EPICODE-CS0124
S11/L4 - Pratica

Flaviano Sedici

Indice

Riferimenti e versioni

Responsabile del documento: Flaviano Sedici

Versionamento

Versione	Descrizione	Riferimento	Data
1.0	Redazione documento	Responsabile	04/04/2024

1. Traccia

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

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

```
.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();
```

1.1. Tipo di Malware

Sulla base dell'analisi effettuata e vista la presenza della funzione **callSetWindowsHook()** possiamo ipotizzare che il Malware sia un **keylogger**. In particolare viene passato il valore **WH_Mouse**, quindi possiamo ipotizzare che il malware sia dedicato alla registrazione dell'input utente proveniente dal Mouse.

1.2. Chiamate di funzioni principali

callSetWindowsHook() è una funzione che viene utilizzata per installare un hook sul sistema, ovvero una procedura che intercetta gli eventi generati dal sistema come ad esempio input da tastiera, mouse o altri input generici dell'utente.

CopyFile() è una funzione utilizzata per copiare un file da una posizione all'altra nel file system. La funzione restituisce True nel caso la copia sia avvenuta con successo.

1.3. Ottenimento persistenza

L'ottenimento della persistenza viene ottenuto tramite la chiamata della funzione **CopyFile()** passando il parametro "**EDI = path to startup_folder_system**" in modo che il malware venga inserito nella cartella di startup per essere avviato automaticamente ogni volta con il sistema operativo.

1.4. Analisi di basso livello

push eax	effettua il push nello stack del registro eax
push ebx	effettua il push nello stack del registro ebx
push ecx	effettua il push nello stack del registro ecx
push WH_Mouse ;hook to Mouse	effettua il push nello stack del parametro WH Mouse
call SetWindowsHook()	chiamata della funzione SetWindowsHook
XOR ECX,ECX	operatore logico per assegnare il valore 0 al registro ecx
mov ecx, [EDI] =path to startup_folder_system	sposta il path della cartella startup nel registro ecx
mov edx, [ESI] =path_to_Malware	sposta il path della cartella malware nel registro edx
push ecx ;destination folder	effettua il push nello stack del registro ecx
push edx ;file to be copied	effettua il push nello stack del registro edx
call CopyFile();	chiamata della funzione CopyFile()