Crypto Currency

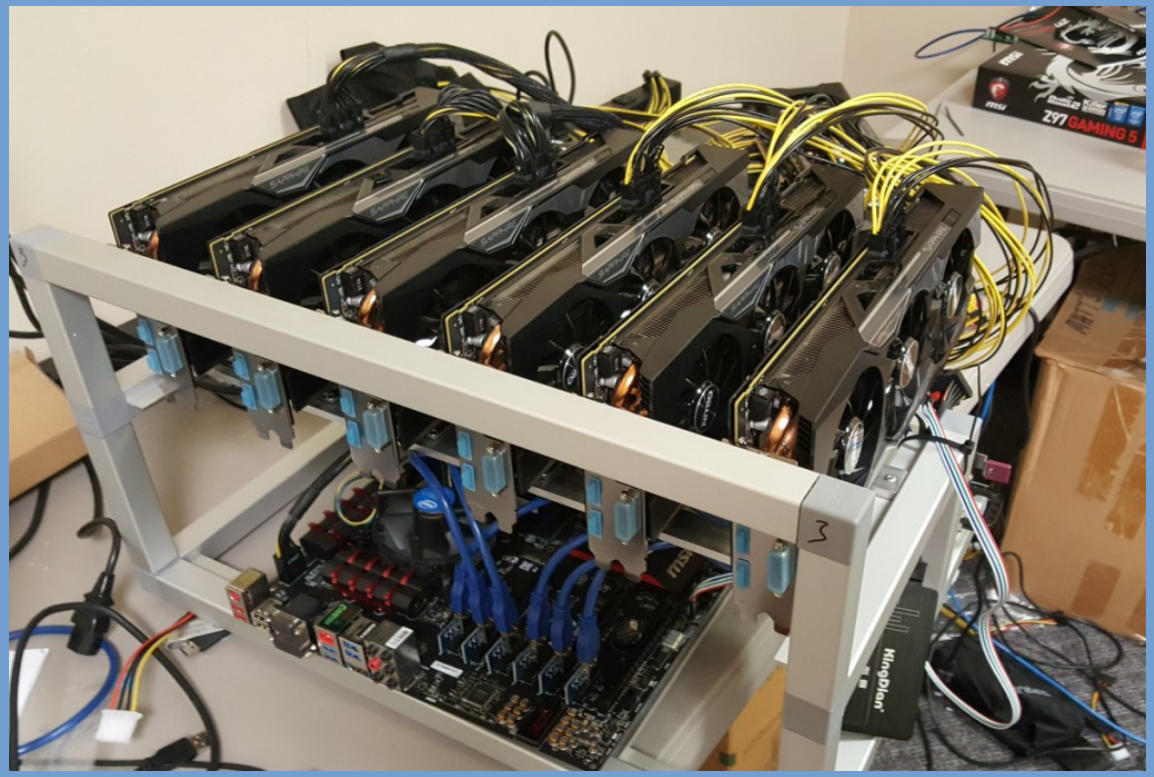
The internet-wide bug bounty program.

Risky.biz 2018 Ep. 482

The Growth of incentives

- First paper on Bitcoin October 2008
- Nov 2013 Bitcoin over $1,000
- Dec 2017 Bitcoin over $19,000

Ignored for quite some time



But wait! CPU mining returns

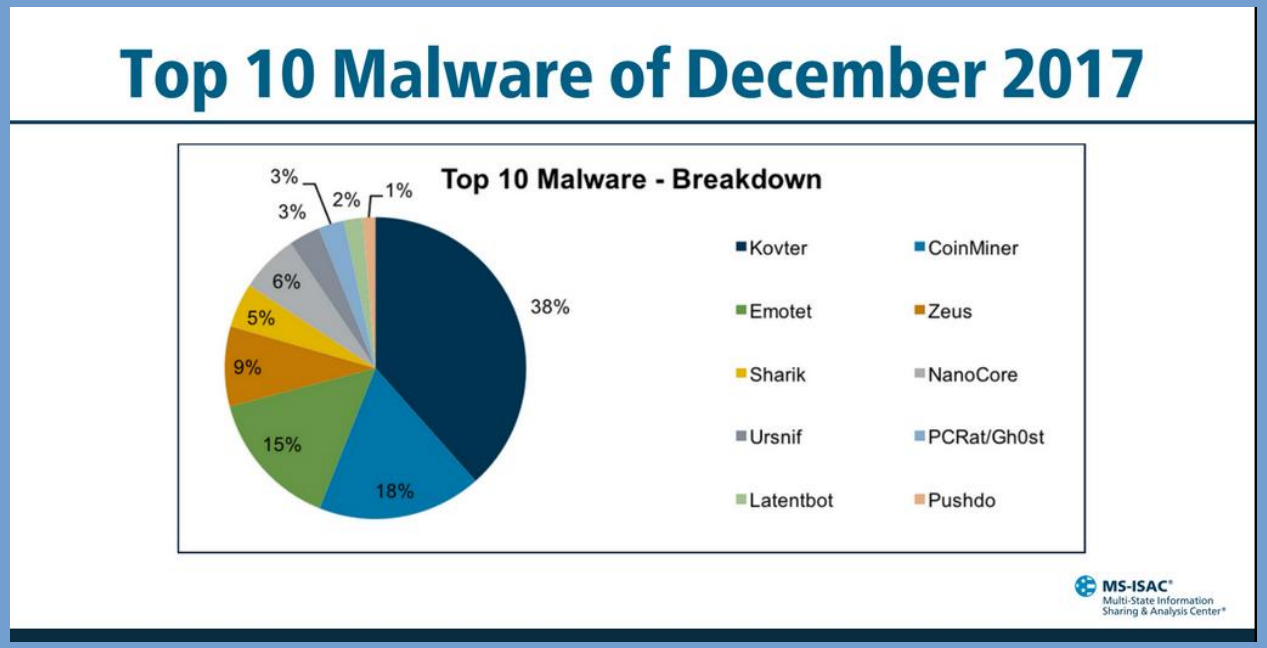
2014 Monero is announced

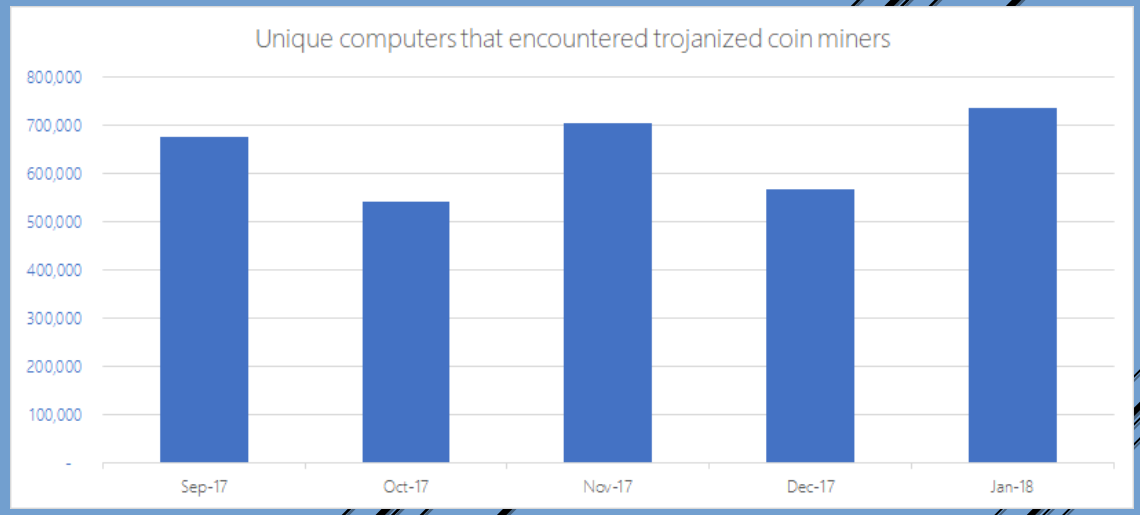
Game changer for malware mining

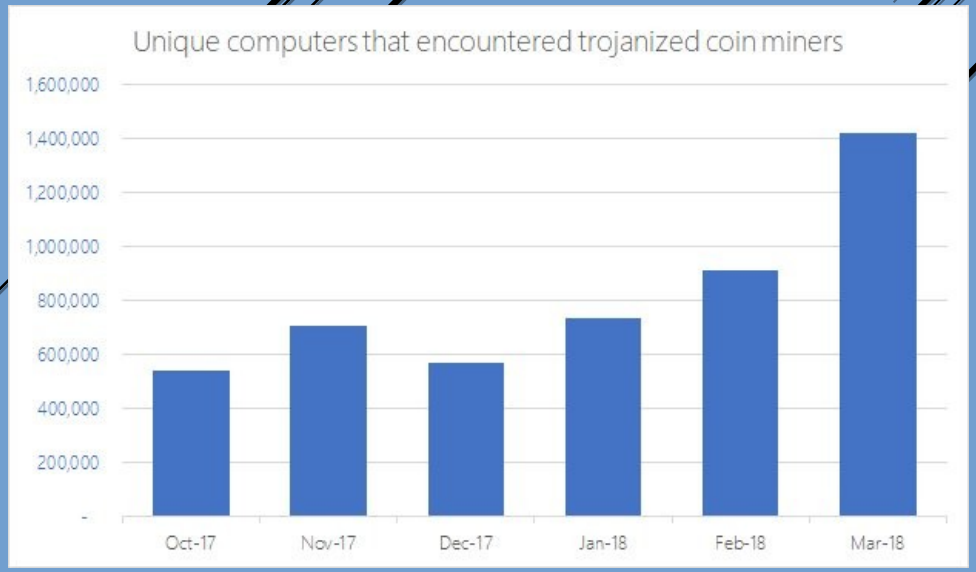
Monero uses the cryptonight algorithm, can be done via CPU and does not scale as nicely with more expensive hardware

Mining efficiently on CPU’s

What happens next?







Source:
Top:
https://www.cisecurity.org/top-10-malware-of-december-2017/

Left:
https://cloudblogs.microsoft.com/microsoftsecure/2018/03/13/invisible-resource-thieves-the-increasing-threat-of-cryptocurrency-miners/?utm_source=t.co&utm_medium=referral

The Beginning Gathering Data

Started pretty informal

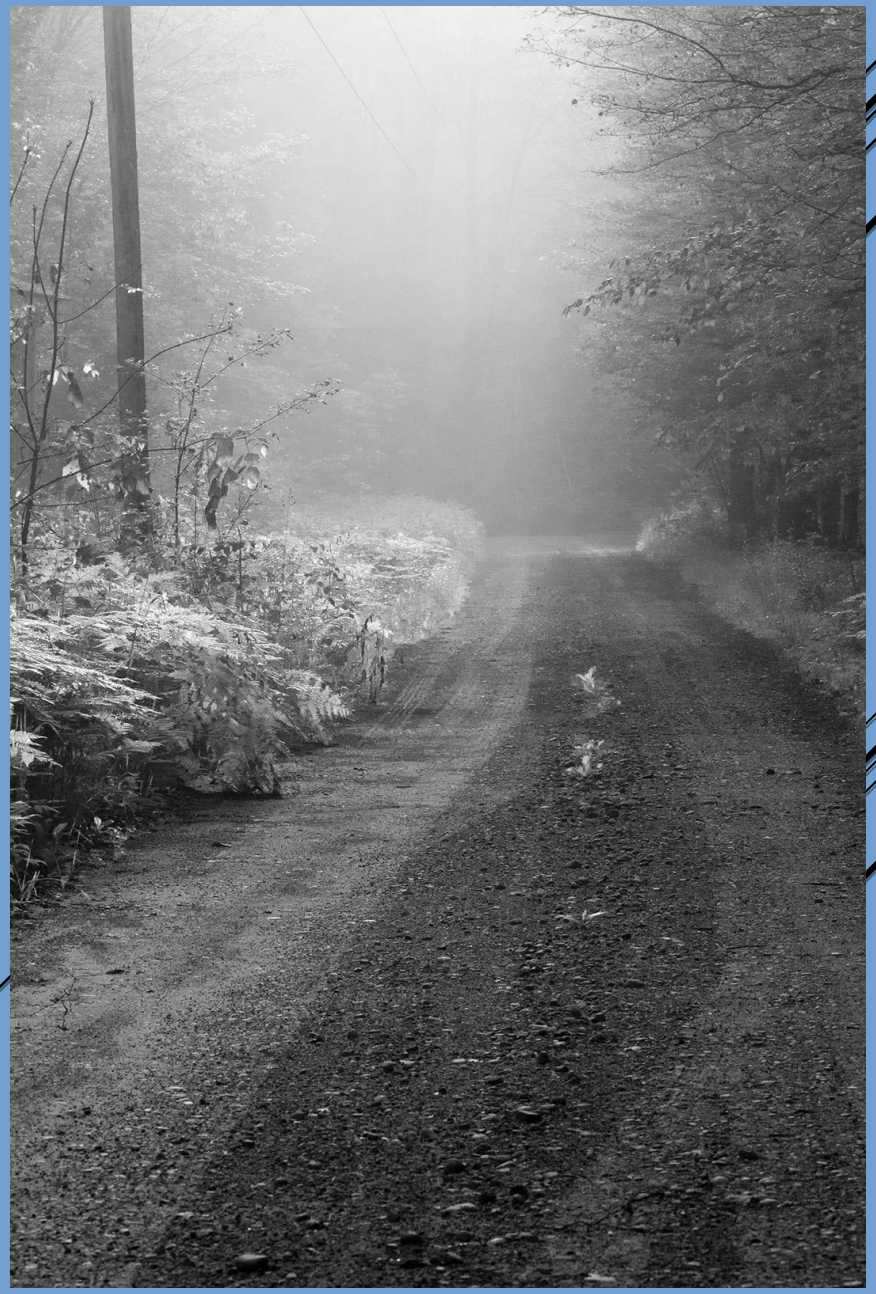
Reviewed cases I had worked on.

Branched out to team slack

Searched through ticketing system

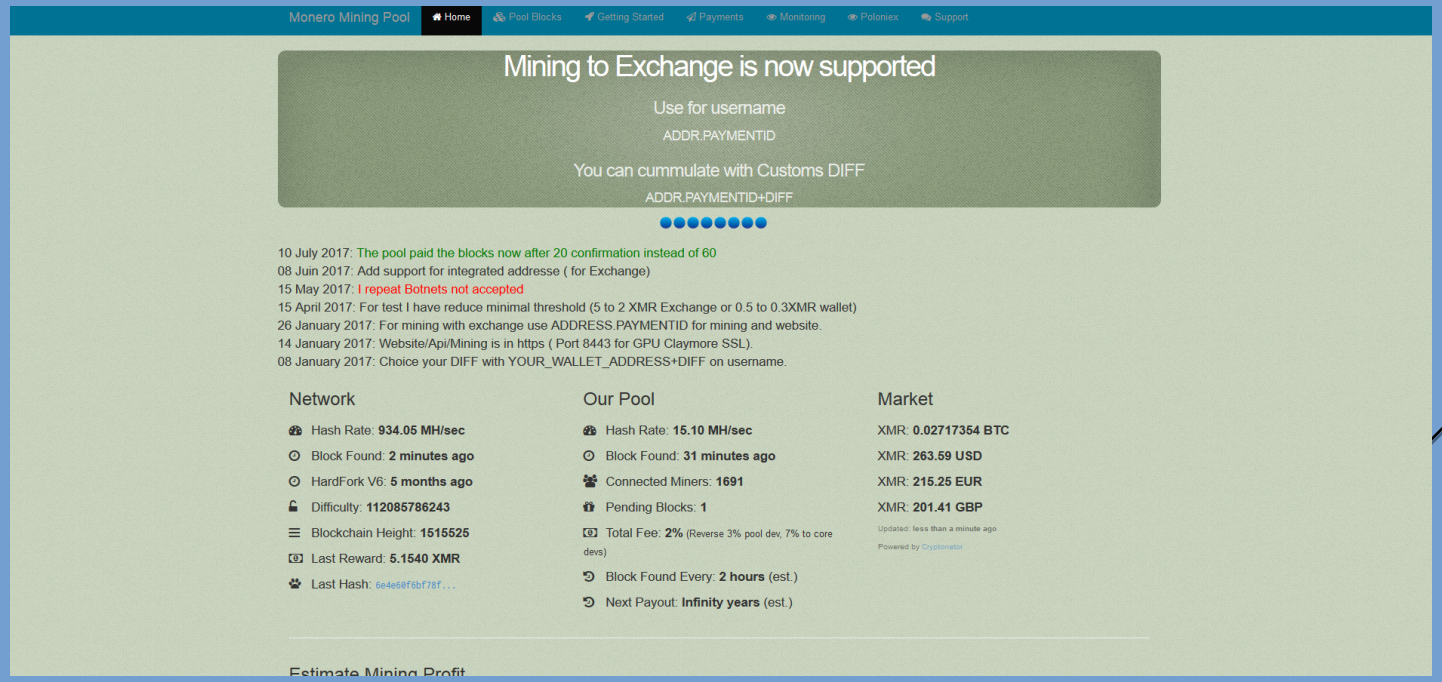
After a few months Over 100 individual cases patterns emerged

Mining pools
Mining software
Network signatures

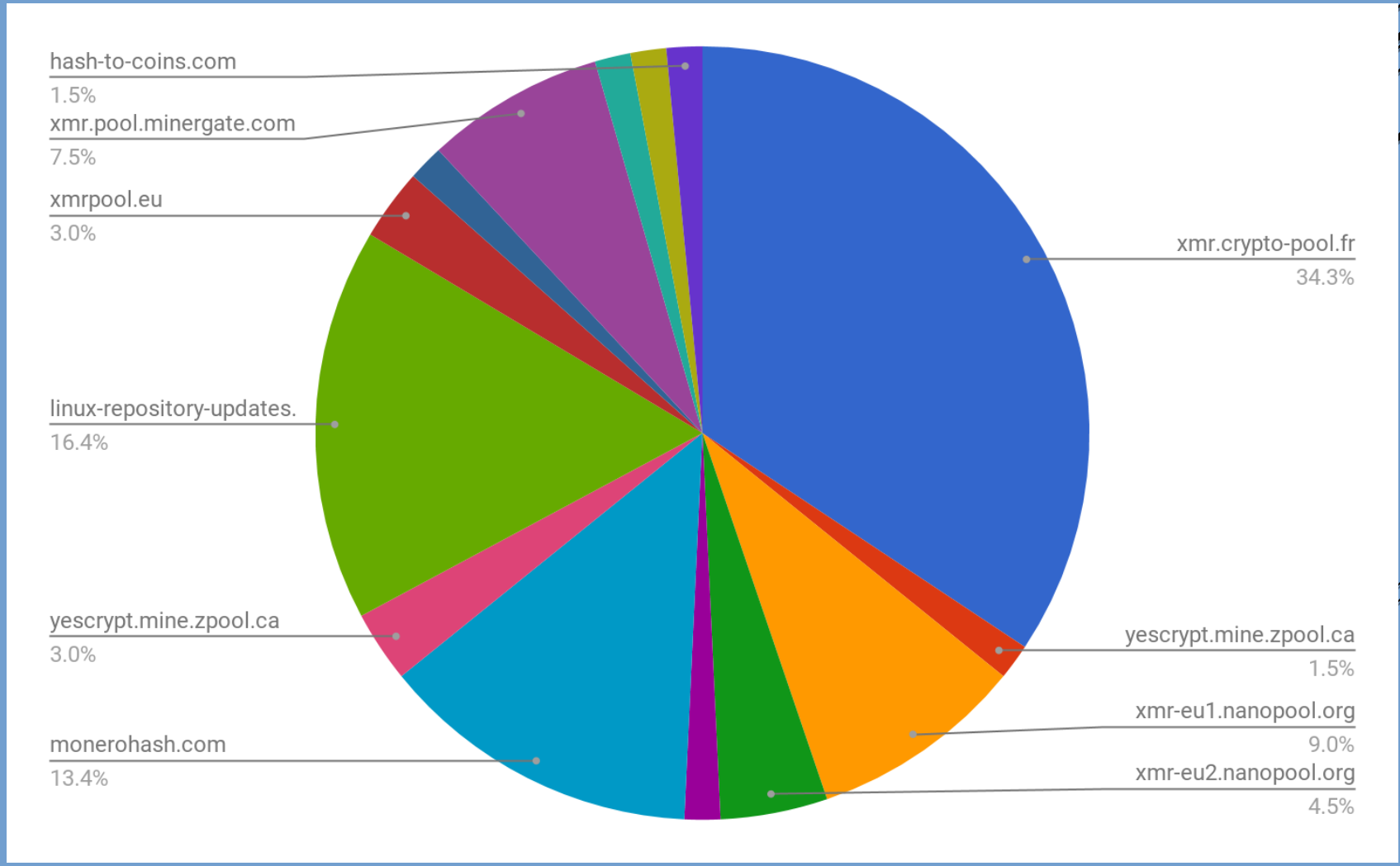


Mining Pools

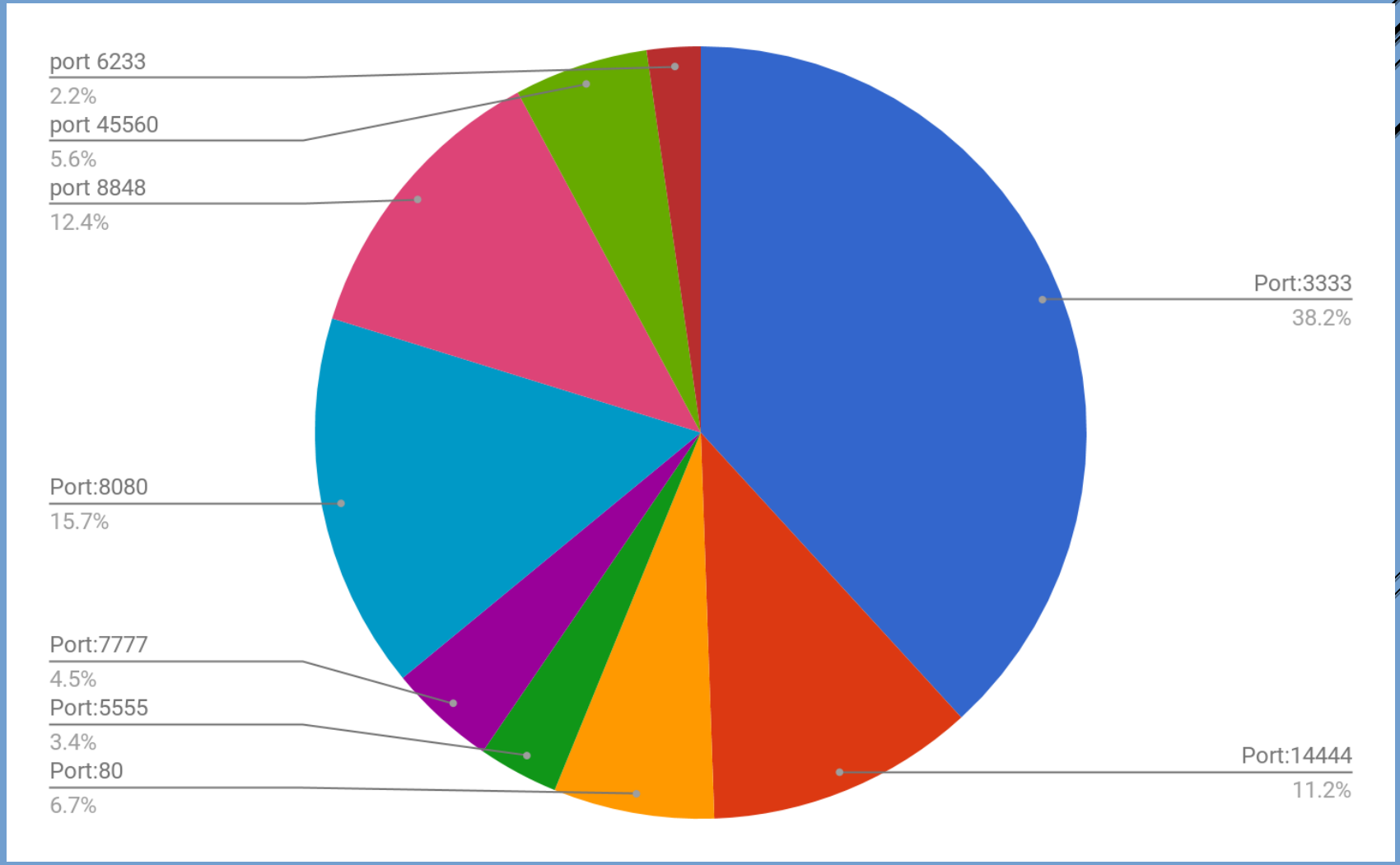
To get a better return on investment many miners participate in pools there they collectively pool the mining resources and get paid out in crypto-currency based on the computing power they submit.



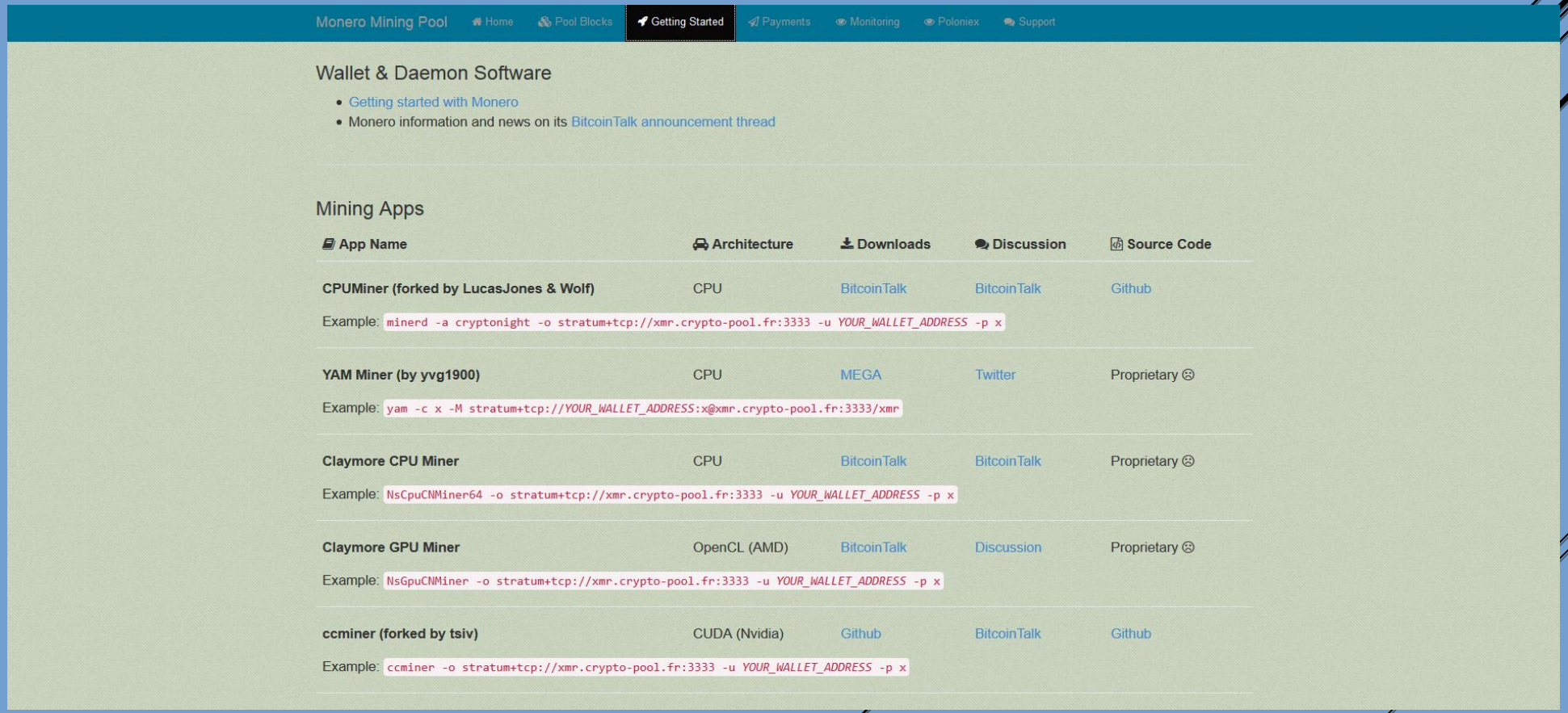
How do we know?



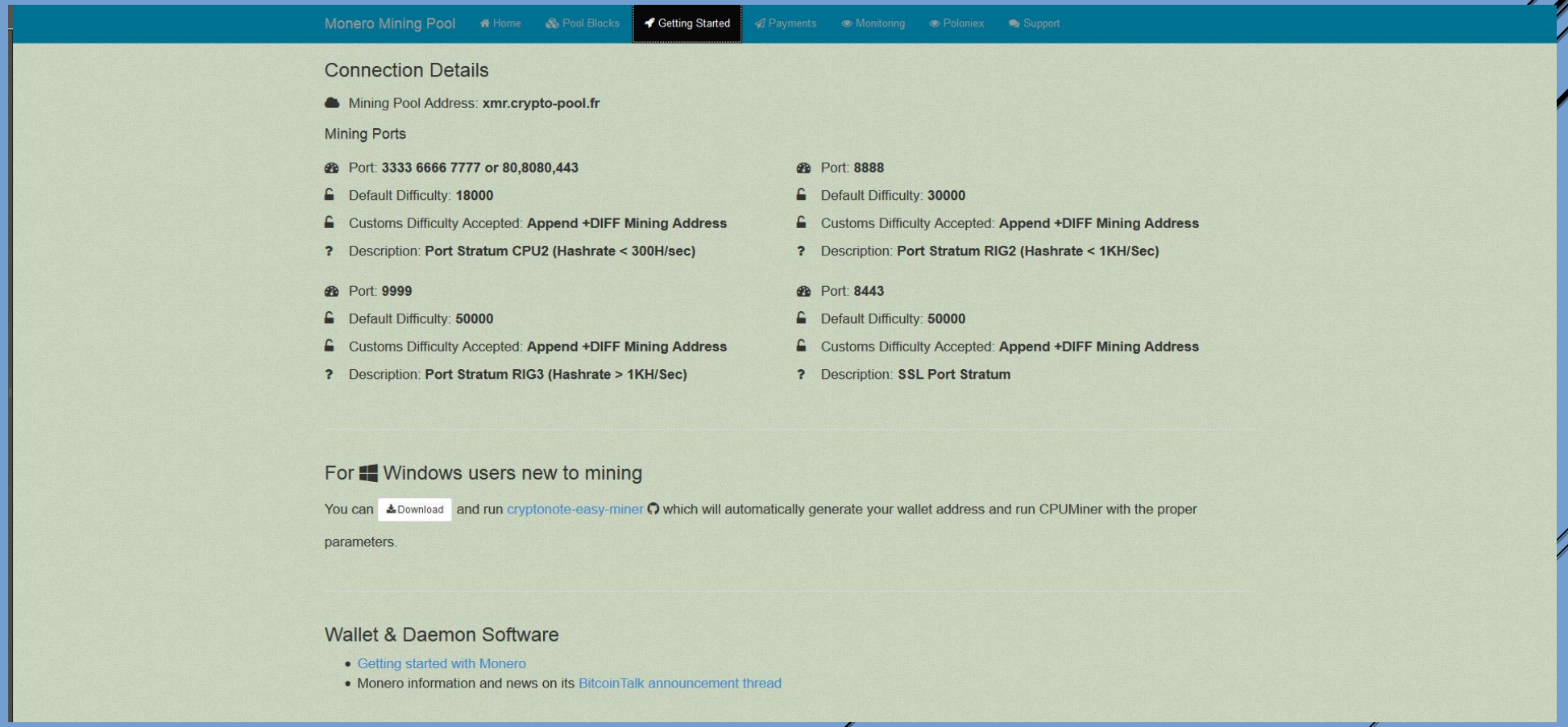
How do we know?



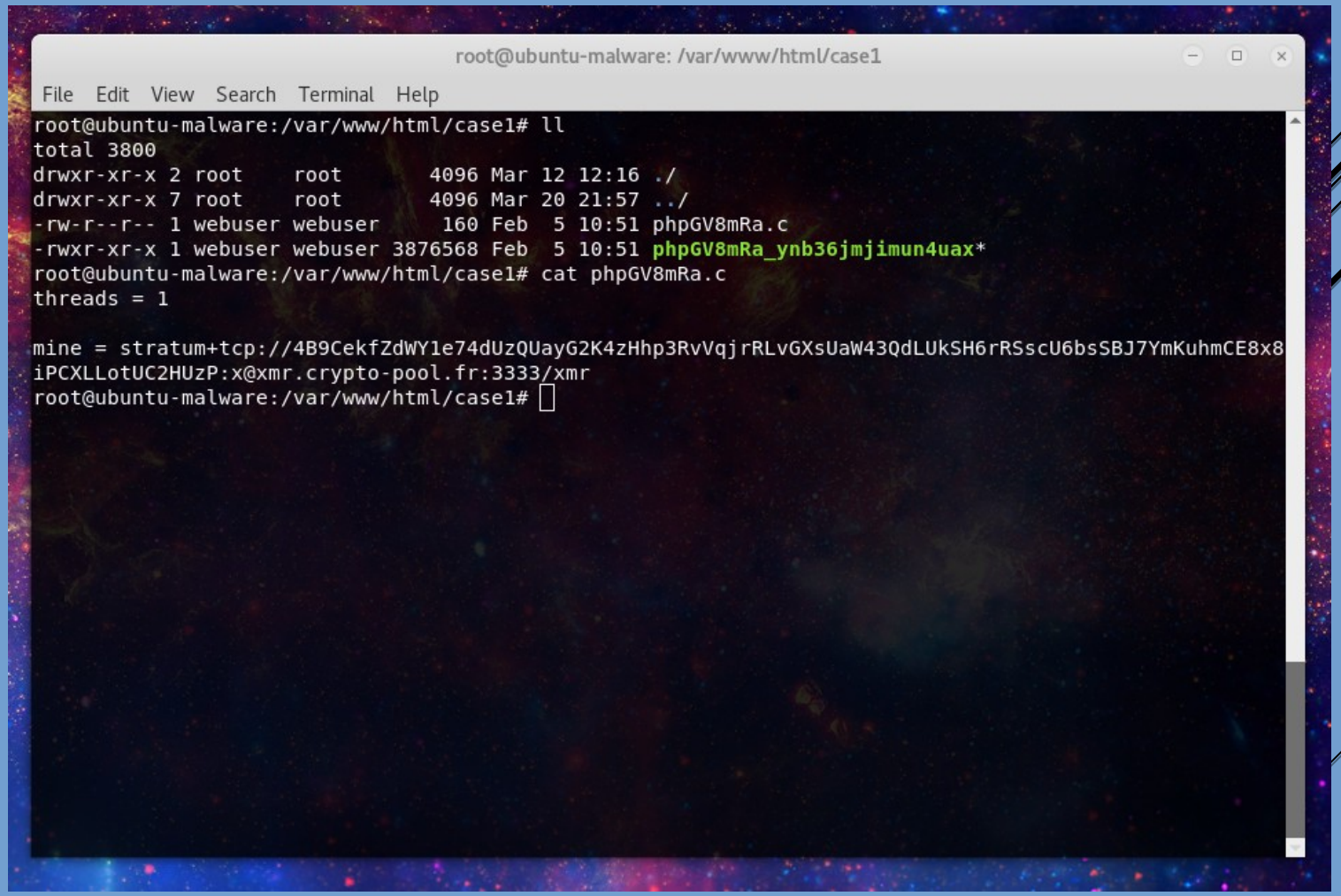
Off the shelf software



Off the shelf software



Getting the keys



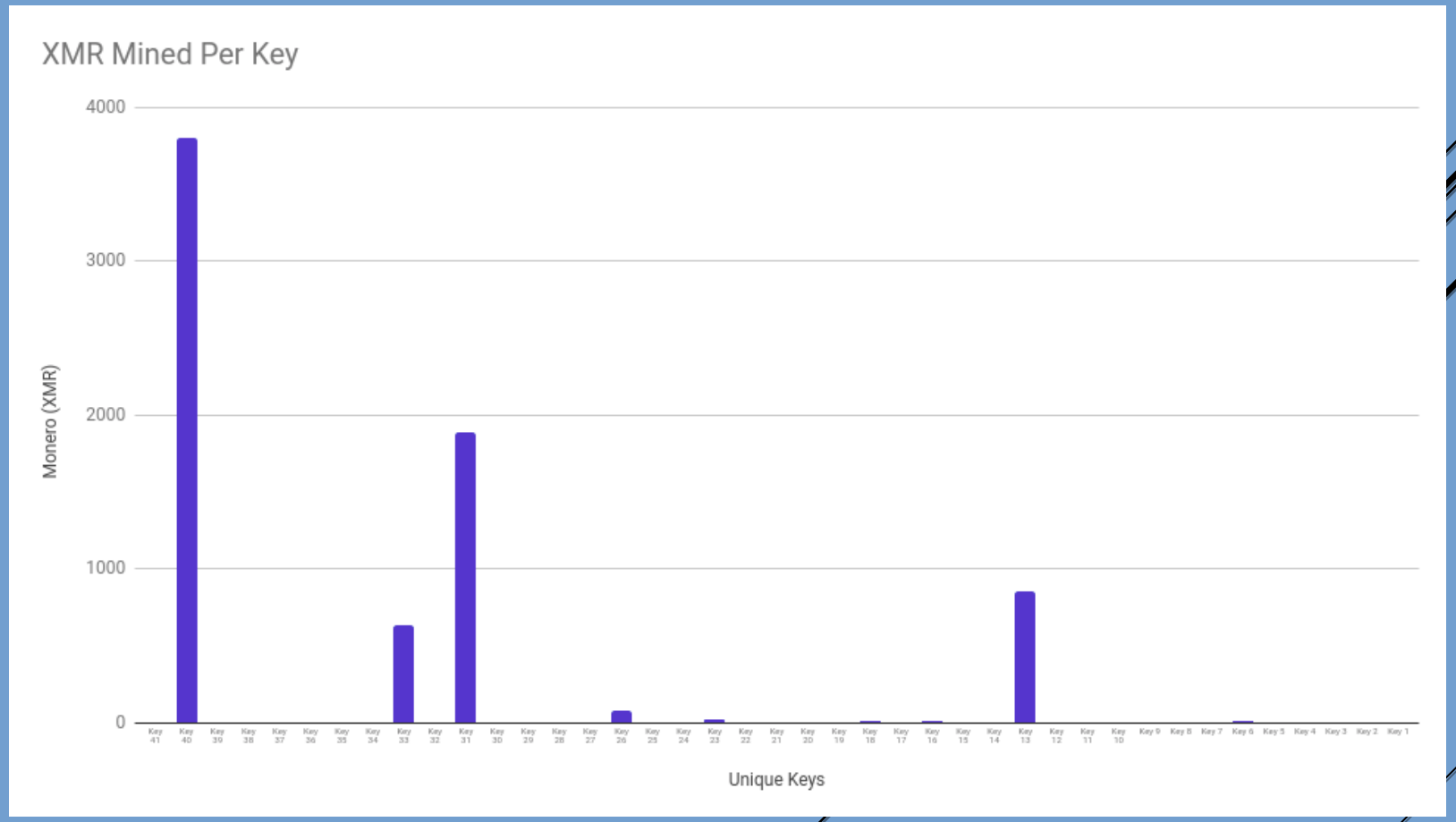
Payouts

As of April 29th

1.61 Million USD

Over 41 unique Monero wallet keys

Unique Wallet Data

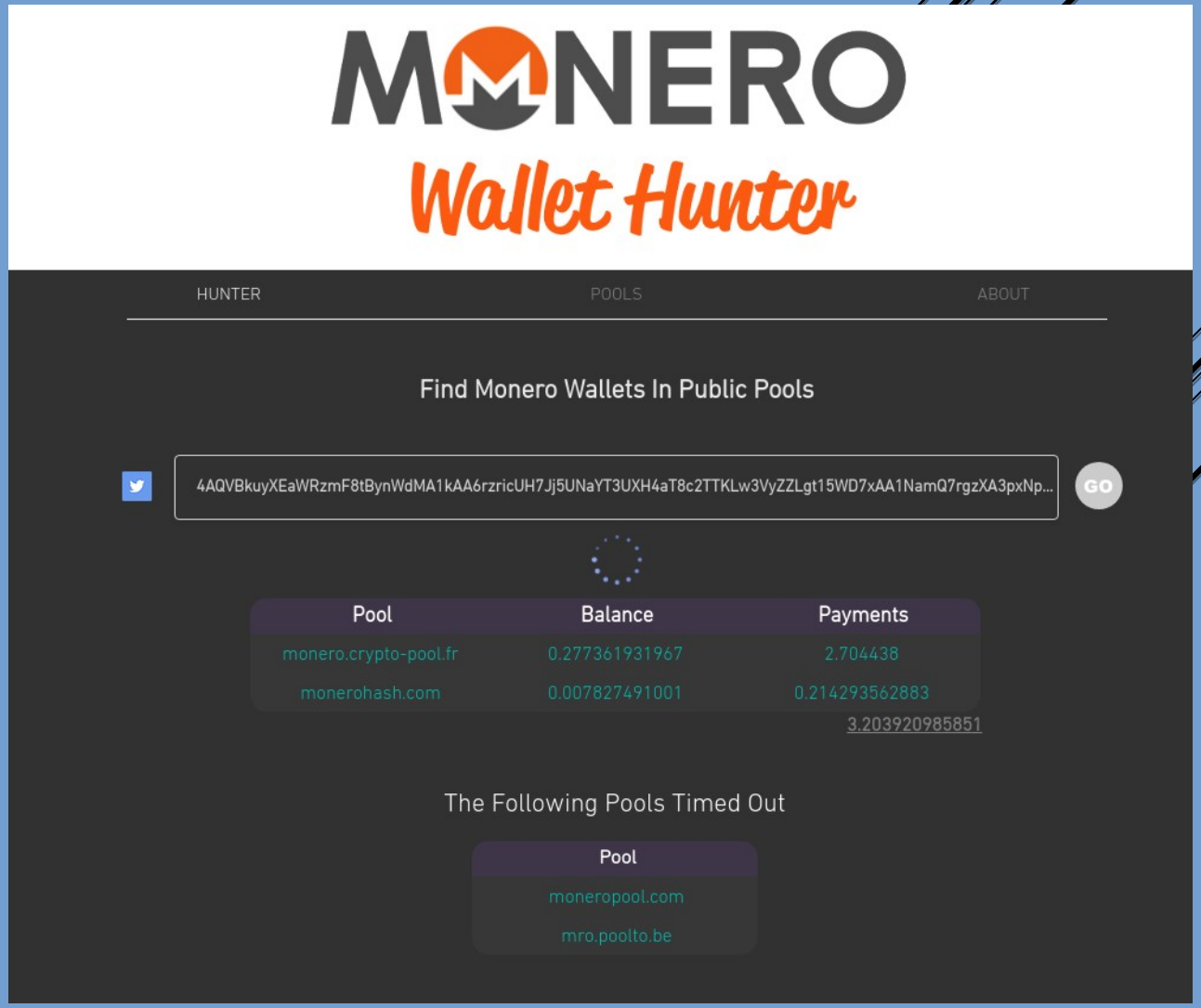


Tracking Wallet Data

Go to individual pools…

Or use xmrhunter.com

By :

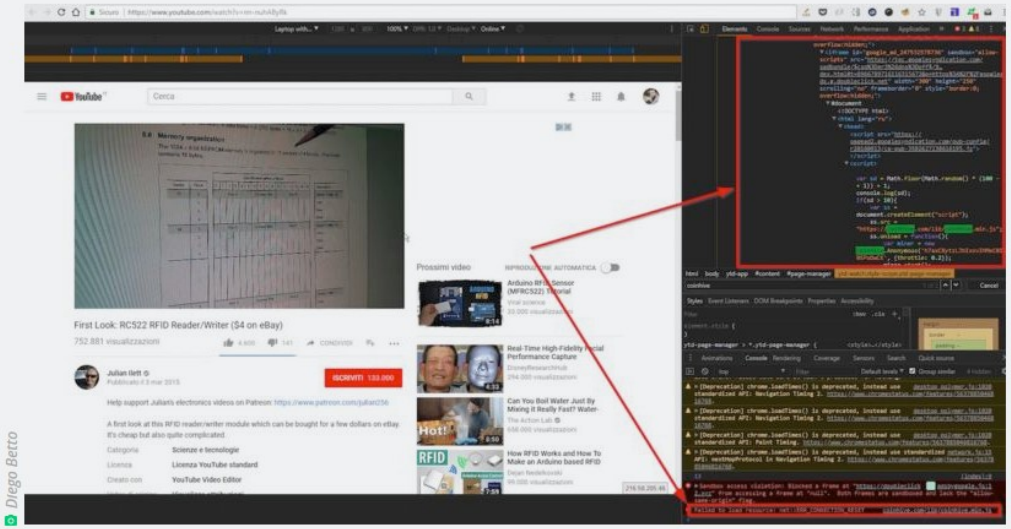


Oh and also crypto-jacking

Now even YouTube serves ads with CPU-draining cryptocurrency miners

Ad campaign lets attackers profit while unwitting users watch videos.

DAN GOODIN - 1/26/2018, 2:27 PM



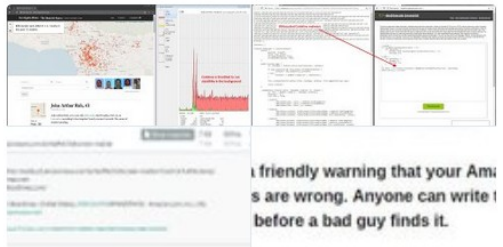
Enlarge

Kevin Beaumont @GossiTheDog 21 Feb
Replying to @GossiTheDog
Also Robbie makes a great point - companies are putting JavaScript files in S3 (a nice CDN) and leaving them world writable. Hello, coin miners and invisible form loggers.

Kevin Beaumont @GossiTheDog

Bingo. It's happening. LA Times is serving cryptomining, their S3 bucket with their JavaScript code was world writable and even contains this file (4th screenshot). H/T @bad_packets pic.twitter.com/xQTRzixpwG

1:54 PM - Feb 22, 2018



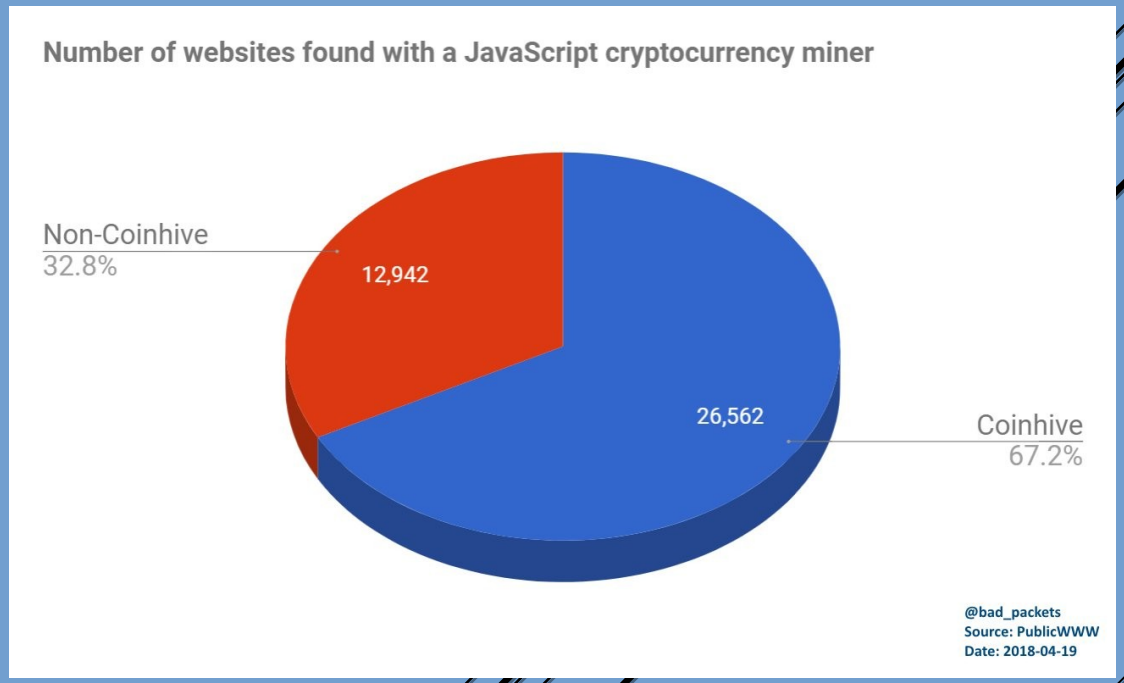
149 145 people are talking about this

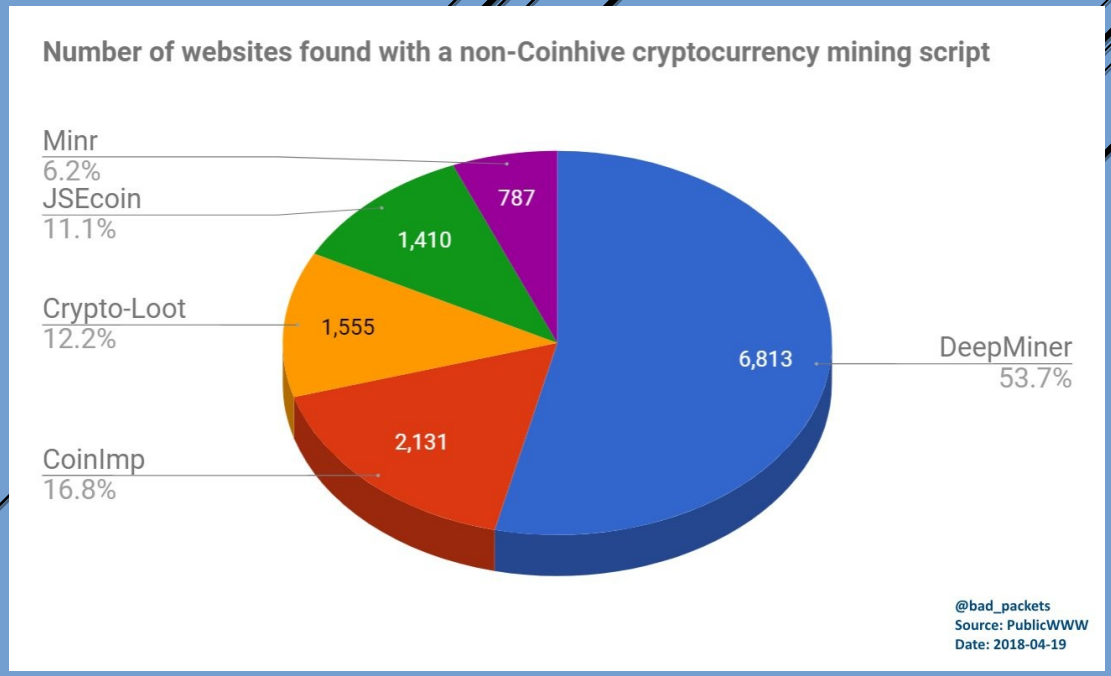
Coinhive

<script src="https://coinhive.com/lib/coinhive.min.js"></script> <script> var miner = new CoinHive.User('<site-key>', 'john-doe'); miner.start(); </script>

The original, but now has plenty of competition:

Check out @bad_packets for more





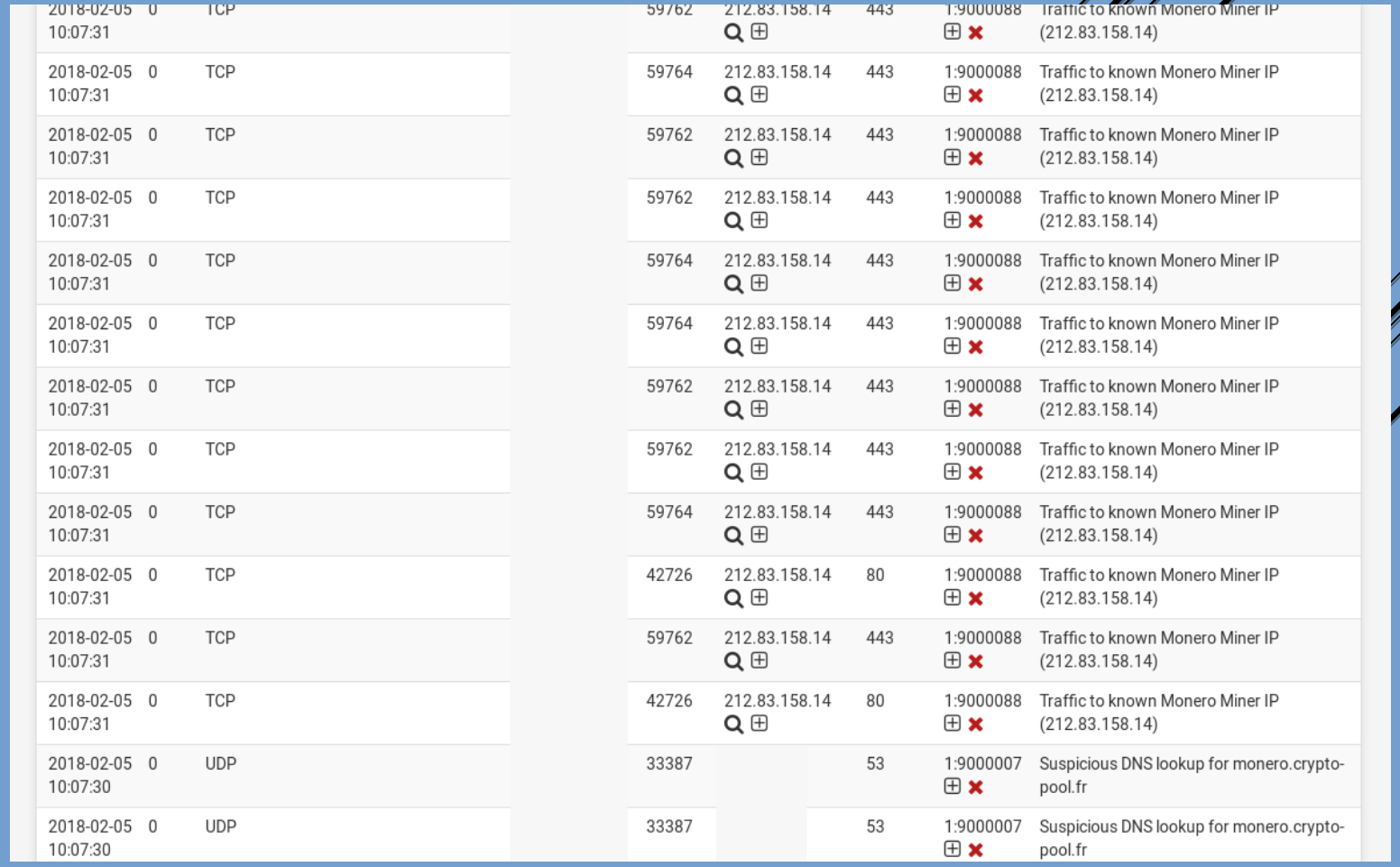
What does it mean?

Why?

Miners are noisy (if you know what to look for)

Rather non destructive

Expose vulnerabilities



2018-02-05 10:07:31	0	TCP		59762	212.83.158.14	443	1:9000088	Traffic to known Monero Miner IP (212.83.158.14)
2018-02-05 10:07:31	0	TCP		59764	212.83.158.14	443	1:9000088	Traffic to known Monero Miner IP (212.83.158.14)
2018-02-05 10:07:31	0	TCP		59762	212.83.158.14	443	1:9000088	Traffic to known Monero Miner IP (212.83.158.14)
2018-02-05 10:07:31	0	TCP		59762	212.83.158.14	443	1:9000088	Traffic to known Monero Miner IP (212.83.158.14)
2018-02-05 10:07:31	0	TCP		59764	212.83.158.14	443	1:9000088	Traffic to known Monero Miner IP (212.83.158.14)
2018-02-05 10:07:31	0	TCP		59764	212.83.158.14	443	1:9000088	Traffic to known Monero Miner IP (212.83.158.14)
2018-02-05 10:07:31	0	TCP		59762	212.83.158.14	443	1:9000088	Traffic to known Monero Miner IP (212.83.158.14)
2018-02-05 10:07:31	0	TCP		59762	212.83.158.14	443	1:9000088	Traffic to known Monero Miner IP (212.83.158.14)
2018-02-05 10:07:31	0	TCP		59764	212.83.158.14	443	1:9000088	Traffic to known Monero Miner IP (212.83.158.14)
2018-02-05 10:07:31	0	TCP		42726	212.83.158.14	80	1:9000088	Traffic to known Monero Miner IP (212.83.158.14)
2018-02-05 10:07:31	0	TCP		59762	212.83.158.14	443	1:9000088	Traffic to known Monero Miner IP (212.83.158.14)
2018-02-05 10:07:31	0	TCP		42726	212.83.158.14	80	1:9000088	Traffic to known Monero Miner IP (212.83.158.14)
2018-02-05 10:07:30	0	UDP		33387		53	1:9000007	Suspicious DNS lookup for monero.crypto-pool.fr
2018-02-05 10:07:30	0	UDP		33387		53	1:9000007	Suspicious DNS lookup for monero.crypto-pool.fr

How?

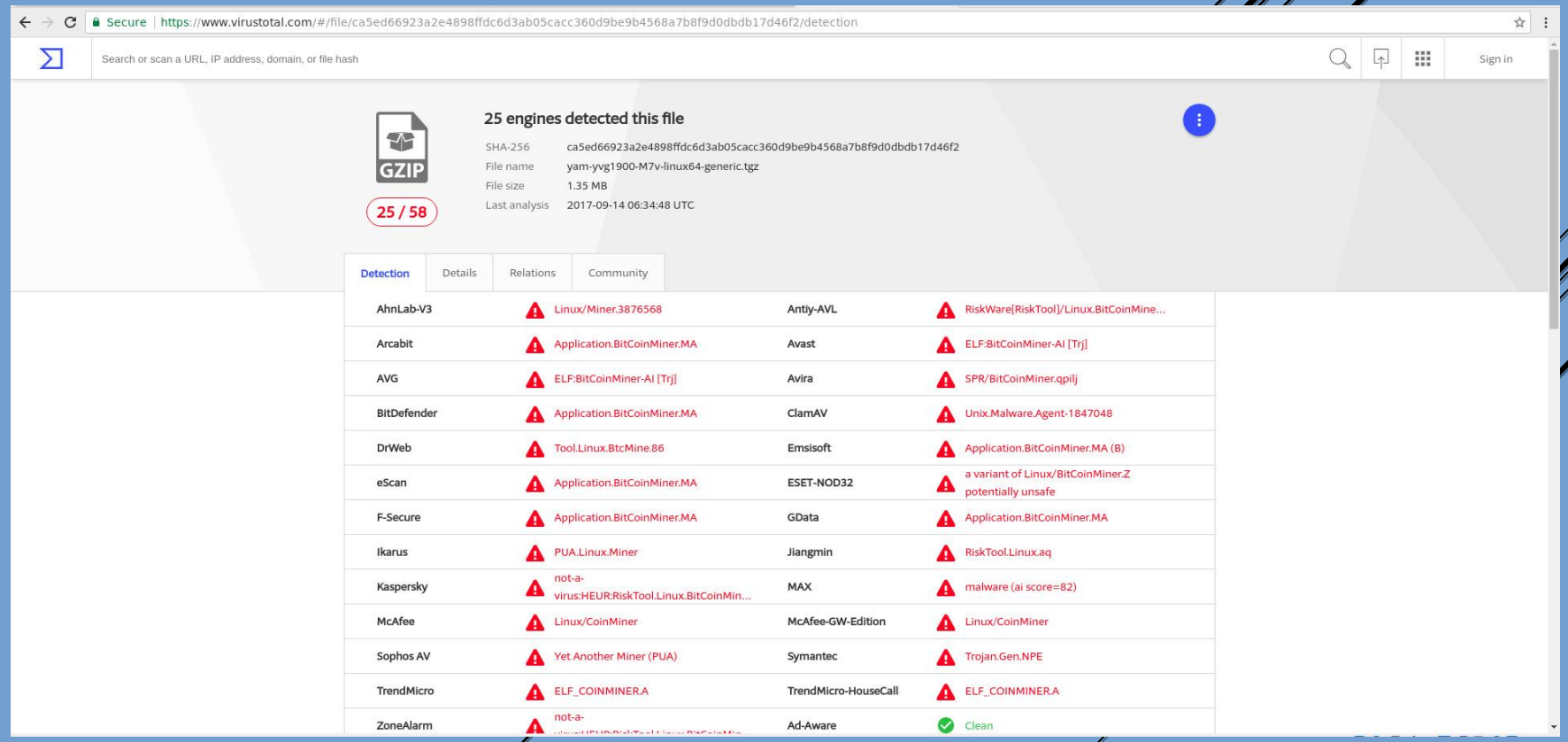
Network Traffic

IP’s and Ports

Reused miner programs

Increase in load

Drops in performance



Tools

Minerchk

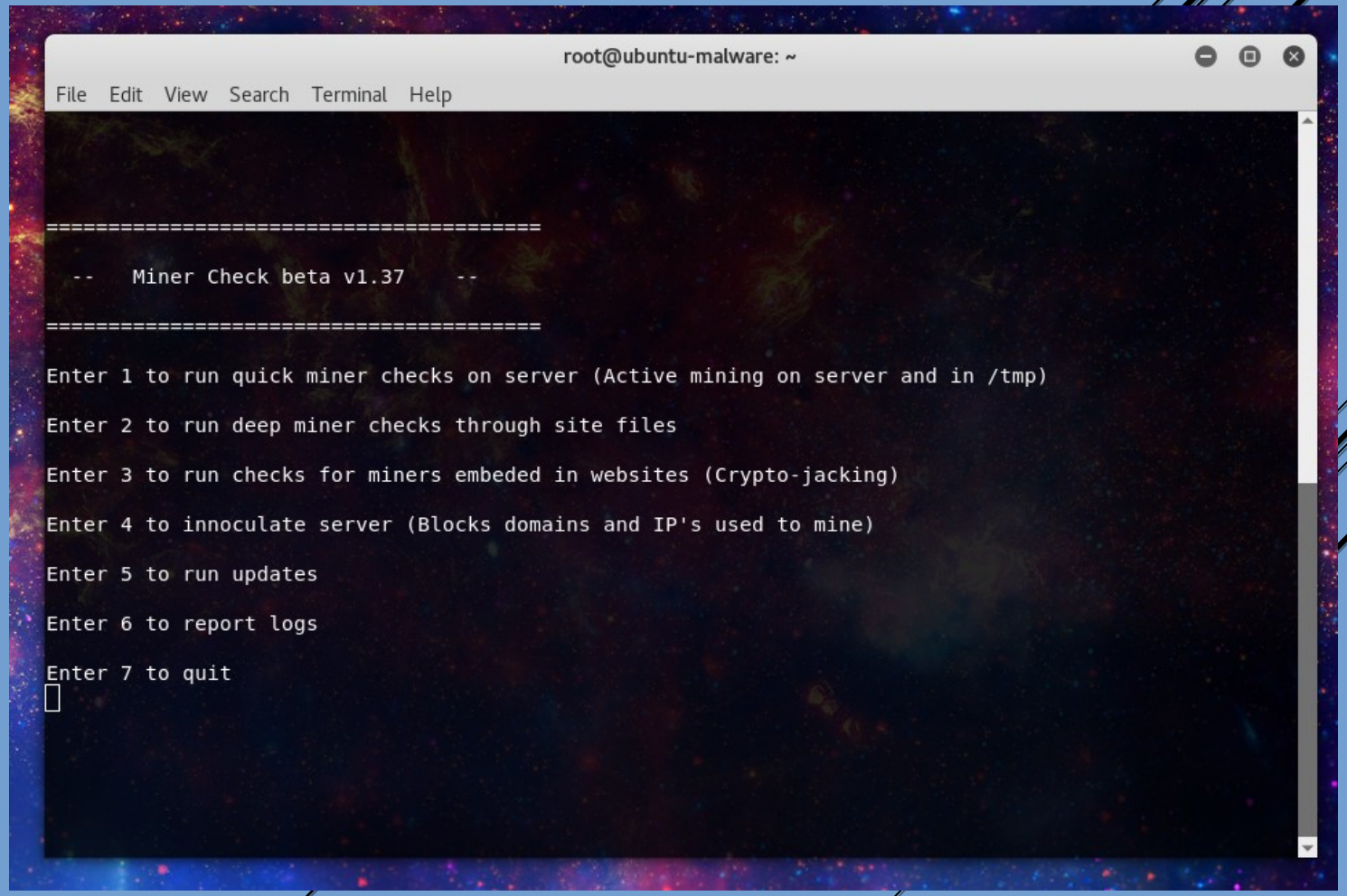
Built for Linux servers

Checks on system

Looks for Cryptojacking

Block access to pools

https://github.com/Hestat/minerchk

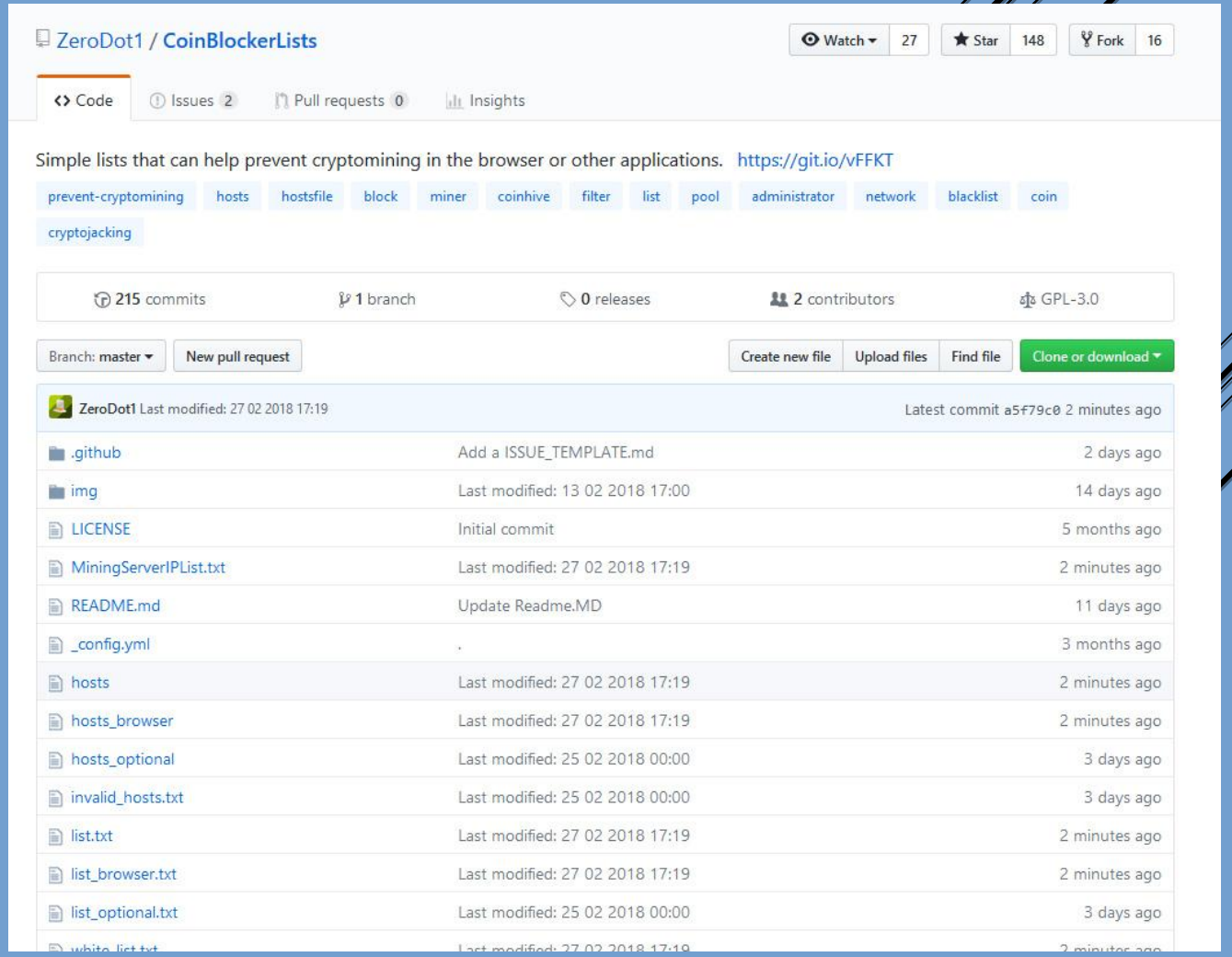


Tools pt 2

Aimed at crypto-jacking

Good for Endpoints or LAN Network blocking

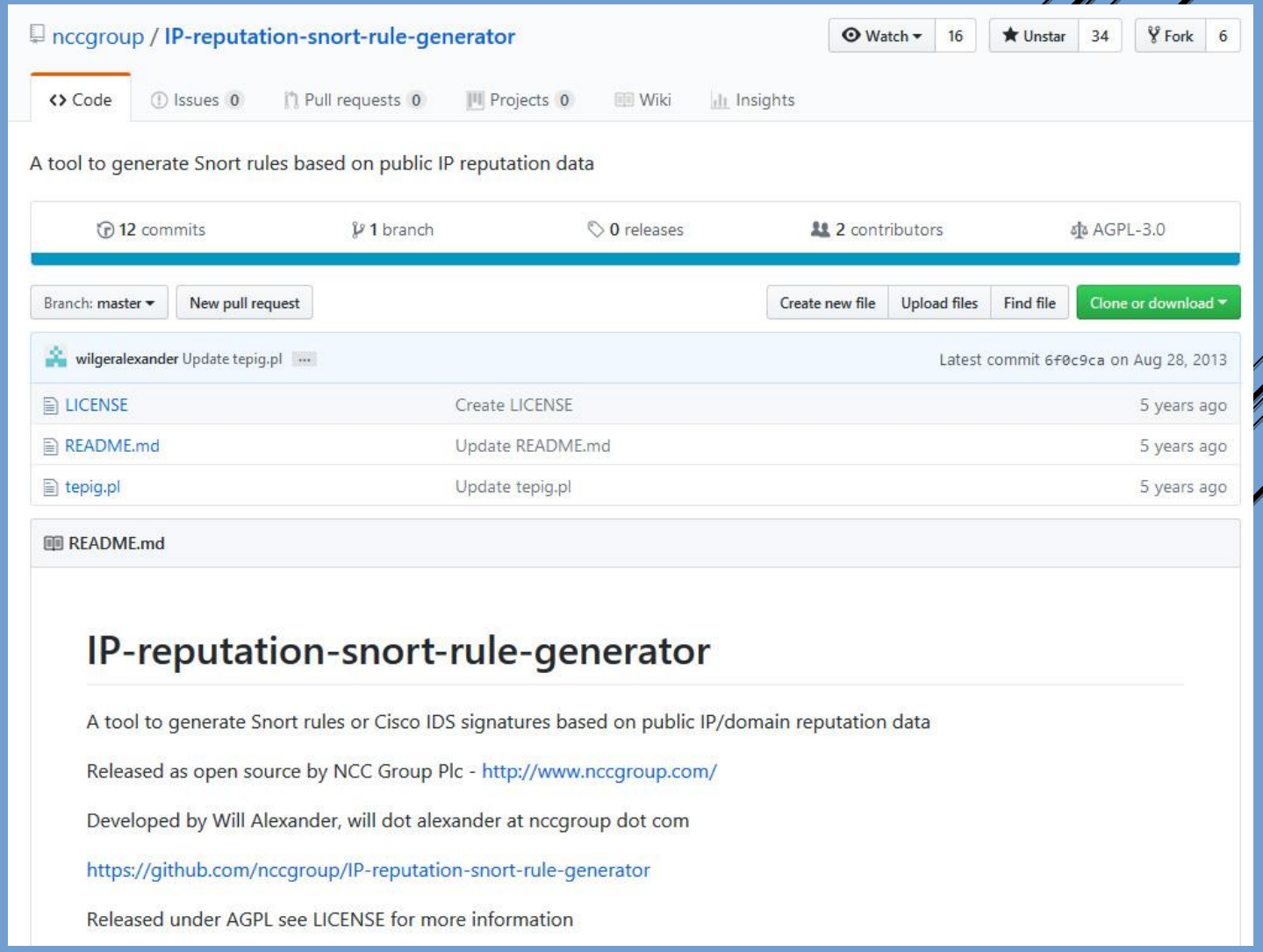
https://github.com/ZeroDot1/CoinBlockerLists



Resources pt 3

Create your own snort rules based on traffic to miners or other indicators.

https://github.com/nccgroup/IP-reputation-snort-rule-generator



FIN

Find out more of the background and other write ups on miner, malware and other web woes:

https://laskowski-tech.com

Or reach out on twitter:

@laskow26