

ANALISI STATICA BASICA

S10L1


INDICE

- TRACCIA
- LIBRERIE
- KERNEL32.DLL
- ADVAPI32.DLL
- MSVCRT.DLL
- WININET.DLL
- HEADER
- CONCLUSIONI



TRACCIA

Con riferimento al file eseguibile contenuto nella cartella «Esercizio_Pratico_U3_W2_L1» presente sul Desktop della vostra macchina virtuale dedicata all'analisi dei malware, rispondere ai seguenti quesiti:

- Indicare le librerie importate dal malware, fornendo una descrizione per ognuna di esse
 - Indicare le sezioni di cui si compone il malware, fornendo una descrizione per ognuna di essa
 - Aggiungere una considerazione finale sul malware in analisi in base alle informazioni raccolte
- 

LIBRERIE

Malware_U3_W2_L1.exe						
Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.DLL	9	00000000	00000000	00000000	0000216C	00002010
ADVAPI32.dll	3	00000000	00000000	00000000	00002179	00002000
MSVCRT.dll	13	00000000	00000000	00000000	00002186	00002038
WININET.dll	2	00000000	00000000	00000000	00002191	00002070

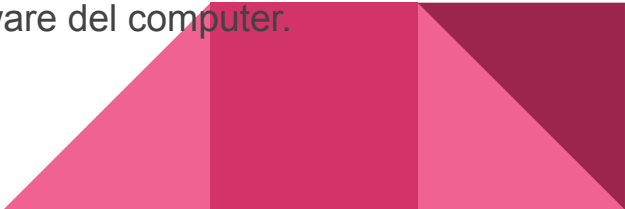
Come possiamo vedere dall'immagine qui sopra sono presenti 4 librerie:
KERNEL32.DLL, ADVAPI32.DLL, MSVCRT.DLL, WININET.DLL

Kernel32.dll

La libreria kernel32.dll è una parte fondamentale del sistema operativo Windows. Contiene una vasta gamma di funzioni utili per il sistema operativo e per le applicazioni che vi girano sopra. Ecco alcuni dei compiti principali svolti da kernel32.dll:

- Gestione della memoria
- Gestione dei file
- Gestione dei processi e dei thread
- Gestione del tempo e delle date
- Gestione degli errori
- Gestione degli input/output
- Gestione della sincronizzazione
- Gestione delle risorse del sistema

In breve, **kernel32.dll** fornisce una serie di funzioni di basso livello essenziali per il funzionamento del sistema operativo Windows e per l'interazione tra le applicazioni e l'hardware del computer.



Kernel32.dll

Come si vede dalla figura di fianco la libreria kernel32.dll nel nostro caso importa: LoadLibraryA, GetProcAddress, VirtualProtect, VirtualAlloc, VirtualFree, ExitProcess.

Module Name	Imports	OFTs	TimeStamp	ForwarderChain	Name RVA	FTs (IAT)
0000216C	N/A	0000208C	00002090	00002094	00002098	0000209C
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.DLL	9	00000000	00000000	00000000	0000216C	00002010

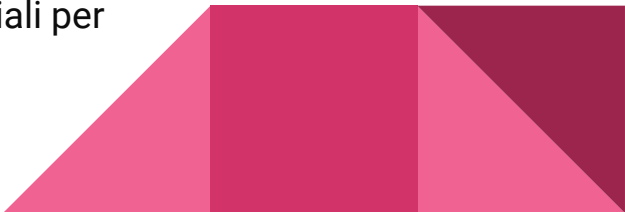
OFTs	FTs (IAT)	Hint	Name	
Dword	Dword	Word	szAnsi	
N/A	0000219E	0000	SystemTimeToFileTime	
N/A	000021B4	0000	GetModuleFileNameA	
N/A	000021C8	0000	CreateWaitableTimerA	
N/A	000021DE	0000	ExitProcess	
N/A	000021EC	0000	OpenMutexA	
N/A	000021F8	0000	SetWaitableTimer	
N/A	0000220A	0000	WaitForSingleObject	
N/A	00002220	0000	CreateMutexA	
N/A	0000222E	0000	CreateThread	

ADVAPI32.DLL

La libreria advapi32.dll è un'altra libreria fondamentale del sistema operativo Windows. Essa fornisce una vasta gamma di funzioni per la gestione della sicurezza, della gestione degli account utente e di altri servizi avanzati per le applicazioni Windows. Ecco alcuni dei compiti principali svolti da advapi32.dll:

- Servizi di autenticazione e autorizzazione
- Gestione dei servizi di Windows
- Criptografia e sicurezza
- Audit e logging
- Gestione dei token di accesso
- Controllo dei privilegi
- Manipolazione del registro di sistema

In sintesi, advapi32.dll è una libreria critica per la gestione della sicurezza e dei servizi avanzati nel sistema operativo Windows, offrendo funzioni essenziali per garantire l'integrità, la sicurezza e la gestione delle risorse del sistema.



ADVAPI32.DLL

Come vediamo
nel nostro caso
abbiamo la
libreria
ADVAPI32.dll
importa:
CreateServiceA,
StartService,
OpenSCManager


Malware_U3_W2_L1.exe						
Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
00002179	N/A	000020A0	000020A4	000020A8	000020AC	000020B0
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
ADVAPI32.dll	3	00000000	00000000	00000000	00002179	00002000
OFTs	FTs (IAT)	Hint	Name			
Dword	Dword	Word	szAnsi			
N/A	0000223C	0000	CreateServiceA			
N/A	0000224C	0000	StartServiceCtrlDispatcherA			
N/A	0000226A	0000	OpenSCManagerA			

MSVCRT.DLL

La libreria MSVCRT.DLL è parte del runtime della libreria Microsoft Visual C++, comunemente noto come Microsoft Visual C++ Runtime Library. Questa libreria fornisce un insieme di funzioni essenziali per programmi compilati con il compilatore Microsoft Visual C++. Di seguito alcuni compiti svolti:

- Gestione della memoria
- Gestione delle stringhe
- Gestione dell'input/output
- Funzioni matematiche
- Gestione dei file
- Gestione dell'errore

In sostanza, MSVCRT.DLL fornisce un insieme di funzioni standard che vengono utilizzate dai programmi compilati con il compilatore Microsoft Visual C++. Queste funzioni aiutano a semplificare lo sviluppo del software e a garantire la compatibilità tra i programmi che utilizzano la stessa libreria runtime.



MSVCRT.dll

Come possiamo vedere nel nostro caso svolge molte funzioni tra cui: exit, filter, initterm, adjust.


Malware_U3_W2_L1.exe						
Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
00002186	N/A	000020B4	000020B8	000020BC	000020C0	000020C4
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
MSVCRT.dll	13	00000000	00000000	00000000	00002186	00002038
OFTs	FTs (IAT)	Hint	Name			
Dword	Dword	Word	szAnsi			
N/A	0000227A	0000	_exit			
N/A	00002282	0000	_XcptFilter			
N/A	00002290	0000	exit			
N/A	00002296	0000	__p__initenv			
N/A	000022A6	0000	__getmainargs			
N/A	000022B6	0000	_initterm			
N/A	000022C2	0000	__setusermatherr			
N/A	000022D4	0000	_adjust_fdiv			
N/A	000022E2	0000	__p__commode			

WININET.dll

Questa libreria è utilizzata principalmente per la comunicazione via Internet e per l'accesso alle risorse Web. Ecco alcuni dei compiti principali svolti da wininet.dll:

- Gestione delle connessioni internet
- Download e upload di file
- Gestione cookie
- Cache delle risorse
- Gestione dei proxy
- Sicurezza internet

In sostanza, wininet.dll è una componente fondamentale per le applicazioni Windows che richiedono funzionalità di rete e accesso a risorse Internet, consentendo loro di comunicare e interagire con i server remoti tramite protocolli Internet standard.



WININTE.dll

Nel nostro caso
gestisce solo
due funzionalità
tra cui
InternetOpenUrl
e InternetOpenA.

Malware_U3_W2_L1.exe						
Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
00002191	N/A	000020C8	000020CC	000020D0	000020D4	000020D8
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
WININET.dll	2	00000000	00000000	00000000	00002191	00002070
OFTs	FTs (IAT)	Hint	Name			
Dword	Dword	Word	szAnsi			
N/A	0000232A	0000	InternetOpenUrlA			
N/A	0000233C	0000	InternetOpenA			

Header

Malware_U3_W2_L1.exe									
Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers ...	Characteristics
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
.text	000002DC	00001000	00001000	00001000	00000000	00000000	0000	0000	60000020
.rdata	00000372	00002000	00001000	00002000	00000000	00000000	0000	0000	40000040
.data	0000008C	00003000	00001000	00003000	00000000	00000000	0000	0000	C0000040

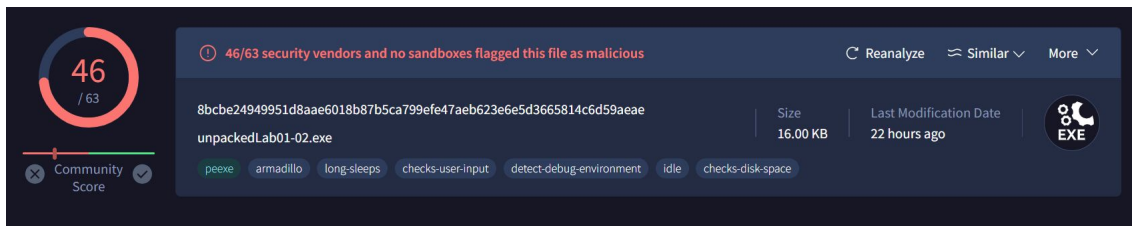
Come possiamo vedere dalla figura, dopo aver utilizzato la “UPX Utility”, abbiamo tre sezioni nell’header:

- .text
- .rdata
- .data

Conclusioni

In conclusione possiamo dire che dalle ricerche che abbiamo fatto abbiamo un Malware complesso che al momento con le conoscenze di adesso non ci è concesso conoscere di più.

Grazie ad un ulteriore piccolo approfondimento, utilizzando “VirusTotal” abbiamo scoperto che è un trojan. Nelle prossime lezioni avremo modo di approfondire.





GRAZIE