



MALWARE ANALYSIS

S10 - L1



MICHELANGELO BORROMEO

TRACCIA

Analizzare l'Applicativo «Esercizio_Pratico_U3_W2_L1» tramite CFF Explorer

- Indicando le librerie importate dal malware
- Fornendo una descrizione per ognuna di essa
- Fare una considerazione finale sulle informazioni raccolte

MALWARE ANALYSIS

Indicare le librerie importate dal malware, fornendo una descrizione per ognuna di esse

Utilizzando il software CFF Explorer siamo riusciti ad analizzare il malware fornendoci informazioni riguardo



Malware_U3_W2_L1



recandoci sulla sezione Import Directory possiamo notare le .dll importate da esso e le sue funzioni

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.DLL	6	00000000	00000000	00000000	00006098	00006064
ADVAPI32.dll	1	00000000	00000000	00000000	000060A5	00006080
MSVCRT.dll	1	00000000	00000000	00000000	000060B2	00006088
WININET.dll	1	00000000	00000000	00000000	000060BD	00006090

KERNEL32.DLL

KERNEL32.DLL	6	00000000	00000000	00000000	00006098	00006064
--------------	---	----------	----------	----------	----------	----------

KERNEL32.dll:

Fornisce funzioni principali per la gestione della memoria, processi e thread.

Può essere utilizzato per:

- Creare processi e thread
- Manipolare la memoria
- Avere accesso ai file di sistema
- E reperire le caratteristiche (OS)

N/A	000060C8	0000	LoadLibraryA
N/A	000060D6	0000	GetProcAddress
N/A	000060E6	0000	VirtualProtect
N/A	000060F6	0000	VirtualAlloc
N/A	00006104	0000	VirtualFree
N/A	00006112	0000	ExitProcess

- LoadLibraryA
carica una libreria dinamica (DLL) nel processo chiamante.
Il processo può chiamare le funzioni esportate dalla DLL.
- GetProcAddress
Recupera l'indirizzo di una funzione esportata dalla DLL caricata.
- VirtualProtect
cambia le protezioni di accesso per una regione di memoria virtuale.
- VirtualAlloc
commette o cambia lo stato di una regione di memoria virtuale in un processo.
- VirtualFree
libera la memoria precedentemente allocata con VirtualAlloc o funzioni simili.
- ExitProcess
chiude immediatamente il processo, il che significa che non ci sono opportunità per eseguire altre operazioni di pulizia o salvataggio dei dati dopo la chiamata.

ADVAPI32.DLL

ADVAPI2.dll	1	00000000	00000000	00000000	000060A5	00006080
-------------	---	----------	----------	----------	----------	----------

ADVAPI32.dll:

contiene le funzioni per interagire con i servizi ed i registri del sistema operativo

Può essere utilizzato per:

- Manipolare i registri di sistema
- Gestire i privilegi e creazione dei Token
- Gestire autenticazioni e le credenziali

N/A	00006120	0000	CreateServiceA
-----	----------	------	----------------

- CreateServiceA:

creare un nuovo servizio nel database dei servizi del sistema
(I servizi sono applicazioni che vengono eseguite in background)

MSVCRT.DLL

MSVCRT.dll	1	00000000	00000000	00000000	000060B2	00006088
------------	---	----------	----------	----------	----------	----------

MSVCRT.dll:

Fornisce le funzioni per eseguire applicazioni scritte in C e C++.

Può essere utilizzato per:

- Manipolare le stringhe e variabili
- Gestire la memoria
- Gestire gli input ed output

N/A	00006130	0000	exit
-----	----------	------	------

WININET.DLL

WININET.dll	1	00000000	00000000	00000000	000060BD	00006090
-------------	---	----------	----------	----------	----------	----------

WININET.dll:

Fornisce funzioni per l'accesso a Internet e per la gestione delle connessioni HTTP e FTP.

Può essere utilizzato per:

- Effettuare download di payload aggiuntivi
- Connettersi a server C2 (command and control)

N/A	00006136	0000	InternetOpenA
-----	----------	------	---------------

- **InternetOpenA**
utilizzata per configurare la connessione a Internet e ottenere un handle per ulteriori operazioni di rete, come l'apertura di URL, l'invio di richieste HTTP, ecc.

MALWARE ANALYSIS

