



DATADEFENDERS

L I B E R I C O M E A Q U I L O T T I



IL NOSTRO PROGETTO

Project 01

Identificazione librerie importate da file.exe

Project 02

Identificazione sezioni del Malware

Project 03

Identificazione costrutti noti

Project 04

Ipotesi sul comportamento della funzionalita' implementata

Project Bonus

Tabella con significato singole righe di codice assembly





IDENTIFICAZIONE LIBRERIE

Per identificare le librerie abbiamo utilizzato CFF explorer e siamo andati nella sezione delle librerie importate.

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
000065EC	N/A	000064DC	000064E0	000064E4	000064E8	000064EC
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.dll	44	00006518	00000000	00000000	000065EC	00006000
WININET.dll	5	000065CC	00000000	00000000	00006664	000060B4



IDENTIFICAZIONE SEZIONI

Per identificare le sezioni abbiamo utilizzato CFF Explorer e siamo andati nella cartella Section Headers.

Le sezioni presenti sono: .text, .rdata e .data

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	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



COSTRUTTI NOTI

I costrutti noti che abbiamo identificato sono : l'inizio dello stack, una condizione (if) e il costrutto della rimozione dello stack.



push	ebp
mov	ebp, esp

cmp	[ebp+var_4], 0
jz	short loc_40102B

mov	esp, ebp
pop	ebp



IPOTESI FUNZIONALITA' IMPLEMENTATE

La funzione “getinternetconnectstate” serve a verificare la presenza o meno di connessione internet ad una macchina.

Il costrutto che abbiamo precedentemente trovato (l’if) verifica se una macchina e’ connessa o meno.

Nello specifico: la funzione segnala la non presenza di internet se la funzione restituisce 0 mentre se !=0 invece ne segnala la presenza.



Istruzione	Mnemonico	Operandi	Descrizione
push ebp	Salva il valore del registro EBP nello stack.	EBP	Il registro EBP viene utilizzato come base del frame di stack. Salvare il suo valore nello stack consente di ripristinare il frame di stack in un secondo momento.
mov ebp, esp	Imposta il registro EBP sul valore del registro ESP.	EBP, ESP	Il registro ESP punta alla parte superiore dello stack. Impostare EBP su ESP significa che EBP punterà ora all'inizio del frame di stack corrente.
push ecx	Salva il valore del registro ECX nello stack.	ECX	Il registro ECX viene utilizzato per scopi generici. Salvare il suo valore nello stack consente di ripristinarlo in un secondo momento.

push	Salva il valore di dwReserved nello stack.	dwReserved	dwReserved è una variabile definita altrove nel codice. Il suo valore viene salvato nello stack per preservarlo.
push	Salva il valore di 1pdwFlags nello stack.	1pdwFlags	1pdwFlags è un'altra variabile definita altrove nel codice. Il suo valore viene salvato nello stack per preservarlo.
call ds:InternetGetConnectedState	Chiama la funzione InternetGetConnectedState.		La funzione InternetGetConnectedState determina se il computer è connesso a Internet.
mov [ebp+var_4], eax	Salva il valore del registro EAX nella variabile var_4.	EBP+var_4, EAX	La variabile var_4 è definita come un offset dal registro EBP. Il valore del registro EAX viene salvato in questa variabile.
cmp [ebp+var_4], 8	Confronta il valore della variabile var_4 con il valore 8.	EBP+var_4, 8	Se il valore della variabile var_4 è uguale a 8, significa che l'pc è

jz short loc 401028	Salta all'istruzione con etichetta loc 401028 se il flag di zero è impostato.		Il flag di zero viene impostato se il risultato dell'ultima istruzione di confronto era uguale a zero. In questo caso, il flag di zero è impostato se il valore della variabile var_4 è uguale a 8, il che significa che il computer è connesso a Internet.
Nul	Etichetta per l'istruzione successiva.		
push offset aSuccess Interne: "Success: Internet Connection\n"	Salva l'indirizzo della stringa "Success: Internet Connection\n" nello stack.	aSuccess Interne	La stringa "Success: Internet Connection\n" viene utilizzata per indicare che il computer è connesso a Internet.
call sub 40117F	Chiama la funzione che stampa la stringa sulla console.		La funzione sullo stack stampa la stringa "Success: Internet Connection\n" sulla console.

add esp, 4	Rimuove quattro byte dallo stack.		Quattro byte vengono rimossi dallo stack perché è la dimensione della stringa "Success: Internet Connection\n".
mov eax, 1	Imposta il registro EAX sul valore 1.	EAX, 1	Il valore 1 viene utilizzato per indicare che il programma è stato eseguito correttamente.
jmp short loc 40103A	Salta all'istruzione con etichetta loc 40103A.		
Nul	Etichetta per l'istruzione successiva.		
loc 40103A:	Etichetta per l'istruzione successiva.		
mov esp, ebp	Ripristina il valore del registro ESP dal valore del registro EBP.	ESP, EBP	Il registro ESP viene ripristinato sul valore del registro EBP, ESP punterà all'inizio.

Istruzione	Mnemonico	Operandi	Descrizione
pop ebp	Ripristina il valore del registro EBP dallo stack.	EBP	Il valore del registro EBP dallo stack.

TRACCIA BONUS

TABELLE



PANORAMICA GENERALE

Il codice assembly: un viaggio tra registri e connessioni internet
Immagina il codice assembly come un esploratore che attraversa un territorio sconosciuto, il computer. Il suo obiettivo? Verificare se c'è una connessione internet e stampare un messaggio di successo o meno.

L'esploratore inizia salvando la sua posizione attuale (registro EBP) e impostando una nuova base per il suo viaggio (registro ESP). Come un alpinista che fissa un campo base, questo prepara il terreno per l'esplorazione.

Lungo la strada, l'esploratore incontra alcuni oggetti preziosi (registri ECX, dwReserved e 1pdwFlags) e li mette al sicuro nello zaino (stack) per non perderli. Questi oggetti saranno utili più avanti nel viaggio.

Finalmente, l'esploratore raggiunge un punto chiave: la funzione InternetGetConnectedState. Come un oracolo, questa funzione rivela se c'è una connessione internet (valore 8) o meno.

Se la connessione c'è, l'esploratore festeggia! Stampa un messaggio di successo ("Success: Internet Connection\n") e aggiorna il suo registro di stato (EAX) per indicare che la missione è compiuta.

In caso contrario, l'esploratore torna indietro, ripristinando la sua posizione originale (registri EBP e ESP) e recuperando gli oggetti preziosi dallo zaino (registri ECX, dwReserved e 1pdwFlags).

In sintesi, questo codice assembly è come un'avventura tra registri e connessioni internet, dove l'esploratore affronta sfide, salva oggetti preziosi e celebra il successo o si prepara per un nuovo tentativo.



GRAZIE A

TUTTI