Analisi con CFF

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.dll	44	00006518	00000000	00000000	000065EC	00006000
WININET.dll	5	000065CC	00000000	00000000	00006664	000060B4

Troviamo due librerie che ci fanno capire che cosa fa il programma:

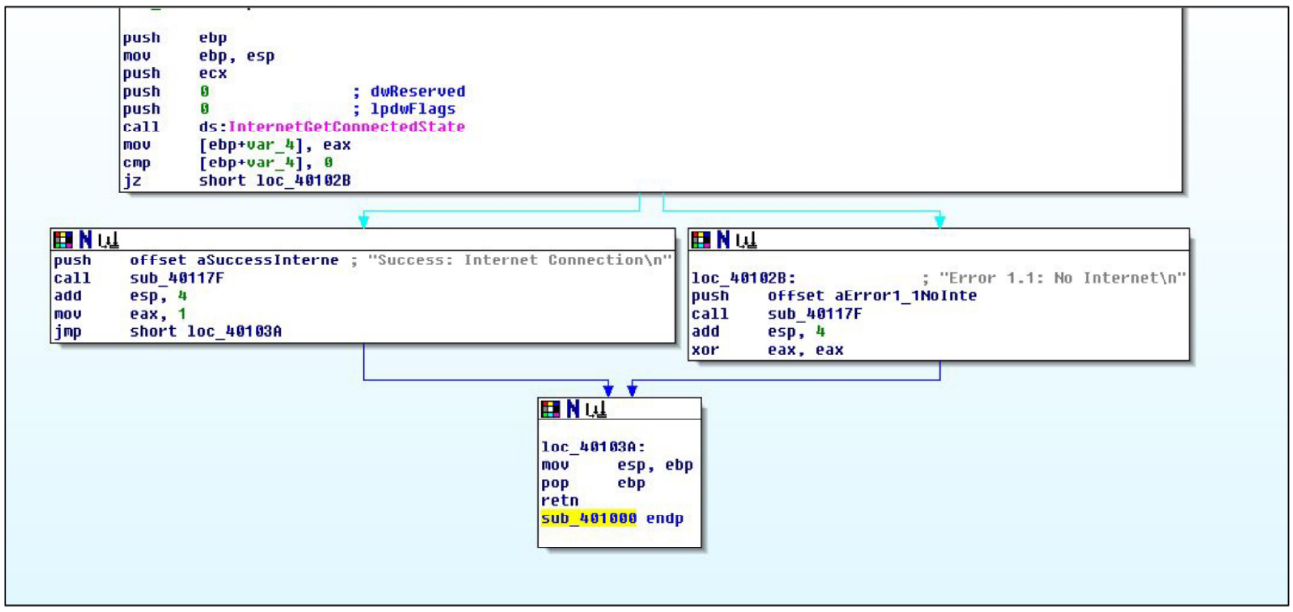
- kernel32.dll: questa libreria fornisce una vasta gamma di funzioni di sistema, come la gestione della memoria, la gestione dei file, la gestione dei processi e dei thread, e la comunicazione tra processi. In pratica, questa libreria è utilizzata da quasi tutti i programmi Windows.
- wininet.dll: questa libreria fornisce funzioni per l'accesso a Internet, come la connessione e la comunicazione con i server web, la gestione delle cache e dei cookie, e la gestione della sicurezza web. Questa libreria è utilizzata principalmente dai programmi che richiedono funzionalità di rete, come i browser web e i programmi di posta elettronica.

Andiamo poi ad analizzare le sezioni del programma:

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
.text	00004A78	00001000	00005000	00001000	00000000	00000000	0000	0000	60000020
.rdata	0000095E	00006000	00001000	00006000	00000000	00000000	0000	0000	40000040
.data	00003F08	00007000	00003000	00007000	00000000	00000000	0000	0000	C0000040

- .text: questa sezione contiene il codice eseguibile del programma.
- .rdata: questa sezione contiene dati solo lettura, come stringhe costanti, tabelle di lookup e altre risorse.
- .data: questa sezione contiene dati inizializzati, come variabili globali, costanti e stringhe.

Analisi di Assembly



- Le istruzioni "push ebp" e "mov ebp, esp" creano uno stack frame per la funzione.
- Le istruzioni "push ecx", "push 0" e "push 0" preparano gli argomenti per la chiamata alla funzione "InternetGetConnectedState".
- La chiamata alla funzione "InternetGetConnectedState" viene effettuata tramite "call ds:InternetGetConnectedState".
- Il valore restituito dalla chiamata alla funzione viene memorizzato nella variabile locale "[ebp+var_4]".
- La funzione esegue un controllo sul valore della variabile "[ebp+var_u]" utilizzando le istruzioni "cmp" e "jz". Se il valore è uguale a zero, la funzione passa al blocco di codice contrassegnato come "loc_40102B", altrimenti passa al blocco di codice contrassegnato come "loc_40103A".
- Nel blocco di codice "loc_40102B", viene chiamata la funzione "sub_40117F" con un messaggio di errore "Error 1.1: No Internet\n".
- Nel blocco di codice "loc_40103A", viene impostato il valore di ritorno della funzione a 1 se la connessione a Internet è stata stabilita con successo, altrimenti viene impostato a 0.
- L'istruzione "mov esp, ebp" ripristina il registro dello stack pointer.
- L'istruzione "pop ebp" ripristina il registro base dello stack.
- L'istruzione "retn" restituisce il valore di ritorno alla funzione chiamante.

In generale, il comportamento della funzione sembra essere quello di controllare se la connessione a Internet è disponibile o meno, e di restituire un valore che indica se il controllo è stato eseguito con successo o meno.

Viene stampato “Error 1.1 ...” se la connessione non è disponibile, altrimenti viene dato il messaggio “Success...”.