MALWARE ANALYSIS: ANALISI STATICA BASICA EPICODE

Giovanni Pisapia

1. LIBRERIE MALWARE

Librerie Malware:

- Kernel32.dll: è una libreria di collegamento dinamico (DLL) in Windows che offre funzionalità di basso livello per le applicazioni. Tra le sue funzioni principali ci sono la gestione della memoria (allocare, gestire e deallocare la memoria), la gestione dei file (creare, aprire, chiudere, leggere e scrivere file), la gestione dei processi e dei thread (creare, terminare e gestire processi e thread), la gestione degli errori, la gestione del tempo e dell'orologio, e la gestione delle librerie dinamiche.
- Advapi32.dll: svolge un ruolo fondamentale nella gestione della sicurezza e delle operazioni di sistema in Windows. Viene utilizzata da molte applicazioni e servizi per accedere alle funzionalità di sicurezza, crittografia, gestione dei servizi e registro di sistema offerte dal sistema operativo.
- Msvcrt.dll è una libreria essenziale per l'esecuzione di programmi scritti in linguaggio C o C++ su Windows. È utilizzata da molte applicazioni e servizi che richiedono il supporto delle funzionalità di runtime del linguaggio C, come la gestione della memoria, l'input/output e la manipolazione delle stringhe.
- Wininet.dll viene spesso utilizzata da applicazioni e servizi che richiedono la connettività di rete e l'accesso a risorse Internet. Fornisce un'interfaccia semplice per interagire con i protocolli di rete come HTTP, FTP e HTTPS, consentendo alle applicazioni di comunicare con server remoti e recuperare dati da Internet.

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
00000A98	N/A	00000A00	00000A04	00000A08	00000A0C	00000A10
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

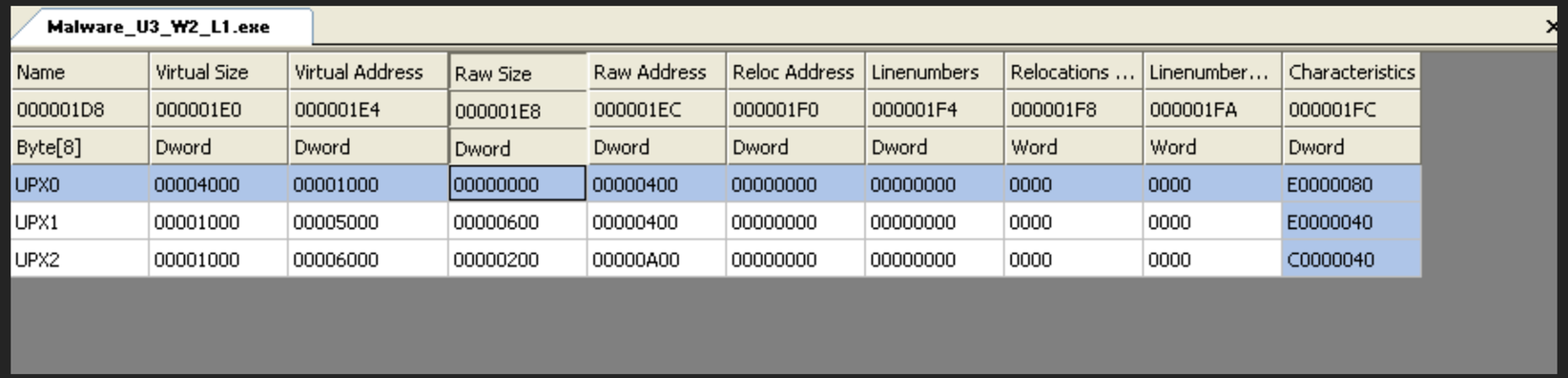
2. SEZIONI MALWARE

Sezioni Malware:

- Nelle sezioni del malware troviamo UPX0, UPX1 e UPX2, che dopo le mie ricerche ho scoperto essere delle sezioni compresse del file eseguibile. Queste sezioni possono contenere dati, codice o risorse compressi. Nel caso di un malware, potrebbe utilizzare queste sezioni per nascondere il suo codice o i suoi dati, rendendoli più difficili da rilevare o analizzare. In tal caso, potrebbe essere necessario decomprimere queste sezioni per recuperare il codice originale o le risorse e analizzarle in dettaglio.

Nella tabella troviamo alcune informazioni utili alla comprensione del malware:

- VirtualSize (Dimensione virtuale): Rappresenta la dimensione virtuale della sezione compressa. Indica lo spazio di memoria che la sezione occupa quando viene caricata in memoria durante l'esecuzione del file.
- VirtualAddress (Indirizzo virtuale): Indica l'indirizzo virtuale a cui la sezione compressa viene mappata in memoria durante l'esecuzione del file.
- RawSize (Dimensione reale): Rappresenta la dimensione reale della sezione prima della compressione. Indica la quantità di dati o codice contenuti nella sezione prima della compressione.
- RawAddress (Indirizzo reale): Indica l'indirizzo reale a cui la sezione inizia nel file prima della compressione.



Malware_U3_W2_L1.exe

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations ...	Linenumber...	Characteristics
000001D8	000001E0	000001E4	000001E8	000001EC	000001F0	000001F4	000001F8	000001FA	000001FC
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
UPX0	00004000	00001000	00000000	00000400	00000000	00000000	0000	0000	E0000080
UPX1	00001000	00005000	00000600	00000400	00000000	00000000	0000	0000	E0000040
UPX2	00001000	00006000	00000200	00000A00	00000000	00000000	0000	0000	C0000040

3. CONCLUSIONI

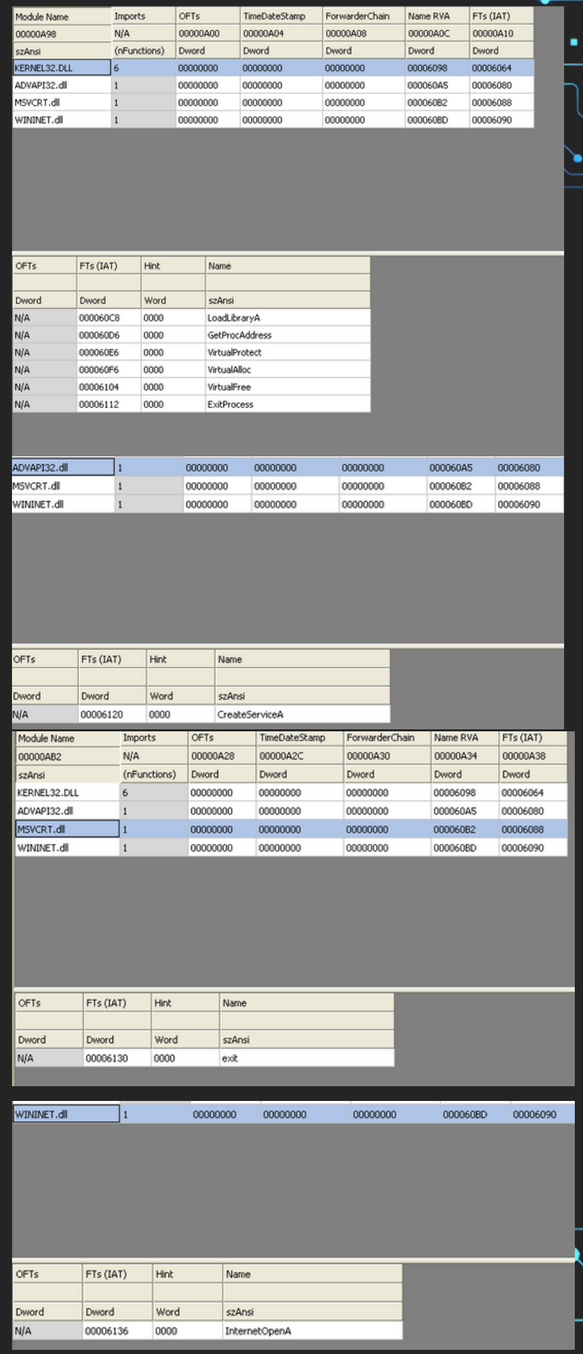
Sulla base delle informazioni raccolte sul malware e le librerie importate, possiamo fare alcune considerazioni generali:

Il malware sembra sfruttare diverse funzionalità fornite dalle librerie importate per eseguire attività malevole nel sistema. Ad esempio, l'utilizzo della funzione "CreateServiceA" dalla libreria "advapi32.dll" potrebbe indicare che il malware cerca di creare un servizio persistente per avviarsi automaticamente ad ogni avvio del sistema, aumentando la sua persistenza.

La funzione "exit" dalla libreria "msvcrt.dll" viene utilizzata per terminare il processo del malware in modo improvviso, cercando di eludere la rilevazione e l'analisi dei sistemi di sicurezza.

La libreria "wininet.dll" e la funzione "InternetOpen" indicano che il malware potrebbe stabilire una connessione Internet per comunicare con un server di comando e controllo remoto. Questo potrebbe consentire al malware di ricevere istruzioni, inviare informazioni sensibili o eseguire altre attività dannose attraverso la rete.

Infine, la presenza di funzioni come "LoadLibraryA", "GetProcAddress", "VirtualProtect", "VirtualAlloc", "VirtualFree" ed "ExitProcess" dalla libreria "kernel32.dll" suggerisce che il malware potrebbe utilizzare queste funzioni per manipolare la memoria, eseguire operazioni di caricamento dinamico di altre librerie o moduli malevoli e controllare il ciclo di vita del suo processo.



Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
00000A98	N/A	00000A00	00000A04	00000A08	00000A0C	00000A10
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

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
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

ADVAPI32.dll	1	00000000	00000000	00000000	000060A5	00006080
MSVCRT.dll	1	00000000	00000000	00000000	000060B2	00006088
WININET.dll	1	00000000	00000000	00000000	000060BD	00006090

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
N/A	00006120	0000	CreateServiceA

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
00000AB2	N/A	00000A28	00000A2C	00000A30	00000A34	00000A38
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

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
N/A	00006130	0000	exit

WININET.dll	1	00000000	00000000	00000000	000060BD	00006090

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
N/A	00006136	0000	InternetOpenA