

REPORT

Proliferation of Mining Malware Signals a Shift in Cybercriminal Operations

Andrei Barysevich
Priscilla Moriuchi
Daniel Hatheway
Recorded Future Insikt Group

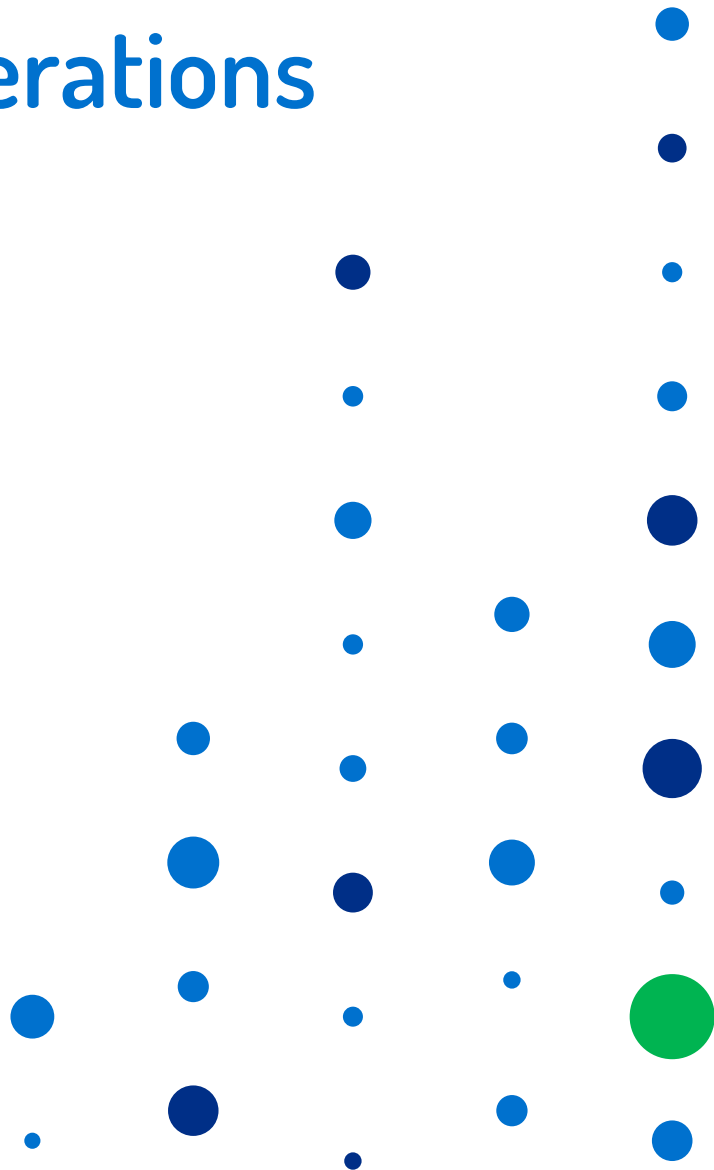


Table of Contents

Executive Summary 3

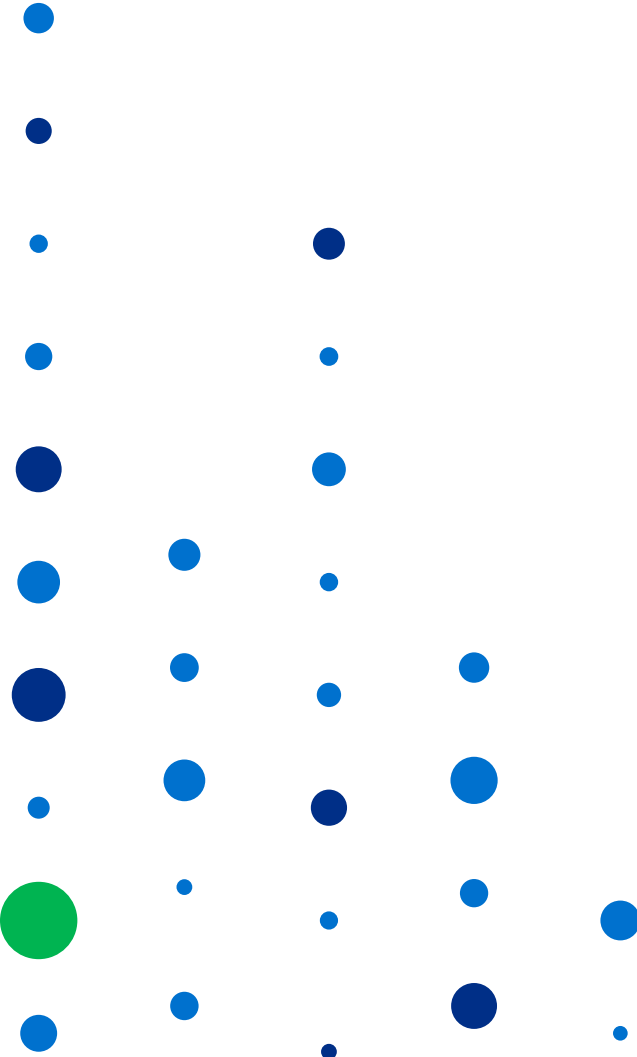
Key Judgments 3

Background 3

Threat Analysis 7

Technical Analysis 11

Outlook 16



Executive Summary

Cybercriminals are utilizing cryptocurrency mining as a way to maintain a steady income and avoid the inherent risks involved in running a large-scale ransomware campaign. This shift in tactics is the first observed since 2015, when threat actors moved from distributing banking malware to using ransomware. Mining malware is readily available, affordable, and easy for a novice to deploy; however, indicators exist that provide a means to detect mining activity on a network.

Key Judgments

- Beginning May 2017 we observed a rapid spike of mining malware alerts across a spectrum of analyzed sources. Our research has confirmed that cybercriminals are shifting attack vectors from highly damaging ransomware infections to long-term, low-velocity crypto mining operations.
- We identified 62 different types of mining malware offered for sale across the criminal underground.
- Although some variants are sold for as high as \$850, the majority of available mining malware today is offered for less than \$50, making it easily accessible to novice and inexperienced members of the underground.
- Due to low productivity of individually infected machines, the majority of all currently available miners will only target x64 systems.
- While we have not identified any North Korea-specific cryptocurrency mining malware, North Korean threat actors have experience in altering publicly available tools, managing botnets, and procuring cryptocurrency both legally and illegally. These skills lead us to conclude that North Koreans will likely employ this technique in the near future, if they haven't already.

Background

In 2015 we began noticing a shift in modus operandi of cyber criminals. At first gradually and later with increasing determination, we saw them abandon proven money-making techniques. While still utilizing the same established infrastructure and delivery methodology, the payload changed. Instead of distributing banking malware, cybercriminals adopted the upcoming ransomware model.

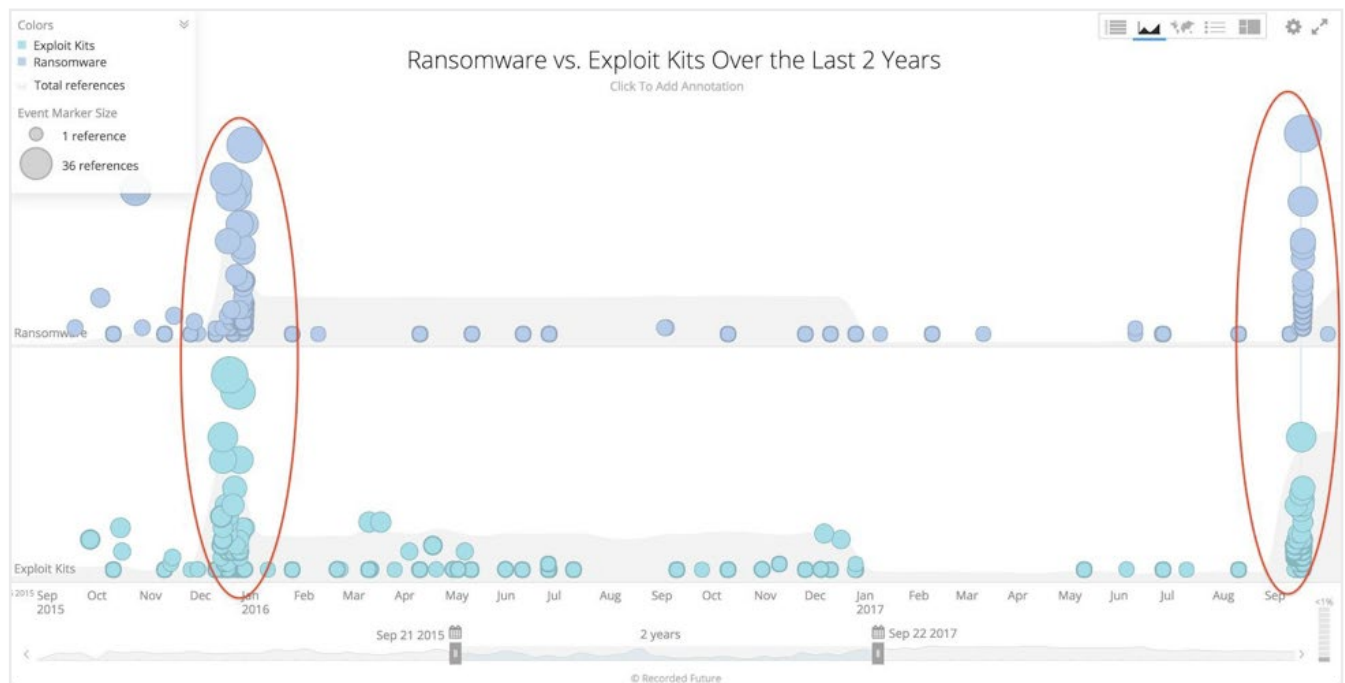
In early 2017, another modus operandi shift was evident. Accustomed to a reliable daily ransomware income and witnessing firsthand the proliferation of bitcoin, cybercriminals saw malicious cryptocurrency mining was seen as the next logical undertaking.

Criminal History

While the potential profitability of fraudulent bank transfers was and remains at the top of the criminal “food pyramid,” operational outcomes are uncertain. To achieve maximum results, threat actors have to work with developers of banking web-injects and automatic money-transferring malware. To receive and launder stolen funds, reliance on a long chain of “money-mule” handlers is unavoidable, and often funds from completed banking transactions will often be stolen by dishonest intermediaries.

At the same time, ransomware presented a very straightforward value proposition, eliminating most of the risks inherent with other methods. Fueled by the mass adoption of bitcoins, a truly global and entirely untraceable payment method, the chances of a successful outcome became very binary. Either infected victims will pay or they won't, but if they do, all money is deposited directly to an attacker's wallet, regardless of the region and the local currencies.

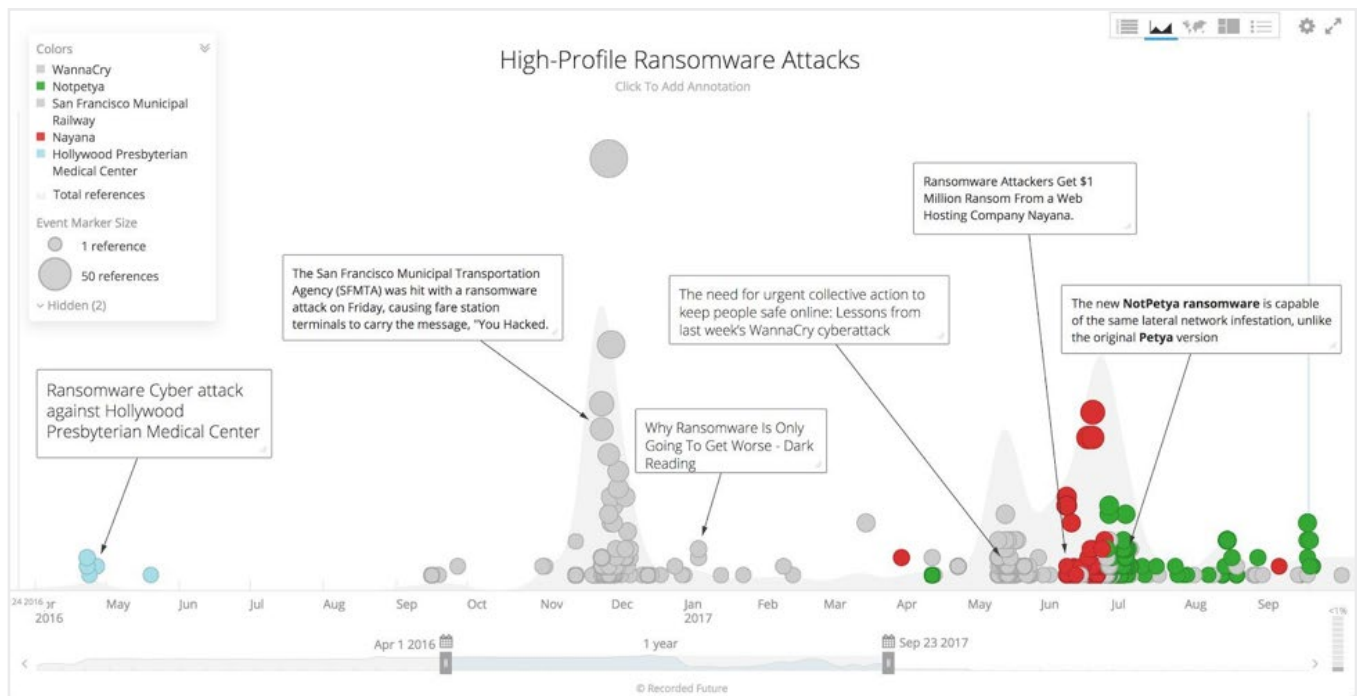
Comprehensive analysis of ransomware distribution levels further confirmed our hypothesis of a direct relation to the use of an already-established exploit kit distribution network.



Simultaneous spike of exploit kits and ransomware propagation.
<https://app.recordedfuture.com/live/app/analyze/sc/2EXH6E0AWXnA>

While initially perceived as an unpleasant annoyance that simply prevented access to a device, the severity of attacks rapidly grew. The sophistication and damaging effects of ransomware have evolved to unstoppable, global epidemic, capable of crippling the economy and costing hundreds of millions of dollars in losses to public and private organizations.

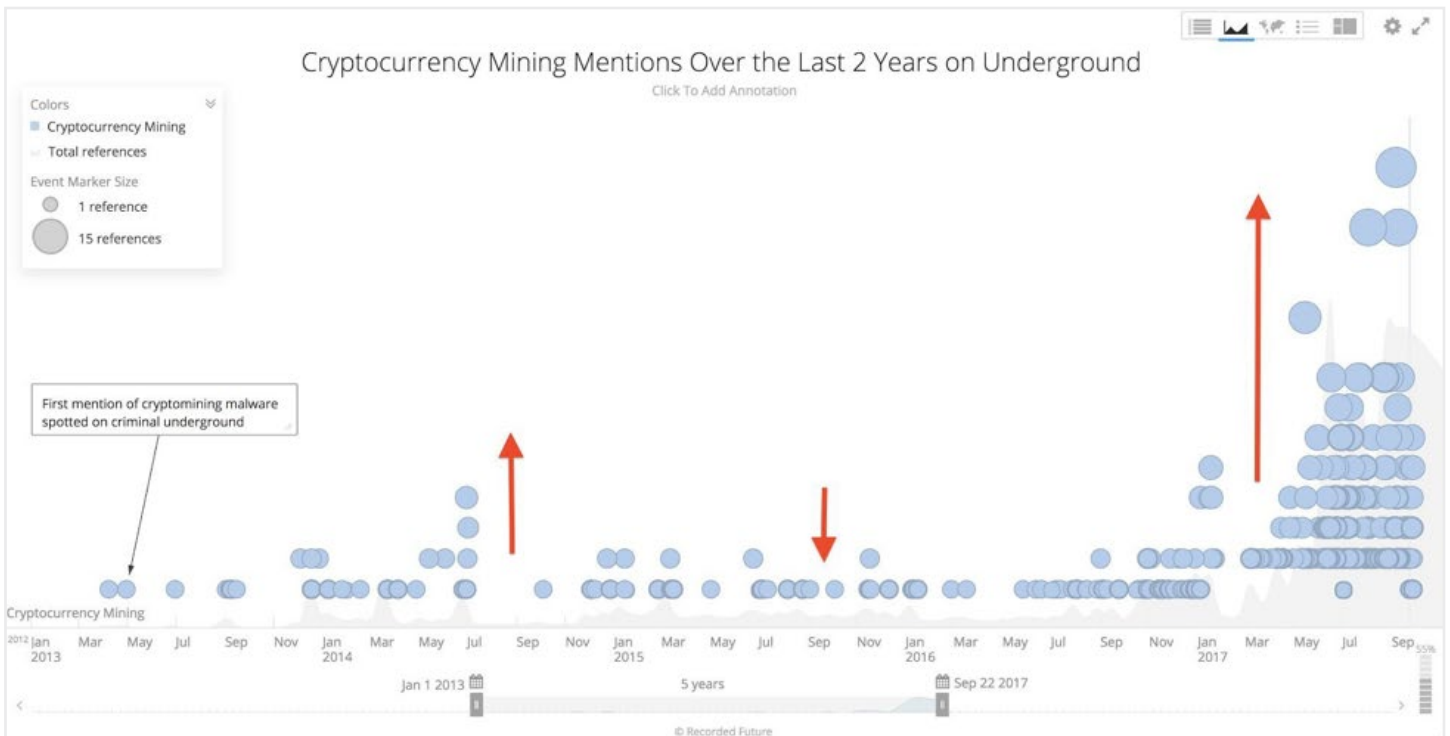
It became evident that the established fragile balance between criminals and law enforcement disappeared and no target was off-limits. Outrageous attacks on healthcare facilities and municipal transit systems culminated in the unprecedented WannaCry and NotPetya campaigns. Overnight, ransomware was recognized as an act of cyberterrorism, and based on the recent Hansa and AlphaBay takedowns, law enforcement agencies around the globe are pursuing and apprehending nefarious cyber actors.



Timeline of the most damaging ransomware attacks.
<https://app.recordedfuture.com/live/sc/7Apox1GWUJtE>

Not all criminals were caught off guard with a sudden change of attitude from police. Longstanding members of the underground, those who thrived, became incredibly influential among peers, and managed to evade prosecution for decades, recognized the impending danger early on.

The first signs of disapproval appeared immediately following the breach of Hollywood Presbyterian Hospital, condemning those engaged in the extortion campaign and citing inevitable retribution from law enforcement. As ransomware attacks became even more harmful and persisting in the media spotlight, acute actors began searching for the new "big idea" which could generate a steady income stream without all of the inherent risks.



Close correlation between crypto-mining activity across the criminal underground and the price of bitcoin.

<https://app.recordedfuture.com/live/app/analyze/sc/3gXtXvQsIxBT>



The spike of bitcoin prices between 2013 and 2017.

<https://blockchain.info/charts/market-price>

Threat Analysis

Crypto-Mining Malware: Designed for Accessibility, Profitability, and Stealth

The first samples of mining malware began appearing in 2013, but it was not until the second half of 2017 that it gained popularity among members of the criminal underground. By then dozens of vendors were offering various mining malware, ranging in pricing and additional functionality.









In 2014, unknown hackers shared a yet-to-be-released Watch Dogs computer game with built-in bitcoin-mining functionality. Knowing that avid gamers use powerful graphics cards, the goal was to leverage the combined GPU power for nefarious use. Unhappy users quickly began noticing a drastic decrease in a game's performance and identified the malware causing the issue.

As bitcoin's mining difficulty has increased, requiring more computing power, criminals have begun experimenting with Monero and Zcash, alternative cryptocurrencies which can be successfully mined with CPU power rather than GPU. Both currencies provided the best balance between hashing power required to obtain it and market price. While the number of potential victims with powerful video cards is fairly small, requiring precise targeting via crafted delivery campaigns, the pool of systems which could be infected with mining malware utilizing CPU is endless.

Mining profitability calculator [?]

Ethereum Cryptonote Bitcoin-like Zcash Cloud Mining

60 kH/s ↕

BTC ↕	 Bytecoin BCN	 Monero XMR [★]	 FantomCoin FCN	 QuazarCoin QCN	 DigitalNote XDN	 MonetaVerde MCN	 Dashcoin DSH	 Aeon coin AEON
1 hour	1.98278 k 0.00063 BTC	0.04328 0.00095 BTC	0.79562 0.00002 BTC	151.661 0.00061 BTC	57.9932 0.00003 BTC	1.81557 k 0 BTC	26.9205 0.00011 BTC	1.19323 0.00069 BTC
24 hours	47.5867 k 0.01523 BTC	1.03873 0.02281 BTC	19.0949 0.00057 BTC	3.63986 k 0.01456 BTC	1.39184 k 0.00074 BTC	43.5737 k 0 BTC	646.091 0.00276 BTC	28.6375 0.01654 BTC
1 week	333.107 k 0.10659 BTC	7.27111 0.15967 BTC	133.664 0.00401 BTC	25.4790 k 0.10192 BTC	9.74286 k 0.00516 BTC	305.016 k 0 BTC	4.52264 k 0.01931 BTC	200.462 0.11580 BTC
Exchange rates by Changelly	0.0003200 mBTC	21.959800 mBTC	0.0300000 mBTC	0.0040000 mBTC	0.0005300 mBTC	0 mBTC	0.0042700 mBTC	0.5776600 mBTC

Minergate mining calculator indicating Monero as the most profitable cryptocurrency.

With profitability levels directly related to how long the malware stays undetected, threat actors have begun improving various obfuscation methods. Some variants of the GPU-dependent malware will terminate the mining process altogether if a videogame is launched to avoid detection. In other cases, the CPU consumption on a hacked machine will be automatically adjusted to ensure processing cores are only partially used. The malware is typically hidden from the Task Manager, utilizes a persistent process, and will be immediately restored after a user deletes it. Some versions will show a fake antivirus message, indicating that the malicious file has been placed in the quarantine; meanwhile, the malware remains fully operational.

In one instance we identified a single bitcoin wallet, which we believe might be a part of a larger mining operation, with daily transactions recorded for the past three months since June of 2017, emphasizing persistent behavior of mining malware.

Reaffirming our hypothesis, we observed several discussions among Russian-speaking actors. In one instance a hacker expressed extreme satisfaction with the results of a trial infection:

"I've used 'bots' already under my control to upload 110 miners before going to sleep. By the time I woke up 108 were still alive, which took me by surprise. I expected a half would be dead by then. "

In the attempt to stand out among the competition and answering to the demand from customers, developers began expanding their products, in some cases adding various key-logging and data intercepting functionality.

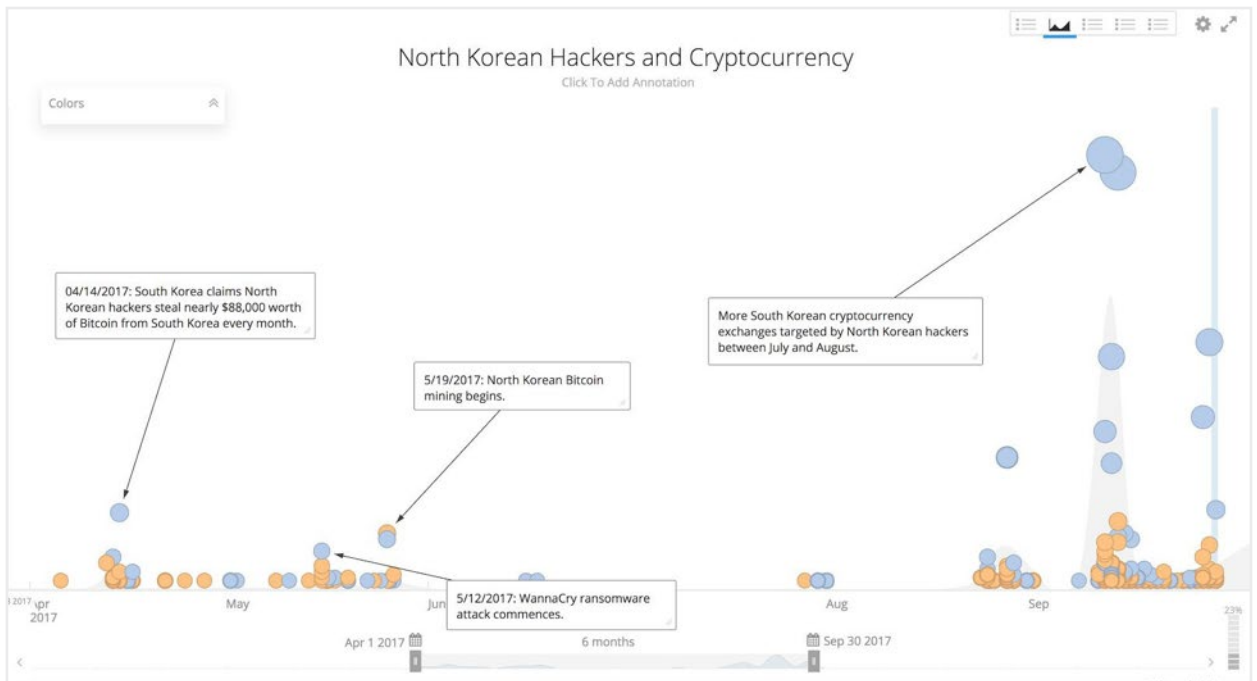
Nation-State Participation: North Korea

North Korean threat actors have been conducting cyber operations to generate funds for the Kim regime likely since at least 2015, but appear to have become interested in bitcoin and cryptocurrency only over the past six months. In May, North Korea's interest in cryptocurrency appears to have converged in three separate events.

On May 12, North Korean threat actors initiated the first global ransomware attack, which utilized a variant of the WanaCrypt0r tool (also called WannaCry) modified to propagate via the SMB vulnerability outlined in Microsoft Security Bulletin (MS17-010), also known as the ETERNALBLUE exploit. After encrypting files on a machine, victims were directed to pay the ransom to one of three bitcoin wallets.

According to [actual ransom](#), the total value of the three wallets when they were emptied on August 2 was 52.19666422 BTC or \$142,361.51. The bitcoin [from these wallets](#) was then run through a mixer and eventually converted to Monero, making it nearly impossible to track the end recipients.

On May 17, Recorded Future analysis discovered that users in North Korea had begun to mine bitcoin. Before that day, there had been virtually no activity to bitcoin-related sites or nodes, or utilizing bitcoin-specific ports or protocols. Beginning on May 17, that activity increased exponentially, from nothing to hundreds per day. The timing of this mining is important because it began very soon after the May WannaCry ransomware attacks, which the NSA [has attributed](#) to North Korea's intelligence service, the [Reconnaissance General Bureau](#) (RGB), as an attempt to raise funds for the Kim regime.



Timeline of North Korean cyber actors targeting or use of cryptocurrency.
<https://app.recordedfuture.com/live/sc/2kKL8c1m2QIB>

By this point (May 17) actors within the government would have realized that moving the bitcoin from the three WannaCry ransom accounts would be easy to track and ill-advised if they wished to retain deniability for the attack.

It is not clear who is running the North Korean bitcoin mining operations; however, given the relatively small number of computers in North Korea coupled with the limited IP space, it is not likely this computationally intensive activity is occurring outside of state control.

There are two sub-hypotheses regarding who is conducting the bitcoin mining:

- The military, intelligence services, or other state organization, for the purposes of raising funds for the Kim regime.
- Individual user activity, but because of bandwidth and energy usage is probably known or permitted by the state. The miner is a senior leader or family member of a senior leader.

Lastly, from May through August, North Korean threat actors are [suspected to have targeted](#) at least three South Korean cryptocurrency exchanges via spearphishing. The spearphishing targeted “personal email accounts of employees” at these exchanges, frequently used “tax-themed lures,” and deployed malware “linked to North Korean actors suspected to be responsible for intrusions into global banks in 2016.”

While we have not identified any North Korea-specific cryptocurrency mining malware, given North Korea’s demonstrated interest in both legally and illegally procuring cryptocurrencies, it is likely that the regime will employ mining malware in the near future if it has not already.

North Korean threat actors have prior experience in assembling and managing botnets, bitcoin mining, and cryptocurrency theft, as well as in custom altering publicly available malware; three elements that would be key to effectively creating and managing a network of covert cryptocurrency miners.

Technical Analysis

We obtained a feature-rich mining malware called 1ms0rry MINERPANEL, which is sold across the criminal underground. The product comes in several packages ranging in price from \$35 to \$850. While the “Premium” version offers barebone functionality, without access to command and control (C2) panel, the most comprehensive and expensive “Source” version includes the source code for the malware. Our evaluation was of the “Extended” version sold for \$100 and offering a range of features including the C2 panel.

In addition to all of the required installation files, a software that joins multiple files together into one payload and a step-by-step guide for building and deploying the miner was provided.

The Control Panel Installation

The process to install the control panel was simple and required a web server, PHP, and MS SQL. After creating the MS SQL database and importing the supplied SQL file, a user updates the variables for the database connection inside config.php. Lastly, the web server is configured to execute index.php from the directory where the files are located.

```
<?php
error_reporting(-1);
$dblocation = "localhost:3306"; // Имя сервера
$dbuser = " "; // Имя пользователя
$dbpasswd = " ";
$dbname = " ";
// устанавливаем соединение с базой данных
$dbcnx = @mysql_connect($dblocation,$dbuser,$dbpasswd);
if (!$dbcnx)
{
    // Выводим предупреждение
    echo("<P>Server unavailable</P>");
    // Завершаем работу в случае неудачи
    exit();
}

// Код соединения с базой данных
if (!@mysql_select_db($dbname, $dbcnx))
{
    echo(" <P>Server is not available now</P>" );
    exit();
}
mysql_set_charset('utf8');
?>
```

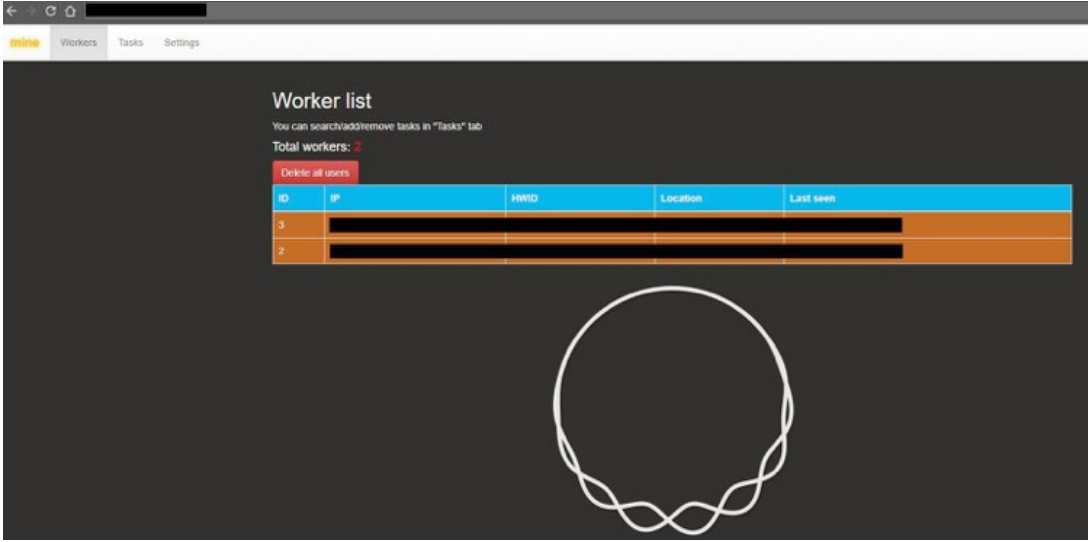
C2 panel installation process.

If the installation was successful a user should see a background image of Kylo Ren from "Star Wars: The Force Awakens" and a login prompt. By default the the username and password is admin:admin; however, both can be updated via the settings page.



1ms0rry Miner login page.

The tasks menu item is where administrators are able to configure the miner to install or update it to a new version, while the workers section displays all the victim machines under control.



The list of infected machines, controlled via admin page.

The Payload

The payload consist of two files, the bot responsible for communicating with the panel and the actual miner. The seller recommends using a file joiner to combine both payloads into a single file, which could then be delivered by a Microsoft Word file or other similar methods.

While bot functionality allows for real-time tracking and payload updates of all infected machines, the likelihood of detection by the victim is significantly increased. Hence, some attackers might choose using a standalone miner, opting to use the simple process of tracking via one of the mining pools.

Admin privileges are not required to launch the payload. While the bot processes can be easily spotted in the Task Manager, the miner activation is delayed and entirely hidden.

By default the miner is utilizing two processing cores, but prior to product delivery, specifications can be adjusted per client's request.

Indicators

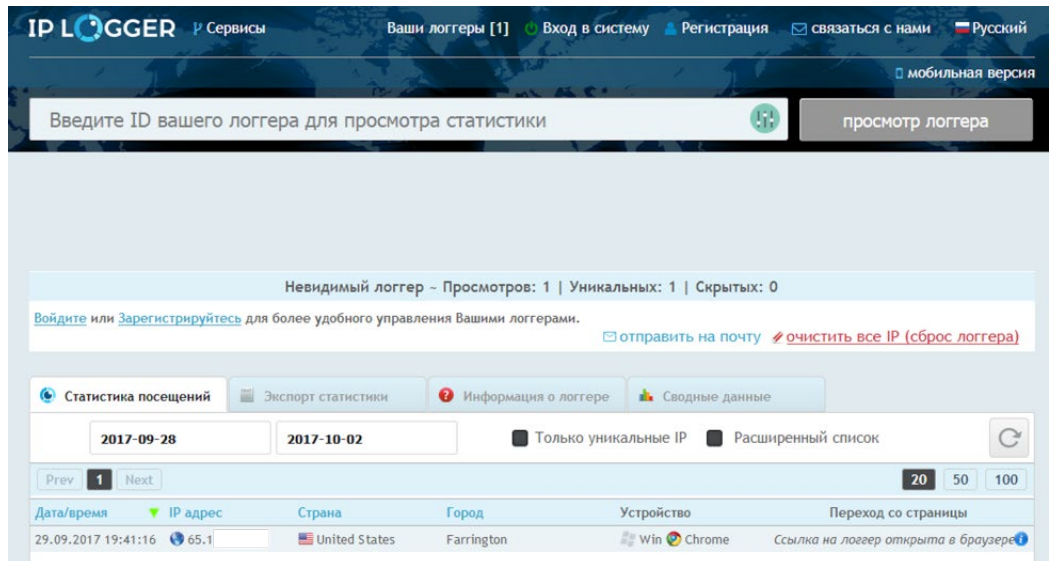
When the bot payload registers with the control panel, a pattern in the registration URL, which can be used to detect infections within the user's network, can be observed. The pattern is `http://Domain.com/cmd.php?hwid=VolumeSerialNumber` where the VolumeSerialNumber is taken from the victim's system and used as the unique ID within the control panel.

Note: "cmd.php?timeout=" appears to be another string to capture the heartbeat between the panel and the bot.

Another more generic way of finding miners on a network is to look for systems communicating to popular servers such as nicehash[.]com and minergate[.]com. This is particularly helpful when miners do not utilize a control panel for the reasons described above.

In some cases, variants without bot modules and C2 support will be utilizing readily available [https://iplogger\[.\]ru](https://iplogger[.]ru) service to maintain minimum visibility into the infected network.

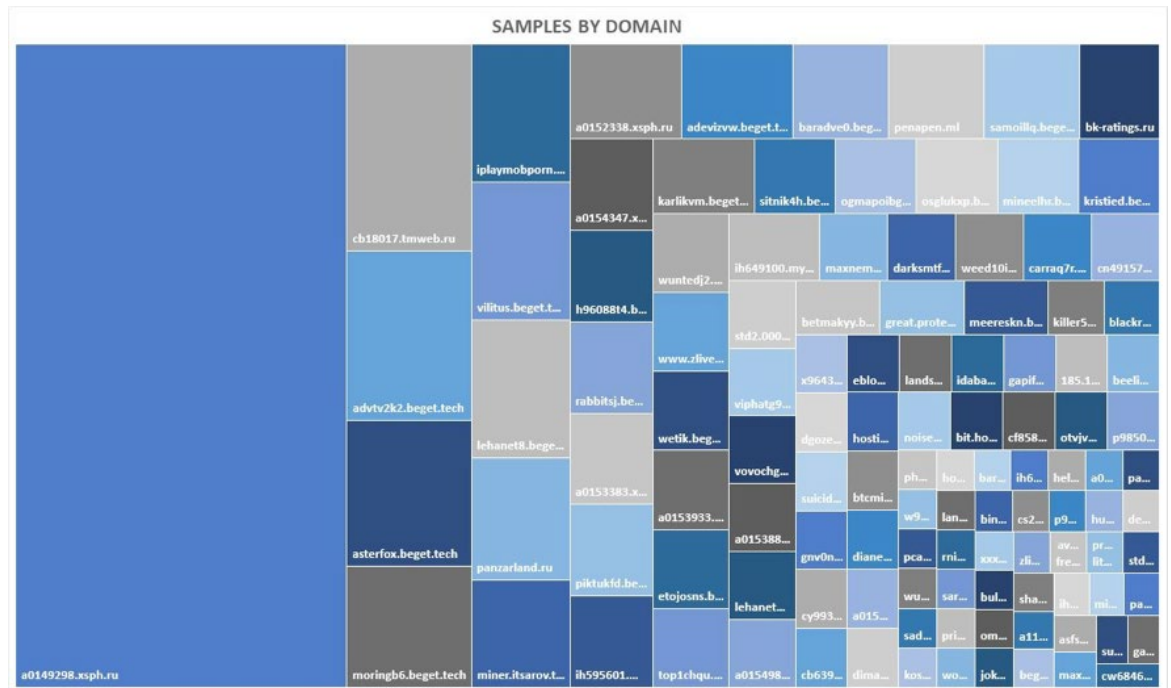
Operated by Russian-speaking owners, the service allows anyone to add various user tracking mechanisms to monitor controlled web resources and applications.



IPLogger control panel displaying the data collected from monitored users.

Hunt for Indicators

Using the above information, we queried VirusTotal for all samples that have HTTP traffic containing “cmd.php?hwid=” and found 487 unique samples communicating to 114 different control panels. Interestingly enough 29% of the samples tied back to one specific domain: a0149298.xsph.ru.




```
ETH: 08/15/17-00:16:44 - New job from eu1.ethermine.org:4444
ETH - Total Speed: 30.829 Mh/s, Total Shares: 681, Rejected: 0, Time: 24:19
ETH: GPU0 30.829 Mh/s
GPU0 t=71C fan=71%
ETH: 08/15/17-00:17:24 - New job from eu1.ethermine.org:4444
ETH - Total Speed: 30.767 Mh/s, Total Shares: 681, Rejected: 0, Time: 24:20
ETH: GPU0 30.767 Mh/s
GPU0 t=71C fan=71%
ETH: 08/15/17-00:17:43 - New job from eu1.ethermine.org:4444
ETH - Total Speed: 30.835 Mh/s, Total Shares: 681, Rejected: 0, Time: 24:20
ETH: GPU0 30.835 Mh/s
GPU0 t=71C fan=71%
ETH: 08/15/17-00:18:11 - New job from eu1.ethermine.org:4444
ETH - Total Speed: 30.911 Mh/s, Total Shares: 681, Rejected: 0, Time: 24:21
ETH: GPU0 30.911 Mh/s
ETH: 08/15/17-00:18:17 - New job from eu1.ethermine.org:4444
ETH - Total Speed: 30.806 Mh/s, Total Shares: 681, Rejected: 0, Time: 24:21
ETH: GPU0 30.806 Mh/s
GPU0 t=71C fan=71%
ETH: 08/15/17-00:18:40 - SHARE FOUND - (GPU 0)
ETH: Share accepted (63 ms)!
ETH: 08/15/17-00:18:43 - New job from eu1.ethermine.org:4444
ETH - Total Speed: 30.959 Mh/s, Total Shares: 682, Rejected: 0, Time: 24:21
ETH: GPU0 30.959 Mh/s
GPU0 t=71C fan=71%
ETH: 08/15/17-00:19:06 - SHARE FOUND - (GPU 0)
ETH: Share accepted (62 ms)!
ETH: 08/15/17-00:19:17 - SHARE FOUND - (GPU 0)
ETH: Share accepted (63 ms)!
ETH: 08/15/17-00:19:19 - New job from eu1.ethermine.org:4444
ETH - Total Speed: 31.179 Mh/s, Total Shares: 684, Rejected: 0, Time: 24:22
ETH: GPU0 31.179 Mh/s
GPU0 t=71C fan=71%
GPU0 t=71C fan=72%
ETH: 08/15/17-00:19:55 - New job from eu1.ethermine.org:4444
ETH - Total Speed: 31.204 Mh/s, Total Shares: 684, Rejected: 0, Time: 24:22
ETH: GPU0 31.204 Mh/s
ETH: 08/15/17-00:20:01 - New job from eu1.ethermine.org:4444
```

Real-time mining statistics report, access to which was identified during malware sample analysis.

Open Source Samples

In some instances we identified chatter among criminal actors, concluding that open source mining projects are being actively used in development of malicious mining software. One such project is known as “cpuminer-multi” and is readily available on [GitHub](#).

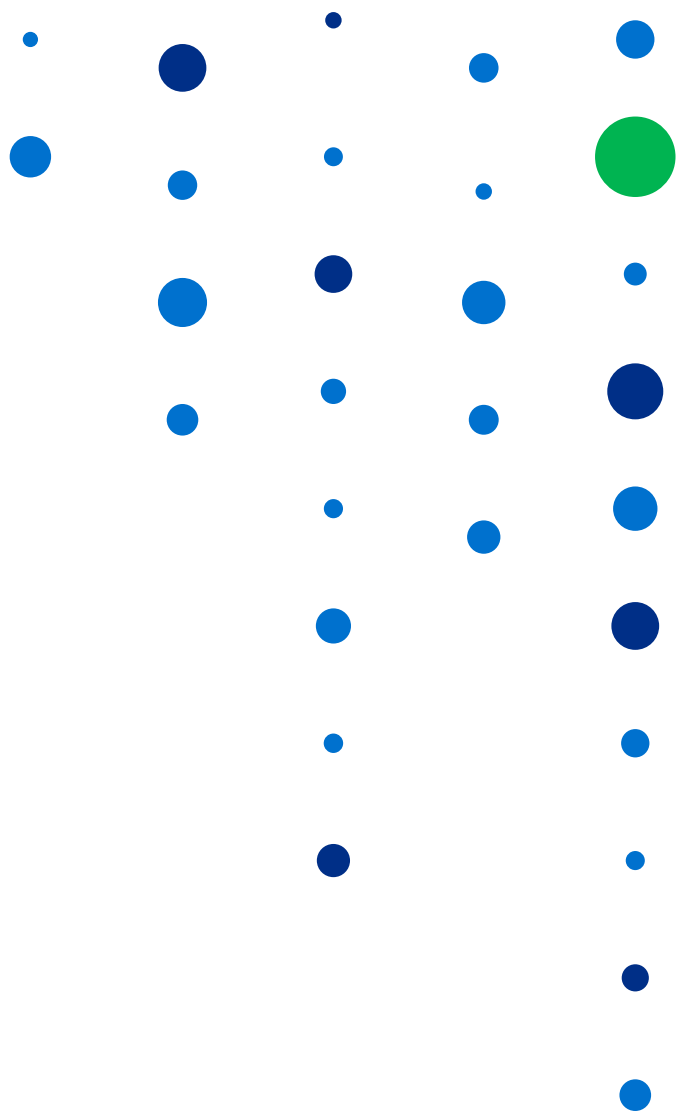
Outlook

In the immediate future, we don't foresee mining malware overtaking ransomware in terms of inflicted infrastructure damages nor monetary gains to its operators. However, for the first time in the last two years, we are seeing a shift in cybercriminal mentality and a growing skepticism for widespread ransomware campaigns. As international law enforcement shows exceptional determination, successfully dismantling several high-profile marketplaces and arresting longtime members of the criminal underground, malicious actors are willing to accept less lucrative, but almost risk-free business models.

Aside from lone criminals, with the same likelihood, we estimate North Korean persistent threat groups to exhibit an utmost interest in cryptocurrency mining. Deprived of reliable cash-flow, the oppressive state will explore every opportunity to provide finance to the ruling regime.

Almost unilaterally the entire list of malware we have researched will take advantage of publicly available mining pools, with [minergate\[.\]com](#) and [nicehash\[.\]com](#) being the preferred choice of criminals. However, several vendors indicated that if a buyer anticipates a very significant level of installations, an independently owned pool is preferred, and even offering their assistance in setting one up. By monitoring network traffic calling any of the known mining pools is a simple and effective method of identification of rogue mining processes.

[Indicators Appendix](#)



 www.recordedfuture.com

 @RecordedFuture

About Recorded Future

Recorded Future arms security teams with threat intelligence powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context that's delivered in real time and packaged for human analysis or instant integration with existing security technology.

© Recorded Future, Inc. All rights reserved. All trademarks remain property of their respective owners.