Alaimo Alessandro
09/01/2023

Report Analisi Statica Basica

Come richiesto dall'esercizio, andiamo ad analizzare le librarie che vengono importate con questo Malware, che sono:

KERNEL32.dll: È una libreria piuttosto comune che contiene le funzioni principali per interagire con il sistema operativo, tra queste funzioni, vengono richiamate:

- LoadLibraryA: Carica il modulo specificato nello spazio degli indirizzi del processo chiamante. Il modulo specificato può causare il caricamento di altri moduli.

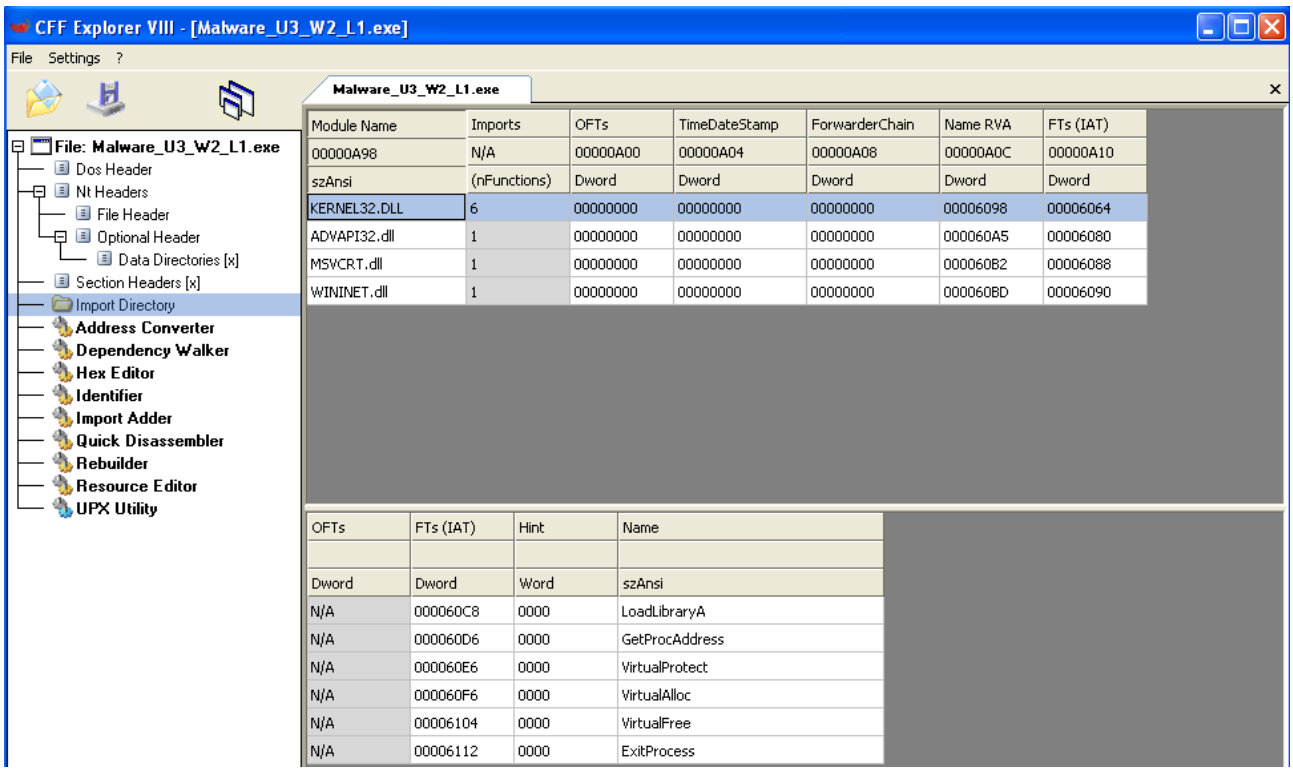
- GetProcAddress: Recupera l'indirizzo di una funzione esportata (nota anche come procedura) o di una variabile dalla libreria a collegamento dinamico (DLL) specificata.

- VirtualProtect: Modifica la protezione in un'area di pagine salvate nello spazio degli indirizzi virtuali del processo chiamante.

- VirtualAlloc: Riserva, impegna o cambia lo stato di una regione di pagine nello spazio degli indirizzi virtuali del processo chiamante. La memoria allocata da questa funzione viene automaticamente inizializzata a zero.

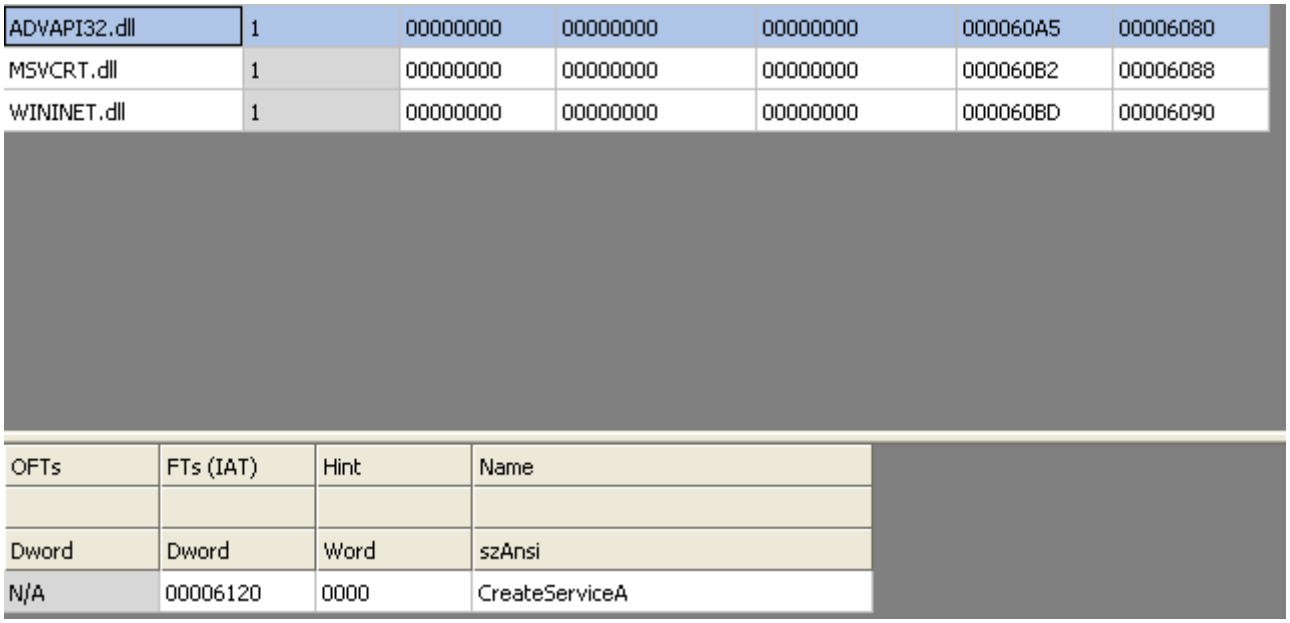
- VirtualFree: Rilascia, disimpegna o rilascia e disimpegna una regione di pagine nello spazio degli indirizzi virtuali del processo chiamante.

- ExitProcess: Termina il processo chiamante e tutti i suoi thread.



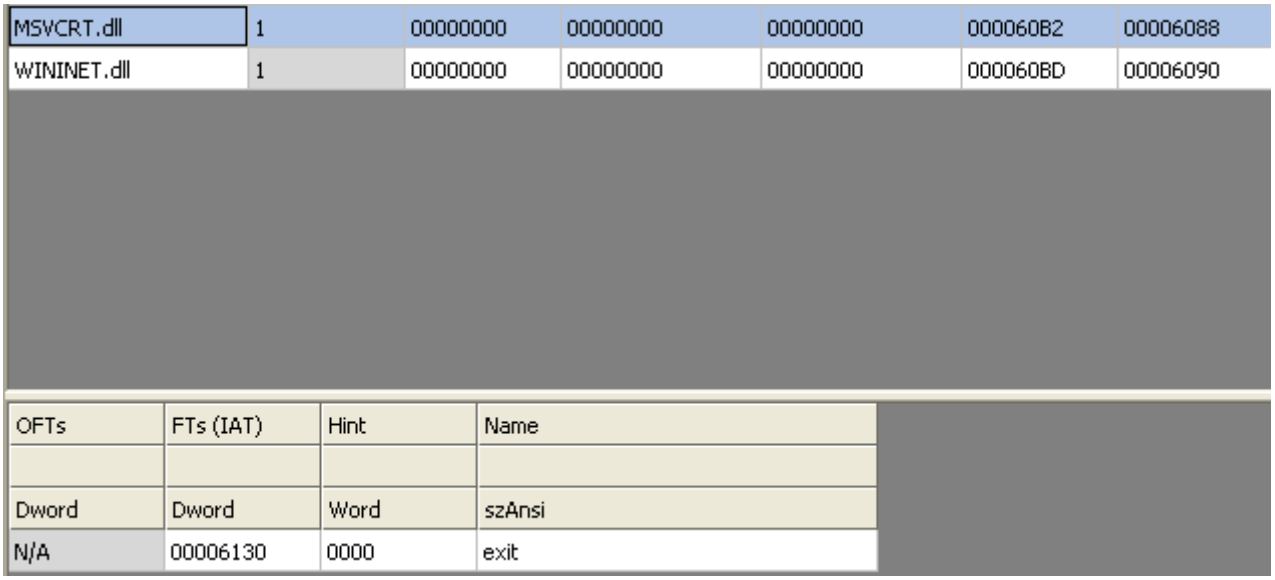
ADVAPI32.dll: Libreria che contiene le funzioni per interagire con i servizi ed i registri del sistema operativo Microsoft, tra le funzioni, quella usata è:

- CreateServiceA: Crea un oggetto di servizio e lo aggiunge al database del gestore del controllo dei servizi specificato.



MSVCRT.dll: Libreria che contiene funzioni per la manipolazione stringhe, allocazione memoria e altro come chiamate per input/output in stile linguaggio C e tra le funzioni presenti, quella usata è:

- exit: Le funzioni di uscita termina il processo chiamante.

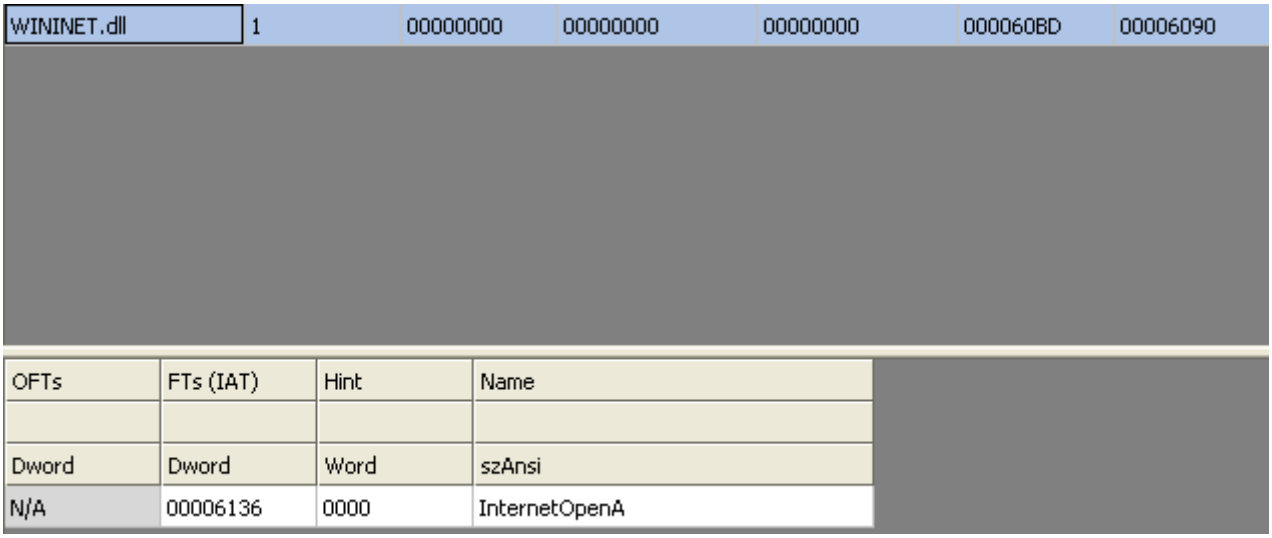


MSVCRT.dll	1	00000000	00000000	00000000	000060B2	00006088
WININET.dll	1	00000000	00000000	00000000	000060BD	00006090

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

WININET.dll: Libreria che contiene le funzioni per l'implementazione di alcuni protocolli di rete come HTTP, FTP, NTP e tra le funzioni presenti, quella usata è:

- InternetOpenA: Inizializza l'uso delle funzioni di WinINet da parte dell'applicazione.



WININET.dll	1	00000000	00000000	00000000	000060BD	00006090

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

Adesso andiamo ad analizzare i 3 settori, vedendo che UPX0 lo possiamo paragonare ad un .text, ossia quella parte contenente tutte le stringhe che andrà ad eseguire la CPU, seguito dall' UPX1, paragonabile ad un .data ed infine dall'UPX2, che lo possiamo trattare come un .rdata, poiché vi sono riportate tutte le informazioni sulle librerie e funzioni importate.

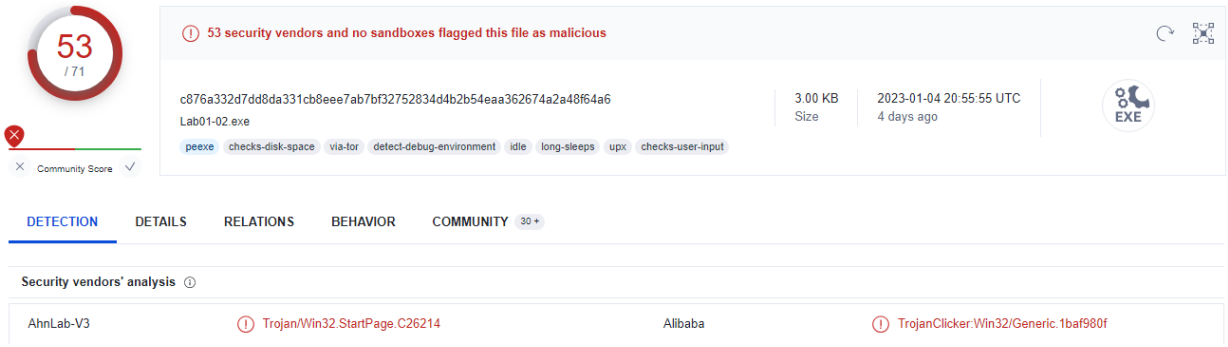
UPX0	00004000	00001000	00000000	00000400	00000000	00000000	0000	0000	E0000080
UPX1	00001000	00005000	00000600	00000400	00000000	00000000	0000	0000	E0000040
UPX2	00001000	00006000	00000200	00000A00	00000000	00000000	0000	0000	C0000040

Andandole ad analizzare singolarmente, possiamo notare che UPX0 funziona anche come la somma tra UPX1 ed UPX2 e possiamo anche ipotizzare ciò che questo malware fa. Difatti il malware raccoglie, associandosi ad un processo, tutti i dati ed insieme all'orario del sistema, manda un email all'ipotetico Hacker.

In aggiunta all'esercizio di oggi, sono andato ad utilizzare md5deep per stamparmi a schermo l'hash del Malware per poi cercarlo su VirusTotal, come riportato di seguito:

```
C:\Documents and Settings\Administrator\Desktop\md5deep-4.3>md5deep "C:\Docum
s and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L1\Malware_U3_W2
.exe"
8363436878404da0ae3e46991e355b83  C:\Documents and Settings\Administrator\Des
p\Esercizio_Pratico_U3_W2_L1\Malware_U3_W2_L1.exe

C:\Documents and Settings\Administrator\Desktop\md5deep-4.3>_
```



Come si può notare, 53 antivirus su 71 lo rilevano o come un virus generico o come un Trojan e difatti, andando su details ricaveremo le stesse informazioni delle librerie importate e sezioni trovate in precedenza. A seguito lascio il link per VirusTotal: https://www.virustotal.com/gui/file/c876a332d7dd8da331cb8eee7ab7bf32752834d4b2b54eaa362674a2a48f64a6/details