



Compito:

Compito di : Mendolia Valerio

Analisi statica e dinamica: Un approccio pratico

Obiettivo

Con riferimento al file Malware_U3_W2_L5 presente all'interno della cartella

«Esercizio_Pratico_U3_W2_L5» sul desktop della macchina virtuale dedicata per l'analisi dei malware, rispondere ai seguenti quesiti:

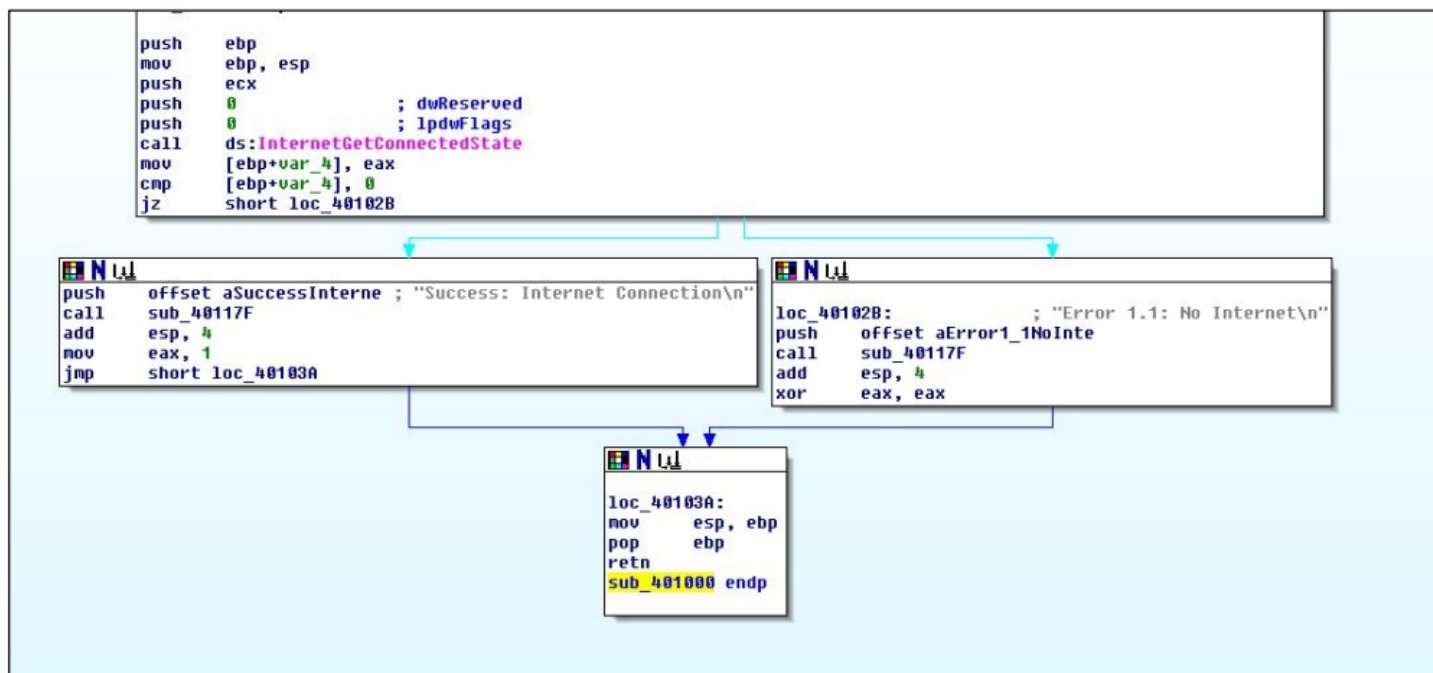
1. Quali librerie vengono importate dal file eseguibile?
2. Quali sono le sezioni di cui si compone il file eseguibile del malware?

Con riferimento alla figura in slide 3, risponde ai seguenti quesiti:

- 1.1. Identificare i costrutti noti (creazione dello stack, eventuali cicli, costrutti)
- 1.3. Ipotizzare il comportamento della funzionalità implementata:
- 1.4. Come ultimo punto, dopo il bonus, spiegare quale istruzione assembly complessa
3. Come membro senior del SOC ti è richiesto di convincere il dipendente che il file non è maligno.

Immagine originale:

Figura 1



Analisi statica:

1. Quali librerie vengono importate dal file eseguibile?

Per verificare le librerie importate si possono utilizzare dei decompilatori come CFF Explorer oppure Ida per facilitare i tempi:
Andando su CFF Explorer su import directory possiamo vedere le librerie che usa il programma:

Malware_U3_W2_L5.exe

Module Name	Imports	OFTs	TimeStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.dll	44	00006518	00000000	00000000	000065EC	00006000
WININET.dll	5	000065CC	00000000	00000000	00006664	000060B4

File: Malware_U3_W2_L5.exe

- Dos Header
- Nt Headers
 - File Header
 - Optional Header
 - Data Directories [x]
 - Section Headers [x]
- Import Directory

Esempio con Ida. Come si vede su Ida vengono divise in base alle funzioni delle librerie:

IDA View-A Hex View-A Exports Imports Names Functions Strings Structures

Address	Ordinal	Name	Library
004060C4		InternetOpenA	WININET
004060C0		InternetGetConnectedState	WININET
004060...		InternetReadFile	WININET
004060B8		InternetCloseHandle	WININET
004060B4		InternetOpenUrlA	WININET
00406054		GetFileType	KERNEL32
00406050		GetStdHandle	KERNEL32
0040604C		SetHandleCount	KERNEL32
00406048		GetEnvironmentStringsW	KERNEL32
00406044		GetEnvironmentStrings	KERNEL32
00406040		WideCharToMultiByte	KERNEL32
0040603C		FreeEnvironmentStringsW	KERNEL32
00406038		FreeEnvironmentStringsA	KERNEL32
00406034		GetModuleFileNameA	KERNEL32
00406030		UnhandledExceptionFilter	KERNEL32
0040602C		GetCurrentProcess	KERNEL32
00406028		TerminateProcess	KERNEL32
00406024		ExitProcess	KERNEL32
00406020		GetVersion	KERNEL32
0040601C		GetCommandLineA	KERNEL32
00406018		MultiByteToWideChar	KERNEL32
00406014		LCMapStringA	KERNEL32
00406010		LCMapStringW	KERNEL32
0040600C		GetStringTypeA	KERNEL32
00406008		GetStringTypeW	KERNEL32
00406004		SetStdHandle	KERNEL32
00406000		Sleep	KERNEL32
004060...		CloseHandle	KERNEL32
004060A8		SetFilePointer	KERNEL32
004060A4		FlushFileBuffers	KERNEL32
004060A0		GetLastError	KERNEL32

Come si vede dai due esempi vengono utilizzate:

KERNEL32.dll: Che è una delle librerie fondamentali di Windows che consentono al sistema operativo di gestire risorse hardware, memoria, processi e file.

WININET.dll: Fornisce funzionalità per creare connessioni, inviare richieste HTTP, scaricare file, eseguire operazioni FTP e molto altro. Insomma viene utilizzata dal malware per inviare o ricevere informazioni per conto dell'attaccante.

2. Quali sono le sezioni di cui si compone il file eseguibile del malware?

Le sezioni sono parti di un file eseguibile o di una libreria che organizzano e memorizzano diversi tipi di dati e codice, compongono il malware e si possono trovare facilmente con l'uso di un decompilatore di nome **CFF Explorer** nel esempio sottostante possiamo vederle:

Malware_U3_W2_L5.exe									
Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations ...	Linenumber...	Characteristics
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
.text	00004A78	00001000	00005000	00001000	00000000	00000000	0000	0000	60000020
.rdata	0000095E	00006000	00001000	00006000	00000000	00000000	0000	0000	40000040
.data	00003F08	00007000	00003000	00007000	00000000	00000000	0000	0000	C0000040

Come possiamo vedere ci sono tre sezioni chiamate **.text**, **.rdata**, **.data**

La prima sezione **.text** contiene il codice eseguibile del programma, come istruzioni e funzioni.

La seconda sezione **.rdata** contiene dati di sola lettura, come costanti o stringhe, che il programma utilizza durante l'esecuzione.

La terza sezione **.data** memorizza dati inizializzati che possono essere modificati durante l'esecuzione del programma, come variabili globali.

Un altro esempio con Ghidra :

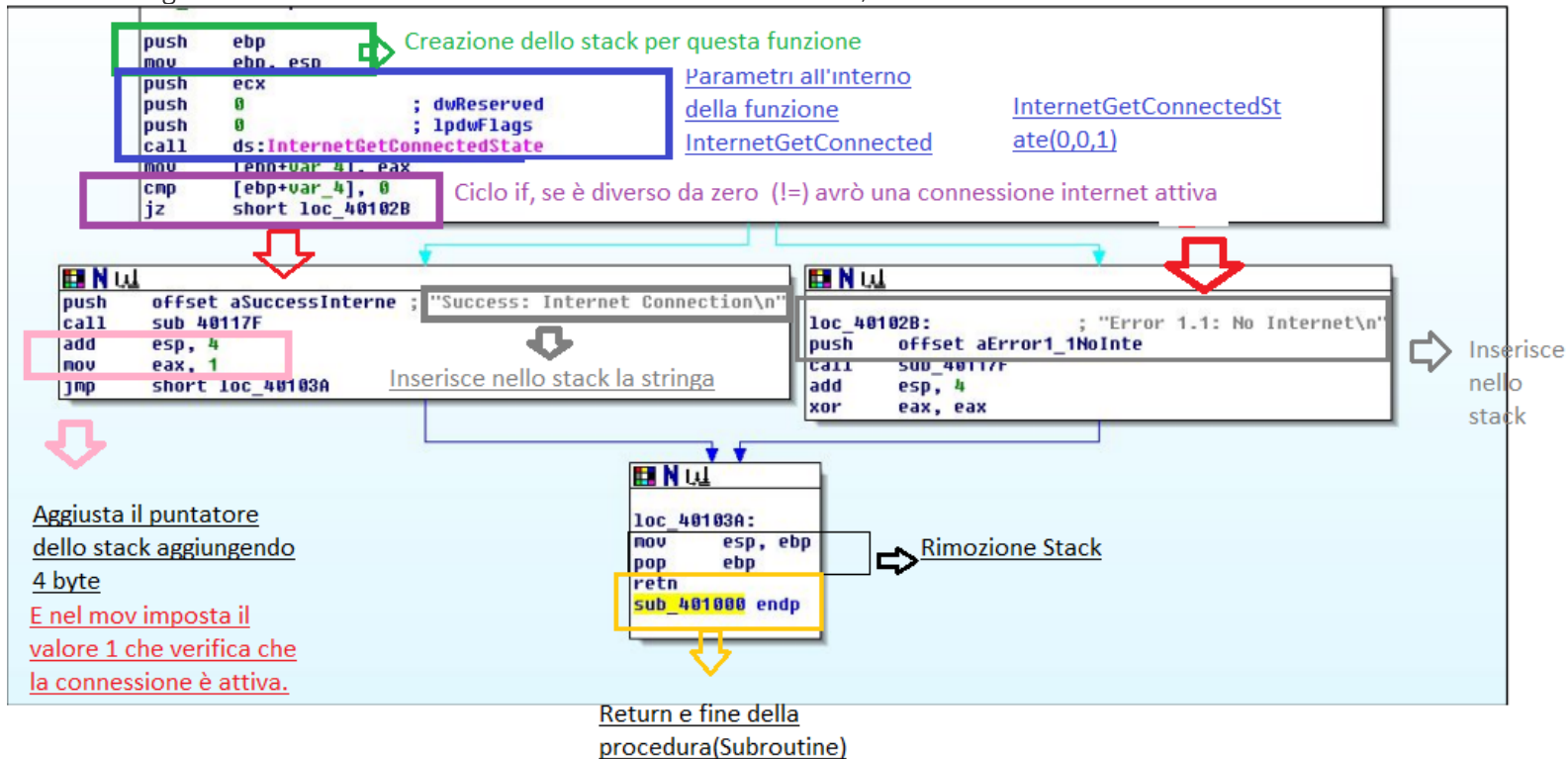
Memory Map [CodeBrowser: test:/Malware_U3_W2_L5.exe]												
Memory Map - Image Base: 00400000												
Memory Blocks												
Name	Start	End	Length	R	W	X	Volatile	Overlay	Type	Initialized	Byte Source	Source
Headers	00400000	00400fff	0x1000	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	<input checked="" type="checkbox"/>	File: Malware_U3_W2...	
.text	00401000	00405fff	0x5000	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	<input checked="" type="checkbox"/>	File: Malware_U3_W2...	
.rdata	00406000	00406fff	0x1000	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	<input checked="" type="checkbox"/>	File: Malware_U3_W2...	
.data	00407000	00409fff	0x3000	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	<input checked="" type="checkbox"/>	File: Malware_U3_W2...	
.data	0040a000	0040af07	0xf08	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	<input type="checkbox"/>		
tdb	ffdf000	ffdffff	0x1000	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default	<input checked="" type="checkbox"/>		

Visualizzazione sul codice delle determinate sezioni all'inizio del programma:

Listing: Malware_U3_W2_L5.exe			
004000df	00	??	00h
004000e0	00	??	00h
004000e1	00	??	00h
004000e2	00	??	00h
004000e3	00	??	00h
004000e4	00	??	00h
004000e5	00	??	00h
004000e6	00	??	00h
004000e7	00	??	00h
004000e8	50 45 00	IMAGE_NT...	= 000065e4
	00 4c 01		= 6518h
	03 00 a1 ...		
004001e0	2e 74 65	IMAGE_SE...	.text
	78 74 00		
	00 00 78 ...		
00400208	2e 72 64	IMAGE_SE...	.rdata
	61 74 61		
	00 00 5e ...		
00400230	2e 64 61	IMAGE_SE...	.data
	74 61 00		
	00 00 08 ...		
00400258	00	??	00h

1.1. Identificare i costrutti noti (creazione dello stack, eventuali cicli, costrutti):

Illustrerò la figura con la descrizione del codice determinando i vari stack, costrutti e cicli:



Quindi posso constatare un paio di cose, elencherò quelle più importanti:

1. Creazione dello stack di memoria nel blocco di istruzioni all'interno del rettangolo verde per questa funzione.
2. I parametri che andranno a comporre la funzione dichiarati con il push, tra cui un parametro sconosciuto richiamato sopra la funzione nel rettangolo blu e richiama la libreria WININET.dll per utilizzare questa funzione

```
51          PUSH      param_1
6a 00       PUSH      0x0
6a 00       PUSH      0x0
ff 15 c0    CALL      dword ptr [->WININET.DLL::InternetGetConnected... = 000065fa
```

3. Costrutto condizionale IF, identificato dalla coppia di istruzioni nel rettangolo viola, dove sicuramente viene utilizzato un diverso da zero(!= 0) .

4. Aggiusta il puntatore dello stack e lo allarga aggiungendo 4 byte, e nel move possiamo vedere che c'è il valore 1 che indica che la connessione è attiva. Si trova nel riquadro rosa.

5. Infine possiamo vedere la rimozione dello stack all'interno della figura nera, è un return nella figura gialla.

Quindi ho ipotizzato questo tipo di codice per la funzione:

```

1 void funzione_generica_controllo_connessione(int param1) {
2
3
4 int statointernet; // Qua sono sicuro perchè si tratta di numeri come inserito nell'assembly
5 int dwReserved = 0;
6 int lpdwFlags = 0;
7 statointernet = internetgetconnectedstate(dwReserved,lpdwFlags,param1); // 0, 0 , parametro sconosciuto
8
9
10 if (statointernet != 0) {
11 printf ("Success: Internet Connection\n");
12 } else {
13 printf ("Error 1.1: No Internet\n");
14 }
15 return;// fine funzione e return
16 }

```

1.3 Ipotesi funzionalità:

Ipotesi funzionalità :

La funzione **getInternetConnectState** viene utilizzata per verificare la presenza di una connessione Internet su un determinato dispositivo.

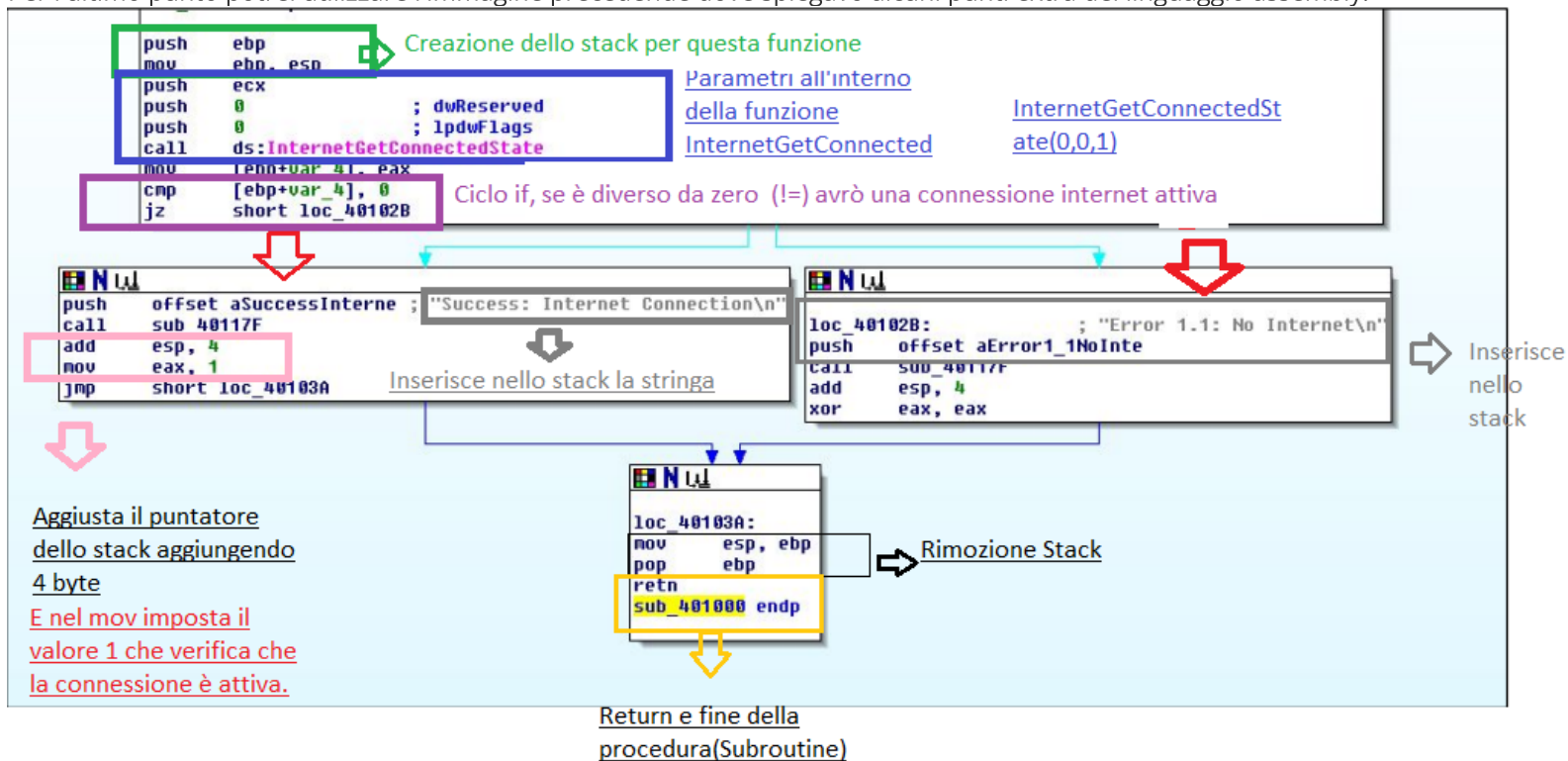
La logica di controllo è implementata attraverso un'istruzione condizionale **"if"**. La condizione dell'istruzione "if" verifica se il valore restituito dalla funzione getInternetConnectState è uguale a 0.

Se il valore restituito è uguale a 0, significa che la connessione Internet non è presente. In questo caso, la funzione mostra il messaggio "no internet" a schermo e completa la sua esecuzione.

Se il valore restituito dalla funzione getInternetConnectState è diverso da 0, indica che la connessione Internet è presente. In questo caso, la funzione mostra il messaggio "Success: Internet Connection" a schermo prima di terminare il suo compito.

1.4 Come ultimo punto, dopo il bonus, spiegare quale istruzione assembly complessa:

Per l'ultimo punto utilizzare l'immagine precedente dove spiegavo alcuni punti extra del linguaggio assembly:



3. BONUS:

Per convincere il dipendente che il processo e il file **IEXPLORE.EXE** non sono maligni, si possono effettuare diverse scansioni, tra cui quella statica e dinamica:

Quindi inizio a fare una scansione statica delle stringhe del file IEXPLORE.EXE con bintext:

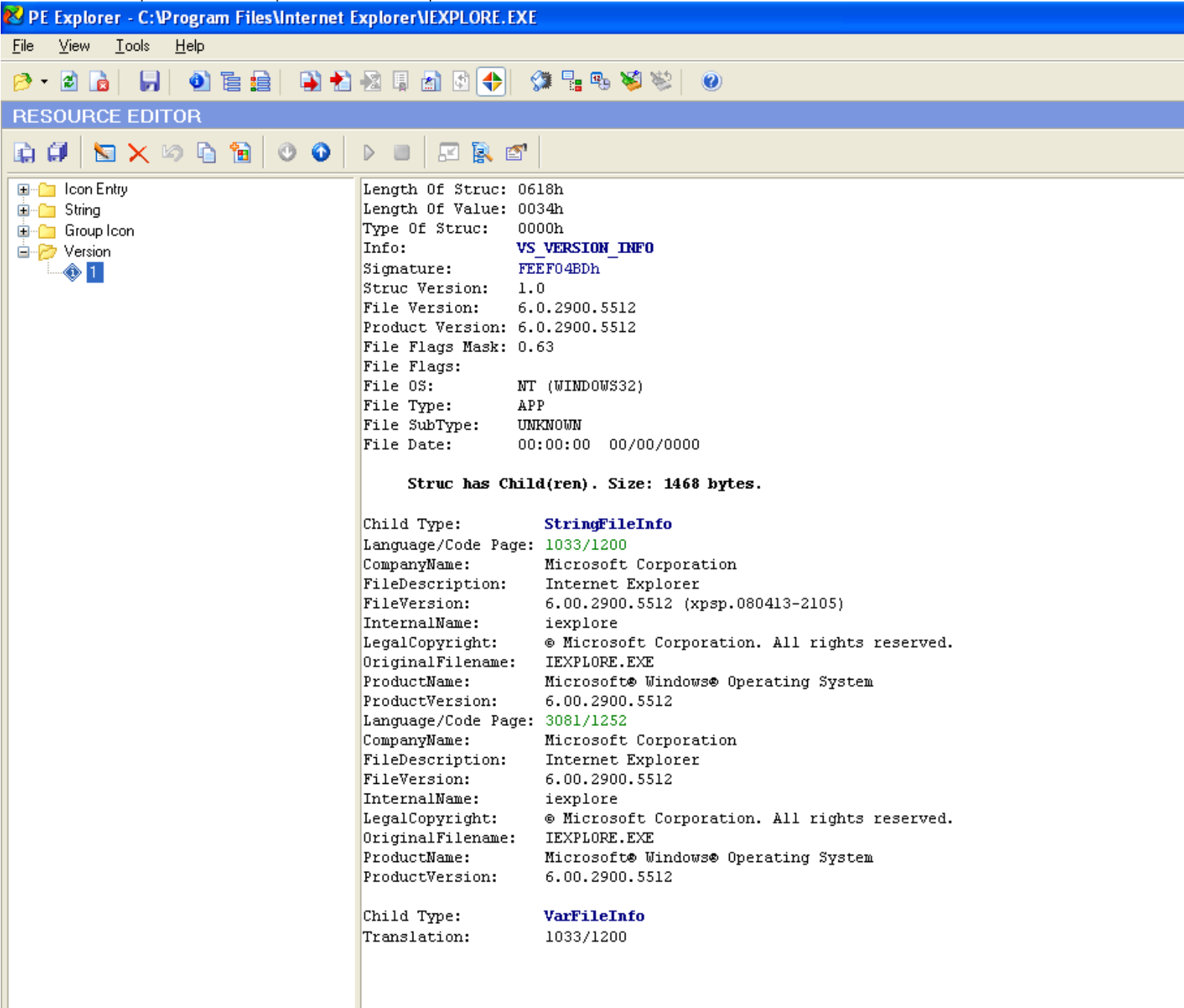
BinText 3.0.3

Search Filter Help			
File to scan C:\Program Files\Internet Explorer\IEXPLORE.EXE			
<input checked="" type="checkbox"/> Advanced view			
File pos	Mem pos	ID	Text
A 00000000004D	00000040004D	0	!This program cannot be run in DOS mode.
A 000000000083	000000400083	0	j:"09,"09,"09
A 000000000091	000000400091	0	%79-"09,"19)"09
A 0000000000A1	0000004000A1	0	%m9!"09
A 0000000000A9	0000004000A9	0	%n9!"09
A 0000000000B1	0000004000B1	0	%o9!"09
A 0000000000B9	0000004000B9	0	%P9!"09
A 0000000000C1	0000004000C1	0	%I9!"09
A 0000000000C9	0000004000C9	0	%I9-"09Rich,"09
A 0000000001E0	0000004001E0	0	.text
A 000000000208	000000400208	0	.data
A 000000000230	000000400230	0	.rsrc
A 000000000290	000000400290	0	msvcrt.dll
A 00000000029B	00000040029B	0	KERNEL32.dll
A 0000000002A8	0000004002A8	0	NTDLL.DLL
A 0000000002B2	0000004002B2	0	USER32.dll
A 0000000002BD	0000004002BD	0	SHLWAPI.dll
A 0000000002C9	0000004002C9	0	SHDOCVW.dll
A 000000000570	000000401170	0	Software\Microsoft\Windows\CurrentVersion\Explorer\BrowseNewProcess
A 0000000005B4	0000004011B4	0	BrowseNewProcess
A 0000000005C8	0000004011C8	0	IE-%08X-%08X
A 0000000005D8	0000004011D8	0	MauiFrame
A 0000000005E4	0000004011E4	0	IEDummyFrame
A 0000000005F4	0000004011F4	0	CompatWarningFor
A 000000000608	000000401208	0	DllRegisterServer
A 00000000061C	00000040121C	0	rsabase.dll
A 000000000628	000000401228	0	Software\Microsoft\Cryptography\Defaults\Provider\Microsoft Base Cryptographic Provider v1.0
A 000000000688	000000401288	0	Signature
A 000000000694	000000401294	0	System\CurrentControlSet\Control\Windows
A 0000000006C0	0000004012C0	0	CSDVersion
A 0000000006DC	0000004012DC	0	dw15-x-\$ %u
A 000000000768	000000401368	0	watson.microsoft.com
A 000000000780	000000401380	0	Software\Microsoft\Internet Explorer\Main
A 0000000007AC	0000004013AC	0	IEWatsonURL
A 0000000007B8	0000004013B8	0	HKLM\Software\Microsoft\Internet Explorer\Registration\DigitalProductID
A 000000000800	000000401400	0	HKCU\Software\Microsoft\Office\10.0\Common\LanguageResources\UILanguage
A 000000000848	000000401448	0	Microsoft\Office\10.0\Common
A 0000000008A0	0000004014A0	0	%s -h %u
A 0000000008AC	0000004014AC	0	iedw.exe
A 0000000008B8	0000004014B8	0	Iexplore.XPExceptionFilter
A 0000000008D4	0000004014D4	0	IEWatsonEnabled
A 0000000008E4	0000004014E4	0	jscrip.dll
A 0000000008F0	0000004014F0	0	mshhtml.dll
A 0000000008FC	0000004014FC	0	mlang.dll
A 000000000908	000000401508	0	urlmon.dll
A 000000000914	000000401514	0	wininet.dll
A 000000000920	000000401520	0	shdocvw.DLL
A 00000000092C	00000040152C	0	browseui.DLL
A 00000000093C	00000040153C	0	comctl32.DLL
A 00000000094C	00000040154C	0	IEXPLORE.EXE
A 00000000095C	00000040155C	0	-nowait
A 00000000096C	00000040156C	0	.

Mi sembra tutto ok, vado a verificare il produttore tramite le stringhe ed esce che la compagnia della creazione del file è proprio microsoft quindi sembra sicuro:

File pos	Mem pos	ID	Text
U 00000001640E	00000041800E	0	VS_VERSION_INFO
U 00000001646A	00000041806A	0	StringFileInfo
U 00000001648E	00000041808E	0	040904B0
U 0000000164A6	0000004180A6	0	CompanyName
U 0000000164C0	0000004180C0	0	Microsoft Corporation
U 0000000164F2	0000004180F2	0	FileDescription
U 000000016514	000000418114	0	Internet Explorer
U 00000001653E	00000041813E	0	FileVersion
U 000000016558	000000418158	0	6.00.2900.5512 (xpsp.080413-2105)
U 0000000165A2	0000004181A2	0	InternalName
U 0000000165BC	0000004181BC	0	iexplore
U 0000000165D6	0000004181D6	0	LegalCopyright
U 0000000165F6	0000004181F6	0	Microsoft Corporation. All rights reserved.
U 000000016656	000000418256	0	OriginalFilename
U 000000016678	000000418278	0	IEXPLORE.EXE
U 00000001669A	00000041829A	0	ProductName
U 0000000166DA	0000004182DA	0	Operating System
U 000000016706	000000418306	0	ProductVersion
U 000000016724	000000418324	0	6.00.2900.5512
U 00000001674A	00000041834A	0	0c0904E4
U 000000016762	000000418362	0	CompanyName
U 00000001677C	00000041837C	0	Microsoft Corporation
U 0000000167AE	0000004183AE	0	FileDescription
U 0000000167D0	0000004183D0	0	Internet Explorer
U 0000000167FA	0000004183FA	0	FileVersion
U 000000016814	000000418414	0	6.00.2900.5512
U 00000001683A	00000041843A	0	InternalName
U 000000016854	000000418454	0	iexplore
U 00000001686E	00000041846E	0	LegalCopyright
U 00000001688E	00000041848E	0	Microsoft Corporation. All rights reserved.
U 0000000168EE	0000004184EE	0	OriginalFilename
U 000000016910	000000418510	0	IEXPLORE.EXE
U 000000016932	000000418532	0	ProductName
U 000000016972	000000418572	0	Operating System
U 00000001699E	00000041859E	0	ProductVersion
U 0000000169BC	0000004185BC	0	6.00.2900.5512
U 0000000169E2	0000004185E2	0	VarFileInfo
U 000000016A02	000000418602	0	Translation
U 000000016B18	000000418718	0	Internet Explorer
R 000000016A38	000000418638	700	This is being run in compatibility mode and not all features are enabled.
R 000000016ACC	0000004186CC	701	Internet Explorer Compatibility mode
R 000000016B16	000000418716	702	Internet Explorer
A 00000000004D	00000040004D	0	!This program cannot be run in DOS mode.
A 000000000083	000000400083	0	j,*09,*09,*09
A 000000000091	000000400091	0	%?9,*09,*19)*09
A 0000000000A1	0000004000A1	0	%m9!*09
A 0000000000A9	0000004000A9	0	%n9,*09

Faccio la controprova con PeExplorer e mi esce questo:



Ora vado a verificare il processo con un analisi dinamica e utilizzo process explorer, per prima cosa controllo le connessioni:

Process Monitor - Sysinternals: www.sysinternals.com					
File Edit Event Filter Tools Options Help					
Time of Day	Process Name	PID	Operation	Path	Result
12:17:01.4646...	IEXPLORE.EXE	1408	UDP Receive	localhost:2276 -> localhost:2276	SUCCESS
12:17:01.4646...	IEXPLORE.EXE	1408	UDP Send	localhost:2276 -> localhost:2276	SUCCESS
				Detail	
				Length: 1	
				Length: 1	

Sembrano connessione legittime, ora vado a verificare cosa fa il processo:

12:16:56.1474...	IEEXPLORE.EXE	1408	CreateFile	C:\DOCUMENTS AND SETTINGS
12:16:56.1474...	IEEXPLORE.EXE	1408	QueryDirectory	C:\Documents and Settings
12:16:56.1474...	IEEXPLORE.EXE	1408	QueryDirectory	C:\Documents and Settings
12:16:56.1478...	IEEXPLORE.EXE	1408	CloseFile	C:\Documents and Settings
12:16:56.1478...	IEEXPLORE.EXE	1408	CreateFile	C:\Documents and Settings\ADMINISTRATOR
12:16:56.1478...	IEEXPLORE.EXE	1408	QueryDirectory	C:\Documents and Settings\Administrator
12:16:56.1482...	IEEXPLORE.EXE	1408	QueryDirectory	C:\Documents and Settings\Administrator
12:16:56.1482...	IEEXPLORE.EXE	1408	CloseFile	C:\Documents and Settings\Administrator
12:16:56.1486...	IEEXPLORE.EXE	1408	CreateFile	C:\Documents and Settings\Administrator\Cookies
12:16:56.1486...	IEEXPLORE.EXE	1408	QueryDirectory	C:\Documents and Settings\Administrator\Cookies
12:16:56.1487...	IEEXPLORE.EXE	1408	QueryDirectory	C:\Documents and Settings\Administrator\Cookies
12:16:56.1492...	IEEXPLORE.EXE	1408	CloseFile	C:\Documents and Settings\Administrator\Cookies
12:16:56.1493...	IEEXPLORE.EXE	1408	CreateFile	C:\Documents and Settings\Administrator\FAVORITES
12:16:56.1493...	IEEXPLORE.EXE	1408	QueryDirectory	C:\Documents and Settings\Administrator\Favorites
12:16:56.1496...	IEEXPLORE.EXE	1408	QueryDirectory	C:\Documents and Settings\Administrator\Favorites
12:16:56.1496...	IEEXPLORE.EXE	1408	CloseFile	C:\Documents and Settings\Administrator\Favorites
12:16:56.1499...	IEEXPLORE.EXE	1408	CreateFile	C:\Documents and Settings\Administrator\LOCAL SETTINGS
12:16:56.1499...	IEEXPLORE.EXE	1408	QueryDirectory	C:\Documents and Settings\Administrator\Local Settings
12:16:56.1499...	IEEXPLORE.EXE	1408	QueryDirectory	C:\Documents and Settings\Administrator\Local Settings
12:16:56.1503...	IEEXPLORE.EXE	1408	CloseFile	C:\Documents and Settings\Administrator\Local Settings
12:16:56.1504...	IEEXPLORE.EXE	1408	CreateFile	C:\Documents and Settings\Administrator\Local Settings\History
12:16:56.1504...	IEEXPLORE.EXE	1408	QueryDirectory	C:\Documents and Settings\Administrator\Local Settings\History
12:16:56.1508...	IEEXPLORE.EXE	1408	QueryDirectory	C:\Documents and Settings\Administrator\Local Settings\History
12:16:56.1509...	IEEXPLORE.EXE	1408	CloseFile	C:\Documents and Settings\Administrator\Local Settings\History
12:16:56.1514...	IEEXPLORE.EXE	1408	CreateFile	C:\Documents and Settings\Administrator\Local Settings\History\History.IE5
12:16:56.1514...	IEEXPLORE.EXE	1408	QueryDirectory	C:\Documents and Settings\Administrator\Local Settings\History\History.IE5
12:16:56.1516...	IEEXPLORE.EXE	1408	QueryDirectory	C:\Documents and Settings\Administrator\Local Settings\History\History.IE5
12:16:56.1523...	IEEXPLORE.EXE	1408	CloseFile	C:\Documents and Settings\Administrator\Local Settings\History\History.IE5
12:16:56.1524...	IEEXPLORE.EXE	1408	CreateFile	C:\Documents and Settings\Administrator\Local Settings\TEMPORARY INTERNET FILES
12:16:56.1524...	IEEXPLORE.EXE	1408	QueryDirectory	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files
12:16:56.1524...	IEEXPLORE.EXE	1408	QueryDirectory	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files
12:16:56.1525...	IEEXPLORE.EXE	1408	CloseFile	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files
12:16:56.1526...	IEEXPLORE.EXE	1408	CreateFile	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5
12:16:56.1526...	IEEXPLORE.EXE	1408	QueryDirectory	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5
12:16:56.1527...	IEEXPLORE.EXE	1408	QueryDirectory	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5
12:16:56.1529...	IEEXPLORE.EXE	1408	CloseFile	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5
12:16:56.1530...	IEEXPLORE.EXE	1408	CreateFile	C:\Documents and Settings\ALL USERS
12:16:56.1530...	IEEXPLORE.EXE	1408	QueryDirectory	C:\Documents and Settings\All Users
12:16:56.1531...	IEEXPLORE.EXE	1408	QueryDirectory	C:\Documents and Settings\All Users
12:16:56.1531...	IEEXPLORE.EXE	1408	CloseFile	C:\Documents and Settings\All Users
12:16:56.1531...	IEEXPLORE.EXE	1408	CreateFile	C:\Documents and Settings\All Users\APPLICATION DATA
12:16:56.1532...	IEEXPLORE.EXE	1408	QueryDirectory	C:\Documents and Settings\All Users\Application Data
12:16:56.1532...	IEEXPLORE.EXE	1408	QueryDirectory	C:\Documents and Settings\All Users\Application Data
12:16:56.1532...	IEEXPLORE.EXE	1408	CloseFile	C:\Documents and Settings\All Users\Application Data
12:16:56.1533...	IEEXPLORE.EXE	1408	CreateFile	C:\PROGRAM FILES
12:16:56.1533...	IEEXPLORE.EXE	1408	QueryDirectory	C:\Program Files

Il processo sembra legittimo poichè come si vede dallo screen va a caricare tutti gli eventuali cookie , cache e preferiti presenti sul nostro computer, quindi deduco che si tratta assolutamente del browser della microsoft internet explorer, e comunque non vedo azioni maligne da parte del processo.

Per sicurezza effettuo un'altra prova con un software della microsoft che si chiama **Microsoft File Checksum Integrity Verifier**

Così andrò a calcolare l'hash di del file e verificarlo su virustotal:

Microsoft File Checksum Integrity Verifier

Important! Selecting a language below will dynamically change the complete page content to that language.

Language:

English

Download

The Microsoft File Checksum Integrity Verifier tool is an unsupported command line utility that computes MD5 or SHA1 cryptographic hashes for files.

Calcolo l'hash del file con il programma :

```
C:\Program Files\Internet Explorer>fciv IEXPLORE.exe -sha1
File Checksum Integrity Verifier version 2.05.
58e80c90bf54850b5f3ccbd8edf0877537e0ea8e iexplore.exe
C:\Program Files\Internet Explorer>
```

Verifico l'hash del file su virustotal, in questo modo controllo anche la scansione dei virus :

0
/ 71

Community Score

File distributed by Microsoft

814a37d89a79aa3975308e723bc1a3a67360323b7e3584de00896fe7c59bbb8e

Size: 91.00 KB

Last Analysis Date: 1 month ago

EXE

peexe

known-distributor

trusted

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY 15

Basic properties

MD5	55794b97a7faabd2910873c85274f409
SHA-1	58e80c90bf54850b5f3ccbd8edf0877537e0ea8e
SHA-256	814a37d89a79aa3975308e723bc1a3a67360323b7e3584de00896fe7c59bbb8e
Vhash	0940366d155az2b01gz11z1fz1
Authenticash	f173fd99db212a5c686a123f32d2de6ce8a8f3699aea14a986a23ce5c125a263
Imphash	b06090332cc8fb8aeb9b846fdd7ff33c
Rich PE header hash	acd22b07f3faa1c5ecfa9d8f4a53a0ba
SSDEEP	1536:PgkByI4BcDQX2oooD+AyxArAlVJ9bayZbScKEang5Kmp:xel46QXMmAIX1tanUKmp
TLSH	T18E93B252FA14ED61CA9C08305867CBA41820BC72DB119BE776F0BB1FAD363D37A35619
File type	Win32 EXE executable windows win32 pe peexe
Magic	PE32 executable (GUI) Intel 80386, for MS Windows
TrID	Win32 Executable MS Visual C++ (generic) (47.3%) Win64 Executable (generic) (15.9%) Win32 Dynamic Link Library (generic) (9.9%) Win16 NE executable (generic) (7.6%) Win32 Executable (generic) (6.8%)
DetectItEasy	PE32 Compiler: EP:Microsoft Visual C/C++ (2005) [EXE32] Compiler: Microsoft Visual C/C++ (2003) Linker: Microsoft Linker (7.10*) [GUI32]
File size	91.00 KB (93184 bytes)

L'hash(SHA1) risulta uguale al programma della microsoft che ha comparato il file, quindi il file è sicuro.

Compito di Mendolia Valerio