

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	OFfs	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

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.

File Settings ?

File: Malware_U3_W2_L1.exe

- Dos Header
- NT Headers
 - File Header
 - Optional Header
 - Data Directories [x]
- Section Headers [x]
- Import Directory
- Address Converter
- Dependency Walker
- Hex Editor
- Identifier
- Import Addr
- Quick Disassembler
- Rebuilder
- Resource Editor
- UPX Utility

Malware_U3_W2_L1.exe












Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers ...	Characteristics
000001D8	000001E0	000001E4	000001E8	000001EC	000001F0	000001F4	000001F8	000001FA	000001FC
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
UPX0	00004000	00001000	00004000	00000400	00000000	00000000	0000	0000	E0000080
UPX1	00001000	00005000	00000600	00000400	00000000	00000000	0000	0000	E0000040
UPX2	00001000	00006000	00000200	00000400	00000000	00000000	0000	0000	C0000040

This section contains:

Code Entry Point: 00005410
Data: 00006000
Import Directory: 00006000

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000000	EF	DD	77	FF	83	EC	10	8D	44	24	00	C7	03	10	30	40	iYvyl+ D8 C+0@
00000010	00	50	08	08	40	10	40	10	E7	FD	E9	DC	0C	00	00	07	.Fcc6+0+ yel...•
00000020	10	FF	15	04	20	15	6A	01	ED	FD	FB	5D	E8	0D	3C	83	+j+ j yru)e.<I
00000030	C4	18	C3	90	00	81	EC	00	04	0F	68	28	30	E9	BE	E9	AtA . i -ch(0ekke
00000040	FE	1C	68	01	00	1F	29	20	85	C0	74	08	6A	0B	1C	67	p h .) lAtc)g
00000050	DF	17	AC	56	1E	0F	2C	45	03	0B	08	F6	6D	EF	36	8B	P-V n.E+ccmi6I
00000060	F0	7E	1C	68	E8	03	44	50	13	14	65	76	E7	FD	0B	01	8~ hA4DF"qev.gd
00000070	8D	4C	24	2C	05	51	0A	02	6A	10	03	D9	6C	63	EE	68	Is .Q. j+ +0icih
00000080	1C	45	04	56	3B	00	33	D2	66	E7	EB	BE	14	89	54	24	E+V. .30f:ekvITs
00000090	04	29	04	07	08	50	04	10	51	6C	49	B6	DF	18	66	C0	+)~cF+Q1IMetfA
000000A0	34	08	50	10	0B	18	BA	AD	6D	93	8D	22	20	7A	07	52	4CF+g+~nI " .z•R
000000B0	4A	24	76	7F	AC	FB	15	FF	08	28	E7	75	2B	57	8B	3D	J8vI~0-yC(-u+Vl=
000000C0	30	0A	BE	14	FF	83	7D	E6	E9	2E	68	50	11	C0	D7	4E	0.8qvI)ae hF4A>N
000000D0	75	EC	5F	33	C0	5E	81	D8	B3	CB	BE	C4	F7	C3	09	90	ui_3A" 0%EkA+A.

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  trojan.ulise/startpage	
Categorie di minacce	troiano  s
Etichette di famiglia	A questo punto
Analisi dei fornitori di sicurezza 	
Vuoi automatizzare i controlli?	
AhnLab-V3	 Trojan.Win32.StartPage.C26214
Alibaba	 TrojanClicker.Win32/Generic.47e7b5e4
ALYac	 Trojan.Startpage.3072
Antiy-AVL	 Trojan.Win32.SGeneric
Arcabit	 Trojan.Ser.Ulise.216
Avast	 Win32:Generazione di malware
MEDIO	 Win32:Generazione di malware
Avira (senza nuvole)	 TR/Downloader.Gen

Vista l'impossibilità di analisi affrontata 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.