

CFF Explorer VIII - [Malware_U3_W2_L1.exe]

File Settings ?

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

File: Malware_U3_W2_L1.exe

- Dos Header
- Nt Headers
 - File Header
 - Optional Header
 - Data Directories [x]
 - Section Headers [x]
 - Import Directory
- Address Converter
- Dependency Walker
- Hex Editor
- Identifier
- Import Adder
- Quick Disassembler
- Rebuilder
- Resource Editor
- UPX Utility

Indicare le librerie importate dal malware, fornendo una descrizione per ognuna di esse

"**KERNEL32.dll**" è una libreria di sistema essenziale nel sistema operativo Windows. Si tratta di una Dynamic Link Library (DLL) che contiene funzioni e procedure di basso livello che sono fondamentali per il funzionamento del sistema operativo. Ecco una breve descrizione delle principali funzioni svolte da "KERNEL32.dll":

1. **Gestione dei Processi e dei Thread:** Fornisce funzioni per la gestione dei processi e dei thread nel sistema, inclusi avvio, sospensione e terminazione dei processi.
2. **Gestione della Memoria:** Contiene funzioni per l'allocazione e la gestione della memoria, come la creazione di spazi di indirizzi virtuali, la lettura/scrittura di memoria e la gestione degli errori di pagina.
3. **Gestione dei File e dei Dischi:** Offre funzioni per la gestione dei file e delle directory, inclusa l'apertura, la chiusura, la lettura e la scrittura di file. Inoltre, fornisce funzionalità di gestione dei dischi.
4. **Gestione degli Errori e delle Eccezioni:** Include funzioni per la gestione degli errori e delle eccezioni, come la cattura e la gestione degli errori, la definizione di gestori di eccezioni e la registrazione degli errori di sistema.
5. **Comunicazione e Sincronizzazione:** Fornisce meccanismi per la comunicazione e la sincronizzazione tra processi e thread, come le code di messaggi, i semafori, i mutex e altri oggetti di sincronizzazione.
6. **Funzioni di Supporto:** Contiene molte altre funzioni di supporto utili per l'interazione con il sistema operativo, tra cui la gestione degli orari, la manipolazione delle stringhe, la gestione dei percorsi e altro ancora.

In sintesi, "**KERNEL32.dll**" svolge un ruolo cruciale nel fornire un'interfaccia tra le applicazioni utente e il sistema operativo Windows, offrendo un'ampia gamma di funzionalità di basso livello necessarie per il funzionamento stabile del sistema.

"ADVAPI32.dll" è un'altra libreria di sistema essenziale in ambienti Windows. Questa Dynamic Link Library (DLL) contiene funzioni che supportano diversi aspetti della sicurezza, della gestione degli account e di altri servizi avanzati. Ecco una breve descrizione delle principali funzioni svolte da "ADVAPI32.dll":

1. **Servizi di Autenticazione e Autorizzazione:** Contiene funzioni per la gestione dell'autenticazione e dell'autorizzazione degli utenti, inclusi metodi per verificare l'identità degli utenti e determinare i loro diritti di accesso.
2. **Registrazione del Servizio e dei Componenti:** Fornisce funzioni per la registrazione e la gestione dei servizi di sistema, così come la registrazione di componenti software. Questo è fondamentale per il corretto funzionamento dei servizi di Windows.
3. **Gestione delle Chiavi di Registro:** Contiene funzioni per la lettura, la scrittura e la gestione delle chiavi di registro di sistema. La gestione delle chiavi di registro è cruciale per le impostazioni di configurazione e le informazioni di sistema.
4. **Crittografia e Sicurezza:** Offre funzioni di crittografia e decrittografia, nonché servizi di sicurezza come la generazione di chiavi, la firma digitale e la verifica delle firme. Queste funzionalità sono fondamentali per garantire la sicurezza delle informazioni.
5. **Event Logging:** Fornisce funzioni per la registrazione degli eventi di sistema, inclusi avvisi, avvisi di sicurezza e informazioni di audit. Questi log sono utilizzati per la diagnostica e la sicurezza.
6. **Gestione dei Servizi di Windows:** Contiene funzioni per la gestione dei servizi di Windows, come l'installazione, la disinstallazione, l'avvio e l'arresto dei servizi.

In sintesi, "ADVAPI32.dll" svolge un ruolo fondamentale nella gestione della sicurezza, dell'autenticazione e di altri servizi avanzati nel sistema operativo Windows. Le sue funzioni sono essenziali per garantire l'integrità, la sicurezza e la corretta operatività del sistema.

"**MSVCRT.dll**" è una Dynamic Link Library (DLL) che fa parte dell'ambiente di runtime di Microsoft Visual C++. Essa fornisce un set di funzioni di runtime necessarie per l'esecuzione di programmi compilati utilizzando il compilatore Microsoft Visual C++. Ecco una breve descrizione delle principali funzioni svolte da "MSVCRT.dll":

1. **Gestione della Memoria Dinamica:** La libreria gestisce le operazioni di allocazione e deallocazione della memoria dinamica attraverso funzioni come **malloc**, **free**, **calloc** e **realloc**.
2. **Gestione dei File e dei Flussi di I/O:** Fornisce funzioni per operazioni di input/output, inclusi metodi per aprire, chiudere, leggere e scrivere file. Ad esempio, **fopen**, **fclose**, **fread**, **fwrite**.
3. **Manipolazione delle Stringhe:** Contiene funzioni per la manipolazione delle stringhe, come **strcpy**, **strcat**, **strlen**, **strcmp**, che sono utili per operazioni di gestione delle stringhe.
4. **Gestione del Tempo:** Include funzioni per operazioni relative al tempo, come **time**, **difftime** e altre funzioni di data/ora.
5. **Conversione di Tipi:** Fornisce funzioni per la conversione tra diversi tipi di dati, come **atoi**, **atof**, **itoa**, e altre funzioni simili.
6. **Matematica:** Contiene alcune funzioni matematiche di base, come **abs**, **fabs**, **sqrt**, **pow**, che sono utili per operazioni matematiche.
7. **Manipolazione dei File Descriptor:** La libreria offre funzioni per la manipolazione dei descrittori di file, come **fileno** e **fdopen**.
8. **Gestione delle Eccezioni:** Supporta funzioni per la gestione delle eccezioni e delle situazioni di errore, come **abort** e **signal**.
9. **Altre Funzioni di Runtime:** Include una varietà di altre funzioni di runtime, come **exit**, **rand**, **qsort** e altre utili operazioni di runtime.

In sostanza, "**MSVCRT.dll**" fornisce un insieme di funzioni di supporto di runtime che sono necessarie per garantire che i programmi compilati con il compilatore Microsoft Visual C++ possano eseguire correttamente e interagire con il sistema operativo.

"**WININET.dll**" è una Dynamic Link Library (DLL) di sistema di Microsoft Windows, ed è parte integrante del sistema operativo. Questa libreria fornisce un insieme di funzioni per la gestione delle operazioni di rete e delle connessioni Internet. Ecco una breve descrizione delle principali funzioni svolte da "**WININET.dll**":

1. **Gestione delle Connessioni HTTP e HTTPS:** Fornisce funzioni per la gestione delle connessioni HTTP e HTTPS, consentendo alle applicazioni di inviare richieste e ricevere risposte dai server Web. Questo include funzioni per l'apertura, la chiusura e la gestione delle sessioni di connessione.
2. **Download e Upload di File:** Permette il download e l'upload di file da e verso server remoti mediante funzioni come **InternetOpenUrl**, **InternetReadFile**, **InternetOpen**, **InternetWriteFile** e altre.
3. **Gestione dei Cookie:** Supporta la gestione dei cookie durante le operazioni di navigazione su Internet, consentendo alle applicazioni di mantenere informazioni sullo stato della sessione.
4. **Cache di Internet:** Fornisce funzioni per l'accesso e la gestione della cache di Internet, permettendo alle applicazioni di controllare e manipolare le risorse memorizzate nella cache.
5. **Gestione dei Proxy:** Consente alle applicazioni di configurare e utilizzare proxy durante le connessioni Internet, inclusa la possibilità di impostare le impostazioni proxy del sistema.
6. **Gestione delle Risorse URL:** Offre funzioni per l'analisi e la manipolazione degli URL, consentendo alle applicazioni di estrarre informazioni specifiche dagli indirizzi Web.
7. **Supporto per i Protocolli Internet:** Supporta vari protocolli Internet, come HTTP, HTTPS, FTP e altri, offrendo agli sviluppatori la flessibilità di utilizzare diversi protocolli di comunicazione.
8. **Gestione delle Connessioni Sicure:** Fornisce funzioni per la gestione di connessioni sicure tramite SSL/TLS, garantendo la sicurezza delle comunicazioni su reti non sicure.

In sintesi, "**WININET.dll**" è essenziale per le applicazioni Windows che richiedono funzionalità di rete e accesso a risorse su Internet. Essa fornisce un'interfaccia per l'implementazione di operazioni di rete, facilitando lo sviluppo di applicazioni che richiedono connettività Internet.

CFF Explorer VIII - [Malware_U3_W2_L1.exe]

File Settings ?

Malware_U3_W2_L1.exe

File: Malware_U3_W2_L1.exe

- Dos Header
- Nt Headers
- File Header
- Optional Header
- Data Directories [x]
- Section Headers [x]
 - Import Directory
 - Address Converter
 - Dependency Walker
 - Hex Editor
 - Identifier
 - Import Adder
 - Quick Disassembler
 - Rebuilder
 - Resource Editor
 - UPX Utility

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

Indicare le sezioni di cui si compone il malware, fornendo una descrizione per ognuna di essa

La sezione denominata "UPX0" è spesso associata a UPX (Ultimate Packer for eXecutables), uno strumento di compressione ed eseguibile. UPX è utilizzato per comprimere e decomprimere file eseguibili, riducendo le dimensioni del file e facilitando la distribuzione di software. La sezione "UPX0" è creata durante il processo di compressione di un file eseguibile con UPX.

Ecco alcune caratteristiche comuni associate alla sezione "UPX0":

1. **Compressore UPX:** La sezione "UPX0" è tipicamente creata da UPX durante la compressione di un file eseguibile. UPX utilizza diverse sezioni, tra cui "UPX0", "UPX1", ecc., per archiviare le diverse parti del codice compresso e le informazioni necessarie per decomprimere il file durante l'esecuzione.
2. **Composizione di UPX:** La sezione "UPX0" contiene il nucleo compresso del file eseguibile. È in questa sezione che risiede il codice compresso e altri dati associati alla compressione.
3. **Decompressione dinamica:** Quando un eseguibile compresso con UPX viene eseguito, UPX si occupa della decompressione dinamica del codice contenuto nella sezione "UPX0" in memoria. Ciò consente all'applicazione di essere eseguita correttamente senza richiedere un passaggio separato di decompressione prima dell'esecuzione.
4. **Rilevamento anti-malware:** Poiché UPX è un tool legittimo utilizzato per la compressione degli eseguibili, alcuni software antivirus potrebbero rilevare la presenza di sezioni come "UPX0" durante la scansione di un file e classificarle come potenzialmente indicative di un eseguibile compresso.

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000600	00	00	00	00	00	00	00	00	00	00	00	00	98	60	00	00	
00000610	64	60	00	00	00	00	00	00	00	00	00	00	00	00	00	00	d
00000620	A5	60	00	00	80	60	00	00	00	00	00	00	00	00	00	00	*
00000630	00	00	00	00	B2	60	00	00	88	60	00	00	00	00	00	00	.
00000640	00	00	00	00	00	00	00	00	BD	60	00	00	90	60	00	00	.
00000650	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.
00000660	00	00	00	00	C8	60	00	00	D6	60	00	00	E6	60	00	00	.
00000670	F6	60	00	00	04	61	00	00	12	61	00	00	00	00	00	00	0
00000680	20	61	00	00	00	00	00	00	30	61	00	00	00	00	00	00	a
00000690	36	61	00	00	00	00	00	00	4B	45	52	4E	45	4C	33	32	6a
000006A0	2E	44	4C	4C	00	41	44	56	41	50	49	33	32	2E	64	6C	.DLL ADVAPI32.dll
000006B0	6C	00	4D	53	56	43	52	54	2E	64	6C	6C	00	57	49	4E	l.MSVCRT.dll.WIN
000006C0	49	4E	45	54	2E	64	6C	6C	00	00	4C	6F	61	64	4C	69	INET.dll.LoadLi
000006D0	62	72	61	72	79	41	00	00	47	65	74	50	72	6F	63	41	braryA.GetProcA
000006E0	64	64	72	65	73	73	00	00	56	69	72	74	75	61	6C	50	ddress.VirtualP
000006F0	72	6F	74	65	63	74	00	00	56	69	72	74	75	61	6C	41	rotect.VirtualA
00000700	6C	6C	6F	63	00	00	56	69	72	74	75	61	6C	46	72	65	lloc.VirtualFre
00000710	65	00	00	00	45	78	69	74	50	72	6F	63	65	73	73	00	e..ExitProcess.
00000720	00	00	43	72	65	61	74	65	53	65	72	76	69	63	65	41	.CreateServiceA
00000730	00	00	65	78	69	74	00	00	49	6E	74	65	72	6E	65	74	.exit..Internet
00000740	4F	70	65	6E	41	00	00	00	00	00	00	00	00	00	00	00	OpenA.....
00000750	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000760	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000770	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000780	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000790	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000007A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000007B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000007C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000007D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000007E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000007F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

Le righe di testo che ho trovato nella sezione "UPX0" sembrano rappresentare una lista di funzioni di libreria di sistema e chiamate di sistema di Windows. Queste voci indicano probabilmente le funzionalità utilizzate dall'eseguibile compresso durante l'esecuzione. Di seguito, spiego brevemente ciascuna di esse:

1. **KERNEL32.DLL:** Questa libreria contiene numerose funzioni fondamentali del kernel di Windows, inclusa la gestione dei processi, la gestione della memoria e molte altre operazioni di basso livello.
2. **ADVAPI32.dll:** Questa libreria fornisce funzioni per la gestione della sicurezza, inclusa l'autenticazione, l'autorizzazione e la manipolazione delle chiavi di registro.
3. **MSVCRT.dll:** Questa libreria è associata al runtime di Microsoft Visual C++ e offre funzioni di supporto per la gestione della memoria, la manipolazione delle stringhe, le operazioni di I/O e altro ancora.
4. **WININET.dll:** Questa libreria è utilizzata per operazioni di rete e gestisce connessioni Internet, download e upload di file, gestione dei cookie e altro.

Le seguenti voci sembrano rappresentare alcune funzioni specifiche utilizzate dall'eseguibile:

5. **LoadLibraryA:** Carica dinamicamente una libreria durante l'esecuzione del programma.
6. **GetProcAddress:** Recupera l'indirizzo di una funzione esportata da una libreria dinamicamente caricata.
7. **VirtualProtect:** Modifica i permessi di protezione della memoria virtuale, ad esempio, per rendere la memoria eseguibile.
8. **VirtualAlloc:** Alloca memoria virtuale per il processo chiamante.
9. **VirtualFree:** Libera la memoria virtuale precedentemente allocata.
10. **ExitProcess:** Termina il processo corrente.
11. **CreateServicesA:** Crea un servizio di Windows.
12. **exit:** Termina il programma corrente.
13. **InternetOpenA:** Apre una sessione Internet.

Queste funzioni sono comuni nelle applicazioni Windows e vengono spesso utilizzate per gestire la memoria, interagire con il sistema operativo, eseguire operazioni di rete e altro ancora.

Le funzioni menzionate nel testo della sezione "UPX0" suggeriscono che l'applicazione potrebbe avere le seguenti caratteristiche:

1. **Caricamento dinamico di librerie:** Le chiamate a **LoadLibraryA** e **GetProcAddress** indicano che l'applicazione potrebbe caricare dinamicamente librerie durante l'esecuzione e recuperare l'indirizzo delle funzioni necessarie.
2. **Manipolazione della memoria:** Le chiamate a **VirtualProtect**, **VirtualAlloc** e **VirtualFree** suggeriscono che l'applicazione potrebbe effettuare operazioni avanzate sulla gestione della memoria, come la modifica dei permessi di protezione, l'allocazione e la liberazione della memoria virtuale.
3. **Operazioni di rete:** La presenza di **InternetOpenA** indica che l'applicazione potrebbe coinvolgere operazioni di rete, come l'apertura di sessioni Internet.
4. **Terminazione del processo:** La chiamata a **ExitProcess** suggerisce che l'applicazione termina il suo processo corrente.
5. **Gestione dei servizi di Windows:** La presenza di **CreateServicesA** indica che l'applicazione potrebbe coinvolgere la creazione di servizi di Windows.
6. **Utilizzo del runtime di Visual C++:** La menzione di "MSVCRT.dll" indica che l'applicazione è stata compilata con il compilatore di Microsoft Visual C++, e quindi può utilizzare le funzionalità del runtime di questo ambiente di sviluppo.