

REPORT

Malware_U3_W2_L5

Eseguito da:
Anatoliy Prsyazhnyuk

Traccia:

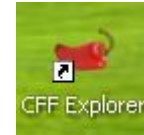
Con riferimento al file **Malware_U3_W2_L5** presente all'interno della cartella «Esercizio_Pratico_U3_W2_L5» sul desktop della macchina virtuale dedicata per l'analisi del malware, rispondere ai seguenti quesiti:

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

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

3. Identificare i **costrutti** noti (creazione dello stack, eventuali cicli, altri costrutti)
4. **Ipotizzare il comportamento della funzionalità implementata**
5. Come ultimo punto, dopo il bonus, spiegare quale istruzione assembly complessa

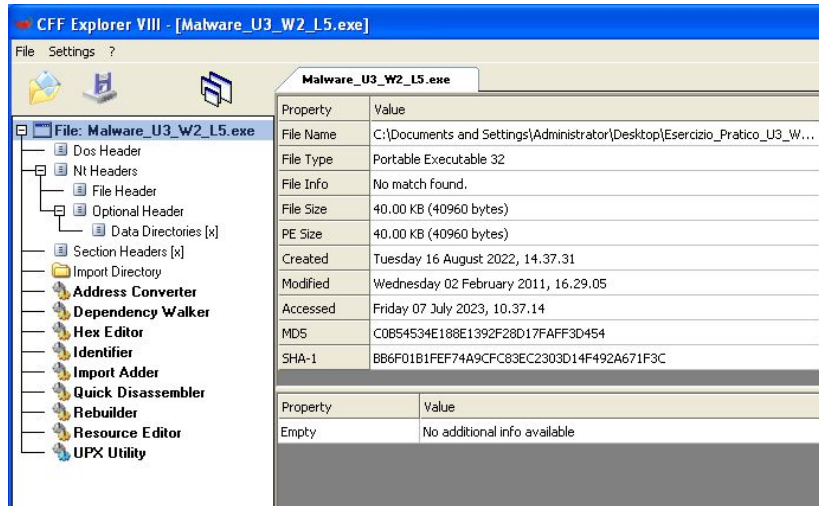
Il programma:



Schermata del programma all'avvio:



Schermata di CFF Explorer appena selezionato il file da analizzare:



Inizio con l'analisi statica per valutare il codice sorgente del file Malware_U3_W2_L5.exe senza doverlo eseguire; Effettuando quest'analisi è possibile ottenere informazioni dettagliate sul malware, come caratteristiche strutturali, le risorse utilizzate (librerie) e le funzioni chiamate, queste informazioni le ricavo con l'aiuto del programma CFF Explorer, che è un software per l'analisi avanzata dei file eseguibili.

Tutti questi dettagli ci possono aiutare per avere una maggiore visione sulle funzionalità di un certo malware.

Parte di traccia: **Le librerie presenti nel file exe**

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

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

Module Name	Imports
szAnsi	(nFunctions)
KERNEL32.dll	44
WININET.dll	5

Da come vediamo sono presenti molteplici funzioni presenti nelle librerie Kernel32.dll e Wininet.dll che possono essere utilizzate durante l'avvio del file .exe, però solamente quelle richiamate nel codice vengono utilizzate;

.dll (dynamic link libraries): sono file di codice precompilato che contengono funzioni, dati e risorse che possono essere utilizzate da più programmi;

Esamino la sezione  Import Directory

Ritrovo che nel file Malware_U3_W2_L5.exe sono presenti librerie: KERNEL32.dll e WININET.dll;

KERNEL32.dll è una libreria di collegamento dinamico di sistemi Windows, fornisce funzionalità di base per la gestione dei processi, delle memorie, dei file, l'accesso alle risorse del sistema e molto altro;

WININET.dll invece è sempre una libreria di collegamento dinamico che però fornisce funzionalità per la comunicazione di rete in ambienti Windows, spesso utilizzata per download/upload di file tramite protocolli come: HTTP, FTP; Supporta anche funzionalità per la gestione dei cookie, la gestione delle cache e altre operazioni di rete.

Parte di traccia: **Kernel32.dll** ed alcune funzionalità principali

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

KERNEL32.dll

44

Tra le funzionalità importate dalla libreria Kernel32.dll, troviamo precisamente 44 funzioni, esamino precisamente codeste funzioni:

Funzione	Breve descrizione	Possibile utilizzo malevolo
Sleep	Sospende l'esecuzione di un thread per un periodo specificato	Potrebbe essere utilizzato per rallentare l'esecuzione del sistema o evitare la rilevazione
WriteFile	Scrive i dati su un file o su un dispositivo di I/O	Potrebbe essere utilizzato per sovrascrivere file o modificare le impostazioni di sistema
GetCommandLineA	Recupera la stringa di comando passata al programma	Potrebbe essere utilizzato per eseguire comandi dannosi o passare parametri malevoli
LoadLibrary	Carica una libreria dinamicamente in memoria	Potrebbe essere utilizzato per caricare librerie dannose o eseguire codice malevolo
GetProcAddress	Recupera l'indirizzo di una funzione all'interno di una libreria dinamica	Potrebbe essere utilizzato per ottenere accesso a funzioni sensibili o per l'iniezione di codice dannoso
VirtualAlloc	Alloca una regione di memoria virtuale	Potrebbe essere utilizzato per creare uno spazio di esecuzione di codice dannoso
TerminateProcess	Termina un processo specificato	Potrebbe essere utilizzato per terminare processi critici o necessari al sistema
VirtualFree	Dealloca una regione di memoria virtuale	Potrebbe essere utilizzato per nascondere o distruggere tracce di codice malevolo
GetCurrentProcess	Recupera l'handle del processo corrente	Potrebbe essere utilizzato per ottenere accesso privilegiato o per nascondere attività
HeapCreate	Crea un heap di memoria	Potrebbe essere utilizzato per allocare memoria per l'esecuzione di codice malevolo

Name	Name	Name
szAnsi	szAnsi	szAnsi
Sleep	FreeEnvironmentStringsW	RtlUnwind
SetStdHandle	WideCharToMultiByte	WriteFile
GetStringTypeW	GetEnvironmentStrings	HeapAlloc
GetStringTypeA	GetEnvironmentStringsW	GetCPInfo
LCMapStringW	SetHandleCount	GetACP
LCMapStringA	GetStdHandle	GetOEMCP
MultiByteToWideChar	GetFileType	VirtualAlloc
GetCommandLineA	GetStartupInfoA	HeapReAlloc
GetVersion	GetModuleHandleA	GetProcAddress
ExitProcess	GetEnvironmentVariableA	LoadLibraryA
TerminateProcess	GetVersionExA	GetLastError
GetCurrentProcess	HeapDestroy	FlushFileBuffers
UnhandledExceptionFilter	HeapCreate	SetFilePointer
GetModuleFileNameA	VirtualFree	CloseHandle
FreeEnvironmentStringsA	HeapFree	

Parte di traccia: **Wininet.dll** e le sue funzioni

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

WININET.dll

5

Le funzioni importate con la libreria Wininet.dll sono 5, una breve descrizione di esse, ed il loro possibile utilizzo malevolo è il seguente:

Name
szAnsi
InternetOpenUrlA
InternetCloseHandle
InternetReadFile
InternetGetConnectedState
InternetOpenA

Funzione	Breve descrizione	Possibile utilizzo malevolo
InternetOpenUrlA	Apri una connessione HTTP, HTTPS o FTP per scaricare un file da un URL	Potrebbe essere utilizzata per scaricare e eseguire file dannosi o per l'accesso a risorse malevole
InternetCloseHandle	Chiude un handle di connessione Internet	Potrebbe essere utilizzata per nascondere o interrompere una connessione malevola
InternetReadFile	Legge dati da una connessione Internet	Potrebbe essere utilizzata per scaricare e analizzare dati malevoli o per lo spionaggio di informazioni sensibili
InternetGetConnectedState	Verifica lo stato della connessione di rete	Potrebbe essere utilizzata per monitorare o manipolare la connettività di rete
InternetOpenA	Inizializza una sessione di connessione Internet	Potrebbe essere utilizzata per stabilire una connessione malevola o per comunicazioni dannose

Parte di traccia: **Le sezioni del file Malware_U3_W2_L5**

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

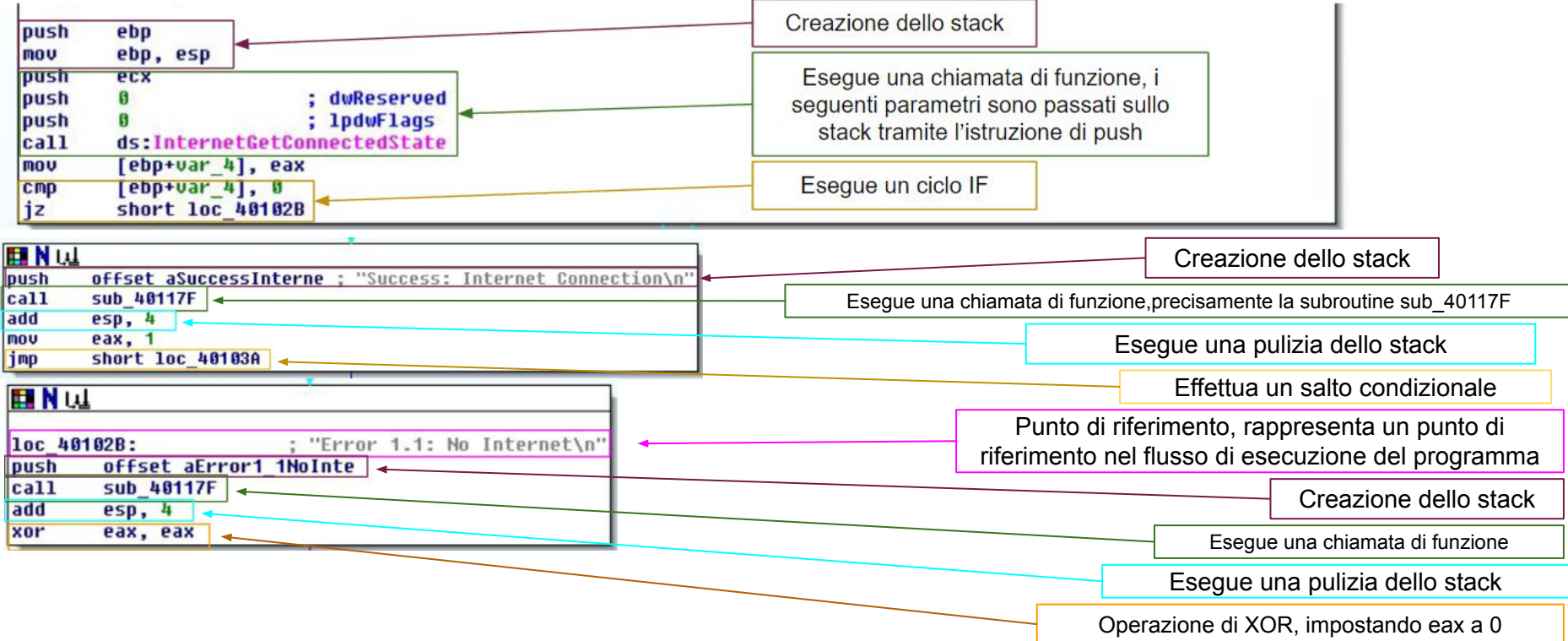
Malware_U3_W2_L5.exe									
Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations ...	Linenumbers...	Characteristics
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
.text	00004A78	00001000	00005000	00001000	00000000	00000000	0000	0000	60000020
.rdata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



Sezione	Descrizione
.text	Contiene il codice eseguibile del programma, compresi gli algoritmi, le istruzioni e le funzioni. È la sezione principale che contiene le istruzioni da eseguire.
.rdata	Contiene i dati di sola lettura (read-only data) utilizzati dal programma. Questi dati sono generalmente costanti, come stringhe o tabelle di lookup.
.data	Contiene i dati modificabili durante l'esecuzione del programma. Questa sezione include variabili globali, stati di programma e altri dati che possono essere modificati durante l'esecuzione.

Parte di traccia: **Identificare i costrutti noti**

3. Identificare i **costrutti** noti (creazione dello stack, eventuali cicli, altri costrutti)
4. **Ipotizzare** il comportamento della funzionalità implementata



Parte di traccia: **Identificare i costrutti noti e ipotizzo il comportamento della funzionalità implementata**

3. Identificare i **costrutti** noti (creazione dello stack, eventuali cicli, altri costrutti)

4. **Ipotizzare il comportamento della funzionalità implementata**

```
loc 40103A:  
mov     esp, ebp  
pop     ebp  
retn  
sub_401000 endp
```

Punto di riferimento, rappresenta un punto di riferimento nel flusso di esecuzione del programma

Rimozione stack

Ritorno dalla funzione, termina la funzione corrente e restituisce il controllo al chiamante

Fine della funzione sub_401000

Il codice verifica lo stato della connessione Internet e mostra un messaggio di successo se la connessione è attiva, altrimenti mostra un messaggio di errore.

Le funzioni di sistema utilizzate, come "InternetGetConnectedState" e "sub_40117F", sono probabilmente responsabili della gestione dell'accesso alle risorse di rete e della visualizzazione dei messaggi all'utente.

Parte di traccia: **Verificare il file IEXPLORE e convincere il dipendente che il file non è maligno**

BONUS:

Un giovane dipendente neo assunto segnala al reparto tecnico la presenza di un programma sospetto.

Il suo superiore gli dice di stare tranquillo ma lui non è soddisfatto e chiede supporto al SOC.

Il file "sospetto" è IEXPLORE.EXE contenuto nella cartella C:\Program Files\Internet Explorer (no, non ridete ragazzi)

Come membro senior del SOC ti è richiesto di convincere il dipendente che il file non è maligno.

Possono essere usati gli strumenti di analisi statica basica e/o analisi dinamica basica visti a lezione.

No disassembly no debug o similari

VirusTotal non basta, ovviamente


Non basta dire iexplorer è Microsoft è buono, punto.

Da come possiamo vedere il file è di proprietà Microsoft, con apportata in seguito la licenza di Copyright

© Microsoft Corporation. All rights reserved.

La scansione del file IEXPLORE.exe su VirusTotal ha fornito un ulteriore segnale che il file sia sicuro e privo di malware. Tuttavia, è importante considerare che la scansione su VirusTotal da sola non garantisce la completa sicurezza del file, dunque eseguo anche un'analisi dinamica, di seguito.

Malware_U3_W2_L5.exe		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	91.00 KB (93184 bytes)		
PE Size	91.00 KB (93184 bytes)		
Created	Monday 20 March 2017, 23.18.53		
Modified	Monday 14 April 2008, 05.42.24		
Accessed	Friday 07 July 2023, 14.03.30		
MD5	55794B97A7FAABD2910873C85274F409		
SHA-1	58E80C90BF54850B5F3CCBD8EDF0877537E0EA8E		
Property	Value		
CompanyName	Microsoft Corporation		
FileDescription	Internet Explorer		
FileVersion	6.00.2900.5512 (xpsp.080413-2105)		
InternalName	iexplore		
LegalCopyright	© Microsoft Corporation. All rights reserved.		
OriginalFilename	IEXPLORE.EXE		
ProductName	Microsoft® Windows® Operating System		



0
/ 71

✔ File distributed by Microsoft

814a37d89a79aa3975308e723bc1a3a67360323b7e3584de00896fe7c59bbb8e

IEXPLORE.EXE

peexe known-distributor trusted

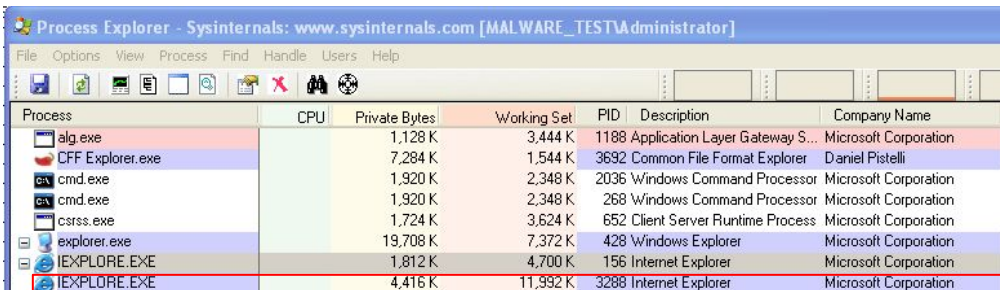
Size
91.00 KB

Last Analysis Date
1 month ago

🔍 EXE

Community Score

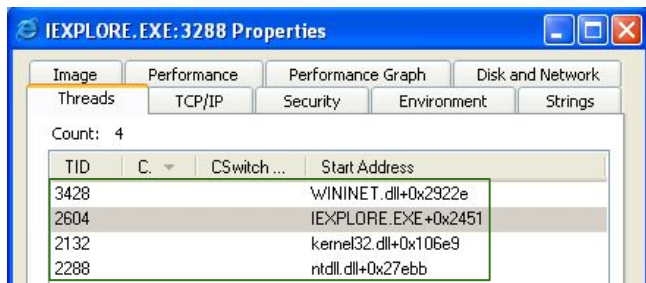
Parte di traccia: **Verificare il file IEXPLORE e convincere il dipendente che il file non è maligno**



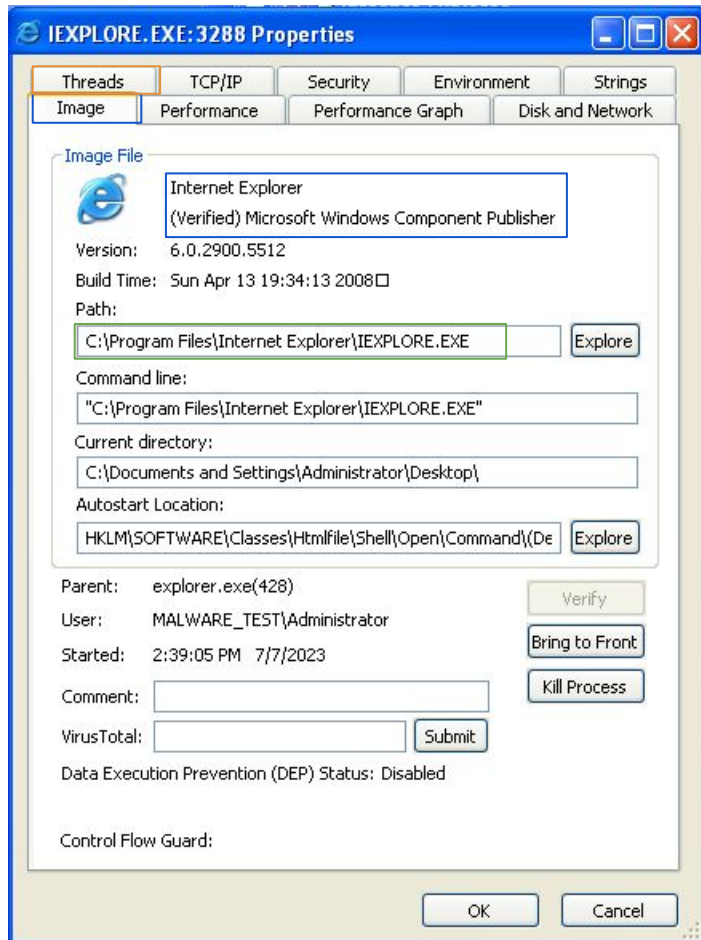
Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
alg.exe		1,128 K	3,444 K	1188	Application Layer Gateway S...	Microsoft Corporation
CFF Explorer.exe		7,284 K	1,544 K	3692	Common File Format Explorer	Daniel Pistelli
cmd.exe		1,920 K	2,348 K	2036	Windows Command Processor	Microsoft Corporation
cmd.exe		1,920 K	2,348 K	268	Windows Command Processor	Microsoft Corporation
csrss.exe		1,724 K	3,624 K	652	Client Server Runtime Process	Microsoft Corporation
explorer.exe		19,708 K	7,372 K	428	Windows Explorer	Microsoft Corporation
IEXPLORE.EXE		1,812 K	4,700 K	156	Internet Explorer	Microsoft Corporation
IEXPLORE.EXE		4,416 K	11,992 K	3288	Internet Explorer	Microsoft Corporation

Possiamo esaminare diverse schede e informazioni per valutare se il processo IEXPLORE potrebbe essere potenzialmente malevolo:

1. Controllo il percorso del file eseguibile e l'origine del processo. Verifico se il percorso corrisponde alla posizione predefinita e attendibile di Internet Explorer.
2. Scheda "Image" (Immagine): Controllo i dettagli sull'immagine del file eseguibile, come la descrizione e il nome del prodotto.
3. Scheda "Threads" (Thread): Esamino i thread associati al processo. Se ci sono thread sospetti o con comportamenti insoliti, potrebbe essere un segno di malware.
Sulla base delle informazioni fornite sui thread associati al processo IEXPLORE, non ci sono evidenti segni di comportamenti insoliti o malevoli.



TID	C.	CSwitch	Start Address
3428			WININET.dll+0x2922e
2604			IEXPLORE.EXE+0x2451
2132			kernel32.dll+0x106e9
2288			ntdll.dll+0x27ebb



IEXPLORE.EXE: 3288 Properties

Image File

Internet Explorer
(Verified) Microsoft Windows Component Publisher

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\Htmfile\Shell\Open\Command\{De [Explore]

Parent: explorer.exe(428) [Verify]

User: MALWARE_TEST\Administrator [Bring to Front]

Started: 2:39:05 PM 7/7/2023 [Kill Process]

Comment: [Submit]

VirusTotal: [Submit]

Data Execution Prevention (DEP) Status: Disabled

Control Flow Guard:

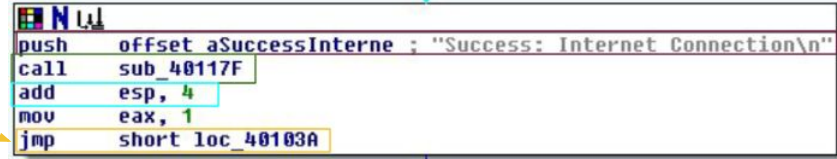
[OK] [Cancel]

Parte di traccia: **Spiegare qualche istruzione assembly complessa**

3. Identificare i **costrutti** noti (creazione dello stack, eventuali cicli, altri costrutti)
4. **Ipotesizzare il comportamento della funzionalità implementata**
5. Come ultimo punto, dopo il bonus, spiegare quale istruzione assembly complessa

Salto condizionale (jmp): esegue un salto incondizionato all'etichetta "loc_480103A".

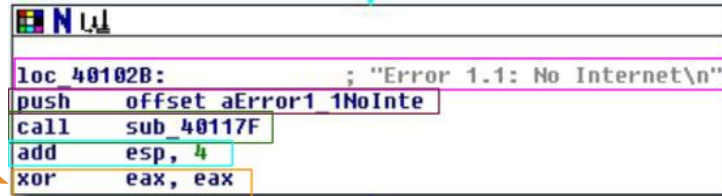
Un salto incondizionato è un'istruzione di controllo di flusso che consente di saltare a un punto specifico nel codice, indipendentemente dalle condizioni. In questo contesto, l'istruzione "jmp short loc_480103A" indica un salto breve (short) all'etichetta "loc_480103A". Ciò significa che il flusso del programma passerà direttamente all'indirizzo corrispondente all'etichetta "loc_480103A", ignorando qualsiasi istruzione successiva nel codice.



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

Operazione di XOR: esegue un'operazione di XOR tra il registro "eax" e se stesso, impostando "eax" a 0. L'XOR (Exclusive OR) è un'operazione logica binaria che confronta i bit corrispondenti di due operandi. Se i bit sono diversi, il risultato sarà 1, altrimenti sarà 0.

Quando "xor eax, eax" viene eseguito, si sta effettivamente confrontando il registro "eax" con se stesso, che restituisce sempre 0.



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