Unità 3/Settimana 2/compito 1

LIBRERIE

Queste sono state le librerie importate dal malware

Malware_U3_W2_L1.exe

Module Name	Imports	OFTs	TimeDateStamp	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
ADVAPI32.dll	3	00000000	00000000	00000000	00002179	00002000
MSVCRT.dll	13	00000000	00000000	00000000	00002186	00002038
WININET.dll	2	00000000	00000000	00000000	00002191	00002070

SPIEGAZIONE 1° LIBRERIA

1)KERNEL32.DLL è una libreria di sistema essenziale nei sistemi operativi Microsoft Windows. Questa DLL (Dynamic Link Library) contiene una vasta gamma di funzioni di basso livello che sono utilizzate dai programmi in esecuzione su piattaforme Windows. Le funzioni contenute in KERNEL32.DLL includono operazioni di gestione della memoria, gestione dei file, gestione dei processi e delle thread, gestione delle risorse, gestione degli errori e altre operazioni di sistema di base.

Gli sviluppatori di software Windows spesso fanno riferimento a questa libreria per eseguire operazioni di sistema essenziali, come la creazione di file, l'allocazione di memoria, la sincronizzazione delle thread e altro ancora. KERNEL32.DLL è parte integrante del sistema operativo Windows e viene caricato in memoria quando il sistema operativo avvia un'applicazione Windows

SPIEGAZIONE 2° LIBRERIA

2)ADVAPI32.dll è un'altra libreria di sistema fondamentale nei sistemi operativi Microsoft Windows. Anche questa è una Dynamic Link Library (DLL) e contiene un insieme di funzioni che gestiscono varie operazioni di sistema relative alla sicurezza, alla gestione degli account utente, alla crittografia, ai servizi di Windows e ad altri aspetti correlati alla sicurezza e all'amministrazione del sistema le funzioni all'interno di ADVAPI32.dll consentono agli sviluppatori di accedere e gestire i servizi di autenticazione, le autorizzazioni di accesso ai file, i certificati digitali, le chiavi di registro, le informazioni sugli account utente e molti altri aspetti della sicurezza e dell'amministrazione del sistema operativo Windows.Gli sviluppatori di software Windows utilizzano ADVAPI32.dll per implementare funzionalità di sicurezza nei loro programmi, come l'autenticazione degli utenti, la crittografia dei dati, l'accesso ai servizi di Windows e altro ancora. Questa libreria è fondamentale per garantire la sicurezza e l'integrità dei sistemi Windows.

SPIEGAZIONE 3° LIBRERIA

MSVCRT.dll è un'altra libreria di sistema di fondamentale importanza nei sistemi operativi Microsoft Windows. Questa DLL (Dynamic Link Library) fornisce un insieme di funzioni di runtime della libreria C standard di Microsoft Visual C++, che è utilizzata dai programmi scritti in linguaggio di programmazione C e C++.Le funzioni all'interno di MSVCRT.dll comprendono operazioni comuni della libreria C, come la gestione della memoria dinamica, le operazioni di input/output, la manipolazione delle stringhe, la matematica e altro ancora.Gli sviluppatori di software C e C++ che usano gli strumenti di sviluppo di Microsoft spesso fanno affidamento su MSVCRT.dll per le operazioni di runtime necessarie per l'esecuzione dei loro programmi. Questa libreria è parte integrante dell'ambiente di runtime di Visual C++ e viene distribuita con il sistema operativo Windows.È importante notare che esistono diverse versioni di MSVCRT.dll, ognuna delle quali corrisponde a una specifica versione del compilatore di Visual C++. Pertanto, è essenziale che i programmi siano compatibili con la versione corretta di MSVCRT.dll per garantire il corretto funzionamento su sistemi Windows.

SPIEGAZIONE 4° LIBRERIA

WININET.dll è una libreria di sistema di Microsoft Windows che fornisce un'interfaccia per l'accesso a Internet da parte delle applicazioni Windows. Questa Dynamic Link Library (DLL) offre una serie di funzioni e strutture dati che consentono agli sviluppatori di scrivere applicazioni in grado di effettuare operazioni di rete, come il recupero di risorse da Internet, l'invio di richieste HTTP, la gestione dei cookie e altro ancora.WININET.dll è ampiamente utilizzata da applicazioni Windows che richiedono accesso a Internet, come browser web, client di posta elettronica, applicazioni di download e molti altri. È parte integrante del sistema operativo Windows e viene caricata in memoria quando un'applicazione che la richiede viene avviata.

SEZIONI

Le sezioni .text, .rdata e .data sono comuni nei file eseguibili, compresi i malware. Esse si riferiscono a parti specifiche del codice del programma e ai dati associati all'interno del file eseguibile. Ecco una breve descrizione di ciascuna di esse:

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

SEZIONE .TEXT

Questa sezione contiene il codice eseguibile del programma. È la parte del file eseguibile che contiene le istruzioni che vengono eseguite dalla CPU. Nel caso di malware, la sezione .text conterrà il codice che svolge le azioni dannose o indesiderate. Questo potrebbe includere istruzioni per la raccolta di informazioni, la manipolazione dei file, l'esecuzione di azioni di rete, e così via.

SEZIONE .RDATA

Questa sezione contiene i dati di sola lettura (read-only data). Spesso, questa sezione contiene dati costanti utilizzati dal programma, come stringhe di testo, tabelle di lookup, costanti numeriche e così via. Nei malware, la sezione .rdata potrebbe contenere informazioni statiche utilizzate dal codice dannoso, come stringhe di comando, indirizzi IP, chiavi di crittografia e simili.

SEZIONE .DATA

Questa sezione contiene i dati variabili utilizzati dal programma. Può includere variabili globali, strutture dati dinamiche allocate durante l'esecuzione e altri dati modificabili. Nei malware, la sezione .data potrebbe contenere variabili utilizzate per tracciare lo stato dell'infezione, memorizzare informazioni rubate o configurazioni specifiche del malware.

CONSIDERAZIONE FINALE

Secondo me si tratta di un Trojan ecco alcune caratteristiche comuni dei trojan che mi hanno permesso di arrivare a questa conclusione:Camuffamento: 1)I trojan spesso si presentano come file o programmi apparentemente legittimi, come software gratuiti, download di musica o video, allegati di email o link dannosi.2)Funzionalità nascoste: Il vero scopo dei trojan è quello di eseguire funzioni dannose sul sistema infetto. Queste funzionalità possono includere il furto di dati personali, la creazione di backdoor per l'accesso remoto, l'installazione di altri malware, la distruzione di file o il danneggiamento del sistema.3)Silenziosità: I trojan spesso operano in modo silenzioso e discreto, cercando di non attirare l'attenzione dell'utente o dei software di sicurezza.4)Interferenza con il kernel: Anche se i trojan non infettano direttamente il kernel, possono comunque causare danni al sistema operativo interferendo con i processi del kernel o sovraccaricandolo con operazioni dannose.