

# MALWARE ANALYSIS | STATICA BASICA

S10 - L1

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

Analizzando il file "Malware\_U3\_W2\_L1.exe" con il programma CFF, possiamo vedere le librerie che vengono richieste per il programma, cioè, importate a tempo di esecuzione (runtime). Come possiamo vedere nell'immagine, il programma richiede 4 librerie:

#### KERNEL32.dll

Fornisce funzioni fondamentali per attività quali gestione della memoria, operazioni di input/output, gestione di processi e thread, gestione degli errori e gestione del tempo di sistema.

#### ADVAPI32.dll

Contiene funzioni relative alla sicurezza, alla manipolazione del registro, alla registrazione degli eventi e ad altri servizi di sistema avanzati.

#### MSVCRT.dll

Fornisce supporto per varie funzioni runtime C, come l'allocazione della memoria, l'input/output di file, la manipolazione delle stringhe e le operazioni matematiche.

#### WININET.dll

È un componente che è viene utilizzato da molte applicazioni per accedere ai e HTTP per eseguire attività come il download di file, il caricamento di file e la navigazione di siti Web.

# Malware Analysis | Analisi statica basica

## S10 - L1

Ora diamo un'occhiata alle "sezioni" del programma. Possiamo vedere che ce ne sono 3: UPX0, UPX1 e UPX2. Selezionandone uno, possiamo ispezionarne il contenuto ASCII. Nell'immagine possiamo vedere uno di questi blocchi di testo ASCII, dove, tra molti altri caratteri, possiamo vedere alcune parole, come un pezzo di URL HTTP, la parola *ysisbook*, *MalService* e *SystemTimeToFile*.

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

Viewer

Section first bytes viewer

00000570	40 45 D8 8D 02 50 FF 35 70 0C 09 E0 50 BE EF D6	@EØ□ Py5p□ âP%äÖ
00000580	6C 03 D4 E4 11 15 48 B0 04 32 00 B6 FB 6D 43 14	l□ôâ□□H"□2 ¶ûm...
00000590	44 6D 4D E0 85 75 E0 02 6D 1B ED CB D4 E4 E8 8D	DmMà...uà m iÊÔàâ□
000005A0	FD A0 3B 30 49 DC FD F7 FF D7 34 40 1F 45 EC 8B	ý ;0IÛý+ÿ×4@□Eκ
000005B0	08 8B 09 89 4D D0 50 51 36 9C 59 59 C3 8B C6 6E	< %dMðPQ6ceYYÄ<Æn
000005C0	B6 AD E0 2B D0 1F 38 FF 25 3C 05 4C F3 35 DE F6	¶-â+ð□8ÿ%<□Ló...
000005D0	60 1F 03 04 65 29 D2 B2 25 EC 05 7E C3 C3 CC 00	`□□□e)Ö²%i□~Ä...
000005E0	2F 64 80 28 32 33 68 00 00 37 A0 39 FF 80 7B 94	/d€(23h 7 9ÿ€{"
000005F0	12 B2 04 44 91 AF 0B 29 FF 8F 8A 4D 61 6C 53 65	□²□D"□)ÿ□ŠMal5e
00000600	72 76 69 63 65 FE DB 3F A4 73 48 47 4C 33 34 35	rvicépÛ?×sHGL345
00000610	07 68 74 74 70 3A 2F 2F 7F FF B7 BF DD 00 2E 6D	□http://wÿ·¿ÿ.m
00000620	1E 77 61 72 65 61 6E 07 79 73 69 73 62 6F 6F 6B	□warean□ysisbook
00000630	2E 63 6F FF DB DB 6F 6D 23 49 6E 74 36 6E 65 74	.coÿÛÛom#Int6net
00000640	20 45 78 70 6C 6F 21 72 20 38 46 45 49 C7 2E 30	ExploIr 8FEIÇ.0
00000650	3C 01 20 01 A0 C0 09 65 73 14 15 98 10 10 BF 9D	<□ □ À es□□"□...
00000660	FF FF 01 53 79 73 74 65 6D 54 69 6D 65 54 6F 46	ÿÿ□SystemTimeToF
00000670	69 6C 65 15 47 65 74 4D 6F C1 B6 FC DA 64 75 0E	ile□GetMoÁ¶ûÚdu□
00000680	12 4E 61 41 13 43 76 67 7F 2B F3 2A 57 61 69 74	□NaA□Cvg□+ó*...
00000690	61 62 27 72 15 45 78 B7 FD ED 0F 50 72 6F 63	ab'r□Ex·ÿið□Proc
000006A0	65 73 73 6C 45 70 65 6F 4D 75 34 70 18 5F 5A 62	...D...Mal...û³&

Clip

Charset

Close

Questo è il contenuto ASCII di UPX2, dove sembra che, oltre ad avere molto "padding", chiami le 4 librerie citate prima, e avvii il servizio "ServiceA" e internet "OpenA"

Viewer

Section first bytes viewer

0000A60	00 00 00 00 C8 60 00 00 D6 60 00 00 E6 60 00 00	È` Ö` æ`				
0000A70	F6 60 00 00 04 61 00 00 12 61 00 00 00 00 00	ö` □a □a				
0000A80	20 61 00 00 00 00 00 00 30 61 00 00 00 00 00	a 0a				
0000A90	36 61 00 00 00 00 00 00 48 45 52 4E 45 4C 33 32	6a KERNEL32				
0000AA0	2E 44 4C 4C 00 41 44 56 41 50 49 33 32 2E 64 6C	.DLL ADVAPI32.dll				
0000AB0	6C 00 4D 53 56 43 52 54 2E 64 6C 6C 00 57 49 4E	IMSVCRT.dll WIN				
0000AC0	49 4E 45 54 2E 64 6C 6C 00 00 4C 6F 61 64 4C 69	INET.dll LoadLi				
0000AD0	62 72 61 72 79 41 00 00 47 65 74 50 72 6F 63 41	braryA GetProcA				
0000AE0	64 64 72 65 73 73 00 00 56 69 72 74 75 61 6C 50	ddress VirtualP				
0000AF0	72 6F 74 65 63 74 00 00 56 69 72 74 75 61 6C 41	rotect VirtualA				
0000B00	6C 6C 6F 63 00 00 56 69 72 74 75 61 6C 46 72 65	lloc VirtualFre				
0000B10	65 00 00 00 45 78 69 74 50 72 6F 63 65 73 73 00	e ExitProcess				
0000B20	00 00 43 72 65 61 74 65 53 65 72 76 69 63 65 41	CreateServiceA				
0000B30	00 00 65 78 69 74 00 00 49 6E 74 65 72 6E 65 74	exit Internet				
0000B40	4F 70 65 6E 41 00 00 00 00 00 00 00 00 00 00 00	OpenA				
0000B50	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00					
0000B60	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00					
0000B70	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00					
0000B80	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00					
0000B90	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00					

Clip Charset Close

Dopo inserire il file su VirusTotal, possiamo vedere che questo programma fa tante cose, come pianificare una task che eseguire codice malizioso, o modificare lo status dei servizi attivi sul sistema.

### MITRE ATT&CK Tactics and Techniques

#### — Execution TA0002

##### 🔒 Scheduled Task/Job T1053

Adversaries may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code.

##### 🔒 Scheduled Task T1053.005

Adversaries may abuse the Windows Task Scheduler to perform task scheduling for initial or recurring execution of malicious code.

##### 🔒 Command and Scripting Interpreter T1059

Very long cmdline option found, this is very uncommon (may be encrypted or packed)

##### 🔒 Shared Modules T1129

The process tried to load dynamically one or more functions.

##### 🔒 Service Execution T1569.002

Uses sc.exe to modify the status of services

#### — Persistence TA0003

##### 🔒 Scheduled Task/Job T1053

Adversaries may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code.

##### 🔒 Scheduled Task T1053.005

Adversaries may abuse the Windows Task Scheduler to perform task scheduling for initial or recurring execution of malicious code.

##### 🔒 Create or Modify System Process T1543

Adversaries may create or modify system-level processes to repeatedly execute malicious payloads as part of persistence.

##### 🔒 Windows Service T1543.003

Modifies existing windows services

Uses sc.exe to modify the status of services

Creates or modifies windows services

Adversaries may create or modify Windows services to repeatedly execute malicious payloads as part of persistence.

##### 🔒 Boot or Logon Autostart Execution T1547

Adversaries may configure system settings to automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges on compromised systems.

##### 🔒 Registry Run Keys / Startup Folder T1547.001

Adversaries may achieve persistence by adding a program to a startup folder or referencing it with a Registry run key.

##### 🔒 LSASS Driver T1547.008

Spawns drivers

##### 🔒 DLL Side-Loading T1574.002

Tries to load missing DLLs