

# PROGETTO SETTIMANALE MODULO 8

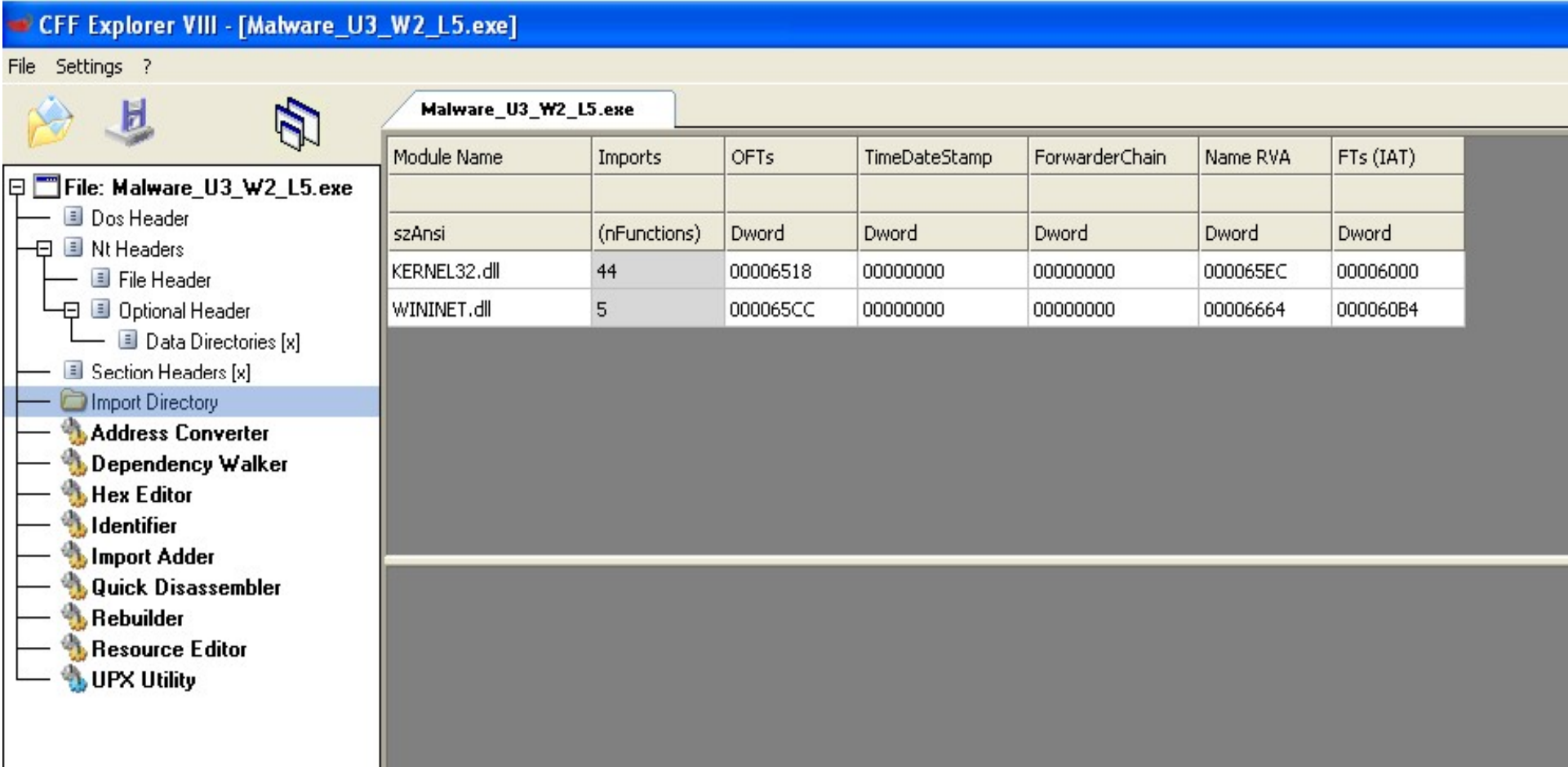
Il progetto di questa settimana ci chiedeva di analizzare il file **Malware\_U3\_W2\_L5** presente nella cartella **Esercizio\_Pratico\_U3\_W2\_L5** e anche di analizzare un **codice assembly x86**.

**Malware\_U3\_W2\_L5:** l'analisi di questo file richiedeva di dare una spiegazione delle librerie che sono state importate dal file eseguibile e delle sezioni di cui si compone il file eseguibile del malware.

**Codice assembly x86:** l'analisi di questo codice richiedeva di identificare i costrutti e di ipotizzare il comportamento della funzionalità implementata.

**Malware\_U3\_W2\_L5:** per analizzare il file in questione ho utilizzato il software CFF Explorer.

## 1) Librerie importate:



CFF Explorer VIII - [Malware\_U3\_W2\_L5.exe]

File Settings ?

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
- Address Converter
- Dependency Walker
- Hex Editor
- Identifier
- Import Adder
- Quick Disassembler
- Rebuilder
- Resource Editor
- UPX Utility

Per vedere le librerie importate sono andato nella sezione **“import Directory”**. E come si può vedere le librerie sono: KERNEL32.dll e WINNET.dll

KERNEL32.dll: questa libreria contiene le funzioni principali per interagire con il sistema operativo: manipolazione di file o gestione della memoria.

WINNET.dll: libreria che contiene le funzioni per l'implementazione di alcuni protocolli di rete come: HTTP,FTP,NTP.

## 2) Sezioni di cui si compone il file eseguibile del malware:



CFF Explorer VIII - [Malware\_U3\_W2\_L5.exe]

File Settings ?

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

File: Malware\_U3\_W2\_L5.exe

- Dos Header
- Nt Headers
  - File Header
  - Optional Header
    - Data Directories [x]
- Section Headers [x]
- Import Directory
- Address Converter
- Dependency Walker
- Hex Editor
- Identifier
- Import Adder
- Quick Disassembler

Nella sezione “**section headers**” si trovano le sezioni di cui è composto il file. Le sezioni sono:

**.text**: contiene le righe di codice che la CPU eseguirà una volta che il software sarà avviato.

**.rdata**: include le informazioni circa le librerie e le informazioni importate ed esportate dal malware.

**.data**: contiene i dati e le variabili globali del malware, che devono essere disponibili a tutte le funzioni del malware.

# Codice Assembly x86

```
push    ebp
mov     ebp, esp
push    ecx
push    0          ; dwReserved
push    0          ; lpdwFlags
call    ds:InternetGetConnectedState
mov     [ebp+var_4], eax
cmp     [ebp+var_4], 0
jz      short loc_40102B
```

```
push    offset aSuccessInterne ; "Success: Internet Connection\n"
call    sub_40117F
add     esp, 4
mov     eax, 1
jmp     short loc_40103A
```

```
loc_40102B:          ; "Error 1.1: No Internet\n"
push    offset aError1_1NoInte
call    sub_40117F
add     esp, 4
xor     eax, eax
```

```
loc_40103A:
mov     esp, ebp
pop     ebp
retn
sub_401000 endp
```

## COSTRUTTI:

1) **push ebp**

**mov ebp,esp**

Queste due istruzioni creano uno stack

2) **push 0**

**push 0**

**call ds:InternetGetConnectedState**

Inserisce due parametri nello stack che serviranno alla funzione InternetGetConnectedState.

3) **cmp [ebp+var\_4],0**

**jz short loc\_40102B**

Queste due righe di codice hanno la sintassi di un ciclo if: se il risultato del “cmp” darà 0 come risultato “jz” salterà all’indirizzo di memoria “short loc\_40102B” altrimenti continuerà in modo graduale.

**4) push offset aSuccessInterne**  
**call sub\_40117F**

Richiama la funzione “sub\_40117F” e mostrerà che la connessione è avvenuta con successo

**5) push offset aError1\_1NotInte**  
**call sub\_40117F**

Richiama la funzione “sub\_40117F” e mostrerà che la connessione NON è avvenuta.

**6) mov esp,ebp**  
**pop ebp**

Queste due istruzioni andranno a fare la pulizia dello stack.

### **Comportamento della funzionalità implementata:**

Da questa porzione di codice si può intuire che il programma verifichi se una macchina è connessa o non connessa a internet.

**BONUS:** ci richiede di fare un'analisi di un file, che un giovane dipendente neo assunto riteneva fosse sospetto, il file in questione è **IEXPLORE.EXE** contenuto nella cartella **C:\Program Files\Internet Explorer**.

Per l'analisi di questo file "sospetto" ho optato per un'analisi dinamica basica:

**1)** Come primo passaggio ho avviato "**Process Explorer**" perché ci permette di avere l'analisi dettagliata di tutti i processi in esecuzione su un sistema.





Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
alg.exe		1,088 K	3,408 K	1804	Application Layer Gateway S...	Microsoft Corporation
apateDNS.exe		18,004 K	4,204 K	2068	Mandiant	Mandiant
cmd	Command Line:	1,920 K	2,348 K	132	Windows Command Processor	Microsoft Corporation
cmd	C:\WINDOWS\System32\alg.exe	1,920 K	2,348 K	200	Windows Command Processor	Microsoft Corporation
csrss	Path:	1,836 K	3,700 K	476	Client Server Runtime Process	Microsoft Corporation
csrss	C:\WINDOWS\system32\alg.exe	1,664 K	4,044 K	3768	Dumpcap	The Wireshark developer ...
exp	Services:	20,524 K	13,724 K	1728	Windows Explorer	Microsoft Corporation
exp	Application Layer Gateway Service [ALG]	1,784 K	4,824 K	192	Internet Explorer	Microsoft Corporation
IEXPLORE.EXE		4,388 K	11,776 K	2788	Internet Explorer	Microsoft Corporation
IEXPLORE.EXE		472 K	1,980 K	180	Intel® PROSet Monitoring S...	Intel Corporation
IPROSetMonitor.exe		3,764 K	5,868 K	728	LSA Shell (Export Version)	Microsoft Corporation
lsass.exe		7,148 K	5,800 K	620	Process Monitor	Sysinternals - www.sysinter...
Procmon.exe		26,760 K	412 K	416	Regshot 1.9.0 x86 Unicode	Regshot Team
Regshot-x86-Unicode.exe		1,612 K	3,716 K	716	Services and Controller app	Microsoft Corporation
services.exe		168 K	388 K	332	Windows NT Session Mana...	Microsoft Corporation
smss.exe		4,012 K	6,488 K	1476	Spooler SubSystem App	Microsoft Corporation
spoolsv.exe						

Type	Name
Desktop	\Default
Directory	\KnownDlls
Directory	\Windows
Directory	\BaseNamedObjects
Event	\BaseNamedObjects\crypt32LogoffEvent
Event	\BaseNamedObjects\userenv: User Profile setup event
File	\Device\KsecDD
File	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0...
File	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0...
File	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0...
File	C:\Documents and Settings\Administrator\Desktop
File	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0...
File	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0...
File	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.I...
File	C:\Documents and Settings\Administrator\Cookies\index.dat

## IEXPLORE.EXE:2788 Properties

Threads TCP/IP Security Environment Strings  
Image Performance Performance Graph Disk and Network

## Image File



Internet Explorer

Microsoft Corporation

Version: 6.0.2900.5512

Build Time: Sun Apr 13 19:34:13 2008

Path:

C:\Program Files\Internet Explorer\IEXPLORE.EXE

Explore

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\De

Explore

Parent: explorer.exe(1728)

Verify

User: MALWARE\_TEST\Administrator

Bring to Front

Started: 3:36:32 PM 7/7/2023

Kill Process

Comment:

VirusTotal:

Submit

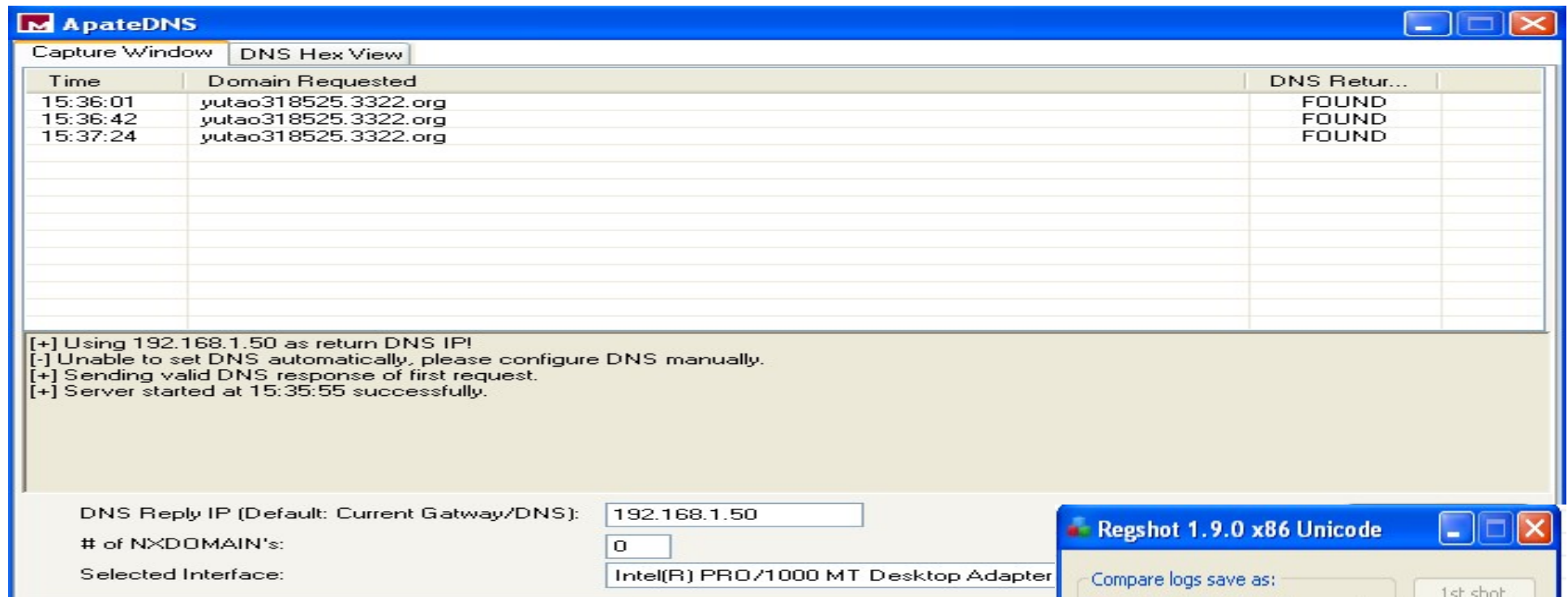
Data Execution Prevention (DEP) Status: Disabled

Control Flow Guard:

OK

Cancel

2) Ho avviato “ApateDNS” ci permette di simulare un server DNS, per intercettare tutte le richieste effettuate dai malware verso i domini di internet.



3) Ho usato il tool “RegShot” che ci permette di paragonare due istantanee di chiavi di registr in due momenti diversi.



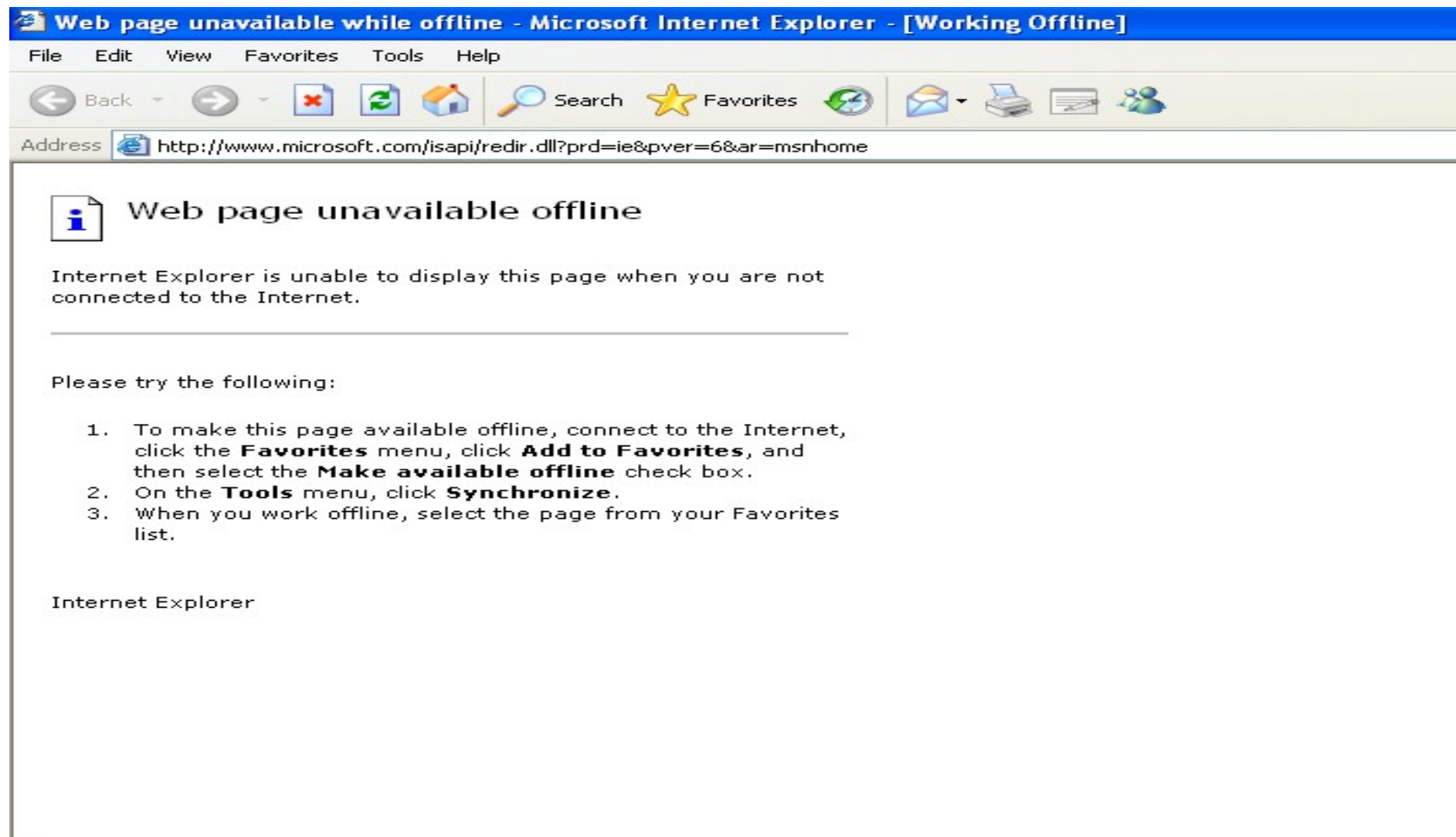
4) Ho avviato procmon, un tool che ci permette di monitorare i processi ed i thread attivi, l'attività di rete l'accesso ai file e le chiamate di sistema effettuata su un sistema operativo e contemporaneamente ho avviato il malware.

Time of Day	Process Name	PID	Operation	Path	Result	Detail
3:47:05.08143...	Explorer.EXE	1728	RegCloseKey	HKCR\exefile\shell\runas	SUCCESS	
3:47:05.08147...	Explorer.EXE	1728	RegCloseKey	HKCR\exefile	SUCCESS	
3:47:05.08151...	Explorer.EXE	1728	RegCloseKey	HKCR\exe	SUCCESS	
3:47:05.08155...	Explorer.EXE	1728	RegCloseKey	HKCR\exefile	SUCCESS	
3:47:05.08158...	Explorer.EXE	1728	RegCloseKey	HKCR\*	SUCCESS	
3:47:05.08603...	IEXPLORE.EXE	536	CloseFile	C:\WINDOWS\Prefetch\IEXPLORE.EXE-27122324.pf	SUCCESS	
3:47:05.08615...	IEXPLORE.EXE	536	CreateFile	C:	SUCCESS	Desired Access: Read
3:47:05.08622...	IEXPLORE.EXE	536	QueryInformationVolume	C:	SUCCESS	VolumeCreationTime: 3
3:47:05.08630...	IEXPLORE.EXE	536	FileSystemControl	C:	SUCCESS	Control: FSCTL_FILE_
3:47:05.08688...	lsass.exe	728	RegOpenKey	HKLM\SECURITY\Policy	SUCCESS	Desired Access: Read
3:47:05.08691...	lsass.exe	728	RegOpenKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	Desired Access: Read
3:47:05.08693...	lsass.exe	728	RegQueryValue	HKLM\SECURITY\Policy\SecDesc\Default	BUFFER OVERFLOW	Length: 12
3:47:05.08698...	lsass.exe	728	RegCloseKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	
3:47:05.08700...	lsass.exe	728	RegOpenKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	Desired Access: Read
3:47:05.08702...	lsass.exe	728	RegQueryValue	HKLM\SECURITY\Policy\SecDesc\Default	SUCCESS	Type: REG_NONE, Le
3:47:05.08706...	lsass.exe	728	RegCloseKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	
3:47:05.08742...	lsass.exe	728	RegCloseKey	HKLM\SECURITY\Policy	SUCCESS	
3:47:05.08748...	Explorer.EXE	1728	RegCloseKey	HKCR\AllFilesystemObjects	SUCCESS	
3:47:05.08753...	Explorer.EXE	1728	RegCloseKey	HKCR\exefile	SUCCESS	
3:47:05.08756...	Explorer.EXE	1728	RegCloseKey	HKCR\*	SUCCESS	
3:47:05.08760...	Explorer.EXE	1728	RegCloseKey	HKCR\AllFilesystemObjects	SUCCESS	
3:47:05.09028...	IEXPLORE.EXE	536	CreateFile	C:\	SUCCESS	Desired Access: Read
3:47:05.09035...	IEXPLORE.EXE	536	QueryDirectory	C:\	SUCCESS	0: 65e5bd5ca391440:
3:47:05.09050...	IEXPLORE.EXE	536	QueryDirectory	C:\	NO MORE FILES	
3:47:05.09342...	IEXPLORE.EXE	536	CloseFile	C:\	SUCCESS	
3:47:05.09362...	IEXPLORE.EXE	536	CreateFile	C:\DOCUMENTS AND SETTINGS	SUCCESS	Desired Access: Read
3:47:05.09370...	IEXPLORE.EXE	536	QueryDirectory	C:\Documents and Settings	SUCCESS	0: ., 1: ., FileInformatio
3:47:05.09495...	IEXPLORE.EXE	536	QueryDirectory	C:\Documents and Settings	NO MORE FILES	
3:47:05.09504...	IEXPLORE.EXE	536	CloseFile	C:\Documents and Settings	SUCCESS	
3:47:05.09610...	IEXPLORE.EXE	536	CreateFile	C:\Documents and Settings\ADMINISTRATOR	SUCCESS	Desired Access: Read
3:47:05.09616...	IEXPLORE.EXE	536	QueryDirectory	C:\Documents and Settings\Administrator	SUCCESS	0: ., 1: ., FileInformatio
3:47:05.09631...	IEXPLORE.EXE	536	QueryDirectory	C:\Documents and Settings\Administrator	NO MORE FILES	
3:47:05.09779...	IEXPLORE.EXE	536	CloseFile	C:\Documents and Settings\Administrator	SUCCESS	

Showing 23,463 of 61,477 events (38%)      Backed by virtual memory

start    Regshot-1.9.0    Process Explorer    apateDNS    Process Monitor    ~res-x86\_0011 - Not...    Process Monitor - Sys...    3:47 PM





Dallo screen di procmon si può notare che il file in questione, non è malevolo, perché quando si avvia il file, fa il controllo dei cookie di sessione.

## 5) Ho stoppato procmon e con RegShot ho fatto una seconda istantanea per fare la comparazione con la prima istantanea.

```
-res-x86_0011 - Notepad
File Edit Format View Help

Regshot 1.9.0 x86 Unicode
Comments:
Datetime: 2023/7/7 14:36:03 , 2023/7/7 14:39:18
Computer: MALWARE_TEST , MALWARE_TEST
Username: Administrator , Administrator

-----
Values modified: 17
-----
HKLM\SOFTWARE\Microsoft\Cryptography\ RNG\Seed: D1 5D 26 F2 BC 60 5C E5 0B FA 9E C5 7C 43 07 28 CC 3F 17 AE AB 55 7F 47 AA F3 19 41 98 44 14 B9 8D 74 2:
HKLM\SOFTWARE\Microsoft\Cryptography\ RNG\Seed: 1B F4 CA 08 81 5A 54 5F 64 FC 20 B1 9A F9 80 D3 22 C7 5D 1D 61 82 3C A8 0A 5D D9 82 0C 6A 12 9D 5A F9 9:
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\C
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\C
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\C
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\C
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\C
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\C
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\C
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\windows\CurrentVersion\Ext\Stats\{E2E2DD38-D088-4134-82B7-F2BA38496583}\iexplore\Coi
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\windows\CurrentVersion\Ext\Stats\{E2E2DD38-D088-4134-82B7-F2BA38496583}\iexplore\Coi
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\windows\CurrentVersion\Ext\Stats\{E2E2DD38-D088-4134-82B7-F2BA38496583}\iexplore\Tir
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\windows\CurrentVersion\Ext\Stats\{FB5F1910-F110-11D2-BB9E-00C04F795683}\iexplore\Coi
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\windows\CurrentVersion\Ext\Stats\{FB5F1910-F110-11D2-BB9E-00C04F795683}\iexplore\Coi
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\windows\CurrentVersion\Ext\Stats\{FB5F1910-F110-11D2-BB9E-00C04F795683}\iexplore\Tir
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings: 3C 00 00
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings: 3C 00 00
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\windows\CurrentVersion\Shell Extensions\Cached\{2559A1F4-21D7-11D4-BDAF-00C04F60B9F
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\windows\CurrentVersion\Shell Extensions\Cached\{2559A1F4-21D7-11D4-BDAF-00C04F60B9F
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\windows\CurrentVersion\Shell Extensions\Cached\{2559A1F5-21D7-11D4-BDAF-00C04F60B9F
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\windows\CurrentVersion\Shell Extensions\Cached\{2559A1F5-21D7-11D4-BDAF-00C04F60B9F
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\windows\ShellNoRoam\BagMRU\MRUListEx: 07 00 00 00 03 00 00 00 06 00 00 00 00 00 00 00
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\windows\ShellNoRoam\BagMRU\MRUListEx: 00 00 00 00 02 00 00 00 07 00 00 00 01 00 00
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\windows\ShellNoRoam\Bags\126\Shell\ScrollPos1366x655(1).y: 0x00000000
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\windows\ShellNoRoam\Bags\126\Shell\ScrollPos1366x655(1).y: 0x00000040
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\windows\ShellNoRoam\Bags\26\Shell\MinPos1366x655(1).x: 0xFFFF8300
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\windows\ShellNoRoam\Bags\26\Shell\MinPos1366x655(1).x: 0xFFFFFFFF
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\windows\ShellNoRoam\Bags\26\Shell\MinPos1366x655(1).y: 0xFFFF8300
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\windows\ShellNoRoam\Bags\26\Shell\MinPos1366x655(1).y: 0xFFFFFFFF
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\sysinternals\Process Monitor\Mainwindow: 2C 00 00 00 02 00 00 00 03 00 00 00 00 83 FF FF 00 }
```

6) Infine ho stoppato ApateDNS e Process Explorer e ho concluso la scansione.

Dai dati raccolti possiamo assicurare il dipendente che il file non è un file malevolo.