



# 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

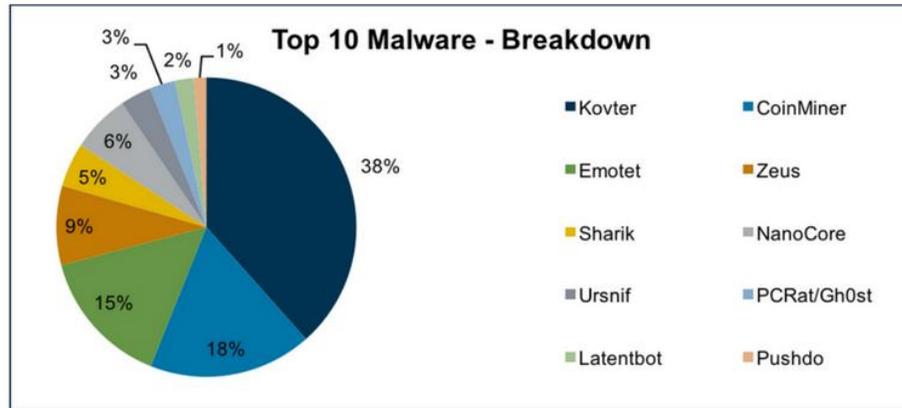
Monero uses the cryptonight algorithm, can be done via CPU and does not scale as nicely with more expensive hardware

Mining efficiently on CPU's



# What happens next?

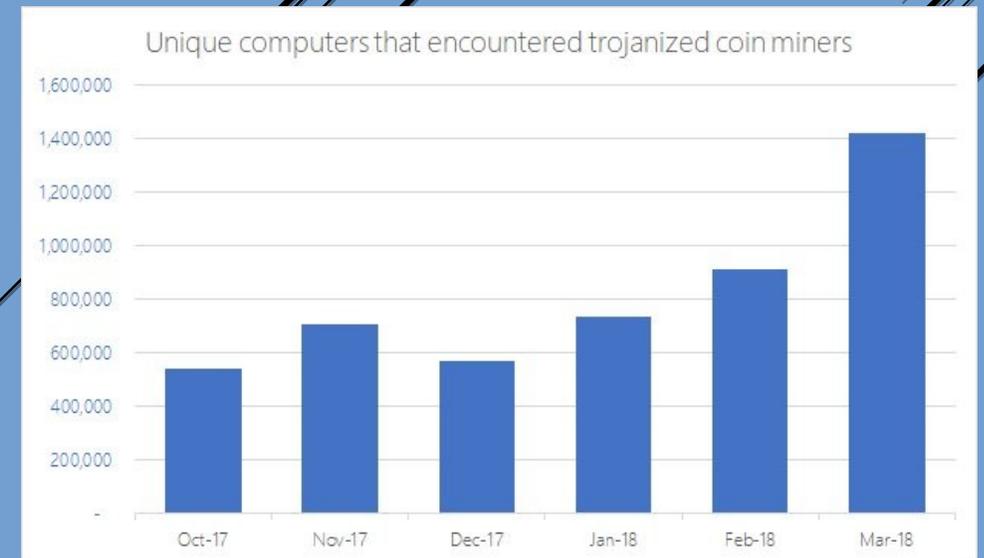
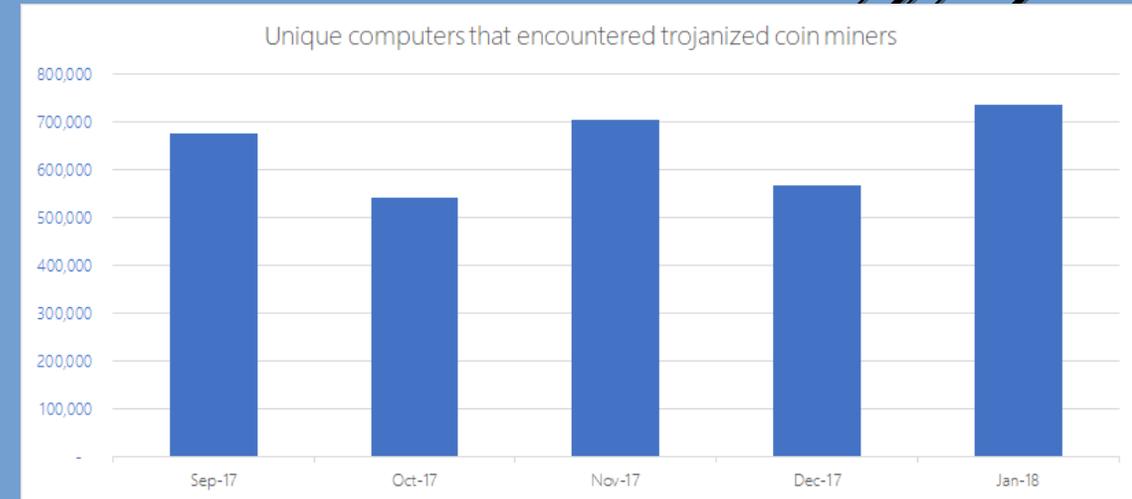
## Top 10 Malware of December 2017



MS-ISAC  
Multi-State Information  
Sharing & Analysis Center

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](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

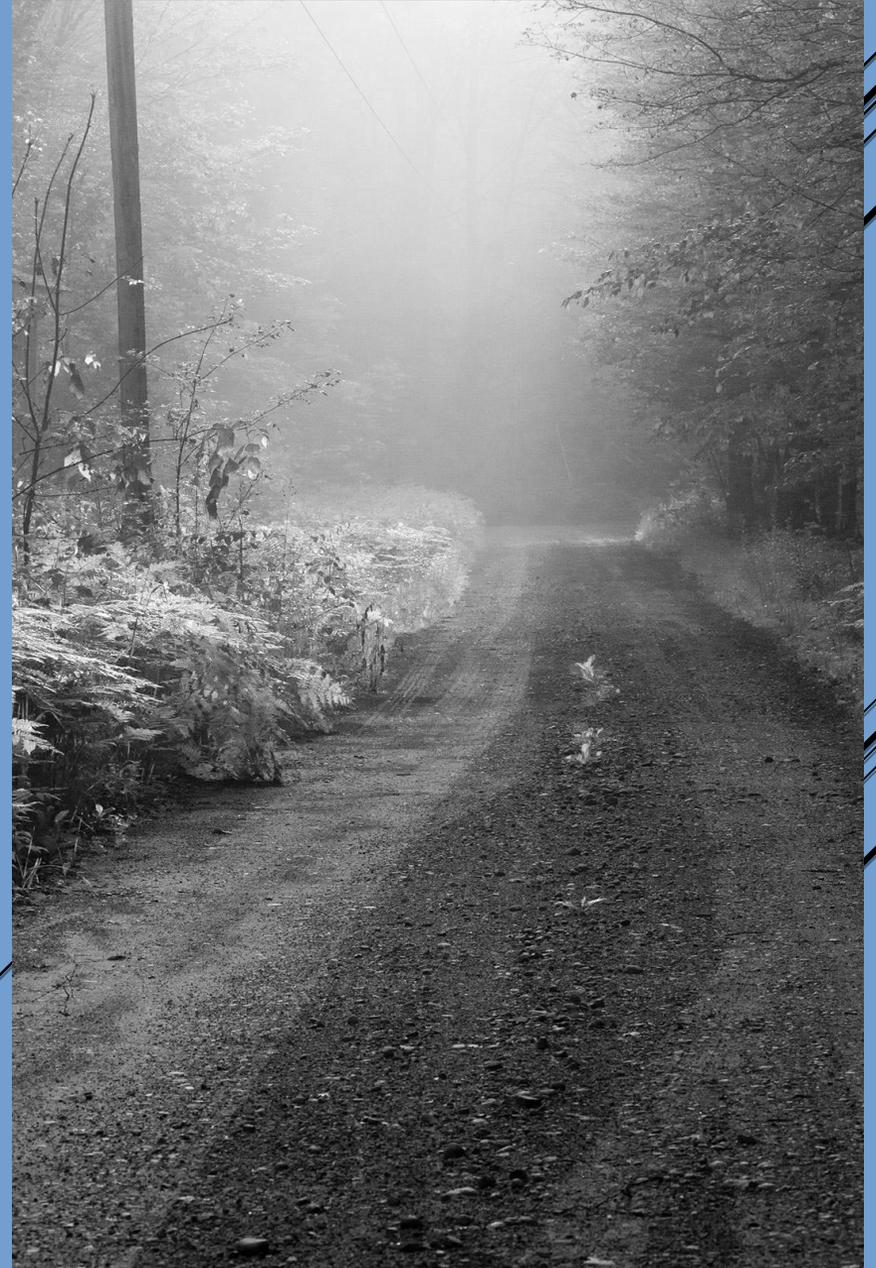
---

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.

The screenshot shows the Monero Mining Pool website interface. At the top, there is a navigation bar with links for Home, Pool Blocks, Getting Started, Payments, Monitoring, Pools, and Support. A prominent green notification box in the center reads "Mining to Exchange is now supported" and provides instructions on how to use the pool's address for mining to an exchange, including a note about cumulating with a custom DIFF. Below the notification, there is a list of recent updates and news items. The main content area is divided into three columns: Network, Our Pool, and Market. The Network column displays metrics like Hash Rate (934.05 MH/sec), Block Found (2 minutes ago), and Difficulty (112085786243). The Our Pool column shows Hash Rate (15.10 MH/sec), Block Found (31 minutes ago), and Connected Miners (1691). The Market column lists XMR prices in BTC, USD, EUR, and GBP. At the bottom, there is a section for "Estimate Mining Profit".

Monero Mining Pool [Home](#) [Pool Blocks](#) [Getting Started](#) [Payments](#) [Monitoring](#) [Pools](#) [Support](#)

**Mining to Exchange is now supported**

Use for username  
ADDR.PAYMENTID

You can cummulate with Customs DIFF  
ADDR.PAYMENTID+DIFF

10 July 2017: **The pool paid the blocks now after 20 confirmation instead of 60**  
08 Jun 2017: Add support for integrated address ( for Exchange)  
15 May 2017: **I repeat Botnets not accepted**  
15 April 2017: For test I have reduce minimal threshold (5 to 2 XMR Exchange or 0.5 to 0.3XMR wallet)  
26 January 2017: For mining with exchange use ADDRESS.PAYMENTID for mining and website.  
14 January 2017: Website/Api/Mining is in https ( Port 8443 for GPU Claymore SSL).  
08 January 2017: Choice your DIFF with YOUR\_WALLET\_ADDRESS+DIFF on username.

**Network**

- Hash Rate: **934.05 MH/sec**
- Block Found: **2 minutes ago**
- HardFork V6: **5 months ago**
- Difficulty: **112085786243**
- Blockchain Height: **1515525**
- Last Reward: **5.1540 XMR**
- Last Hash: [6e4e6f6bf78f...](#)

**Our Pool**

- Hash Rate: **15.10 MH/sec**
- Block Found: **31 minutes ago**
- Connected Miners: **1691**
- Pending Blocks: **1**
- Total Fee: **2%** (Reverse 3% pool dev, 7% to core devs)
- Block Found Every: **2 hours** (est.)
- Next Payout: **Infinity years** (est.)

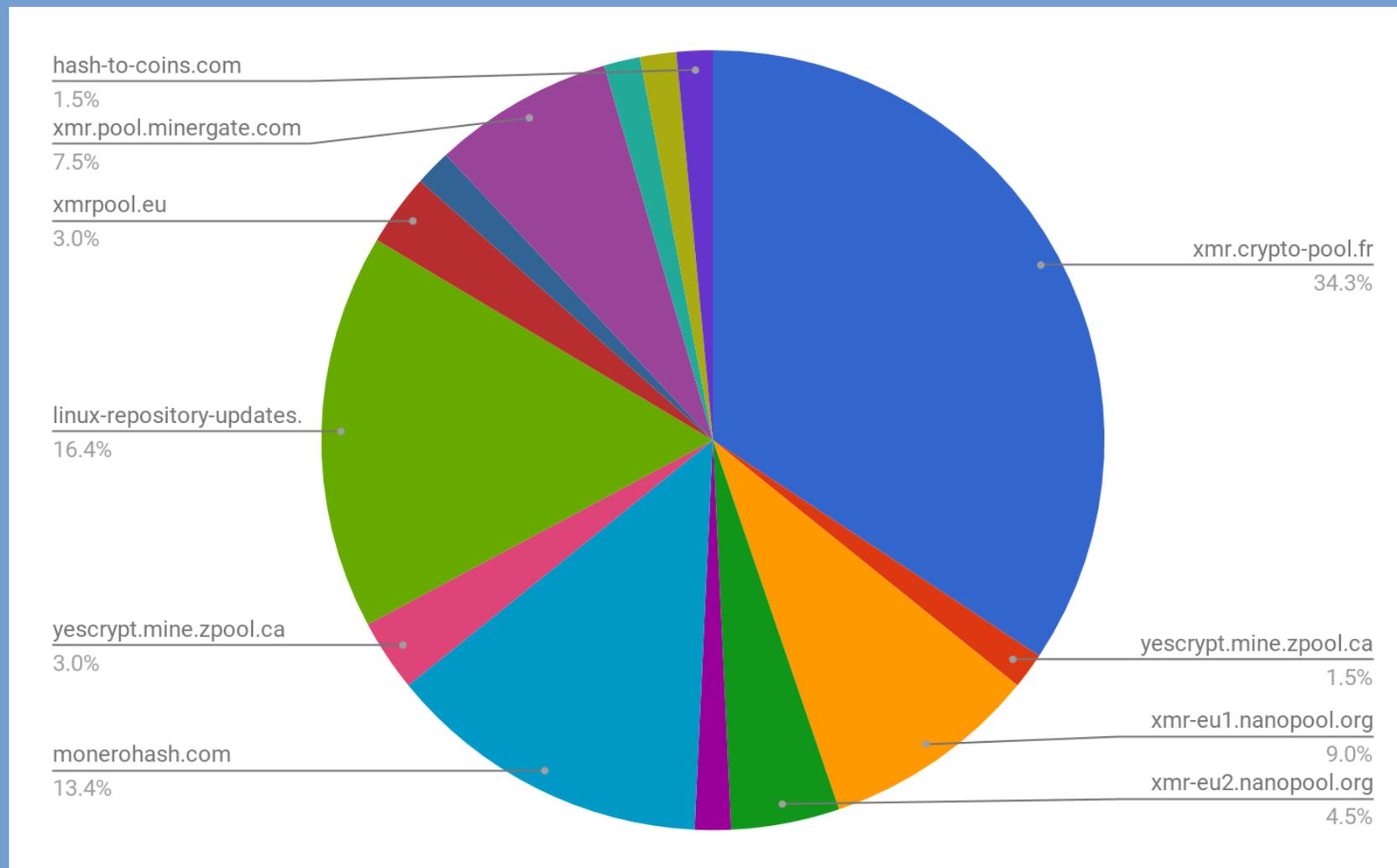
**Market**

- XMR: **0.02717354 BTC**
- XMR: **263.59 USD**
- XMR: **215.25 EUR**
- XMR: **201.41 GBP**

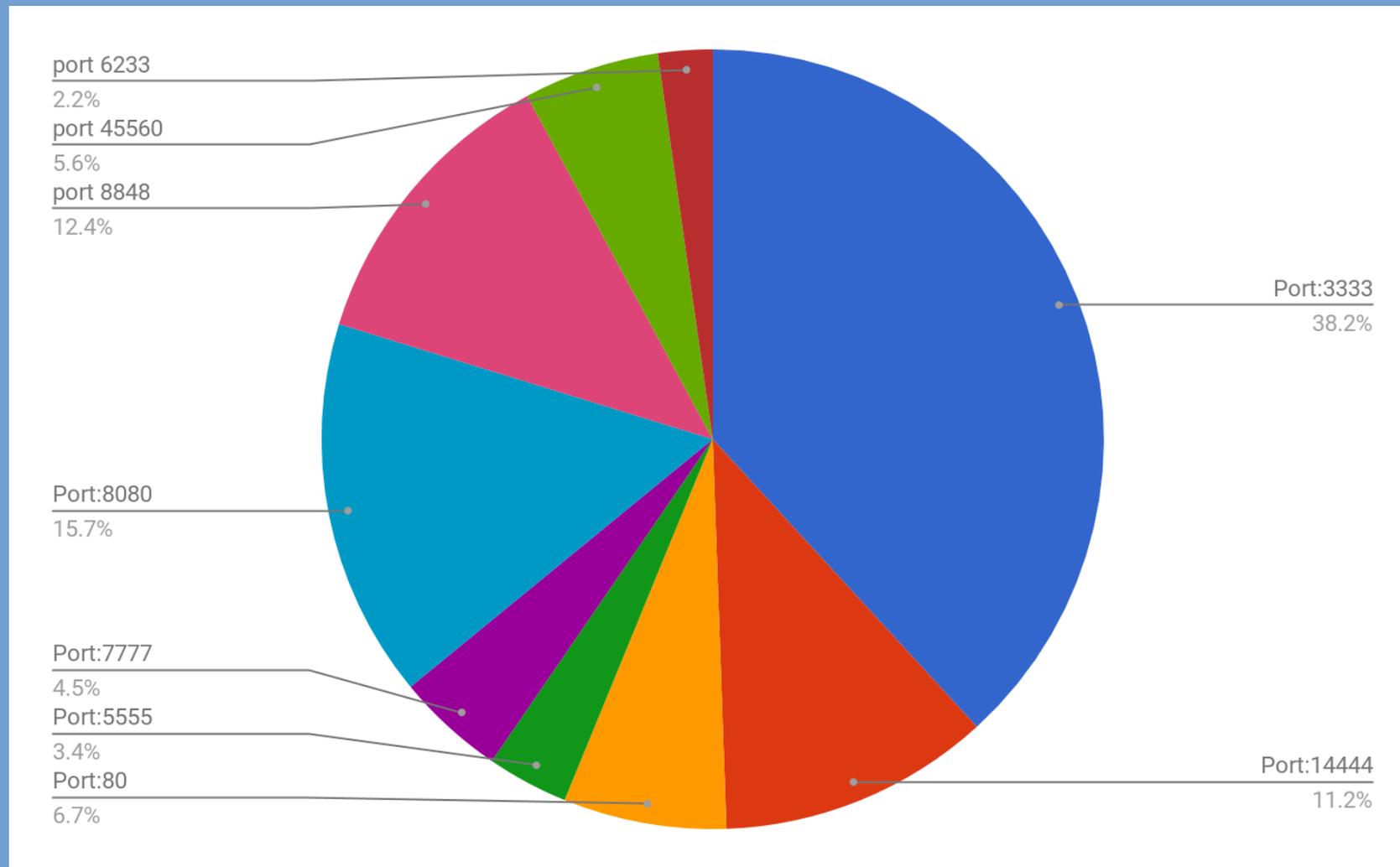
Updated: less than a minute ago  
Powered by [Crypsnator](#)

Estimate Mining Profit

# How do we know?



# How do we know?



# Off the shelf software

Monero Mining Pool [Home](#) [Pool Blocks](#) [Getting Started](#) [Payments](#) [Monitoring](#) [Poloniex](#) [Support](#)

## Wallet & Daemon Software

- [Getting started with Monero](#)
- Monero information and news on its [BitcoinTalk announcement thread](#)

---

## Mining Apps

App Name	Architecture	Downloads	Discussion	Source Code
<b>CPUMiner (forked by LucasJones &amp; Wolf)</b>	CPU	<a href="#">BitcoinTalk</a>	<a href="#">BitcoinTalk</a>	<a href="#">Github</a>
Example:	<code>minerd -a cryptonight -o stratum+tcp://xmr.crypto-pool.fr:3333 -u YOUR_WALLET_ADDRESS -p x</code>			
<b>YAM Miner (by yvg1900)</b>	CPU	<a href="#">MEGA</a>	<a href="#">Twitter</a>	Proprietary ©
Example:	<code>yam -c x -M stratum+tcp://YOUR_WALLET_ADDRESS:x@xmr.crypto-pool.fr:3333/xmr</code>			
<b>Claymore CPU Miner</b>	CPU	<a href="#">BitcoinTalk</a>	<a href="#">BitcoinTalk</a>	Proprietary ©
Example:	<code>NsCpuCNMiner64 -o stratum+tcp://xmr.crypto-pool.fr:3333 -u YOUR_WALLET_ADDRESS -p x</code>			
<b>Claymore GPU Miner</b>	OpenCL (AMD)	<a href="#">BitcoinTalk</a>	<a href="#">Discussion</a>	Proprietary ©
Example:	<code>NsGpuCNMiner -o stratum+tcp://xmr.crypto-pool.fr:3333 -u YOUR_WALLET_ADDRESS -p x</code>			
<b>ccminer (forked by tsiv)</b>	CUDA (Nvidia)	<a href="#">Github</a>	<a href="#">BitcoinTalk</a>	<a href="#">Github</a>
Example:	<code>ccminer -o stratum+tcp://xmr.crypto-pool.fr:3333 -u YOUR_WALLET_ADDRESS -p x</code>			

# Off the shelf software

Monero Mining Pool [Home](#) [Pool Blocks](#) [Getting Started](#) [Payments](#) [Monitoring](#) [Poloniex](#) [Support](#)

### Connection Details

📍 Mining Pool Address: **xmr.crypto-pool.fr**

#### Mining Ports

📍 Port: <b>3333 6666 7777 or 80,8080,443</b>	📍 Port: <b>8888</b>
🔒 Default Difficulty: <b>18000</b>	🔒 Default Difficulty: <b>30000</b>
🔒 Customs Difficulty Accepted: <b>Append +DIFF Mining Address</b>	🔒 Customs Difficulty Accepted: <b>Append +DIFF Mining Address</b>
? Description: <b>Port Stratum CPU2 (Hashrate &lt; 300H/sec)</b>	? Description: <b>Port Stratum RIG2 (Hashrate &lt; 1KH/Sec)</b>
📍 Port: <b>9999</b>	📍 Port: <b>8443</b>
🔒 Default Difficulty: <b>50000</b>	🔒 Default Difficulty: <b>50000</b>
🔒 Customs Difficulty Accepted: <b>Append +DIFF Mining Address</b>	🔒 Customs Difficulty Accepted: <b>Append +DIFF Mining Address</b>
? Description: <b>Port Stratum RIG3 (Hashrate &gt; 1KH/Sec)</b>	? Description: <b>SSL Port Stratum</b>

---

For Windows users new to mining

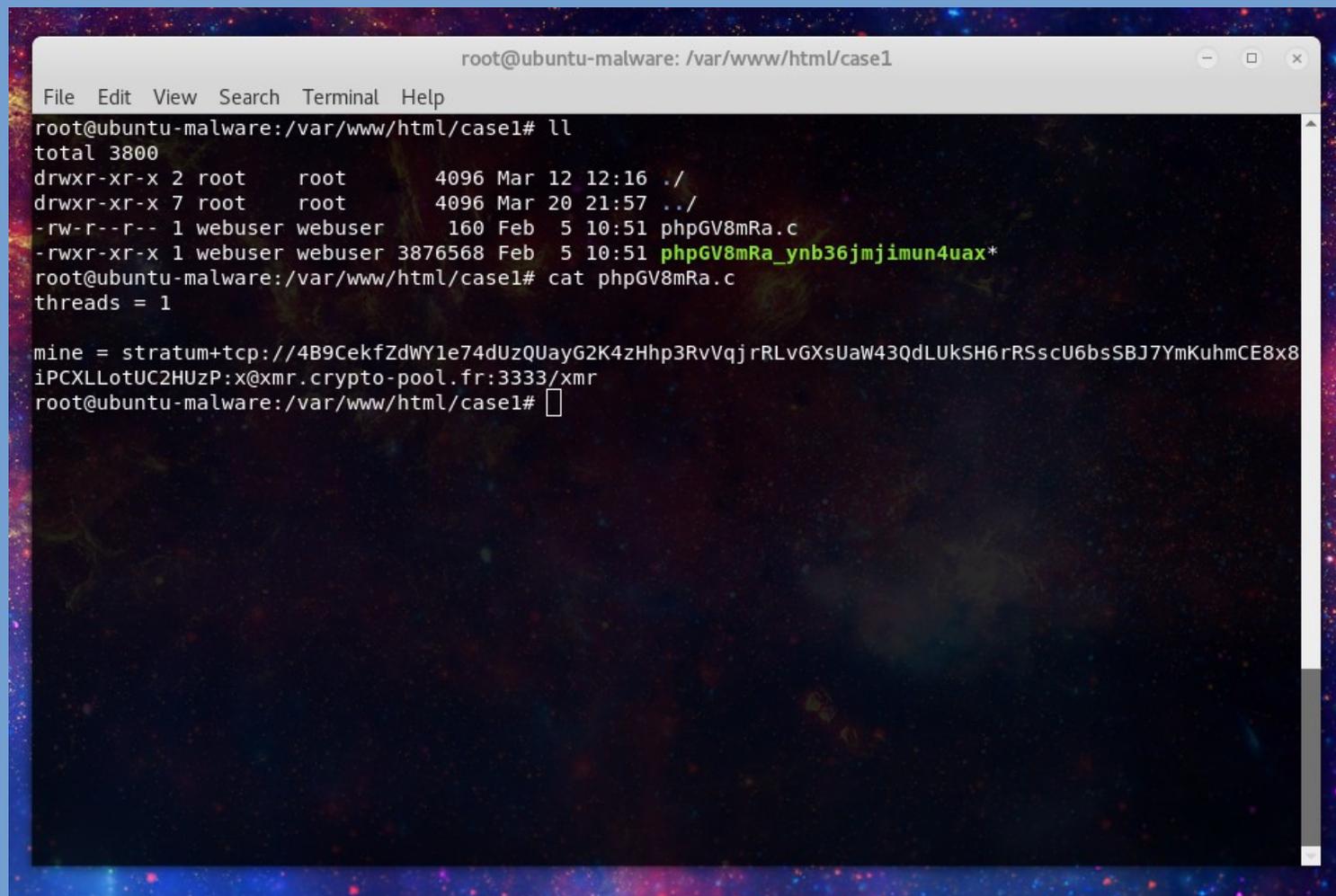
You can [Download](#) and run [cryptonote-easy-miner](#) which will automatically generate your wallet address and run CPU Miner with the proper parameters.

---

### Wallet & Daemon Software

- [Getting started with Monero](#)
- Monero information and news on its [BitcoinTalk announcement thread](#)

# Getting the keys



```
root@ubuntu-malware: /var/www/html/case1
File Edit View Search Terminal Help
root@ubuntu-malware:/var/www/html/case1# ll
total 3800
drwxr-xr-x 2 root  root    4096 Mar 12 12:16 ./
drwxr-xr-x 7 root  root    4096 Mar 20 21:57 ../
-rw-r--r-- 1 webuser webuser  160 Feb  5 10:51 phpGV8mRa.c
-rwxr-xr-x 1 webuser webuser 3876568 Feb  5 10:51 phpGV8mRa_ynb36jmjimun4uax*
root@ubuntu-malware:/var/www/html/case1# cat phpGV8mRa.c
threads = 1

mine = stratum+tcp://4B9CekfZdWY1e74dUzQUayG2K4zHhp3RvVqjrRLvGXsUaW43QdLUkSH6rRSscU6bsSBJ7YmKuhmCE8x8
iPCXLLotUC2HUzP:x@xmr.crypto-pool.fr:3333/xmr
root@ubuntu-malware:/var/www/html/case1#
```

# Payouts

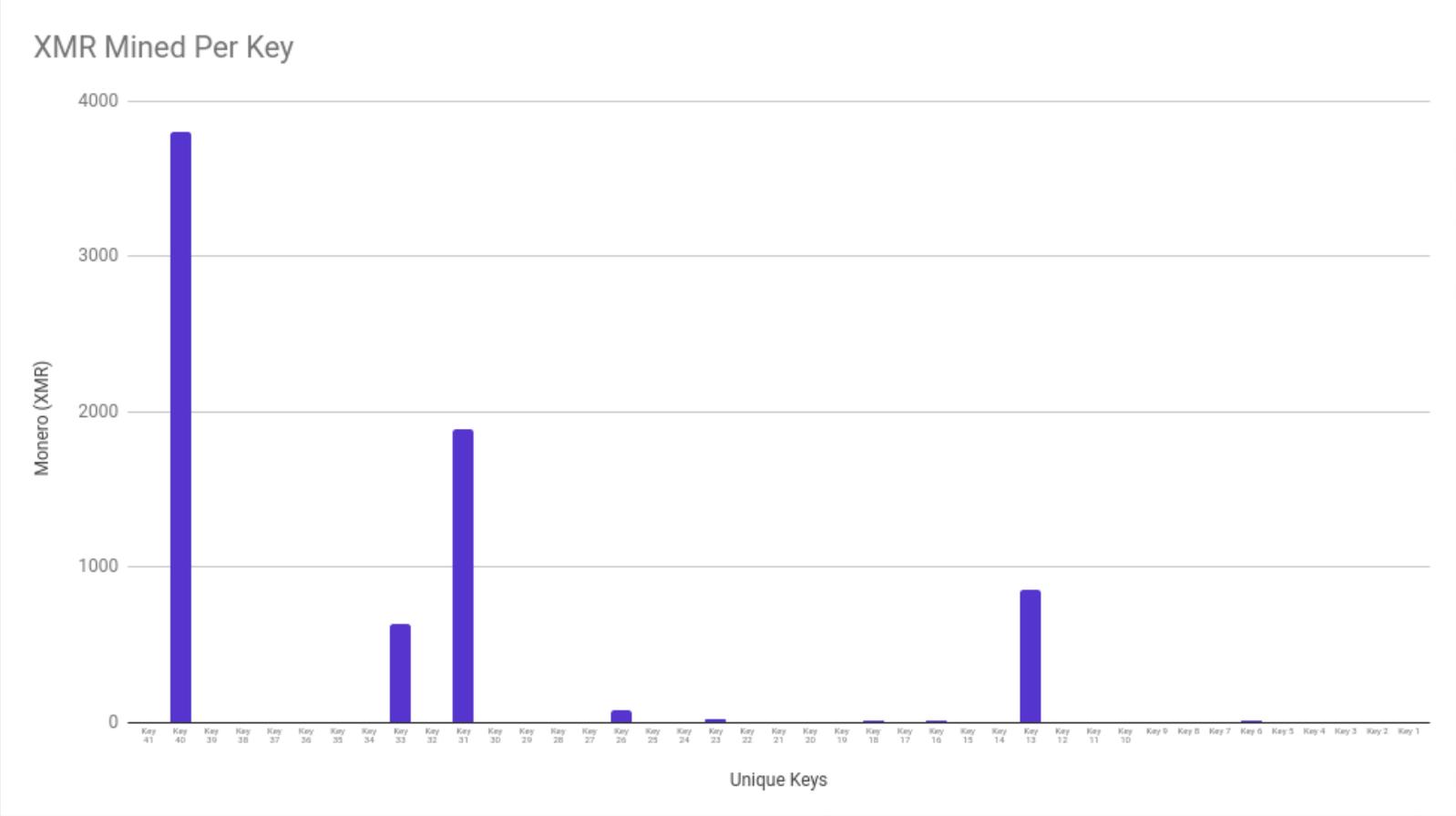
As of April 29<sup>th</sup>

1.61 Million USD

Over 41 unique Monero  
wallet keys



# Unique Wallet Data

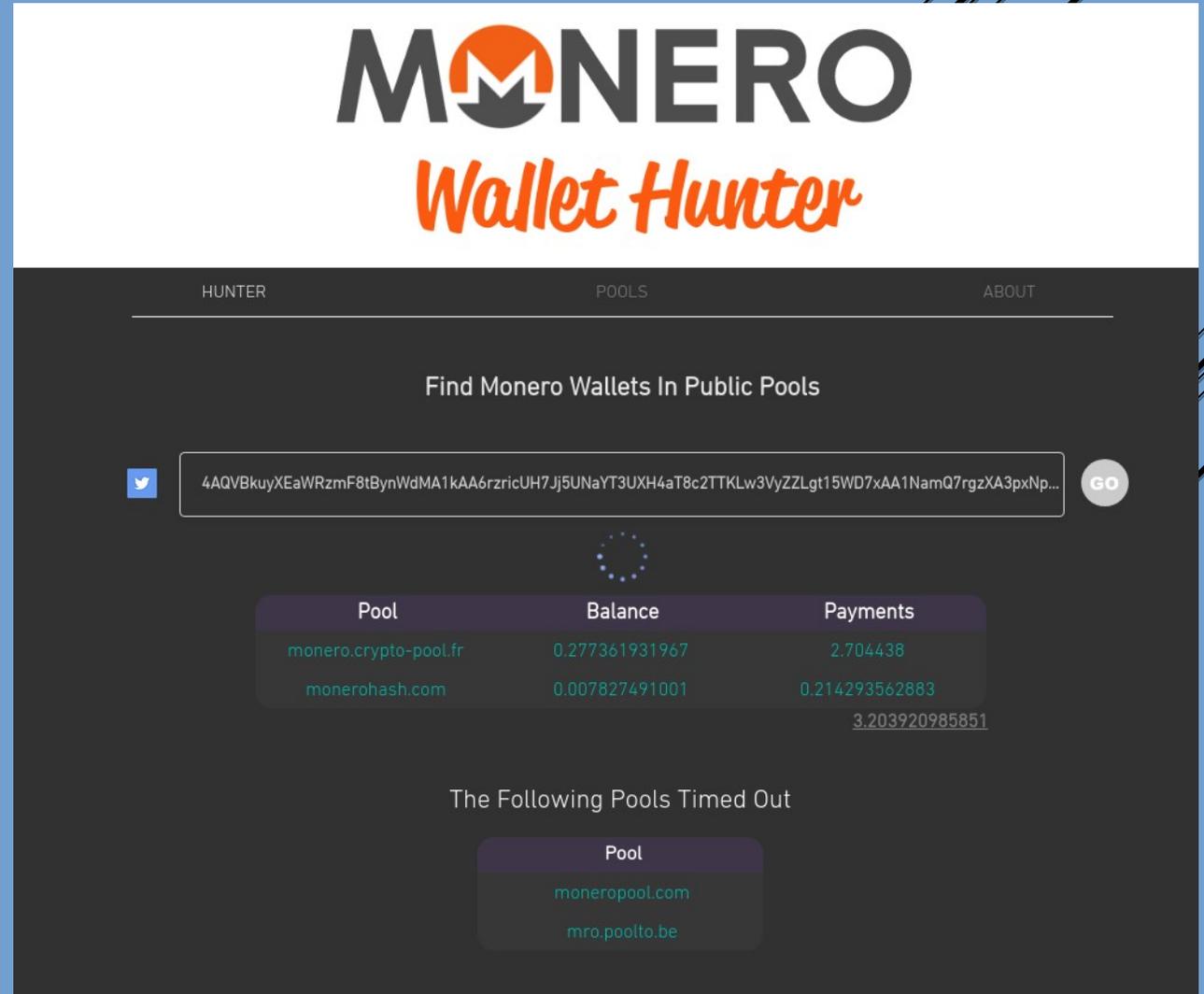


# Tracking Wallet Data

Go to individual pools...

Or use [xmrhunter.com](https://xmrhunter.com)

By :



The screenshot shows the MONERO Wallet Hunter website. At the top, the logo "MONERO" is in black with an orange 'M' containing a white arrow, and "Wallet Hunter" is in orange script. Below the logo are navigation links: HUNTER, POOLS, and ABOUT. The main heading is "Find Monero Wallets In Public Pools". A search bar contains a long alphanumeric string: "4AQVBkuyXEaWRzmF8tBynWdMA1kAA6rzricUH7Jj5UNaYT3UXH4aT8c2TTKLw3VyZZLgt15WD7xAA1NamQ7rgzXA3pxNp...". A "GO" button is to the right of the search bar. Below the search bar is a loading spinner. A table displays search results:

Pool	Balance	Payments
<a href="#">monero.crypto-pool.fr</a>	0.277361931967	2.704438
<a href="#">monerohash.com</a>	0.007827491001	0.214293562883
		<a href="#">3.203920985851</a>

Below the table, it says "The Following Pools Timed Out" and lists two pools in a rounded box:

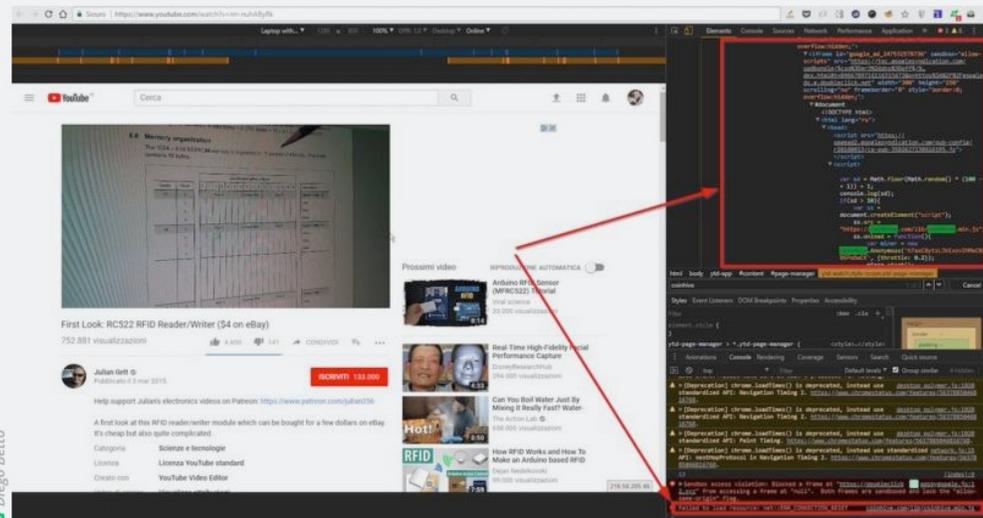
- [moneropool.com](#)
- [mro.poolto.be](#)

# Oh and also crypto-jacking

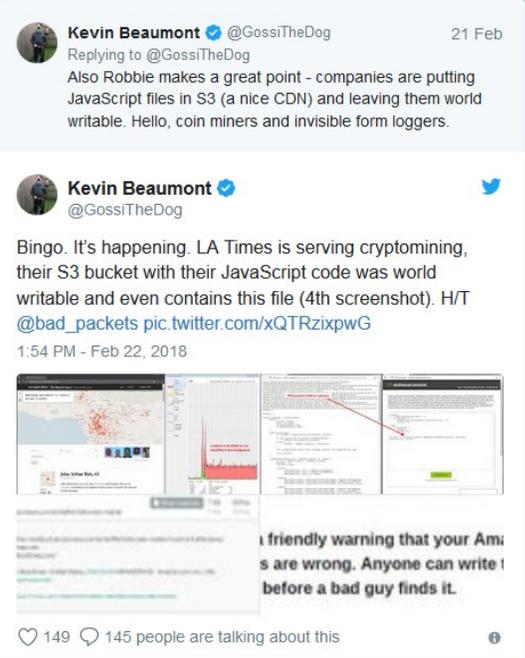
## Now even YouTube serves ads with CPU-draining cryptocurrency miners

Ad campaign lets attackers profit while unwitting users watch videos.

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



Enlarge



# Coinhive

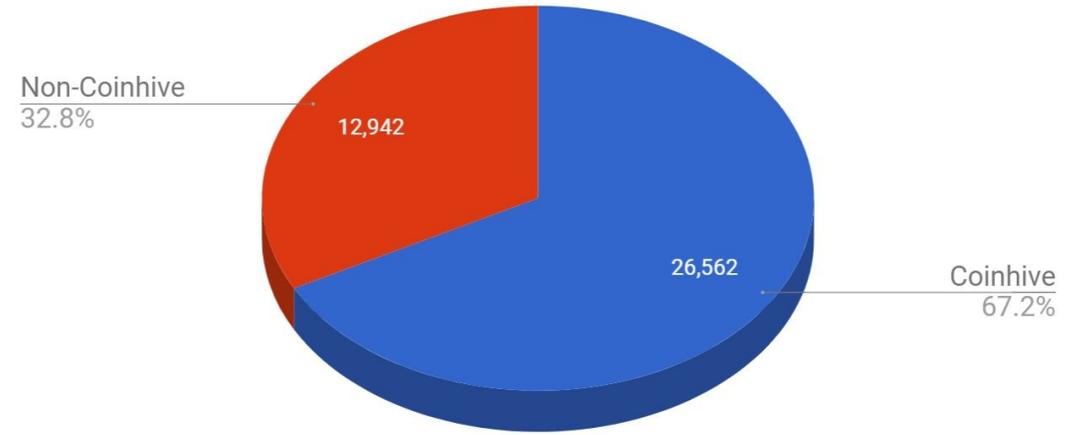
```
<script  
src="https://coinhive.com/lib/coinhive.min.js"></script>  
<script> var miner = new CoinHive.User('<site-key>',  
'john-doe'); miner.start(); </script>
```

The original, but now has plenty of competition:

Check out @bad\_packets for more

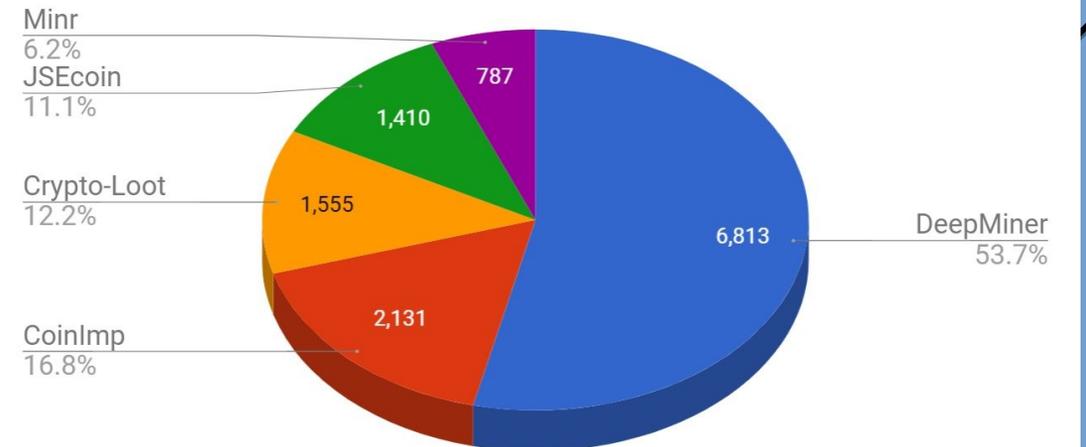


Number of websites found with a JavaScript cryptocurrency miner



@bad\_packets  
Source: PublicWWW  
Date: 2018-04-19

Number of websites found with a non-Coinhive cryptocurrency mining script



@bad\_packets  
Source: PublicWWW  
Date: 2018-04-19

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)
			Q	⊕		⊕	✖
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)
			Q	⊕		⊕	✖
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)
			Q	⊕		⊕	✖
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)
			Q	⊕		⊕	✖
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)
			Q	⊕		⊕	✖
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)
			Q	⊕		⊕	✖
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)
			Q	⊕		⊕	✖
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)
			Q	⊕		⊕	✖
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)
			Q	⊕		⊕	✖
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)
			Q	⊕		⊕	✖
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)
			Q	⊕		⊕	✖
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)
			Q	⊕		⊕	✖
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

Secure | <https://www.virustotal.com/#/file/ca5ed66923a2e4898ffdc6d3ab05cacc360d9be9b4568a7b8f9d0dbdb17d46f2/detection>

Search or scan a URL, IP address, domain, or file hash

**25 / 58** engines detected this file

SHA-256: ca5ed66923a2e4898ffdc6d3ab05cacc360d9be9b4568a7b8f9d0dbdb17d46f2  
File name: yam-yvg1900-M7v-linux64-generic.tgz  
File size: 1.35 MB  
Last analysis: 2017-09-14 06:34:48 UTC

Detection	Details	Relations	Community	
AhnLab-V3	Linux/Miner.3876568		Antiy-AVL	RiskWare[RiskTool]/Linux.BitCoinMine...
Arcabit	Application.BitCoinMiner.MA		Avast	ELF.BitCoinMiner-AI [Trj]
AVG	ELF.BitCoinMiner-AI [Trj]		Avira	SPR/BitCoinMiner.qpilj
BitDefender	Application.BitCoinMiner.MA		ClamAV	Unix.Malware.Agent-1847048
DrWeb	Tool.Linux.BtcMine.86		Emsisoft	Application.BitCoinMiner.MA (B)
eScan	Application.BitCoinMiner.MA		ESET-NOD32	a variant of Linux/BitCoinMiner.Z potentially unsafe
F-Secure	Application.BitCoinMiner.MA		GData	Application.BitCoinMiner.MA
Ikarus	PUA.Linux.Miner		Jiangmin	RiskTool.Linux.aq
Kaspersky	not-a-virus:HEUR:RiskTool.Linux.BitCoinMin...		MAX	malware (ai score=82)
McAfee	Linux/CoinMiner		McAfee-GW-Edition	Linux/CoinMiner
Sophos AV	Yet Another Miner (PUA)		Symantec	Trojan.Gen.NPE
TrendMicro	ELF_COINMINERA		TrendMicro-HouseCall	ELF_COINMINERA
ZoneAlarm	not-a-virus:HEUR:RiskTool.Linux.BitCoinMin...		Ad-Aware	Clean

# Tools

Minerchk

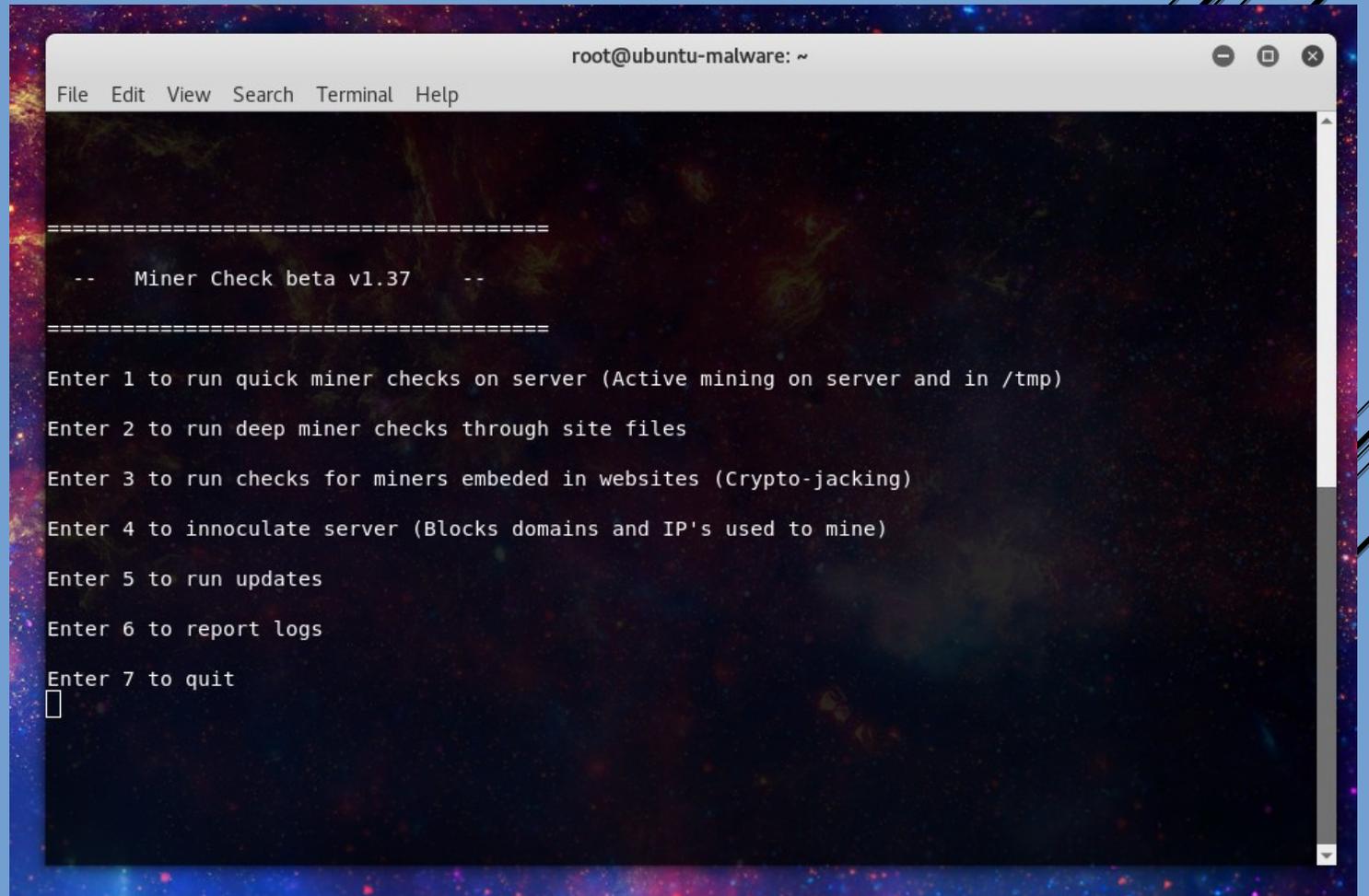
Built for Linux servers

Checks on system

Looks for Cryptojacking

Block access to pools

<https://github.com/Hestat/minerchk>

A screenshot of a terminal window titled 'root@ubuntu-malware: ~'. The window has a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The terminal content shows a menu for 'Miner Check beta v1.37' with options 1 through 7. The background of the terminal is a dark space with colorful nebulae. A cursor is visible at the bottom left of the terminal area.

```
root@ubuntu-malware: ~
File Edit View Search Terminal Help

=====
-- Miner Check beta v1.37 --
=====

Enter 1 to run quick miner checks on server (Active mining on server and in /tmp)
Enter 2 to run deep miner checks through site files
Enter 3 to run checks for miners embeded in websites (Crypto-jacking)
Enter 4 to innoculate server (Blocks domains and IP's used to mine)
Enter 5 to run updates
Enter 6 to report logs
Enter 7 to quit
█
```

# Tools pt 2

Aimed at crypto-jacking

Good for Endpoints or LAN Network blocking

<https://github.com/ZeroDot1/CoinBlockerLists>

ZeroDot1 / CoinBlockerLists

Watch 27 Star 148 Fork 16

Code Issues 2 Pull requests 0 Insights

Simple lists that can help prevent cryptomining in the browser or other applications. <https://git.io/vFFKT>

prevent-cryptomining hosts hostsfile block miner coinhive filter list pool administrator network blacklist coin

cryptojacking

215 commits 1 branch 0 releases 2 contributors GPL-3.0

Branch: master New pull request Create new file Upload files Find file Clone or download

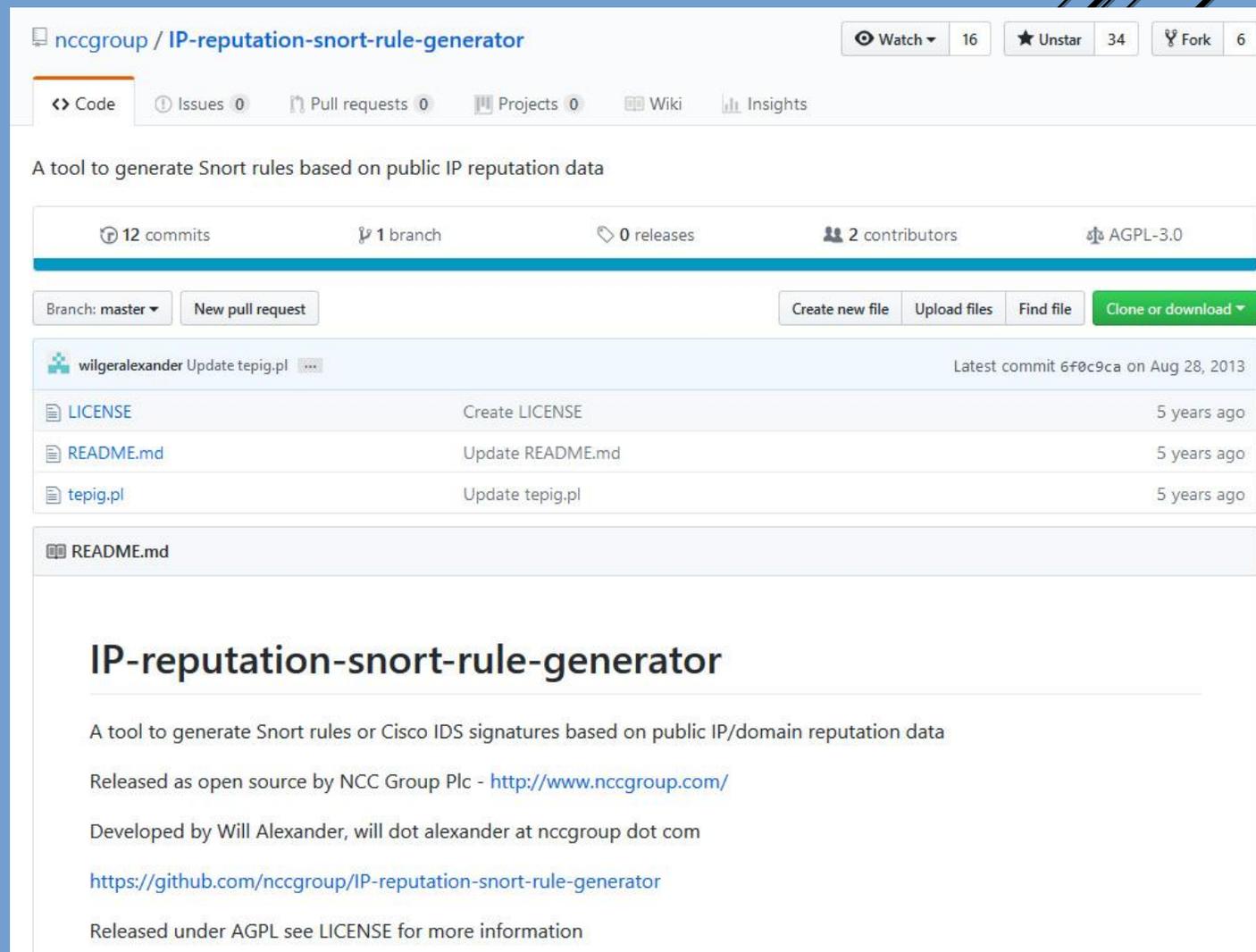
ZeroDot1 Last modified: 27 02 2018 17:19 Latest commit a5f79c0 2 minutes ago

File	Commit Message	Last Modified
.github	Add a ISSUE_TEMPLATE.md	2 days ago
img	Last modified: 13 02 2018 17:00	14 days ago
LICENSE	Initial commit	5 months ago
MiningServerIPList.txt	Last modified: 27 02 2018 17:19	2 minutes ago
README.md	Update README.MD	11 days ago
_config.yml	.	3 months ago
hosts	Last modified: 27 02 2018 17:19	2 minutes ago
hosts_browser	Last modified: 27 02 2018 17:19	2 minutes ago
hosts_optional	Last modified: 25 02 2018 00:00	3 days ago
invalid_hosts.txt	Last modified: 25 02 2018 00:00	3 days ago
list.txt	Last modified: 27 02 2018 17:19	2 minutes ago
list_browser.txt	Last modified: 27 02 2018 17:19	2 minutes ago
list_optional.txt	Last modified: 25 02 2018 00:00	3 days ago
white_list.txt	Last modified: 27 02 2018 17:19	2 minutes ago

# 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>



The screenshot shows the GitHub repository page for `nccgroup / IP-reputation-snort-rule-generator`. The repository has 16 watchers, 34 stars, and 6 forks. It contains 12 commits, 1 branch, 0 releases, and 2 contributors. The license is AGPL-3.0. The latest commit by `wilgeralexander` is titled "Update tepig.pl" and was made on August 28, 2013. The repository includes files for `LICENSE`, `README.md`, and `tepig.pl`. The `README.md` file is displayed, containing the following text:

## IP-reputation-snort-rule-generator

A tool to generate Snort rules or Cisco IDS signatures based on public IP/domain reputation data

Released as open source by NCC Group Plc - <http://www.nccgroup.com/>

Developed by Will Alexander, will dot alexander at nccgroup dot com

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

Released under AGPL see LICENSE for more information

# 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