5.1挖矿密码概述

挖矿的英语为Mining，早期主要与比特币相关。用户使用个人计算机下载软件，然后运行特定算法，与远方服务器通信后可得到相应比特币。挖矿就是利用比特币挖矿机赚取比特币。挖矿木马是利用各种方法入侵计算机，利用被入侵计算机的算力挖掘加密数字货币以牟取利益的木马。其既可以是一段自动化扫描、攻击的脚本，也可以集成在单个可执行文件中。挖矿木马为了能够长期在服务器中驻留，会采用多种安全对抗技术，如修改任务计划、修改防火墙配置、修改系统动态链接库等，使用这些技术手段严重时可能造成服务器业务中断。

挖矿木马传播方法：

1）利用漏洞传播

2）利用弱密码暴力破解传播

3）通过僵尸网络传播

4）采用无文件攻击方法传播

5）利用网页挂马传播

6）利用软件供应链攻击传播

7）利用社交软件、邮件传播

8）内部人员私自安装挖矿程序

挖矿木马利用的常见漏洞：

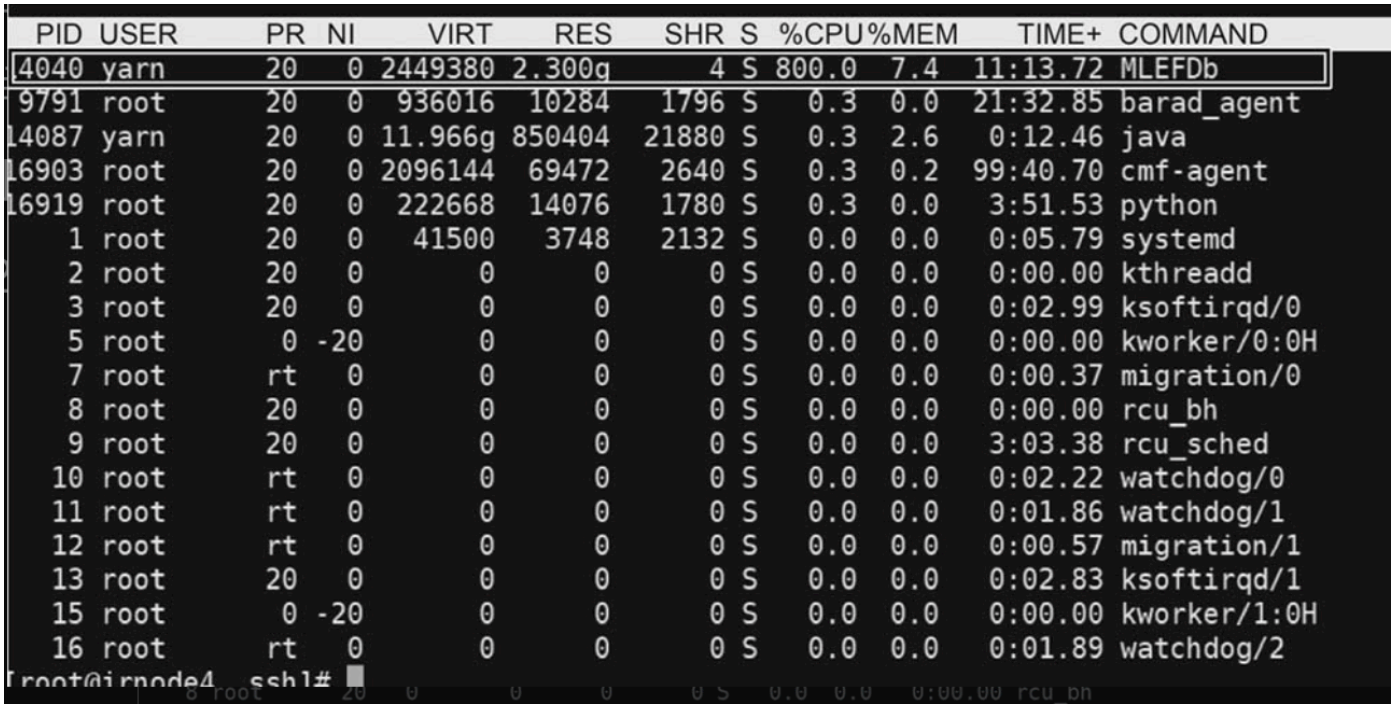
攻 击 平 台	漏 洞 编 号
Struts2	CVE-2017-5638
	CVE-2017-9805
	CVE-2018-11776
ThinkPHP	-（ThinkPHPv5 GetShell）
Windows Server	-（弱密码暴力破解）
	CVE-2017-0143
PHPStudy	-（弱密码暴力破解）
PHPMyAdmin	-（弱密码暴力破解）
MySQL	-（弱密码暴力破解）
Spring Data Commons	CVE-2018-1273
Tomcat	-（弱密码暴力破解）
	CVE-2017-12615
MsSQL	-（弱密码暴力破解）
Jekins	CVE-2019-1003000
JBoss	CVE-2010-0738
	CVE-2017-12149

应　　用	漏 洞 名 称
Docker	Docker 未授权漏洞
Nexus Repository	Nexus Repository Manager 3 远程代码执行漏洞
ElasticSearch	ElasticSearch 未授权漏洞
Hadoop Yarn	Hadoop Yarn REST API 未授权漏洞
Kubernetes	Kubernetes API Server 未授权漏洞
Jenkins	Jenkins RCE（CVE-2019-1003000）
Spark	Spark REST API 未授权漏洞

5.2常规处置方法

1）查看系统实时运行状态：

```
top
```



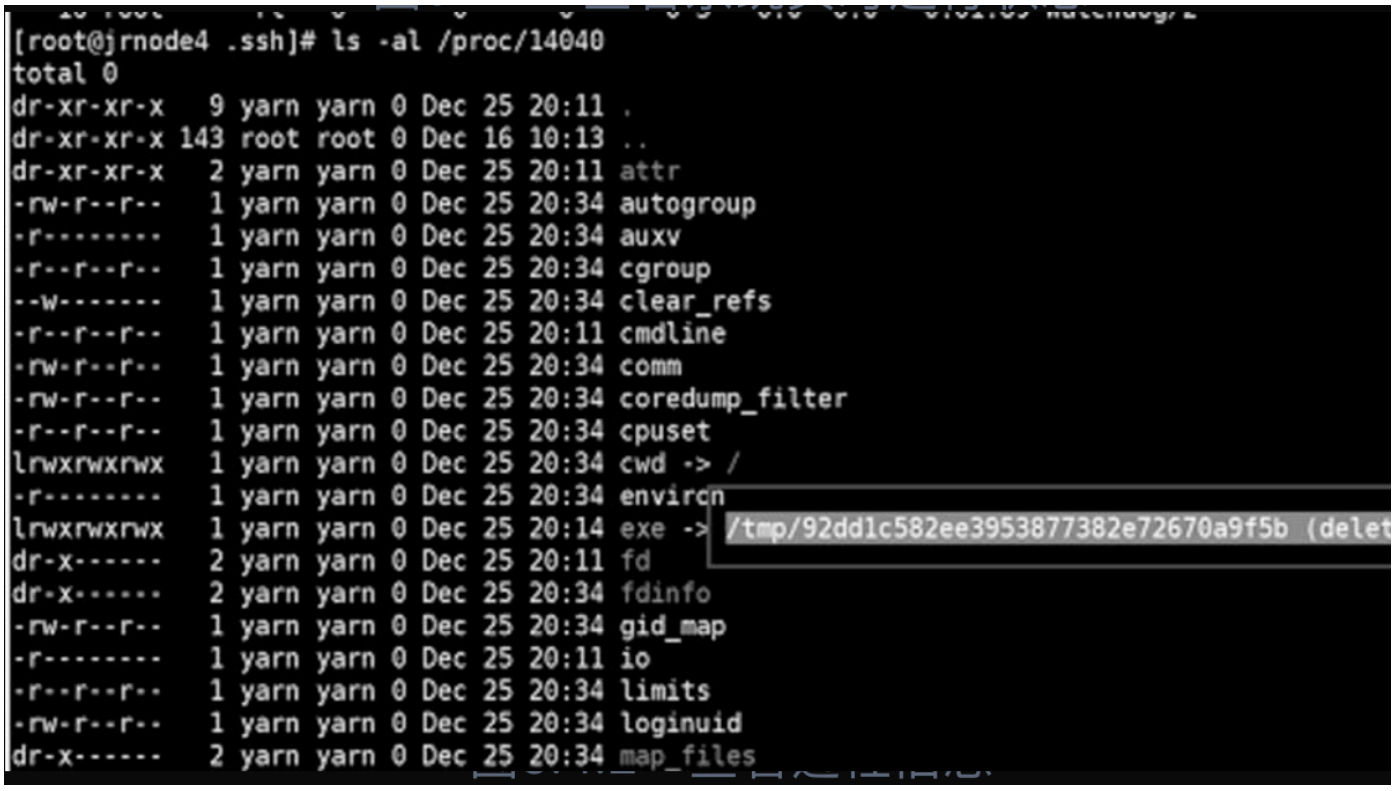
PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
14040	yarn	20	0	2449380	2.300g	4	S	800.0	7.4	11:13.72	MLEFDb
9791	root	20	0	936016	10284	1796	S	0.3	0.0	21:32.85	barad_agent
14087	yarn	20	0	11.966g	850404	21880	S	0.3	2.6	0:12.46	java
16903	root	20	0	2096144	69472	2640	S	0.3	0.2	99:40.70	cmf-agent
16919	root	20	0	222668	14076	1780	S	0.3	0.0	3:51.53	python
1	root	20	0	41500	3748	2132	S	0.0	0.0	0:05.79	systemd
2	root	20	0	0	0	0	S	0.0	0.0	0:00.00	kthreadd
3	root	20	0	0	0	0	S	0.0	0.0	0:02.99	ksoftirqd/0
5	root	0	-20	0	0	0	S	0.0	0.0	0:00.00	kworker/0:0H
7	root	rt	0	0	0	0	S	0.0	0.0	0:00.37	migration/0
8	root	20	0	0	0	0	S	0.0	0.0	0:00.00	rcu_bh
9	root	20	0	0	0	0	S	0.0	0.0	3:03.38	rcu_sched
10	root	rt	0	0	0	0	S	0.0	0.0	0:02.22	watchdog/0
11	root	rt	0	0	0	0	S	0.0	0.0	0:01.86	watchdog/1
12	root	rt	0	0	0	0	S	0.0	0.0	0:00.57	migration/1
13	root	20	0	0	0	0	S	0.0	0.0	0:02.83	ksoftirqd/1
15	root	0	-20	0	0	0	S	0.0	0.0	0:00.00	kworker/1:0H
16	root	rt	0	0	0	0	S	0.0	0.0	0:01.89	watchdog/2

[root@jrnode4 .ssh]#

2）定位恶意进程，上图进程14040CPU占用率过高，确定为恶意进程

3）查看进程信息

```
ls -al /proc/PID
```



```
[root@jrnode4 .ssh]# ls -al /proc/14040
total 0
dr-xr-xr-x   9 yarn yarn 0 Dec 25 20:11 .
dr-xr-xr-x 143 root root 0 Dec 16 10:13 ..
dr-xr-xr-x   2 yarn yarn 0 Dec 25 20:11 attr
-rw-r--r--   1 yarn yarn 0 Dec 25 20:34 autogroup
-r--------   1 yarn yarn 0 Dec 25 20:34 auxv
-r--r--r--   1 yarn yarn 0 Dec 25 20:34 cgroup
--w-------   1 yarn yarn 0 Dec 25 20:34 clear_refs
-r--r--r--   1 yarn yarn 0 Dec 25 20:11 cmdline
-rw-r--r--   1 yarn yarn 0 Dec 25 20:34 comm
-rw-r--r--   1 yarn yarn 0 Dec 25 20:34 coredump_filter
-r--r--r--   1 yarn yarn 0 Dec 25 20:34 cpuset
lrwxrwxrwx   1 yarn yarn 0 Dec 25 20:34 cwd -> /
-r--------   1 yarn yarn 0 Dec 25 20:34 environ
lrwxrwxrwx   1 yarn yarn 0 Dec 25 20:14 exe -> /tmp/92dd1c582ee3953877382e72670a9f5b (delet
dr-x------   2 yarn yarn 0 Dec 25 20:11 fd
dr-x------   2 yarn yarn 0 Dec 25 20:34 fdinfo
-rw-r--r--   1 yarn yarn 0 Dec 25 20:34 gid_map
-r--------   1 yarn yarn 0 Dec 25 20:11 io
-r--r--r--   1 yarn yarn 0 Dec 25 20:34 limits
-rw-r--r--   1 yarn yarn 0 Dec 25 20:34 loginuid
dr-x------   2 yarn yarn 0 Dec 25 20:34 map_files
```

4)结束恶意进程、删除恶意文件

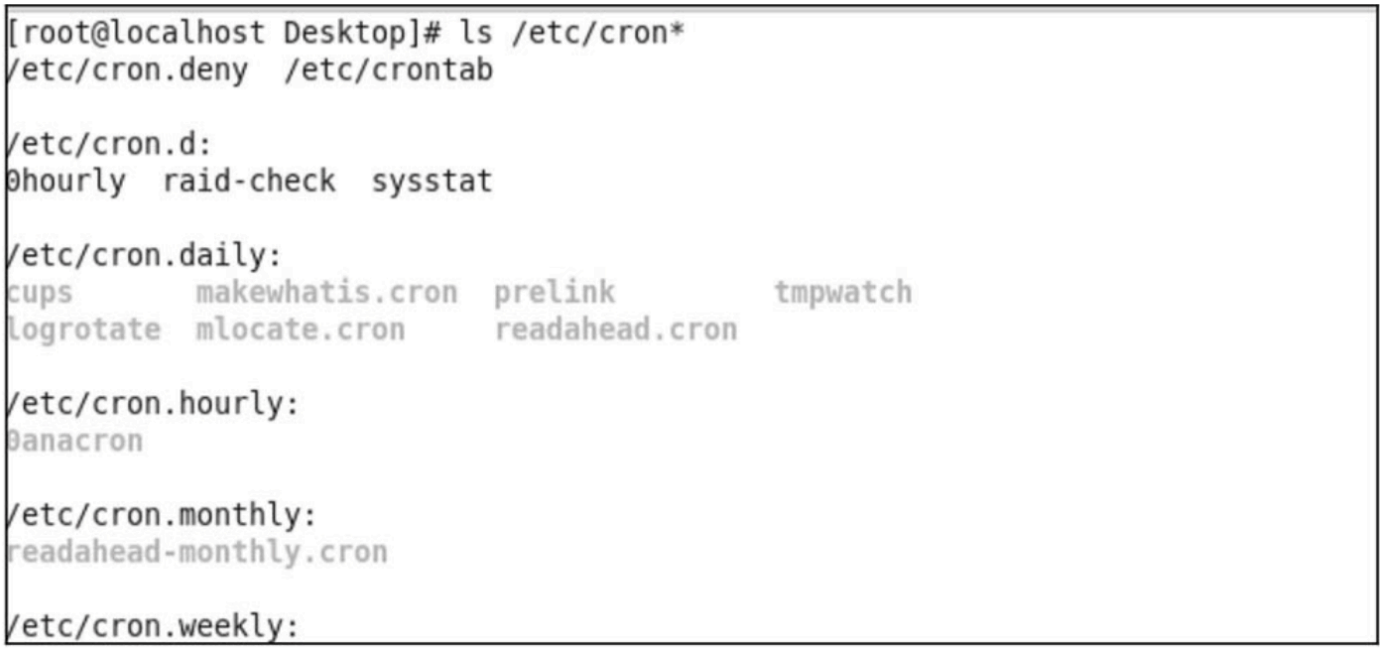
```
kill -9 PID
```

```
rm -rf fileName(文件夹名或者文件名都行)
```

5）查看是否有定时任务并删除

```
crontabl -l 查看当前用户的定时任务
crontab -u user -l 查看用户名为user的定时任务
crontab -r 删除所有的定时任务，如果只想删除特定的定时任务，可以删除定时任务文件中的对应行
```

一般在Linux系统中的任务计划文件是以cron开头的，可以利用正则表达式的*筛选出etc目录下的所有以cron开头的文件，具体表达式为/etc/cron*。例如，查看etc目录下的所有任务计划文件就可以输入【ls /etc/cron*】命令，如图所示：



crontab文件的含义：用户所建立的crontab文件中，每一行都代表一项任务，每行的每个字段代表一项设置，它的格式共分为六个字段，前五段是时间设定段，第六段是要执行的命令段，格式如下：

```
minute   hour   day   month   week   command     顺序：分 时 日 月 周
```

其中：

- minute： 表示分钟，可以是从0到59之间的任何整数。
- hour：表示小时，可以是从0到23之间的任何整数。
- day：表示日期，可以是从1到31之间的任何整数。
- month：表示月份，可以是从1到12之间的任何整数。
- week：表示星期几，可以是从0到7之间的任何整数，这里的0或7代表星期日。
- command：要执行的命令，可以是系统命令，也可以是自己编写的脚本文件。

在以上各个字段中，还可以使用以下特殊字符：

- 星号（*）：代表所有可能的值，例如month字段如果是星号，则表示在满足其它字段的制约条件后每月都执行该命令操作。
- 逗号（,）：可以用逗号隔开的值指定一个列表范围，例如，“1,2,5,7,8,9”
- 中杠（-）：可以用整数之间的中杠表示一个整数范围，例如“2-6”表示“2,3,4,5,6”
- 正斜线（/）：可以用正斜线指定时间的间隔频率，例如“0-23/2”表示每两小时执行一次。同时正斜线可以和星号一起使用，例如*/10，如果用在minute字段，表示每十分钟执行一次。