MineSweeper: An In-depth Look into Drive-by Mining and its Defense

Radhesh Krishnan Konoth, Emanuele Vineti, Veelasha Moonsamy, Martina Lindorfer, Christopher Kruegel, Herbert Bos and Giovanni Vigna.
2017: The year of cryptocurrencies
Brought a new cyberthreat: Cryptojacking

Cryptojacking Displaces Ransomware As Most Popular Cyberthreat

Ads don't work so websites are using your electricity to pay the bills

Cryptojacking attacks surge against enterprise cloud environments

January’s Most Wanted Malware: Cryptomining Malware Continues to Cripple Enterprise CPU Power
Motivation

- Drive-by mining a.k.a cryptojacking
  - A web-based attack to steal computation power and electricity from visitors
Motivation

- Drive-by mining a.k.a cryptojacking
  - A web-based attack to steal computation power and electricity from visitors
  - ... to mine cryptocurrency
Motivation

● Drive-by mining a.k.a cryptojacking
  ○ A web-based attack to steal computation power and electricity from visitors
  ○ … to mine cryptocurrency

● Why is it bad?
Motivation

- Drive-by mining a.k.a cryptojacking
  - A web-based attack to steal computation power and electricity from visitors
  - ... to mine cryptocurrency

- Why is it bad?
  - No consent
Motivation

- Drive-by mining a.k.a cryptojacking
  - A web-based attack to steal computation power and electricity from visitors
  - … to mine cryptocurrency

- Why is it bad?
  - No consent
  - System performance
Motivation

• Drive-by mining a.k.a cryptojacking
  ○ A web-based attack to steal computation power and electricity from visitors
  ○ … to mine cryptocurrency

• Why is it bad?
  ○ No consent
  ○ System performance
  ○ Power consumption
Motivation

- Drive-by mining a.k.a cryptojacking
  - A web-based attack to steal computation power and electricity from visitors
  - … to mine cryptocurrency

- Why is it bad?
  - No consent
  - System performance
  - Power consumption
  - Longevity of the device
Existing defenses

CPU Usage Heuristics
Existing defenses

CPU Usage Heuristics

URL Blacklists
Existing defenses

- **CPU Usage Heuristics**
- **URL Blacklists**

Easily defeated by:
- CPU throttling
- URL randomization
Contributions

1. In-depth study of this cyberthreat
Contributions

1. In-depth study of this cyberthreat
   - Analyzing Alexa’s top 1 million websites
Contributions

1. In-depth study of this cyberthreat
   - Analyzing Alexa’s top 1 million websites
     - 1735 drive-by mining websites
     - 20 active campaigns
     - CryptoNight-based cryptocurrencies
Contributions

1. In-depth study of this cyberthreat
   - Analyzing Alexa’s top 1 million websites
     - 1735 drive-by mining websites
     - 20 active campaigns
     - CryptoNight-based cryptocurrencies

2. Proposes a better detection tool: MineSweeper
Catalysts of drive-by mining

1. Advent of privacy-focused, and CPU mineable cryptocurrencies
Catalysts of drive-by mining

1. Advent of privacy-focused, and CPU mineable cryptocurrencies

CryptoNight (PoW)
Catalysts of drive-by mining

1. Advent of privacy-focused, and CPU mineable cryptocurrencies

2. Advanced web technologies:
   - asm.js (2013)
Catalysts of drive-by mining

1. Advent of privacy-focused, and CPU mineable cryptocurrencies

2. Advanced web technologies:
   - asm.js (2013)
   - WebAssembly aka WASM (2017)
In-browser mining services

In 2017, Coinhive miner is launched:

- Provides JavaScript API to mine a cryptocurrency Monero:

```html
<script src="https://coinhive.com/lib/coinhive.min.js"></script>
<script>
    var miner = new CoinHive.Anonymous('CLIENT-ID',
        {throttle: 0.9});

    miner.start();
</script>
```

Orchestrator Code
In-browser mining services

In 2017, Coinhive miner is launched:

- Provides JavaScript API to mine a cryptocurrency Monero:

```html
<script src="https://coinhive.com/lib/coinhive.min.js"></script>
<script>
  var miner = new CoinHive.Anonymous('CLIENT-ID',
                                       {throttle: 0.9});

  miner.start();
</script>
```
In-browser mining services

In 2017, Coinhive miner is launched:

- Provides JavaScript API to mine a cryptocurrency Monero:

```html
<script src="https://coinhive.com/lib/coinhive.min.js"></script>
<script>
  var miner = new CoinHive.Anonymous(CLIENT_ID,
    {throttle: 0.9});
  miner.start();
</script>
```

Orchestrator Code
Lead to proliferation of in-browser mining services

FREE JavaScript Mining - Browser Mining
Use our Monero JavaScript Web Miner and EARN MONEY with your page traffic!

Online cryptocurrency miner

NF WebMiner: a simple web mining service

35,904 Registered Users

Monetize your web!

Earn More From Your Visitors

Start collecting more money from your website or app in minutes.
An interesting drive-by mining case
An interesting drive-by mining case
An interesting drive-by mining case
An interesting drive-by mining case
Threat model: Drive-by mining
Threat model: Drive-by mining

User

No consent

HTTP Request
HTTP Response (Orchestrator Code)
Fetch Mining Payload

Webserver
Webserver/External Server

WebSocket Proxy

Mining Pool

Relay Communication

Mining pool Communication
Threat model: Drive-by mining

User

HTTP Request
HTTP Response
(Orchestrator Code)
Fetch Mining Payload

Webserver

No consent

In-browser mining service

Webserver/External Server

Mining pool
Communication

WebSocket
Proxy

Relay
Communication

Mining Pool
Threat model: Drive-by mining
Threat model: Drive-by mining
Part 1: In-depth analysis

Studied Alexa’s top 1 million websites to understand:
Part 1: In-depth analysis

Studied Alexa’s top 1 million websites to understand:

1. How **prevalent** is drive-by mining in the wild?
Part 1: In-depth analysis

Studied Alexa’s top 1 million websites to understand:

1. How **prevalent** is drive-by mining in the wild?

2. Which **evasion** tactics do drive-by mining services employ?
Part 1: In-depth analysis

Studied Alexa’s top 1 million websites to understand:

1. How **prevalent** is drive-by mining in the wild?

2. Which **evasion** tactics do drive-by mining services employ?

3. How much **profit** do these websites make?
Part 1: In-depth analysis

Studied Alexa’s top 1 million websites to understand:

1. How prevalent is drive-by mining in the wild?
2. Which evasion tactics do drive-by mining services employ?
3. How much profit do these websites make?
4. Are there any drive-by mining campaigns?
Part 1: In-depth analysis

Studied Alexa’s top 1 million websites to understand:

1. How prevalent is drive-by mining in the wild?
2. Which evasion tactics do drive-by mining services employ?
3. How much profit do these websites make?
4. Are there any drive-by mining campaigns?
5. What are the common characteristics across different drive-by mining services?
Data collection

Alexa top 1 million websites (Mid-March 2018)
Data collection

Alexa top 1 million websites (Mid-March 2018)

Crawler configuration:

- Crawled 3 internal pages
Data collection

Alexa top 1 million websites (Mid-March 2018)

Crawler configuration:

- Crawled 3 internal pages
- Visited a page for only 4 seconds
Data collection

Alexa top 1 million websites (Mid-March 2018)

Crawler configuration:

- Crawled 3 internal pages
- Visited a page for only 4 seconds
- Did not simulate any interaction, i.e. the crawler did not give any consent for cryptomining.
Large-scale Analysis: Experiment Set-Up
Large-scale Analysis: Experiment Set-Up
Large-scale Analysis: Experiment Set-Up

4.6 TB raw data
Large-scale Analysis: Experiment Set-Up
Detecting Mining Payload (WASM)

'js' : 'cryptonight\WASMWrapper\crytenight\load.jssecin.com\hash_cn',
'wasm' : b'\x00\x61\x73\x6d',
'rwasm' : '.wasm|.wasl|.wsm',

13
Detecting Stratum communication

<table>
<thead>
<tr>
<th>Command</th>
<th>Keywords</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>type:auth</td>
</tr>
<tr>
<td></td>
<td>identifier:handshake</td>
</tr>
<tr>
<td>Authentication accepted</td>
<td>type:authed</td>
</tr>
<tr>
<td>Fetch job</td>
<td>identifier:job</td>
</tr>
<tr>
<td>Submit solved hash</td>
<td>type:submit</td>
</tr>
<tr>
<td>Solution accepted</td>
<td>command:accepted</td>
</tr>
<tr>
<td>Set CPU limits</td>
<td>command:set_cpu_load</td>
</tr>
</tbody>
</table>
1. Prevalence of drive-by mining

<table>
<thead>
<tr>
<th>Crawling period</th>
<th>March 12, 2018 – March 19, 2018</th>
</tr>
</thead>
<tbody>
<tr>
<td># websites crawled</td>
<td>991,513</td>
</tr>
<tr>
<td># drive-by mining websites</td>
<td>1,735</td>
</tr>
</tbody>
</table>
2. Evasion techniques

Code obfuscation on orchestrator code:

- Packed code, CharCode, Name obfuscation, Dead code injection, URL randomization
2. Evasion techniques

Code obfuscation on orchestrator code:
  ○ Packed code, CharCode, Name obfuscation, Dead code injection, URL randomization

Encoded Stratum Communication: 174 websites
2. Evasion techniques

Code obfuscation on orchestrator code:

- Packed code, CharCode, Name obfuscation, Dead code injection, URL randomization

Encoded Stratum Communication : 174 websites

Anti-debugging tricks : 139 websites
2. Evasion techniques

Code obfuscation on orchestrator code:
  - Packed code, CharCode, Name obfuscation, Dead code injection, URL randomization

Encoded Stratum Communication: 174 websites

Anti-debugging tricks: 139 websites

CPU throttling (< 25%) : 12 websites
3. Profit Estimation
3. Profit Estimation

Visitor Statistics from SimilarWeb:
3. Profit Estimation

Visitor Statistics from SimilarWeb:

• Average monthly traffic from Mobile device and Laptop
• Average time spent by visitors
3. Profit Estimation

Visitor Statistics from SimilarWeb:

• Average monthly traffic from Mobile device and Laptop
• Average time spent by visitors

Monero (XMR) value on May 2018 : US$ 253
3. Profit Estimation

Visitor Statistics from SimilarWeb:

• Average monthly traffic from Mobile device and Laptop
• Average time spent by visitors

Monero (XMR) value on May 2018: US$ 253
3. Profit Estimation

Visitor Statistics fromSimilarWeb:

- Average monthly traffic from Mobile device and Laptop
- Average time spent by visitors

Monero (XMR) value on May 2018: US$ 253
3. Profit Estimation

Visitor Statistics from SimilarWeb:

- Average monthly traffic from Mobile device and Laptop
- Average time spent by visitors

Monero (XMR) value on May 2018: US$ 253

Average hashrate:
- Mobile devices: 14.56 h/s
- Laptops: 40.5 h/s
3. Profit distribution of drive-by mining websites

- Most profitable website (tumangaonline.com) : US$ 17,166.97
3. Profit distribution of drive-by mining websites

- Most profitable website (tumangaonline.com): US$ 17,166.97
  
  avg. time : 18 mints
4. Identifying Campaigns

Two valuable pieces of information in the WebSocket frames:
4. Identifying Campaigns

Two valuable pieces of information in the WebSocket frames:

1. Site-Key/ Client ID
4. Campaigns and monthly revenue: Site-key

We discovered 11 campaigns by clustering websites based on site-key:

<table>
<thead>
<tr>
<th>Site Key</th>
<th>#</th>
<th>Main Pool</th>
<th>Type</th>
<th>Profit (US$)</th>
</tr>
</thead>
<tbody>
<tr>
<td>“428347349263284”</td>
<td>139</td>
<td>weline.info</td>
<td>Third party (video)</td>
<td>$31,060.80</td>
</tr>
<tr>
<td>OT1CfcklOCO7yVMxcmqjmqSWoDWOri06</td>
<td>53</td>
<td>coinhive.com</td>
<td>Torrent portals</td>
<td>$8,343.18</td>
</tr>
<tr>
<td>ricewithchicken</td>
<td>32</td>
<td>datasetu.download</td>
<td>Advertisement-based</td>
<td>$1,078.27</td>
</tr>
<tr>
<td>jscustomkey2</td>
<td>27</td>
<td>207.246.88.253</td>
<td>Third party (counter12.com)</td>
<td>$86.98</td>
</tr>
<tr>
<td>CryptoNoter</td>
<td>27</td>
<td>minercry.pt</td>
<td>Advertisement-based</td>
<td>$20.35</td>
</tr>
<tr>
<td>489dJE22mdZ3[..]y4PBWLb4tc1X8ADsu</td>
<td>24</td>
<td>datasetu.download</td>
<td>Compromised websites</td>
<td>$142.40</td>
</tr>
<tr>
<td>first</td>
<td>23</td>
<td>cloudflare.com</td>
<td>Compromised websites</td>
<td>$120.02</td>
</tr>
<tr>
<td>vBaNYz4tVYKV9Q9tZIL0BPGq8rnZE100</td>
<td>20</td>
<td>hemnes.win</td>
<td>Third party (video)</td>
<td>$303.14</td>
</tr>
<tr>
<td>45CQjsiBr46U[..]o2C5uo3u23p5SkMN</td>
<td>17</td>
<td>rand.com.ru</td>
<td>Compromised websites</td>
<td>$306.60</td>
</tr>
<tr>
<td>Tumblr</td>
<td>14</td>
<td>count.im</td>
<td>Third party</td>
<td>$11.31</td>
</tr>
<tr>
<td>ClmAQqOiKXawAMBVzuc51G31uDYdJ8F</td>
<td>12</td>
<td>coinhive.com</td>
<td>Third party (night-skin.com)</td>
<td>$14.36</td>
</tr>
</tbody>
</table>
4. Campaigns and monthly revenue: Site-key

We discovered 11 campaigns by clustering websites based on site-key:

<table>
<thead>
<tr>
<th>Site Key</th>
<th>#</th>
<th>Main Pool</th>
<th>Type</th>
<th>Profit (US$)</th>
</tr>
</thead>
<tbody>
<tr>
<td>“428347349263284”</td>
<td>139</td>
<td>weline.info</td>
<td>Third party (video)</td>
<td>$31,060.80</td>
</tr>
<tr>
<td>OT1ClcpkIOCO7yVMxcJiqmSWoDWOri06</td>
<td>53</td>
<td>coinhive.com</td>
<td>Torrent portals</td>
<td>$8,343.18</td>
</tr>
<tr>
<td>ricewithchicken</td>
<td>32</td>
<td>datasetu.download</td>
<td>Advertisement-based</td>
<td>$1,078.27</td>
</tr>
<tr>
<td>jscustomkey2</td>
<td>27</td>
<td>207.246.88.253</td>
<td>Third party (counter12.com)</td>
<td>$86.98</td>
</tr>
<tr>
<td>CryptoNoter</td>
<td>26</td>
<td>minercry.pt</td>
<td>Advertisement-based</td>
<td>$20.35</td>
</tr>
<tr>
<td>489djE22mdZ3[..]y4PBWLb4tc1X8ADsu</td>
<td>24</td>
<td>datasetu.download</td>
<td>Compromised websites</td>
<td>$142.40</td>
</tr>
<tr>
<td>first</td>
<td>25</td>
<td>cloudflare.com</td>
<td>Compromised websites</td>
<td>$120.02</td>
</tr>
<tr>
<td>vBaNYz4tVYKV9Q9tZil0BPGQ8rnZEL00</td>
<td>20</td>
<td>hemnes.win</td>
<td>Third party (video)</td>
<td>$303.14</td>
</tr>
<tr>
<td>45CQjsiBr46U[..]o2C5uo3u23p5SkMN</td>
<td>17</td>
<td>rand.com.ru</td>
<td>Compromised websites</td>
<td>$306.60</td>
</tr>
<tr>
<td>Tumblr</td>
<td>14</td>
<td>count.im</td>
<td>Third party</td>
<td>$11.31</td>
</tr>
<tr>
<td>ClmAXQqQiKXawAMBVzuc51G31uDYdJ8F</td>
<td>12</td>
<td>coinhive.com</td>
<td>Third party (night-skin.com)</td>
<td>$14.36</td>
</tr>
</tbody>
</table>
4. Campaigns and monthly revenue: Site-key

We discovered 11 campaigns by clustering websites based on site-key:

<table>
<thead>
<tr>
<th>Site Key</th>
<th>#</th>
<th>Main Pool</th>
<th>Type</th>
<th>Profit (US$)</th>
</tr>
</thead>
<tbody>
<tr>
<td>“428347349263284”</td>
<td>139</td>
<td>wecline.info</td>
<td>Third party (video)</td>
<td>$31,060.80</td>
</tr>
<tr>
<td>OT1CIcpkIOCO7yVMxcJiqmSWoDWOri06</td>
<td>53</td>
<td>coinhive.com</td>
<td>Torrent portals</td>
<td>$8,343.18</td>
</tr>
<tr>
<td>ricewithchicken</td>
<td>32</td>
<td>datasetu.download</td>
<td>Advertisement-based</td>
<td>$1,078.27</td>
</tr>
<tr>
<td>jscustomkey2</td>
<td>27</td>
<td>207.246.88.253</td>
<td>Third party (counter12.com)</td>
<td>$86.98</td>
</tr>
<tr>
<td>CryptoNote</td>
<td>27</td>
<td>minercry.pt</td>
<td>Advertisement-based</td>
<td>$20.35</td>
</tr>
<tr>
<td>489djEf2mdZz[...]y4PBWLb4tc1X8ADsu</td>
<td>24</td>
<td>datasetu.download</td>
<td>Compromised websites</td>
<td>$142.40</td>
</tr>
<tr>
<td>first</td>
<td>23</td>
<td>cloudflane.com</td>
<td>Compromised websites</td>
<td>$120.02</td>
</tr>
<tr>
<td>vBaNYz4tVYKV9Q9tZIL0BPGq8rnZEI000</td>
<td>20</td>
<td>hemnes.win</td>
<td>Third party (video)</td>
<td>$303.14</td>
</tr>
<tr>
<td>45CQjsiBr46U[..]o2C5uo3u23p5SkMN</td>
<td>17</td>
<td>rand.com.ru</td>
<td>Compromised websites</td>
<td>$306.60</td>
</tr>
<tr>
<td>tumblr</td>
<td>14</td>
<td>count.im</td>
<td>Third party</td>
<td>$11.31</td>
</tr>
<tr>
<td>ClmAAXQqOiXawAMBVzuc51G31uDYdj8F</td>
<td>12</td>
<td>coinhive.com</td>
<td>Third party (night-skin.com)</td>
<td>$14.36</td>
</tr>
</tbody>
</table>
4. Campaigns and monthly revenue : Site-key

We discovered 11 campaigns by clustering websites based on site-key:

<table>
<thead>
<tr>
<th>Site Key</th>
<th>#</th>
<th>Main Pool</th>
<th>Type</th>
<th>Profit (US$)</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;428347349263284&quot;</td>
<td>139</td>
<td>weline.info</td>
<td>Third party (video)</td>
<td>$31,060.80</td>
</tr>
<tr>
<td>OT1CclqkIOCo7yVMxcJiqmSWoDWOri06</td>
<td>53</td>
<td>coinhive.com</td>
<td>Torrent portals</td>
<td>$8,343.18</td>
</tr>
<tr>
<td>ricewithchicken</td>
<td>32</td>
<td>datasetu.download</td>
<td>Advertisement-based</td>
<td>$1,078.27</td>
</tr>
<tr>
<td>jscustomkey2</td>
<td>27</td>
<td>207.246.88.253</td>
<td>Third party (counter12.com)</td>
<td>$86.98</td>
</tr>
<tr>
<td>CryptoNoter</td>
<td>27</td>
<td>minercry.pt</td>
<td>Advertisement-based</td>
<td>$20.35</td>
</tr>
<tr>
<td>489djE22mdZ3[..]y4PBWLb4tc1X8ADsu</td>
<td>24</td>
<td>datasetu.download</td>
<td>Compromised websites</td>
<td>$142.40</td>
</tr>
<tr>
<td>first</td>
<td>23</td>
<td>cloudflare.com</td>
<td>Compromised websites</td>
<td>$120.02</td>
</tr>
<tr>
<td>vBaNYz4tVYKV9Q9tZL0BPGq8rnZEl00</td>
<td>20</td>
<td>hemnes.win</td>
<td>Third party (video)</td>
<td>$303.14</td>
</tr>
<tr>
<td>45CQjsiBr46U[..]o2C5uo3u23p5SkMN</td>
<td>17</td>
<td>rand.com.ru</td>
<td>Compromised websites</td>
<td>$306.60</td>
</tr>
<tr>
<td>Tumblr</td>
<td>14</td>
<td>count.im</td>
<td>Third party</td>
<td>$11.31</td>
</tr>
<tr>
<td>ClmAQBQoIKXawAMBVzuc51G31uDYdJ8F</td>
<td>12</td>
<td>coinhive.com</td>
<td>Third party (night-skin.com)</td>
<td>$14.36</td>
</tr>
</tbody>
</table>
4. Campaigns and monthly revenue: Site-key

We discovered 11 campaigns by clustering websites based on site-key:

<table>
<thead>
<tr>
<th>Site Key</th>
<th>#</th>
<th>Main Pool</th>
<th>Type</th>
<th>Profit (US$)</th>
</tr>
</thead>
<tbody>
<tr>
<td>“428347349263284”</td>
<td>139</td>
<td>weline.info</td>
<td>Third party (video)</td>
<td>$31,060.80</td>
</tr>
<tr>
<td>OT1CepkIOCO7yVMxcJiqmSWoDWOr06</td>
<td>53</td>
<td>coinhive.com</td>
<td>Torrent portals</td>
<td>$8,343.18</td>
</tr>
<tr>
<td>ricewithchicken</td>
<td>32</td>
<td>datasetu.download</td>
<td>Advertisement-based</td>
<td>$1,078.27</td>
</tr>
<tr>
<td>jscustomkey2</td>
<td>27</td>
<td>207.246.88.253</td>
<td>Third party (counter12.com)</td>
<td>$86.98</td>
</tr>
<tr>
<td>CryptoNoter</td>
<td>27</td>
<td>minercry.pt</td>
<td>Advertisement-based</td>
<td>$20.35</td>
</tr>
<tr>
<td>489djE22mdZ3[..]y4PBWLb4tc1X8ADsu</td>
<td>24</td>
<td>datasetu.download</td>
<td>Compromised websites</td>
<td>$142.40</td>
</tr>
<tr>
<td>first</td>
<td>23</td>
<td>cloudflare.com</td>
<td>Compromised websites</td>
<td>$120.02</td>
</tr>
<tr>
<td>vBaNYz4tvYKV9Q9tZl0BPQg8rnZEl00</td>
<td>20</td>
<td>hemnes.win</td>
<td>Third party (video)</td>
<td>$303.14</td>
</tr>
<tr>
<td>45CQjsiBr46U[..]o2C5uo3u23p5SkMN</td>
<td>17</td>
<td>rand.com.ru</td>
<td>Compromised websites</td>
<td>$306.60</td>
</tr>
<tr>
<td>Tumblr</td>
<td>14</td>
<td>count.im</td>
<td>Third party</td>
<td>$11.31</td>
</tr>
<tr>
<td>C1mAXQqOiKXawAMBVzuc51G31uDYdJ8F</td>
<td>12</td>
<td>coinhive.com</td>
<td>Third party (night-skin.com)</td>
<td>$14.36</td>
</tr>
</tbody>
</table>
4. Campaigns and monthly revenue: Site-key

We discovered 11 campaigns by clustering websites based on site-key:

<table>
<thead>
<tr>
<th>Site Key</th>
<th>#</th>
<th>Main Pool</th>
<th>Type</th>
<th>Profit (US$)</th>
</tr>
</thead>
<tbody>
<tr>
<td>“428347349263284”</td>
<td>139</td>
<td>weline.info</td>
<td>Third party (video)</td>
<td>$31,060.80</td>
</tr>
<tr>
<td>OT1CicpI0CO7yVMxcJiqmSWoDWOri06</td>
<td>53</td>
<td>coinhive.com</td>
<td>Torrent portals</td>
<td>$8,343.18</td>
</tr>
<tr>
<td>ricewithchicken</td>
<td>32</td>
<td>datasecu.download</td>
<td>Advertisement-based</td>
<td>$1,078.27</td>
</tr>
<tr>
<td>jscustomkey2</td>
<td>27</td>
<td>207.246.88.253</td>
<td>Third party (counter12.com)</td>
<td>$86.98</td>
</tr>
<tr>
<td>CryptoNoter</td>
<td>27</td>
<td>minercry.pt</td>
<td>Advertisement-based</td>
<td>$20.35</td>
</tr>
<tr>
<td>489djE22mdZ3[..]y4PBWLb4tc1X8ADsu</td>
<td>24</td>
<td>datasecu.download</td>
<td>Compromised websites</td>
<td>$142.40</td>
</tr>
<tr>
<td>first</td>
<td>23</td>
<td>cloudflare.com</td>
<td>Compromised websites</td>
<td>$120.02</td>
</tr>
<tr>
<td>vBaNYz4tVYKV9Q9tZL0BPQg8rnZEl00</td>
<td>20</td>
<td>hemnes.win</td>
<td>Third party (video)</td>
<td>$303.14</td>
</tr>
<tr>
<td>45CQjsiBr46U[..]o2C5uo3u23p5SkMN</td>
<td>17</td>
<td>rand.com.ru</td>
<td>Compromised websites</td>
<td>$306.60</td>
</tr>
<tr>
<td>Tumblr</td>
<td>14</td>
<td>count.im</td>
<td>Third party</td>
<td>$11.31</td>
</tr>
<tr>
<td>ClmAXQqOiKXawAMBVZuc51G31uDYdJ8F</td>
<td>12</td>
<td>coinhive.com</td>
<td>Third party (night-skin.com)</td>
<td>$14.36</td>
</tr>
</tbody>
</table>
4. Identifying Campaigns

Two valuable pieces of information in the WebSocket frames:

1. Site-Key/ Client ID
4. Identifying Campaigns

Two valuable pieces of information in the WebSocket frames:

1. Site-Key/ Client ID
2. WebSocket Proxy
We discovered 9 campaigns using the proxy aggregation:

<table>
<thead>
<tr>
<th>WebSocket Proxy</th>
<th>#</th>
<th>Type</th>
<th>Profit (US$)</th>
</tr>
</thead>
<tbody>
<tr>
<td>advisorstat.space</td>
<td>63</td>
<td>Advertisement-based</td>
<td>$321.71</td>
</tr>
<tr>
<td>zenoviaexchange.com</td>
<td>37</td>
<td>Advertisement-based</td>
<td>$1,516.08</td>
</tr>
<tr>
<td>stati.bid</td>
<td>20</td>
<td>Compromised websites</td>
<td>$34.94</td>
</tr>
<tr>
<td>staticsfs.host</td>
<td>20</td>
<td>Compromised websites</td>
<td>$384.91</td>
</tr>
<tr>
<td>webmetric.loan</td>
<td>17</td>
<td>Compromised websites</td>
<td>$181.32</td>
</tr>
<tr>
<td>insdrbot.com</td>
<td>7</td>
<td>Third party (video)</td>
<td>$1,689.26</td>
</tr>
<tr>
<td>1q2w3.website</td>
<td>5</td>
<td>Third party (video)</td>
<td>$2,012.90</td>
</tr>
<tr>
<td>streamplay.to</td>
<td>5</td>
<td>Third party (video)</td>
<td>$239.71</td>
</tr>
<tr>
<td>estream.to</td>
<td>4</td>
<td>Third party (video)</td>
<td>$872.72</td>
</tr>
</tbody>
</table>
5. Drive-by mining services commonalities:

1. CryptoNight-based cryptocurrency (Specifically, Monero)
5. Drive-by mining services commonalities:

1. CryptoNight-based cryptocurrency (Specifically, Monero)

2. CryptoNight (PoW) is implemented in **WebAssembly**
5. Drive-by mining services commonalities:

1. CryptoNight-based cryptocurrency (Specifically, Monero)

2. CryptoNight (PoW) is implemented in WebAssembly

3. WebWorker threads
5. Drive-by mining services commonalities:

1. CryptoNight-based cryptocurrency (Specifically, Monero)

2. CryptoNight (PoW) is implemented in WebAssembly

3. WebWorker threads

4. WebSocket
5. Drive-by mining services commonalities:

1. CryptoNight-based cryptocurrency (Specifically, Monero)

2. CryptoNight (PoW) is implemented in WebAssembly

3. WebWorker threads

4. WebSocket
Part II : MineSweeper
CryptoNight Algorithm

- CryptoNight is a proof of work algorithm proposed in 2013
CryptoNight Algorithm

- CryptoNight is a proof of work algorithm proposed in 2013
- We exploit two fundamental characteristics:

  ![Diagram of CryptoNight Algorithm]

  - Keccak 1600-512
  - Key expansion + 10 AES rounds
  - 8 rounds
  - AES Read → Write
  - XOR Read → Write
  - 8bt_MUL
  - 8bt_ADD
  - XOR
  - Keccak-f 1600
  - KEY expansion + 10 AES rounds
  - 8 rounds AES
  - XOR
  - BLAKE-Groestl-Skein hash-select
CryptoNight Algorithm

- CryptoNight is a proof of work algorithm proposed in 2013
- We exploit two fundamental characteristics:
  1. Uses several standard cryptographic functions
CryptoNight Algorithm

- CryptoNight is a proof of work algorithm proposed in 2013

- We exploit two fundamental characteristics:
  1. Uses several standard cryptographic functions
  2. A memory hard algorithm
CryptoNight Algorithm

- CryptoNight is a proof of work algorithm proposed in 2013

- We exploit two fundamental characteristics:
  1. Uses several standard cryptographic functions
  2. A memory hard algorithm
     - 2MB scratchpad (CPU cache)
MineSweeper stage 1

WASM module

MineSweeper

Analyze WASM Module

Result

Groestl, Blake, Keccak, Skein, AES

AES
Analyzing WASM

- Uses WebAssembly Binary Toolkit to translate it to the linear assembly code:

```
(func $f21 (type 1) (param $p0 i32)
  (local $l0 i32) (local $l1 i32)
  ....
  loop ;; label = @1
  get_local $l31
  i64.xor
  ....
  loop ;; label = @2
  get_local $l9
  i32.shl
  ....
```
Analyzing WASM

- Uses WebAssembly Binary Toolkit to translate it to linear assembly code

- Identify functions with cryptographic operations (XOR, shift, and rotate operations) inside loop
Analyzing WASM

Number of loops and cryptographic operations:

- loop
- i32.xor / i64.xor
- i32.shl / i64.shl
- i32.shr_u / i64.shr_u
- i32.shr_s / i64.shr_s
- i32.rotl / i64.rotl
- i32.rotr / i64.rotr
Analyzing WASM

Number of loops and cryptographic operations:

- loop
- i32.xor / i64.xor
- i32.shl / i64.shl
- i32.shr_u / i64.shr_u
- i32.shr_s / i64.shr_s
- i32.rotl / i64.rotl
- i32.rotr / i64.rotr

To identify: Keccak, AES, BLAKE-256, Groestl-256, and Skein-256
Evaluation of CryptoNight detection

- Used `--dump-wasm-module` flag in Chrome to dump the loaded WASM modules
Evaluation of CryptoNight detection

- Used `--dump-wasm-module` flag in Chrome to dump the loaded WASM modules
- Collected 748 WASM samples from Alexa 1 million webpages (only visiting landing page)
Evaluation of CryptoNight detection

- Used --dump-wasm-module flag in Chrome to dump the loaded WASM modules
- Collected 748 WASM samples from Alexa 1 million webpages (only visiting landing page)
- Only 40 unique samples
Evaluation of CryptoNight detection

<table>
<thead>
<tr>
<th># of samples</th>
<th>CryptoNight Primitives Detected</th>
<th>Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>30</td>
<td>Groestl, Blake, Keccak, Skein, AES</td>
<td>Cryptominer</td>
</tr>
<tr>
<td>3</td>
<td>Groestl, Blake, Keccak, Skein</td>
<td>Cryptominer</td>
</tr>
<tr>
<td>3</td>
<td>Groestl, Blake</td>
<td>Cryptominer</td>
</tr>
<tr>
<td>4</td>
<td>----</td>
<td>Benign</td>
</tr>
</tbody>
</table>
### Evaluation of CryptoNight detection

<table>
<thead>
<tr>
<th># of samples</th>
<th>CryptoNight Primitives Detected</th>
<th>Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>30</td>
<td>Groestl, Blake, Keccak, Skein, AES</td>
<td>Cryptominer</td>
</tr>
<tr>
<td>3</td>
<td>Groestl, Blake, Keccak, Skein</td>
<td>Cryptominer</td>
</tr>
<tr>
<td>3</td>
<td>Groestl, Blake</td>
<td>Cryptominer</td>
</tr>
<tr>
<td>4</td>
<td>----</td>
<td>Benign</td>
</tr>
</tbody>
</table>
Evaluation of CryptoNight detection

<table>
<thead>
<tr>
<th># of samples</th>
<th>CryptoNight Primitives Detected</th>
<th>Threat Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>30</td>
<td>Groestl, Blake, Keccak, Skein, AES</td>
<td>Cryptominer</td>
</tr>
<tr>
<td>3</td>
<td>Groestl, Blake, Keccak, Skein</td>
<td>Cryptominer</td>
</tr>
<tr>
<td>3</td>
<td>Groestl, Blake</td>
<td>Cryptominer</td>
</tr>
<tr>
<td>4</td>
<td>----</td>
<td>Benign</td>
</tr>
</tbody>
</table>
Evaluation of CryptoNight detection

<table>
<thead>
<tr>
<th># of samples</th>
<th>CryptoNight Primitives Detected</th>
<th>Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>30</td>
<td>Groestl, Blake, Keccak, Skein, AES</td>
<td>Cryptominer</td>
</tr>
<tr>
<td>3</td>
<td>Groestl, Blake, Keccak, Skein</td>
<td>Cryptominer</td>
</tr>
<tr>
<td>3</td>
<td>Groestl, Blake</td>
<td>Cryptominer</td>
</tr>
<tr>
<td>4</td>
<td>----</td>
<td>Benign</td>
</tr>
</tbody>
</table>
## Evaluation of CryptoNight detection

<table>
<thead>
<tr>
<th># of samples</th>
<th>CryptoNight Primitives Detected</th>
<th>Categorization</th>
</tr>
</thead>
<tbody>
<tr>
<td>30</td>
<td>Groestl, Blake, Keccak, Skein, AES</td>
<td>Cryptominer</td>
</tr>
<tr>
<td>3</td>
<td>Groestl, Blake, Keccak, Skein</td>
<td>Cryptominer</td>
</tr>
<tr>
<td>3</td>
<td>Groestl, Blake</td>
<td>Cryptominer</td>
</tr>
<tr>
<td>4</td>
<td>----</td>
<td>Benign</td>
</tr>
</tbody>
</table>
MineSweeper stage 2

Obfuscated WASM module → MineSweeper
  Analyze WASM Module
  Monitor CPU Cache events

Result

Load events
Store events
MineSweeper stage 2

Obfuscated WASM module

MineSweeper

Analyze WASM Module

Monitor CPU
Cache events

Result

Load events
Store events
MineSweeper stage 2

Obfuscated WASM module → MineSweeper

- Analyze WASM Module
- Monitor CPU Cache events

Result

Load events
Store events
Evaluation of CPU Cache Events Monitoring

We visited 7 websites from following categories:

1. Cryptominers
2. Video players
3. Wasm-based games
4. JavaScript (JS) games
Evaluation of CPU Cache Events Monitoring
Evaluation of CPU Cache Events Monitoring

Miner induces 35.6 times more L1 dcache load events

Miner induces 16.13 times more L1 dcache store events
Evaluation of CPU Cache Events Monitoring

Miner induces 35.6 times more L1 dcache load events
Miner induces 16.13 times more L1 dcache store events
Evaluation of CPU Cache Events Monitoring

Miner induces 13.96 times more L1 dcache load events

Miner induces 6.29 times more L1 dcache store events
Conclusion

<table>
<thead>
<tr>
<th>Crawling period</th>
<th>March 12, 2018 – March 19, 2018</th>
</tr>
</thead>
<tbody>
<tr>
<td># of crawled websites</td>
<td>991,513</td>
</tr>
<tr>
<td># of drive-by mining websites</td>
<td>1,735 (0.18%)</td>
</tr>
<tr>
<td># of drive-by mining services</td>
<td>28</td>
</tr>
<tr>
<td># of drive-by mining campaigns</td>
<td>20</td>
</tr>
<tr>
<td># of websites in biggest campaign</td>
<td>139</td>
</tr>
<tr>
<td>Estimated overall profit</td>
<td>US$ 188,878.84</td>
</tr>
<tr>
<td>Most profitable/biggest campaign</td>
<td>US$ 31,060.80</td>
</tr>
<tr>
<td>Most profitable website</td>
<td>US$ 17,166.97</td>
</tr>
</tbody>
</table>

- Drive-by mining is real and can be very profitable for high traffic websites
- MineSweeper exploits the core properties of the CryptoNight to detect drive-by mining websites
- FTC is currently looking into our dataset
- Dataset and code will be available soon at [https://github.com/vusec](https://github.com/vusec)