Esercizio S10/L1

Traccia:

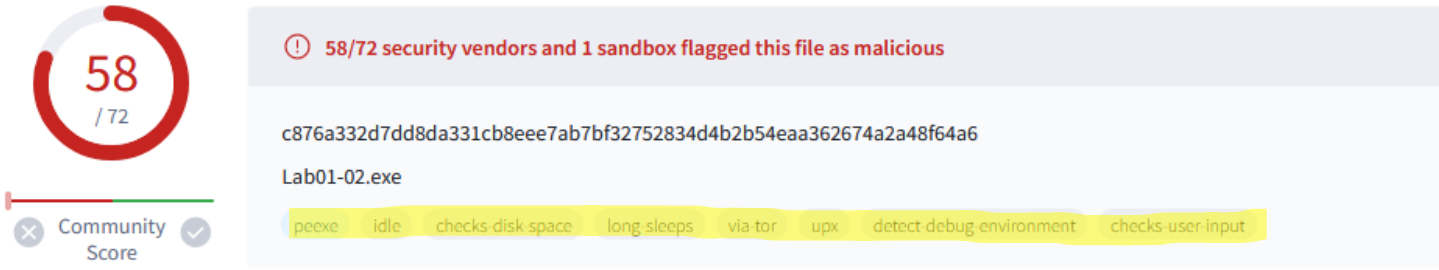
Effettuare il “**Malware Analysis**” sul file eseguibile contenuto nella cartella «*Esercizio_Pratico_U3_W2_L1*» e rispondere ai seguenti quesiti:

- Indicare le librerie importate dal malware, fornendo una descrizione per ognuna di esse;
- Indicare le sezioni di cui si compone il malware, fornendo una descrizione per ognuna di essa;
- Aggiungere una considerazione finale sul malware in analisi in base alle informazioni raccolte.

File Hash:

Malware_U3_W2_L1.exe

Property	Value
File Name	C:\Users\user\Desktop\MALWARE\Esercizio_Pratico_U3_W2_L1\Malw...
File Type	Portable Executable 32
File Info	UPX v3.0
File Size	3.00 KB (3072 bytes)
PE Size	3.00 KB (3072 bytes)
Created	Wednesday 19 January 2011, 11.10.42
Modified	Wednesday 17 January 2024, 17.48.15
Accessed	Wednesday 19 January 2011, 11.10.42
MD5	8363436878404DA0AE3E46991E355B83
SHA-1	5A016FACBCB77E2009A01EA5C67B39AF209C3FCB



Come prima cosa sono andato a verificare le proprietà del file e ho copiato il **file signature** (hash) per poi andarlo a verificare su Virus Total. Già facendo questo primo passaggio notiamo come abbiamo identificato che il file si tratta di un **Malware** e dove mette mano (Parte evidenziata in giallo), ma proseguiamo.

Esercizio S10/L1

Librerie:

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

KERNEL32.dll: È una libreria di sistema di Windows che fornisce funzionalità di basso livello per la gestione delle risorse del sistema, la gestione dei processi, la gestione della memoria, le operazioni di input/output e altre funzioni di base del sistema operativo.

ADVAPI32.dll: È una libreria di sistema di Windows che fornisce funzionalità avanzate per l'accesso e la gestione dei servizi, la gestione delle credenziali, la crittografia dei dati, la gestione degli eventi e altre operazioni relative alla sicurezza e all'amministrazione del sistema.

MSVCRT.dll: È una libreria di runtime di Microsoft Visual C++ (MSVCRT) che fornisce le funzioni standard del linguaggio C come la gestione della memoria dinamica, le operazioni di input/output standard (printf, scanf) e altre funzioni utili nei programmi scritti in linguaggio C o C++.

WININET.dll: È una libreria di sistema di Windows che fornisce supporto per le operazioni di rete e l'accesso a risorse Internet. Include funzioni per l'invio e la ricezione di dati tramite protocolli Internet come HTTP, FTP e altri, nonché funzionalità per la gestione delle connessioni di rete e dei cookie.

Sezioni Headers:

Malware_U3_W2_L1.exe

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers ...	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

Queste sezioni header UPX sono aggiunte durante il processo di compressione del file eseguibile per camuffare il malware e sono utilizzate dal loader UPX durante la decompressione per ripristinare il file eseguibile nel suo stato originale e avviarlo correttamente.

Conclusione:

Siamo riusciti quindi ad individuare e a prendere un sacco di informazioni utili grazie all'analisi basica statica e siamo riusciti a concludere che il Malware: Si camuffa, importa librerie dinamicamente, interagisce con i registri e i servizi di sistema, controlla gli input e gli output e crea sessioni tramite protocolli di rete.