ https://en.bitcoin.it/wiki/Main_Page

APPENDIX B: TOOLS AND SIGNALS

While studying shadow mining, Exabeam used a mix of tools in a relatively simple scenario that simulated how it might occur in the wild. As part of this study, we collected packet captures and host logs to later characterize and provide suggestions as to how to detect shadow mining.

For each miner type (CPU, GPU, and disk), the core behavior (program start, DNS requests, socket connections) is very similar and is summarized below in a single set of signals. Where signals differ (e.g., browser mining and disk mining), we have broken out additional tables for these miners.

Cryptocurrency by Mining Type

CPU	GPU	DISK	BROWSER
Monero	Zcash	BURST	Monero

Tools by Cryptocurrency

CPU	GPU	DISK	BROWSER
xmrig	dstm	Turboplotter 9000	Coinhive
minergate-cli	bminer	creepminer	
xmr-stak	ewbf	blago	

Detection by Mining Type by Tool

CPU

	DETECTED BY DEFENDER AV	BLOCKED BY SMARTSCREEN	BLOCKED BY CHROME	WANTS ELEVATED PRIVILEGES*
xmrig	Yes	No	Yes	No
minergate-cli	No	No	No	No
xmr-stak	No	Yes	No	Yes

GPU

	DETECTED BY DEFENDER AV	BLOCKED BY SMARTSCREEN	BLOCKED BY CHROME	WANTS ELEVATED PRIVILEGES*
dstm	No	No	No	No
bminer	No	No	No	No
ewbf	Yes	No	No	No

DISK

	DETECTED BY DEFENDER AV	BLOCKED BY SMARTSCREEN	BLOCKED BY CHROME	WANTS ELEVATED PRIVILEGES*
Turboplotter 9000	No	Yes	No	Yes
creepminer	Yes	Yes	No	No
blago	Yes	No	No	Yes

*DISPLAYS A UAC DIALOG

DATA GATHERING PHASES

Miner Evaluation

Each tool was downloaded and executed directly on a 64-bit, Windows 10 Enterprise system participating in a Windows domain. We initially configured Windows Group Policy to only gather information about processes. Later we modified

it to ensure that miner executables were allowed by Windows Defender antivirus and that each miner process could create files.

In their default configuration, miners were more likely to be noticed by a user because of their high CPU utilization:

		51%	7%	0%	0%
		CPU	Memory	Disk	Network
Name		Status			
Apps (4)					
>	Notepad	0%	6.5 MB	0 MB/s	0 Mbps
>	Task Manager	0.1%	15.7 MB	0 MB/s	0 Mbps
▼	Windows Command Processor ...	50.9%	12.4 MB	0 MB/s	0 Mbps
	Console Window Host	0%	5.7 MB	0 MB/s	0 Mbps
	Windows Command Processor	0%	0.8 MB	0 MB/s	0 Mbps
	xmr-stak.exe	50.9%	5.9 MB	0 MB/s	0 Mbps
>	Windows Explorer	0%	31.7 MB	0 MB/s	0 Mbps
Background processes (36)					
>	Antimalware Service Executable	0%	113.3 MB	0 MB/s	0 Mbps
	Application Frame Host	0%	4.5 MB	0 MB/s	0 Mbps
>	blnsrv.exe	0%	1.1 MB	0 MB/s	0 Mbps
	COM Surrogate	0%	1.5 MB	0 MB/s	0 Mbps
	COM Surrogate	0%	1.1 MB	0 MB/s	0 Mbps
>	COM Surrogate	0%	3.1 MB	0 MB/s	0 Mbps

Miner Configuration and Pooled Mining

Next, we configured each miner to participate in a mining pool, while exploring configuration options to limit resource usage.

We also gathered network signals for each miner process at this point.

(Events are numbered in sequence.)

EVENT NUMBER	TYPE	FAMILY	SIGNAL
1	Network	DNS	Request to miner pool (pool.supportxmr.com)
2	Network	TLS	Connection to miner pool
3	Network	Certificate	TLS server certificate (hash) for mining pool
4	Network	Stratum Inside TLS	<pre>{ "method": "login", "params": { "login": "<redacted>", "pass": "", "rigid": "<redacted>", "agent": "xmr-stak/2.5.2/752fd1e7e/master/win/nvidia-amd-cpu/20", "id": 1 }, "jsonrpc": "2.0", "error": null, "result": { "id": "bb1a6af2-8738-40d9-bae2-2603785cc84a", "job": { "blob": "0909cc9ab7df05bf155e9fb402f0aa8c71aa95e8e0a07896218815235e36ab72416bb091c74ee200000000b6f7fd66865-efdb67226bd8b3da1743327a0806eb448c066af31e32ebe9090f401", "job_id": "TxsdDtbtthSdi8GxVUC/QoC6QCQjZ", "target": "711b0d00", "id": "bb1a6af2-8738-40d9-bae2-2603785cc84a", "status": "OK" } }, "jsonrpc": "2.0", "method": "job", "params": { "blob": "0909e19ab7df054f7f6dd1b360a8ca768d149f93fe55d9135bc408351fc7fd92a4c8a3d62648b400000000eb5df83555838bcc3b789e70689ad4e6959343d66ea90442ffd a46a9adb92ec902", "job_id": "cSWIPbp2UJOxB3vJnf4qNBRJAOs", "target": "711b0d00", "id": "bb1a6af2-8738-40d9-bae2-2603785cc84a" }, "method": "submit", "params": { "id": "bb1a6af2-8738-40d9-bae2-2603785cc84a", "job_id": "cSWIPbp2UJOxB3vJnf4qNBRJAOs", "nonce": "ce210000", "result": "fccad48304dc25af08ff0050ffa1bb8bbb1f2a79385b07fd8b273d92c66d0600", "id": 1 }, "jsonrpc": "2.0", "error": null, "result": { "status": "OK" } }</pre>
5	Host	Security Log	<p>PROCESS CREATION</p> <p>Process Information:</p> <ul style="list-style-type: none"> • New Process ID: 0x1d34 • New Process Name: C:\Users\badmin\Downloads\xmrig-2.8.3-msvc-win64\xmrig.exe • Token Elevation Type: %%1938 • Mandatory Label: Mandatory Label\Medium Mandatory Level • Creator Process ID: 0x1d54 • Creator Process Name: C:\Windows\System32\cmd.exe • Process Command Line: xmrig.exe -c config.json <p>Event ID: 4688</p>

EVENT NUMBER	TYPE	FAMILY	SIGNAL
6	Host	Security Log	<p>PROCESS BINDS TO A LOCAL PORT</p> <p>Application Name: \device\harddiskvolume2\users\badmin\downloads\xmrig-2.8.3-msvc-win64\xmrig.exe</p> <p>Network Information:</p> <ul style="list-style-type: none"> Source Address: 0.0.0.0 Source Port: 50683 Protocol: 6 <p>Event ID: 5158</p>
7	Host	Security Log	<p>PROCESS CREATES AN OUTBOUND CONNECTION</p> <p>Application Name: \device\harddiskvolume2\users\badmin\downloads\xmrig-2.8.3-msvc-win64\xmrig.exe</p> <p>Network Information:</p> <ul style="list-style-type: none"> Direction: Outbound Source Address: 192.168.168.240 Source Port: 50683 Destination Address: 192.110.160.114 Destination Port: 443 Protocol: 6 <p>Event ID: 5156</p>

Miner Remote Installation and Execution

Finally, in the same way a system administrator might remotely deploy miners, we deployed ours onto user systems from an administrative system.

(Events are numbered in sequence.)

EVENT NUMBER	ACTION	TYPE	FAMILY	SIGNAL
1	Create Directory (PsExec)	Host	Security Log	<p>Detailed File Share</p> <ul style="list-style-type: none"> Share Name: *\ADMIN\$ Share Local Path: \\?\C:\Windows Relative Target Name: PSEXESVC.exe
2		Host	Security Log	<p>PROCESS CREATION</p> <p>Process Information:</p> <ul style="list-style-type: none"> New Process ID: 0xebc New Process Name: C:\Windows\PSEXESVC.exe Token Elevation Type: %%1936 Mandatory Label: Mandatory Label\Medium Mandatory Level Creator Process ID: 0x294 Creator Process Name: C:\Windows\System32\services.exe Process Command Line: C:\Windows\PSEXESVC.exe <p>Event ID: 4688</p>

EVENT NUMBER	ACTION	TYPE	FAMILY	SIGNAL
3		Host	Security Log	Detailed File Share <ul style="list-style-type: none"> Share Name: *\IPC\$ Share Path: Relative Target Name: PSEXESVC
4		Host	Security Log	Detailed File Share <ul style="list-style-type: none"> Share Name: *\IPC\$ Share Path: Relative Target Name: PSEXESVC-<Redacted>--6296-stder
5		Host	Security Log	PROCESS CREATION Process Information: <ul style="list-style-type: none"> New Process ID: 0x1ff0 New Process Name: C:\Windows\System32\cmd.exe Token Elevation Type: %%1936 Mandatory Label: Mandatory Label\Medium Mandatory Level Creator Process ID: 0xbec Creator Process Name: C:\Windows\PSEXESVC.exe Process Command Line: "cmd" /c mkdir C:\Windows\Quarry\quarry1 Event ID: 4688
6		Network	SMB	Session Setup
7		Network	SMB	Tree Connect: \\<Redacted>\ADMIN\$
8		Network	SMB	Create Request File: PSEXESVC.exe
9		Network	SMB	Write Request File: PSEXESVC.exe
10		Network	SMB	Close Response File: PSEXESVC.exe
11		Network	SMB	Tree Disconnect
12		Network	SMB	Session Logoff
13		Network	SMB	Session Setup
14		Network	SMB	Tree Connect: \\<Redacted>\IPC\$
15		Network	SMB/DCERPC	BIND - SVCCTL 2.0
16	Remote File Copy (xcopy)	Host	Security Log	Detailed File Share <ul style="list-style-type: none"> Share Name: *\C\$ Share Path: \??\C:\ Relative Target Name: C:\Windows\Quarry\quarry1
17		Host	Security Log	For each file copied: Detailed File Share <ul style="list-style-type: none"> Share Name: *\C\$ Share Path: \??\C:\ Relative Target Name: C:\Windows\Quarry\Quarry1\<file>

EVENT NUMBER	ACTION	TYPE	FAMILY	SIGNAL
18		Network	SMB	Session Setup
19		Network	SMB	Tree Connect: \\<Redacted>\IPC\$
20		Network	SMB	Tree Connect: \\<Redacted>\C\$
21		Network	SMB	For each file copied: Create Request File: <file>
22		Network	SMB	Tree Disconnect
23		Network	SMB	Session Logoff
24	Run Miner (PsExec)	Host	Security Log	PROCESS CREATION Process Information: <ul style="list-style-type: none"> New Process ID: 0x6d4 New Process Name: C:\Windows\System32\wscript.exe Token Elevation Type: %%1936 Mandatory Label: Mandatory Label\Medium Mandatory Level Creator Process ID: 0x2248 Creator Process Name: C:\Windows\PSEXESVC.exe Process Command Line: "wscript.exe" invis.vbs run.bat Event ID: 4688
25		Host	Security Log	PROCESS CREATION Process Information: <ul style="list-style-type: none"> New Process ID: 0x1580 New Process Name: C:\Windows\System32\cmd.exe Token Elevation Type: %%1936 Mandatory Label: Mandatory Label\Medium Mandatory Level Creator Process ID: 0x6d4 Creator Process Name: C:\Windows\System32\wscript.exe Process Command Line: C:\Windows\system32\cmd.exe /c ""C:\Windows\Quarry\quarry1\run.bat" " Event ID: 4688
26		Network	SMB	Session Setup
27		Network	SMB	Tree Connect: \\<Redacted>\IPC\$
28		Network	SMB/ DCERPC	BIND - SVCCTL 2.0

Browser Mining

Though a subset of CPU mining, we explored browser mining for its feasibility in shadow mining. Signals collected while studying browser mining appear below.

(Events are numbered in sequence.)

EVENT NUMBER	TYPE	FAMILY	SIGNAL
1	Network	DNS	Request for mining infrastructure (coinhive.com)
2	Network	TLS	Connection to mining infrastructure
3	Network	Certificate	TLS server certificate (hash) for mining infrastructure
4	Network	Data	TLS encapsulated data
5	Network	DNS	Request for mining infrastructure (authedmine.com)
6	Network	TLS	Connection to mining infrastructure
7	Network	Certificate	TLS server certificate (hash) for mining infrastructure
8	Network	Data	TLS encapsulated data
9	Network	DNS	Request for mining infrastructure (ws004.authedmine.com)
10	Network	TLS	Connection to mining infrastructure
11	Network	Certificate	TLS server certificate (hash) for mining infrastructure
12	Network	Data	TLS encapsulated data
25	Host	Security Log	<p>Creates three threads resembling:</p> <p>PROCESS CREATION</p> <p>Process Information:</p> <ul style="list-style-type: none"> • New Process ID: 0x2120 • New Process Name: C:\Program Files (x86)\Google\Chrome\Application\chrome.exe • Token Elevation Type: %%1938 • Mandatory Label: Mandatory Label\Medium Mandatory Level • Creator Process ID: 0x27b0 • Creator Process Name: C:\Program Files (x86)\Google\Chrome\Application\chrome.exe • Process Command Line: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=renderer --field-trial-handle=1340,4730730913716481267,13405782208964557255,131072 --disable-gpu-compositing --service-pipe-token=60994997709113429 --lang=en-US --enable-offline-auto-reload --enable-offline-auto-reload-visible-only --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=60994997709113429 --renderer-client-id=13 --no-v8-untrusted-code-mitigations --mojo-platform-channel-handle=1172 /prefetch:1 <p>Event ID: 4688</p>

Disk Mining with a File Share

Unlike CPU and GPU mining, disk mining generates unique network signals when performed in conjunction with a file share.

While this represents an unlikely deployment scenario, we explored it and gathered data for analysis. Listed below are the signals unique to disk mining over a share.

(Events are numbered in sequence.)

EVENT NUMBER	TYPE	FAMILY	SIGNAL
1	Network	SMB	Session Setup
2	Network	SMB	Tree Connect: \\<Redacted>\IPC\$
3	Network	SMB	Tree Connect: \\<Redacted>\Shared
4	Network	SMB	Find Request File: plots; Pattern: *
5	Network	SMB	Find Response (Returns all files in directory and metadata for each file)
6	Network	SMB	Create Request File: plots; GetInfo Request FileFsSizeInformation
7	Network	SMB	Close Request File
8	Network	SMB	For each file in the directory: Create Request File: plots\<file> GetInfoRequest File: plots\<file> Read Request Len:32K File: plots\<file> Close Request File: plots\<file>
9	Network	SMB	Tree Disconnect

APPENDIX C: DETECTION

As part of our research, Exabeam developed a Windows Group Policy that enabled Windows systems to disable audit logs by default. These logs were activated by enabling the following audit categories in the Group Policy:

- Audit Process Creation
- Audit Registry
- Audit Credential Validation
- Audit File Share
- Audit Detailed File Share
- Audit Filtering Platform Connection
- Audit Kerberos Service Ticket Operations

Mining

At program start, a Windows application log is generated. Immediately, miners perform a DNS lookup, followed by a network connection.

APPLICATION LOG DETECTION

While the application name can be changed, a blacklist rule that generates an alert using a substring match is a straightforward initial detection method:

```
If executable_name in MINER_EXECUTABLE_
BLACKLIST:
    alert()
```

DNS DATA DETECTION

Likewise, blacklists maintained by gathering information in mining pools also provide a DNS blacklist detection means:

```
If dns_request_name in MINING_POOL_DNS_
BLACKLIST:
    alert()
```

IP DATA DETECTION

In addition, blacklists maintained by performing DNS lookups of mining pool DNS names (composed of the IP addresses contained in DNS answers) provide for a method of IP-based blacklist detection:

```
If destination_ip_address in MINING_POOL_
IP_BLACKLIST:
    alert()
```

This can further be enhanced by adding port information, as mining pools naturally publish TCP ports used in conjunction with the IP addresses. Here the IP/TCP port blacklist detection method resembles:

```
If destination_ip_address_and_port in
MINING_POOL_IP_PORT_BLACKLIST:
    alert()
```

PERIODIC COMMUNICATION/ BEACONING DETECTION

Beaconing detection provides another axis for detecting mining activity. The fact that miners periodically communicate to obtain new blocks for verification provides a straightforward detection vector. There are surely dozens of approaches to clustering on various features of network traffic; below we present a few that can further enhance detection.

The following features seem fairly stable for clustering, including:

- Packet/Flow Frequency
- Packet/Flow Size
- Clustering by Destination IP

The frequency of a miner communicating with a mining pool is a function of the currency being mined, the type of mining, the configuration of the mining pool by its operators, and the resources dedicated to mining on each system.

Because shadow mining seeks to stay hidden, and because of the relative homogeneity of corporate systems, frequency and size should be fairly stable across a large number of systems—assuming all are participating in the same mining pool. Once again this a fairly safe assumption, given that very little power would be dedicated to mining on each system, and only through their collective effort would the entire scheme earn enough money for it to be worth the effort of the person behind the shadow mining.

In the course of running an enterprise network, there are a number of external addresses that many hosts will visit. Where shadow mining exists on a network, the mining pool IP address(es) will be among these clusters.

HTTP(S) DATA DETECTION

While many miners wrap Stratum messages inside TLS, others use Stratum inside HTTP/HTTPS. As discussed in the preceding Detecting Shadow Mining section, miners that do use TLS as an encapsulating transport may not be validating the server TLS signature. In this case, the HTTPS communication can be intercepted and decapsulated, providing the same visibility as HTTP.

For miners communicating via HTTP, the structure of Stratum messages (encoded in JSON), is both well documented and detectable at all communication stages. Client-side Stratum detection at miner startup resembles:

```
if message is JSON:
    If keys (id, method, params) in message:
        alert()
```

Server-side Stratum detection at miner startup resembles:

```
if message is JSON:
    If keys (id, result, error) in message:
        alert()
```

Additionally, most miner applications aren't commercial software (which is subject to a traditional software development life cycle (SDLC)) and may be more prone

to contain bugs. During our research, Exabeam observed the Blago miner performing HTTP POSTs without a HOST header. These messages were subsequently rejected by the Cloudflare web server used by the configured mining pool.

Deploying Miners for Shadow Mining

There are many ways in which a miner might be deployed locally and remotely. One simple technique we used during our research is fairly straightforward: we remotely created file directories using PsExec and remotely copied files onto user systems using Xcopy. Both generate host and network signals for detection. These signals would be similar for deploying disk mining plot files as well.

PSEXEC LOG-BASED DETECTION

PSEXEC is rather noisy in relation to signals generated for each use. Some that are suitable for detection are enumerated below:

- Each invocation connects to the ADMIN\$ share and generates a corresponding event in the Windows Security Log. Refer to event 1 in the Miner Remote Installation and Execution table in Appendix B.
- Each invocation creates a new process having the name PSEXESVC.EXE in the Windows Security Log. Refer to event 2 in the Miner Remote Installation and Execution table in Appendix B.
- Each invocation connects to the IPC\$ share and generates a corresponding event in the Windows Security Log. Refer to event 3 in the Miner Remote Installation and Execution table from Appendix B.

Commands executed by PsExec also create a new process and a corresponding Windows Security Log entry. This meant creating a cmd.exe process for creating folders. Refer to event 5 in the Miner Remote Installation and Execution table in Appendix B.

Any process created by PsExec will have the PsExec process ID as its Creator Process ID (as would be the case with any process that creates subprocesses). Tracking the hierarchy of PsExec-created processes is relatively straightforward by following it (and its service) from its invocation.

PSEXEC NETWORK-BASED DETECTION

As it creates an SMB session, PsExec generates Tree Connect requests to the ADMIN\$ and IPC\$ shares. In typical usage, it also remotely creates a PSEXEC.EXE file before execution. This generates additional SMB messages related to this activity: Create, Write, and Close. Refer to events 7 – 10 in the Miner Remote Installation and Execution table in Appendix B.

XCOPY LOG-BASED DETECTION

Deploying miners using Xcopy generates Detailed File Share entries in the Windows Security Log on the destination system. At invocation, Xcopy generates a Detailed File Share log entry as it connects to the C\$ share. Refer to event 17 in the Miner Remote Installation and Execution table in Appendix B.

As each file is copied, it creates another Detailed File Share entry in the Windows Security Log on the destination system, along with the Relative Target Name portion of the log specifying the copied file. Refer to event 18 in the Miner Remote Installation and Execution table in Appendix B.

XCOPY NETWORK-BASED DETECTION

As it creates an SMB session, Xcopy generates Tree Connect requests to the IPC\$ and C\$ shares. SMB Create Request messages are generated for each file copied. Refer to event 21 in the Miner Remote Installation and Execution table in Appendix B.

With all the previous information in mind, detection across these various axes might resemble:

```
If new_process_name is PSEXESVC:
    alert ()

If smb_session_creates_file PSEXESVC:
    alert ()

If smb_session_creates_file PSEXESVC:
    alert ()
```

VBSCRIPT DETECTION

The technique we used to remotely execute the miners during testing—and prior to using Group Policy to run them at startup—was to use a VBScript wrapper to launch a command line executable untethered to a Windows Command window. We used PsExec to invoke wscript, which in turn called some VBScript to ultimately run a batch file that started a miner.

With the wide acceptance of Windows PowerShell, there is very little reason for this VBScript technique to be used in any enterprise environment. Bearing this in mind, looking for any process having wscript.exe or cscript.exe in its command line would aid in identifying potential misuse. Refer to event 24 in the Miner Remote Installation and Execution table in Appendix B.

Logic to detect this might be as simple as:

```
If process_name is "wscript.exe":
    alert ()
```


DISK MINING WITH A FILE SHARE

The final outlier is disk mining, which largely only distinguishes itself as a process with sequential read operations on disk. With 1G of space dedicated to plot files, we saw that the Blago miner read in consistent 32K segments over a network share. From the perspective of the miner application, it was accessing a local file, as the share was soft linked to a directory by having used mklink.

Given the relatively poor performance, it's unlikely that anyone would use this technique for shadow mining, but it's not impossible. With a number of systems all accessing the same directory and files within, a fairly obvious pattern is created in the similarity of the SMB traffic generated, as all these systems access plot files during mining.



ABOUT US

Exabeam delivers next-generation security management technology that enables organizations to protect their most valuable information. The Exabeam Security Management Platform combines unlimited log data collection, advanced behavioral analytics, and automated incident response. It's all supported by Exabeam's patented Smart Timelines technology that uses machine learning to track identity and behavior over time. The company's recent industry accolades include Forbes Cloud 100, Inc. 500, and SC Awards Europe, among many other distinctions. Exabeam is privately funded by Aspect Ventures, Cisco Investments, Icon Ventures, Lightspeed Venture Partners, Norwest Venture Partners, and well-known security investor Shlomo Kramer. For more information, visit <https://www.exabeam.com>. 

TO LEARN MORE ABOUT
HOW WE CAN HELP YOU,
VISIT [EXABEAM.COM](https://www.exabeam.com) TODAY.