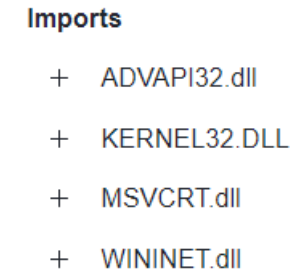
ANALISI STATICA BASICA MALWARE

Come richiesto dall'esercizio, analizzando l'eseguibile tramite i vari tool disponibili (gli screen di questo report provengono da Virus Total, ma si può utilizzare anche CFF Explorer o ExeInfoPE), possiamo vedere quali librerie importa il malware:



ADVAPI32.dll fornisce funzioni avanzate relative al registro di Windows, ai servizi, alle applicazioni e agli account utente. Se questo file risulta mancante o danneggiato, il sistema non è in grado di caricarsi correttamente;

KERNEL32.dll è un modulo del kernel (parte centrale di un sistema operativo che esegue le operazioni di base e fondamentali tra cui la gestione della memoria, le operazioni di input/output e gli interrupt) di Windows. È una libreria a collegamento dinamico a 32 bit utilizzata nei sistemi operativi Windows. All'avvio del sistema, kernel32.dll viene caricato in una memoria protetta in modo che non venga danneggiato da altri processi di sistema o utente. Funziona come un processo in background e svolge funzioni importanti come la gestione della memoria, operazioni di input/output e interruzioni;

MSVCRT.dll fornisce la maggior parte delle funzioni della libreria C, tra cui manipolazione delle stringhe, l'allocazione della memoria, le chiamate di input/output;

WININET.dll fornisce l'interfaccia tra le applicazioni che utilizzano WinInet e Windows Sockets. Le applicazioni che utilizzano questa API controllano se esiste una connessione Internet e, una volta verificata, l'applicazione può aprire un handle alla risorsa remota, richiedere una connessione per un protocollo specifico e aprire sessioni su quell'handle per comunicazioni HTTP, FTP o Gopher. WinINet fornisce funzionalità come caching, cronologia, gestione dei cookie, autenticazione base, NTLM, Kerberos, connessioni sia sicure (schannel) che non sicure, Dial-up, Diretto, Proxy, gestione del protocollo e dell'intestazione http.

Nella descrizione delle sezioni invece, vediamo come al posto dei vari .data, .rdata , .text, ecc… ci siano UPX0, UPX1 e UPX2; questo sta a significare che il file è compresso e che, senza decomprimerlo, non riusciamo a capire quali sezioni vengono usate:

Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5	Chi2
UPX0	4096	16384	0	0	d41d8cd98f00b204e9800998ecf8427e	-1
UPX1	20480	4096	1536	7.07	ad0f236c2b34f1031486c8cc4803a908	5848.3
UPX2	24576	4096	512	2.8	f998d25f473e69cc89bf43af3102beea	53922

Prima di fare considerazioni, andiamo effettivamente a capire se è un malware oppure no; sempre da Virus Total inseriamo l'hash del file:

Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

Vediamo come ci siano 53 segnalazioni su 71 che dichiarano che questo è un software malevolo: