Remcos

github.com/itaymigdal/malware-analysis-writeups/blob/main/Remcos/Remcos.md

itaymigdal

itaymigdal/**malware-analysis-writeups**

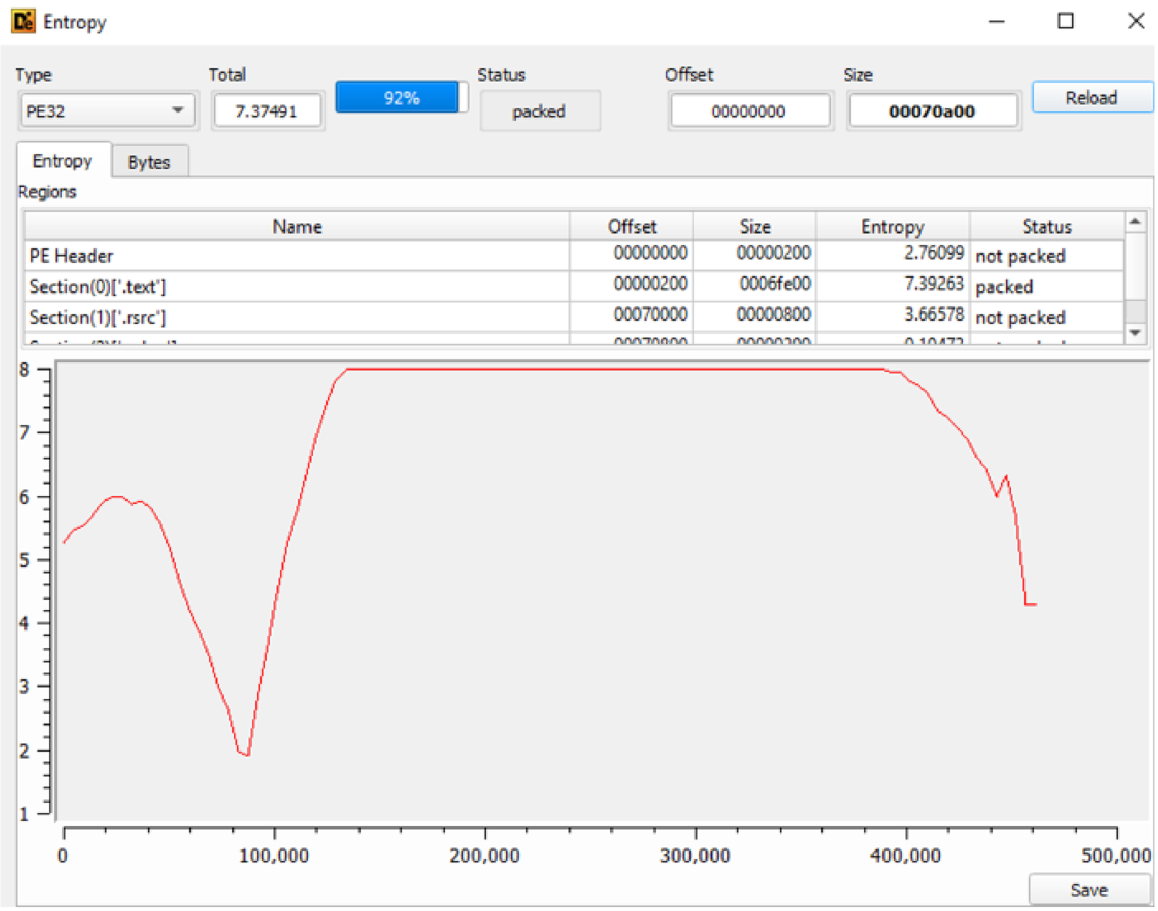
Some of my Malware Analysis writeups.

Malware Name	File Type	SHA256
Remcos	x32 exe (.NET)	5eb996275b36c1e8c1d3daa71e6469507a29401c77f2b1fd91e4d354ccde9860

Analysis process

This writeup starts with a suspicious executable that was sent via mail.

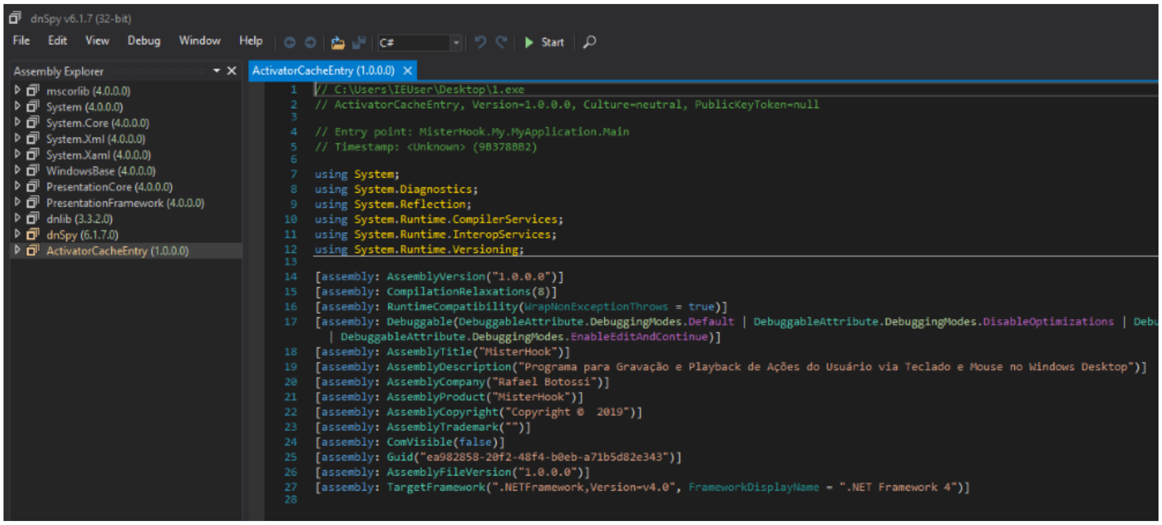
We can see that most part of the PE is packed (entropy ~ 8 -> High entropy indicates on encrypted / compressed data):



Type	Total		Status	Offset	Size
PE32	7.37491	92%	packed	00000000	00070a00

Name	Offset	Size	Entropy	Status
PE Header	00000000	00000200	2.76099	not packed
Section(0)['.text']	00000200	0006fe00	7.39263	packed
Section(1)['.rsrc']	00070000	00000800	3.66578	not packed

The PE is .NET so we'll check it out in Dnspy:



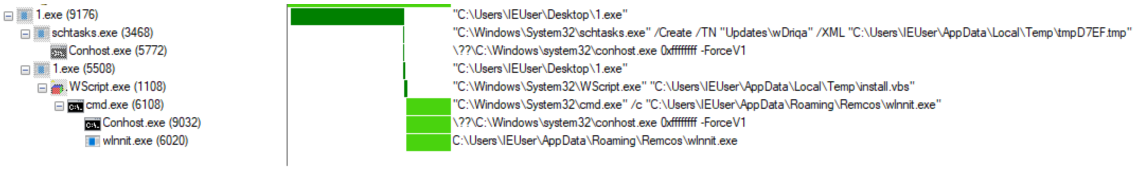
```
// C:\Users\IEUser\Desktop\1.exe
// ActivatorCacheEntry, Version=1.0.0.0, Culture=neutral, PublicKeyToken=null

// Entry point: MisterHook.My.MyApplication.Main
// Timestamp: <Unknown> (9B378BB2)

using System;
using System.Diagnostics;
using System.Reflection;
using System.Runtime.CompilerServices;
using System.Runtime.InteropServices;
using System.Runtime.Versioning;

[assembly: AssemblyVersion("1.0.0.0")]
[assembly: CompilationRelaxations(8)]
[assembly: RuntimeCompatibility(WrapNonExceptionThrows = true)]
[assembly: Debuggable(DebuggableAttribute.DebuggingModes.Default | DebuggableAttribute.DebuggingModes.DisableOptimizations | Debu
  | DebuggableAttribute.DebuggingModes.EnableEditAndContinue)]
[assembly: AssemblyTitle("MisterHook")]
[assembly: AssemblyDescription("Programa para Gravação e Playback de Ações do Usuário via Teclado e Mouse no Windows Desktop")]
[assembly: AssemblyCompany("Rafael Botossi")]
[assembly: AssemblyProduct("MisterHook")]
[assembly: AssemblyCopyright("Copyright ©  2019")]
[assembly: AssemblyTrademark("")]
[assembly: ComVisible(false)]
[assembly: Guid("ea982858-20f2-48f4-b0eb-a71b5d82e343")]
[assembly: AssemblyFileVersion("1.0.0.0")]
[assembly: TargetFramework(".NETFramework,Version=v4.0", FrameworkDisplayName = ".NET Framework 4")]
```

As usual, we'll watch it under Procmon. this is the interesting process tree:

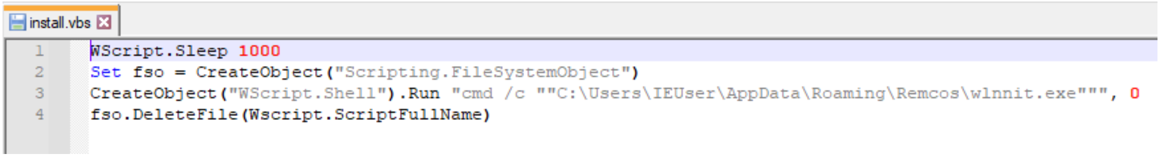


1.exe (9176)	"C:\Users\IEUser\Desktop\1.exe"
schtasks.exe (3468)	"C:\Windows\System32\schtasks.exe" /Create /TN "Updates\wDriqa" /XML "C:\Users\IEUser\AppData\Local\Temp\tmpD7EF.tmp"
Conhost.exe (5772)	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
1.exe (5508)	"C:\Users\IEUser\Desktop\1.exe"
WScript.exe (1108)	"C:\Windows\System32\WScript.exe" "C:\Users\IEUser\AppData\Local\Temp\install.vbs"
cmd.exe (6108)	"C:\Windows\System32\cmd.exe" /c "C:\Users\IEUser\AppData\Roaming\Remcos\wlnnit.exe"
Conhost.exe (9032)	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
wlnnit.exe (6020)	C:\Users\IEUser\AppData\Roaming\Remcos\wlnnit.exe

We can see that:

- The file creates scheduled task for persistence
- The file writes a vbs script to `\AppData\Local\Temp\` and runs it
- The vbs script copies the malware to `\AppData\Roaming\remcos\` (Nice spoiler, thank you malware author 😘), and executes it from there.

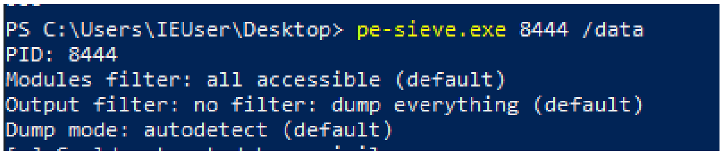
The Script content:



```
WScript.Sleep 1000
Set fso = CreateObject("Scripting.FileSystemObject")
CreateObject("WScript.Shell").Run "cmd /c ""C:\Users\IEUser\AppData\Roaming\Remcos\wlnnit.exe""", 0
fso.DeleteFile(Wscript.ScriptFullName)
```

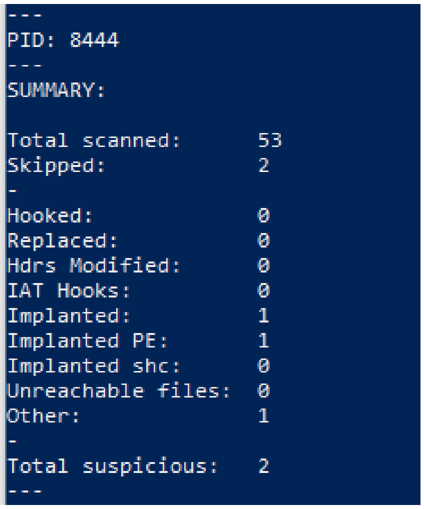
As we can see, after the copy & execute, the vbs script deletes itself (and is written back next execution).

In this analysis i took the "quick and dirty" approach, so i in order to unpack the file, i let it run for about a minute or two, and then dumped it using Pe-Sieve (i added the /data argument, because this is .NET executable):



```
PS C:\Users\IEUser\Desktop> pe-sieve.exe 8444 /data
PID: 8444
Modules filter: all accessible (default)
Output filter: no filter: dump everything (default)
Dump mode: autodetect (default)
```

And Vwalla:

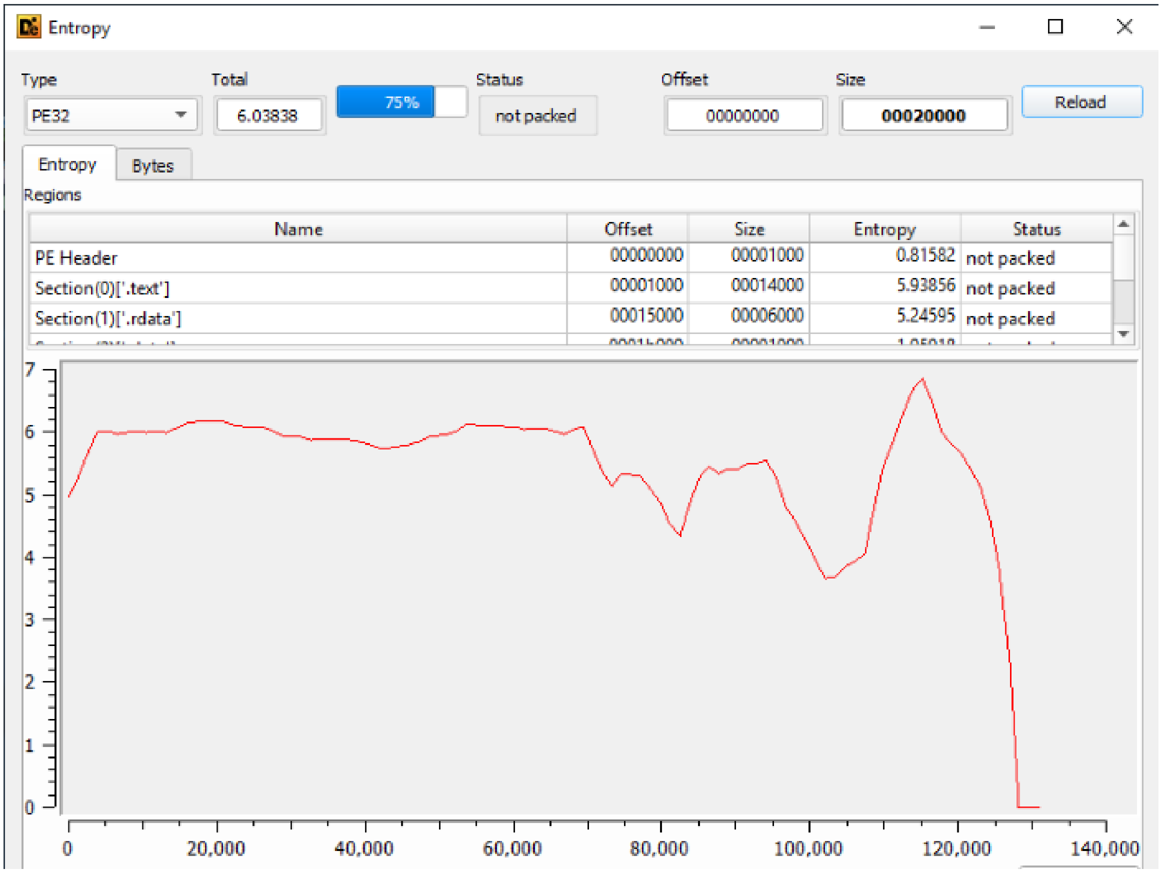


```
---
PID: 8444
---
SUMMARY:

Total scanned:      53
Skipped:            2
-
Hooked:             0
Replaced:           0
Hdrs Modified:      0
IAT Hooks:          0
Implanted:          1
Implanted PE:       1
Implanted shc:      0
Unreachable files:  0
Other:              1
-
Total suspicious:   2
---
```

We've got our unpacked version with nice icon:

And it isn't packed:

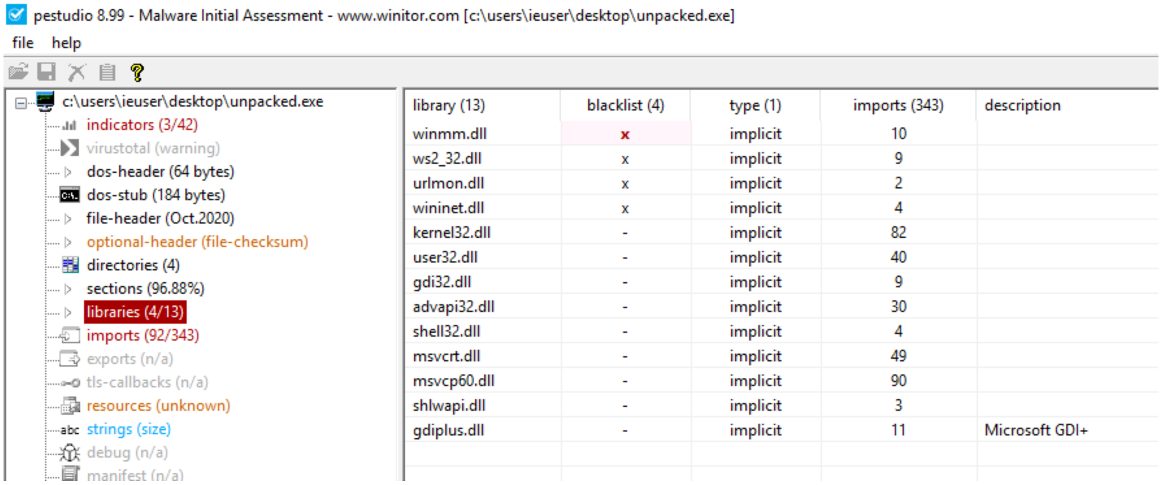


Entropy

Type: PE32 | Total: 6.03838 | 75% | Status: not packed | Offset: 00000000 | Size: 00020000

Name	Offset	Size	Entropy	Status
PE Header	00000000	00001000	0.81582	not packed
Section(0)['.text']	00001000	00014000	5.93856	not packed
Section(1)['.rdata']	00015000	00006000	5.24595	not packed

The file is a native PE file (i.e. written in C\C++, unlike the loader which was written in .NET), and it's importing a lot of interesting libraries:



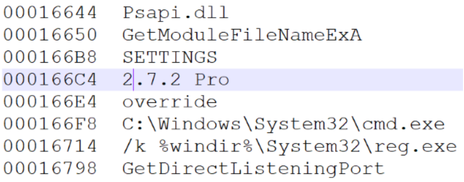
pestudio 8.99 - Malware Initial Assessment - www.winitor.com [c:\users\ieuser\desktop\unpacked.exe]

- c:\users\ieuser\desktop\unpacked.exe
  - indicators (3/42)
  - virustotal (warning)
  - dos-header (64 bytes)
  - dos-stub (184 bytes)
  - file-header (Oct.2020)
  - optional-header (file-checksum)
  - directories (4)
  - sections (96.88%)
  - libraries (4/13)
  - imports (92/343)
  - exports (n/a)
  - tls-callbacks (n/a)
  - resources (unknown)
  - strings (size)
  - debug (n/a)
  - manifest (n/a)

library (13)	blacklist (4)	type (1)	imports (343)	description
winmm.dll	x	implicit	10	
ws2_32.dll	x	implicit	9	
urlmon.dll	x	implicit	2	
wininet.dll	x	implicit	4	
kernel32.dll	-	implicit	82	
user32.dll	-	implicit	40	
gdi32.dll	-	implicit	9	
advapi32.dll	-	implicit	30	
shell32.dll	-	implicit	4	
msvcrt.dll	-	implicit	49	
msvcp60.dll	-	implicit	90	
shlwapi.dll	-	implicit	3	
gdiplus.dll	-	implicit	11	Microsoft GDI+

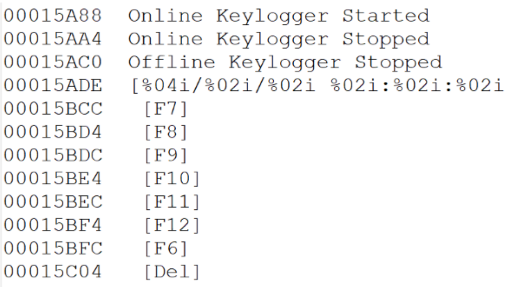
Observing the strings we find very interesting finds:

Indeed the malware is Remcos PRO 2.7.2:



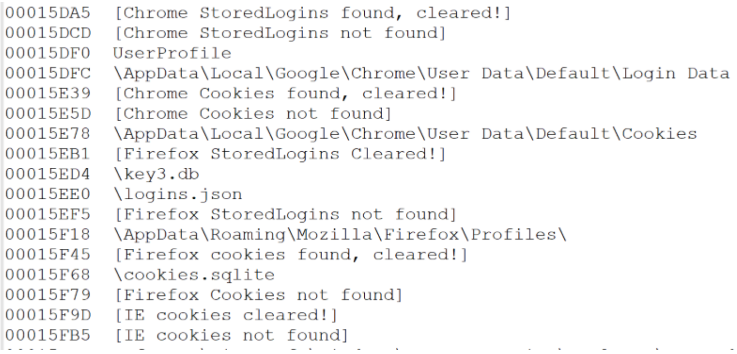
```
00016644   Psapi.dll
00016650   GetModuleFileNameExA
000166B8   SETTINGS
000166C4   2.7.2 Pro
000166E4   override
000166F8   C:\Windows\System32\cmd.exe
00016714   /k %windir%\System32\reg.exe
00016798   GetDirectListeningPort
```

Keylogger capabilities:



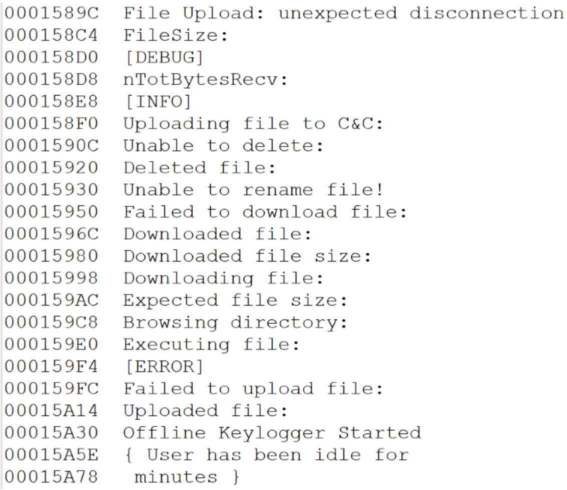
```
00015A88  Online Keylogger Started
00015AA4  Online Keylogger Stopped
00015AC0  Offline Keylogger Stopped
00015ADE  [%04i/%02i/%02i %02i:%02i:%02i
00015BCC   [F7]
00015BD4   [F8]
00015BDC   [F9]
00015BE4   [F10]
00015BEC   [F11]
00015BF4   [F12]
00015BFC   [F6]
00015C04   [Del]
```

Browser stealing capabilities:



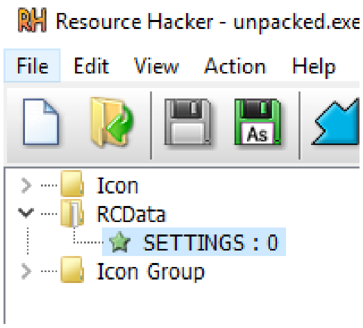
```
00015DA5  [Chrome StoredLogins found, cleared!]
00015DCD  [Chrome StoredLogins not found]
00015DF0  UserProfile
00015DFC  \AppData\Local\Google\Chrome\User Data\Default\Login Data
00015E39  [Chrome Cookies found, cleared!]
00015E5D  [Chrome Cookies not found]
00015E78  \AppData\Local\Google\Chrome\User Data\Default\Cookies
00015EB1  [Firefox StoredLogins Cleared!]
00015ED4  \key3.db
00015EE0  \logins.json
00015EF5  [Firefox StoredLogins not found]
00015F18  \AppData\Roaming\Mozilla\Firefox\Profiles\
00015F45  [Firefox cookies found, cleared!]
00015F68  \cookies.sqlite
00015F79  [Firefox Cookies not found]
00015F9D  [IE cookies cleared!]
00015FB5  [IE cookies not found]
```

Exfilitration and Infilitration capabilities:

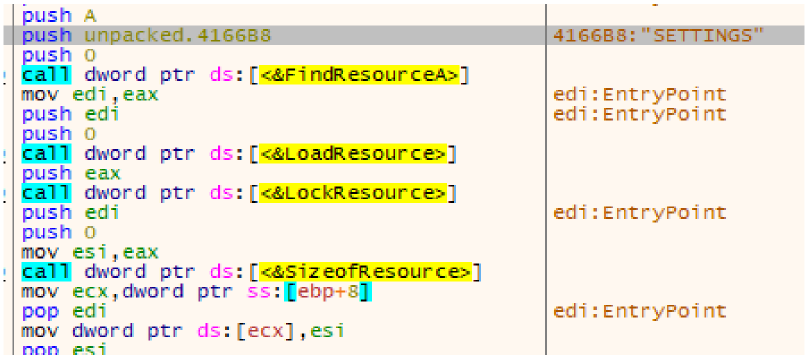


```
0001589C  File Upload: unexpected disconnection
000158C4  FileSize:
000158D0  [DEBUG]
000158D8  nTotBytesRecv:
000158E8  [INFO]
000158F0  Uploading file to C&C:
0001590C  Unable to delete:
00015920  Deleted file:
00015930  Unable to rename file!
00015950  Failed to download file:
0001596C  Downloaded file:
00015980  Downloaded file size:
00015998  Downloading file:
000159AC  Expected file size:
000159C8  Browsing directory:
000159E0  Executing file:
000159F4  [ERROR]
000159FC  Failed to upload file:
00015A14  Uploaded file:
00015A30  Offline Keylogger Started
00015A5E  { User has been idle for
00015A78   minutes }
```

The malware contains a setting resource which looks encrypted:

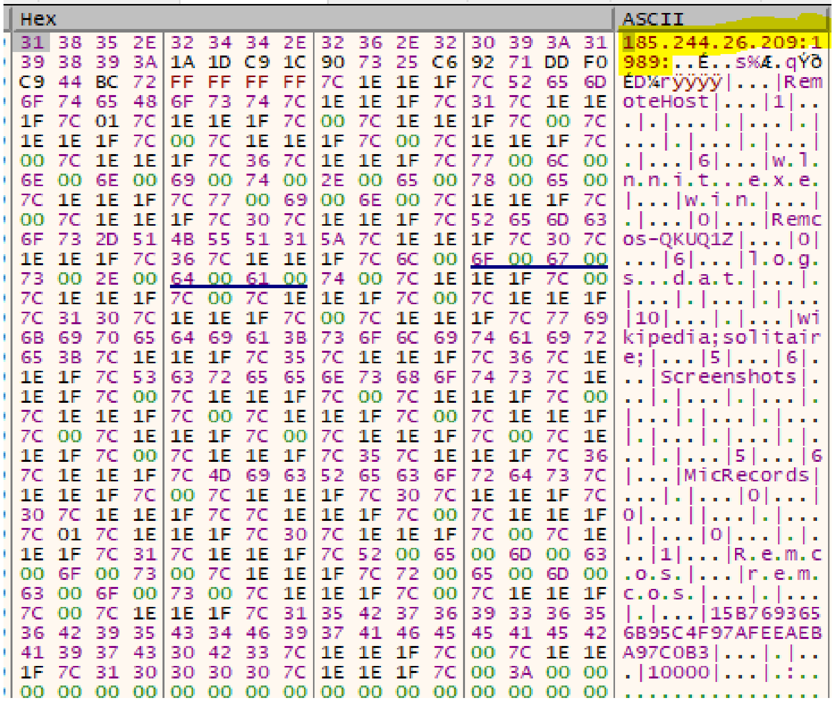


So we will try to watch it decrypted in memory. here we can see the file loads it:



```
push A
push unpacked.4166B8                 4166B8:"SETTINGS"
push 0
call dword ptr ds:[<&FindResourceA>]
mov edi,eax                          edi:EntryPoint
push edi                             edi:EntryPoint
push 0
call dword ptr ds:[<&LoadResource>]
push eax
call dword ptr ds:[<&LockResource>]
push edi                             edi:EntryPoint
push 0
mov esi,eax
call dword ptr ds:[<&SizeofResource>]
mov ecx,dword ptr ss:[ebp+8]
pop edi                              edi:EntryPoint
mov dword ptr ds:[ecx],esi
pop esi
```

And after some math we see the settings in clear text:

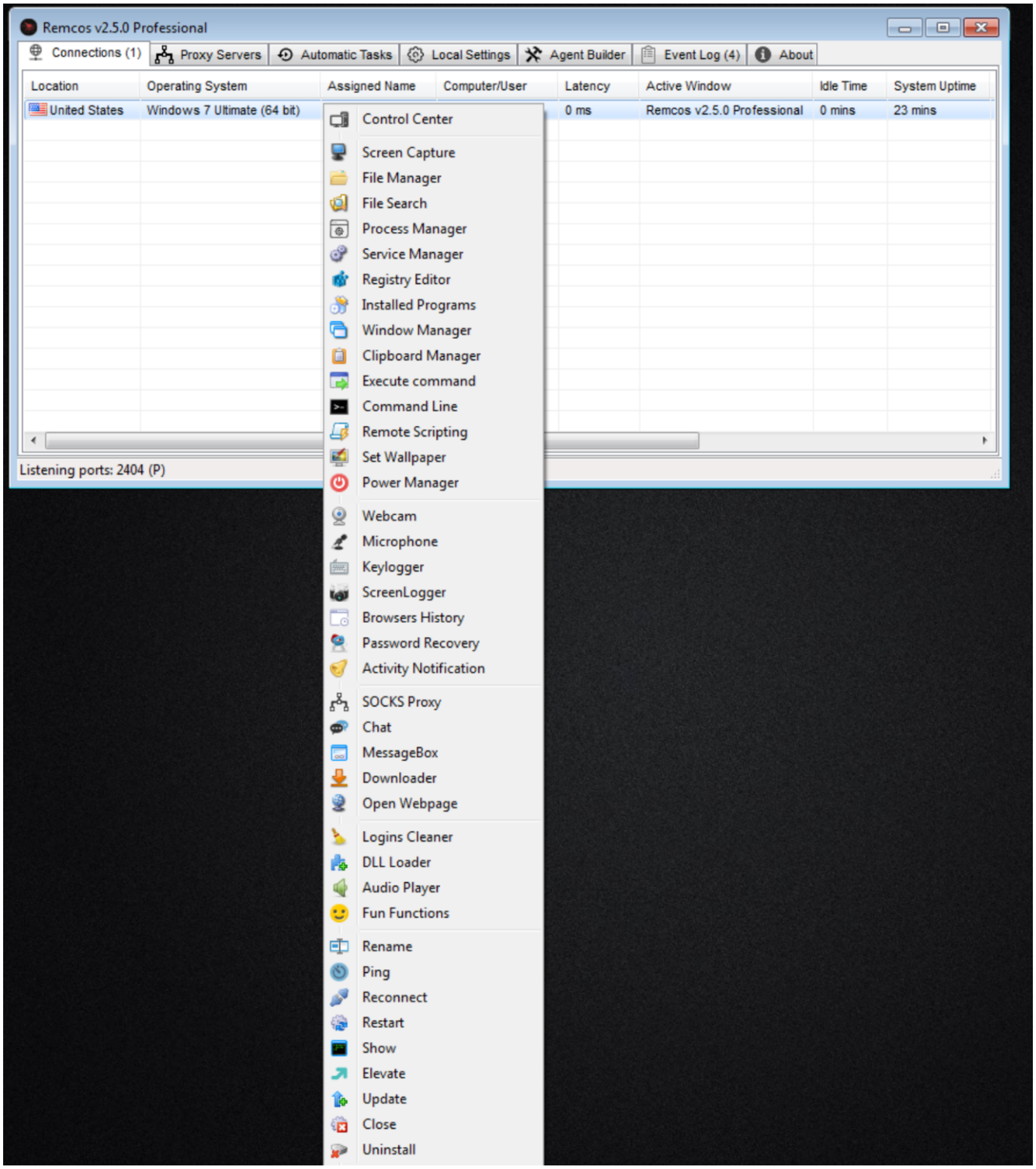


```
Hex                                                  ASCII
31 38 35 2E 32 34 34 2E 32 36 2E 32 30 39 3A 31  185.244.26.209:1
39 38 39 3A 1A 1D C9 1C 90 73 25 C6 92 71 DD F0  989:..É..s%Æ.qÝð
C9 44 BC 72 FF FF FF FF 7C 1E 1E 1F 7C 52 65 6D  ÉD¼rÿÿÿÿ|...|Rem
6F 74 65 48 6F 73 74 7C 1E 1E 1F 7C 31 7C 1E 1E  oteHost|...|1|..
1F 7C 01 7C 1E 1E 1F 7C 00 7C 1E 1E 1F 7C 00 7C  .|.|...|.|...|.|
1E 1E 1F 7C 00 7C 1E 1E 1F 7C 00 7C 1E 1E 1F 7C  ...|.|...|.|...|
00 7C 1E 1E 1F 7C 36 7C 1E 1E 1F 7C 77 00 6C 00  .|...|6|...|w.l.
6E 00 6E 00 69 00 74 00 2E 00 65 00 78 00 65 00  n.n.i.t...e.x.e.
7C 1E 1E 1F 7C 77 00 69 00 6E 00 7C 1E 1E 1F 7C  |...|w.i.n.|...|
00 7C 1E 1E 1F 7C 30 7C 1E 1E 1F 7C 52 65 6D 63  .|...|0|...|Remc
6F 73 2D 51 4B 55 51 31 5A 7C 1E 1E 1F 7C 30 7C  os-QKUQ1Z|...|0|
1E 1E 1F 7C 36 7C 1E 1E 1F 7C 6C 00 6F 00 67 00  ...|6|...|l.o.g.
73 00 2E 00 64 00 61 00 74 00 7C 1E 1E 1F 7C 00  s...d.a.t.|...|.
7C 1E 1E 1F 7C 00 7C 1E 1E 1F 7C 00 7C 1E 1E 1F  |...|.|...|.|...
7C 31 30 7C 1E 1E 1F 7C 00 7C 1E 1E 1F 7C 77 69  |10|...|.|...|wi
6B 69 70 65 64 69 61 3B 73 6F 6C 69 74 61 69 72  kipedia;solitair
65 3B 7C 1E 1E 1F 7C 35 7C 1E 1E 1F 7C 36 7C 1E  e;|...|5|...|6|.
1E 1F 7C 53 63 72 65 65 6E 73 68 6F 74 73 7C 1E  ..|Screenshots|.
1E 1F 7C 00 7C 1E 1E 1F 7C 00 7C 1E 1E 1F 7C 00  ..|.|...|.|...|.
7C 1E 1E 1F 7C 00 7C 1E 1E 1F 7C 00 7C 1E 1E 1F  |...|.|...|.|...
7C 00 7C 1E 1E 1F 7C 00 7C 1E 1E 1F 7C 00 7C 1E  |.|...|.|...|.|.
1E 1F 7C 00 7C 1E 1E 1F 7C 35 7C 1E 1E 1F 7C 36  ..|.|...|5|...|6
7C 1E 1E 1F 7C 4D 69 63 52 65 63 6F 72 64 73 7C  |...|MicRecords|
1E 1E 1F 7C 00 7C 1E 1E 1F 7C 30 7C 1E 1E 1F 7C  ...|.|...|0|...|
30 7C 1E 1E 1F 7C 7C 1E 1E 1F 7C 00 7C 1E 1E 1F  0|...||...|.|...
7C 01 7C 1E 1E 1F 7C 30 7C 1E 1E 1F 7C 00 7C 1E  |.|...|0|...|.|.
1E 1F 7C 31 7C 1E 1E 1F 7C 52 00 65 00 6D 00 63  ..|1|...|R.e.m.c
00 6F 00 73 00 7C 1E 1E 1F 7C 72 00 65 00 6D 00  .o.s.|...|r.e.m.
63 00 6F 00 73 00 7C 1E 1E 1F 7C 00 7C 1E 1E 1F  c.o.s.|...|.|...
7C 00 7C 1E 1E 1F 7C 31 35 42 37 36 39 33 36 35  |.|...|15B769365
36 42 39 35 43 34 46 39 37 41 46 45 45 41 45 42  6B95C4F97AFEEAEB
41 39 37 43 30 42 33 7C 1E 1E 1F 7C 00 7C 1E 1E  A97C0B3|...|.|..
1F 7C 31 30 30 30 30 7C 1E 1E 1F 7C 00 3A 00 00  .|10000|...|.:..
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

> c2 Server: 185.244.26.209

We can see some more juicy stuff, like Mutex string, execution path, logs path and encryption keys.

After some Googling about Remcos, seems like it is total legal software which has a very detailed site. This is how the panel from the attacker side looks like:



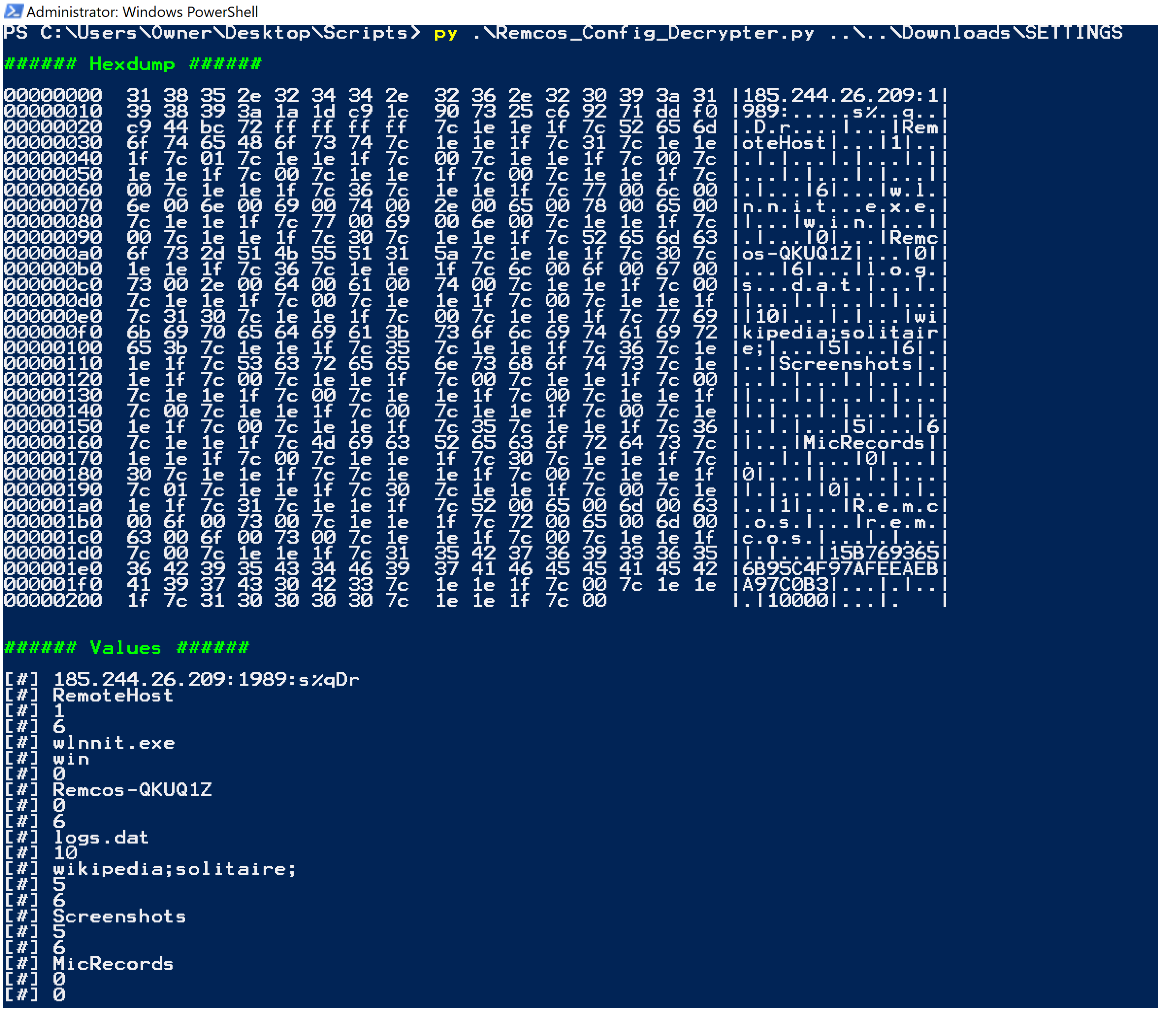
Location	Operating System	Assigned Name	Computer/User	Latency	Active Window	Idle Time	System Uptime
United States	Windows 7 Ultimate (64 bit)			0 ms	Remcos v2.5.0 Professional	0 mins	23 mins

Listening ports: 2404 (P)

A lot of nice and evil capabilities 😏.

Bonus

After watching this, i learned how Remcos encrypts his config, so i wrote a little script that retrieves a Remcos encrypted SETTINGS file, and decrypts is:



Administrator: Windows PowerShell

```
PS C:\Users\Owner\Desktop\Scripts> py .\Remcos_Config_Decrypter.py ..\..\Downloads\SETTINGS
###### Hexdump ######

00000000  31 38 35 2e 32 34 34 2e  32 36 2e 32 30 39 3a 31 |185.244.26.209:1|
00000010  39 38 39 3a 1a 1d c9 1c  90 73 25 c6 92 71 dd f0 |989:.....s%..q..|
00000020  c9 44 bc 72 ff ff ff ff  7c 1e 1e 1f 7c 52 65 6d |.D.r....|...|Rem|
00000030  6f 74 65 48 6f 73 74 7c  1e 1e 1f 7c 31 7c 1e 1e |oteHost|...|1|..|
00000040  1f 7c 01 7c 1e 1e 1f 7c  00 7c 1e 1e 1f 7c 00 7c |.|.|...|.|...|.||
00000050  1e 1e 1f 7c 00 7c 1e 1e  1f 7c 00 7c 1e 1e 1f 7c |...|.|...|.|...||
00000060  00 7c 1e 1e 1f 7c 36 7c  1e 1e 1f 7c 77 00 6c 00 |.|...|6|...|w.l.|
00000070  6e 00 6e 00 69 00 74 00  2e 00 65 00 78 00 65 00 |n.n.i.t...e.x.e.|
00000080  7c 1e 1e 1f 7c 77 00 69  00 6e 00 7c 1e 1e 1f 7c ||...|w.i.n.|...||
00000090  00 7c 1e 1e 1f 7c 30 7c  1e 1e 1f 7c 52 65 6d 63 |.|...|0|...|Remc|
000000a0  6f 73 2d 51 4b 55 51 31  5a 7c 1e 1e 1f 7c 30 7c |os-QKUQ1Z|...|0||
000000b0  1e 1e 1f 7c 36 7c 1e 1e  1f 7c 6c 00 6f 00 67 00 |...|6|...|l.o.g.|
000000c0  73 00 2e 00 64 00 61 00  74 00 7c 1e 1e 1f 7c 00 |s...d.a.t.|...|.|
000000d0  7c 1e 1e 1f 7c 00 7c 1e  1e 1f 7c 00 7c 1e 1e 1f ||...|.|...|.|...|
000000e0  7c 31 30 7c 1e 1e 1f 7c  00 7c 1e 1e 1f 7c 77 69 ||10|...|.|...|wi|
000000f0  6b 69 70 65 64 69 61 3b  73 6f 6c 69 74 61 69 72 |kipedia;solitair|
00000100  65 3b 7c 1e 1e 1f 7c 35  7c 1e 1e 1f 7c 36 7c 1e |e;|...|5|...|6|.|
00000110  1e 1f 7c 53 63 72 65 65  6e 73 68 6f 74 73 7c 1e |..|Screenshots|.|
00000120  1e 1f 7c 00 7c 1e 1e 1f  7c 00 7c 1e 1e 1f 7c 00 |..|.|...|.|...|.|
00000130  7c 1e 1e 1f 7c 00 7c 1e  1e 1f 7c 00 7c 1e 1e 1f ||...|.|...|.|...|
00000140  7c 00 7c 1e 1e 1f 7c 00  7c 1e 1e 1f 7c 00 7c 1e ||.|...|.|...|.|.|
00000150  1e 1f 7c 00 7c 1e 1e 1f  7c 35 7c 1e 1e 1f 7c 36 |..|.|...|5|...|6|
00000160  7c 1e 1e 1f 7c 4d 69 63  52 65 63 6f 72 64 73 7c ||...|MicRecords||
00000170  1e 1e 1f 7c 00 7c 1e 1e  1f 7c 30 7c 1e 1e 1f 7c |...|.|...|0|...||
00000180  30 7c 1e 1e 1f 7c 7c 1e  1e 1f 7c 00 7c 1e 1e 1f |0|...||...|.|...|
00000190  7c 01 7c 1e 1e 1f 7c 30  7c 1e 1e 1f 7c 00 7c 1e ||.|...|0|...|.|.|
000001a0  1e 1f 7c 31 7c 1e 1e 1f  7c 52 00 65 00 6d 00 63 |..|1|...|R.e.m.c|
000001b0  00 6f 00 73 00 7c 1e 1e  1f 7c 72 00 65 00 6d 00 |.o.s.|...|r.e.m.|
000001c0  63 00 6f 00 73 00 7c 1e  1e 1f 7c 00 7c 1e 1e 1f |c.o.s.|...|.|...|
000001d0  7c 00 7c 1e 1e 1f 7c 31  35 42 37 36 39 33 36 35 ||.|...|15B769365|
000001e0  36 42 39 35 43 34 46 39  37 41 46 45 45 41 45 42 |6B95C4F97AFEEAEB|
000001f0  41 39 37 43 30 42 33 7c  1e 1e 1f 7c 00 7c 1e 1e |A97C0B3|...|.|..|
00000200  1f 7c 31 30 30 30 30 7c  1e 1e 1f 7c 00          |.|10000|...|.   |


###### Values ######

[#] 185.244.26.209:1989:s%qDr
[#] RemoteHost
[#] 1
[#] 6
[#] wlnnit.exe
[#] win
[#] 0
[#] Remcos-QKUQ1Z
[#] 0
[#] 6
[#] logs.dat
[#] 10
[#] wikipedia;solitaire;
[#] 5
[#] 6
[#] Screenshots
[#] 5
[#] 6
[#] MicRecords
[#] 0
[#] 0
```