S11 L4

Davide Andreozzi

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.

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

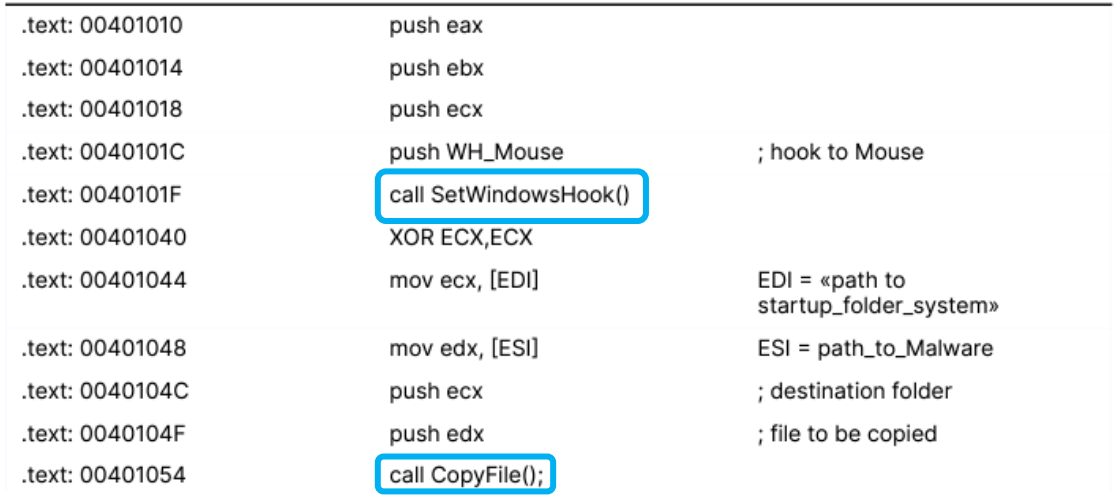
4. BONUS: Effettuare anche un'analisi basso livello delle singole istruzioni

½) Tipologia di Malware – Funzioni chiamate

Dalle seguenti chiamate presenti nel codice:

- **SetWindowsHook**
  - Questa funzione va a installare l'hook **WH_Mouse**, ovvero una funzione che và a monitorare i movimenti del mouse sulla macchina bersaglio, in sostanza gli input del mouse vengono intercettati e registrati.
- **CopyFile**
  - Questa è una funzione di Windows utilizzata per copiare un file da una posizione di origine a una posizione di destinazione. Questa funzione è utilizzata comunemente nei programmi per eseguire operazioni di copia di file.

Andiamo a definire il malware come **Keylogger**, infatti va a monitorare e registrare l'input del mouse.



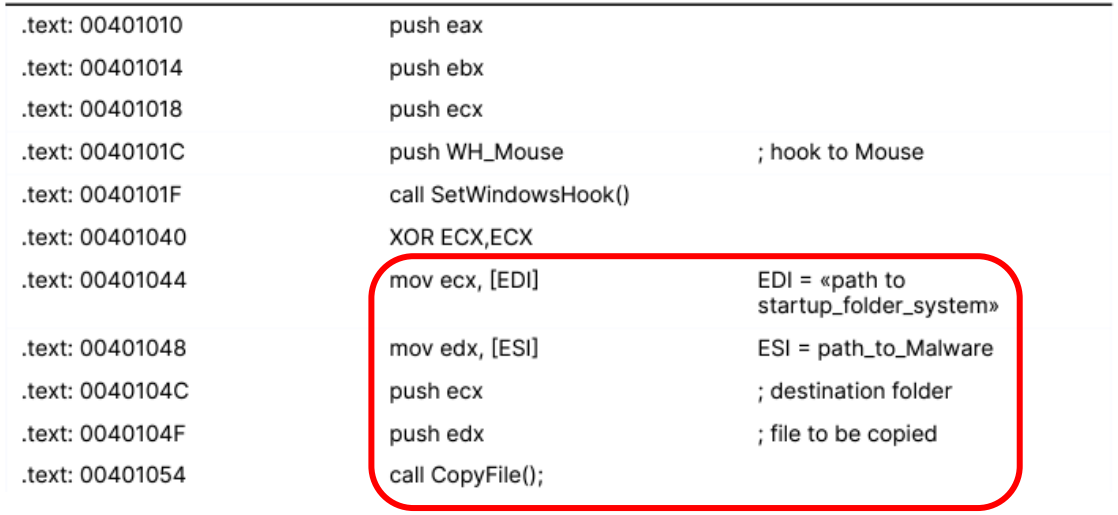
```
.text: 00401010    push eax
.text: 00401014    push ebx
.text: 00401018    push ecx
.text: 0040101C    push WH_Mouse                ; hook to Mouse
.text: 0040101F    call SetWindowsHook()
.text: 00401040    XOR ECX,ECX
.text: 00401044    mov ecx, [EDI]               EDI = «path to
                                                startup_folder_system»
.text: 00401048    mov edx, [ESI]               ESI = path_to_Malware
.text: 0040104C    push ecx                     ; destination folder
.text: 0040104F    push edx                     ; file to be copied
.text: 00401054    call CopyFile();
```

3) Persistenza

Per ottenere persistenza il malware utilizzerà la funzione CopyFile e in particolare la metodologia utilizzata sarà quella di «**Startup Folder**».

Possiamo infatti vedere dal codice che tramite la precedente funzione va a «prendere» la path dov'è contenuto il malware e la path di startup di Windows (dove sono contenuti i programmi da eseguire all'avvio) per copiare il malware in quest'ultima.

Il malware otterrà persistenza in quanto verrà automaticamente avviato all'avvio del sistema.



```
.text: 00401010    push eax
.text: 00401014    push ebx
.text: 00401018    push ecx
.text: 0040101C    push WH_Mouse          ; hook to Mouse
.text: 0040101F    call SetWindowsHook()
.text: 00401040    XOR ECX,ECX
.text: 00401044    mov ecx, [EDI]         EDI = «path to
                                          startup_folder_system»
.text: 00401048    mov edx, [ESI]         ESI = path_to_Malware
.text: 0040104C    push ecx               ; destination folder
.text: 0040104F    push edx               ; file to be copied
.text: 00401054    call CopyFile();
```

4)Analisi a basso livello

1) Vengono eseguiti i Push dei registri eax, ebx e ecx nello stack.
2) Viene fatto il Push di WH_Mouse, in sostanza viene pushato nello stack e preparato per essere installato.
3) Chiamata alla funzione SetWindowsHook, Questa funzione installerà l'hook per monitorare il mouse.
4) XOR ECX,ECX In questa chiamata si inizializza il registro ecx.
5) MOV ECX, [EDI]: Copia il valore contenuto in EDI in ECX.
6) MOV EDX, [ESI]: Copia il valore contenuto in ESI in EDX.
7) Vengono pushati i valori di ecx e edx nello stack. Questi sono i percorsi visti precedentemente per poi essere passati alla funzione CopyFile e dare persistenza al malware.
8) Viene chiamata la funzione CopyFile per copiare il malware nella path di Startup. I percorsi precedentemente pushati vengono utilizzati come argomenti in questa funzione.

```
push eax
push ebx
push ecx
push WH_Mouse                ; hook to Mouse
call SetWindowsHook()
XOR ECX,ECX
mov ecx, [EDI]               EDI = «path to
                             startup_folder_system»
mov edx, [ESI]               ESI = path_to_Malware
push ecx                     ; destination folder
push edx                     ; file to be copied
call CopyFile();
```