

Sections viewer : [ Malware\_U3\_W2\_L1.exe ] 3 sections - alignment : 1000h

Nr	Virtual ...	Virtual s...	RAW D...	RAW size	Flags	Name	First bytes (hex)	First Ascii 20
01	00001000	00004000	00000400	00000000	E0000080	UPX0	! Z E R O S I Z E !	?
02 ep	00005000	00001000	00000400	00000600	E0000040	UPX1	EF DD 77 FF 83 EC 10 8D 44	w +D\$
03 im	00006000	00001000	00000A00	00000200	C0000040	UPX2	00 00 00 00 00 00 00 00	* d

  

Viewer

Section first bytes viewer

00000A80	20 61 00 00 00 00 00 30 61 00 00 00 00 00	a 0a
00000A90	36 61 00 00 00 00 00 4B 45 52 4E 45 4C 33 32	6a KERNEL32
00000AA0	2E 44 4C 4C 00 41 44 56 41 50 49 33 32 2E 64 6C	.DLL ADVAPI32.dl
00000AB0	6C 00 4D 53 56 43 52 54 2E 64 6C 6C 00 57 49 4E	MSVCRT.dll WIN
00000AC0	49 4E 45 54 2E 64 6C 6C 00 00 4C 6F 61 64 4C 69	INET.dll LoadLi
00000AD0	62 72 61 72 79 41 00 00 47 65 74 50 72 6F 63 41	braryA GetProcA
00000AE0	64 64 72 65 73 73 00 00 56 69 72 74 75 61 6C 50	ddress VirtualP
00000AF0	72 6F 74 65 63 74 00 00 56 69 72 74 75 61 6C 41	rotect VirtualA
00000B00	6C 6C 6F 63 00 00 56 69 72 74 75 61 6C 46 72 65	lloc VirtualFre
00000B10	65 00 00 00 45 78 69 74 50 72 6F 63 65 73 73 00	e ExitProcess

Overlay : No overlay data  
End of file : 00 00 00 00  
Section status : 01

Malware\_U3\_W2\_L1.exe

Module Name	Imports	OFs	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

Malware\_U3\_W2\_L1.exe

Name	Virtual Size	Virtual Address	Raw Size	Raw Address
Byte[8]	Dword	Dword	Dword	Dword
.text	000002DC	00001000	00001000	00001000
.rdata	00000372	00002000	00001000	00002000
.data	0000008C	00003000	00001000	00003000

- **Kernel32.dll**: libreria piuttosto comune che contiene le funzioni principali per interagire con il sistema operativo, ad esempio: manipolazione dei file, la gestione della memoria.
- **Advapi32.dll**: libreria che contiene le funzioni per interagire con i servizi ed i registri del sistema operativo Microsoft
- **.data**: la sezione «data» contiene tipicamente i dati / le variabili globali del programma eseguibile, che devono essere disponibili da qualsiasi parte del programma. Ricordate che una variabile si dice globale quando non è definita all'interno di un contesto di una funzione, ma bensì è **globalmente dichiarata** ed è di conseguenza accessibile da qualsiasi funzione dell'eseguibile.
- **.text**: la sezione «text» contiene le istruzioni (le righe di codice) che la CPU eseguirà una volta che il software sarà avviato. Generalmente questa è l'unica sezione di un file eseguibile che viene eseguita dalla CPU, in quanto tutte le altre sezioni contengono dati o informazioni a supporto.
- **.rdata**: la sezione «rdata» include generalmente le informazioni circa le librerie e le funzioni importate ed esportate dall'eseguibile, informazione che come abbiamo visto possiamo ricavare con CFF Explorer.
- **MSVCRT.dll**: libreria che contiene funzioni per la manipolazione stringhe, allocazione memoria e altro come chiamate per input/output in stile linguaggio C.

Possiamo notare che questo malware tenta di fare un'accesso verso l'esterno mantenendo la sessione