

Anno Accademico 2018/2019



Analisi Malware

Sample2.exe

Candidati:

Riccardo Astolfi

Giacomo Ferro

Francesco Gobbi

Fasi del progetto

1 - Analisi Statica

L'analisi statica consiste nel verificare proprietà semantiche di un programma stabilendo quali sono verificate o meno

2 - Analisi Dinamica

L'analisi dinamica consiste nell'osservare le funzionalità del file in esame dal “vivo”. Di solito l'analisi dinamica viene eseguita dopo quella statica. Si segue questo schema perché una stringa eseguibile in analisi statica potrebbe essere non eseguita dal programma stesso

3 - Reverse Engineering

Il Reverse Engineering è una tecnica per decomporre un oggetto, capirne il funzionamento, analizzandone a fondo il codice macchina che crea il sorgente del linguaggio originale

4 - Conclusioni

1 - Analisi Statica

Per l'analisi statica abbiamo usato dei tool già presenti nella macchina Windows.ova, ovvero:

- *PEStudio*

- *PEID*

- *VirusTotal (database online per i virus)*

1 - Analisi Statica (PEStudio)

pestudio 8.70 - Malware Initial Assessment - www.winitor.com

File Help

INTRO

c:\users\malware\desktop\sampl

- indicators (5/26)
- virusotal (network error)
- dos-stub (!This program cann
- file-header (Aug.2001)
- optional-header (GUI)
- directories (5)
- sections (self-modifying)
- libraries (6)
- imports (132/0/21)
- exports (0)
- tls-callbacks (n/a)
- resources (26)
- strings (38/23/3/14499)
- debug (Aug.2001)
- manifest (missing Trust Info)
- version (CALC.EXE)
- certificate (n/a)
- overlay (n/a)

property	value
md5	F83C765FB553146712FCF2C6066670B5
sha1	A6B849E7A8312F5D7E3D7C96501887F39E3BE512
sha256	34558AC38FAB17CA1A1FF70860B35296395F1DF7FA8D86B39C56FAECF9C3CFFC
first-bytes (hex)	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
first-bytes (text)	M Z @
size	626688 bytes
entropy	7.189
imphash	08F6A1B121DA8CEDDE2D1089D0906ED8
cpu	32-bit
signature	n/a
entry-point (hex)	50 90 51 52 90 53 90 54 55 56 57 55 89 E5 83 EC 7C
file-version	5.1.2600.0 (xpdient.010817-1148)
file-description	Windows Calculator application file
file-type	executable
subsystem	GUI
compiler-stamp	Fri Aug 17 21:52:32 2001
debugger-stamp	Fri Aug 17 21:52:32 2001

Hash del virus

Entropia

Architettura del software

Ulteriori informazioni
di base sul virus

pestudio 8.70 - Malware Initial Assessment - www.winitor.com

File Help

MANIFESTO

c:\users\malware\desktop\sampl

- indicators (5/26)
- virusotal (network error)
- dos-stub (!This program cann
- file-header (Aug.2001)
- optional-header (GUI)
- directories (5)
- sections (self-modifying)
- libraries (6)
- imports (132/0/21)
- exports (0)
- tls-callbacks (n/a)
- resources (26)
- strings (38/23/3/14499)
- debug (Aug.2001)
- manifest (missing Trust Info)
- version (CALC.EXE)
- certificate (n/a)
- overlay (n/a)

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
  <assemblyIdentity
    name="Microsoft.Windows.Shell.calc"
    processorArchitecture="x86"
    version="5.1.0.0"
    type="win32"/>
  <description>Windows Shell</description>
  <dependency>
    <dependentAssembly>
      <assemblyIdentity
        type="win32"
        name="Microsoft.Windows.Common-Controls"
        version="6.0.0.0"
        processorArchitecture="x86"
        publicKeyToken="6595b64144ccf1df"
        language="**"
      />
    </dependentAssembly>
  </dependency>
</assembly>
```

1 - Analisi Statica (PEStudio)

pestudio 8.70 - Malware Initial Assessment - www.winitor.com

File Help

VERSION

c:\users\malware\desktop\sampl

- indicators (5/26)
- virustotal (network error)
- dos-stub (!This program cann
- file-header (Aug.2001)
- optional-header (GUI)
- directories (5)
- sections (self-modifying)
- libraries (6)
- imports (132/0/21)
- exports (0)
- tls-callbacks (n/a)
- resources (26)
- strings (38/23/3/14499)
- debug (Aug.2001)
- manifest (missing Trust Info)
- version (CALC.EXE)**
- certificate (n/a)
- overlay (n/a)

property	value
file-type	executable
date	n/a
language	english United States
code-page	Unicode UTF-16, little endian
CompanyName	Microsoft Corporation
FileDescription	Windows Calculator application file
FileVersion	5.1.2600.0 (xpcient.010817-1148)
InternalName	CALC
LegalCopyright	© Microsoft Corporation. All rights reserved.
OriginalFilename	CALC.EXE
ProductName	Microsoft® Windows® Operating System
ProductVersion	5.1.2600.0

*Ulteriori informazioni
di base sul virus*

Indicatori: componente o
caratteristica del software.

*In rosso le componenti più
sospette*

pestudio 8.70 - Malware Initial Assessment - www.winitor.com

File Help

INDICATORI

c:\users\malware\desktop\samples\other\sample2.e

- indicators (5/26)
- virustotal (offline)
- dos-stub (!This program cannot be run in DOS m
- file-header (Aug.2001)
- optional-header (GUI)
- directories (5)
- sections (self-modifying)
- libraries (6)
- imports (132/0/21)
- exports (0)
- tls-callbacks (n/a)
- resources (26)
- strings (38/23/3/14499)
- debug (Aug.2001)
- manifest (missing Trust Info)
- version (CALC.EXE)**
- certificate (n/a)
- overlay (n/a)

indicator (26)	severity
The file references the Clipboard	1
The section (name:.vmp0) is blacklisted	1
The last section (name:.vmp0) is executable	1
The file has (1) writable and executable section(s)	1
The file contains self-modifying code	1
The file references the Desktop window	2
The file references the Event Log	2
The file references the HTML Help Control	2
The file references (38) blacklisted string(s)	2
The file imports (21) blacklisted function(s)	2
The file references (2) rtti string(s)	3
The file references the Registry API	5
The file references the Memory Management API	5
The file references the Clipboard API	5
The file references the Dynamic-Link Library API	5
The file references the Process and Thread API	5
The file imports (3) decorated function(s)	5
The file imports (1) undocumented function(s)	5
The file does not contain a digital Certificate	7
The file references (3) whitelist strings	9
The file ignores Data Execution Prevention (DEP)	9
The file ignores Address Space Layout Randomization (ASLR)	9
The manifest identity name is "Microsoft.Windows.Shell.calc"	9
The file references a debug symbols file (path:"calc.pdb")	9
The file ignores cookies on the stack (GS)	9
The file ignores Code Integrity	9

1 - Analisa Statica (PEStudio)

pestudio 8.70 - Malware Initial Assessment - www.winitor.com

File Help

c:\users\malware\Desktop\samples\other\samp

indicators (5/26)

virusotal (network error)

dos-stub (!This program cannot be run in D

file-header (Aug. 2001)

optional-header (GUI)

directories (5)

sections (self-modifying)

libraries (6)

imports (132/0/21)

exports (0)

tls-callbacks (n/a)

resources (26)

strings (38/23/3/14499)

debug (Aug. 2001)

manifest (missing Trust Info)

version (CALC.EXE)

certificate (n/a)

overlay (n/a)

SEZIONI

property	value	value	value	value
name	.text	.data	.rsrc	.vmp0
md5	179745C927697911BAA6...	8E8381392A4F163121AB...	86CBAEA46AB7F1C62572...	5FC458D95F5306F811C5.
file-ratio (99.84 %)	12.09 %	0.41 %	5.64 %	81.70 %
virtual-size (1843244 bytes)	75440 bytes	4124 bytes	35168 bytes	1728512 bytes
virtual-address	0x00001000	0x00014000	0x00016000	0x0001F000
raw-size (625664 bytes)	75776 bytes	2560 bytes	35328 bytes	512000 bytes
raw-address	0x00000400	0x00012C00	0x00013600	0x0001C000
cave (496 bytes)	336 bytes	0 bytes	160 bytes	0 bytes
entropy	6.195	3.587	4.984	7.107
entry-point (0x00012475)	x	-	-	-
blacklisted	-	-	-	x
writable	-	x	-	x
executable	x	-	-	x
shareable	-	-	-	-
discardable	-	-	-	-
cacheable	x	x	x	x
pageable	x	x	x	x
initialized-data	-	x	x	-
uninitialized-data	-	-	-	-
readable	x	x	x	x

***In rosso sono
indicate le sezioni
presenti nel virus.
La sezione .vmp0 è la
sezione malevola,
infatti è anche nella
blacklist***

LIBRERIE

library (6)	blacklist (0)	missing (0)	type	imports (132)	file-description
shell32.dll	-	-	Implicit	1	Windows Shell Common Dll
msvcrt.dll	-	-	Implicit	26	Windows NT CRT DLL
advapi32.dll	-	-	Implicit	3	Advanced Windows 32 Base API
kernel32.dll	-	-	Implicit	30	Windows NT BASE API Client DLL
gdi32.dll	-	-	Implicit	3	GDI Client DLL
user32.dll	-	-	Implicit	69	Multi-User Windows USER API Client DLL

Numero di import per ogni libreria

**Sono
mostrate le
librerie
importate
dal virus**

**Numero di import
per ogni libreria**

1 - Analisi Statica (PEStudio)

pestudio 8.70 - Malware Initial Assessment - www.winator.com

File Help

STRINGHE

c:\users\malware\desktop\samples\other\samp

indicators (5/26)

virustotal (network error)

dos-stub (This program cannot be run in D

file-header (Aug.2001)

optional-header (GUI)

directories (5)

sections (self-modifying)

libraries (6)

imports (132/0/21)

exports (0)

tls-callbacks (n/a)

resources (26)

strings (38/23/3/14499)

debug (Aug.2001)

manifest (missing Trust Info)

version (CALC.EXE)

certificate (n/a)

overlay (n/a)

type	size	location	blacklist (38)	hint (23)	whitelist (3)	value (14499)
ascii	10	0x0000...	x	-	-	hhctrl.ocx
ascii	11	.text:0...	x	-	-	RegCloseKey
ascii	15	.text:0...	x	-	-	RegQueryValueEx
ascii	12	.text:0...	x	-	-	RegOpenKeyEx
ascii	14	.text:0...	x	-	-	GetCommandLine
ascii	10	.text:0...	x	-	-	LocalAlloc
ascii	16	.text:0...	x	-	-	GetProfileString
ascii	13	.text:0...	x	-	-	GetProfileInt
ascii	12	.text:0...	x	-	-	LocalReAlloc
ascii	8	.text:0...	x	-	-	SetEvent
ascii	10	.text:0...	x	-	-	ResetEvent
ascii	12	.text:0...	x	-	-	CreateThread
ascii	12	.text:0...	x	-	-	GlobalUnlock
ascii	10	.text:0...	x	-	-	GlobalSize
ascii	10	.text:0...	x	-	-	GlobalLock
ascii	18	.text:0...	x	-	-	WriteProfileString
ascii	5	.text:0...	x	-	-	Sleep
ascii	13	.text:0...	x	-	-	GlobalReAlloc
ascii	10	.text:0...	x	-	-	GlobalFree
ascii	11	.text:0...	x	-	-	GlobalAlloc
ascii	13	.text:0...	x	-	-	GlobalCompact
ascii	14	.text:0...	x	-	-	GetProcAddress
ascii	11	.text:0...	x	-	-	LoadLibrary
ascii	15	.text:0...	x	-	-	GetModuleHandle
ascii	14	.text:0...	x	-	-	GetStartupInfo
ascii	11	.text:0...	x	-	-	SendMessage
ascii	13	.text:0...	x	-	-	SetWindowLong
ascii	20	.text:0...	x	-	-	SystemParametersInfo
ascii	14	.text:0...	x	-	-	CloseClipboard
ascii	16	.text:0...	x	-	-	GetClipboardData
ascii	13	.text:0...	x	-	-	OpenClipboard
ascii	16	.text:0...	x	-	-	
ascii	26	.text:0...	x	-	-	
ascii	15	.text:0...	x	-	-	
ascii	7	.text:0...	x	-	-	
ascii	14	.text:0...	x	-	-	
unicode	15	.rsrc:0...	x	-	-	
unicode	11	.rsrc:0...	x	-	-	
ascii	40	0x0000...	-	x	-	

sha256: 34558AC38FAB17CA1A1FF70860B35296395F1DF7FA8D86B39C56FAECF9C3CFFC | cpu: 32-bit | file-type: executable

Qui sono presenti tutte le stringhe, ovvero le chiamate a funzione eseguite e rispetto alla libreria di provenienza. Le prime stringhe sono quelle malevole, che il tool inserisce nella blacklist

Qui invece sono presenti le stringhe offuscate, ovvero le stringhe non in chiaro e su cui sono stati usati dei tool di compressione per ridurre la ridondanza statistica

pestudio 8.70 - Malware Initial Assessment - www.winator.com

File Help

STRINGHE OFFUSCATE

c:\users\malware\desktop\samples\other\samp

indicators (5/26)

virustotal (network error)

dos-stub (This program cannot be run in D

file-header (Aug.2001)

optional-header (GUI)

directories (5)

sections (self-modifying)

libraries (6)

imports (132/0/21)

exports (0)

tls-callbacks (n/a)

resources (26)

strings (38/23/3/14499)

debug (Aug.2001)

manifest (missing Trust Info)

version (CALC.EXE)

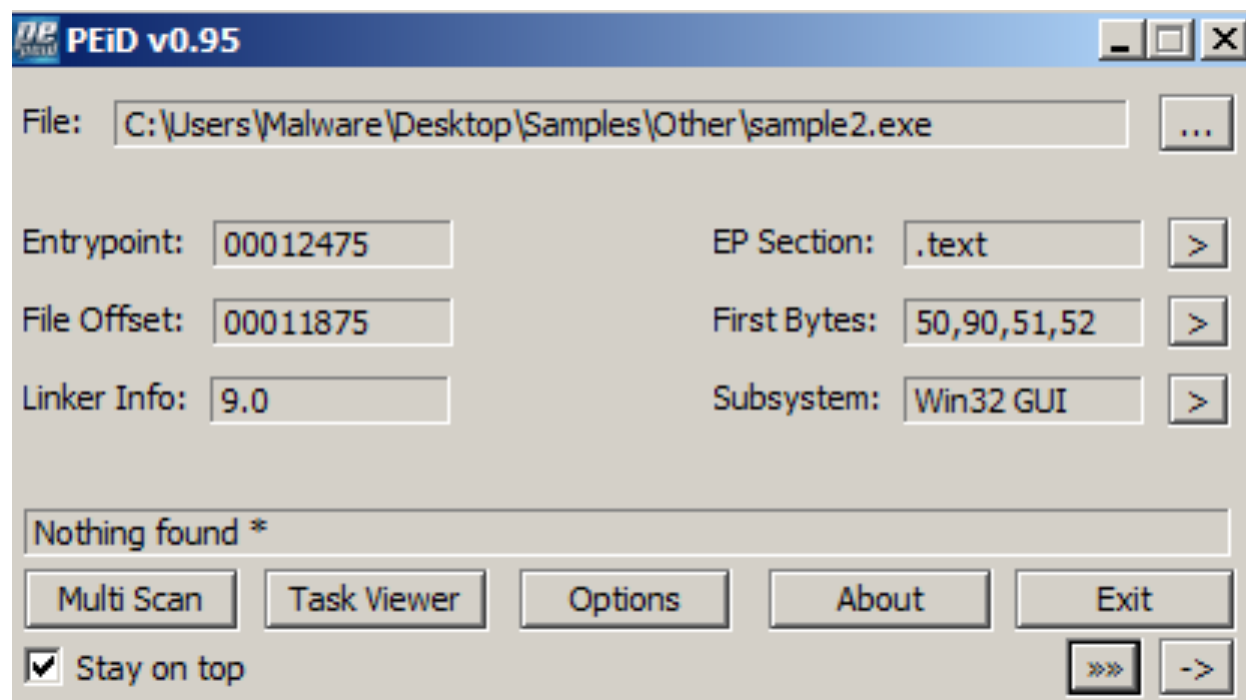
certificate (n/a)

overlay (n/a)

type	size	location	blacklist (38)	hint (23)	whitelist (3)	value (14499)
ascii	4	0x0000008D	-	-	-	\$x79
ascii	8	0x000000A9	-	-	-	\$y7D\$x79
ascii	4	0x000000B5	-	-	-	\$x7T
ascii	4	0x000000C5	-	-	-	\$x79
ascii	7	0x000000CD	-	-	-	\$x7Rich
ascii	5	0x000001E8	-	-	-	.text
ascii	6	0x0000020F	-	-	-	.data
ascii	5	0x00000238	-	x	-	.rsrc
ascii	6	0x0000025F	-	-	-	@.vmp0
ascii	11	0x000002C0	-	-	-	SHELL32.dll
ascii	10	0x000002CC	-	-	-	msvrt.dll
ascii	12	0x000002D7	-	-	-	ADVAPI32.dll
ascii	12	0x000002E4	-	-	-	KERNEL32.dll
ascii	9	0x000002F1	-	-	-	GDI32.dll
ascii	10	0x000002FB	-	-	-	USER32.dll
ascii	59	0x000009A0	-	x	-	CLSID_{ADB880A6-D8FF-11CF-9377-00AA003B7A11}\InprocServer32
ascii	4	0x00000A0C	-	-	-	NB10
ascii	8	0x00000A1C	-	x	-	calc.pdb
ascii	4	0x00000AA1	-	-	-	t f
ascii	4	0x00000C4D	-	-	-	SVWh
ascii	4	0x00000EFC	-	-	-	QPJB
ascii	4	0x00000F77	-	-	-	9=HM
ascii	7	0x00000F83	-	-	-	WWWTrjf
ascii	4	0x00001072	-	-	-	~{h
ascii	4	.text:00001147	-	-	-	9=HM
ascii	4	.text:00001190	-	-	-	9=HM
ascii	4	.text:00001367	-	-	-	j1Y3
ascii	4	.text:0000145D	-	-	-	uPQQ
ascii	4	.text:000014DA	-	-	-	PQPh
ascii	4	.text:0000162D	-	-	-	SVW3
ascii	4	.text:000016F2	-	-	-	_ ^[]
ascii	4	.text:00001B0D	-	-	-	{vD;
ascii	4	.text:00001BEC	-	-	-	ywP9
ascii	4	.text:0000238E	-	-	-	NYYN
ascii	4	.text:00002398	-	-	-	Nt(N
ascii	4	.text:000025B2	-	-	-	u`Sh
ascii	4	.text:0000363D	-	-	-	t+Ht
ascii	4	.text:00003837	-	-	-	_ ^[3

sha256: 34558AC38FAB17CA1A1FF70860B35296395F1DF7FA8D86B39C56FAECF9C3CFFC | cpu: 32-bit | file-type: executable | subsystem: GUI | entry-point: 0x00012475 | signature: n/a

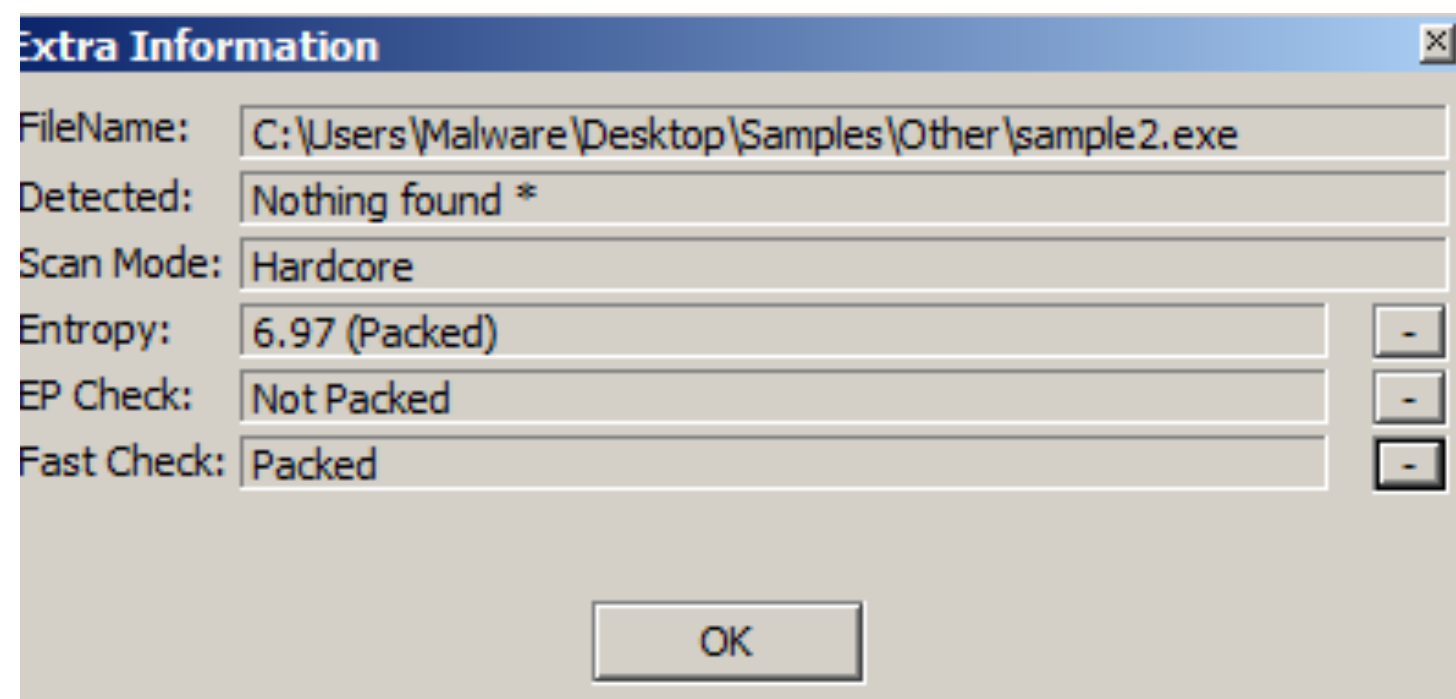
1 - Analisi Statica (PEID)



*Interfaccia grafica di PEID.
PEID analizza il file e vede se è
packed o meno*

Risultato dell'analisi in "Hardcore Mode" di PEID che identifica "non packed" il virus.

Dall'analisi, invece, in "Normal Mode" PEID fa un'analisi più grossolana del file e lo dichiara "Packed".



1 - Analisi Statica (VirusTotal)

Score del virus

55 / 66

55 engines detected this file

34558ac3bfab17ca1a1ff70860b35296395f1df7fa8d86b39c56faecf9c3cffc

CALC

612 KB Size

2019-07-09 11:52:35 UTC 2 months ago

Community Score

DETECTION DETAILS BEHAVIOR COMMUNITY 1

Basic Properties

MD5	f83c765fb553146712fc2c6066670b5
SHA-1	a6b849e7a8312f5d7e3d7c96501887f39e3be512
SHA-256	34558ac3bfab17ca1a1ff70860b35296395f1df7fa8d86b39c56faecf9c3cffc
Authentihash	3bf37c832e8b480b2db81d04611aafddcf1fa7cc2e30b276c7c33fb9eed25e1
Imphash	08f6a1b121da8cedde2d1089d0906ed8
SSDEEP	12288:3SIhduItV9wgtW//fxoVg4p1v0R9MeYQZwctBr:CGDtG/faBvKYyBr
File type	Win32 EXE
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
File size	612 KB (626688 bytes)

History

Creation Time	2001-08-17 20:52:32
First Submission	2016-12-06 02:47:35
Last Submission	2017-12-09 16:45:02
Last Analysis	2019-07-09 11:52:35

Risultato di VirusTotal inserendo l'hash md5.

Qui, ovviamente vengono ripetute le informazioni che sono già state trovate dal tool PESTudio

Anche VirusTotal trova le sezioni del file, i suoi import, la dati di creazione e altro

Portable Executable Info

Header

Target Machine	Intel 386 or later processors and compatible processors
Compilation Timestamp	2001-08-17 20:52:32
Entry Point	74869
Contained Sections	4

Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5
.text	4096	75440	75776	6.2	179745c927697911baa61a2d3981ca9b
.data	81920	4124	2560	3.59	8e8381392a4f163121ab9e1cfbe54486
.rsrc	90112	35168	35328	4.98	86cbaea46ab7f1c625724785d76254f6
.vmp0	126976	1728512	512000	7.11	5fc458d95f5306f811c5b8b76b8a4067

Imports

+	ADVAPI32.dll
+	GDI32.dll
+	KERNEL32.dll
+	SHELL32.dll
+	USER32.dll
+	msvcrt.dll

1 - Analisi Statica (VirusTotal)

Files Written

c:\windows\microsoft.net\framework\v2.0.50727\aspnet_state.vir
c:\windows\system32\cisvc.vir
c:\windows\system32\clipsrv.vir
c:\windows\system32\dmadmin.vir
c:\windows\microsoft.net\framework\v3.0\windows communication foundation\infocard.vir
c:\windows\system32\netdde.vir
c:\windows\system32\locator.vir
c:\windows\system32\smlogsvc.vir
c:\windows\system32\tlntsvr.vir
C:\WINDOWS\system32\magnify.vir



Files Deleted

c:\windows\microsoft.net\framework\v2.0.50727\aspnet_state.vir
c:\windows\system32\cisvc.vir
c:\windows\system32\clipsrv.vir
c:\windows\system32\dmadmin.vir
c:\windows\microsoft.net\framework\v3.0\windows communication foundation\infocard.vir
c:\windows\system32\msiexec.vir
c:\windows\system32\netdde.vir
c:\windows\system32\locator.vir
c:\windows\system32\smlogsvc.vir
c:\windows\system32\tlntsvr.vir



Files Copied

— c:\windows\microsoft.net\framework\v2.0.50727\aspnet_state.vir
| c:\windows\microsoft.net\framework\v2.0.50727\aspnet_state.exe
+ c:\windows\system32\cisvc.vir

VirusTotal mostra anche i file che vengono modificati, quelli copiati e quelli eliminati.



VirusTotal indica anche i vari anti-virus che lo hanno riconosciuto.

DETECTION	DETAILS	BEHAVIOR	COMMUNITY
Acronis		Suspicious	Ad-Aware Win32.Expiro.Gen.2
AegisLab		Virus.Win32.Expiro.nlc	AhnLab-V3 Win32/Expiro4.Gen
Alibaba		Virus:Win32/Expiro.4cbc616e	ALYac Win32.Expiro.Gen.2
Antiy-AVL		Virus/Win32.Expiro.ao	SecureAge APEX Malicious
Arcabit		Win32.Expiro.Gen.2	Avast Win32:Xpirat
AVG		Win32:Xpirat	Avira (no cloud) W32/Expiro.caj
Baidu		Win32.Virus.Expiro.a	BitDefender Win32.Expiro.Gen.2
Bkav		W32.Expiro1NHc.PE	CAT-QuickHeal W32.Expiro.AX
CMC		Virus.Win32.Expiro!O	Comodo Virus.Win32.Expiro.isn@42
CrowdStrike Falcon		Win/malicious_confidence_100% (D)	Cybereason Malicious.fb5531
Cylance		Unsafe	Cyren W32/Expiro.AP
DrWeb		Win32.Expiro.56	Emsisoft Win32.Expiro.Gen.2 (B)
Endgame		Malicious (high Confidence)	eScan Win32.Expiro.Gen.2
ESET-NOD32		Win32/Expiro.NBF	F-Prot W32/Expiro.AP
F-Secure		Malware.W32/Expiro.caj	FireEye Generic.mg.f83c765fb5531

1 - Analisi Statica (Conclusioni)

A questo punto dell'analisi siamo riusciti comprendere meglio alcune sue caratteristiche:

- *Si tratti di un virus di tipologia **Expiro**, che cerca sostanzialmente di prelevare dati dalla macchina ed inviarli successivamente in rete*
- *Si tratta di un virus vecchio o comunque già per ben analizzato da altri utenti e bloccato da anti-virus, infatti è del **2001***
- *Ha un'**entropia elevata**, questo vuol dire che è stato offuscato*
- *Il virus **modifica diverse chiavi di registro e di file***
- *Il virus **infetta eseguibili** (comportamento polimorfico)*
- ***Crea connessione di rete** con l'esterno*

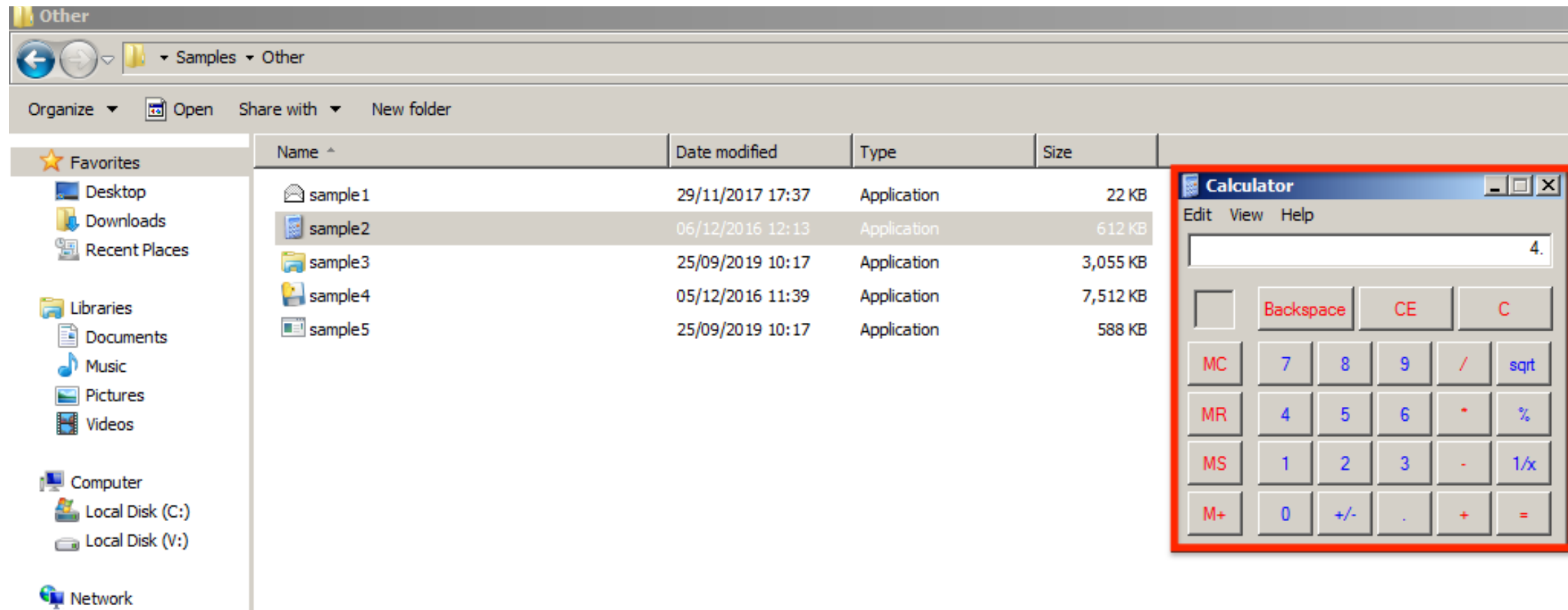
2 - Analisi Dinamica

Per l'analisi dinamica abbiamo usato altri tool già presenti nella macchina Windows.ova, ovvero:

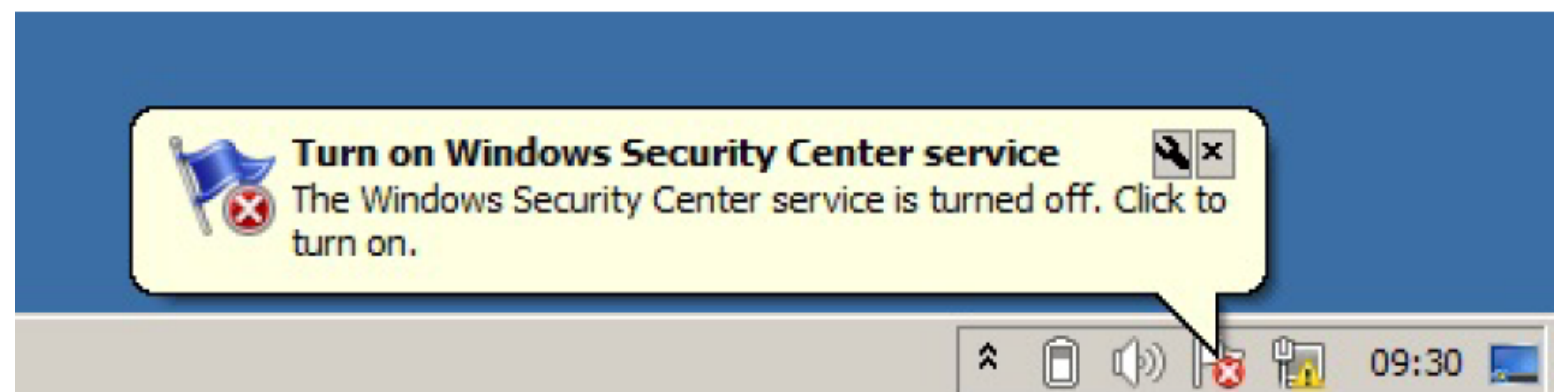
- *RegShot***
- *ProcMon***
- *FakeNet***
- *Wireshark***

2 - Analisi Dinamica (sample2.exe)

Durante l'esecuzione il virus si mostra come una calcolatrice con GUI di Windows

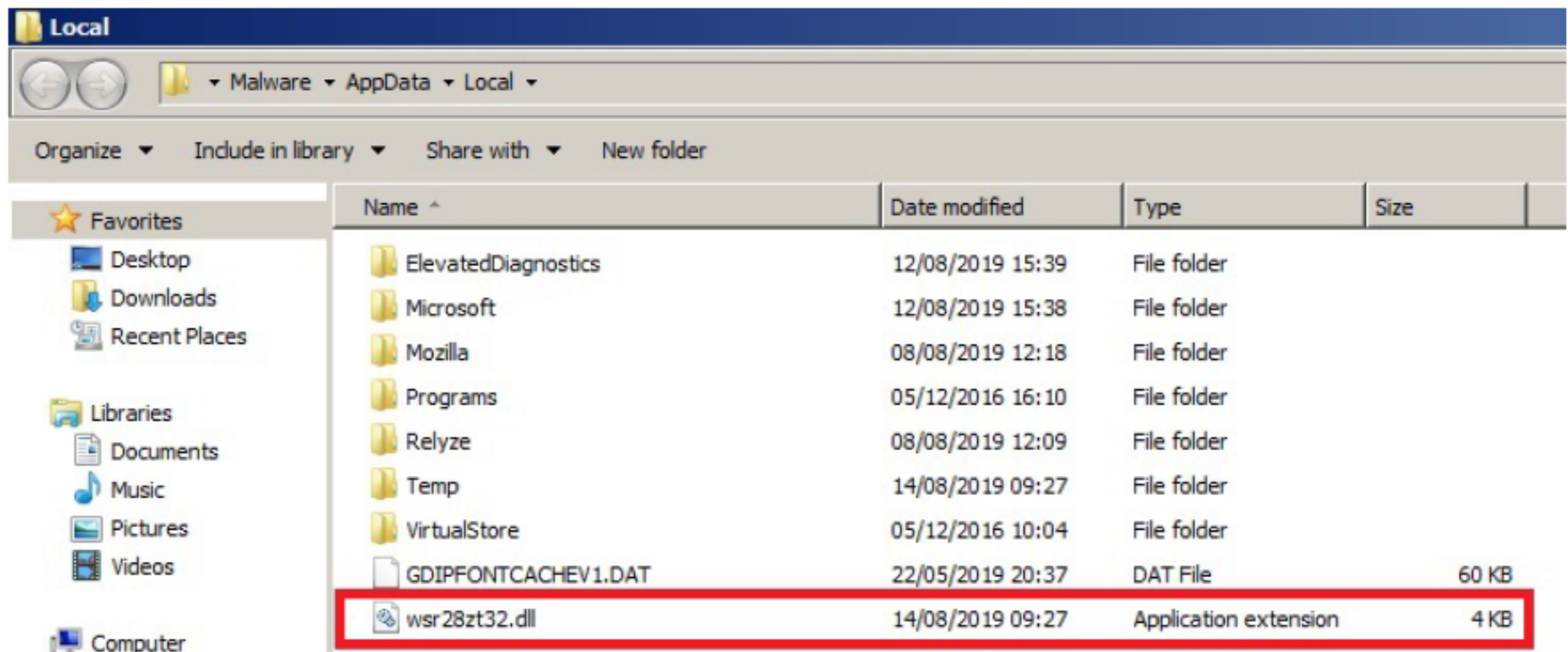


***Dopo un po' il virus disattiverà
"Windows Security Center",
abbassando di fatto la sicurezza
del sistema, oltre alla modifica
dei privilegi di esecuzione di
molti programmi***



2 - Analisi Dinamica (sample2.exe)

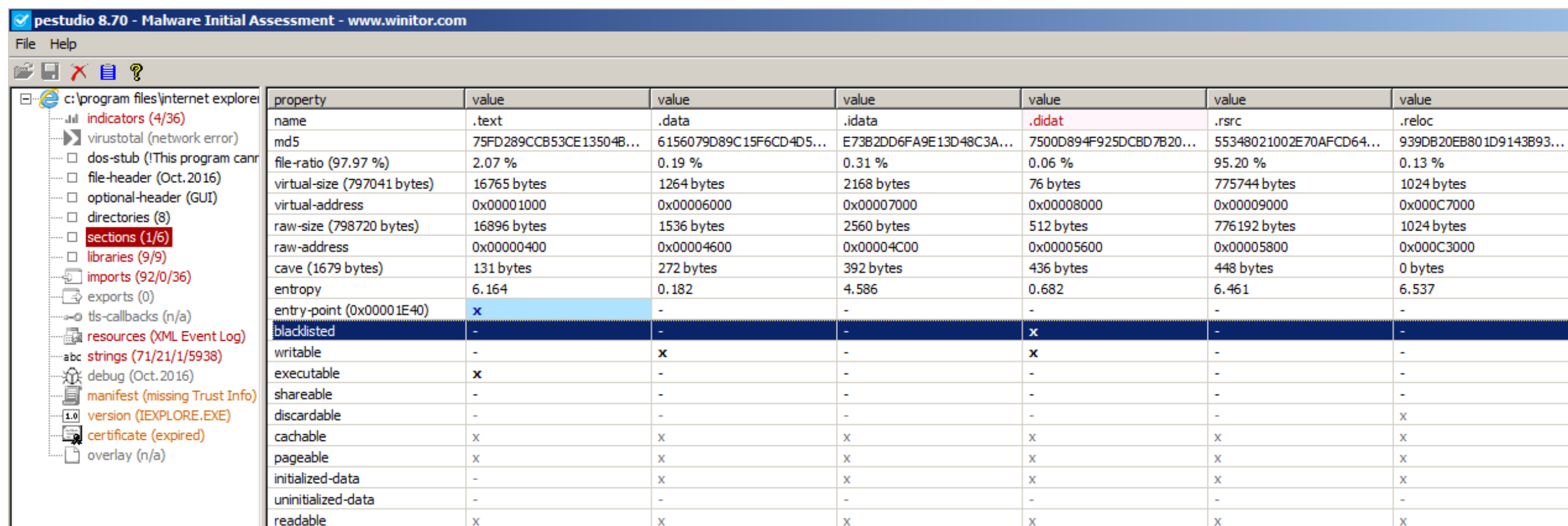
Dopo alcuni minuti si vede la creazione di questa nuova libreria, che contiene tutte le informazioni che il virus è riuscito a prendere dal pc infettato



Questa libreria “wsr28zt32.dll” è molto conosciuta e fa riferimento a virus di tipo Expiro

2 - Analisi Dinamica (Regshot e ProcMon)

L'utente non si accorge di nulla durante l'esecuzione del virus, infatti è possibile eseguire dei calcoli come una calcolatrice normale, mentre la sezione malevola infetta i vari eseguibili

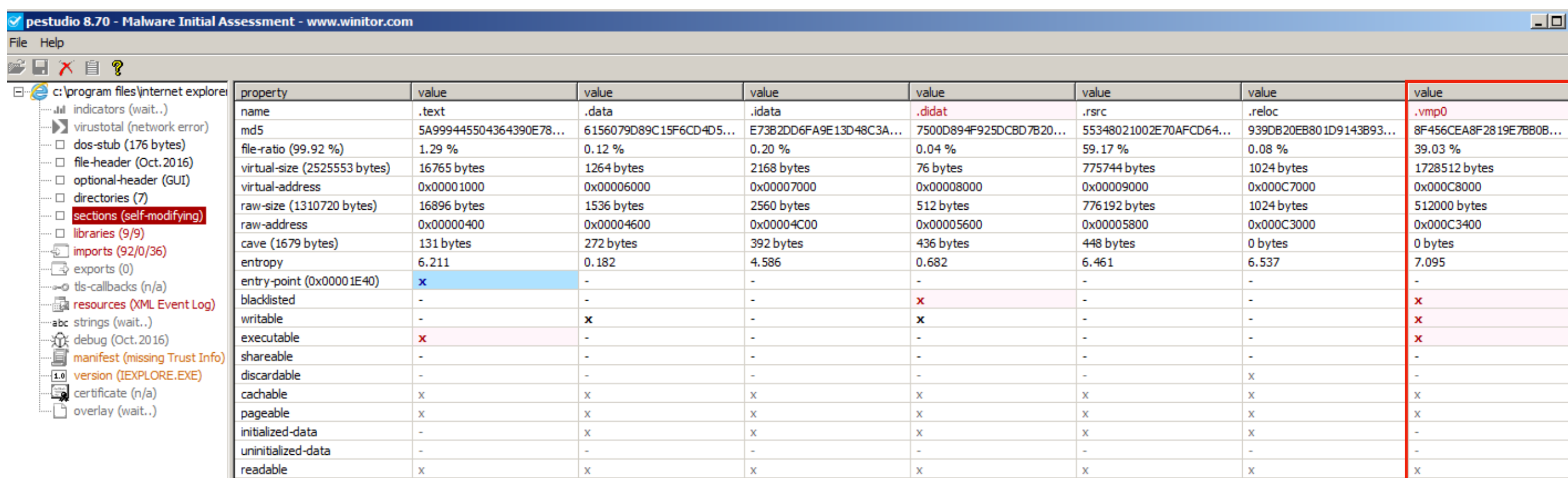


property	value	value	value	value	value	value
name	.text	.data	.idata	.didat	.rsrc	.reloc
md5	75FD289CCB53CE13504B...	6156079D89C15F6CD4D5...	E73B2DD6FA9E13D48C3A...	7500D894F925DCBD7B20...	55348021002E70AFCD64...	939DB20EB801D9143B93...
file-ratio (97.97 %)	2.07 %	0.19 %	0.31 %	0.06 %	95.20 %	0.13 %
virtual-size (797041 bytes)	16765 bytes	1264 bytes	2168 bytes	76 bytes	775744 bytes	1024 bytes
virtual-address	0x00001000	0x00006000	0x00007000	0x00008000	0x00009000	0x000C7000
raw-size (798720 bytes)	16896 bytes	1536 bytes	2560 bytes	512 bytes	776192 bytes	1024 bytes
raw-address	0x00000400	0x00004600	0x00004C00	0x00005600	0x00005800	0x000C3000
cave (1679 bytes)	131 bytes	272 bytes	392 bytes	436 bytes	448 bytes	0 bytes
entropy	6.164	0.182	4.586	0.682	6.461	6.537
entry-point (0x00001E40)	x	-	-	-	-	-
blacklisted	-	-	-	x	-	-
writable	-	x	-	x	-	-
executable	x	-	-	-	-	-
shareable	-	-	-	-	-	-
discardable	-	-	-	-	-	x
cacheable	x	x	x	x	x	x
pageable	x	x	x	x	x	x
initialized-data	-	x	x	x	x	x
uninitialized-data	-	-	-	-	-	-
readable	x	x	x	x	x	x

Sopra si vede l'esecuzione di PEStudio sull'eseguibile di Internet Explorer prima dell'infezione. Non sono presenti sezioni malevole.

2 - Analisi Dinamica (Regshot e ProcMon)

Sotto si vede l'analisi di PEStudio sull'eseguibile di Internet Explorer dopo l'infezione. Si vede infatti che è presente una nuova sezione, ovvero .vmp0



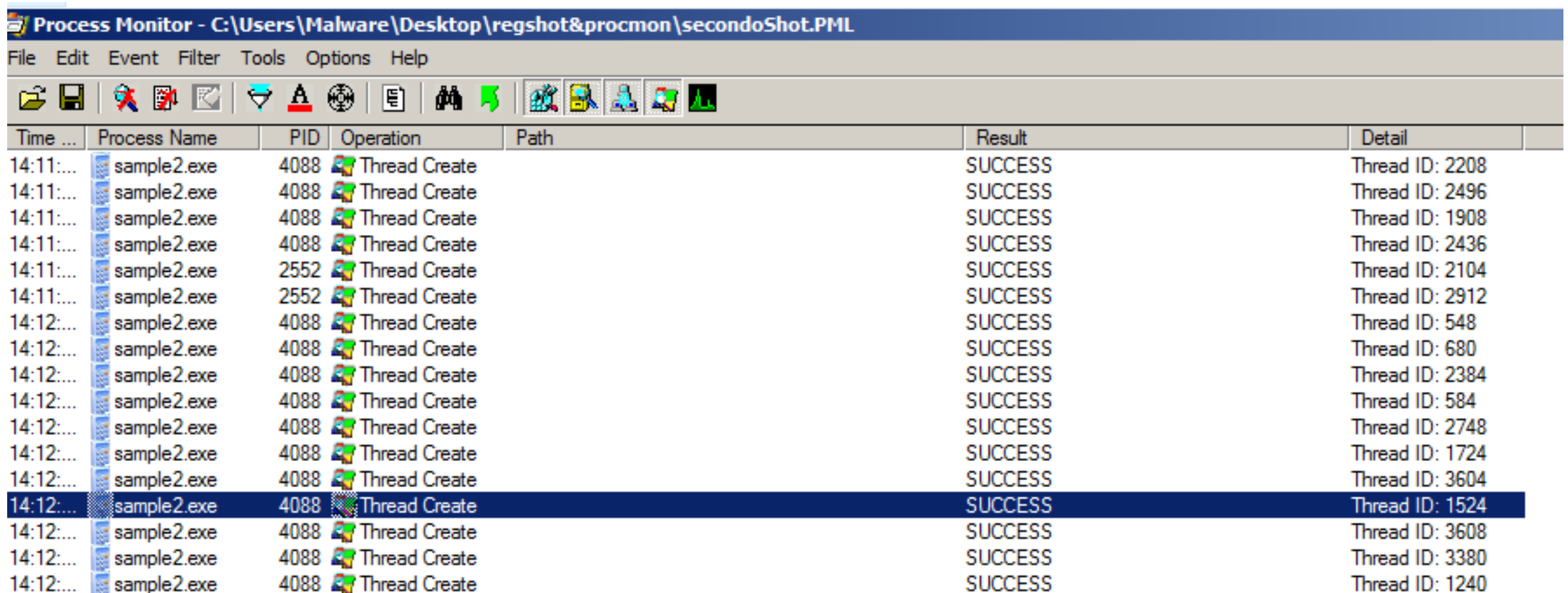
property	value	value	value	value	value	value	value
name	.text	.data	.idata	.didat	.rsrc	.reloc	.vmp0
md5	5A999445504364390E78...	6156079D89C15F6CD4D5...	E73B2DD6FA9E13D48C3A...	7500D894F925DCBD7B20...	55348021002E70AFCD64...	939DB20EB801D9143B93...	8F456CEA8F2819E7BB0B...
file-ratio (99.92 %)	1.29 %	0.12 %	0.20 %	0.04 %	59.17 %	0.08 %	39.03 %
virtual-size (2525553 bytes)	16765 bytes	1264 bytes	2168 bytes	76 bytes	775744 bytes	1024 bytes	1728512 bytes
virtual-address	0x00001000	0x00006000	0x00007000	0x00008000	0x00009000	0x000C7000	0x000C8000
raw-size (1310720 bytes)	16896 bytes	1536 bytes	2560 bytes	512 bytes	776192 bytes	1024 bytes	512000 bytes
raw-address	0x00000400	0x00004600	0x00004C00	0x00005600	0x00005800	0x000C3000	0x000C3400
cave (1679 bytes)	131 bytes	272 bytes	392 bytes	436 bytes	448 bytes	0 bytes	0 bytes
entropy	6.211	0.182	4.586	0.682	6.461	6.537	7.095
entry-point (0x00001E40)	x	-	-	-	-	-	-
blacklisted	-	-	-	x	-	-	x
writable	-	x	-	x	-	-	x
executable	x	-	-	-	-	-	x
shareable	-	-	-	-	-	-	-
discardable	-	-	-	-	-	x	-
cachable	x	x	x	x	x	x	x
pageable	x	x	x	x	x	x	x
initialized-data	-	x	x	x	x	x	-
uninitialized-data	-	-	-	-	-	-	-
readable	x	x	x	x	x	x	x

Questo ci dice che la sezione malevola è .vmp0 e che questa va ad aggiungersi al codice di tutti gli eseguibili, durante l'infezione del virus.

Gli eseguibili infettati presentano un lucchetto sull'icona del programma, che ne impedisce l'esecuzione

2 - Analisi Dinamica (Regshot e ProcMon)

Il virus è altamente infetto e genera molte copie di se stesso, con la replicazione binaria, causando un'elevata densità di thread nei processi di sistema


























The screenshot shows the Process Monitor application window. The title bar reads "Process Monitor - C:\Users\Malware\Desktop\regshot&procmon\secondoShot.PML". The menu bar includes "File", "Edit", "Event", "Filter", "Tools", "Options", and "Help". The toolbar contains various icons for file operations and monitoring. The main display area is a table with the following columns: "Time ...", "Process Name", "PID", "Operation", "Path", "Result", and "Detail". The table contains 18 rows of data, all showing "Thread Create" operations for "sample2.exe" with PID 4088. The "Result" column for all entries is "SUCCESS". The "Detail" column lists the "Thread ID" for each operation. The 14th row is highlighted in blue.

Time ...	Process Name	PID	Operation	Path	Result	Detail
14:11:...	sample2.exe	4088	Thread Create		SUCCESS	Thread ID: 2208
14:11:...	sample2.exe	4088	Thread Create		SUCCESS	Thread ID: 2496
14:11:...	sample2.exe	4088	Thread Create		SUCCESS	Thread ID: 1908
14:11:...	sample2.exe	4088	Thread Create		SUCCESS	Thread ID: 2436
14:11:...	sample2.exe	2552	Thread Create		SUCCESS	Thread ID: 2104
14:11:...	sample2.exe	2552	Thread Create		SUCCESS	Thread ID: 2912
14:12:...	sample2.exe	4088	Thread Create		SUCCESS	Thread ID: 548
14:12:...	sample2.exe	4088	Thread Create		SUCCESS	Thread ID: 680
14:12:...	sample2.exe	4088	Thread Create		SUCCESS	Thread ID: 2384
14:12:...	sample2.exe	4088	Thread Create		SUCCESS	Thread ID: 584
14:12:...	sample2.exe	4088	Thread Create		SUCCESS	Thread ID: 2748
14:12:...	sample2.exe	4088	Thread Create		SUCCESS	Thread ID: 1724
14:12:...	sample2.exe	4088	Thread Create		SUCCESS	Thread ID: 3604
14:12:...	sample2.exe	4088	Thread Create		SUCCESS	Thread ID: 1524
14:12:...	sample2.exe	4088	Thread Create		SUCCESS	Thread ID: 3608
14:12:...	sample2.exe	4088	Thread Create		SUCCESS	Thread ID: 3380
14:12:...	sample2.exe	4088	Thread Create		SUCCESS	Thread ID: 1240

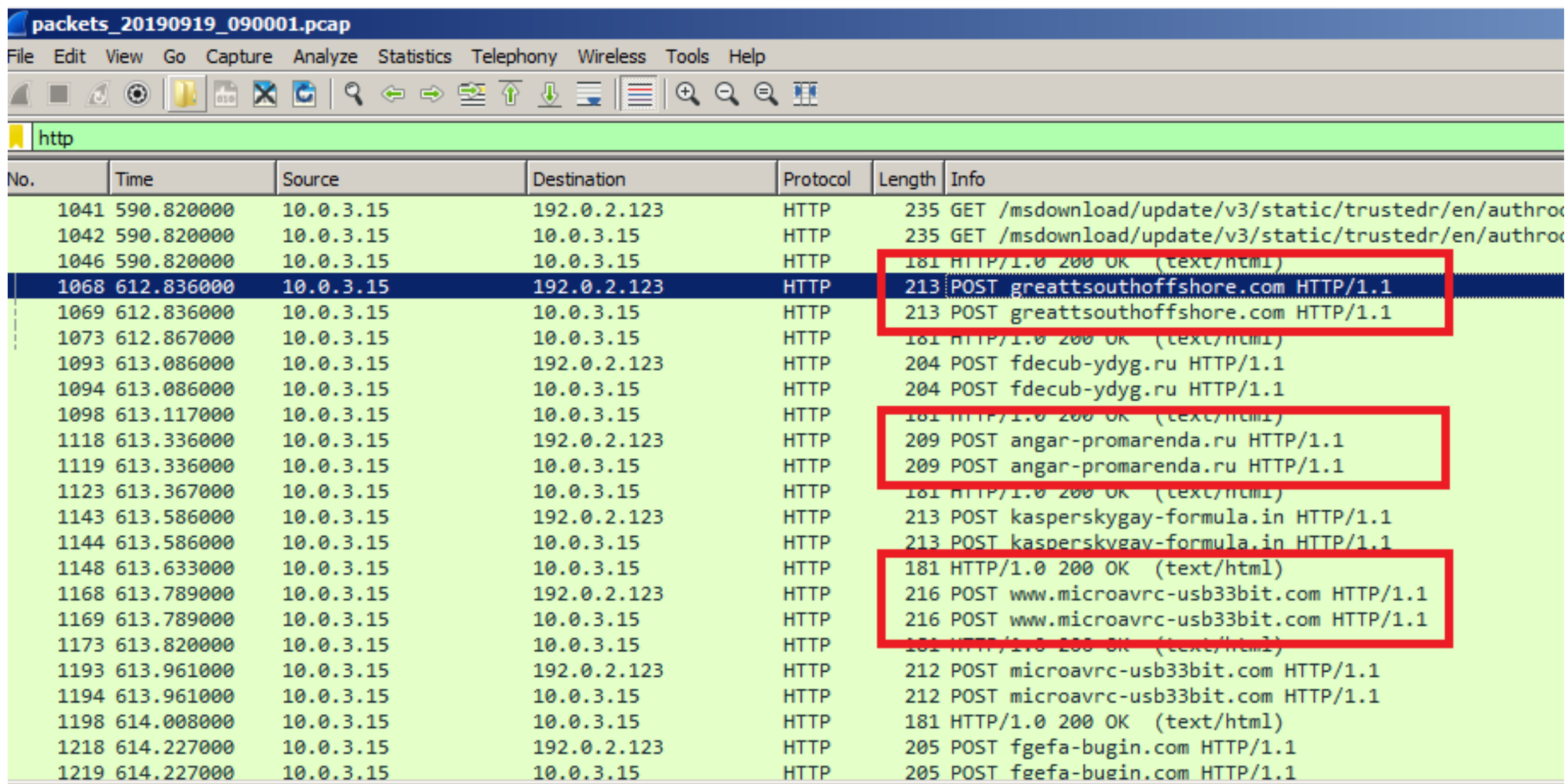
2 - Analisi Dinamica (FakeNet e Wireshark)

Il virus, dopo aver ricercato e salvato le informazioni da rubare, si connettere alla rete per passare queste informazioni a vari siti russi (ora irraggiungibili) instaurando delle connessioni HTTP. Sotto si vedono i file testuali con all'interno i vari URL dei siti

 listeners	28/11/2017 15:42	File folder	
 CHANGELOG	28/11/2017 15:42	Text Document	1 KB
 fakenet	28/11/2017 15:42	Application	6,852 KB
 fakenet.exe.manifest	28/11/2017 15:42	MANIFEST File	1 KB
 http_20190919_091342	19/09/2019 11:57	Text Document	1 KB
 http_20190919_091343	19/09/2019 11:57	Text Document	1 KB
 http_20190919_091344	19/09/2019 11:57	Text Document	1 KB
 http_20190919_091345	19/09/2019 11:57	Text Document	1 KB
 http_20190919_091346	19/09/2019 11:57	Text Document	1 KB
 http_20190919_091347	19/09/2019 11:57	Text Document	1 KB
 http_20190919_091348	19/09/2019 11:57	Text Document	1 KB
 http_20190919_091349	19/09/2019 11:57	Text Document	1 KB
 http_20190919_091351	19/09/2019 11:57	Text Document	1 KB
 http_20190919_091352	19/09/2019 11:57	Text Document	1 KB
 http_20190919_091353	19/09/2019 11:57	Text Document	1 KB
 http_20190919_091355	19/09/2019 11:57	Text Document	1 KB
 http_20190919_091356	19/09/2019 11:57	Text Document	1 KB
 http_20190919_091357	19/09/2019 11:57	Text Document	1 KB
 http_20190919_091358	19/09/2019 11:57	Text Document	1 KB
 http_20190919_091359	19/09/2019 11:57	Text Document	1 KB
 http_20190919_091400	19/09/2019 11:57	Text Document	1 KB
 http_20190919_091401	19/09/2019 11:57	Text Document	1 KB
 http_20190919_091402	19/09/2019 11:57	Text Document	1 KB

2 - Analisi Dinamica (FakeNet e Wireshark)

Con Wireshark si è analizzato il traffico di rete individuato le richieste ai siti sospetti, come quelli presenti in foto



The screenshot shows the Wireshark interface with a packet capture of HTTP traffic. The 'http' filter is applied. The following table represents the data visible in the packet list pane, with suspicious POST requests highlighted by red boxes in the original image.

No.	Time	Source	Destination	Protocol	Length	Info
1041	590.820000	10.0.3.15	192.0.2.123	HTTP	235	GET /msdownload/update/v3/static/trustedr/en/authroo
1042	590.820000	10.0.3.15	10.0.3.15	HTTP	235	GET /msdownload/update/v3/static/trustedr/en/authroo
1046	590.820000	10.0.3.15	10.0.3.15	HTTP	181	HTTP/1.0 200 OK (text/html)
1068	612.836000	10.0.3.15	192.0.2.123	HTTP	213	POST greattsouthoffshore.com HTTP/1.1
1069	612.836000	10.0.3.15	10.0.3.15	HTTP	213	POST greattsouthoffshore.com HTTP/1.1
1073	612.867000	10.0.3.15	10.0.3.15	HTTP	181	HTTP/1.0 200 OK (text/html)
1093	613.086000	10.0.3.15	192.0.2.123	HTTP	204	POST fdecub-ydyg.ru HTTP/1.1
1094	613.086000	10.0.3.15	10.0.3.15	HTTP	204	POST fdecub-ydyg.ru HTTP/1.1
1098	613.117000	10.0.3.15	10.0.3.15	HTTP	181	HTTP/1.0 200 OK (text/html)
1118	613.336000	10.0.3.15	192.0.2.123	HTTP	209	POST angar-promarenda.ru HTTP/1.1
1119	613.336000	10.0.3.15	10.0.3.15	HTTP	209	POST angar-promarenda.ru HTTP/1.1
1123	613.367000	10.0.3.15	10.0.3.15	HTTP	181	HTTP/1.0 200 OK (text/html)
1143	613.586000	10.0.3.15	192.0.2.123	HTTP	213	POST kasperskygay-formula.in HTTP/1.1
1144	613.586000	10.0.3.15	10.0.3.15	HTTP	213	POST kasperskygav-formula.in HTTP/1.1
1148	613.633000	10.0.3.15	10.0.3.15	HTTP	181	HTTP/1.0 200 OK (text/html)
1168	613.789000	10.0.3.15	192.0.2.123	HTTP	216	POST www.microavrc-usb33bit.com HTTP/1.1
1169	613.789000	10.0.3.15	10.0.3.15	HTTP	216	POST www.microavrc-usb33bit.com HTTP/1.1
1173	613.820000	10.0.3.15	10.0.3.15	HTTP	181	HTTP/1.0 200 OK (text/html)
1193	613.961000	10.0.3.15	192.0.2.123	HTTP	212	POST microavrc-usb33bit.com HTTP/1.1
1194	613.961000	10.0.3.15	10.0.3.15	HTTP	212	POST microavrc-usb33bit.com HTTP/1.1
1198	614.008000	10.0.3.15	10.0.3.15	HTTP	181	HTTP/1.0 200 OK (text/html)
1218	614.227000	10.0.3.15	192.0.2.123	HTTP	205	POST fgefa-bugin.com HTTP/1.1
1219	614.227000	10.0.3.15	10.0.3.15	HTTP	205	POST fgefa-bugin.com HTTP/1.1

2 - Analisi Dinamica (FakeNet e Wireshark)

Focus con Wireshark di una richiesta di connessione HTTP

http						
No.	Time	Source	Destination	Protocol	Length	Info
1068	612.836000	10.0.3.15	192.0.2.123	HTTP	213	POST greattsouthoffshore.com HTTP/1.1
1069	612.836000	10.0.3.15	10.0.3.15	HTTP	213	POST greattsouthoffshore.com HTTP/1.1
1073	612.867000	10.0.3.15	10.0.3.15	HTTP	181	HTTP/1.0 200 OK (text/html)
1093	613.086000	10.0.3.15	192.0.2.123	HTTP	204	POST fdecub-ydyg.ru HTTP/1.1
1094	613.086000	10.0.3.15	10.0.3.15	HTTP	204	POST fdecub-ydyg.ru HTTP/1.1
1098	613.117000	10.0.3.15	10.0.3.15	HTTP	181	HTTP/1.0 200 OK (text/html)
1118	613.336000	10.0.3.15	192.0.2.123	HTTP	209	POST angar-promarenda.ru HTTP/1.1
1119	613.336000	10.0.3.15	10.0.3.15	HTTP	209	POST angar-promarenda.ru HTTP/1.1
1123	613.367000	10.0.3.15	10.0.3.15	HTTP	181	HTTP/1.0 200 OK (text/html)
1143	613.586000	10.0.3.15	192.0.2.123	HTTP	213	POST kasperskygay-formula.in HTTP/1.1
1144	613.586000	10.0.3.15	10.0.3.15	HTTP	213	POST kasperskygay-formula.in HTTP/1.1
1148	613.633000	10.0.3.15	10.0.3.15	HTTP	181	HTTP/1.0 200 OK (text/html)
1168	613.789000	10.0.3.15	192.0.2.123	HTTP	216	POST www.microavrc-usb33bit.com HTTP/1.1
1169	613.789000	10.0.3.15	10.0.3.15	HTTP	216	POST www.microavrc-usb33bit.com HTTP/1.1
1173	613.820000	10.0.3.15	10.0.3.15	HTTP	181	HTTP/1.0 200 OK (text/html)
1193	613.961000	10.0.3.15	192.0.2.123	HTTP	212	POST microavrc-usb33bit.com HTTP/1.1
1194	613.961000	10.0.3.15	10.0.3.15	HTTP	212	POST microavrc-usb33bit.com HTTP/1.1
1198	614.008000	10.0.3.15	10.0.3.15	HTTP	181	HTTP/1.0 200 OK (text/html)
1218	614.227000	10.0.3.15	192.0.2.123	HTTP	205	POST fgefa-bugin.com HTTP/1.1

+

Frame 1168: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits)

Raw packet data

+

Internet Protocol Version 4, Src: 10.0.3.15, Dst: 192.0.2.123

+

Transmission Control Protocol, Src Port: 49213, Dst Port: 80, Seq: 1, Ack: 1, Len: 176

+

Hypertext Transfer Protocol

0000	45 00 00 d8 04 a0 40 00	80 06 25 f6 0a 00 03 0f	E.....@. ..%.....
0010	c0 00 02 7b c0 3d 00 50	27 11 92 d4 47 0e f4 72	...{.=.P '...G..r
0020	50 18 01 00 f9 80 00 00	50 4f 53 54 20 77 77 77	P..... POST www
0030	2e 6d 69 63 72 6f 61 76	72 63 2d 75 73 62 33 33	.microav rc-usb33
0040	62 69 74 2e 63 6f 6d 20	48 54 54 50 2f 31 2e 31	bit.com HTTP/1.1
0050	0d 0a 55 73 65 72 2d 41	67 65 6e 74 3a 20 4d 6f	..User-Agent: Mo
0060	7a 69 6c 6c 61 2f 34 2e	30 20 28 63 6f 6d 70 61	zilla/4. 0 (compa
0070	74 69 62 6c 65 3b 20 4d	53 49 45 20 32 38 3b 20	tible; M SIE 28;
0080	4e 54 36 2e 31 2e 37 36	30 31 2d 44 30 38 41 44	NT6.1.76 01-D08AD
0090	42 36 46 2e 45 4e 47 2e	32 37 32 32 32 37 44 43	B6F.ENG. 272227DC
00a0	2d 37 33 36 36 38 30 2d	39 35 35 39 30 34 2d 31	-736680- 955904-1
00b0	34 42 34 31 35 45 38 3b	20 2e 4e 45 54 20 43 4c	4B415E8; .NET CL
00c0	52 20 30 30 30 30 30 30	30 30 2f 30 30 30 30 30	R 000000 00/00000
00d0	30 30 30 29 0d 0a 0d 0a		000)....

2 - Analisi Dinamica (Conclusioni)

A questo punto dell'analisi siamo riusciti comprendere ulteriori caratteristiche del virus, in particolare del suo comportamento:

- Durante l'esecuzione il **virus si maschera** come una calcolatrice e **abbassa i sistemi di sicurezza di Windows**
- Il virus **aggiunge la sezione malevola** ai vari eseguibili (.vmp0)
- Il virus **genera molte copie di sé stesso**
- Il virus **crea connessioni HTTP** con siti russi

3 - Reverse Engineering

In questa sezione abbiamo usato tool già presenti nella macchina Windows.ova, ovvero:

- *IDA*

- *x32dbg*

- *Ollydbg*

3 - Reverse Engineering

Dal tool Ollydbg si evidenziano chiamate di sistema che lanciano il prompt dei comandi

The screenshot shows the Ollydbg interface with the assembly window displaying code for 'ScyllaHide - [CPU - main thread, module sample2]'. A red box highlights a call instruction at address 01012E42: `CALL EBX, 53 48 45 4C`. The comment for this instruction is `ASCII "SHELL32.dll",0`. The registers window on the right shows the current state of the CPU registers, with EIP pointing to 01012475, which is the address of the `sample2.<ModuleEntryPoint>` function.

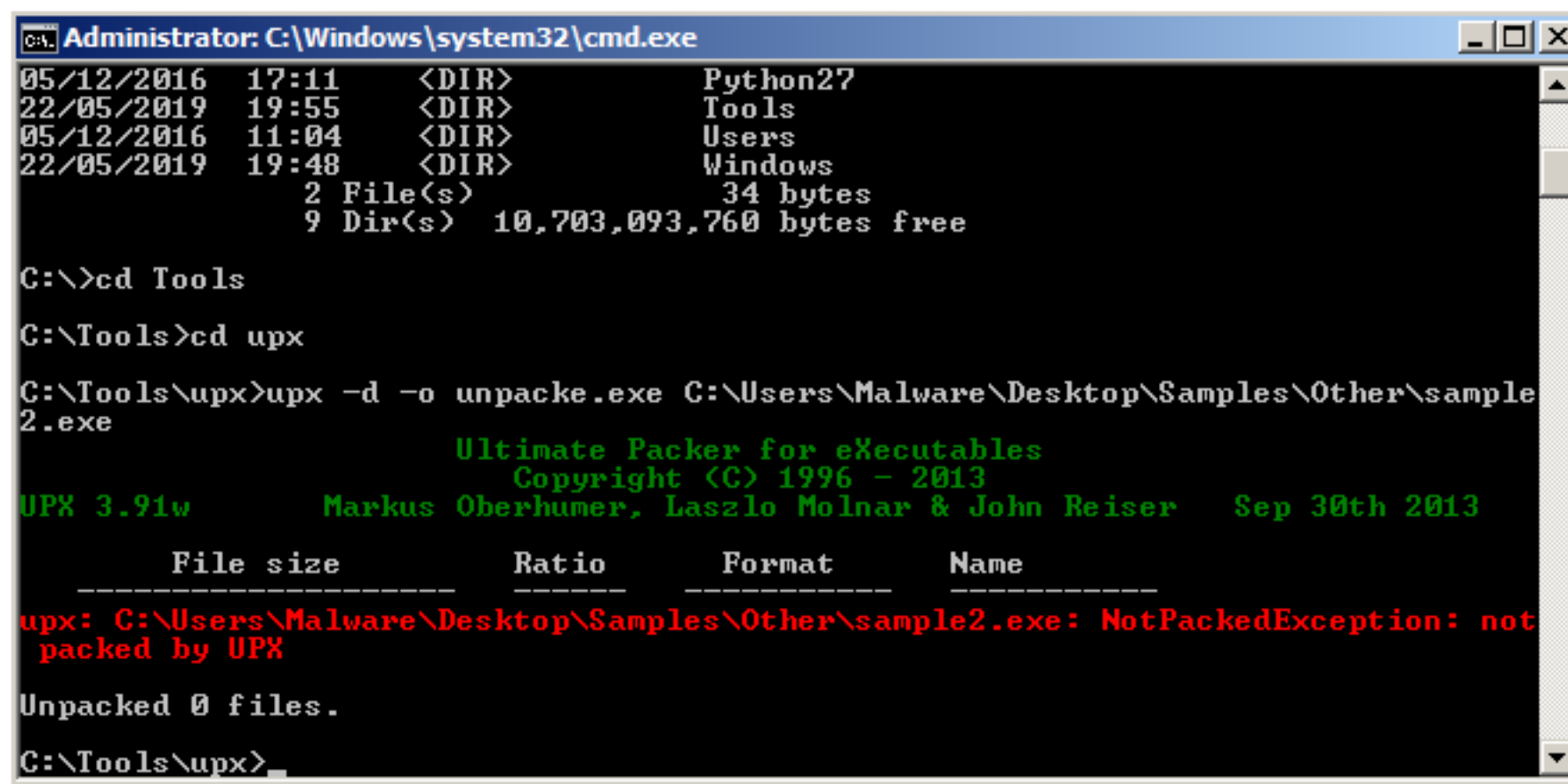
Address	Disassembly	Comment
01012DCC	62 2E 01 00	DD 00012E62
01012DD0	78 2E 01 00	DD 00012E78
01012DD4	82 2E 01 00	DD 00012E82
01012DD8	8C 2E 01 00	DD 00012E8C
01012DDC	96 2E 01 00	DD 00012E96
01012DE0	A0 2E 01 00	DD 00012EA0
01012DE4	AA 2E 01 00	DD 00012EAA
01012DE8	B4 2E 01 00	DD 00012EB4
01012DEC	BE 2E 01 00	DD 00012EBE
01012DF0	C6 2E 01 00	DD 00012EC6
01012DF4	D4 2E 01 00	DD 00012ED4
01012DF8	DE 2E 01 00	DD 00012EDE
01012DFC	E6 2E 01 00	DD 00012EE6
01012E00	F0 2E 01 00	DD 00012EF0
01012E04	00 2F 01 00	DD 00012F00
01012E08	0C 2F 01 00	DD 00012F0C
01012E0C	18 2F 01 00	DD 00012F18
01012E10	24 2F 01 00	DD 00012F24
01012E14	30 2F 01 00	DD 00012F30
01012E18	3C 2F 01 00	DD 00012F3C
01012E1C	48 2F 01 00	DD 00012F48
01012E20	54 2F 01 00	DD 00012F54
01012E24	60 2F 01 00	DD 00012F60
01012E28	6C 2F 01 00	DD 00012F6C
01012E2C	78 2F 01 00	DD 00012F78
01012E30	84 2F 01 00	DD 00012F84
01012E34	90 2F 01 00	DD 00012F90
01012E38	9C 2F 01 00	DD 00012F9C
01012E3C	A8 2F 01 00	DD 00012FA8
01012E40	B4 2F 01 00	DD 00012FB4
01012E42	CALL EBX, 53 48 45 4C	ASCII "SHELL32.dll",0
01012E44	52 00	DD 00000052
01012E48	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012E4C	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012E50	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012E54	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012E58	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012E5C	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012E60	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012E64	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012E68	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012E6C	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012E70	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012E74	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012E78	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012E7C	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012E80	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012E84	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012E88	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012E8C	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012E90	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012E94	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012E98	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012E9C	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012EA0	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012EA4	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012EA8	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012EAC	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012EAE	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012EB0	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012EB4	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012EB8	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012EBC	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012EBE	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012EC0	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012EC4	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012EC8	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012ECE	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012ED0	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012ED4	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012ED8	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012EDC	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012EE0	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012EE4	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012EE8	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012EEC	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012EF0	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012EF4	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012EF8	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012EFC	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012F00	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012F04	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012F08	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012F0C	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012F10	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012F14	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012F18	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012F1C	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012F20	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012F24	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012F28	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012F2C	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012F30	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012F34	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012F38	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012F3C	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012F40	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012F44	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012F48	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012F4C	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012F50	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012F54	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012F58	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012F5C	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012F60	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012F64	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012F68	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012F6C	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012F70	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012F74	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012F78	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012F7C	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012F80	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012F84	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012F88	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012F8C	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012F90	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012F94	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012F98	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012F9C	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012FA0	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012FA4	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012FA8	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012FAC	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012FAE	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012FB0	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012FB4	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012FB8	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012FBC	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012FBE	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012FC0	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012FC4	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012FC8	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012FCC	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012FCE	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012FD0	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012FD4	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012FD8	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012FDC	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012FE0	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012FE4	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012FE8	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012FEC	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012FEF	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012FF0	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012FF4	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012FF8	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012FFC	5F 5F 43 78	ASCII "___CxxFrameHandle"
01012FFF	5F 5F 43 78	ASCII "___CxxFrameHandle"

Registers (FPU)

Register	Value	Comment
EAX	757FEF0A	kernel32.BaseThreadInitThunk
ECX	00000000	
EDX	01012475	sample2.<ModuleEntryPoint>
EBX	7FFD4000	
ESP	0016FF8C	
EBP	0016FF94	
ESI	00000000	
EDI	00000000	
EIP	01012475	sample2.<ModuleEntryPoint>
C 0	ES 0023 32bit 0(FFFFFFFF)	
P 1	CS 001B 32bit 0(FFFFFFFF)	
A 0	SS 0023 32bit 0(FFFFFFFF)	
Z 1	DS 0023 32bit 0(FFFFFFFF)	
S 0	FS 003B 32bit 7FFDF000(FFF)	
T 0	GS 0000 NULL	
D 0		
O 0	LastErr 00000000 ERROR_SUCCESS	
EFL	00000246 (NO,NB,E,BE,NS,PE,GE,LE)	
ST0	empty 0.0	
ST1	empty 0.0	
ST2	empty 0.0	
ST3	empty 0.0	
ST4	empty 0.0	
ST5	empty 0.0	
ST6	empty 0.0	
ST7	empty 0.0	
FST	0000 Cond 3 2 1 0 E S P U O Z D I	
FCW	027F Prec NEAR,53 Err 0 0 0 0 0 0 0 (GT)	
Last cmd	0000:00000000	
XMM0	00000000 00000000 00000000 00000000	
XMM1	00000000 00000000 00000000 00000000	
XMM2	00000000 00000000 00000000 00000000	
XMM3	00000000 00000000 00000000 00000000	
XMM4	00000000 00000000 00000000 00000000	
XMM5	00000000 00000000 00000000 00000000	
XMM6	00000000 00000000 00000000 00000000	

3 - Reverse Engineering

Come visto dall'analisi (hardcore mode) con PEID il virus non è packed



```
Administrator: C:\Windows\system32\cmd.exe
05/12/2016 17:11 <DIR> Python27
22/05/2019 19:55 <DIR> Tools
05/12/2016 11:04 <DIR> Users
22/05/2019 19:48 <DIR> Windows
                2 File(s)          34 bytes
                9 Dir(s) 10,703,093,760 bytes free

C:\>cd Tools
C:\Tools>cd upx
C:\Tools\upx>upx -d -o unpacke.exe C:\Users\Malware\Desktop\Samples\Other\sample
2.exe

                Ultimate Packer for eXecutables
                Copyright (C) 1996 - 2013
UPX 3.91w      Markus Oberhumer, Laszlo Molnar & John Reiser   Sep 30th 2013

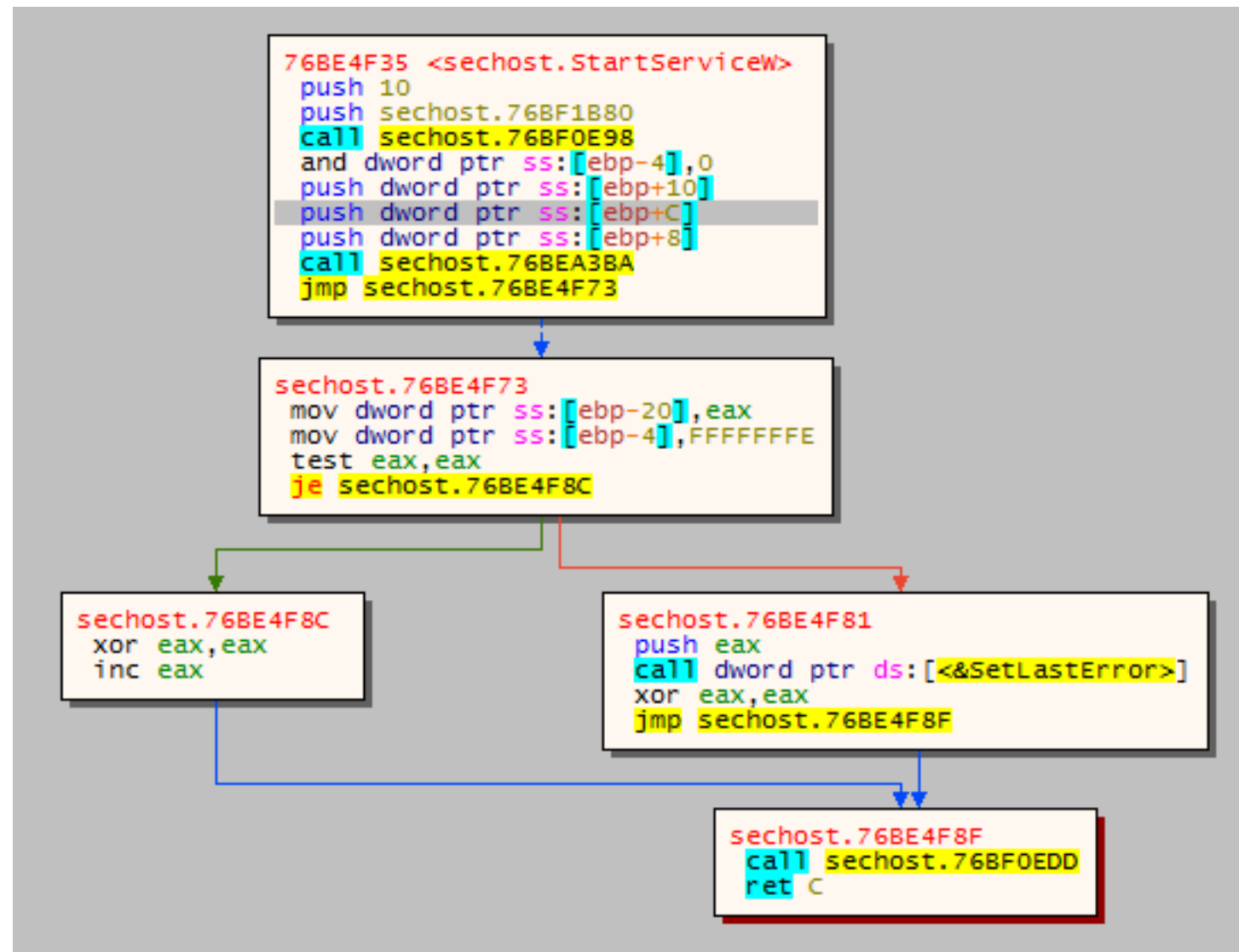
      File size      Ratio      Format      Name
      -----
upx: C:\Users\Malware\Desktop\Samples\Other\sample2.exe: NotPackedException: not
packed by UPX

Unpacked 0 files.
C:\Tools\upx>
```

Usando Upx si nota che il virus non è stato compresso con questo particolare tool

3 - Reverse Engineering

Con x32dbg si analizza la disattivazione del Firewall tramite la chiamata alla libreria "ComSysApp" che configura .dll atte alla sua disattivazione



3 - Reverse Engineering

Salvataggio dei file carpiti nella libreria "wsr28zt32.dll" presente nei file nascosti

The screenshot displays the x32dbg debugger interface. The main window shows assembly code for the `kernel32.dll` module, specifically the `776CEC11` to `776CEC70` range. The code includes instructions like `push ebp`, `mov ebp, esp`, `push ecx`, `push dword ptr ss:[ebp+8]`, `lea eax, dword ptr ss:[ebp-8]`, `call <kernel32.Basep8BitStringToDynamic>`, `test eax, eax`, `je kernel32.776EC009`, `push esi`, `push dword ptr ss:[ebp+20]`, `push dword ptr ss:[ebp+1C]`, `push dword ptr ss:[ebp+18]`, `push dword ptr ss:[ebp+14]`, `push dword ptr ss:[ebp+10]`, `push dword ptr ss:[ebp+C]`, `push dword ptr ss:[ebp-4]`, `call <kernel32.CreateFileW>`, `mov esi, eax`, `lea eax, dword ptr ss:[ebp-8]`, `push eax`, `call dword ptr ds:[<RtlFreeUnicodeStri>`, `mov eax, esi`, `pop esi`, `leave`, `ret 1C`, `jmp dword ptr ds:[<GetFullPathNameA>]`, `GetFullPathNameA`, `mov edi, edi`, `push ebp`, `mov ebp, esp`, `pop ebp`, and `jmp <kernel32.GetFullPathNameA>`.

The right-hand pane shows the register window with the following values:

- EAX: 00000000
- EBX: 00000000
- ECX: 0016FB08
- EDX: 77946C74
- ESP: 0016FB50
- ESI: 0016FB24
- EDI: FFFFFFFF
- EIP: 779A05DA

The bottom pane shows the memory dump with the following data:

Address	Hex	ASCII
77901000	53 00 59 00 53 00 54 00 45 00 40 00 00 00 90 90	S.Y.S.T.E.M.
77901010	72 00 63 00 00 00 88 46 0C 3B C7 0F 85 DE BC 09	r.c...F.;C...b4.
77901020	00 64 A1 18 00 00 00 88 40 30 56 57 FF 70 18 E8	.d....@ovwyp.e
77901030	4E 18 05 00 33 C0 E9 DE 98 06 00 33 C0 E9 BD 98	N...3Aeb...3Aes.
77901040	06 00 83 CF 02 E9 D4 90 06 00 83 CF 08 E9 DE 90	...I.eo...I.ep.
77901050	06 00 33 C0 E9 42 9E 06 00 39 40 10 0F 84 14 9E	...3Aes...9M....
77901060	06 00 E9 C7 C0 09 00 50 E8 48 28 05 00 50 E8 A0	...eCA...PEH(...Pe
77901070	1C 05 00 33 C0 E9 EF 97 06 00 90 90 90 90 88	...3Aei.....
77901080	FF 55 88 EC 83 7D 08 00 0F 84 16 C8 09 00 57 88	yU.i...}.E.W.
77901090	7D 0C 85 FF 75 03 6A 0A 5F 64 A1 18 00 00 00 88	}.yu.j...dj....
779010A0	40 30 56 6A 0C 6A 08 FF 70 18 E8 3F 19 05 00 88	@ovj.j.y.p.e?...
779010B0	F0 85 F6 74 38 64 A2 18 00 00 00 88 40 30 88 CF	0.ot8dj...@.I
779010C0	C1 E1 02 51 6A 00 FF 70 18 E9 20 19 05 00 89 46	Aa.Qj.y.p.e...F
779010D0	08 85 C0 0F 84 D2 C7 09 00 88 45 08 83 26 00 89	...A.O.C...E..e..
779010E0	7E 04 89 30 33 C0 40 5E 5F 5D C2 08 00 33 C0 EB	...03AaA..jA...3Ae
779010F0	F6 90 90 90 90 90 88 FF 55 88 EC 56 88 75 08 85	0.....yU.iV.u..
77901100	F6 74 2F 88 46 08 85 C0 74 14 50 64 A1 18 00 00	0t..F..At.Pdi...

4 - Conclusioni

Confronto degli score tra le due analisi eseguite

Static Analysis		
Category	Select	Score
Packed		0
Strings		3
Imports		2
Sections		1
Main Icon		1
Additional Icons		0
Dialogs		0
Version Information		0
Digital Signature		2
Total Score		9
Verdict		Potentially Suspicious

Dynamic Analysis		
Category	Select	Score
Persistence		2
File Manipulation		2
Process Manipulation		2
Registry Manipulation		2
Additional Processes		0
Removal Resistance		2
Analysis Resistance		2
Interface/Visible Activity		0
Network Activity		2
Rootkit Behaviour		0
System Calls		1
Behaviour		2
Total Score		17
Verdict		Suspicious

Come si nota l'analisi statica è più importante in quanto ha più parametri di analisi e di conseguenza risulta essere un'analisi più precisa

Grazie per l'attenzione

Bibliografia

Link utili:

<https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32/Expiro>

<https://www.virustotal.com/gui/file/34558ac3bfab17ca1a1ff70860b35296395f1df7fa8d86b39c56faecf9c3cffc>

https://en.wikipedia.org/wiki/Microsoft_Windows_library_files