

1. Malware analysis: Analisi statica basica

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
00000A98	N/A	00000A00	00000A04	00000A08	00000A0C	00000A10
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

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
N/A	000060C8	0000	LoadLibraryA
N/A	000060D6	0000	GetProcAddress
N/A	000060E6	0000	VirtualProtect
N/A	000060F6	0000	VirtualAlloc
N/A	00006104	0000	VirtualFree
N/A	00006112	0000	ExitProcess

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
00000AA5	N/A	00000A14	00000A18	00000A1C	00000A20	00000A24
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

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
N/A	00006120	0000	CreateServiceA

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
00000AB2	N/A	00000A28	00000A2C	00000A30	00000A34	00000A38
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

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
N/A	00006130	0000	exit

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
00000ABD	N/A	00000A3C	00000A40	00000A44	00000A48	00000A4C
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

OFTs	FTs (IAT)	Hint	Name
N/A	00000A90	00000B36	00000B38
Dword	Dword	Word	szAnsi
N/A	00006136	0000	InternetOpenA

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

Malware

Kernel.32.dll libreria piuttosto comune che contiene le funzioni principali per interagire con il sistema operativo, ad esempio: manipolazione file; gestione memoria.

Advapi32.dll libreria che contiene le funzioni per integrare con i servizi ed i registri del sistema operativo Microsoft

GDI32.dll libreria che contiene le funzioni per implementare e manipolare delle grafiche e dei suoi effetti.

Wininet.dll libreria che contiene le funzioni per l'implementazione di alcuni protocolli di rete http,ftp,ntp.

PE

UPX supporta due meccanismi per la decompressione: una tecnica sul posto e l'estrazione in un file temporaneo.

La tecnica sul posto, che decompone l'eseguibile in memoria, non è possibile su tutte le piattaforme supportate. Ha il vantaggio di essere più efficiente in termini di memoria e che l'ambiente impostato dal sistema operativo rimane corretto.

Il resto utilizza l'estrazione in un file temporaneo. Questa procedura comporta un sovraccarico aggiuntivo e altri svantaggi; tuttavia, consente di comprimere qualsiasi formato di file eseguibile. Il metodo di estrazione su file temporaneo presenta diversi svantaggi:

I permessi speciali vengono ignorati, come suid.

argv[0] non sarà significativo.

Più istanze in esecuzione dell'eseguibile non sono in grado di condividere segmenti comuni.

L'imballaggio UPX non modificato viene spesso rilevato e decompresso dagli scanner del software antivirus. UPX ha anche una funzione incorporata per decomprimere gli eseguibili non modificati impacchettati con se stesso.