Salford & Co.

S11L4

2024

PREPARED BY :

Sarah Ortiz

PRESENTED TO :

Epicode

Salford & Co.

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

```
.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();
```

Salford & Co.

1 TIPO DI MALWARE

Il codice sembra appartenere a un a uno keylogger. Cerca di spiare l’utente monitorando il mouse (SetWindowsHook()), e allo stesso tempo copia se stesso in una cartella per eseguire automaticamente all'avvio del computer.

Salford & Co.

2 FUNZIONI PRINCIPALI

Il codice usa due chiamate di funzione principali:

SetWindowsHook():

Questa funzione è utilizzata per installare una procedura hook che può monitorare vari eventi del sistema come input di tastiera, mouse, ecc. In questo caso, il malware sta monitorando gli eventi del mouse e l'hook è (WH_Mouse)

Serve per intercettare input del mouse, potenzialmente per registrare i movimenti o i clic

CopyFile():

Questa funzione copia un file da una posizione all'altra. Nel contesto del malware, viene usata per copiare il file del malware nella cartella di avvio del sistema, in questo modo il malware può avviarsi ogni volta che il pc viene avviato, assicurando cosi anche la sua persistenza.

Salford & Co.

3 METODO

Il malware vuole essere eseguito ogni volta che accendi il computer utilizzando la funzione Copyfile() n. Cosa fa? Copia il proprio file in una cartella speciale del sistema che sarebbe (startup_ folder_system) che avvia automaticamente i file al boot del sistema, permettendogli di rimanere attivo anche dopo un riavvio, e quindi la sua persistenza

.text: 00401044	mov ecx, [EDI]	EDI = «path to startup_folder_system»

Salford & Co.

4 BONUS

Analisi di basso livello del codice

push eax, push ebx, push ecx:

Salvano il contenuto temporaneamente nei registri eax, ebx, e ecx sullo stack prima di chiamare la funzione SetWindowsHook(); è fatto per preservare i valori dei registri per un eventuale ripristino dopo la chiamata di funzione. Tutto questo avviene perche cosi i valori sono messi da parte in modo temporaneo per poter essere ripristinati dopo.

push WH_Mouse:

Inserisce un valore chiamato WH_Mouse nello stack. Indica che il malware vuole monitorare gli eventi del mouse

call SetWindowsHook():

Qui chiama la funzione che inizia a monitorare gli eventi del mouse. Usando questa funzione, il malware può vedere tutto ciò che fai con il mouse registrandolo.

XOR ECX, ECX:

Azzera il registro ECX, mettendolo a 0. È un modo rapido e semplice di pulire il registro

mov ecx, [EDI] e mov edx, [ESI]:

Queste istruzioni prendono due percorsi di indirizzi e li mettono nei registri ecx e edx.

EDI contiene il percorso della cartella di avvio startup_folder_system

ESI contiene il percorso del file del malware Malware

Inserisce i valori di ecx e edx nello stack.

call CopyFile():

Chiama la funzione che copia il file del malware nella cartella di avvio del sistema. Questo è il passaggio cruciale che garantisce la persistenza. Dopo questa operazione, il malware sarà copiato e si avvierà automaticamente ogni volta che il computer si accende.