

Report UNIT3 WEEK 10

ANALISI STATICA E DINAMICA BASICA

Non avendo connessione internet sulla macchina vado a calcolare l'hash del file con **md5deep**.

```
Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>cd Desktop
C:\Documents and Settings\Administrator\Desktop>cd MALW
C:\Documents and Settings\Administrator\Desktop\MALW>cd md5deep-4.3
C:\Documents and Settings\Administrator\Desktop\MALW\md5deep-4.3>dir
Volume in drive C has no label.
Volume Serial Number is 9430-816D

Directory of C:\Documents and Settings\Administrator\Desktop\MALW\md5deep-4.3

07/03/2023  12:26 PM    <DIR>          .
07/03/2023  12:26 PM    <DIR>          ..
07/03/2023  12:26 PM             17,715  CHANGES.txt
07/03/2023  12:26 PM             19,422  COPYING.txt
07/03/2023  12:26 PM              2,261  FILEFORMAT.txt
07/03/2023  12:26 PM             800,256  hashdeep.exe
07/03/2023  12:26 PM             12,291  HASHDEEP.txt
07/03/2023  12:26 PM             988,160  hashdeep64.exe
07/03/2023  12:26 PM             800,256  md5deep.exe
07/03/2023  12:26 PM             14,717  MD5DEEP.txt
07/03/2023  12:26 PM             988,160  md5deep64.exe
07/03/2023  12:26 PM             800,256  sha1deep.exe
07/03/2023  12:26 PM             988,160  sha1deep64.exe
07/03/2023  12:26 PM             800,256  sha256deep.exe
07/03/2023  12:26 PM             988,160  sha256deep64.exe
07/03/2023  12:26 PM             800,256  tigerdeep.exe
07/03/2023  12:26 PM             988,160  tigerdeep64.exe
07/03/2023  12:26 PM             800,256  whirlpooldeep.exe
07/03/2023  12:26 PM             988,160  whirlpooldeep64.exe
               17 File(s)          10,796,902 bytes
               2 Dir(s)          5,709,873,152 bytes free
```

L'hash risulta essere **c0b54534e188e1392f28d17faff3d454**.

```
C:\Documents and Settings\Administrator\Desktop\MALW\md5deep-4.3>md5deep "c:\Documents and Settings\Administrator\Desktop\MALW\Esercizio_Pratico_U3_W2_L5\Malware_U3_W2_L5.exe"
c0b54534e188e1392f28d17faff3d454  c:\Documents and Settings\Administrator\Desktop\MALW\Esercizio_Pratico_U3_W2_L5\Malware_U3_W2_L5.exe
```

Apro il browser su una macchina con internet e vado a fare una scansione dell'hash del file.



Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

FILE	URL	SEARCH
------	-----	--------



Search for a hash, domain, IP address, URL or gain additional context and threat landscape visibility with **VT ENTERPRISE**.

c0b54534e188e1392f28d17faff3d454

39
/ 71

Community Score

39 security vendors and no sandboxes flagged this file as malicious

b71777edbf21167c96d20ff803cbcb25d24b94b3652db2f286dcd6efd3d8416a

Lab01-02.exe.exe

peexe checks-network-adapters runtime-modules armadillo direct-cpu-clock-access

Il file è etichettato comunemente come trojan, un tipo di malware progettato per infiltrarsi nel sistema senza il consenso dell'utente.

Popular threat label (1) trojan.r002c0pdm21

Threat categories trojan

Family labels r002c0pdm21

Con le informazioni ricavate possiamo fare un'ipotesi iniziale sul comportamento del file.

peexe fa riferimento al tipo di file eseguibile PE (Portable Executable) in Windows.

check-network-adapters verifica le schede di rete presenti per configurazione o monitoraggio.

runtime-modules indica i moduli o componenti (funzioni o librerie) che il file utilizza durante l'esecuzione.

armadillo è un programma usato per crittografare, il file potrebbe essere criptato.

direct-cpu-clock-access accede direttamente al clock della CPU manipolandolo o controllandolo.

Andando ad analizzare i dettagli dell'hash inserita nel sito, vengono forniti dettagli e stime riguardo il file, incluse librerie importate e sezioni.

Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5	Chi2
.text	4096	19064	20480	6.37	4b8aaeb128744c00b1f9b29dd120616e	196535.5
.rdata	24576	2398	4096	3.66	e5e39acc53e64c50fa5a35693a911478	304856
.data	28672	16136	12288	0.7	305514f6ece00473b7f8bc023f57e15	2765274

Imports

+ KERNEL32.dll
+ WININET.dll

Si possono visualizzare molti altri dettagli riguardo questa scansione, incluso il comportamento del file una volta eseguito in sandbox.

Da windows XP utilizzo il comando **strings** nel cmd per ricavare le stringhe del file.

```
C:\Documents and Settings\Administrator\Desktop\MALW\SysinternalsSuite>strings "
c:\Documents and Settings\Administrator\Desktop\MALW\Esercizio_Pratico_U3_W2_L5\
Malware_U3_W2_L5.exe"
```

```
Microsoft Visual C++ Runtime Library
Runtime Error!
Program:
...
<program name unknown>
GetLastActivePopup
GetActiveWindow
MessageBoxA
user32.dll
nQe
nQE
'RE
&RE
Sleep
KERNEL32.dll
InternetGetConnectedState
InternetReadFile
InternetCloseHandle
InternetOpenUrlA
InternetOpenA
WININET.dll
GetCommandLineA
GetVersion
ExitProcess
TerminateProcess
GetCurrentProcess
UnhandledExceptionFilter
GetModuleFileNameA
FreeEnvironmentStringsA
FreeEnvironmentStringsW
WideCharToMultiByte
GetEnvironmentStrings
GetEnvironmentStringsW
SetHandleCount
GetStdHandle
GetFileType
GetStartupInfoA
GetModuleHandleA
GetEnvironmentVariableA
GetVersionExA
HeapDestroy
HeapCreate
VirtualFree
HeapFree
RtlUnwind
WriteFile
HeapAlloc
GetCPIInfo
GetACP
GetOEMCP
VirtualAlloc
HeapReAlloc
GetProcAddress
LoadLibraryA
GetLastError
FlushFileBuffers
SetFilePointer
MultiByteToWideChar
LCMapStringA
LCMapStringW
GetStringTypeA
GetStringTypeW
SetStdHandle
CloseHandle
d5p
Error 1.1: No Internet
Success: Internet Connection
Error 2.3: Fail to get command
Error 2.2: Fail to ReadFile
Error 2.1: Fail to OpenUrl
http://www.practicalmalwareanalysis.com/cc.htm
Internet Explorer 7.5/pma
Success: Parsed command is %c
```

Le stringhe includono diverse funzioni di librerie di sistema di Windows, tuttavia alcune sembrano sospette.

La presenza delle funzioni **LoadLibraryA** e **GetProcAddress** fanno riferimento a funzioni importate a tempo di esecuzione (runtime) dove viene chiamata una determinata funzione solo all'occorrenza per risultare quanto meno invasivi e rilevabili possibile.

Viene caricata la libreria **user32.dll** in runtime per interagire con l'interfaccia utente di Windows. Le stringhe suggeriscono che il file potrebbe mostrare finestre di dialogo o messaggi all'utente utilizzando le funzioni come **GetLastActivePopup** e **MessageBoxA**. Inoltre, potrebbe analizzare la riga di comando con la stringa **GetCommandLineA** e utilizzare funzioni per la gestione delle risorse di sistema come **SetStdHandle**, **CloseHandle** e **FlushFileBuffers**.

Le funzioni **InternetOpenA**, **InternetReadFile** e **InternetCloseHandle** vengono utilizzate insieme alla libreria **Wininet.dll**. Questo suggerisce un possibile tentativo del malware di connettersi a risorse esterne tramite Internet. Queste funzioni consentono l'apertura di una connessione, la lettura di file e la chiusura delle risorse di connessione.

Le varie stringhe **Success** e **Error** sembrano essere utilizzate per gestire il flusso di esecuzione del malware in base alle operazioni di connessione eseguite. Potrebbero indicare se le operazioni di connessione hanno avuto successo o sono fallite, influenzando così le azioni successive del malware.

La stringa <http://www.practicalmalwareanalysis.com/cc.htm> sembra essere un URL che potrebbe indicare che il file sta cercando di connettersi a un server remoto. Questo potrebbe essere un tentativo del file di ottenere istruzioni o di scaricare ulteriori componenti dannosi.

La stringa **internet explorer 7.5/pma** sembra essere un'informazione relativa all'applicazione o all'ambiente in cui viene eseguito il malware, ma potrebbe anche essere un tentativo di mascherare l'attività dannosa facendola apparire come un normale comportamento di Internet Explorer.

Infine, la stringa **success parsed command is %c** indica che il malware ha analizzato un comando specifico.

Successivamente vado a ricavare informazioni dall'header dell'eseguibile con **CFF Explorer**.

In **Section Headers** vengono mostrate le sezioni.

.text contiene le istruzioni (righe di codice) che la CPU eseguirà una volta che il software sarà avviato.

.rdata include informazioni su librerie e funzioni importate dall'eseguibile.

.data contiene dati/variabili globali del programma, accessibili da qualsiasi funzione all'interno dell'eseguibile.

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

In **Import Directories** vengono mostrate le librerie importate dinamicamente.

KERNEL32.dll contiene le funzioni principali per interagire con il sistema operativo.

WININET.dll contiene le funzioni per l'implementazione di alcuni protocolli di rete (HTTP, FTP, NTP).

Malware_U3_W2_L5.exe						
Module Name	Imports	OFTs	TimeDateStamp	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

Andando a cliccare sopra le librerie si possono analizzare le funzioni importate da ognuna di essa.

Da **KERNEL32.dll**:

Dword	Dword	Word	szAnsi				
000065E4	000065E4	0296	Sleep	00006796	00006796	0115	GetFileType
00006940	00006940	027C	SetStdHandle	000067A4	000067A4	0150	GetStartupInfoA
0000692E	0000692E	0156	GetStringTypeW	000067B6	000067B6	0126	GetModuleHandleA
0000691C	0000691C	0153	GetStringTypeA	000067CA	000067CA	0109	GetEnvironmentVariableA
0000690C	0000690C	01C0	LCMapStringW	000067E4	000067E4	0175	GetVersionExA
000068FC	000068FC	01BF	LCMapStringA	000067F4	000067F4	019D	HeapDestroy
000068E6	000068E6	01E4	MultiByteToWideChar	00006802	00006802	019B	HeapCreate
00006670	00006670	00CA	GetCommandLineA	00006810	00006810	02BF	VirtualFree
00006682	00006682	0174	GetVersion	0000681E	0000681E	019F	HeapFree
00006690	00006690	007D	ExitProcess	0000682A	0000682A	022F	RtlUnwind
0000669E	0000669E	029E	TerminateProcess	00006836	00006836	02DF	WriteFile
000066B2	000066B2	00F7	GetCurrentProcess	00006842	00006842	0199	HeapAlloc
000066C6	000066C6	02AD	UnhandledExceptionFilter	0000684E	0000684E	00BF	GetCPInfo
000066E2	000066E2	0124	GetModuleFileNameA	0000685A	0000685A	00B9	GetACP
000066F8	000066F8	00B2	FreeEnvironmentStringsA	00006864	00006864	0131	GetOEMCP
00006712	00006712	00B3	FreeEnvironmentStringsW	00006870	00006870	02BB	VirtualAlloc
0000672C	0000672C	02D2	WideCharToMultiByte	00006880	00006880	01A2	HeapReAlloc
00006742	00006742	0106	GetEnvironmentStrings	0000688E	0000688E	013E	GetProcAddress
0000675A	0000675A	0108	GetEnvironmentStringsW	000068A0	000068A0	01C2	LoadLibraryA
00006774	00006774	026D	SetHandleCount	000068B0	000068B0	011A	GetLastError
00006786	00006786	0152	SetStdHandle	000068C0	000068C0	00AA	FlushFileBuffers
				000068D4	000068D4	026A	SetFilePointer
				00006950	00006950	001B	CloseHandle

Oltre alle funzioni menzionate precedentemente con l'analisi delle stringhe, molte altre potrebbero essere sfruttate.

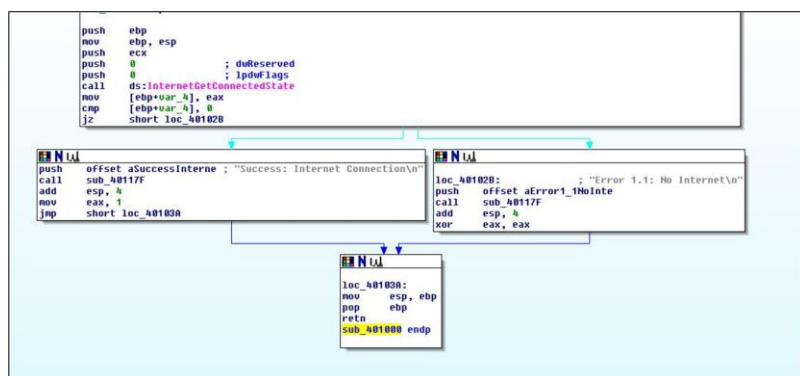
- **Sleep** per introdurre ritardi nell'esecuzione del file al fine di evitare la rilevazione o rallentare le analisi.
- **GetStringTypeW** e **GetStringTypeA** per manipolare o analizzare le stringhe all'interno del file al fine di eseguire operazioni di crittografia, decodifica o analisi.
- **LCMapStringW** e **LCMapStringA** per manipolare le conversioni di caratteri al fine di mascherare o modificare testo o codice all'interno del malware.
- **MultiByteToWideChar** per convertire stringhe multibyte in formato wide (Unicode) al fine di manipolare o nascondere informazioni all'interno del malware.
- **GetVersion** per ottenere informazioni sulla versione del sistema operativo al fine di adattare le azioni del file a specifiche versioni di sistema o per identificare potenziali vulnerabilità.
- **ExitProcess** e **TerminateProcess** per terminare il processo in cui il file è in esecuzione al fine di interrompere il funzionamento normale del sistema o per evitare la rilevazione.
- **GetCurrentProcess** per ottenere l'handle del processo corrente al fine di per ottenere informazioni sul processo stesso o per eseguire azioni specifiche in relazione al processo corrente.
- **GetModuleFileNameA** per ottenere il percorso completo del file eseguibile del modulo corrente al fine di ottenere informazioni sul percorso del malware o per manipolare la sua posizione.
- **GetEnvironmentVariableA** per ottenere il valore di una variabile d'ambiente specificata al fine di acquisire informazioni sensibili o per adattare il comportamento del malware in base alle variabili d'ambiente presenti nel sistema.
- **GetLastError** per ottenere il codice dell'ultimo errore verificatosi al fine di gestire errori o per generare messaggi di log nel malware.
- **WriteFile** per scrivere dati su un file o un altro tipo di handle al fine di eseguire operazioni di scrittura dannose o per sovrascrivere file esistenti.
- **CloseHandle** per chiudere l'handle di un oggetto del sistema operativo al fine di rilasciare risorse o nascondere l'attività del malware.

Da **WININET.dll**:

Dword	Dword	Word	szAnsi
00006640	00006640	0071	InternetOpenUrlA
0000662A	0000662A	0056	InternetCloseHandle
00006616	00006616	0077	InternetReadFile
000065FA	000065FA	0066	InternetGetConnectedState
00006654	00006654	006F	InternetOpenA

Oltre alle funzioni già menzionate precedentemente, sia **InternetGetConnectedState** che **InternetOpenA** possono essere utilizzate per facilitare attività dannose come il trasferimento di dati sensibili, l'infiltrazione di malware aggiuntivo o la comunicazione con server remoti per scopi malevoli.

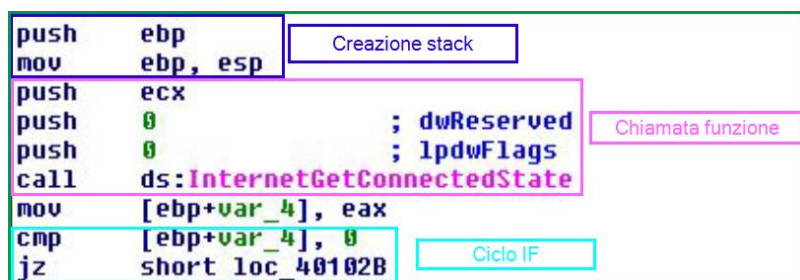
ANALISI ASSEMBLY



Viene inizializzato lo stack per la funzione, **InternetGetConnectedState** è una funzione della libreria **WININET.dll** in ambienti Windows. Viene usata per determinare se l'utente ha una connessione internet attiva.

Questa funzione confronta i parametri, se il risultato è uguale a zero salta alla funzione **loc_40102B** (print "**Error 1.1: No Internet**") che chiama la **sub_40117F**. In seguito, vengono puliti gli argomenti dallo stack e con xor viene impostato EAX a 0.

Se il risultato è diverso da zero salta alla funzione **loc_40102B** (print "**Success: Internet Connection**"), vengono puliti gli argomenti dallo stack e viene impostato EAX a 1. Successivamente fa un jump a **loc_40103A** che ripristina lo stato dello stack ed esegue la funzione di **retn** (return) che termina la funzione **sub_401000(endp)**.



CREAZIONE STACK

push ebp

Inserisce il valore di EBP (base point register) nello stack. Crea un frame pointer per accedere ai parametri e alle variabili locali.

mov ebp, esp

Collega il frame pointer allo stack, copiando il valore di ESP (stack point register) in EBP.

CHIAMATA FUNZIONE

push ecx

Inserisce il valore di ECX (extended counter register) nello stack.

push 0 ; dwReserved

Inserisce il valore 0 nello stack come argomento preparatore per la funzione "InternetGetConnectedState".

Questo valore corrisponde a dwReserved.

push 0 ; lpdwFlags

Inserisce il valore 0 nello stack come argomento preparatore per la funzione "InternetGetConnectedState".

Questo valore corrisponde a lpdwFlags.

call ds:InternetGetConnectedState

Chiama la funzione **InternetGetConnectedState** dal segmento DS (Data Segment) per verificare lo stato della connessione Internet.

CICLO IF

cmp [ebp+var_4], 0

Confronta il valore della variabile locale [ebp+var_4] con 0.

jz short loc_40102B

Salta all'indirizzo loc_40102B se il risultato del confronto precedente è uguale a zero.



CHIAMATA FUNZIONE

push offset aSuccessInterne

Push dell'offset della stringa "Success: Internet Connection\n" nello stack.

call sub_40105F

Chiama la funzione sub_40105F per eseguire l'output se la condizione precedente risulta [ebp+var_4] != 0.

PULIZIA STACK

Add esp, 4

Ripristina l'indicatore dello stack dai valori pushati per continuare con le istruzioni successive.

ASSEGNAZIONE VALORE E SALTO

mov eax, 1

Imposta EAX a 1.

jmp short loc_40103A

Salta all'indirizzo loc_40103A.

loc_40102B:		; "Error 1.1: No Internet\n"
push	offset aError1_1NoInte	Chiamata funzione
call	sub_40117F	
add	esp, 4	Pulizia stack
xor	eax, eax	Assegnazione valore

CHIAMATA FUNZIONE

push offset aError1_1NoInte

Push dell'offset della stringa "Error 1.1: No Internet\n" nello stack.

call sub_40117F

Chiama la funzione sub_40117F per eseguire l'output se la condizione precedente risulta $[ebp+var_4] = 0$.

PULIZIA STACK

add esp, 4

Ripristina l'indicatore dello stack dai valori pushati per continuare con le istruzioni successive.

ASSEGNAZIONE VALORE

xor eax, eax

Imposta EAX a 0.

loc_40103A:		
mov	esp, ebp	Pulizia stack
pop	ebp	
retn		
sub_401000	endp	Ritorno alla main

PULIZIA STACK

mov esp, ebp

Ripristina il puntatore dello stack alla posizione iniziale copiando il valore di EBP in ESP.

pop ebp

Ripristina il valore originale di EBP prima di terminare l'esecuzione della funzione.

RITORNO ALLA MAIN

retn

Termina la funzione in questo punto consentendo di continuare dall'istruzione successiva alla chiamata originale.

sub_401000 endp

Indica la fine del blocco di codice della funzione.

CODICE IN C DA ASSEMBLY

```
#include <stdio.h>
#include <wininet.h>

void sub_401000() {
    int var_4;

    int dwReserved = 0;
    int lpdwFlags = 0;

    InternetGetConnectedState(&lpdwFlags, dwReserved);

    var_4 = lpdwFlags;

    if (var_4 == 0) {
        printf("Success: Internet Connection\n");
    } else {
        printf("Error 1.1: No Internet\n");
    }
}

int main() {
    sub_401000();


    return 0;
}
```

BONUS ANALISI STATICA

Ricavo l’hash di IEXPLORER.exe su **CFF Explorer**.


IEXPLORE.EXE	
Property	Value
File Name	C:\Program Files\Internet Explorer\IEXPLORE.EXE
File Type	Portable Executable 32
File Info	No match found.
File Size	623.84 KB (638816 bytes)
PE Size	618.00 KB (632832 bytes)
Created	Wednesday 14 June 2023, 11.29.55
Modified	Wednesday 29 January 2020, 05.40.36
Accessed	Friday 07 July 2023, 15.06.52
MD5	B60DDDD2D63CE41CB8C487FCFB66419E
SHA-1	EADCE51C88C8261852C1903399DDE742FBA2061B

In seguito, faccio una ricerca su **VirusTotal**.



Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

FILEURLSEARCH



Search for a hash, domain, IP address, URL or gain additional context and threat landscape visibility with VT ENTERPRISE.

b60ddddd2d63ce41cb8c487fcb66419e

Non risulta malevolo.

0 / 70

Community Score

No security vendors and no sandboxes flagged this file as malicious

b18a0d4beba606bf305010ba3c72abafac80d5f303a8bfb24d77b78b786e6
IEXPLORE.EXE

peexe via-tor overlay runtime-modules signed detect-debug-environment idle

Da CFF analizzo le sezioni.

Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
.text	00009E65	00001000	0000A000	00000400	00000000	00000000	0000	0000	60000020
.data	00000660	0000B000	00000800	0000A400	00000000	00000000	0000	0000	C0000040
.rsrc	0008EE18	0000C000	0008F000	0000AC00	00000000	00000000	0000	0000	40000040
.reloc	00000B04	0009B000	00000C00	00099C00	00000000	00000000	0000	0000	42000040

Successivamente analizzo le librerie importate.

ADVAPI32.dll	9	0000A2CC	00000000	00000000	0000A250	00001000
KERNEL32.dll	63	0000A2F4	00000000	00000000	0000A25E	00001028
USER32.dll	6	0000A3F4	00000000	00000000	0000A26C	00001128
msvcrt.dll	29	0000A410	00000000	00000000	0000A278	00001144
ntdll.dll	1	0000A488	00000000	00000000	0000A284	000011BC
SHLWAPI.dll	18	0000A490	00000000	00000000	0000A28E	000011C4
SHELL32.dll	2	0000A4DC	00000000	00000000	0000A29A	00001210
ole32.dll	2	0000A4E8	00000000	00000000	0000A2A6	0000121C
iertutil.dll	14	0000A4F4	00000000	00000000	0000A2B0	00001228
urlmon.dll	3	0000A530	00000000	00000000	0000A2BE	00001264

Entrambe sembrano rispecchiare quelle del file legittimo.

Utilizzo il comando **strings** nel cmd per ricavare le stringhe del file.

VirusTotal ha verificato la firma digitale ritenendola attendibile, si riscontra lo stesso risultato dall'analisi delle stringhe del file. Una firma digitale è una forma di autenticazione e verifica dell'integrità di un file, e una firma valida indica che il file non è stato alterato e che l'autore è identificato correttamente.

Il file è protetto da copyright e appartiene a Microsoft Corporation. Il nome originale è IEXPLORE.EXE, comunemente associato a Internet Explorer (browser web sviluppato da Microsoft). Anche il nome del prodotto (Windows Internet Explorer) e la versione del prodotto corrispondono ad una versione lecita.

LegalCopyright
Microsoft Corporation. All rights reserved.
OriginalFilename
IEXPLORE.EXE
ProductName
Windows
Internet Explorer
ProductVersion
8.00.6001.18702
VarFileInfo
Translation
WEUT_TEMPLATE
MUI
MUI
en-US

Signature info ⓘ

Signature Verification

✔ Signed file, valid signature

File Version Information

Copyright © Microsoft Corporation. All rights reserved.
Product Windows® Internet Explorer
Description Internet Explorer
Original Name IEXPLORE.EXE
Internal Name iexplore
File Version 8.00.6001.18702 (longhorn_ie8_rtm(wmbla).090308-0339)
Date signed 2009-03-08 20:09:00 UTC

I link conducono a siti web ufficiali di Microsoft, contengono informazioni sulle certificazioni e certificati di sicurezza (CRL Certificate Revocation List). Questi vengono usati per verificare l'autenticità e l'integrità dei file firmati Microsoft.

3http://crl.microsoft.com/pki/crl/products/CSPCA.crl0H
<0:08
,http://www.microsoft.com/pki/certs/CSPCA.crt0

3http://crl.microsoft.com/pki/crl/products/tspca.crl0H
<0:08
,http://www.microsoft.com/pki/certs/tspca.crt0

Anche analizzando le proprietà del processo in esecuzione possiamo vedere come sia verificato.

Image File

Internet Explorer
(Verified) Microsoft Corporation
Version: 8.0.6001.18702
Build Time: Sun Mar 08 12:34:06 2009□
Path:
C:\Program Files\Internet Explorer\IEXPLORE.EXE
Command line:
"C:\Program Files\Internet Explorer\IEXPLORE.EXE"
Current directory:
C:\Documents and Settings\Administrator\Desktop\
Autostart Location:
HKLM\SOFTWARE\Classes\Htmlfile\Shell\Open\Command(Default)

Image File

Internet Explorer
(Verified) Microsoft Corporation
Version: 8.0.6001.18702
Build Time: Sun Mar 08 12:34:06 2009□
Path:
C:\Program Files\Internet Explorer\IEXPLORE.EXE
Command line:
"C:\Program Files\Internet Explorer\IEXPLORE.EXE" SCODEF:168 CREDAT:14337
Current directory:
C:\Documents and Settings\Administrator\Desktop\
Autostart Location:
HKLM\SOFTWARE\Classes\Htmlfile\Shell\Open\Command(Default)

IEXPLORE Properties

General Version Compatibility Digital Signatures Summary

Signature list

Name of signer:	E-mail address:	Timestamp
Microsoft Corporation	Not available	Sunday, March 08, 2...

BONUS ANALISI DINAMICA

Su Windows XP avvio **Process Monitor** e ne analizzo il comportamento.

Il prefetching anticipa quali risorse web un utente potrebbe richiedere successivamente per precargarle in background.

IEEXPLORE.EXE	168	CloseFile	C:\WINDOWS\WindowsShell.Manifest
IEEXPLORE.EXE	168	CreateFile	C:\WINDOWS\system32\comctl32.dll
IEEXPLORE.EXE	168	CreateFileMap...	C:\WINDOWS\system32\comctl32.dll
IEEXPLORE.EXE	168	QueryStandardl...	C:\WINDOWS\system32\comctl32.dll
IEEXPLORE.EXE	168	CreateFileMap...	C:\WINDOWS\system32\comctl32.dll
IEEXPLORE.EXE	168	CreateFile	C:\WINDOWS\system32\comctl32.dll.124.Manifest
IEEXPLORE.EXE	168	CreateFile	C:\WINDOWS\system32\comctl32.dll.124.Config
IEEXPLORE.EXE	168	CloseFile	C:\WINDOWS\system32\comctl32.dll
IEEXPLORE.EXE	168	QueryNameInfo...	C:\Program Files\Internet Explorer\IEEXPLORE.EXE
IEEXPLORE.EXE	168	QueryNameInfo...	C:\Program Files\Internet Explorer\IEEXPLORE.EXE
IEEXPLORE.EXE	168	SetEndOfFileIn...	C:\WINDOWS\system32\config\software.LOG
IEEXPLORE.EXE	168	SetEndOfFileIn...	C:\WINDOWS\system32\config\software.LOG
IEEXPLORE.EXE	168	CreateFile	C:\WINDOWS\system32\urlmon.dll.123.Manifest
IEEXPLORE.EXE	168	CreateFile	C:\WINDOWS\system32\urlmon.dll.123.Config

Vengono poi caricate le librerie necessarie per il funzionamento del browser. (come user32.dll, kernel32.dll, wininet.dll, ecc.) per svolgere varie funzioni.

Successivamente vengono eseguite query relative alla lettura di file temporanei dal percorso della cache di Internet Explorer, archiviando temporaneamente i file scaricati, le immagini, i cookie e altre risorse in una cache locale.

IEEXPLORE.EXE	168	QueryOpen	C:\Program Files\Internet Explorer\IEEXPLORE.EXE.Local
IEEXPLORE.EXE	168	QueryOpen	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
IEEXPLORE.EXE	168	CreateFile	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files
IEEXPLORE.EXE	168	QueryOpen	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files
IEEXPLORE.EXE	168	QueryOpen	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files
IEEXPLORE.EXE	168	CreateFile	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files
IEEXPLORE.EXE	168	SetBasicInfor...	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files
IEEXPLORE.EXE	168	CloseFile	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files
IEEXPLORE.EXE	168	QueryOpen	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\desktop.ini
IEEXPLORE.EXE	168	QueryOpen	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5
IEEXPLORE.EXE	168	QueryOpen	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5
IEEXPLORE.EXE	168	CreateFile	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5
IEEXPLORE.EXE	168	SetBasicInfor...	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5
IEEXPLORE.EXE	168	CloseFile	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5
IEEXPLORE.EXE	168	QueryOpen	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\desktop.ini

Vengono poi eseguite query relative alla lettura, scrittura o cancellazione dei cookies da parte di Internet Explorer.

IEEXPLORE.EXE	168	QueryOpen	C:\Documents and Settings\Administrator\Cookies
IEEXPLORE.EXE	168	CreateFile	C:\Documents and Settings\Administrator\Cookies
IEEXPLORE.EXE	168	SetBasicInfor...	C:\Documents and Settings\Administrator\Cookies
IEEXPLORE.EXE	168	CloseFile	C:\Documents and Settings\Administrator\Cookies
IEEXPLORE.EXE	168	CreateFile	C:\Documents and Settings\Administrator\Cookies\index.dat
IEEXPLORE.EXE	168	SetBasicInfor...	C:\Documents and Settings\Administrator\Cookies\index.dat
IEEXPLORE.EXE	168	CloseFile	C:\Documents and Settings\Administrator\Cookies\index.dat
IEEXPLORE.EXE	168	QueryStandardl...	C:\Documents and Settings\Administrator\Cookies\index.dat

Tutte le query rispecchiano un comportamento legittimo di Internet Explorer.