S11L5 PROGETTO SETTIMANALE MALWARE ANALISIS

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.

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

***1. Spiegate, motivando, quale salto condizionale effettua il Malware.***

Il malware effettua il salto condizionale alla locazione di memoria ***00401068***.

Dopo aver controllato se il registro *EBX* è uguale a *11*.

Questo è indicato dall'istruzione *cmp EBX, 11* seguita da *jz loc0040FFA0* alla locazione 00401064 (tabella 1).

La condizione *jz* controlla se l'ultimo confronto (in questo caso *cmp EBX, 11*) ha prodotto un risultato *zero*. Se il risultato del confronto è zero, il salto viene eseguito; altrimenti, viene continuata l'esecuzione sequenziale delle istruzioni.

Quindi, se il registro *EBX* contiene il valore *11* (e il confronto produce zero), il salto viene effettuato, portando l'esecuzione alla locazione *0040FFA0* (tabella 3), altrimenti, l'esecuzione prosegue normalmente. Questo controllo condizionale potrebbe essere utilizzato dal malware per eseguire un certo ramo del codice solo se si verifica una determinata condizione, potenzialmente per attivare o disattivare specifiche funzionalità o comportamenti del malware in base allo stato del sistema o ad altri fattori.

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement



***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.***

Une image contenant capture d’écran, texte, nombre, ligne

Description générée automatiquement

La condizione di salto *jnz* non viene rispettata quindi non c’è salto invece la seconda *jz* condizione di salto venga rispettata quindi avvenga il Salto.

***3. Quali sono le diverse funzionalità implementate all’interno del Malware?***

Dalle istruzioni fornite, sembra che il malware abbia almeno due funzionalità principali:

* ***Download di un file da un URL specifico***: Il malware utilizza la funzione *DownloadToFile(*) per scaricare un file da un URL specifico *(www.malwaredownload.com).* Questo viene indicato dalla sequenza di istruzioni nella tabella 2, dove viene caricato l'URL nel registro *EAX* e successivamente passato alla funzione *DownloadToFile(*).
* ***Esecuzione di un file specifico:*** Dopo aver scaricato il file, il malware sembra eseguire il file scaricato tramite la funzione *WinExec().* Questo viene indicato dalla sequenza di istruzioni nella tabella 3, dove il percorso del file *(.exe)* viene caricato nel registro EDX e poi passato alla funzione *WinExec(*).

Queste due funzionalità suggeriscono che il malware potrebbe essere progettato per scaricare ed eseguire un file dannoso o pericoloso sul sistema target. Il file scaricato potrebbe essere un altro malware, soprattutto un ransomware progettato per scopi dannosi, come il furto di dati o la compromissione del sistema.

***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.***

Nel contesto delle istruzioni di call presenti nelle tabelle 2 e 3, sembra che gli argomenti vengano passati principalmente attraverso i registri e lo stack:

* ***Tabella 2 - Chiamata a DownloadToFile():***

L'URL del file da scaricare (www.malwaredownload.com) viene caricato nel registro EAX.

Successivamente, il contenuto di *EAX* (cioè l'URL) viene spinto nello stack.

La funzione DownloadToFile() sarà quindi responsabile di estrarre l'URL dallo stack.

* ***Tabella 3 - Chiamata a WinExec():***

Il percorso del file .exe da eseguire viene caricato nel registro *EDX*.

Quindi, il contenuto di EDX (cioè il percorso del file) viene spinto nello stack.

La funzione *WinExec()* utilizzerà poi il valore presente nello stack per ottenere il percorso del file da eseguire.