S11L4

TRACCIA: LA FIGURA 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

Figura 1:

.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();	

- **push eax, push ebx, push ecx**: Queste istruzioni spingono i registri **eax, ebx** e **ecx** sulla pila. Questi registri potrebbero contenere valori importanti che il malware non vuole sovrascrivere.
- **push WH_Mouse**: Questa istruzione spinge l'identificatore WH_MOUSE sulla pila. WH_MOUSE è una costante che indica un hook del mouse, suggerendo che il malware potrebbe essere interessato a monitorare l'input del mouse.
- **call SetWindowsHook():** Questa funzione imposta un hook in un thread del sistema. L'hook del mouse precedentemente spinto sulla pila verrà utilizzato qui. Questo suggerisce che il malware potrebbe essere un keylogger o un tipo simile di spyware.
- **XOR ECX,ECX**: Questa istruzione azzera il registro ecx. Potrebbe essere utilizzata per inizializzare o ripristinare il valore del registro.
- **mov ecx, [EDI], mov edx, [ESI]:** Queste istruzioni spostano i valori puntati da **EDI** e **ESI** nei registri **ecx** e **edx**. **EDI** e **ESI** sono utilizzati qui come puntatori alla cartella di avvio del sistema e al percorso del malware, rispettivamente.
- **push ecx, push edx**: Queste istruzioni spingono i percorsi della cartella di destinazione e del file da copiare sulla pila.
- **call CopyFile**(): Questa funzione copia un file esistente in una nuova posizione. Qui, il malware si copia nella cartella di avvio del sistema per ottenere la persistenza.
- In base a queste chiamate di funzione, il malware sembra essere un tipo di spyware che utilizza tecniche di hooking per monitorare l'input dell'utente e tecniche di copia dei file per ottenere la persistenza sul sistema operativo. Ricorda, questa è solo un'analisi delle chiamate di funzione presenti nel codice condiviso e potrebbero esserci altre funzionalità nascoste nel codice completo del malware.