MALWARE ANALYSIS | STATICA BASICA

S10 - L1

Malware_U3_W2_L1.exe

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

Analizando il file "Malware_U3_W2_L1.exe" con il programma CFF, possiamo vedere le librerie che vengono richieste per il programma, cioè, importate a tempo di esecuzione (runtime). Come possiamo vedere nell'immagine, il programma richiede 4 librerie:

KERNEL32.dll

Fornisce funzioni fondamentali per attività quali gestione della memoria, operazioni di input/output, gestione di processi e thread, gestione degli errori e gestione del tempo di sistema.

ADVAPI32.dll

Contiene funzioni relative alla sicurezza, alla manipolazione del registro, alla registrazione degli eventi e ad altri servizi di sistema avanzati.

MSVCRT.dll

Fornisce supporto per varie funzioni runtime C, come l'allocazione della memoria, l'input/output di file, la manipolazione delle stringhe e le operazioni matematiche.

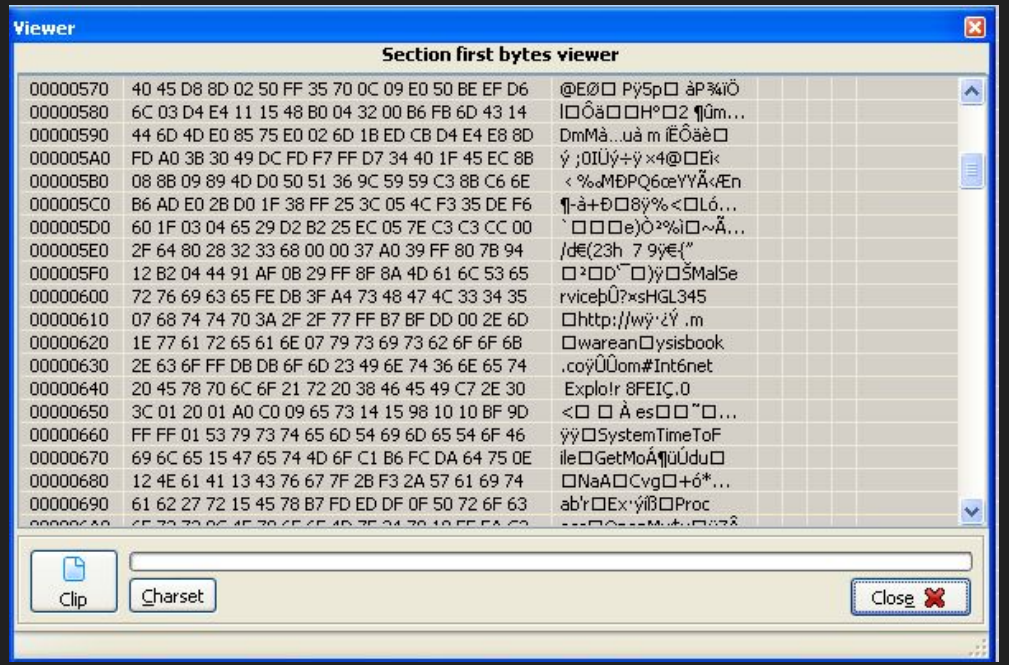
WININET.dll

È un componente che e viene utilizzato da molte applicazioni per accedere ai e HTTP per eseguire attività come il download di file, il caricamento di file e la navigazione di siti Web.

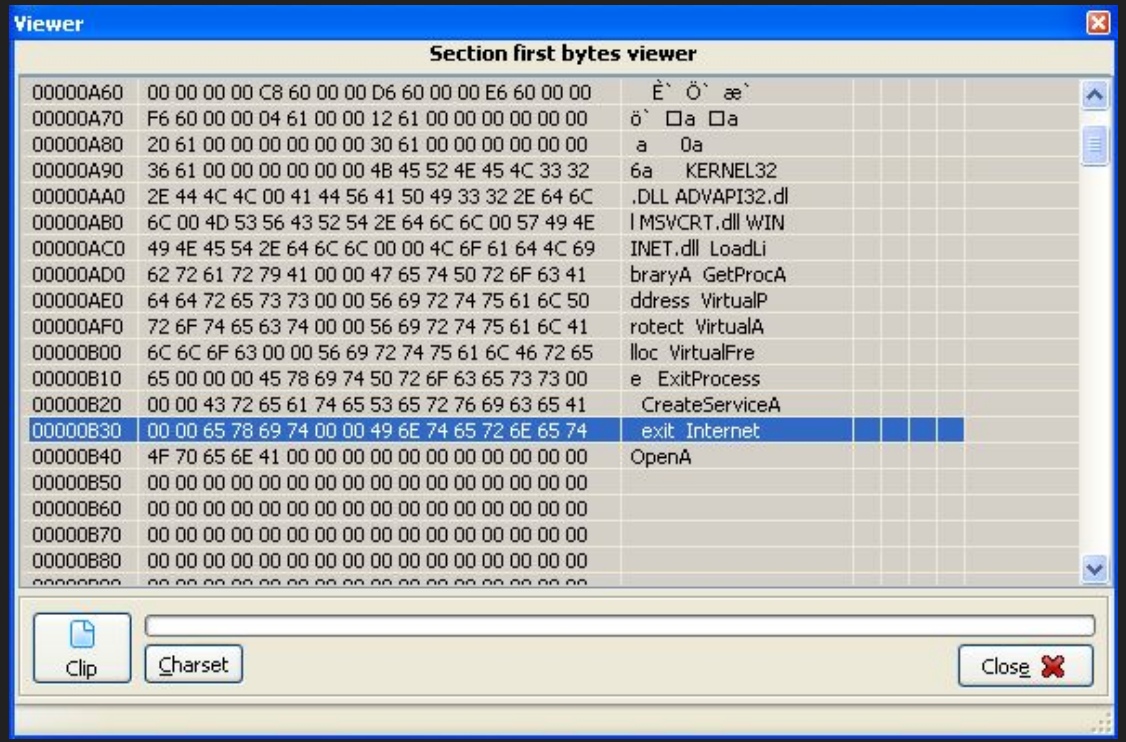
Ora diamo un'occhiata alle "sezioni" del programma. Possiamo vedere che ce ne sono 3: UPX0, UPX1 e UPX2. Selezionandone uno, possiamo ispezionarne il contenuto ASCII. Nell'immagine possiamo vedere uno di questi blocchi di testo ASCII, dove, tra molti altri caratteri, possiamo vedere alcune parole, come un pezzo di URL HTTP, la parola *ysisbook*, *MalService* e *SystemTimeToFile*.

Malware_U3_W2_L1.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
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



Questo è il contenuto ASCII di UPX2, dove sembra che, oltre ad avere molto "padding", chiami le 4 librerie citate prima, e avvii il servizio "ServiceA" e internet "OpenA"



Dopo inserire il file su VirusTotal, possiamo vedere che questo programma fa tante cose, come pianificare una task che eseguire codice malizioso, o modificare lo status dei servizi attivi sul sistema.

MITRE ATT&CK Tactics and Techniques

— **Execution** TA0002

Scheduled Task/Job T1053
Adversaries may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code.

Scheduled Task T1053.005
Adversaries may abuse the Windows Task Scheduler to perform task scheduling for initial or recurring execution of malicious code.

Command and Scripting Interpreter T1059
Very long cmdline option found, this is very uncommon (may be encrypted or packed)

Shared Modules T1129
The process tried to load dynamically one or more functions.

Service Execution T1569.002
Uses sc.exe to modify the status of services

— **Persistence** TA0003

Scheduled Task/Job T1053
Adversaries may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code.

Scheduled Task T1053.005
Adversaries may abuse the Windows Task Scheduler to perform task scheduling for initial or recurring execution of malicious code.

Create or Modify System Process T1543
Adversaries may create or modify system-level processes to repeatedly execute malicious payloads as part of persistence.

Windows Service T1543.003
Modifies existing windows services
Uses sc.exe to modify the status of services
Creates or modifies windows services
Adversaries may create or modify Windows services to repeatedly execute malicious payloads as part of persistence.

Boot or Logon Autostart Execution T1547
Adversaries may configure system settings to automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges on compromised systems.

Registry Run Keys / Startup Folder T1547.001
Adversaries may achieve persistence by adding a program to a startup folder or referencing it with a Registry run key.

LSASS Driver T1547.008
Spawns drivers

DLL Side-Loading T1574.002
Tries to load missing DLLs