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

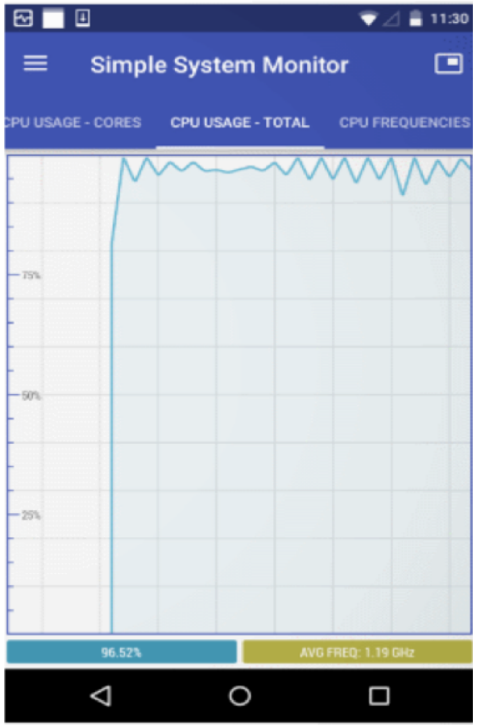
- Why is it bad?
  - No consent
  - System performance
  - Power consumption

Motivation

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

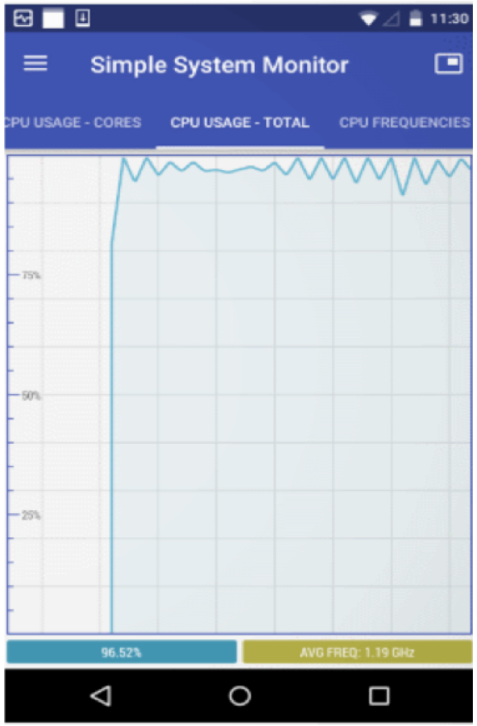
- Why is it bad?
  - No consent
  - System performance
  - Power consumption
  - Longevity of the device

Existing defenses



CPU Usage Heuristics

Existing defenses

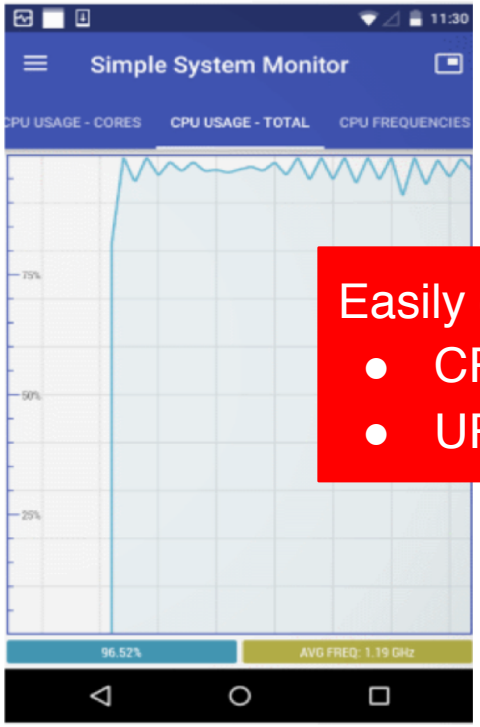


CPU Usage Heuristics

```
0aqpqdju.me
0x1f4b0.com
1480876790.rsc.cdn77.org
1beb2a44.space
1q2w3.fun
1q2w3.me
1q2w3.top
1q2w3.website
2giga.download
2giga.link
2ledhenone.com
300ca0d0.space
310ca263.space
320ca3f6.space
330ca589.space
340ca71c.space
360caa42.space
370cabd5.space
3c0cb3b4.space
3d0cb547.space
50bots.nullrefexcep.com
```

URL Blacklists

Existing defenses



CPU Usage Heuristics

```
0aqpqdju.me
0x1f4b0.com
1480876790.rsc.cdn77.org
1beb2a44.space
1q2w3.fun
1q2w3.me
1q2w3.top
                bsite
                wnload
                nk
                ne.com
                .space
                .space
                .space
330ca589.space
340ca71c.space
360caa42.space
370cabd5.space
3c0cb3b4.space
3d0cb547.space
50bots.nullrefexcep.com
```

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





CryptoNight (PoW)

2. Advanced web technologies:
   - asm.js (2013)

Catalysts of drive-by mining

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

CryptoNight (PoW)

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:

```
<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:

```
<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:

```
<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

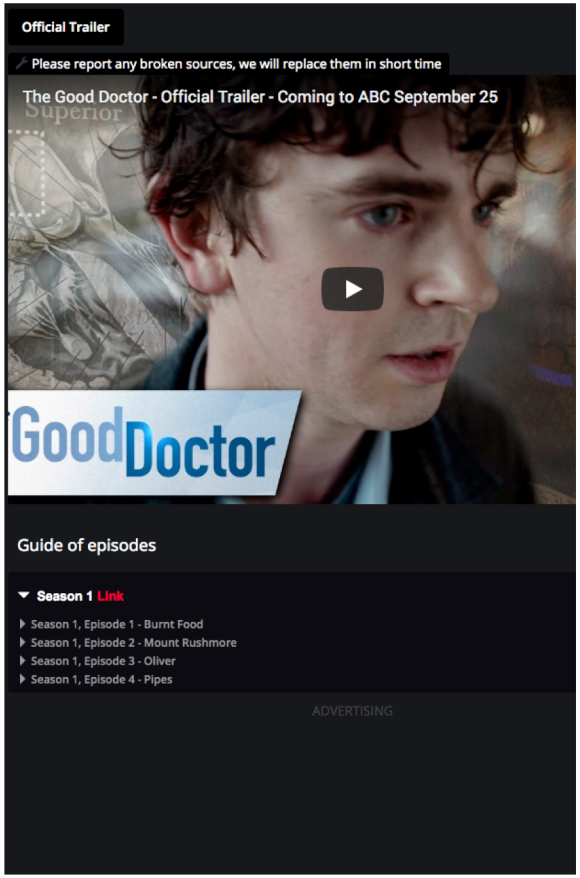
Online cryptocurrency miner

NF WebMiner : a simple web mining service

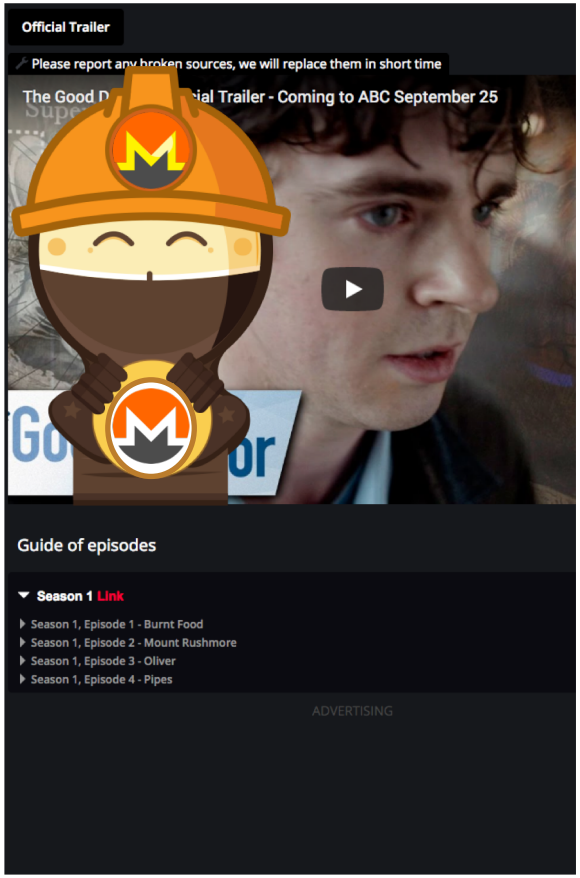
35,904 Registered Users

Monetize your web!

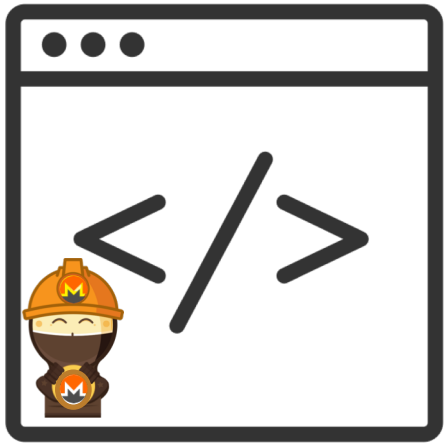
An interesting drive-by mining case

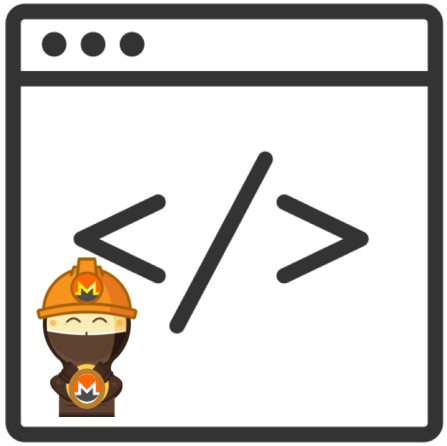


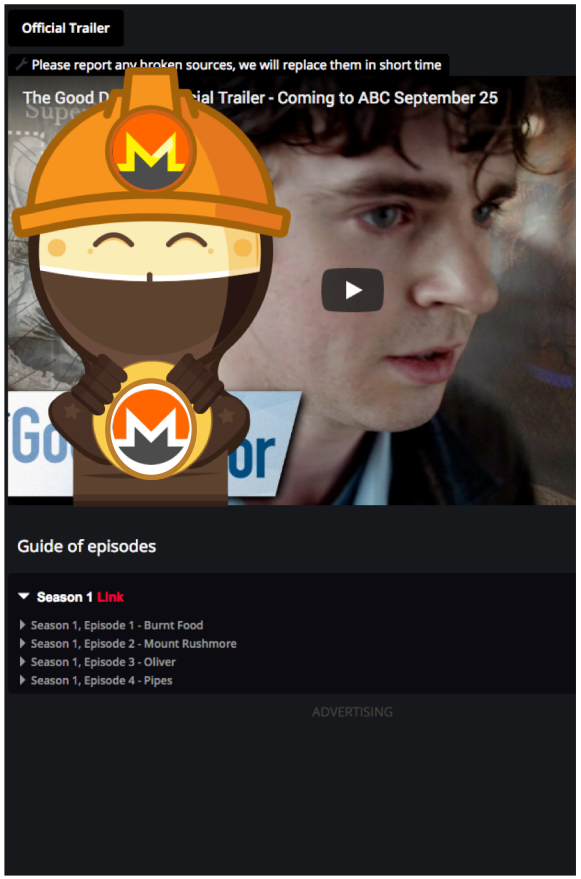
An interesting drive-by mining case



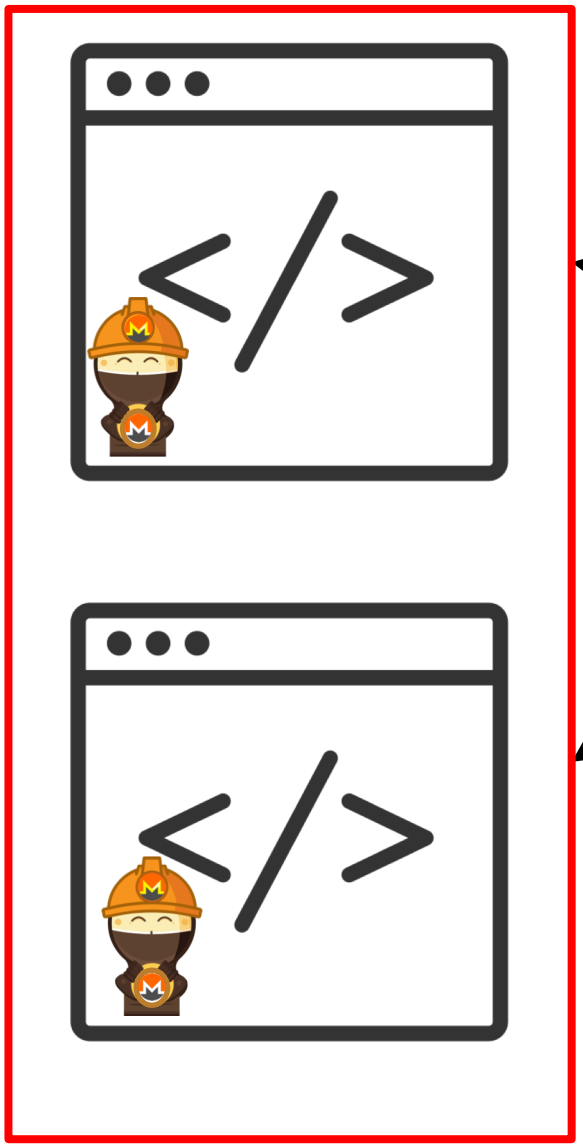
An interesting drive-by mining case

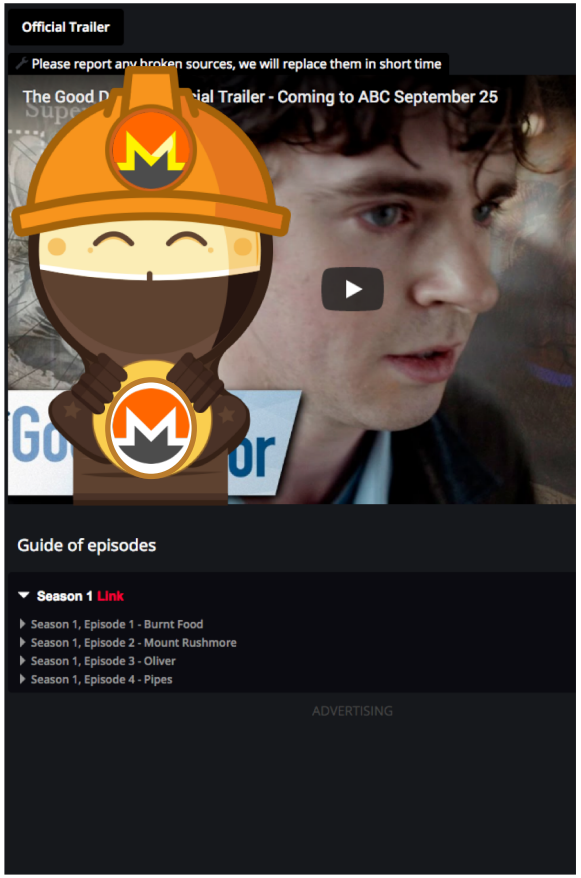




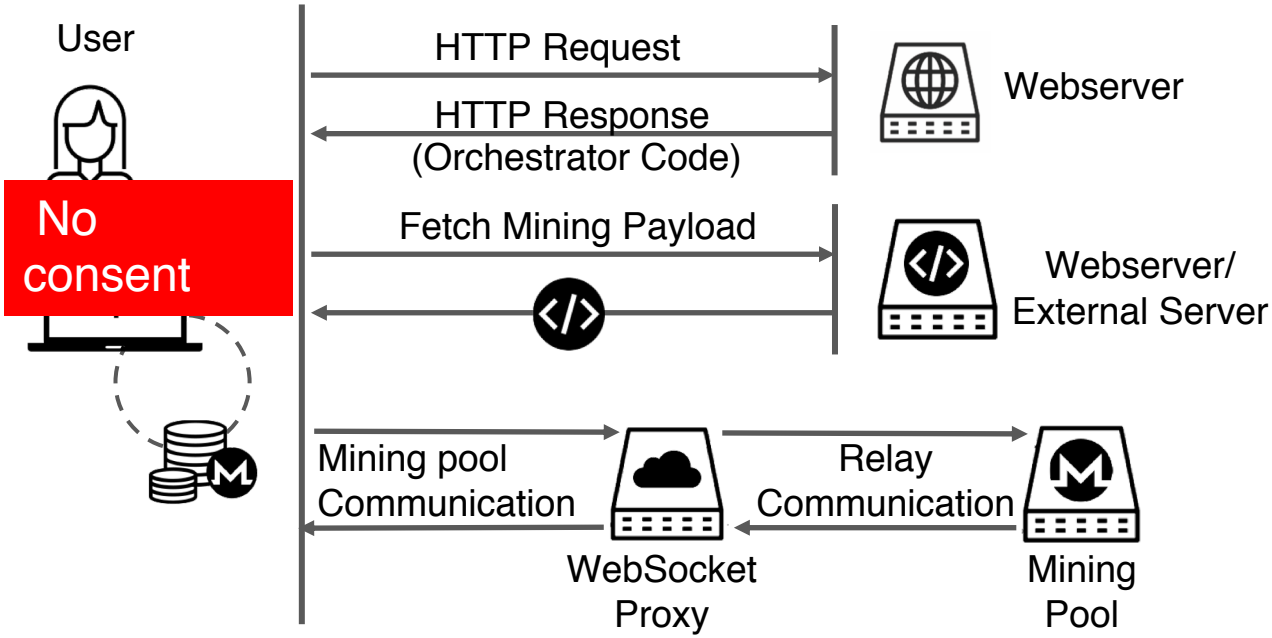


An interesting drive-by mining case

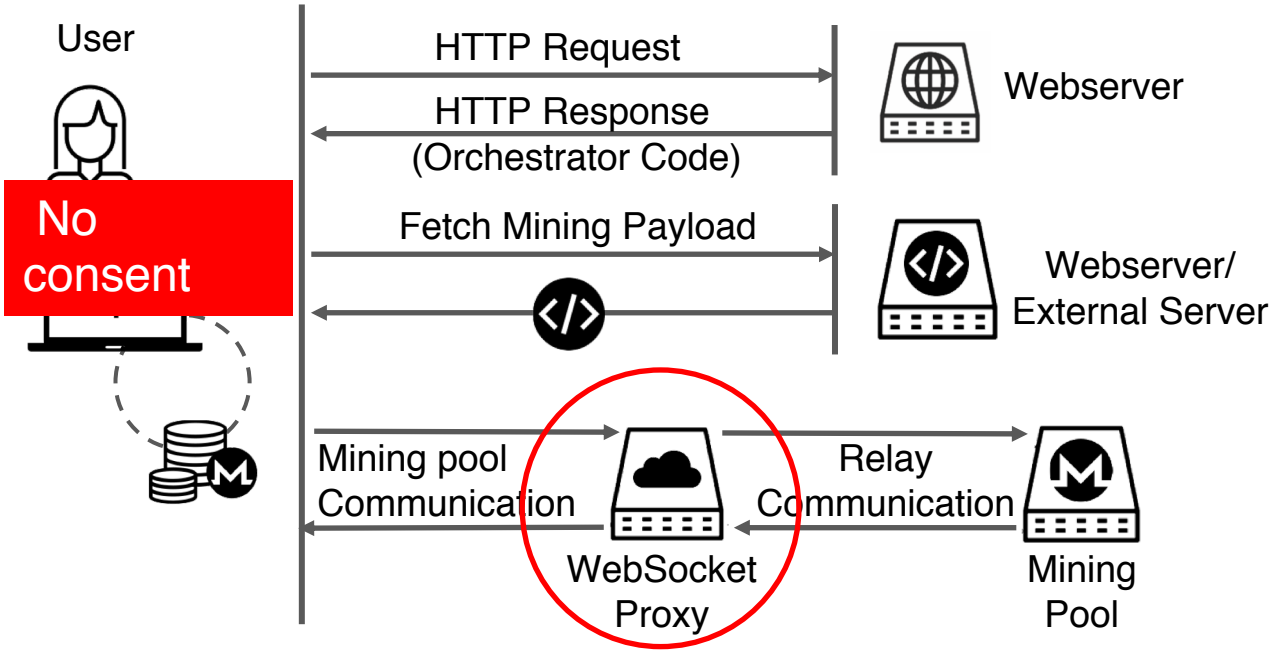




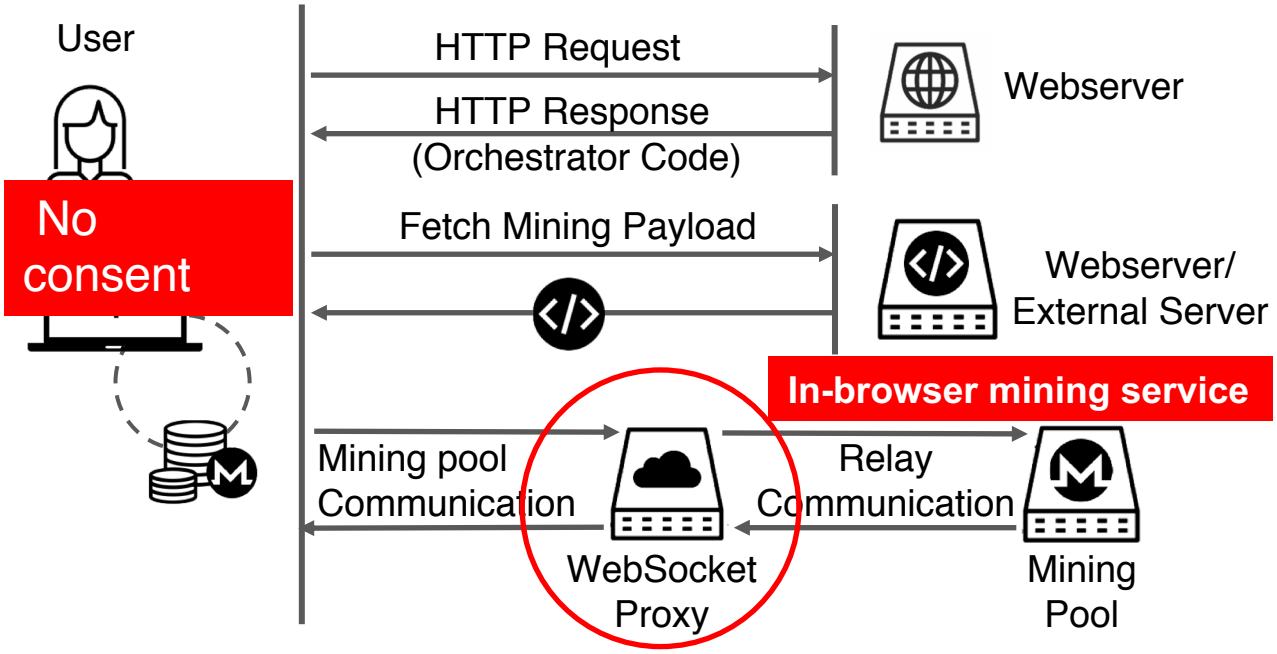
Threat model: Drive-by mining



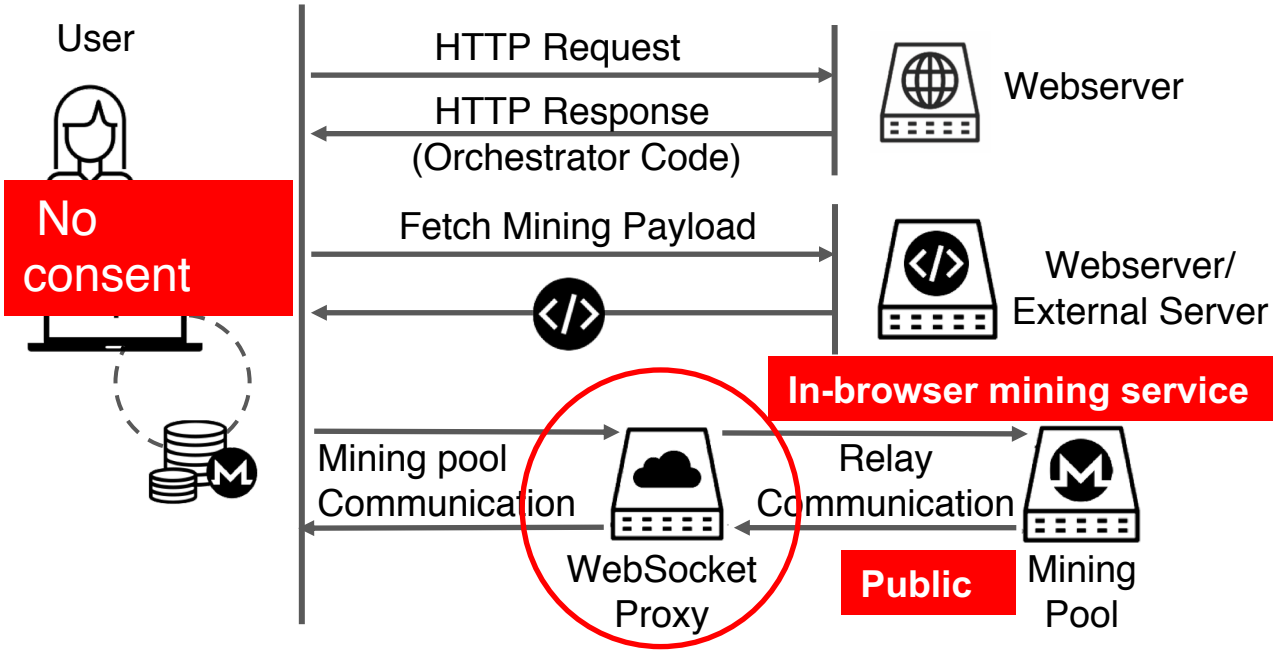
Threat model: Drive-by mining



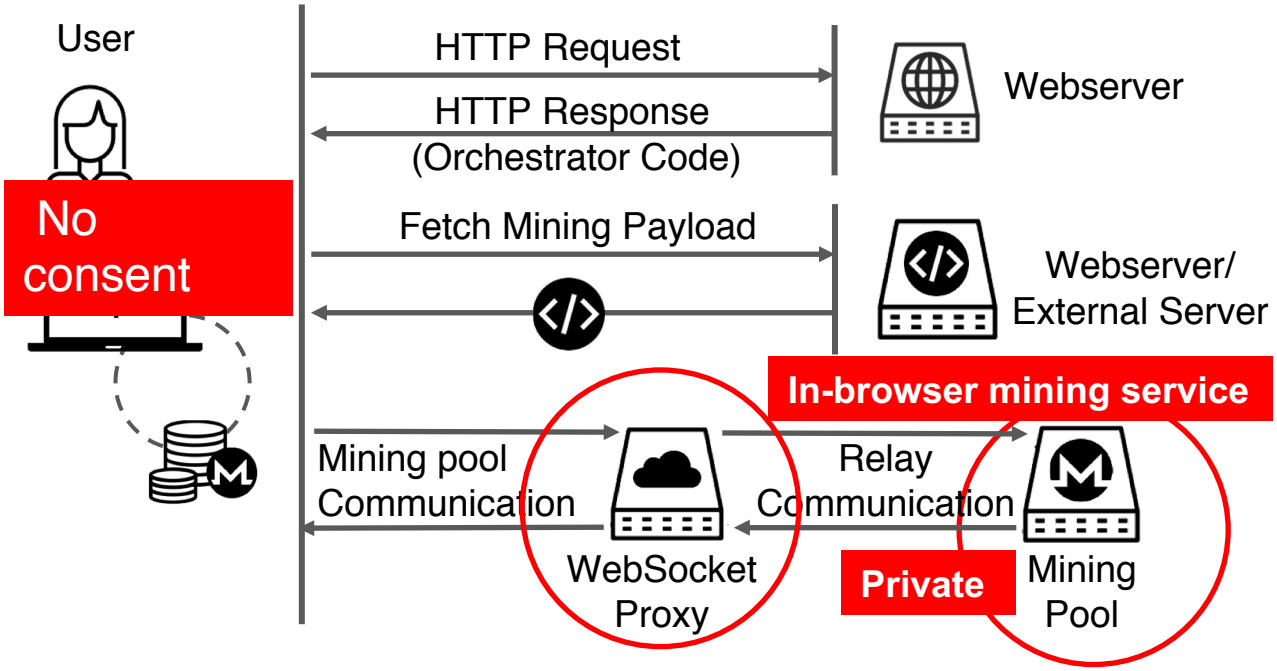
Threat model: Drive-by mining



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

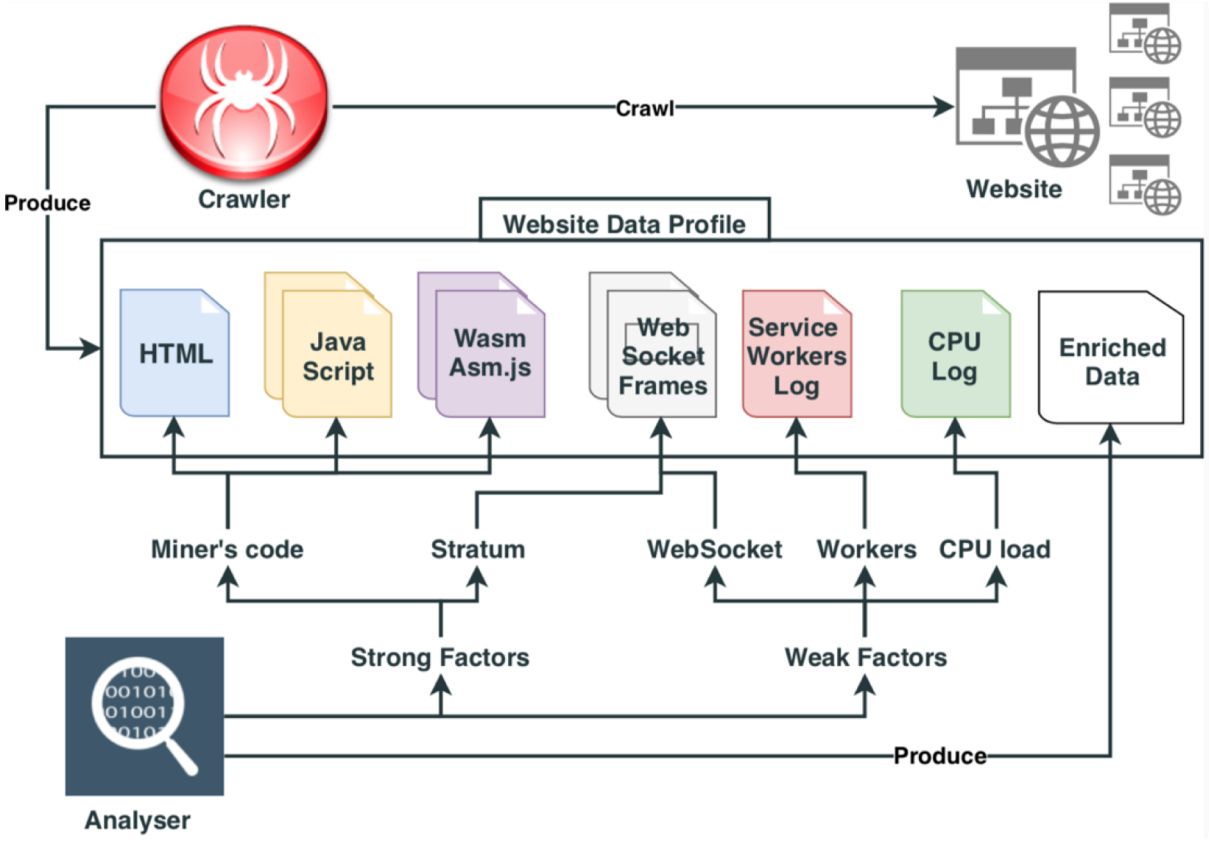
Data collection

Alexa top 1 million websites (Mid-March 2018)

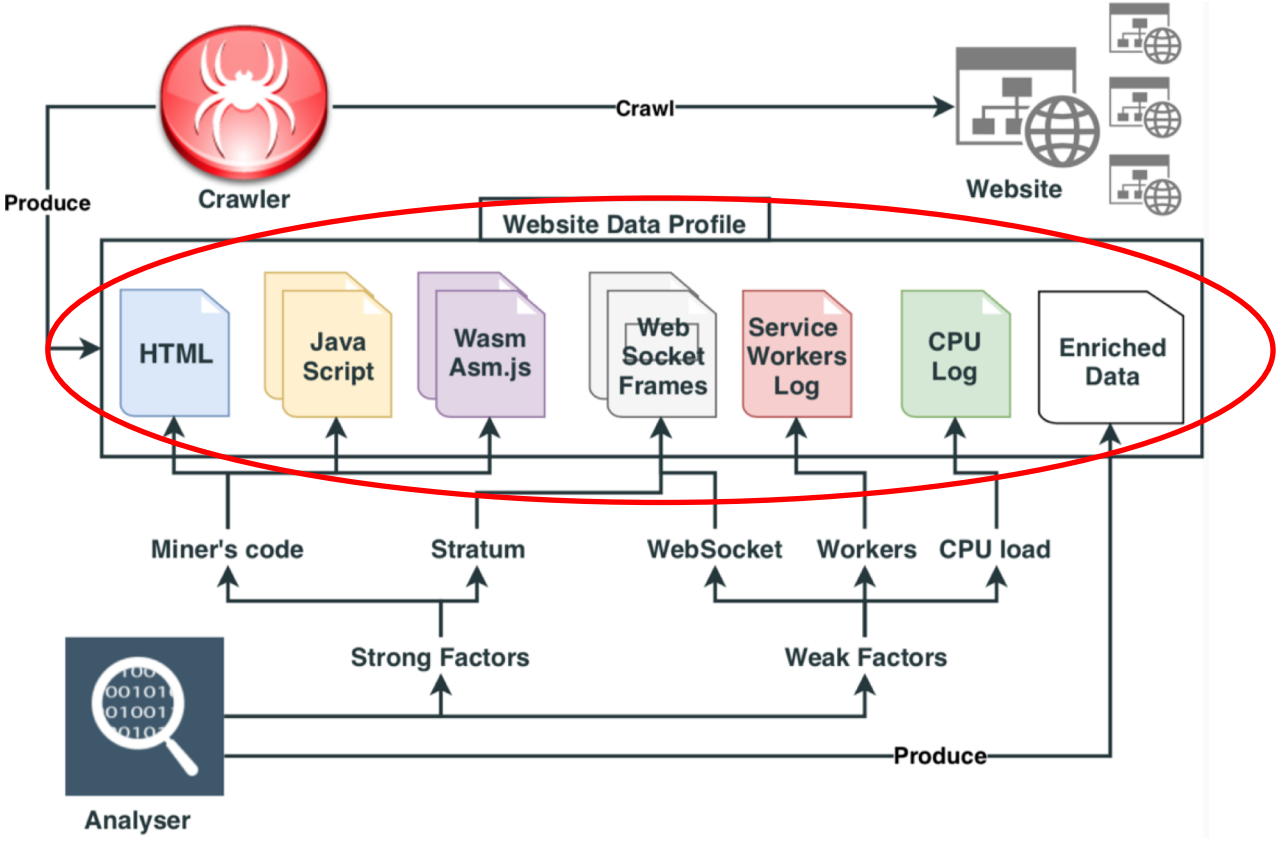
Crawler configuration:

- 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

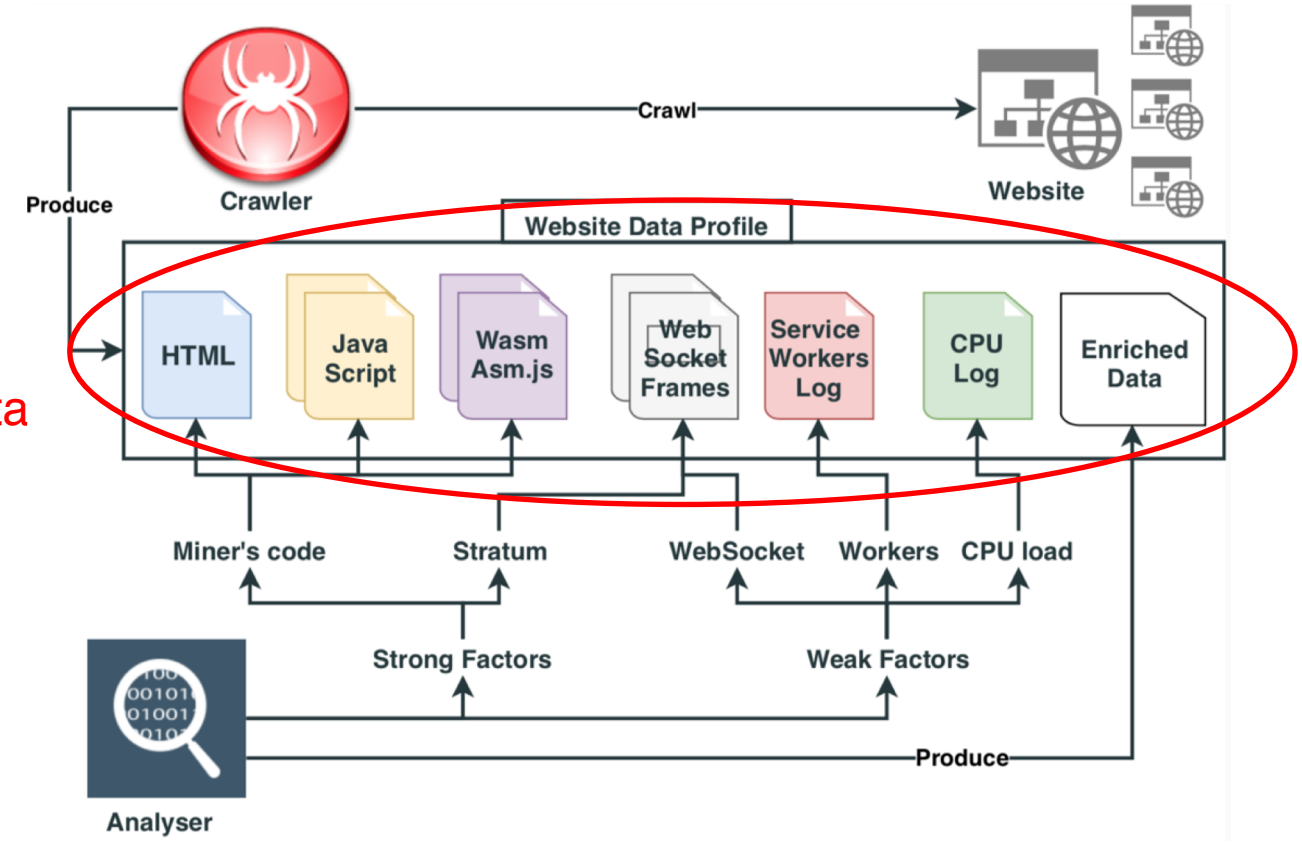


Large-scale Analysis: Experiment Set-Up

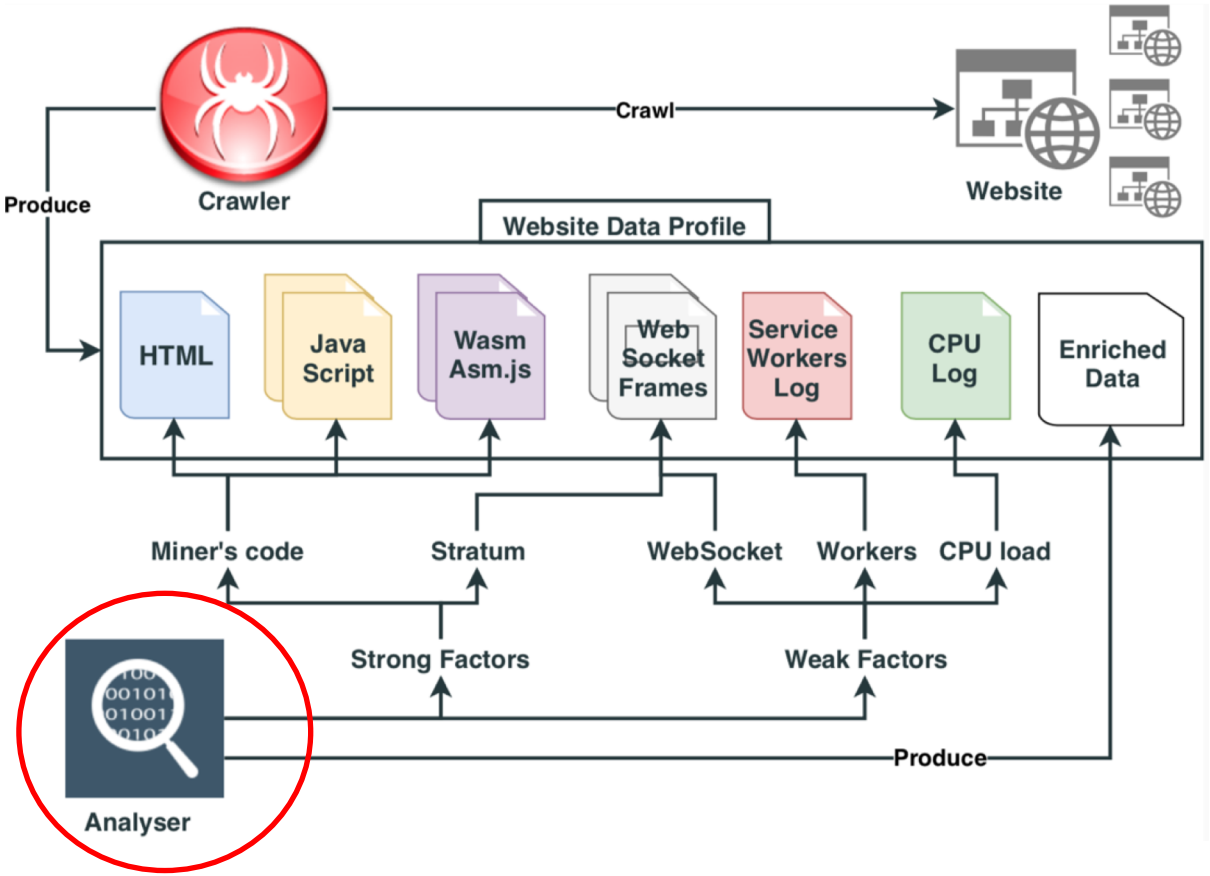


Large-scale Analysis: Experiment Set-Up

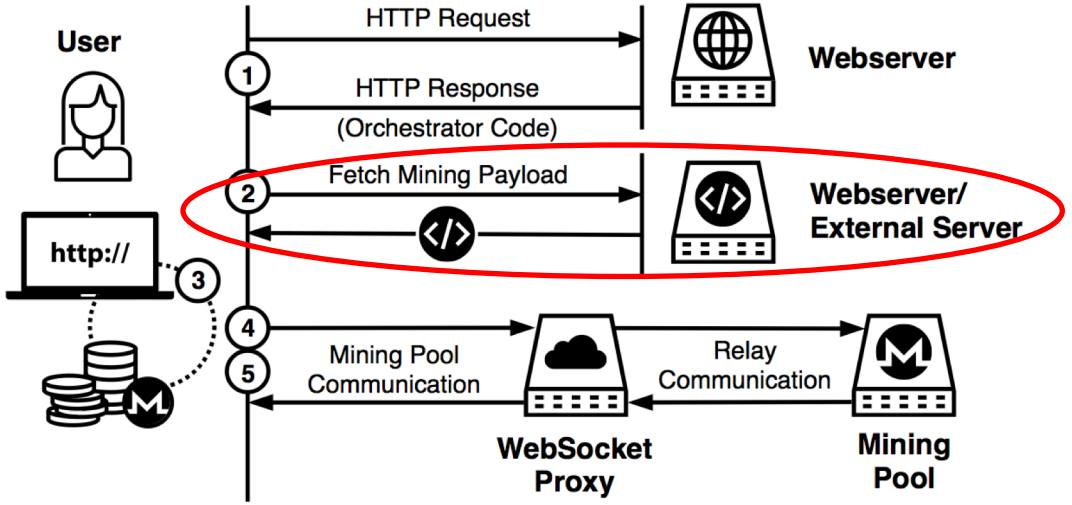
4.6 TB raw data



Large-scale Analysis: Experiment Set-Up

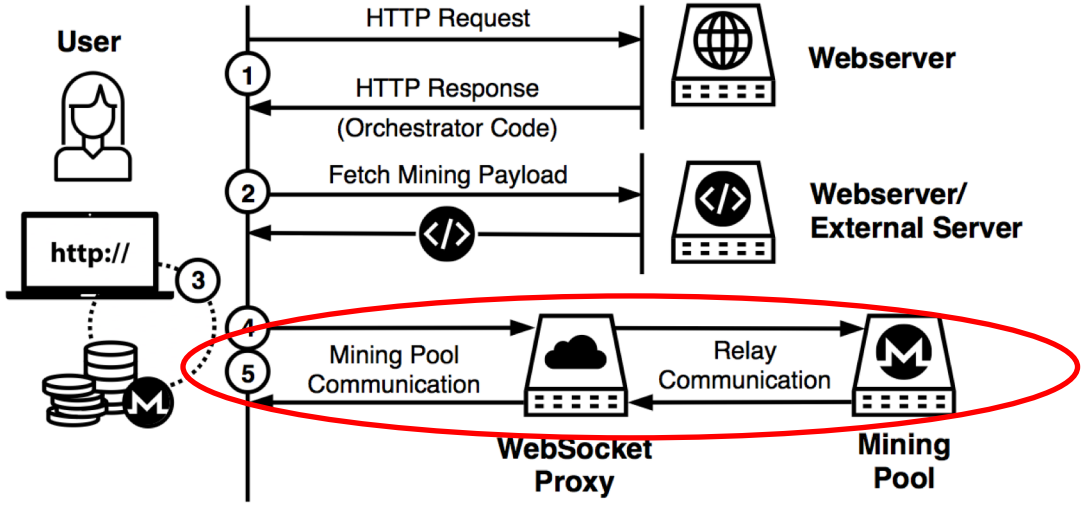


Detecting Mining Payload (WASM)




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

Detecting Stratum communication



Command	Keywords
Authentication	type:auth | command:connect | identifier:handshake | command:info
Authentication accepted	type:authed | command:work
Fetch job	identifier:job | type:job | command:work | command:get_job | command:set_job
Submit solved hash	type:submit | command:share
Solution accepted	command:accepted
Set CPU limits	command:set_cpu_load

1. Prevalence of drive-by mining

Crawling period	March 12, 2018 – March 19, 2018
# websites crawled	991,513
# drive-by mining websites	**1,735**

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:

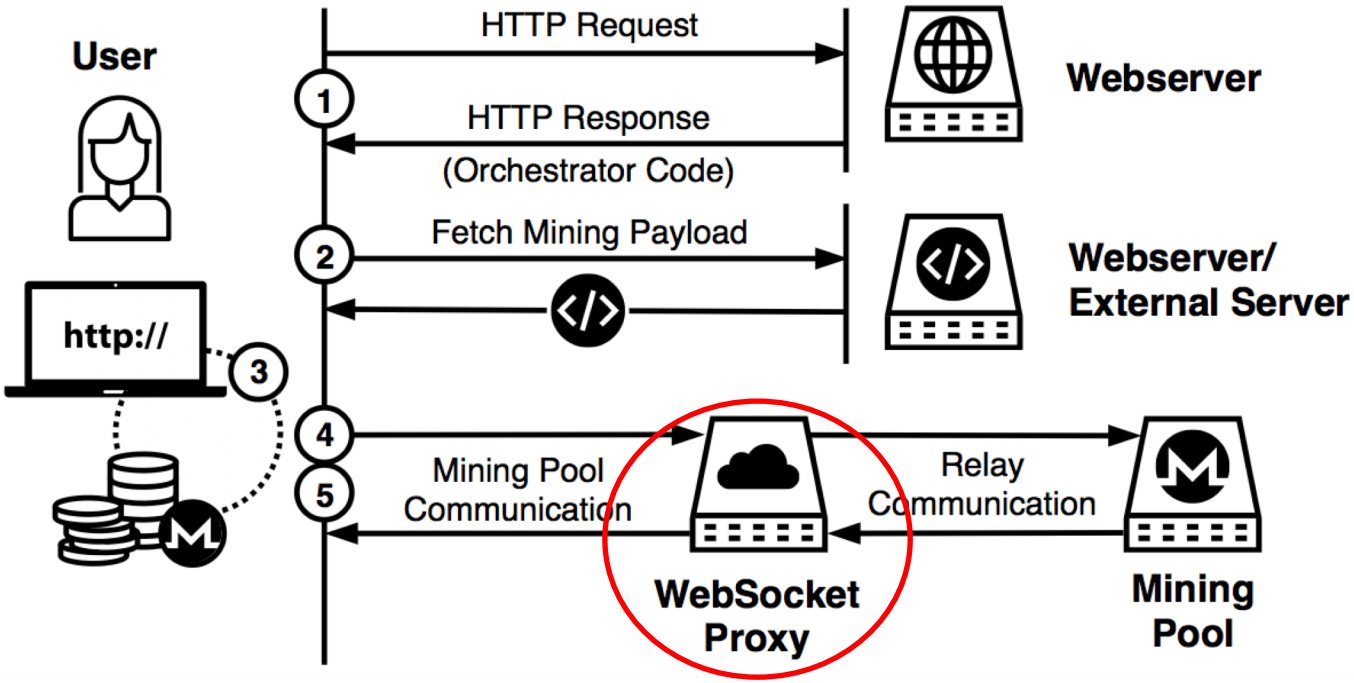
- Packed code, CharCode, Name obfuscation, Dead code injection, URL randomization

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 from SimilarWeb:

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

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

	Device Type	Hash Rate (H/s)
Mobile Device	Nokia 3	5
	iPhone 5s	5
	iPhone 6	7
	Wiko View 2	8
	Motorola Moto G6	10
	Google Pixel	10
	OnePlus 3	12
	Huawei P20	13
	Huawei Mate 10 Lite	13
	iPhone 6s	13
	iPhone SE	14
	iPhone 7	19
	OnePlus 5	21
	Sony Xperia	24
	Samsung Galaxy S9 Plus	28
	iPhone 8	31
	Mean	*14.56*
Laptop Desktop	Intel Core i3-5010U	16
	Intel Core i7-6700K	65
	Mean	*40.50*

3. Profit Estimation

Visitor Statistics from SimilarWeb:

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

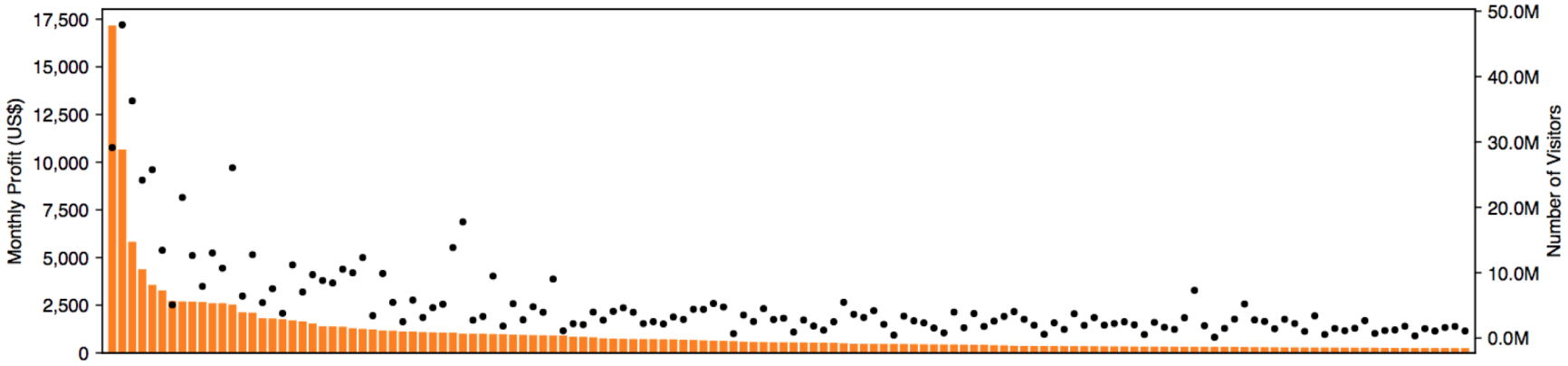
Monero (XMR) value on May 2018 : US$ 253

Average hashrate:

- Mobile devices : 14.56 h/s
- Laptops : 40.5 h/s

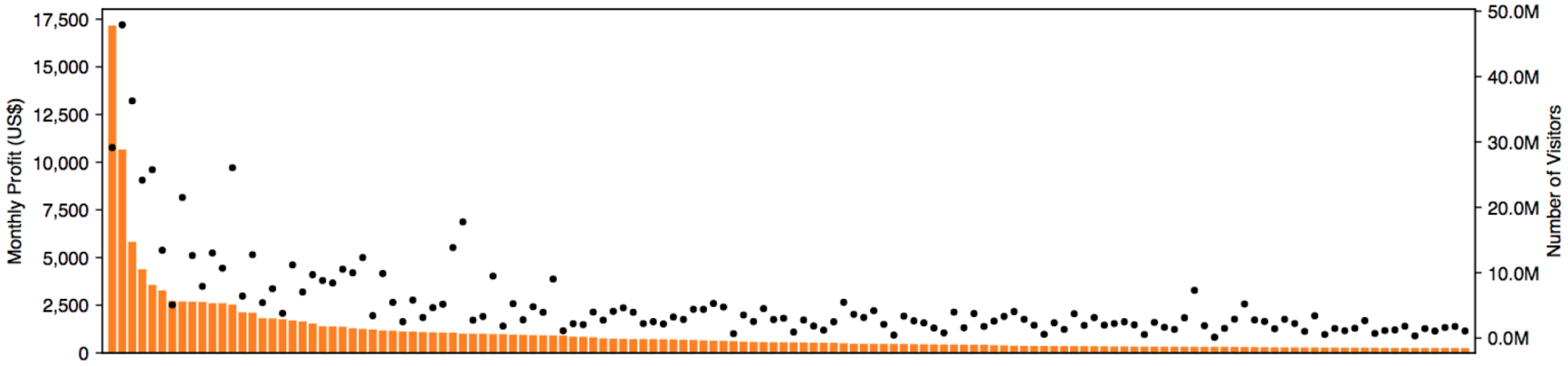
	Device Type	Hash Rate (H/s)
Mobile Device	Nokia 3	5
	iPhone 5s	5
	iPhone 6	7
	Wiko View 2	8
	Motorola Moto G6	10
	Google Pixel	10
	OnePlus 3	12
	Huawei P20	13
	Huawei Mate 10 Lite	13
	iPhone 6s	13
	iPhone SE	14
	iPhone 7	19
	OnePlus 5	21
	Sony Xperia	24
	Samsung Galaxy S9 Plus	28
	iPhone 8	31
	Mean	*14.56*
Laptop Desktop	Intel Core i3-5010U	16
	Intel Core i7-6700K	65
	Mean	*40.50*

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

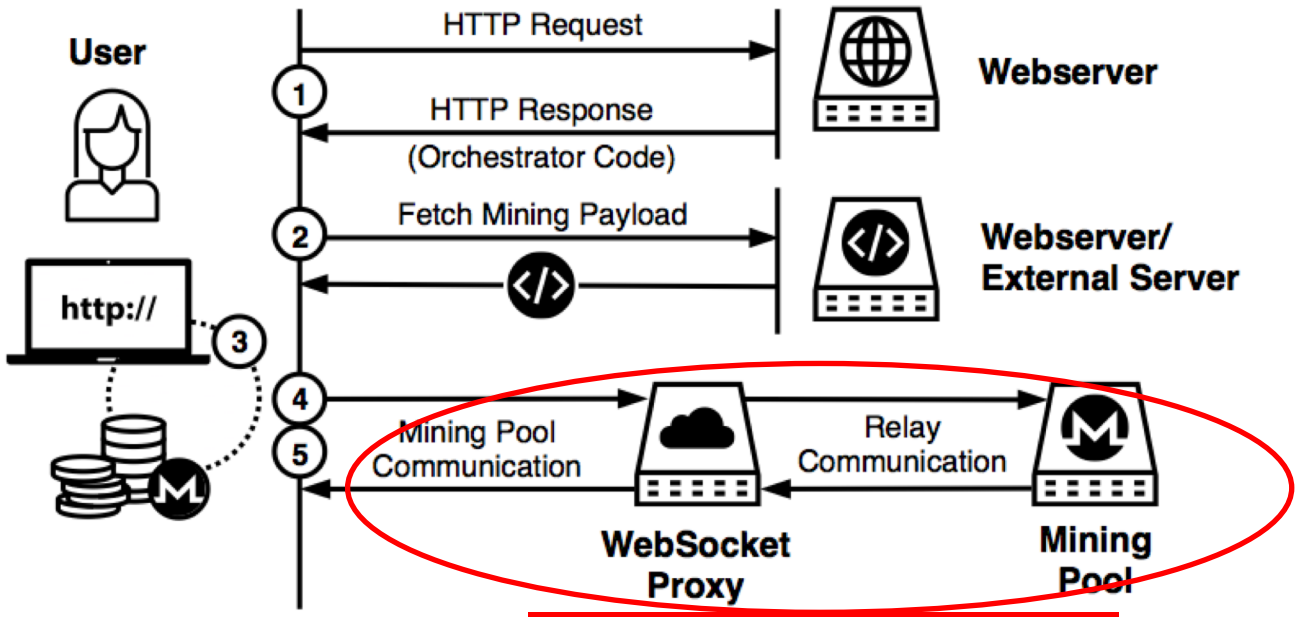


- Most profitable website (tumangaonline.com) : US$ 17,166.97

avg. time : 18 mints

4. Identifying Campaigns

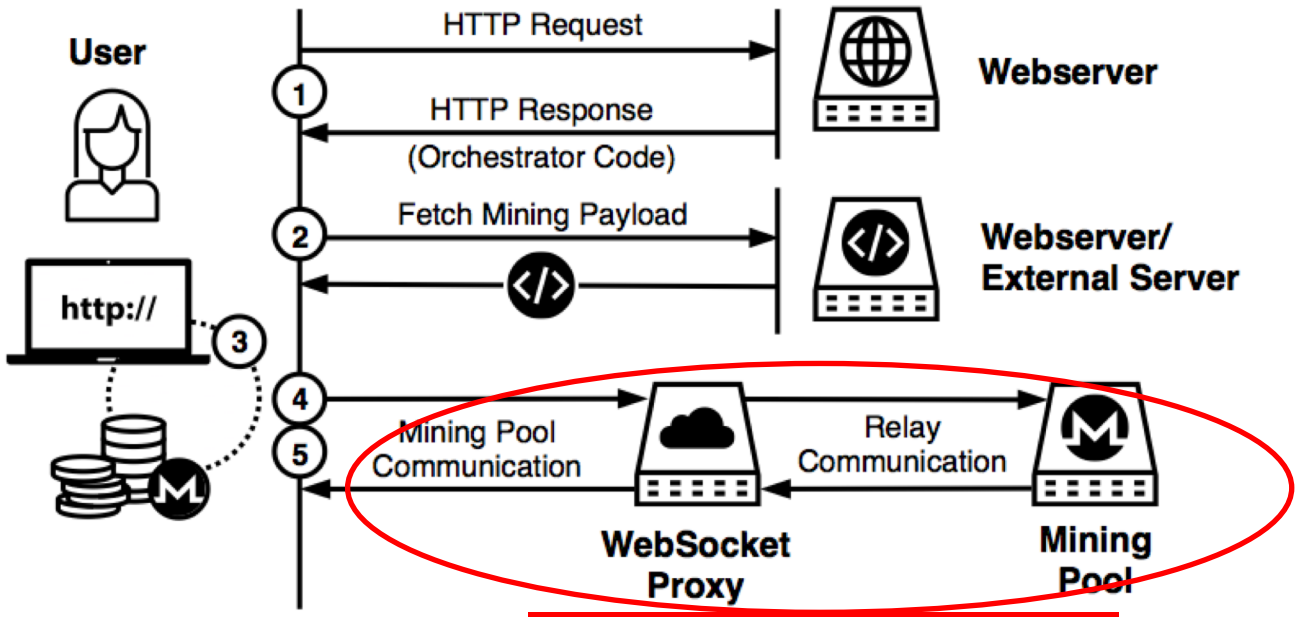
Two valuable pieces of information in the WebSocket frames:



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:

Site Key	#	Main Pool	Type	Profit (US$)
"428347349263284"	139	weline.info	Third party (video)	$31,060.80
OT1CIcpkIOCO7yVMxcJiqmSWoDWOri06	53	coinhive.com	Torrent portals	$8,343.18
ricewithchicken	32	datasecu.download	Advertisement-based	$1,078.27
jscustomkey2	27	207.246.88.253	Third party (counter12.com)	$86.98
CryptoNoter	27	minercry.pt	Advertisement-based	$20.35
489djE22mdZ3[..]y4PBWLb4tc1X8ADsu	24	datasecu.download	Compromised websites	$142.40
first	23	cloudflane.com	Compromised websites	$120.02
vBaNYz4tVYKV9Q9tZlL0BPGq8rnZEl00	20	hemnes.win	Third party (video)	$303.14
45CQjsiBr46U[..]o2C5uo3u23p5SkMN	17	rand.com.ru	Compromised websites	$306.60
Tumblr	14	count.im	Third party	$11.31
ClmAXQqOiKXawAMBVzuc51G31uDYdJ8F	12	coinhive.com	Third party (night-skin.com)	$14.36

4. Campaigns and monthly revenue : Site-key

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

Site Key	#	Main Pool	Type	Profit (US$)
"428347349263284"	139	weline.info	Third party (video)	$31,060.80
OT1CIcpkIOCO7yVMxcJiqmSWoDWOri06	53	coinhive.com	Torrent portals	$8,343.18
ricewithchicken	32	datasecu.download	Advertisement-based	$1,078.27
jscustomkey2	27	207.246.88.253	Third party (counter12.com)	$86.98
CryptoNoter	27	minercry.pt	Advertisement-based	$20.35
489djE22mdZ3[..]y4PBWLb4tc1X8ADsu	24	datasecu.download	Compromised websites	$142.40
first	23	cloudflane.com	Compromised websites	$120.02
vBaNYz4tVYKV9Q9tZlL0BPGq8rnZEl00	20	hemnes.win	Third party (video)	$303.14
45CQjsiBr46U[..]o2C5uo3u23p5SkMN	17	rand.com.ru	Compromised websites	$306.60
Tumblr	14	count.im	Third party	$11.31
ClmAXQqOiKXawAMBVzuc51G31uDYdJ8F	12	coinhive.com	Third party (night-skin.com)	$14.36

4. Campaigns and monthly revenue : Site-key

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

Site Key	#	Main Pool	Type	Profit (US$)
"428347349263284"	139	weline.info	Third party (video)	$31,060.80
OT1CIcpkIOCO7yVMxcJiqmSWoDWOri06	53	coinhive.com	Torrent portals	$8,343.18
ricewithchicken	32	datasecu.download	Advertisement-based	$1,078.27
jscustomkey2	27	207.246.88.253	Third party (counter12.com)	$86.98
CryptoNoter	27	minercry.pt	Advertisement-based	$20.35
489djE22mdZ3[..]y4PBWLb4tc1X8ADsu	24	datasecu.download	Compromised websites	$142.40
first	23	cloudflane.com	Compromised websites	$120.02
vBaNYz4tVYKV9Q9tZlL0BPGq8rnZEl00	20	hemnes.win	Third party (video)	$303.14
45CQjsiBr46U[..]o2C5uo3u23p5SkMN	17	rand.com.ru	Compromised websites	$306.60
Tumblr	14	count.im	Third party	$11.31
ClmAXQqOiKXawAMBVzuc51G31uDYdJ8F	12	coinhive.com	Third party (night-skin.com)	$14.36

4. Campaigns and monthly revenue : Site-key

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

Site Key	#	Main Pool	Type	Profit (US$)
"428347349263284"	139	weline.info	Third party (video)	$31,060.80
OT1CIcpkIOCO7yVMxcJiqmSWoDWOri06	53	coinhive.com	Torrent portals	$8,343.18
ricewithchicken	32	datasecu.download	Advertisement-based	$1,078.27
jscustomkey2	27	207.246.88.253	Third party (counter12.com)	$86.98
CryptoNoter	27	minercry.pt	Advertisement-based	$20.35
489djE22mdZ3[..]y4PBWLb4tc1X8ADsu	24	datasecu.download	Compromised websites	$142.40
first	23	cloudflane.com	Compromised websites	$120.02
vBaNYz4tVYKV9Q9tZlL0BPGq8rnZEl00	20	hemnes.win	Third party (video)	$303.14
45CQjsiBr46U[..]o2C5uo3u23p5SkMN	17	rand.com.ru	Compromised websites	$306.60
Tumblr	14	count.im	Third party	$11.31
ClmAXQqOiKXawAMBVzuc51G31uDYdJ8F	12	coinhive.com	Third party (night-skin.com)	$14.36

4. Campaigns and monthly revenue : Site-key

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

Site Key	#	Main Pool	Type	Profit (US$)
"428347349263284"	139	weline.info	Third party (video)	$31,060.80
OT1CIcpkIOCO7yVMxcJiqmSWoDWOri06	53	coinhive.com	Torrent portals	$8,343.18
ricewithchicken	32	datasecu.download	Advertisement-based	$1,078.27
jscustomkey2	27	207.246.88.253	Third party (counter12.com)	$86.98
CryptoNoter	27	minercry.pt	Advertisement-based	$20.35
489djE22mdZ3[..]y4PBWLb4tc1X8ADsu	24	datasecu.download	Compromised websites	$142.40
first	23	cloudflane.com	Compromised websites	$120.02
vBaNYz4tVYKV9Q9tZlL0BPGq8rnZEl00	20	hemnes.win	Third party (video)	$303.14
45CQjsiBr46U[..]o2C5uo3u23p5SkMN	17	rand.com.ru	Compromised websites	$306.60
Tumblr	14	count.im	Third party	$11.31
ClmAXQqOiKXawAMBVzuc51G31uDYdJ8F	12	coinhive.com	Third party (night-skin.com)	$14.36

4. Campaigns and monthly revenue : Site-key

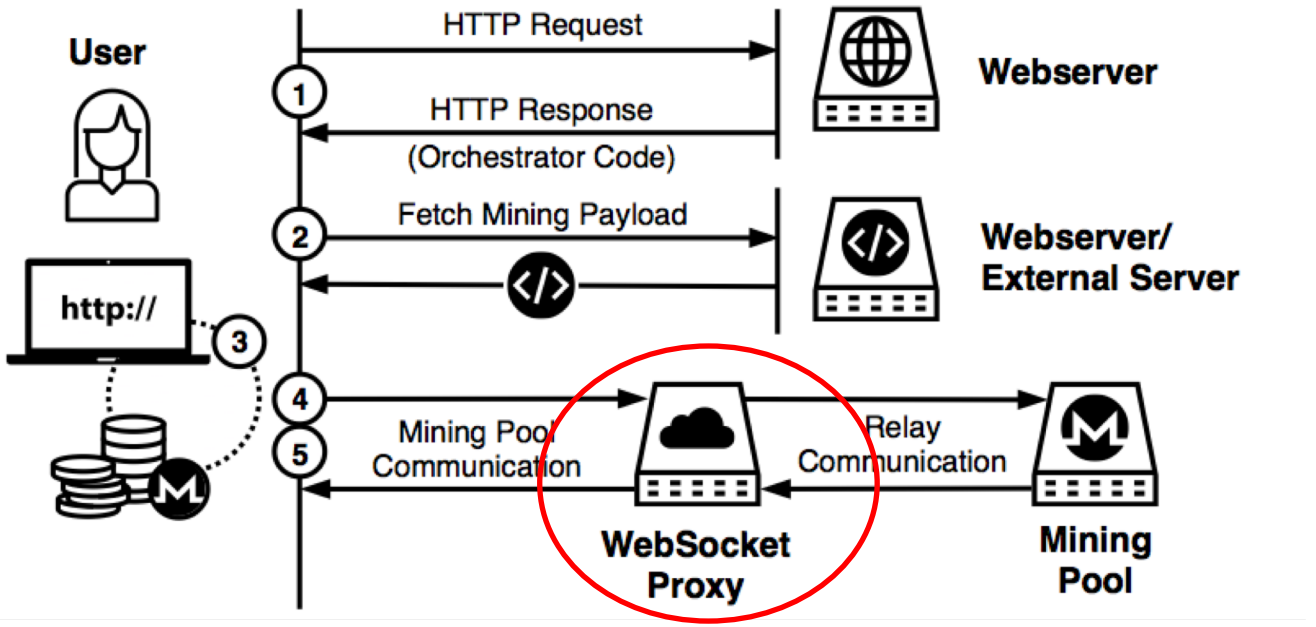
We discovered 11 campaigns by clustering websites based on site-key:

Site Key	#	Main Pool	Type	Profit (US$)
"428347349263284"	139	weline.info	Third party (video)	$31,060.80
OT1CIcpkIOCO7yVMxcJiqmSWoDWOri06	53	coinhive.com	Torrent portals	$8,343.18
ricewithchicken	32	datasecu.download	Advertisement-based	$1,078.27
jscustomkey2	27	207.246.88.253	Third party (counter12.com)	$86.98
CryptoNoter	27	minercry.pt	Advertisement-based	$20.35
489djE22mdZ3[..]y4PBWLb4tc1X8ADsu	24	datasecu.download	Compromised websites	$142.40
first	23	cloudflane.com	Compromised websites	$120.02
vBaNYz4tVYKV9Q9tZlL0BPGq8rnZEl00	20	hemnes.win	Third party (video)	$303.14
45CQjsiBr46U[..]o2C5uo3u23p5SkMN	17	rand.com.ru	Compromised websites	$306.60
Tumblr	14	count.im	Third party	$11.31
ClmAXQqOiKXawAMBVzuc51G31uDYdJ8F	12	coinhive.com	Third party (night-skin.com)	$14.36

4. Identifying Campaigns

Two valuable pieces of information in the WebSocket frames:

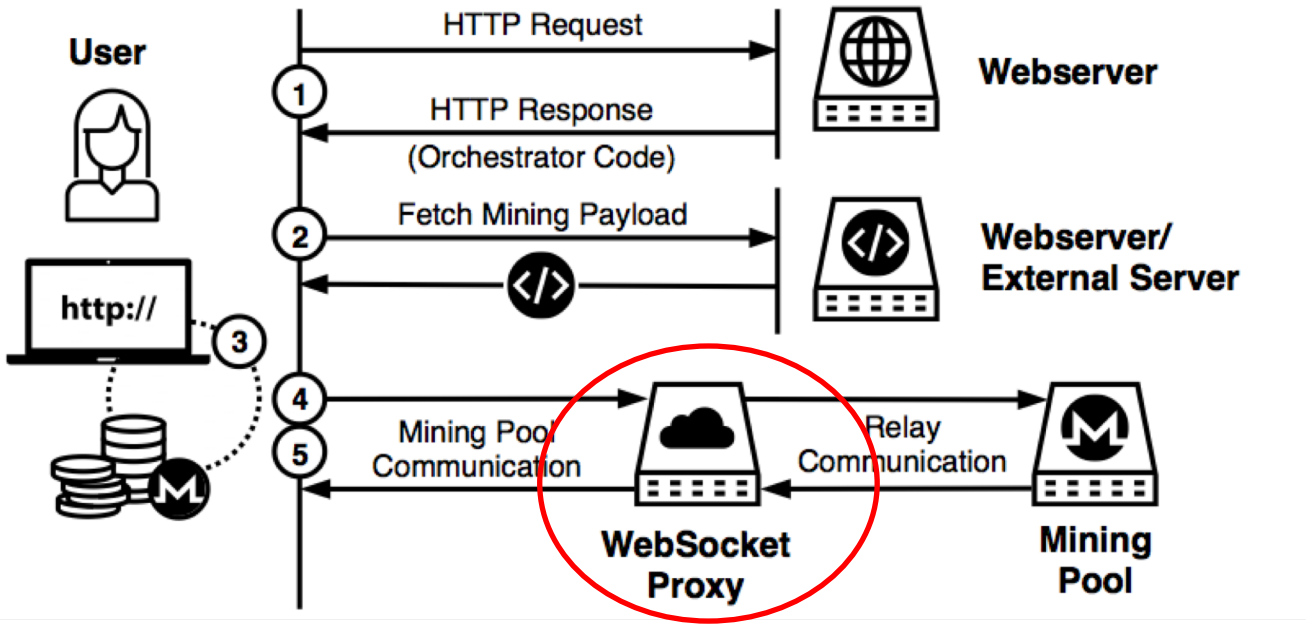
1. Site-Key/ Client ID



4. Identifying Campaigns

Two valuable pieces of information in the WebSocket frames:

1. Site-Key/ Client ID
2. WebSocket Proxy



4. Campaigns : WebSocket Proxy

We discovered 9 campaigns using the proxy aggregation:

WebSocket Proxy	#	Type	Profit (US$)
advisorstat.space	63	Advertisement-based	$321.71
zenoviaexchange.com	37	Advertisement-based	$1,516.08
stati.bid	20	Compromised websites	$34.94
staticsfs.host	20	Compromised websites	$384.91
webmetric.loan	17	Compromised websites	$181.32
insdrbot.com	7	Third party (video)	$1,689.26
1q2w3.website	5	Third party (video)	$2,012.90
streamplay.to	5	Third party (video)	$239.71
estream.to	4	Third party (video)	$872.72

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

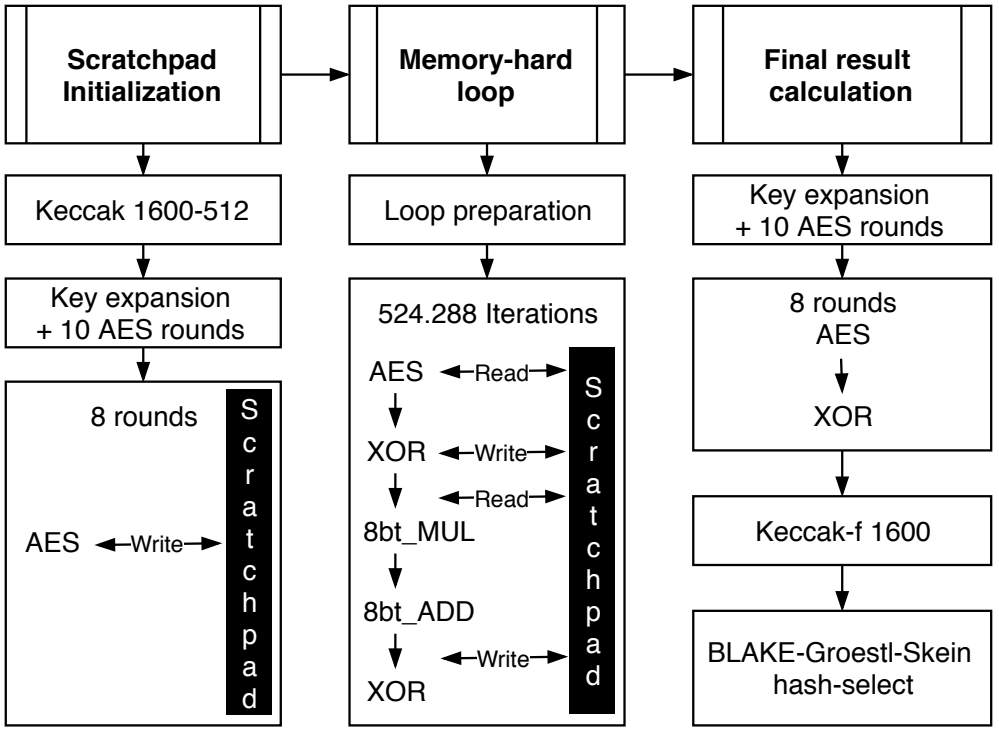
5. Drive-by mining services commonalities:

1. **CryptoNight-based cryptocurrency (Specifically, Monero)**
2. **CryptoNight (PoW) is implemented in WebAssembly**
3. WebWorker threads
4. WebSocket

Part II : MineSweeper

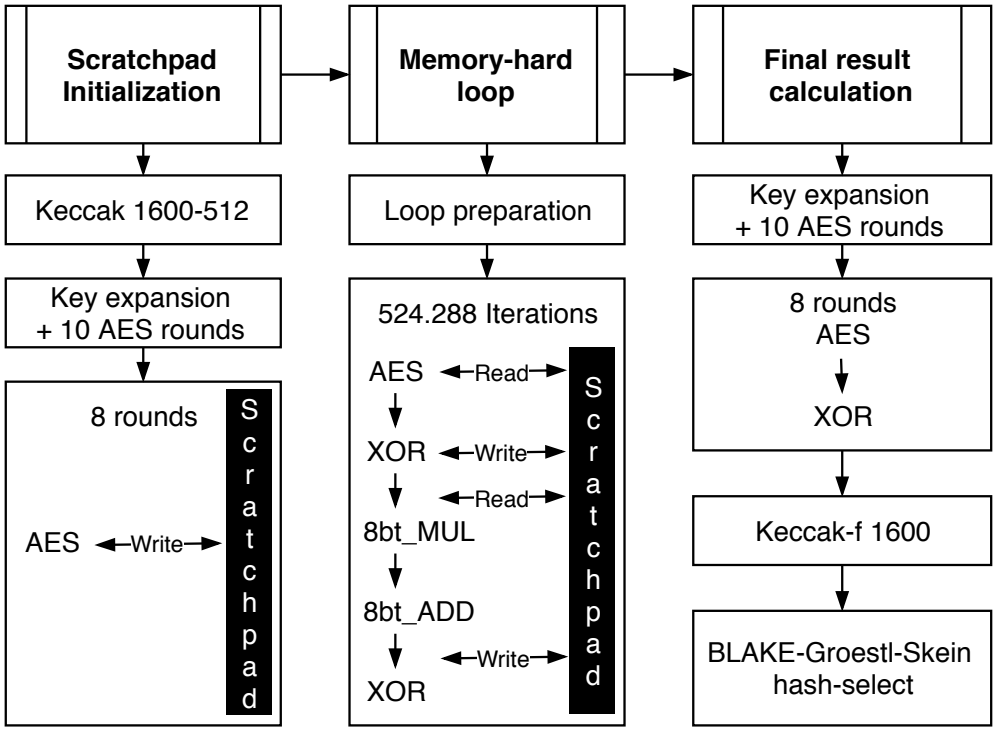
CryptoNight Algorithm

- CryptoNight is a proof of work algorithm proposed in 2013



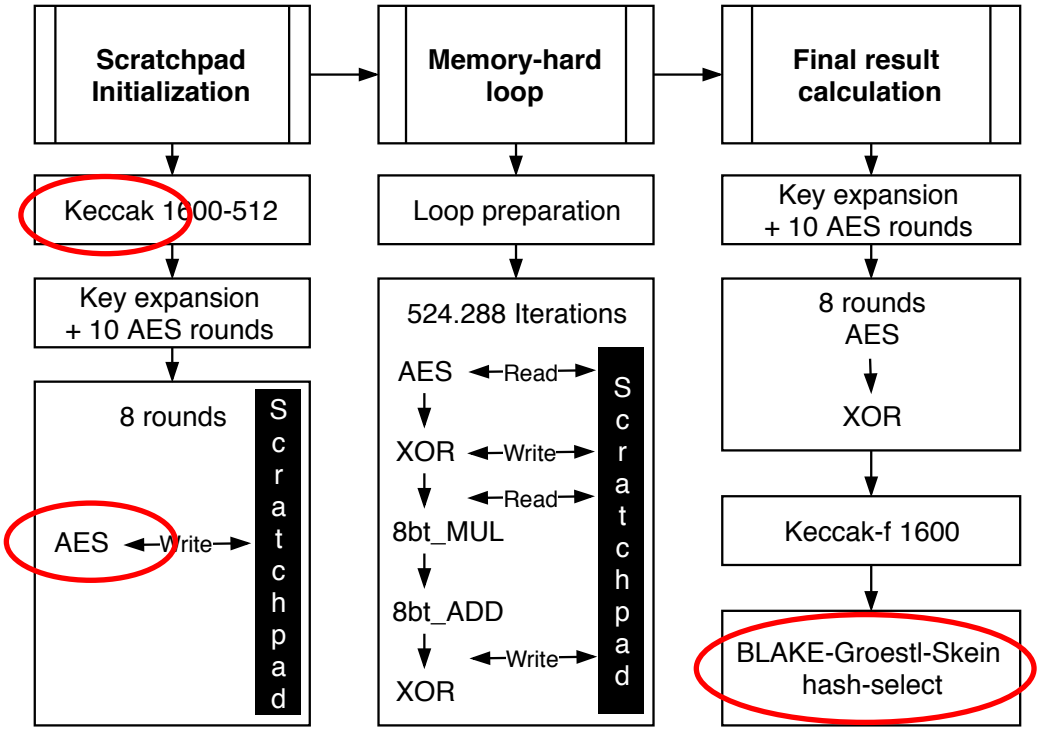
CryptoNight Algorithm

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



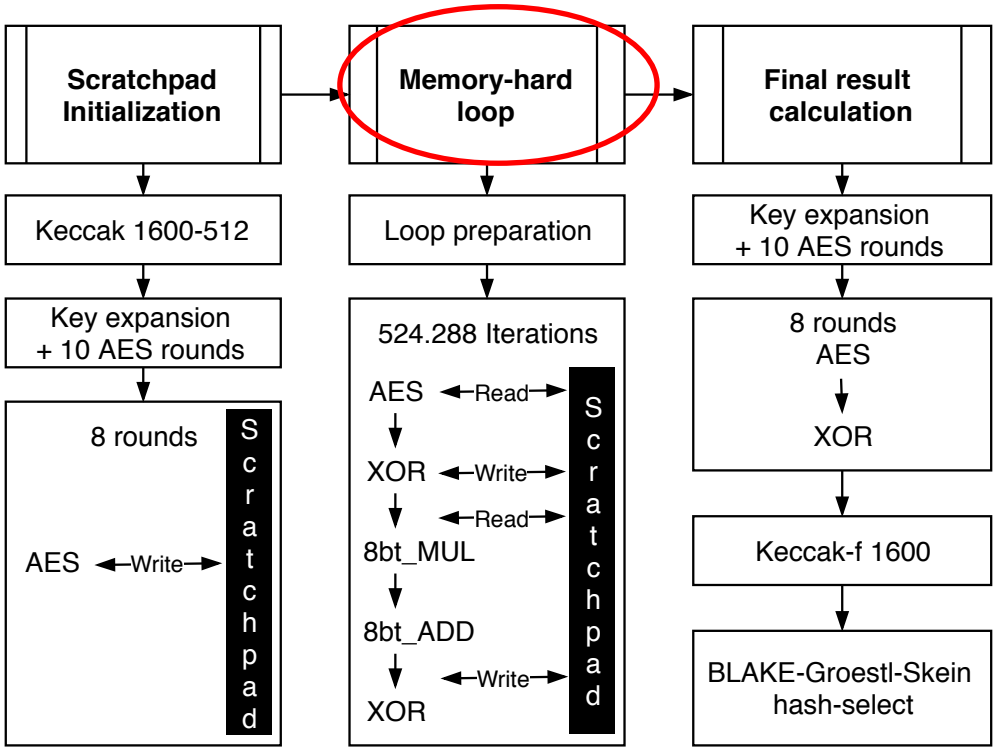
CryptoNight Algorithm

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



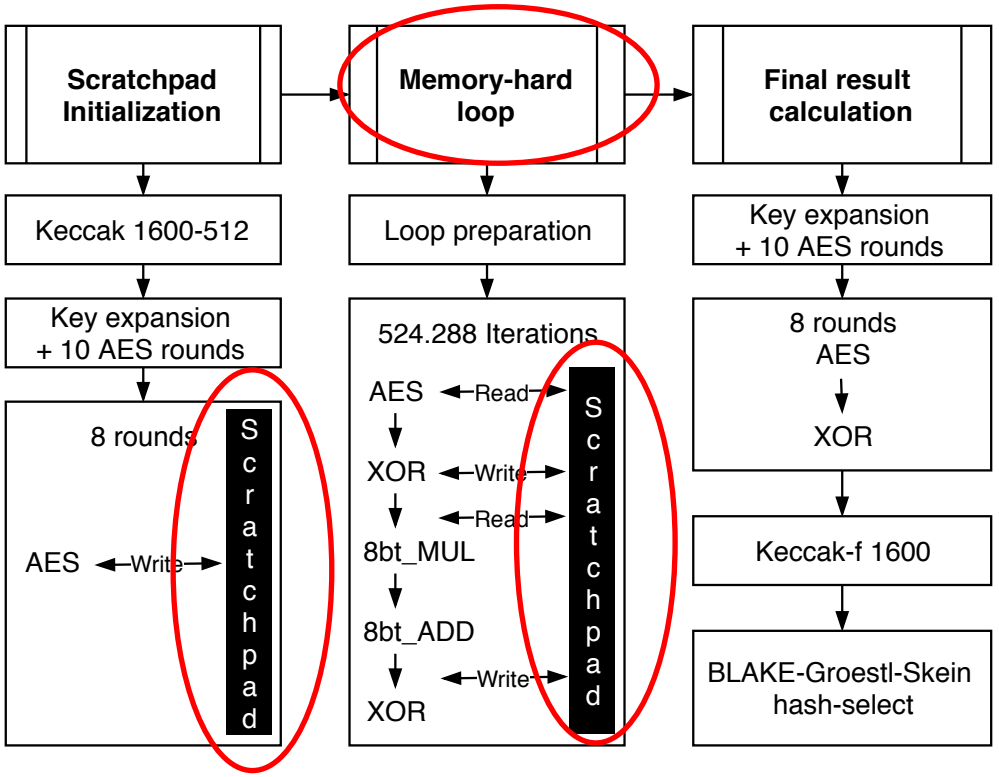
CryptoNight Algorithm

- 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

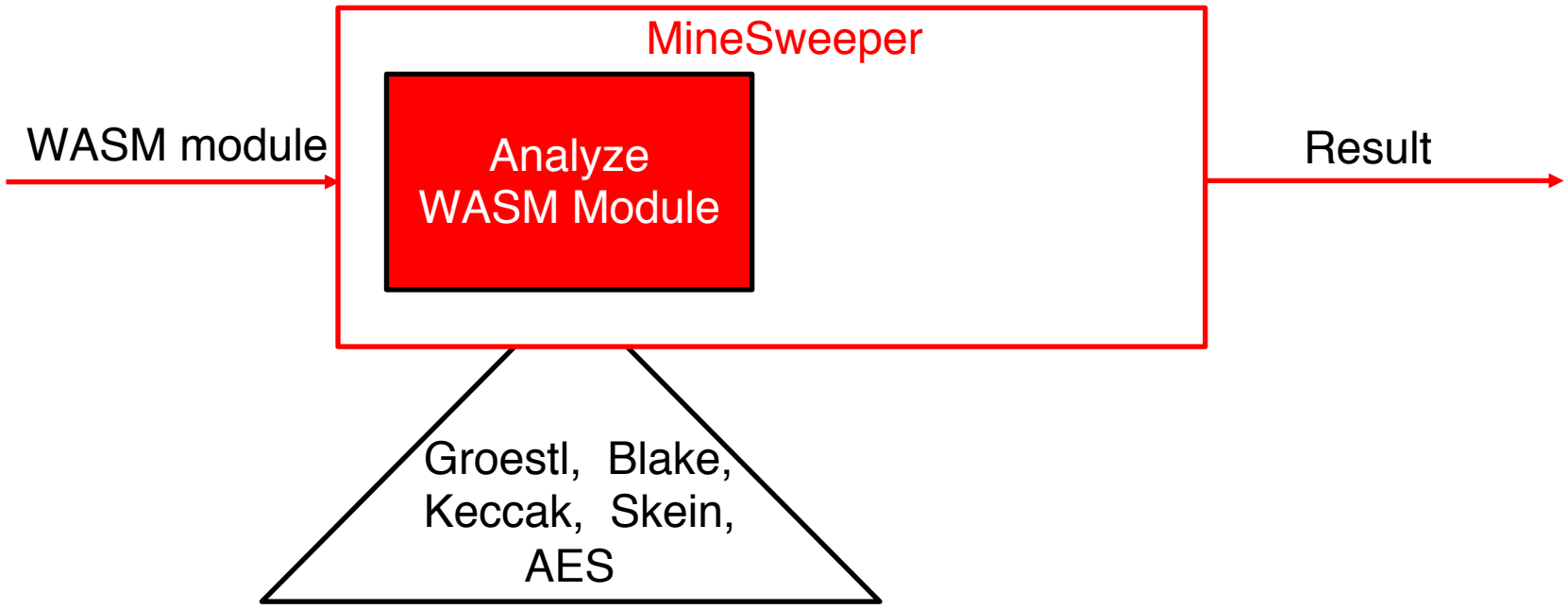


CryptoNight Algorithm

- 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



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 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
      ….
```

- 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

# of samples	CryptoNight Primitives Detected	
30	Groestl, Blake, Keccak, Skein, AES	Cryptominer
3	Groestl, Blake, Keccak, Skein	Cryptominer
3	Groestl, Blake	Cryptominer
4	----	Benign

Evaluation of CryptoNight detection

# of samples	CryptoNight Primitives Detected	
30	Groestl, Blake, Keccak, Skein, AES	Cryptominer
3	Groestl, Blake, Keccak, Skein	Cryptominer
3	Groestl, Blake	Cryptominer
4	----	Benign

Evaluation of CryptoNight detection

# of samples	CryptoNight Primitives Detected	
30	Groestl, Blake, Keccak, Skein, AES	Cryptominer
3	Groestl, Blake, Keccak, Skein	Cryptominer
3	Groestl, Blake	Cryptominer
4	----	Benign

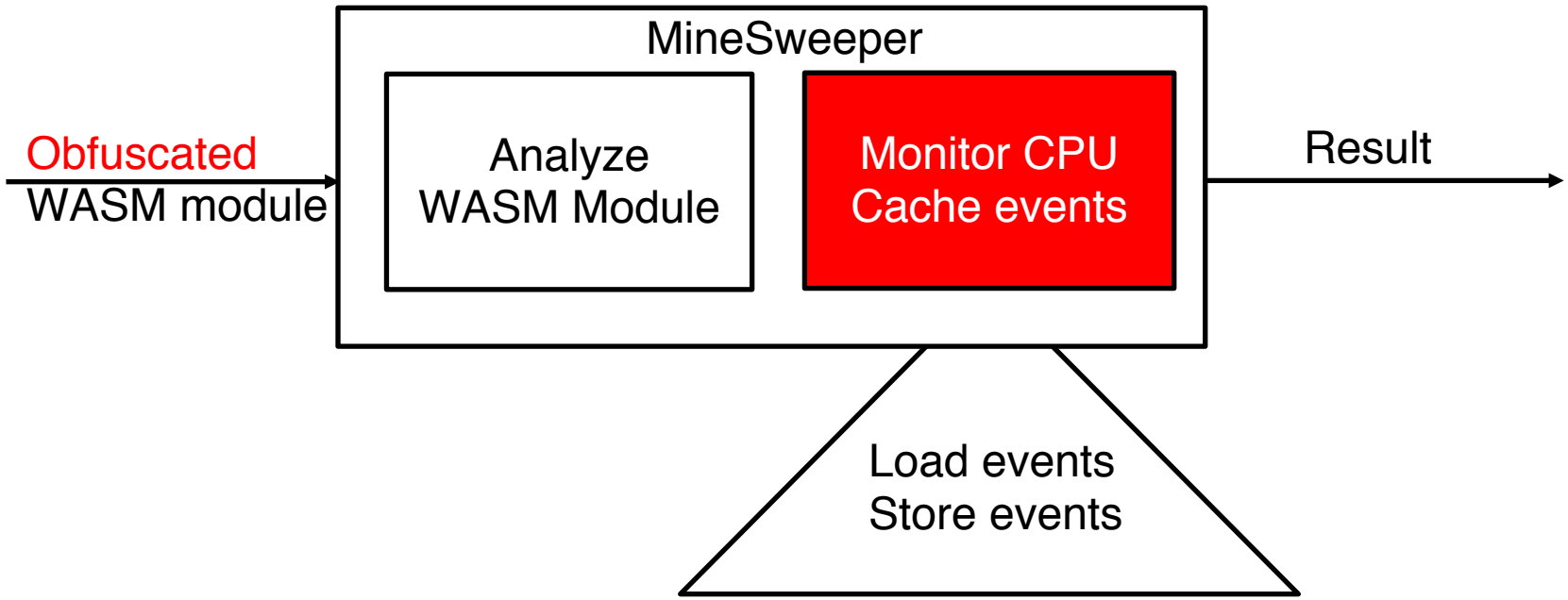
Evaluation of CryptoNight detection

# of samples	CryptoNight Primitives Detected	
30	Groestl, Blake, Keccak, Skein, AES	Cryptominer
3	Groestl, Blake, Keccak, Skein	Cryptominer
3	Groestl, Blake	Cryptominer
4	----	Benign

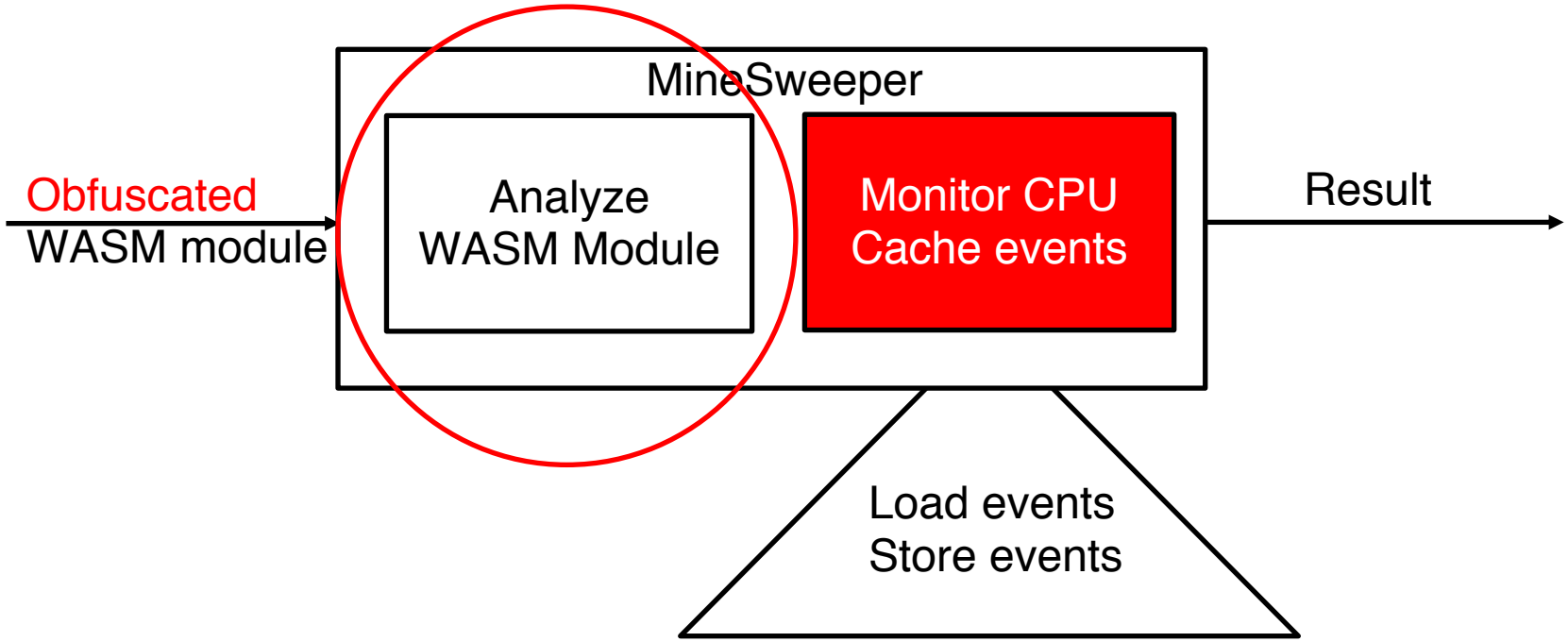
Evaluation of CryptoNight detection

# of samples	CryptoNight Primitives Detected	
30	Groestl, Blake, Keccak, Skein, AES	Cryptominer
3	Groestl, Blake, Keccak, Skein	Cryptominer
3	Groestl, Blake	Cryptominer
4	----	Benign

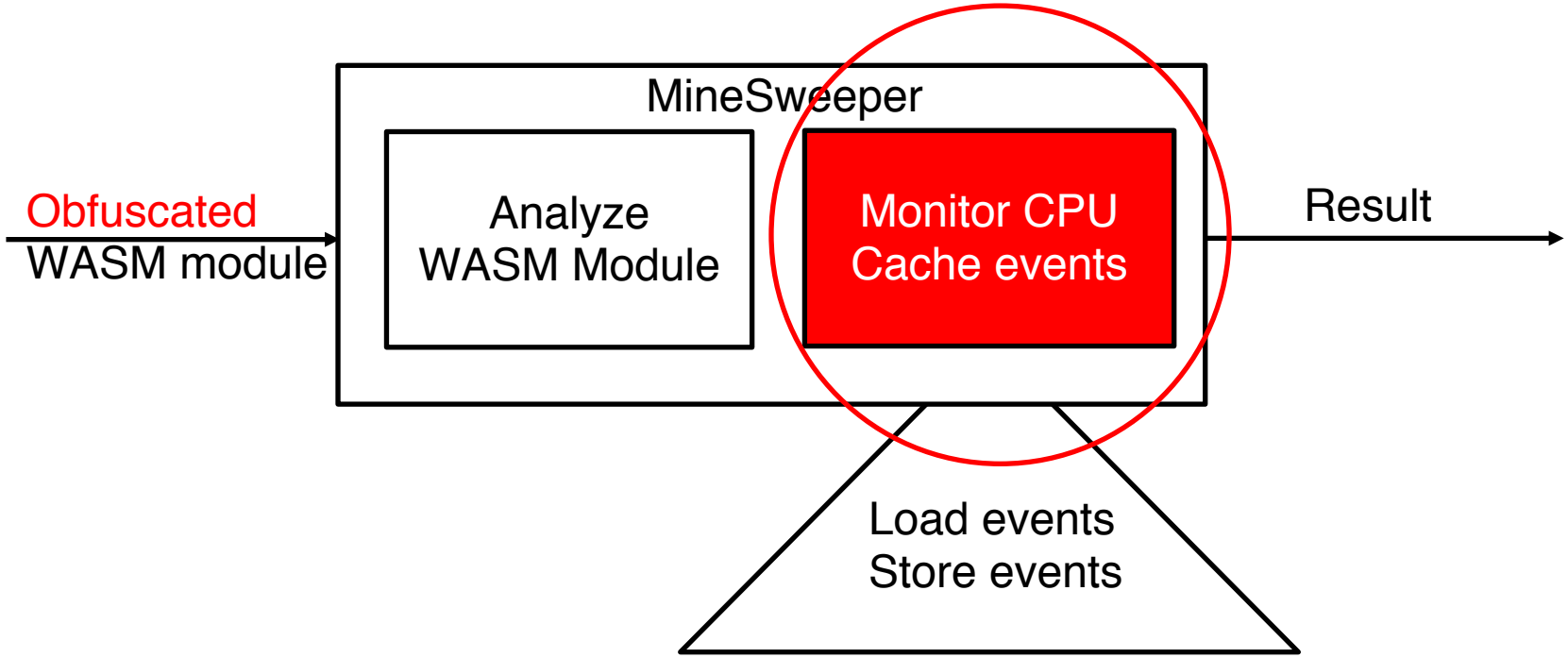
MineSweeper stage 2



MineSweeper stage 2



MineSweeper stage 2

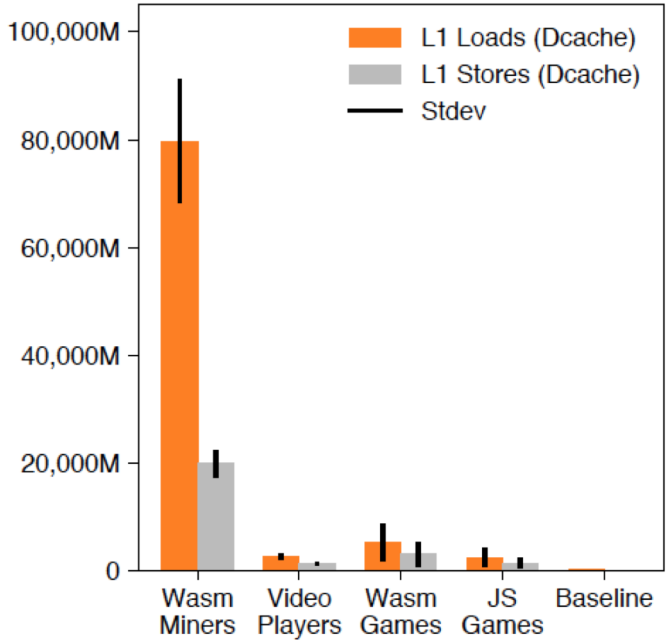


Evaluation of CPU Cache Events Monitoring

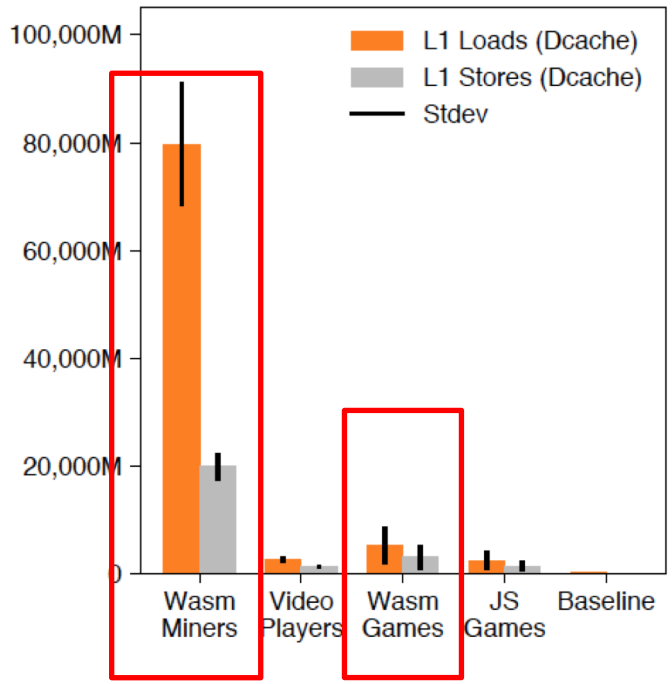
We visited 7 websites from following categories:

1. Cryptominers
2. Video players
3. Wasm-based games
4. JavaScript (JS) games

Evaluation of CPU Cache Events Monitoring



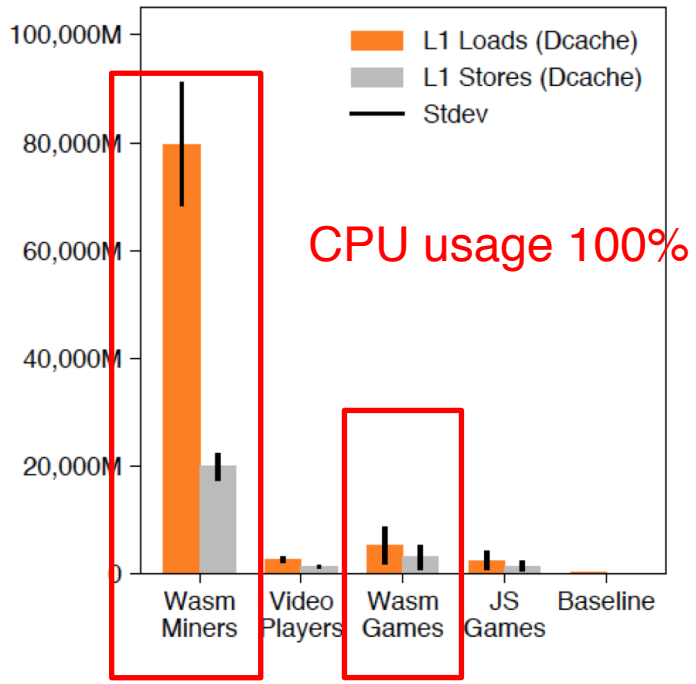
Evaluation of CPU Cache Events Monitoring



Miner induces 35.6 times more L1 dcache load events

Miner induces 16.13 times more L1 dcache store events

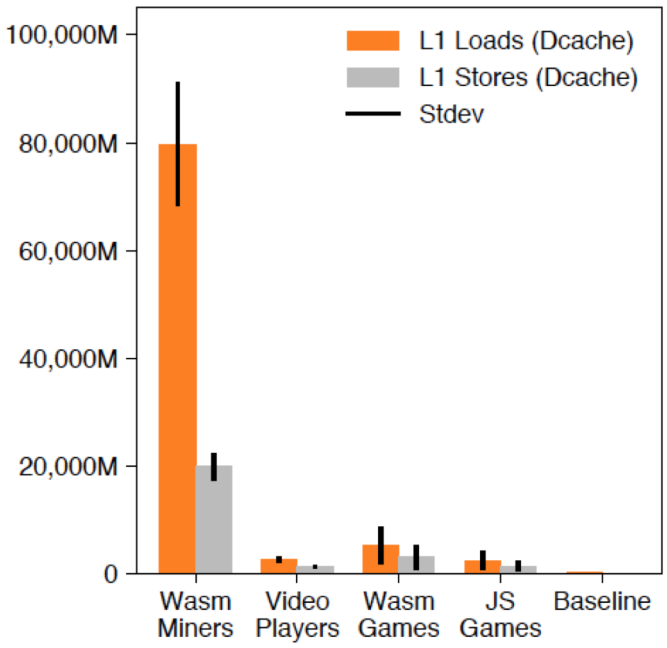
Evaluation of CPU Cache Events Monitoring

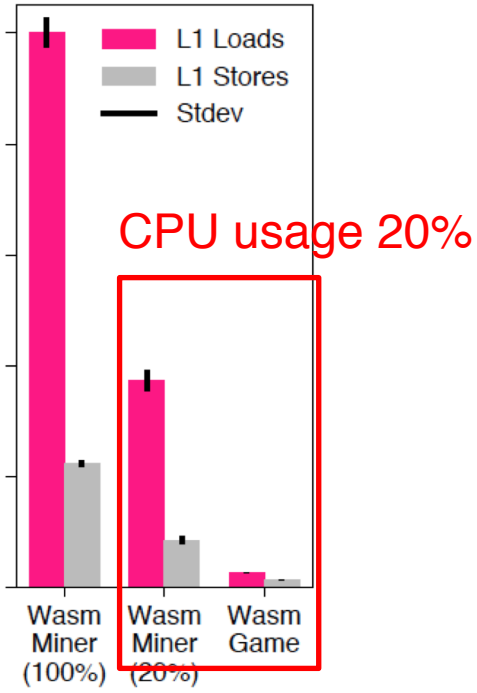


Miner induces 35.6 times more L1 dcache load events

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

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

- 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

VU UNIVERSITY AMSTERDAM

UNIVERSITY OF CALIFORNIA · SANTA BARBARA

TU WIEN

Universiteit Utrecht