S10/L1 Epicode Cybersecurity

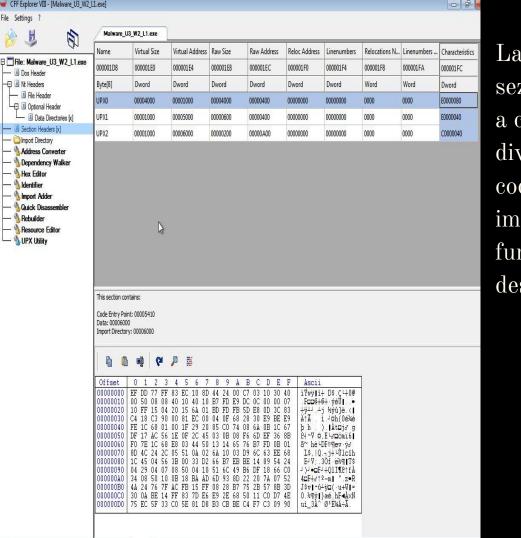
Analisi statica basica

Nell'esercizio di oggi ci viene richiesto di effettuare una analisi statica su un eseguibile malevolo e descrivere le librerie usate, le sezioni ed aggiungere delle nostre considerazioni finali.

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
ADVAPB2.dll	1	00000000	00000000	00000000	000060A5	00006080
MSVCRT.dll	1	00000000	00000000	00000000	000060B2	00006088
WININET.dll	1	00000000	00000000	00000000	000060BD	00006090

La prima cosa che andremo ad analizzare sono le librerie utilizzate in questo malware:

- KERNEL32.dll: libreria basilare contenente le principali funzioni di interazione col sistema operativo.
- ADVAPI32.dll: anche questa è una libreria basilare contenente funzioni di interazione con servizi e registri di Microsoft.
- MSVCRT.dll: libreria contenente funzioni in linguaggio C.
- WININET.dll: libreria contenente funzioni di implementazione di protocolli di rete.



La seconda richiesta era di analizzare le sezioni componenti il malware. Andando a controllare vediamo come esso sia diviso in tre sezioni che sono però codificate in ASCII, rendendo impossibile la comprensione delle funzioni che esplica e la conseguente descrizione richiesta.

Etichetta
di
minaccia
popolare

Categorie di minacce troiano s Etichette di famiglia A questo punt

Vuoi automatizzare i controlli?

AhnLab-V3

Trojan/Win32.StartPage.C26214

Alibaba

ALYac

Antiy-AVL

Arcabit

Avast

MEDIO

Avira (senza nuvole)

TrojanClicker:Win32/Generic.47e7b5e4

Trojan.Startpage.3072

Trojan/Win32.SGeneric

Win32:Generazione di malware

Win32:Generazione di malware

Trojan.Ser.Ulise.216

TR/Downloader.Gen

nella slide precedente, inseriamo il malware su un sito chiamato VirusTotal per verificare il suo funzionamento. Questo ci dirà quindi che il malware è di tipo **Trojan**, un virus che si presenta sotto forma di file non dannoso, che può prendere il controllo dell'intero sistema per farne ciò che più ritiene utile.

Vista l'impossibilità di analisi affrontata