CYBER SECURITY & ETHICAL HACKING

MALWARE ANALYSIS

report Rafael Manago

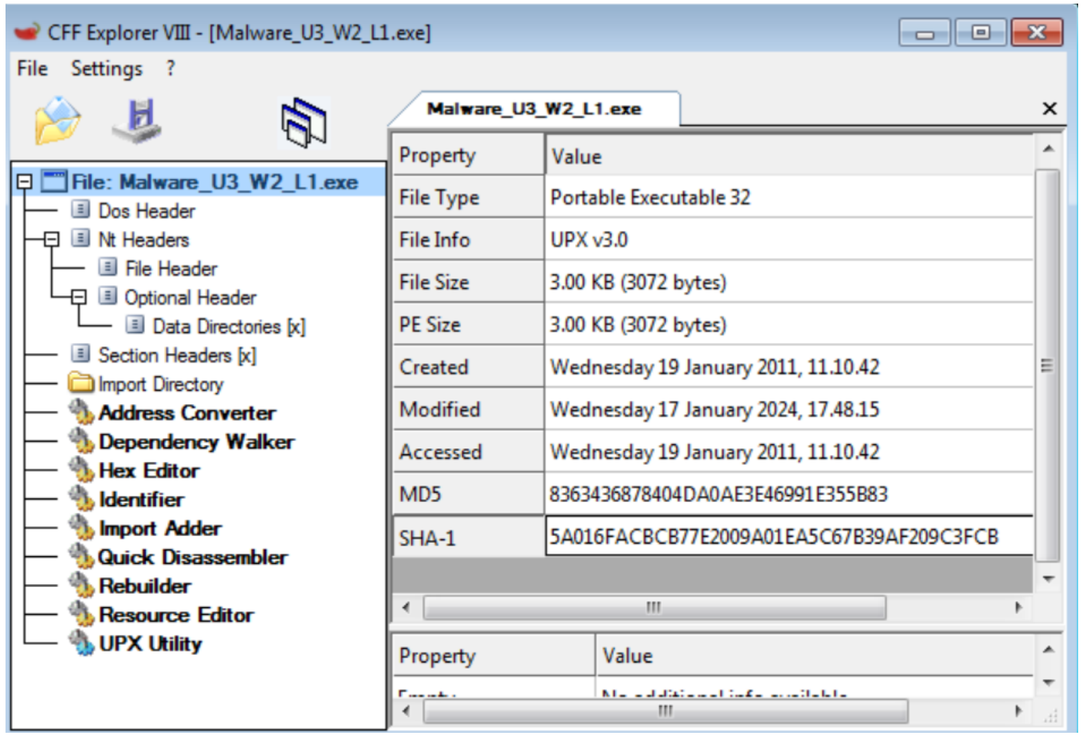
traccia

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 descrizioneper ognuna di esse

• Indicare le sezionidi cui si compone il malware, fornendo una descrizioneper ognuna di essa

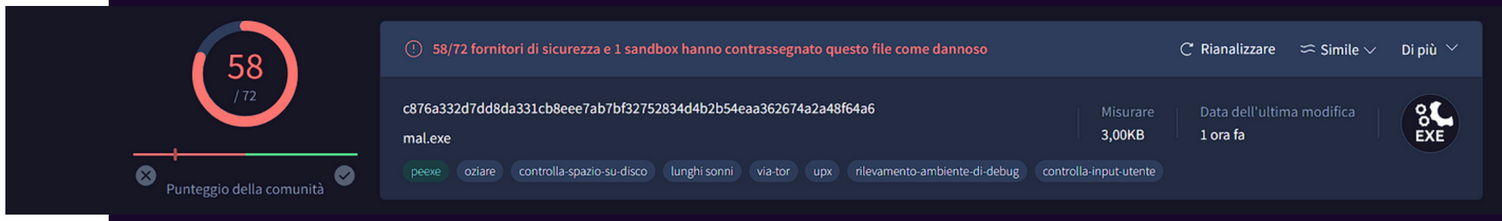
• Aggiungere una considerazione finale sul malware in analisi in base alle informazioni raccolte

Esaminare le librerie e le funzioni richieste dall'eseguibile contenute nell'header PE è cruciale per comprendere la natura del malware. L'header PE del file eseguibile fornisce un elenco delle funzioni che possono essere utilizzate da altri programmi o dall'utente. Identificare le funzioni importanti esportate dal malware, come nel caso del file eseguibile Malware U3 W2 L1.exe, richiede l'uso di strumenti appositi come CFF Explorer, un'applicazione per Windows progettata per eseguire questa analisi. Questo strumento consente di esaminare in dettaglio le funzioni esportate dal malware, fornendo informazioni cruciali per comprendere il suo comportamento e il suo potenziale impatto sul sistema.



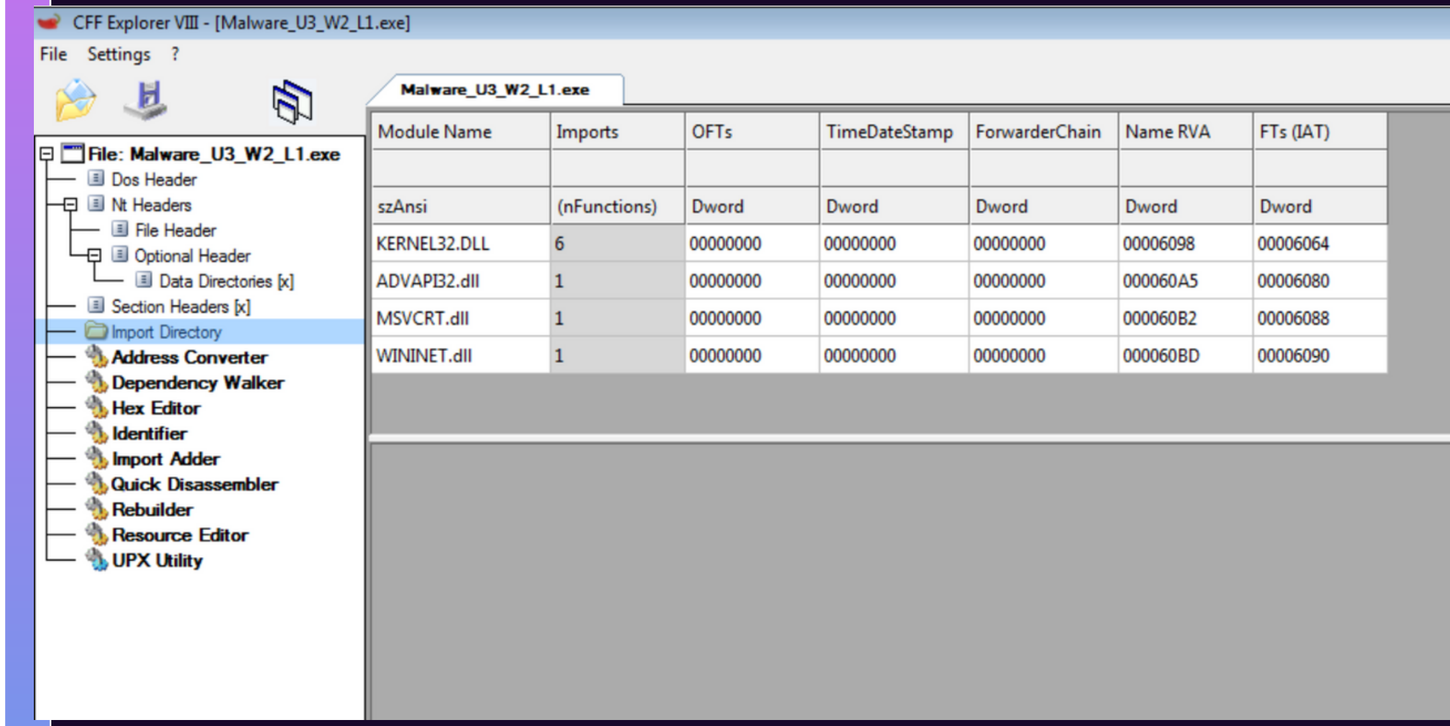
Primi passi

Utilizzando il codice hash in formato MD5, che rappresenta un identificatore univoco del file, è possibile consultare servizi come VirusTotal per ottenere informazioni sull'andamento storico del malware. Attraverso questo metodo, è possibile accedere a una vasta base di dati che contiene analisi e informazioni su come il malware sia stato trattato in passato, inclusi eventuali rilevamenti da parte di motori antivirus, comportamenti osservati e altre informazioni pertinenti. Questa analisi storica fornisce una panoramica utile per comprendere la natura e l'evoluzione del malware nel tempo.



CFF Explorer

Per individuare le librerie cruciali utilizzate dal malware, possiamo dirigerci verso la sezione dedicata all'analisi delle librerie all'interno di CFF Explorer. Qui possiamo constatare che il malware ha importato un totale di quattro librerie.



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

Analisi delle librerie

Name
szAnsi
LoadLibraryA
GetProcAddress
VirtualProtect
VirtualAlloc
VirtualFree
ExitProcess

Kernel32.DLL

Questa libreria costituisce il fulcro per le interazioni con il sistema operativo, includendo una serie di funzioni fondamentali richiamate dal malware.

Name
szAnsi
CreateServiceA

ADVAPI32.dll

La libreria ADVAPI32.dll offre una gamma di funzioni avanzate per i servizi, concentrando le sue operazioni sulla gestione dei servizi di sistema, sicurezza e privilegi. Inoltre, gestisce operazioni avanzate relative ai token di sicurezza, crittografia, eventi e altro ancora. La sua funzione esecutiva è unica.

Name
szAnsi
exit

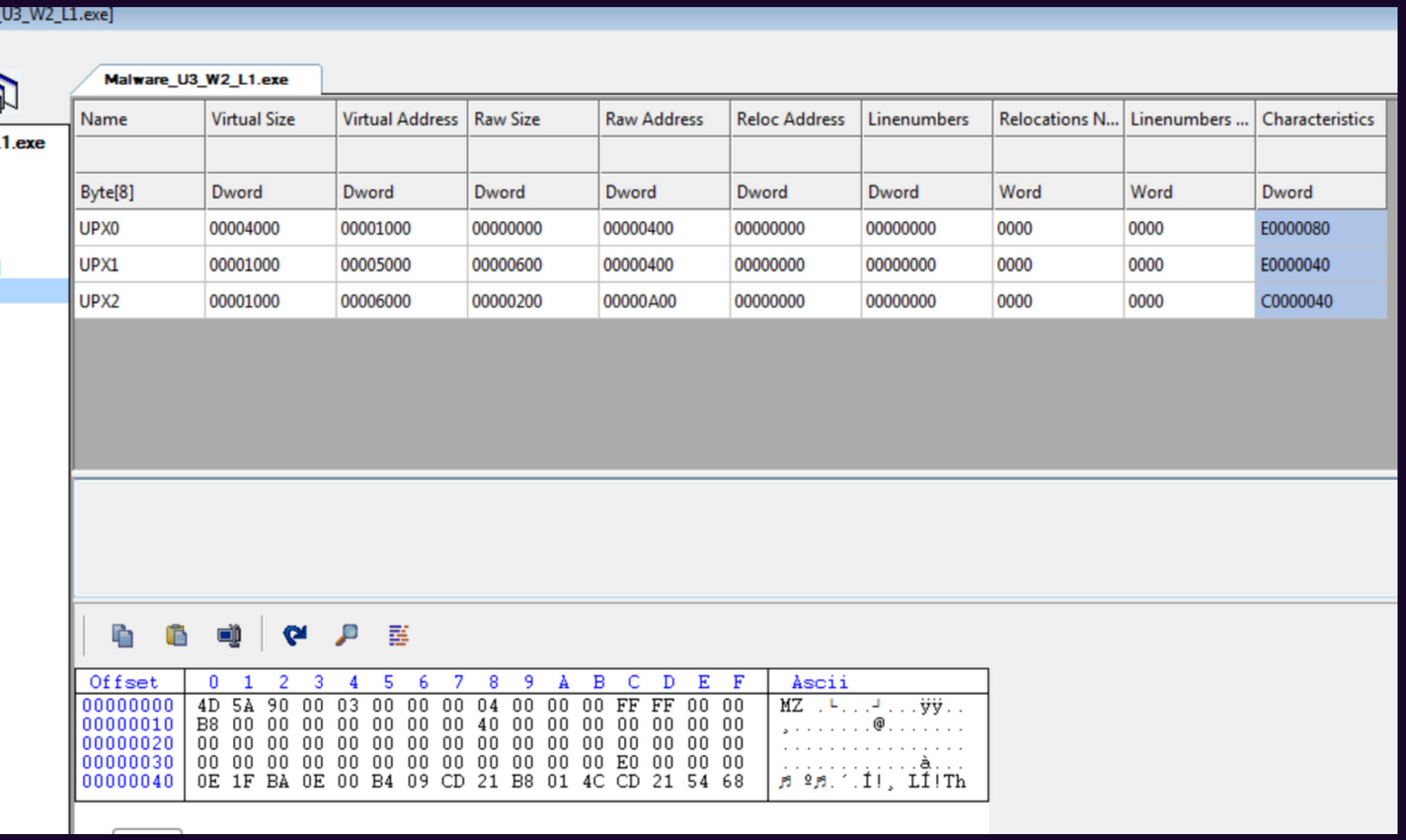
MSVCRT.dll

Questa libreria fornisce un insieme di funzioni essenziali per il runtime dei linguaggi di programmazione C e C++. È una componente fondamentale dell'ambiente di sviluppo Microsoft Visual C++, indispensabile per l'esecuzione di programmi scritti in C o C++ su sistemi operativi Windows.

Name
szAnsi
InternetOpenA

WININET.dll

Questa libreria fornisce un insieme di strumenti per accedere alle risorse su Internet in ambienti Windows. È una componente integrante del sistema operativo che offre un'interfaccia per connettersi e comunicare tramite protocolli Internet come HTTP, HTTPS, FTP e altri.



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
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

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000000	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	MZ ..└...┘...ÿÿ..
00000010	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	¸.......@.......
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00000030	00	00	00	00	00	00	00	00	00	00	00	00	E0	00	00	00	............à...
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	♫ º♫.´.Í!¸.LÍ!Th

SEZIONE DELL'HEADER

l'header del formato PE ci indica anche le sezioni di cui sei compone il software ,ogni sezione ha un preciso scopo .

Quando si utilizza UPX per comprimere un file eseguibile, il contenuto viene diviso in diverse sezioni gestite da UPX stesso. Una di queste sezioni, comunemente chiamata UPX0, generalmente contiene il nucleo dell'eseguibile dopo la compressione, mentre le altre sezioni sono numerate in modo incrementale, come UPX1, UPX2 e così via. È stato notato che il malware potrebbe aver mascherato il vero nome di queste sezioni, rendendo difficile identificarle e comprenderne il contenuto.

Considerazioni finali

Questo malware mostra caratteristiche avanzate che rendono complessa l'esecuzione di un'analisi statica di base. Ciò è dovuto al fatto che il malware importa le librerie necessarie durante l'esecuzione del programma anziché durante la compilazione.

THANK YOU