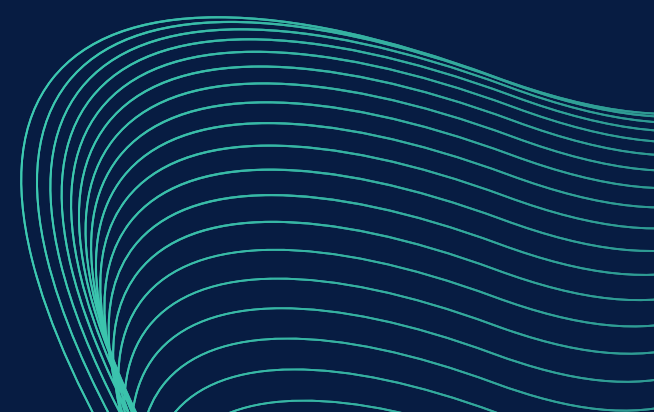




Traccia: La figura nella slide successiva mostra un estratto del codice di un malware.
Identificate:

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();	

Inizio funzione:

.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();	

intesa per installare un hook del mouse attraverso la chiamata alla funzione SetWindowsHook().

Inizializzazione dei registri:

.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();	

Viene effettuata un'operazione di XOR sul registro ECX, seguita dalla lettura dei percorsi dei file da due posizioni di memoria specifiche (EDI e ESI).

Copia del file:

```
.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();
```

I percorsi letti vengono poi utilizzati come argomenti per la chiamata alla funzione CopyFile(), che indica un'operazione di copia del file.

Chiamata a SetWindowsHook()

La chiamata a SetWindowsHook() suggerisce che il malware sta cercando di installare un hook del mouse. Se il malware riesce a installare un hook del mouse in modo persistente, potrebbe monitorare e intercettare gli eventi del mouse durante l'esecuzione del sistema.

```
.text: 0040101E      push     win_mouse_hook, hook to mouse  
.text: 0040101F      call SetWindowsHook()  
.text: 00401040      XOR     ECX,ECX
```

Copia del file in una posizione specifica:

La copia di un file potrebbe essere utilizzata come parte di un meccanismo di persistenza, ad esempio, copiando il malware in una posizione specifica del sistema in modo che venga eseguito automaticamente durante l'avvio.

```
.text: 00401054
```

```
call CopyFile();
```

push eax: Inserisce il contenuto del registro eax nello stack. Non conosciamo il valore specifico di eax in questo contesto, ma potrebbe essere utilizzato successivamente.

push ebx: Inserisce il contenuto del registro ebx nello stack. Come nel caso di eax, il valore specifico di ebx non è chiaro da questo frammento di codice.

push ecx: Inserisce il contenuto del registro ecx nello stack.

push WH_Mouse: Inserisce il valore WH_Mouse nello stack. Questo valore potrebbe essere un parametro per la funzione successiva.

call SetWindowsHook(): Chiama la funzione SetWindowsHook() che potrebbe essere utilizzata per installare un hook del mouse. Il tipo di hook dipende dal valore passato come parametro (WH_Mouse in questo caso).

XOR ECX, ECX: Esegue un'operazione di XOR tra ecx e se stesso, impostando il registro ecx a zero.

mov ecx, [EDI]: Muove il contenuto della memoria all'indirizzo puntato da EDI nel registro ecx. Questo potrebbe rappresentare il percorso alla cartella di avvio del sistema.

mov edx, [ESI]: Muove il contenuto della memoria all'indirizzo puntato da ESI nel registro edx. Questo potrebbe rappresentare il percorso al malware.

push ecx: Inserisce il contenuto del registro ecx (presumibilmente il percorso alla cartella di avvio) nello stack.

push edx: Inserisce il contenuto del registro edx (presumibilmente il percorso al malware) nello stack.

call CopyFile(): Chiama la funzione CopyFile(), che potrebbe essere utilizzata per copiare il malware nella cartella di avvio.