

Emanuele Di Stefano S11-L4

Funzionalità dei Malware

Esercizio S11 L3 – Malware Analysis

Traccia:

La figura nella slide successiva mostra un estratto del codice di un malware. Identificate:

1. Il tipo di Malware in base alle chiamate di funzione utilizzate. Esercizio Funzionalità Malware
2. Evidenziate le chiamate di funzione principali aggiungendo una descrizione per ognuna di essa
3. Il metodo utilizzato dal Malware per ottenere la persistenza sul sistema operativo
4. BONUS: Effettuare anche un'analisi basso livello delle singole istruzioni

Identificare il tipo di Malware:

Il frammento di codice mostrato sembra utilizzare la funzione SetWindowsHook, che è comunemente usata da keylogger o spyware. L'hook a WH_MOUSE indica che potrebbe monitorare o catturare eventi del mouse, suggerendo che si tratta di un tipo di spyware o keylogger che registra gli input dell'utente. La funzione CopyFile è tipicamente utilizzata nei trojan o nei worm per replicare il malware.

Evidenziare e descrivere le principali chiamate di funzione:

- SetWindowsHook: Questa funzione viene utilizzata per impostare un hook che monitora determinati tipi di eventi, come l'input della tastiera o del mouse. In questo caso, sta agganciando gli eventi del mouse (WH_MOUSE). Questo è spesso usato dagli spyware per catturare le azioni dell'utente.
- CopyFile: Questa funzione viene utilizzata per copiare un file da una posizione all'altra. Qui, viene utilizzata per copiare il file malware in un'altra posizione, probabilmente per garantire la persistenza o la diffusione del malware.

Metodo utilizzato per ottenere la persistenza:

Il malware ottiene persistenza copiando sé stesso in una cartella del sistema di avvio, come indicato dall'istruzione mov ecx, [EDI] che punta al percorso della cartella di avvio. Copiandosi in questa cartella, il malware si assicura di essere eseguito ogni volta che il sistema viene avviato.

Analisi a basso livello delle singole istruzioni:

- push eax, push ebx, push ecx: Queste istruzioni salvano i valori correnti dei registri nello stack, una pratica comune prima di eseguire operazioni che potrebbero modificare questi registri. Questo aiuta a preservare lo stato in modo che possa essere ripristinato in seguito.
- call SetWindowsHook: Questa istruzione chiama la funzione SetWindowsHook per agganciare gli eventi del mouse.
- XOR ecx, ecx: Questa istruzione azzera il registro ecx, impostandolo a zero.
- mov ecx, [EDI]: Questa istruzione sposta il valore presente all'indirizzo di memoria puntato da EDI nel registro ecx. Qui, EDI contiene il percorso alla cartella di avvio.
- mov edx, [ESI]: Questa istruzione sposta il valore presente all'indirizzo di memoria puntato da ESI nel registro edx. ESI probabilmente contiene il percorso del file malware.
- push ecx, push edx: Queste istruzioni inseriscono nello stack il percorso della cartella (destinazione) e il percorso del file (origine) in preparazione per la chiamata alla funzione CopyFile.
- call CopyFile: Questa istruzione copia il file dall'origine alla destinazione, garantendo che il malware venga copiato in una posizione in cui può persistere.