[S10/E1 - Natalino Imbrogno]

Il file eseguibile *Esercizio_Pratico_U3_W2_L1* analizzato attraverso CFF Explorer mostra che il malware importa le seguenti 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

In particolare, abbiamo:

- *KERNEL32.DLL*, ovvero una libreria di sistema di windows che fornisce accesso alle funzionalità di base del sistema operativo, come l'accesso ai file, la gestione della memoria e l'esecuzione di thread;
- *ADVAPI32.DLL*, e cioè un'altra libreria di sistema di windows che fornisce accesso alle funzionalità di sicurezza del sistema operativo, come l'autenticazione, l'autorizzazione e l'accesso al registro di sistema;
- *MSVCRT.DLL*, che è una libreria di runtime di C e C++ che fornisce funzioni di base per la gestione della memoria, l'input/output e la matematica;
- *WININET*, ovvero una libreria di windows che fornisce accesso alle funzionalità di rete, come la connessione a siti web, il download di file e l'invio di email.

Le sezioni di cui si compone il malware, invece, sono le seguenti

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

dove:

- *UPX0* rappresenta la dimensione della sezione *.text* del malware;
- *UPX1* rappresenta la dimensione della sezione *.data* del malware;

- *UPX2* rappresenta la dimensione totale del malware.

La sezione *.text* contiene il codice eseguibile del malware, e pertanto è responsabile dell'esecuzione delle azioni dannose dello stesso.
La sezione *.data* contiene i dati statici del malware, ovvero dati che non cambiano durante l'esecuzione dello stesso, come le stringhe e le costanti.

In definitiva, il presente malware può:

- in base alla libreria *KERNEL32.DLL*
  - leggere, scrivere e cancellare file
  - allocare e deallocare memoria
  - eseguire più attività contemporaneamente
- in base alla libreria *ADVAPI32.DLL*
  - aggirare le protezioni di sicurezza del sistema, come ad esempio l'autenticazione a due fattori
  - accedere a informazioni riservate
  - modificare le impostazioni del sistema
- in base alla libreria *MSVCRT.DLL*
  - allocare e deallocare memoria
  - leggere e scrivere dati da e verso file, porte seriali e altri dispositivi
  - eseguire calcoli
- in base alla libreria *WININET.DLL*
  - infettare altri computer
  - scaricare file dannosi
  - inviare email di spam