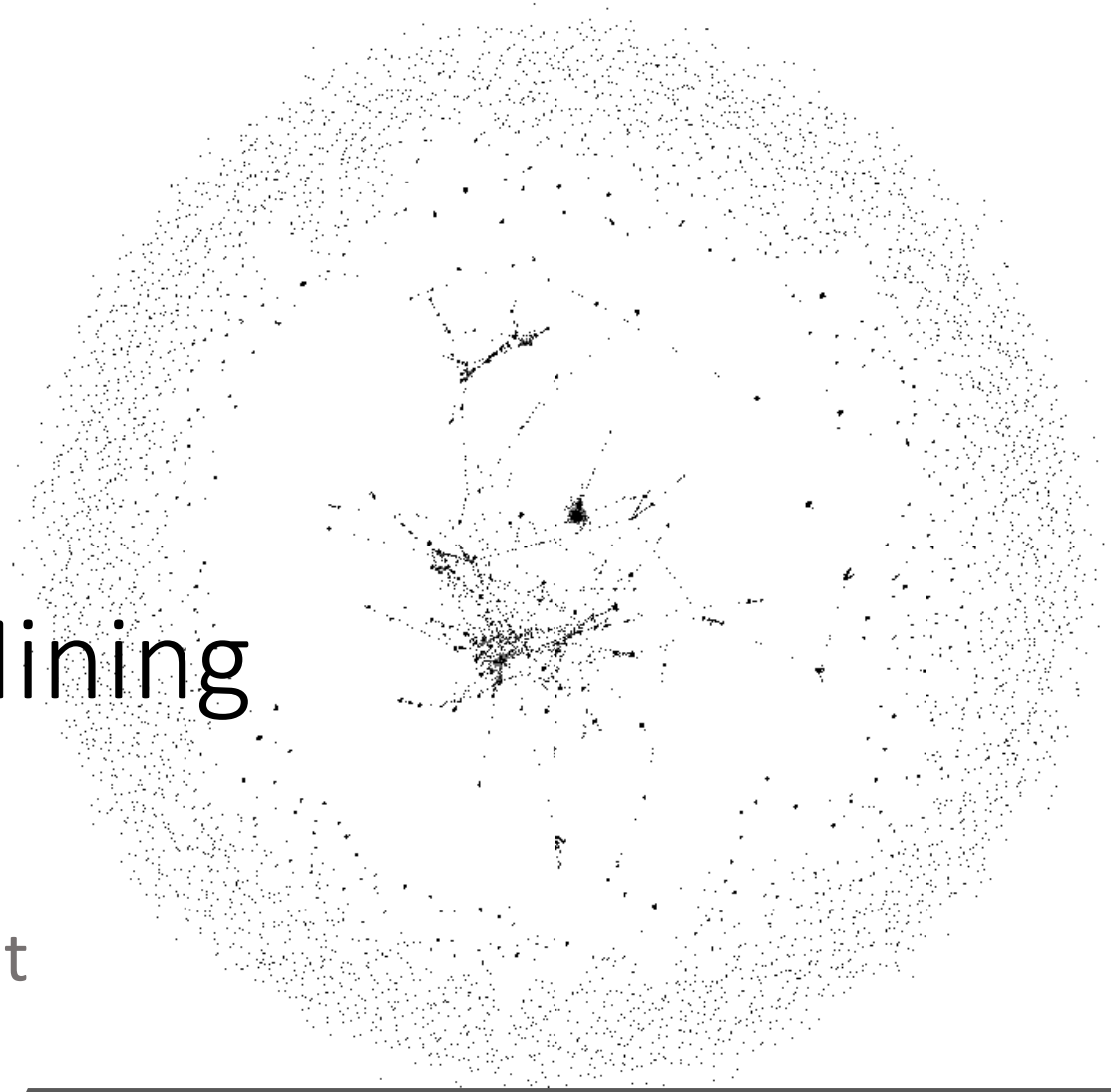


A First Look at the Crypto-Mining Malware Ecosystem

A Decade of Unrestricted Wealth and Profit

Sergio Pastrana

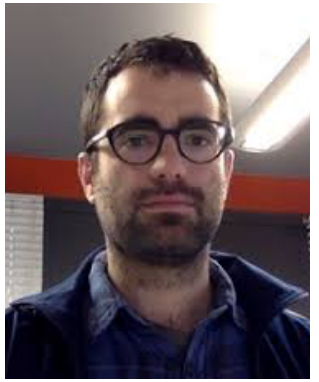
Universidad Carlos III de Madrid

@THANKS:
Slides design by Guillermo Suarez-Tangil

A First Look at the Crypto-Mining Malware Ecosystem: A Decade of Unrestricted Wealth

Sergio Pastrana
Universidad Carlos III de Madrid*
spastran@inf.uc3m.es

Guillermo Suarez-Tangil
King's College London
guillermo.suarez-tangil@kcl.ac.uk



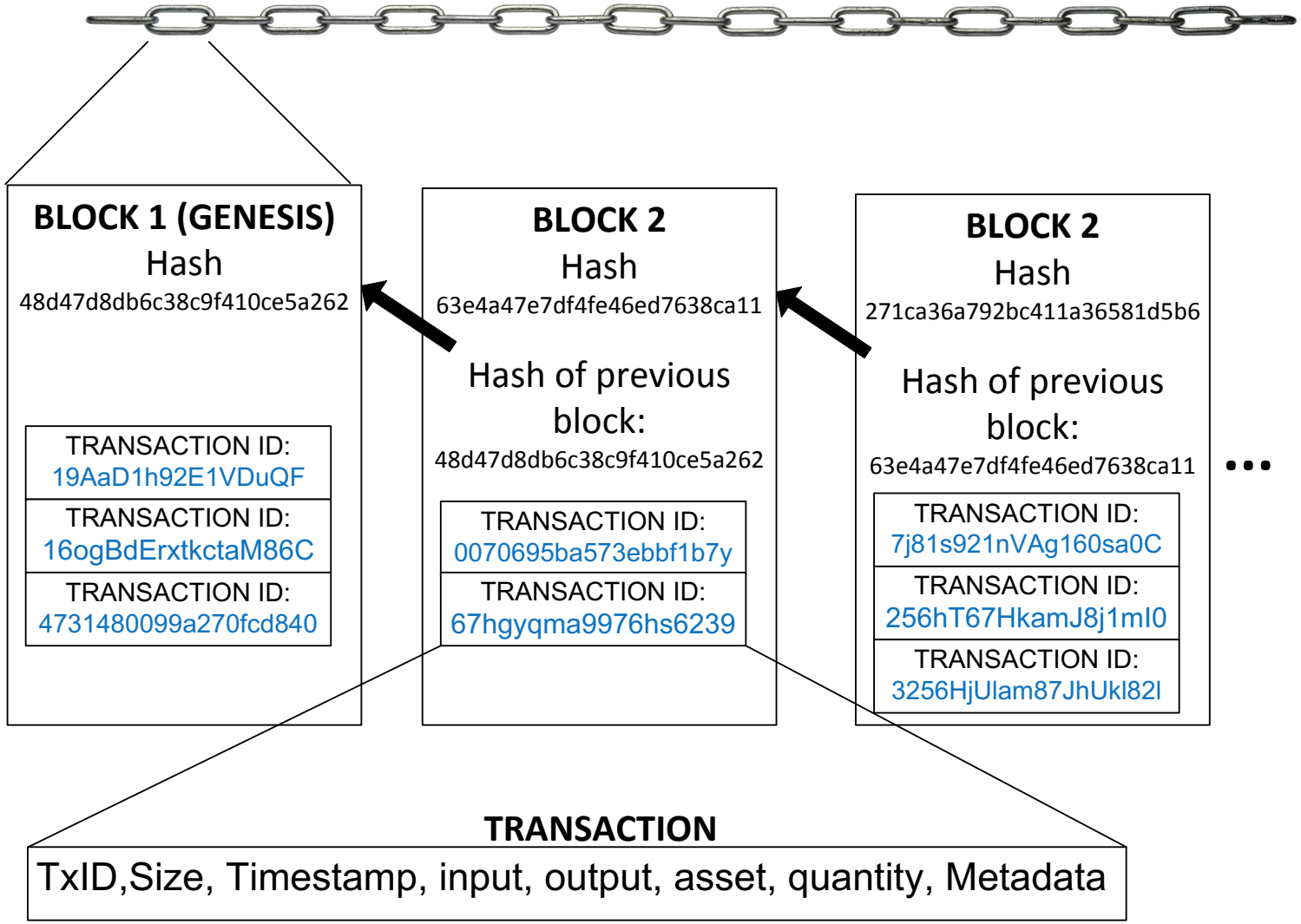
***Abstract*—Illicit crypto-mining leverages resources stolen from victims to mine cryptocurrencies on behalf of criminals. While recent works have analyzed one side of this threat, i.e.: web-browser cryptojacking, only white papers and commercial reports have partially covered binary-based crypto-mining malware. In this paper, we conduct the largest measurement of crypto-mining malware to date, analyzing approximately 4.4 million malware samples (1 million malicious miners), over a period of twelve years from 2007 to 2018. Our analysis pipeline applies both static and dynamic analysis to extract mining profiles, which we leverage to search for samples sold as wallet identifiers and mining tools. Together with public data, this information is used to group samples into campaigns. We then analyze publicly-available payments sent to the wallets from mining-pools as a reward for mining, and estimate profits for the different campaigns.**

Our profit analysis reveals campaigns with multi-million earnings, associating over 4.3% of Monero with illicit mining. We analyze the infrastructure related with the different campaigns, showing that a high proportion of this ecosystem is supported by underground economies such as Pay-Per-Install services. We also uncover novel techniques that allow criminals to run successful campaigns.

https://arxiv.org/pdf/1901.00846.pdf

has different characterizing features and unique challenges, specially when it comes to devising effective countermeasures. For example, in browser-based cryptojacking the damage ceases when the victim stops browsing the site. Also, users can reduce the threat by restricting the use of JavaScript. Meanwhile, crypto-mining malware entails classical malware-related challenges, such as persistence and obfuscation. Also, we observe a new paradigm aimed at evading user- rather than AntiVirus-detection using techniques such as *idle mining* (mining only when the CPU is idle) or reducing CPU consumption when monitoring tools (e.g., Task Manager) are running. For readers unfamiliar with the topic, we refer to *Background* in Appendix A for an introduction to cryptocurrency mining and its threats.

Motivation. While illicit crypto-mining has been less notorious than other threats such as ransomware, it poses nonetheless



Background: Blockchain basics

Cryptocurrency mining

Done by voluntary miners in exchange for a reward

Complex mathematical puzzles (PoW)

Consumes electricity and deteriorates hardware

Illicit crypto-mining

Uses stolen resources to mine cryptocurrencies for free

Types

Web-browser

Binary-based

Crypto-mining malware

A binary-based illicit crypto-mining program operated remotely by a criminal, typically through a botnet

Background: Crypto-mining Malware

The Mining Competition

First-come, first-served basis

- When a new block is added to the blockchain, only the first miner being able to verify the block will get the reward

The race

- The higher the hashrate, the higher the probability to “win” a block

Pools

- Mining is typically done using public mining pools
- Partnership services between various workers where the complexity of the mining challenge is distributed among the partners

Is it all about “men power”?

It is for Monero!

Difficulty to mine new blocks

- Depends on the combined computing power
- Botnets can combine a decent amount of power

Problems with botnets

- They usually lack on specialized hardware (e.g., GPUs, FPGAs, or even ASICs)
- They cost money

Botcoin – Yuxing Huang et al. NDSS 2014

- The potential revenue from Bitcoin mining alone is unlikely to cover the costs of a botnet, but may be attractive as a secondary activity for large botnets with already established primary monetization schemes

Things have changed since 2014

Outline

1. What are the preferred cryptocurrencies mined by criminals?
2. What is the role of the underground economy?
   - What are the tools/techniques adopted?
3. What is the level of sophistication used and how does this affect the earnings?
4. How many actors are involved in this ecosystem and what are their financial profits?
5. Are current countermeasures and intervention approaches effective?

BACKGROUND

THE UNDERGROUND ECONOMY

METHODOLOGY

RESULTS

The depths of the Web: where the criminals operate

The Underground Economy

As simple as:

Cost(Attack) < Potential Revenue

Costs
- They don't pay electricity
- But they need to infect computers

Underground markets play a key role in the business of **malicious crypto-mining**

Users with few technical skills can easily acquire services and tools to set up their own mining campaign

Forums are used for sharing knowledge

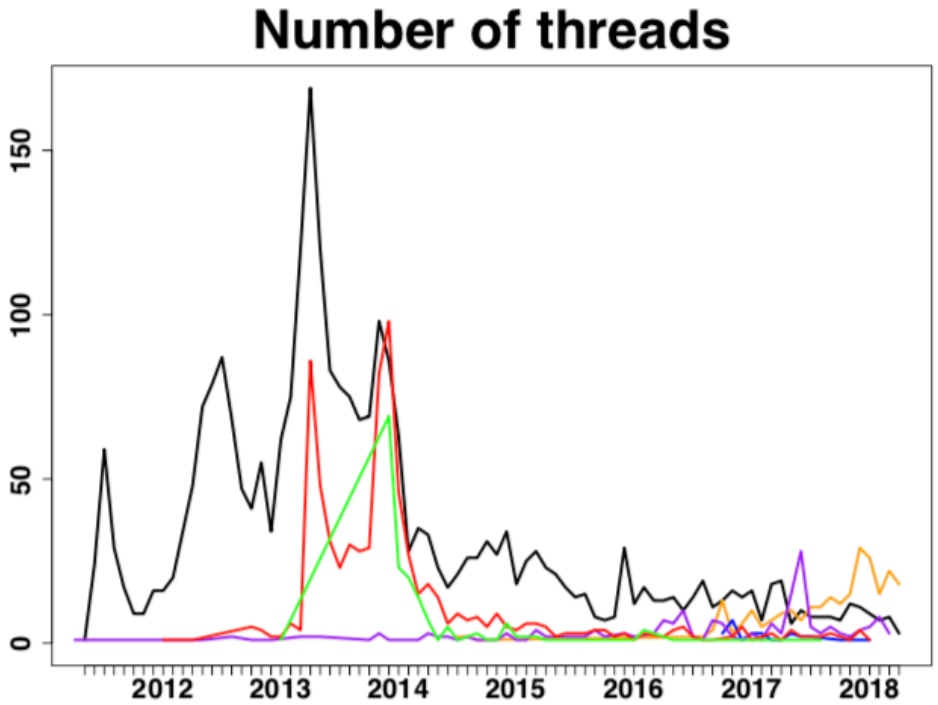
CrimeBB 56M post: Hackforums, Kernelmode, OffensiveCommunity, MPGH, Stresserforums, Greysec,…

The Underground Economy

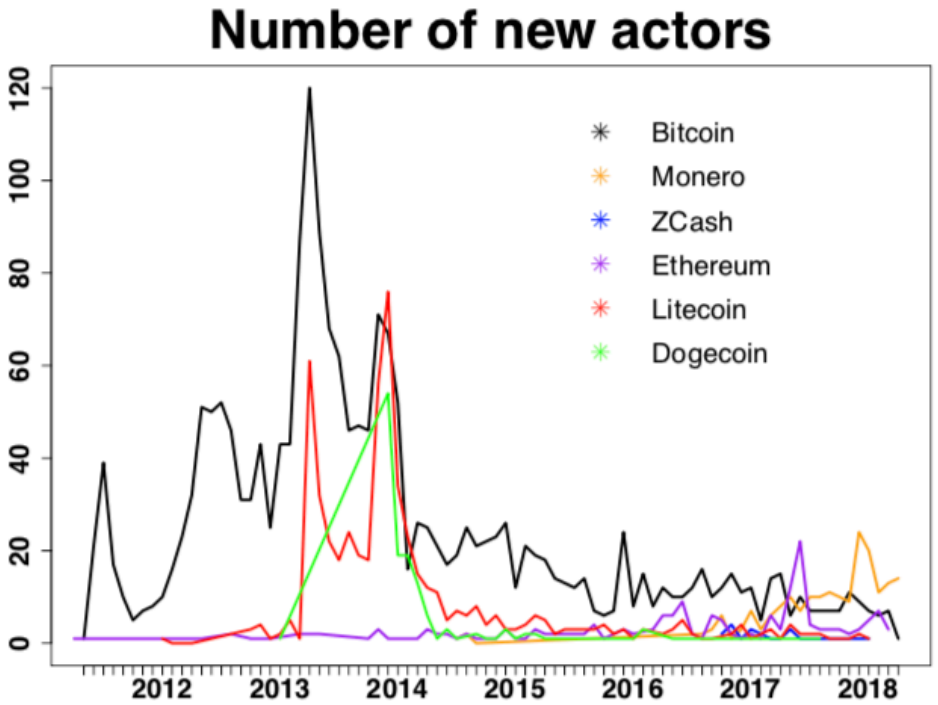
- Inexpensive and sophisticated
  - The average cost for an encrypted Monero miner is 35$
  - Free: "`Miner is free, we charge a fee of 2%`"
  - Vouch copies
- Customized
  - Custom cryptonote miner for $13
  - Stealthy-related techniques such as **idle mining** or **execution-stalling code**
- Support

```
Status: CLEAN
Detections
    AVG - Clean.
    Acavir - Clean.
    ...
    Avast 5 -Clean.
```

"`The latest update has been released. We have removed all of the net reactor obfuscation and switched it. There is now anti emulation and it is FUD.`"



a



b

Figure 1: Number of threads (a) and new actors (b) talking about mining of various cryptocurrencies observed underground forums per month

The Underground Economy

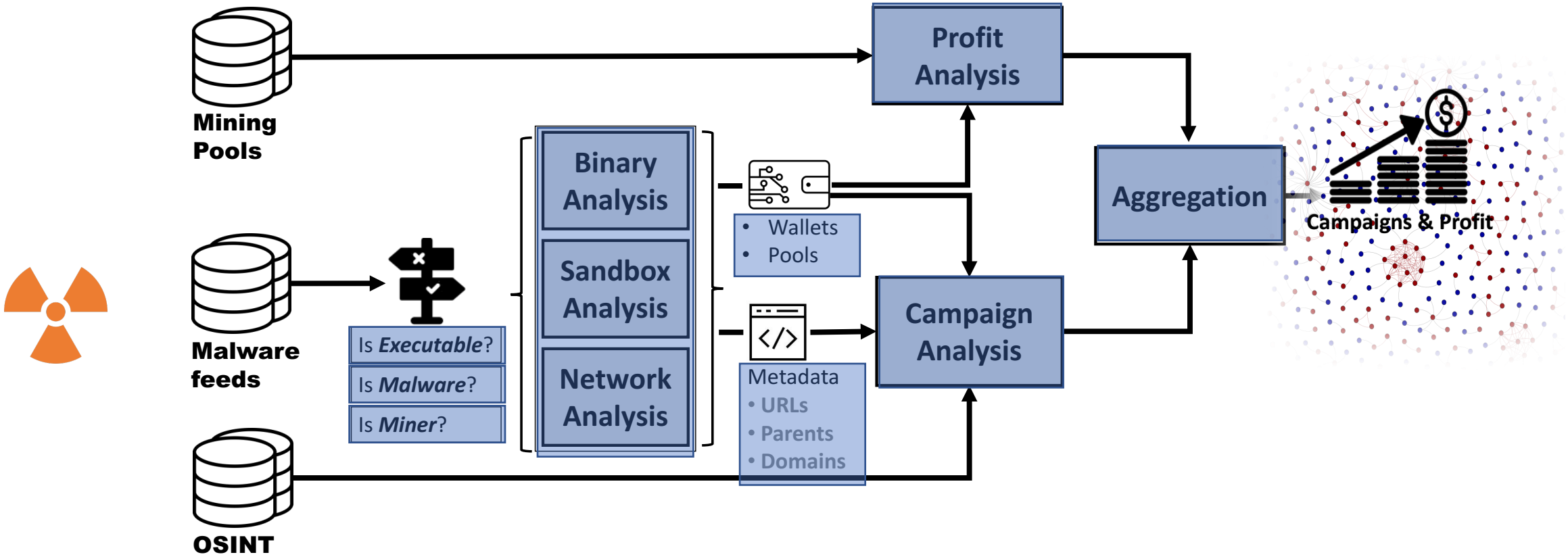
Proliferation

Observed 2 common approaches to create crypto-mining malware

1. The mining tool is encapsulated into a binary with classical malware capabilities to gain persistence and stealthiness
   - anti-sandbox,
   - anti-VM detection,
   - registry key modifications, etc.
2. Instruct existing botnets to download the original mining binary and a configuration file
   - e.g. Set the mining in the background whenever the computer is in idle mode

Take-away: Crypto-mining malware typically rely on open-source tools aimed at benign mining, e.g. XMRig, SRBMiner

Methodology



4.4M malware samples: 1.1M miners and ancillary binaries

Methodology

Architecture

Wallets (i.e., public key of a wallet for):			
Monero	2,472	Aeon	58
Bitcoin	1,585	Sumokoin	18
zCash	184	Intensecoin	8
Ethereum	167	Turtlecoin	3
Electroneum	152	Bytecoin	2
Mixed			16
Sub-total			4,633

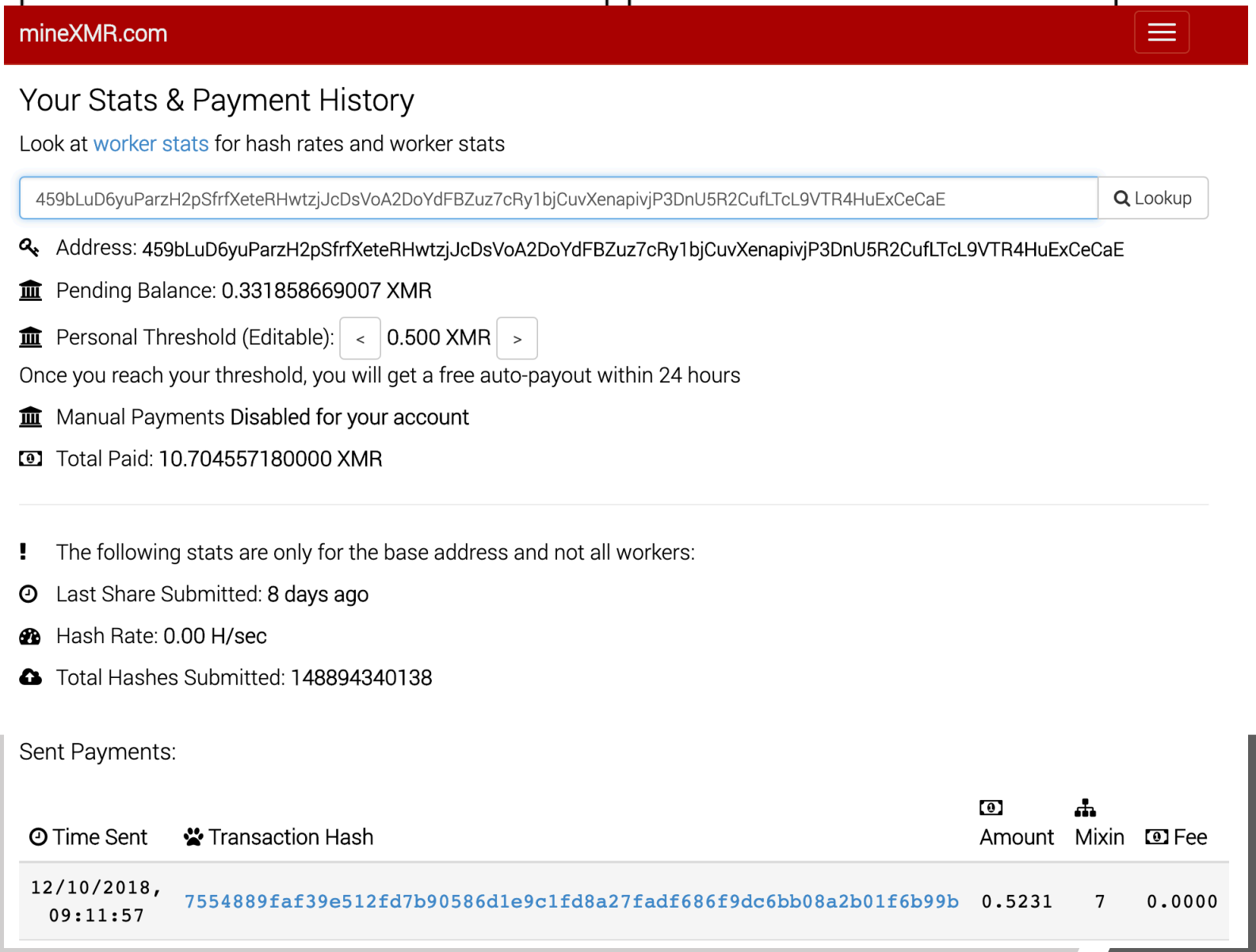
Other Identifiers:	
Email	5,024
Unknown	2,280

TOTAL	11,887

Methodology

Wallets (i.e., public key of a wallet for):			
Monero	2,472	Aeon	58

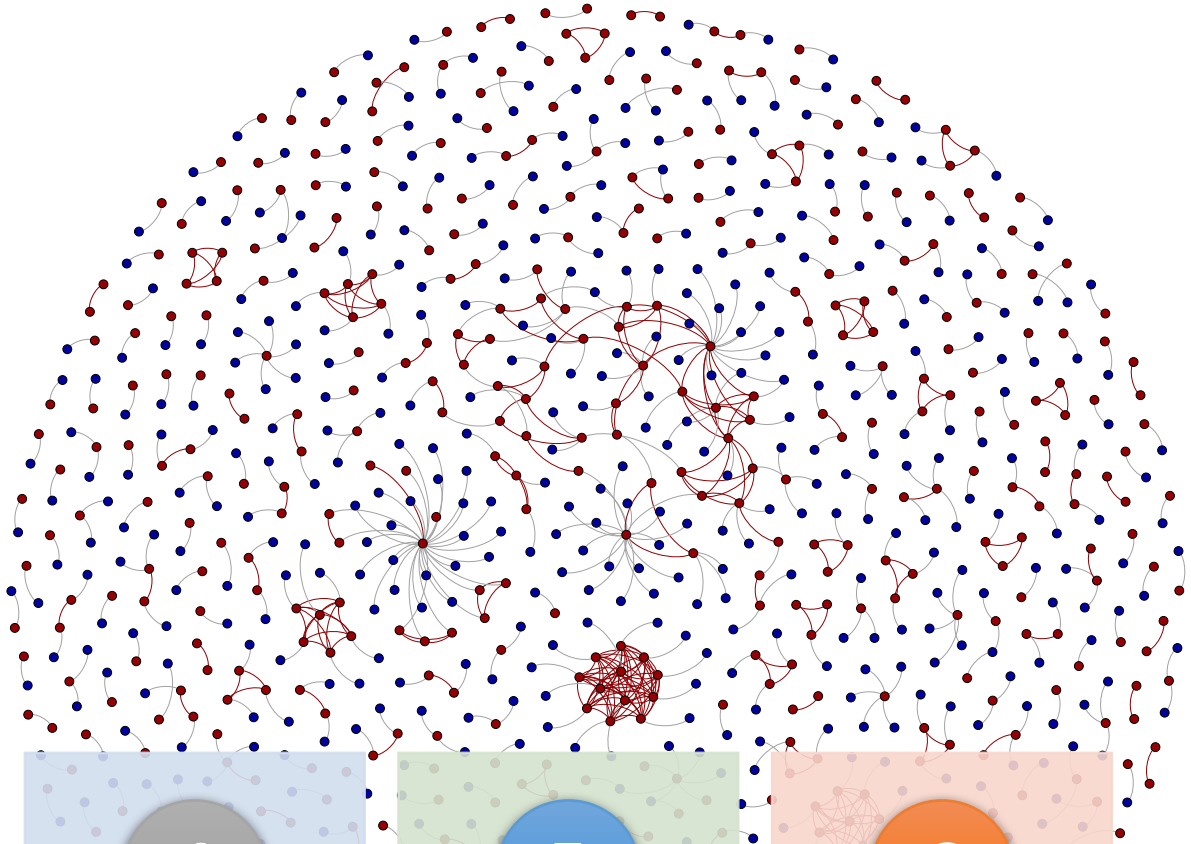
Pool
crypto-pool
dwarfpool
minexmr
prohash
monerohash
nanopool
ppxmr
supportxmr
hashvault
xmrpool
moneropool
bohemianpool



Wallets Extracted

Grouping Features

- Common currencies obfuscate transactions
- We cannot rely on public Blockchain data to aggregate different wallets into related campaigns
- Campaigns
  - Collection of samples
  - Common characterizing features



1. Same identifier
2. Ancestors
3. Hosting servers
4. Known mining campaigns
5. Domain aliases (CNAMEs)
6. Mining proxies

Results

Campaign	#S	#W	Period	XMR	$
C#623	62	7	06/16 to [active]*	163,754	18M
C#3039	19	2	06/16 to 10/18	59,620	8M
C#148	58	1	09/14 to 04/18	32,886	52K
C#685	105	2	08/14 to 04/18	27,982	283K
C#1298	91	14	06/16 to [active]*	27,093	2M
C#7481	6	1	06/16 to 04/18	23,300	1M
C#3318	9	1	06/16 to 05/18	22,520	5M
C#2656	44	1	09/14 to 04/18	21,389	40K
C#2078	25	1	09/14 to 04/18	20,694	37K
C#1440	38	1	08/14 to 04/18	19,995	33K
TOP-10	457	31	14/08/28 - *	419,233	34M
ALL-2218	62 K	2492	14/08/17 - *	720,461	57M

22%

58%

4.5% of Monero in circulation

Results

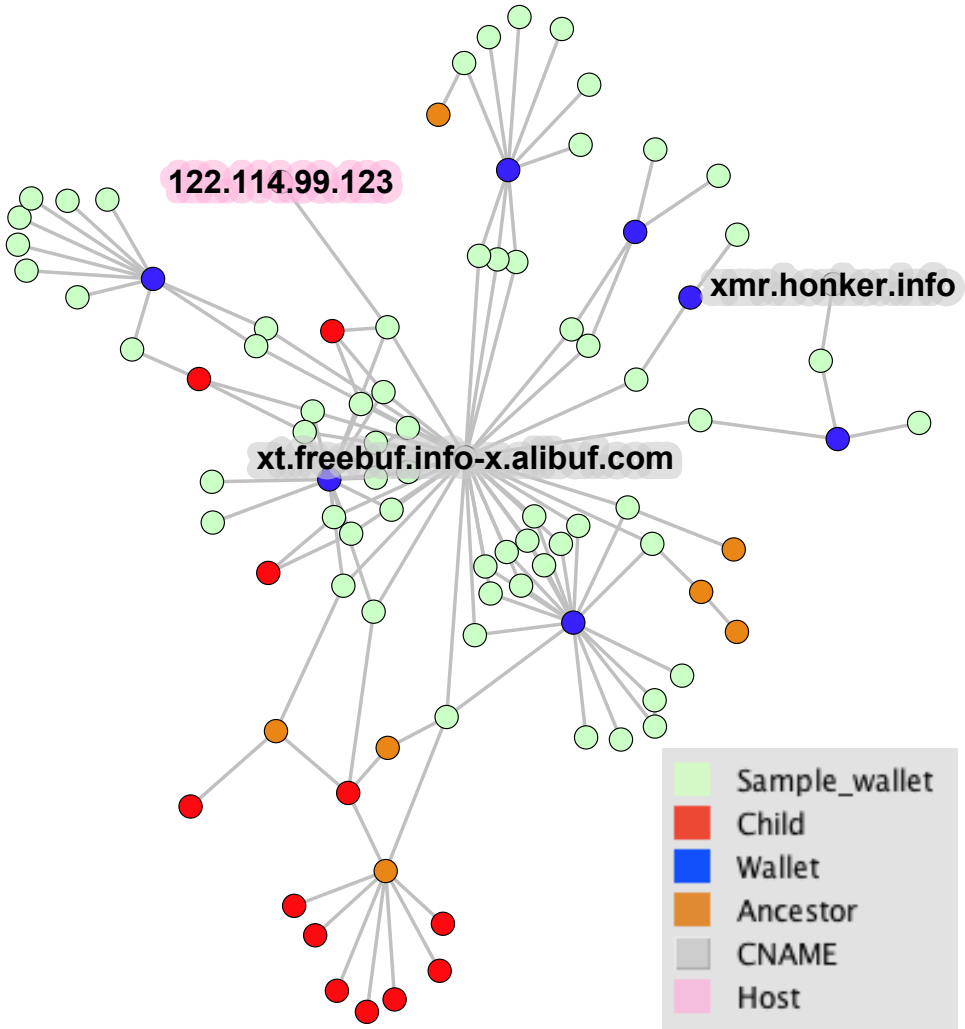
Top 10 Campaigns

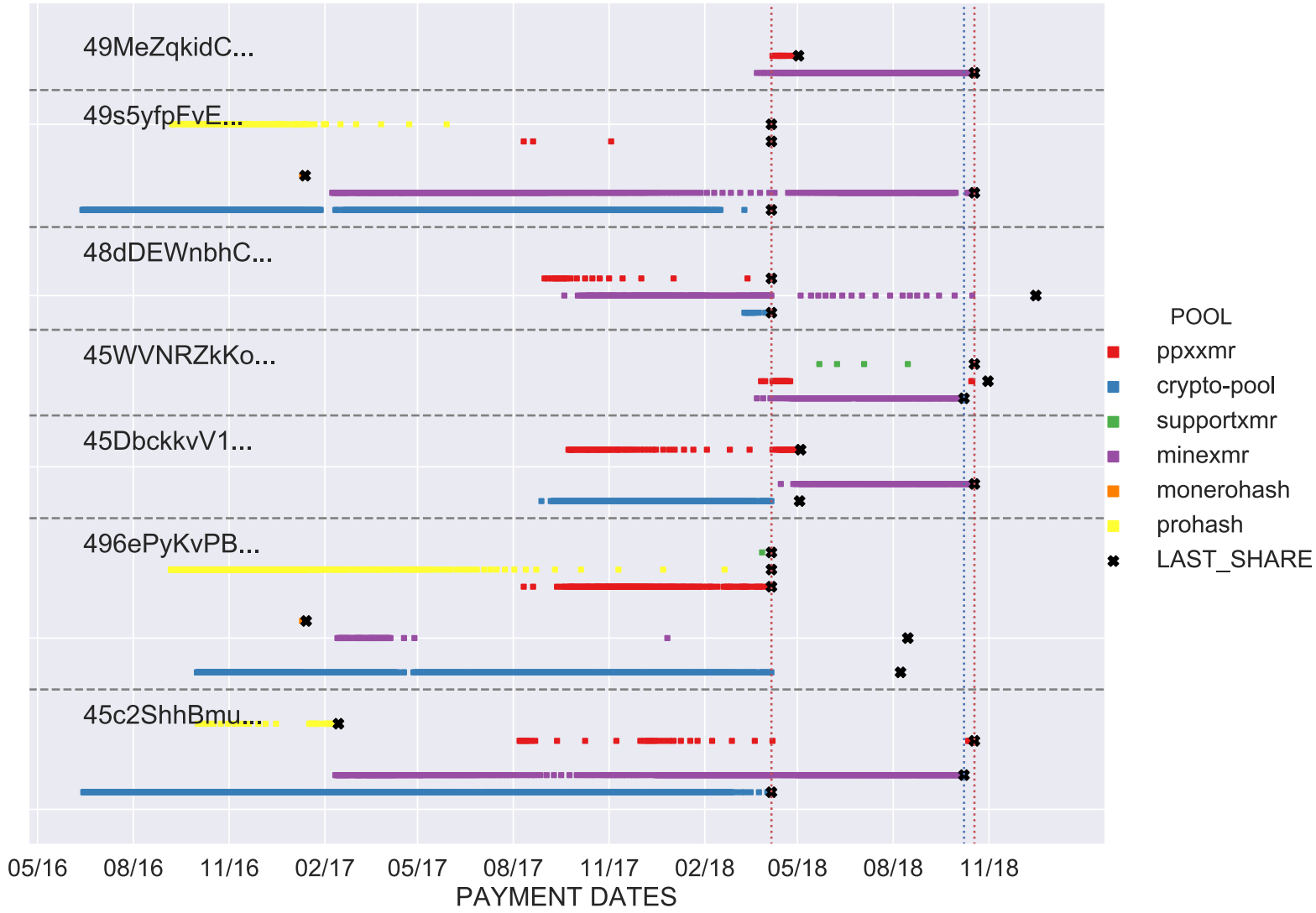
We have identified about 2K campaigns

We look at contacted domains to learn more about each campaign

- Network evasion:
  - Some samples do not directly use mining pools domains
  - They use domain aliases (i.e. CNAMEs)
- Associate wallets to particular botnets based on C&C
- We have identified 3 botnets operating Monero mining malware:
  - **The Evil Miner botnet**. We found 4 wallets appearing in 1667 different samples. These have mined a total of 16,863.43 XMR (2,529,514.66 USD)
  - **The Jenking botnet**. We found 2 wallets appearing in 63 different samples. They have mined a total of 10,942.67 XMR (1,641,400.92 USD)
  - **The Xbooster botnet**. We found 23 wallets in 839 different samples. They have mined a total of 459.63 XMR (68,944.22 USD)

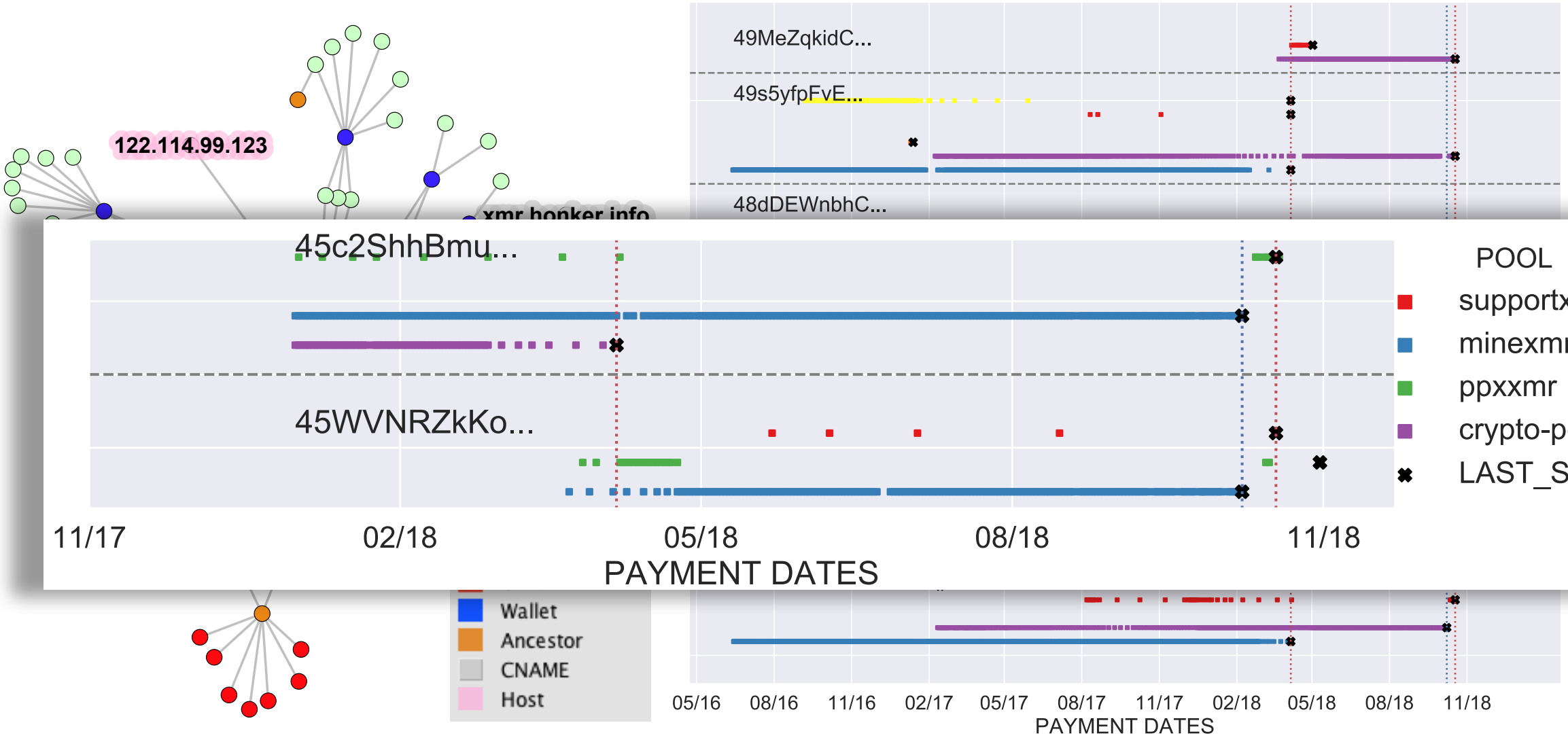
But not all domains were known





Results

The Freebuf Campaign



Results

163,754 XMR – **$18M**

The Freebuf Campaign

	< 100	[100-1k)	[1k-10k)	>10k	ALL
#Campaigns	1,999	151	52	16	2,218
THIRD-PARTY INFRASTRUCTURE					
PPI	1.2%	4.6%	9.6%	12.5%	1.7%
Mining SW	8.2%	16.6%	28.8%	12.5%	9.2%
Both	0.4%	2.6%	5.8%	0.0%	0.7%
STEALTH TECHNIQUES					
Obfuscation	4.2%	4.6%	3.8%	0.0%	4.1%
CNAMEs	0.4%	4.6%	9.6%	25.0%	1.1%
Proxies	2.7%	6.0%	3.8%	18.8%	3.0%
PERIOD OF ACTIVITY					
+ Apr-18	18.9%	53.0%	50.0%	37.5%	22.0%
+ Oct-18	8.9%	25.8%	23.1%	25.0%	10.5%
Start: 2014	0.1%	3.3%	11.5%	43.8%	0.1%
Start: 2015	0.2%	0.7%	3.8%	12.5%	0.2%
Start: 2016	4.9%	27.8%	38.5%	37.5%	4.4%
Start: 2017	32.1%	54.3%	46.2%	6.2%	28.9%
Start: 2018	62.7%	13.9%	0.0%	0.0%	56.5%
Years: 0	67.2%	11.3%	0.0%	0.0%	60.6%
Years: 1	30.7%	60.9%	46.2%	6.2%	27.7%
Years: 2	1.9%	24.5%	38.5%	18.8%	1.7%
Years: 3	0.2%	2.0%	5.8%	25.0%	0.2%
Years: 4	0.1%	1.3%	9.6%	50.0%	0.0%

We look at the difference between successful and non-successful campaigns

We analyze

1. The use of 3P infrastructure
   - **Pay-Per-Install**
   - **Stock mining tools**
2. The use of stealthy techniques
3. The period of activity

What are medium actors doing?

- Use known packers
- Use known mining software
- Started very recently

What are these wealthy actors doing?

Raise the bar in the **Arms Race**:

- **Pay-Per-Install**
- CNAMEs
- Proxies
- Avoid using known Packers
- Have been around for some time

Conclusions

01

Preferred cryptocurrency?

Monero

02

Underground economy?

Plays a key role

- Enables crime (script-kiddies)
- Gives support (PPI, stealthy)
- Fuels other crimes

03

Actors and Profit?

The core of this illicit business is monopolized by a small number of wealthy actors.

04

Sophistication?

- Obfuscation
- CNAMEs
- Proxies

05

Are current countermeasures and intervention approaches effective?

A First Look at the Crypto-Mining Malware Ecosystem

A Decade of Unrestricted Wealth and Profit

Thanks!

- **Audience**
- **Cambridge Cybercrime Centre**
  - **Specially Alexander Vetterl**
- **Virus Total**
- **minexmr**
  - **And non-cooperative pools**

Sergio Pastrana Portillo

Universidad Carlos III de Madrid

@serpastrana

spastran@inf.uc3m.es