The Emergence of Cryptocurrencies

Number of available cryptocurrencies

Nada Lachtar, An Application Agnostic Defense Against the Dark Arts of Cryptojacking, DSN 2021
The Emergence of Cryptocurrencies

Number of available cryptocurrencies

- Bitcoin
- Ethereum
- Zcash
- Monero
- Dogecoin
- Ripple
- Litecoin

Nada Lachtar, An Application Agnostic Defense Against the Dark Arts of Cryptojacking, DSN 2021
A Decentralized Type of Currency
A Decentralized Type of Currency

Customer initiates transaction

Broadcast network of P2P nodes (miners)
A Decentralized Type of Currency

Customer initiates transaction

Broadcast network of P2P nodes (miners)

Mine new block
A Decentralized Type of Currency

Customer initiates transaction

Broadcast network of P2P nodes (miners)

Mine new block

Add newly mined block to blockchain

Nada Lachtar, An Application Agnostic Defense Against the Dark Arts of Cryptojacking, DSN 2021
A Decentralized Type of Currency

Customer initiates transaction

Broadcast network of P2P nodes (miners)

Complete transaction

Add newly mined block to blockchain

Mine new block
The Rise of Cryptojacking Malware
The Rise of Cryptojacking Malware
The Rise of Cryptojacking Malware

Attacker

Victim

Nada Lachtar, An Application Agnostic Defense Against the Dark Arts of Cryptojacking, DSN 2021
The Rise of Cryptojacking Malware
The Rise of Cryptojacking Malware

Nada Lachtar, An Application Agnostic Defense Against the Dark Arts of Cryptojacking, DSN 2021
The Rise of Cryptojacking Malware

Victim

Attacker

Monero

Zcash

Verge

Nada Lachtar, An Application Agnostic Defense Against the Dark Arts of Cryptojacking, DSN 2021
Our Work

• Proposes an application agnostic defense that harnesses innovations at the microarchitecture and OS layers
Our Work

• Proposes an application agnostic defense that harnesses innovations at the microarchitecture and OS layers

• Demonstrate that instructions commonly present in cryptographic functions serve as reliable signatures for fingerprinting cryptojacking activity
Our Work

• Proposes an application agnostic defense that harnesses innovations at the microarchitecture and OS layers

• Demonstrate that instructions commonly present in cryptographic functions serve as reliable signatures for fingerprinting cryptojacking activity

• Characterize a variety of instruction types across several applications while evaluating their relevance for accurate cryptojacking detection
Our Work

• Proposes an application agnostic defense that harnesses innovations at the microarchitecture and OS layers

• Demonstrate that instructions commonly present in cryptographic functions serve as reliable signatures for fingerprinting cryptojacking activity

• Characterize a variety of instruction types across several applications while evaluating their relevance for accurate cryptojacking detection

• Present a design that is robust against code obfuscation, multi-threaded, and throttling attacks while maintaining a low false positive rate
The Cryptojacking Defense System

Microarchitecture Level

Operating System Level

Nada Lachtar, An Application Agnostic Defense Against the Dark Arts of Cryptojacking, DSN 2021
The Cryptojacking Defense System

Microarchitecture Level

Operating System Level

Front End

ucode Decoder
BPU Fetch
ITLB I$
The Cryptojacking Defense System

Nada Lachtar, An Application Agnostic Defense Against the Dark Arts of Cryptojacking, DSN 2021
The Cryptojacking Defense System

Nada Lachtar, An Application Agnostic Defense Against the Dark Arts of Cryptojacking, DSN 2021
The Cryptojacking Defense System

Front End
- ucode Decoder
- BPU Fetch
- ITLB I$

Out-of-Order Engine
- Exec. Units
- Retire
- ROB
- Scheduler

ROB
- ADD ….,r5,....
- XOR ….,r3,....
- CMP ….,r2,....
- ROR ….,r4,....
- SUB ….,r1,....
- SRL ….,r5,....

Microarchitecture Level

Scheduler
- Sample Counter
- Update Struct
- Check Threshold
- Select Next Task
- Context Switch

Operating System Level

Nada Lachtar, An Application Agnostic Defense Against the Dark Arts of Cryptojacking, DSN 2021
The Cryptojacking Defense System

Microarchitecture Level

- Core
  - ucode Decoder
  - BPU Fetch
  - ITLB I$

Front End

- Core
  - ucode Decoder
  - BPU Fetch
  - ITLB I$

Out-of-Order Engine

- Core
  - Exec. Units
  - Retire
  - ROB
  - Scheduler

ROB

- Microarchitecture Level
  - Performance Counters
    - PC1
    - PC2
    - PC3
  - ADD ....,r5,....
  - XOR ....,r3,....
  - CMP ....,r2,....
  - ROR ....,r4,....
  - SUB ....,r1,....
  - SRL ....,r5,....

Scheduler

- Operating System Level
  - Sample Counter
  - Update Struct
  - Check Threshold
  - Select Next Task
  - Context Switch

Nada Lachtar, An Application Agnostic Defense Against the Dark Arts of Cryptojacking, DSN 2021

```
struct task_struct
{
    pid;
    tgid;
    ...
    *rsx_counter;
}
```
The Cryptojacking Defense System

Nada Lachtar, An Application Agnostic Defense Against the Dark Arts of Cryptojacking, DSN 2021
Experimental Framework

- Gem5 Simulator
- Ubuntu OS 16.04
- Linux kernel v4.19.91
- Intel Software Development Emulator
Experimental Framework

- Gem5 Simulator
- Ubuntu OS 16.04
- Linux kernel v4.19.91
- Intel Software Development Emulator
- SPEC2k6 Benchmark Suite
- 150 Standard User Apps
- Crypto-wallets & Decentralized Apps
- Mining Services

Nada Lachtar, An Application Agnostic Defense Against the Dark Arts of Cryptojacking, DSN 2021
Cryptojacking Evasion Techniques

• Code Obfuscation Attacks

\[ p = \neg(\neg p) \]
\[ p \lor q = \overline{p} \land \overline{q} \]
Cryptojacking Evasion Techniques

- Code Obfuscation Attacks

- Multi-threaded Attacks

\[ p = \sim(\sim p) \]
\[ p \lor q = \overline{p} \land \overline{q} \]
Cryptojacking Evasion Techniques

- Code Obfuscation Attacks
- Multi-threaded Attacks
- Throttling Attacks

\[ p = \neg(\neg p) \]
\[ p \lor q = \overline{p} \land \overline{q} \]
Mitigating Code Obfuscation Attacks

• Substitute Rotate Instructions

\[ R_i^n = S_i^n \lor S_r^{64-n} \]

\[ R_r^n = S_r^n \lor S_l^{64-n} \]
Mitigating Code Obfuscation Attacks

• Substitute Rotate Instructions

\[ R_l^n = S_l^n \vee S_r^{64-n} \]

\[ R_r^n = S_r^n \vee S_l^{64-n} \]

• Track Rotate, Shift, and XOR (RSX) instructions
Mitigating Code Obfuscation Attacks

• Substitute Rotate Instructions

\[ R_l^n = S_l^n \lor S_r^{64-n} \]

\[ R_r^n = S_r^n \lor S_l^{64-n} \]

• Track Rotate, Shift, and XOR (RSX) instructions

Total number of Rotate, Shift, and XOR instructions (Millions)
Mitigating Code Obfuscation Attacks

- Substitute Rotate Instructions

\[ R^n_l = S^n_l \lor S^n_{64-n} \]
\[ R^n_r = S^n_r \lor S^n_{64-n} \]

- Track Rotate, Shift, and XOR (RSX) instructions

Total number of Rotate, Shift, and XOR instructions (Millions)

SHA2: 3x higher
SHA3: 3.5x higher

124.6M
Mitigating Code Obfuscation Attacks

• Substitute Exclusive-OR instructions

\[ A \oplus B = AB \lor \bar{A}B \]
Mitigating Code Obfuscation Attacks

• Substitute Exclusive-OR instructions

\[ A \oplus B = A\overline{B} \lor \overline{A}B \]

• Track Rotate, Shift, XOR, and OR (RSXO) instructions
Mitigating Code Obfuscation Attacks

• Substitute Exclusive-OR instructions

\[ A \oplus B = AB \lor \bar{A}\bar{B} \]

• Track Rotate, Shift, XOR, and OR (RSXO) instructions

Total number of Rotate, Shift, XOR, and OR instructions (Millions)
Mitigating Code Obfuscation Attacks

- Substitute Exclusive-OR instructions

\[ A \oplus B = AB \lor \overline{AB} \]

- Track Rotate, Shift, XOR, and OR (RSXO) instructions

Total number of Rotate, Shift, XOR, and OR instructions (Millions)

SHA2: 7x higher
SHA3: 9x higher

Nada Lachtar, An Application Agnostic Defense Against the Dark Arts of Cryptojacking, DSN 2021
Mitigating Code Obfuscation Attacks

```html
<script>
var miner = CoinHive.Anonymous('SK_OBKc7fs7W3bJHMsAmdHzJ', {
  threads: 1,
  autoThreads: false,
  throttle: 0.3,
});
miner.start();
</script>

Malicious Code

Nada Lachtar, An Application Agnostic Defense Against the Dark Arts of Cryptojacking, DSN 2021
Mitigating Code Obfuscation Attacks

- Distribute workload across multiple threads

```javascript
<script>
  var miner = CoinHive.Anonymous('SK_OBKc7fs7W3bJHMsAmdHzJ', {
    threads: 4,
    autoThreads: false,
    throttle: 0.3,
  });
  miner.start();
</script>
```

Malicious Code
Mitigating Code Obfuscation Attacks

- Distribute workload across multiple threads
- Allocate threads to different cores
Mitigating Multi-threaded Attacks

Malicious Code

```html
<script>
var miner = CoinHive.Anonymous('SK_OBKc7fs7W3bJHMsAmdHzJ', {
    threads: 4,
    autoThreads: false,
    throttle: 0.3,
});
miner.start();
</script>
```
Mitigating Multi-threaded Attacks

```c
struct task_struct {
    pid;
    tgid;
    ...
    tgid_rsx_t *rsx_ptr;
};
```

Multi-threaded Program

```javascript
<script>
var miner = CoinHive.Anonymous('SK_OBkC7fs7W3bJHMsAmdHzJ', {
    threads: 4,
    autoThreads: false,
    throttle: 0.3,
});
miner.start();
</script>
```

Malicious Code
Mitigating Multi-threaded Attacks

```c
struct tgid_rsx_t {
    rsx_count;
    tcount;
}

struct task_struct {
    pid;
    tgid;
    ...
    tgid_rsx_t *rsx_ptr;
} t0
  t1
  t2
  t3

Multi-threaded Program

<script>
var miner = CoinHive.Anonymous('SK_OBKc7fs7W3bJHMsAmdHzJ', {
    threads: 4,
    autoThreads: false,
    throttle: 0.3,
});
miner.start();
</script>

Malicious Code

Nada Lachtar, An Application Agnostic Defense Against the Dark Arts of Cryptojacking, DSN 2021
Mitigating Multi-threaded Attacks

Nada Lachtar, An Application Agnostic Defense Against the Dark Arts of Cryptojacking, DSN 2021

```c
struct tgid_rsx_t {
    rsx_count;
    tcount;
};

struct task_struct {
    pid;
    tgid;
    ...
    tgid_rsx_t *rsx_ptr;
};
```

```javascript
<script>
var miner = CoinHive.Anonymous('SK_OBKc7fs7W3bJHMsAmdHzJ', {
    threads: 4,
    autoThreads: false,
    throttle: 0.3,
});
miner.start();
</script>
```
Mitigating Multi-threaded Attacks

```c
struct tgid_rsx_t {
  rsx_count;
  tcount;
}

struct task_struct {
  pid;
  tgid;
  ...
  tgid_rsx_t *rsx_ptr;
}
```

```javascript
<script>
var miner = CoinHive.Anonymous('SK_OBKc7fs7W3bJHMsAmdHzJ', {
  threads: 4,
  autoThreads: false,
  throttle: 0.3,
});
miner.start();
</script>
```

Malicious Code

Nada Lachtar, An Application Agnostic Defense Against the Dark Arts of Cryptojacking, DSN 2021
Mitigating Multi-threaded Attacks

```c
struct task_struct
{
    pid;
    tgid;
    ...
    tgid_rsx_t *rsx_ptr;
}
```

```javascript
var miner = CoinHive.Anonymous('SK_OBKc7fs7W3bJHMsAmdHzJ', {
    threads: 4,
    autoThreads: false,
    throttle: 0.3,
});
miner.start();
</script>
```

Malicious Code

Nada Lachtar, An Application Agnostic Defense Against the Dark Arts of Cryptojacking, DSN 2021
Mitigating Multi-threaded Attacks

```c
struct task_struct {
    pid;
    tgid;
    ...
    tgid_rsx_t *rsx_ptr;
}:
```

```javascript
var miner = CoinHive.Anonymous('SK_OBKc7fs7W3bJHMsAmdHzJ', {
threads: 4,
autoThreads: false,
throttle: 0.3,
});
miner.start();
```

Nada Lachtar, An Application Agnostic Defense Against the Dark Arts of Cryptojacking, DSN 2021
Mitigating Multi-threaded Attacks

```
struct task_struct {
    pid;
    tgid;
...
    tgid_rsx_t *rsx_ptr;
}
```

```
INPUT

Multi-threaded Program

var miner = CoinHive.Anonymous('SK_OBKe7fs7W3bJHMsAmdHzJ',
    {
        threads: 4,
        autoThreads: false,
        throttle: 0.3,
    });
miner.start();
```

```
long _do_fork()
{
    ... If (p->tgid != parent->tgid) {
        create_tgid_crypt_struct(p);
    } else {
        p->rsx_ptr = parent->rsx_ptr;
    }
    wake_up_new_task(p);
    ...
}
```

Malicious Code
Mitigating Multi-threaded Attacks

Malicious Code

```javascript
var miner = CoinHive.Anonymous('SK_OBKc7fs7W3bJHMsAmdHzJ', {
  threads: 4,
  autoThreads: false,
  throttle: 0.3,
});
miner.start();
</script>

Nada Lachtar, An Application Agnostic Defense Against the Dark Arts of Cryptojacking, DSN 2021
Mitigating Multi-threaded Attacks

```c
struct tgid_rsx_t {
    rsx_count;
    tcount;
}

long _do_fork(){
    ...
    if (p->tgid != parent->tgid) {
        create_tgid_crypt_struct(p);
    } else {
        p->rsx_ptr = parent->rsx_ptr;
        wake_up_new_task(p);
    }
    ...
}

struct task_struct {
    pid;
    tgid;
    ...
    tgid_rsx_t *rsx_ptr;
}

Malicious Code

<SCRIPT>
var miner = CoinHive.Anonymous('SK_OBKc7fs7W3bJHMsAmdHzJ', {
    threads: 4,
    autoThreads: false,
    throttle: 0.3,
});
miner.start();
</SCRIPT>
```
Mitigating Multi-threaded Attacks

Malicious Code

```javascript
Multi-threaded Program

```
Mitigating Throttling Attacks

```
<script>
var miner = CoinHive.Anonymous('SK_OBKe7fs7W3bJHMsAmgHzJ', {
    threads: 4,
    autoThreads: false,
    throttle: 0.3,
});
miner.start();
</script>
```

Malicious Code
Mitigating Throttling Attacks

- Use limited amount of the system’s power

```javascript
<script>
var miner = CoinHive.Anonymous('SK_OBKc7fs7W3bJHMsAmdHzJ', {
  threads: 4,
  autoThreads: false,
  throttle: 0.3,
});
miner.start();
</script>
```

Malicious Code
Mitigating Throttling Attacks

- Use limited amount of the system’s power
- Common throttling rate is 30%

```html
<script>
var miner = CoinHive.Anonymous('SK_OBKc7fs7W3bJHMsAmdHzJ', {
    threads: 4,
    autoThreads: false,
    throttle: 0.3,
});
miner.start();
</script>

Malicious Code

70% processing power

Nada Lachtar, An Application Agnostic Defense Against the Dark Arts of Cryptojacking, DSN 2021
Mitigating Throttling Attacks

- Ramme has the highest RSX count (5.2B) upon tested apps
- Monero mining service has 65x higher RSX count than Ramme
- Zcash mining service has $3 \times 10^3$ higher RSX count than Ramme
- Non-mining Crypto Apps have an avg. of 1B RSX count

**Total number of Rotate, Shift, XOR instructions (Billions)**
Mitigating Throttling Attacks

- Ramme has the highest RSX count (5.2B) upon tested apps
- Monero mining service has 65x higher RSX count than Ramme
- Zcash mining service has $3 \times 10^3$ higher RSX count than Ramme
- Non-mining Crypto Apps have an avg. of 1B RSX count

Total number of Rotate, Shift, XOR instructions (Billions)
Mitigating Throttling Attacks

- Ramme has the highest RSX count (5.2B) upon tested apps
- Monero mining service has 65x higher RSX count than Ramme
- Zcash mining service has $3 \times 10^3$ higher RSX count than Ramme
- Non-mining Crypto Apps have an avg. of 1B RSX count
Mitigating Throttling Attacks

- Ramme has the highest RSX count (5.2B) upon tested apps
- Monero mining service has 65x higher RSX count than Ramme
- Zcash mining service has $3 \times 10^3$ higher RSX count than Ramme
- Non-mining Crypto Apps have an avg. of 1B RSX count

Total number of Rotate, Shift, XOR instructions (Billions)
Mitigating Throttling Attacks

- Ramme has the highest RSX count (5.2B) upon tested apps
- Monero mining service has 65x higher RSX count
- Zcash mining service has $3 \times 10^3$ higher RSX count than Ramme
- Non-mining Crypto Apps have an avg. of 1B RSX count

Total number of Rotate, Shift, XOR instructions (Billions)

> 50% Throttling Rate
Mitigating Throttling Attacks

- Principle Components Analysis
- Reduce feature set from 527 to 11
- SVM and Logistic Regression: 100% detection rate
- SVM – Less than 2% False Positives
- Logistic Regression – 40% False Positives

Detection rate as a function of throttling rate
Application Agnostic Solution
Code Obfuscation Attacks
Multi-threaded Attacks
Throttling Attacks
100%

True Positive Rate
100% True Positive Rate

<2% False Positive Rate
100% True Positive Rate

<2% False Positive Rate

<1% Overhead

Nada Lachtar, An Application Agnostic Defense Against the Dark Arts of Cryptojacking, DSN 2021
Thank you!

Nada Lachtar
nlachtar@umich.edu