ERT Threat Alert
ADB Miner: A New Botnet Surfaces
February 6, 2018

Abstract

Radware's Emergency Response Team has been monitoring the emergence of a new botnet this week. The ADB.miner malware takes advantage of Android-based devices that expose debug capabilities to the Internet. When a remote host exposes its Android Debug Bridge (ADB) control port, any Android emulator on the Internet has full install, start, reboot and root shell access without authentication. Part of the malware, xmrig binaries (Monero cryptocurrency miners) are executing on the devices.


```
root@dolphin-fvd-p1:/data/local/tmp # ls -la
-rwxr-xr-x root     root       466048 2018-02-03 00:20 bot.dat
-rwxr-xr-x root     root           10 2018-02-04 02:51 botsuinit_1_1.txt
-rwxr-xr-x root     root         1981 2018-02-04 02:50 config.json
-rwxr-xr-x root     root       169624 2018-02-04 02:50 droidbot
-rw-rw-rw- root     root        46526 2018-02-04 02:50 droidbot.apk
-rw------- root     root            0 2018-02-06 05:17 ip.dat
-rwxr-xr-x root     root       153208 2018-02-04 02:50 nohup
-rwxr-xr-x root     root       165528 2018-02-02 22:36 sss
-rwxr-xr-x root     root       588348 2018-02-04 02:50 xmrig32
-rwxr-xr-x root     root       440592 2018-02-04 02:50 xmrig64
```

Figure 1: Malware binaries

Based on the information from the Radware Deception Network, a multitude of devices are impacted by this new malware, including but not limited to, mobile phones, media players and smart TVs. Netlab360 recently published a detailed analysis and coined the name ADB.miner.

Background

Radware's Deception Network algorithms detected a significant increase of activity against port 5555, both in number of hits and in number of distinct IPs. Port 5555 is one of the known ports used by TR069/064 exploits such as witnessed during the attack on Deutsche Telekom using a Mirai-based malware in November, 2016. In this case, the payload delivered to the port was not SOAP/HTTP but the ADB remote debugging protocol.

Bot User Tools

Getting root shell access using Android SDK platform tools:

```
C:\bin\android-platform-tools\platform-tools>adb shell "id" <victim_ip>
                        uid=0(root) gid=0(root)
```

All ADB connections start with the CNXN fixed string, matching the pattern intercepted by Radware's honeypots:

- `0000000: 43 4e 58 4e 00 00 00 01 00 10 00 00 07 00 00 00  CNXN`
- `0000010: 32 02 00 00 bc b1 a7 b1 68 6f 73 74 3a 3a 00     2.......host`

Commands performed against a target device:

- `{ name: "adb"; service: "adb"; host: "100.115.92.2"; port: "5555"; probe: [ "^CNXN" ]; }`

The Monero wallet address that collects the return on the mining investment is 44XT4KvmobTQfeWa6PCQF5RDosr2MLWm43AsaE3o5iNRXXTfDbYk2VPHTVedTQHZyfXNzMn8YYF2466d3FSDT7gJS8gdHAr.

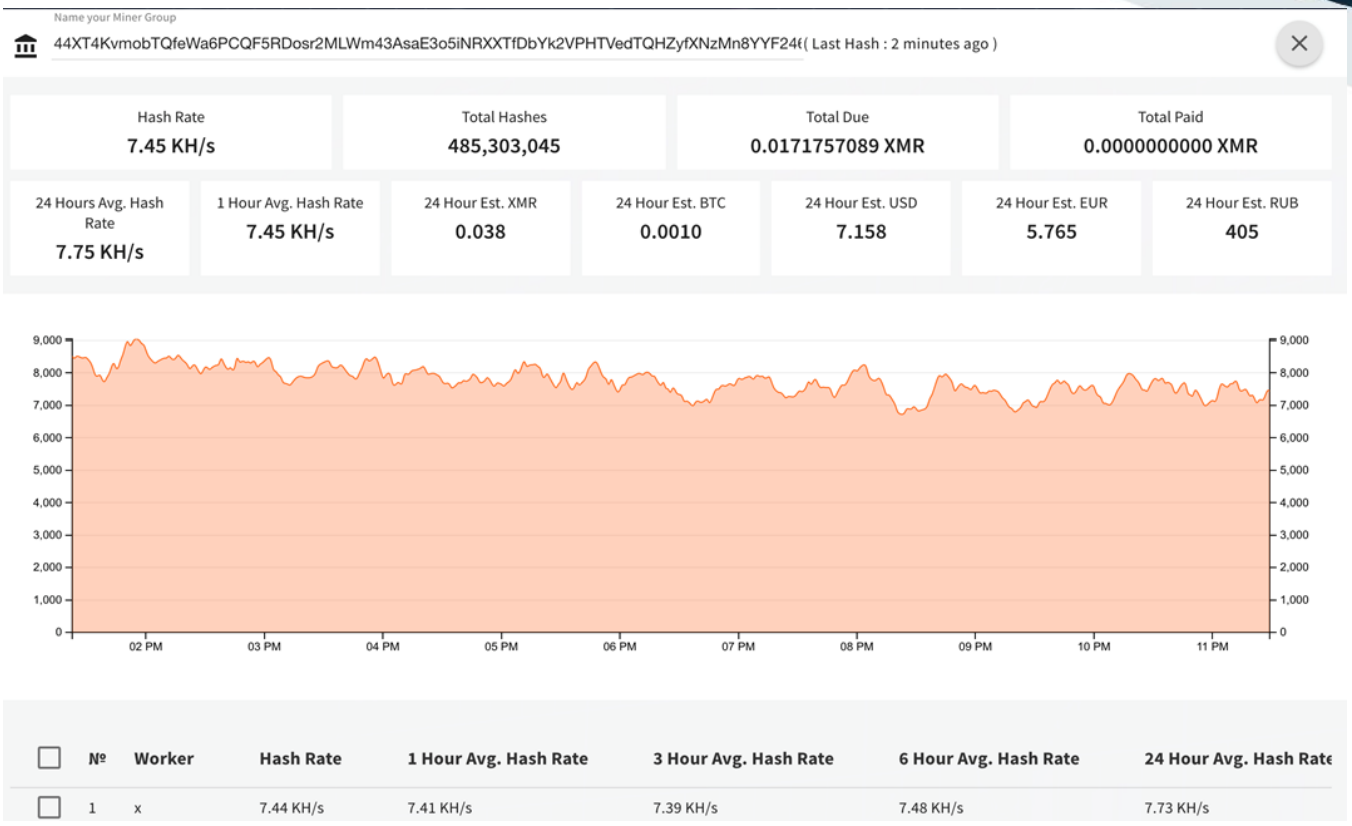

Figure 2: Monero miner

Even if the mining effort is not returning large amounts for hackers, the thread is spreading globally and impacting the infected devices in terms of CPU resources and power consumed.

Hashes/IOC

- 91f0ffdec958388adab53b5a473265d7ce86d0a3da4622490c9199baecce31b8 xmrig32
- a881b27c388448cf9d77443ea23be4d751b3b565b773e1d97a7dbb0702189812 xmrig64
- 940b47e9b71ba4968cfefd7ae6c374a319f2439e9b71ee0965e20a0ce00dcd67 droidbot
- 6b973256325b0f93c45a1ae8a964218b6c86aa3c509453f0325754eb2dcfef0e droidbot.apk

Effective DDoS Protection Essentials

- **Hybrid DDoS Protection** - On-premise and cloud DDoS protection for real-time DDoS attack prevention that also addresses high volume attacks and protects from pipe saturation
- **Behavioral-Based Detection** - Quickly and accurately identify and block anomalies while allowing legitimate traffic through
- **Real-Time Signature Creation** - Promptly protect from unknown threats and zero-day attacks
- **A Cyber-Security Emergency Response Plan** - A dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks
- **Intelligence on Active Threat Actors** – high fidelity, correlated and analyzed date for preemptive protection against currently active known attackers.

For further network and application protection measures, Radware urges companies to inspect and patch their network in order to defend against risks and threats.

Under Attack and in Need of Emergency Assistance? Radware Can Help

Radware offers a service to help respond to security emergencies, neutralize the risk and better safeguard operations before irreparable damages occur. If you're under DDoS attack or malware outbreak and in need of emergency assistance, contact us with the code "Red Button."

Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.