ESERCIAZIONE S11-L4

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

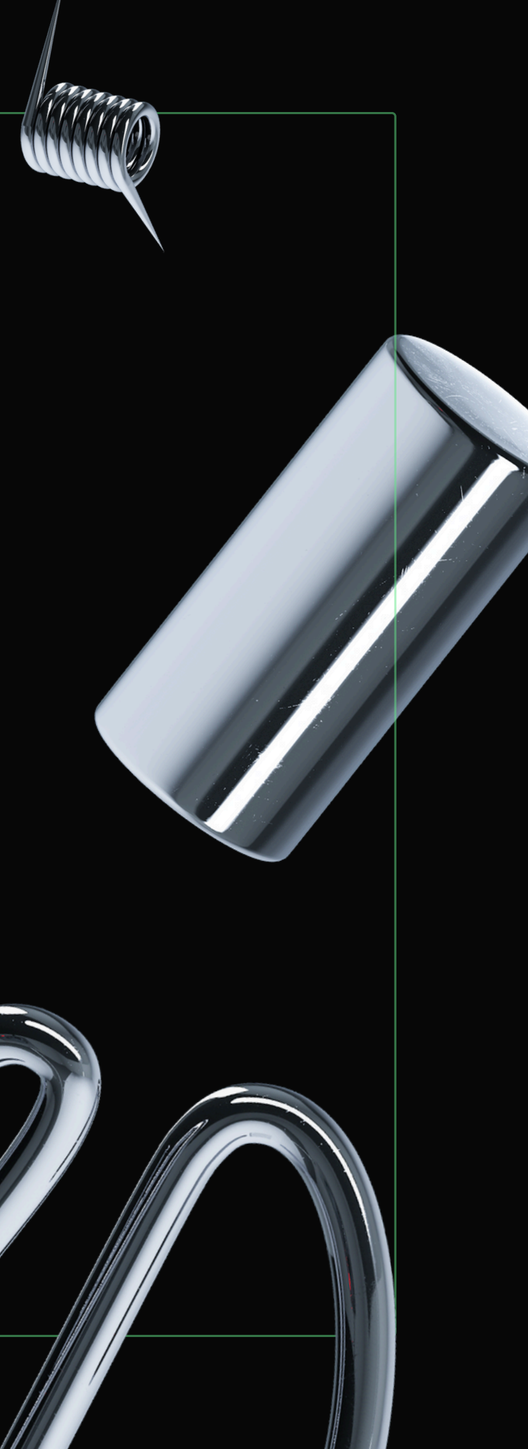
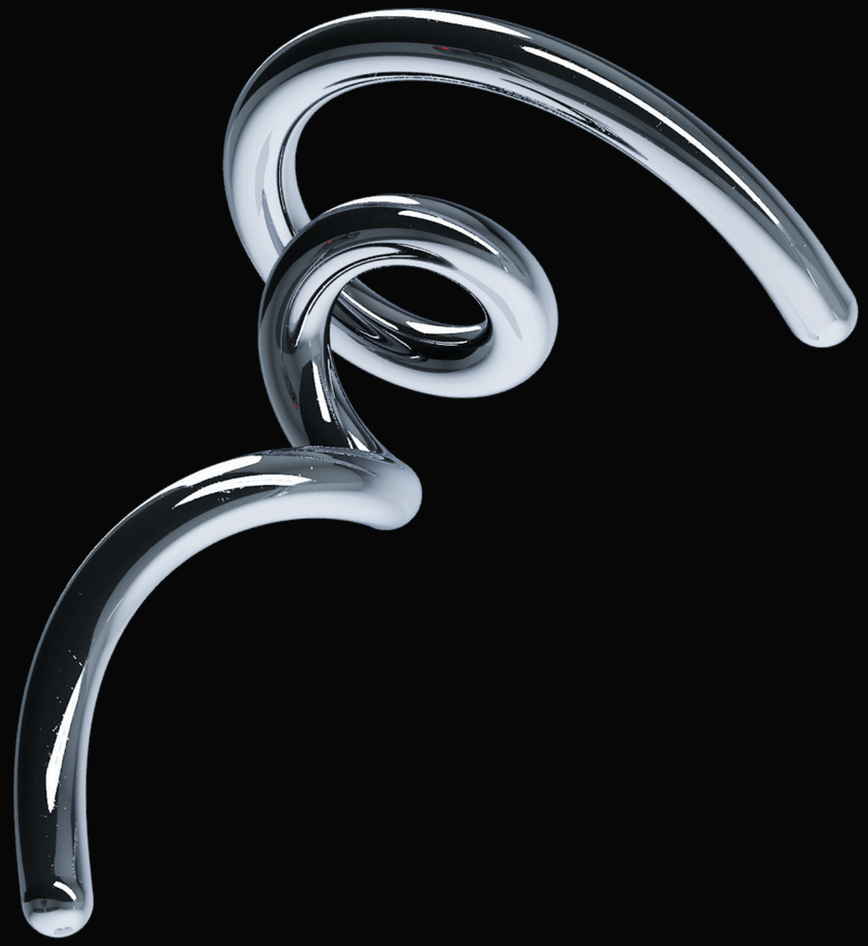


Figura 1:

```
.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();
```

DESCRIZIONE MALWARE



Il malware come possiamo vedere chiama la funzione SetWindowHook(), che non fa altro che installare il metodo Hook per monitorare eventi su una determinata periferica come mouse o tastiera.
Da quello che vediamo in Figura 1 la funzione cerca di registrare gli eventi del mouse come specificato da WH_Mouse .hook to Mouse

DESCRIZIONE PERSISTENZA

Per quanto riguarda la persistenza, sempre da Figura 1, viene ottenuta inserendo il Malware e il path della cartella “startup_folder_system” nei registri ECX e EDX, che poi verrà copiato con la funzione “CopyFyle()” nella cartella di startup del sistema operativo.

BONUS:

ISTRUZIONE	OPERANDI	DESCRIZIONE
push eax	eax	Salva il valore del registro eax nello stack.
push ebx	ebx	Salva il valore del registro ebx nello stack.
push ecx	ecx	Salva il valore del registro ecx nello stack.
push WH_Mouse	WH_Mouse	Salva un valore nello stack. Il valore è l'identificatore del hook del mouse.
call SetWindowsHook()	SetWindowsHook()	Chiama la funzione SetWindowsHookEx per installare l'hook del mouse.
XOR ECX, ECX	ECX, ECX	Imposta il registro ecx su zero.
mov ecx, [EDI]	ecx, [EDI]	Copia il valore contenuto nell'indirizzo di memoria puntato da EDI nel registro
mov edx, [ESI]	edx, [ESI]	Copia il valore contenuto nell'indirizzo di memoria puntato da ESI nel registro
push ecx	ecx	Salva il valore del registro ecx nello stack.
push edx	edx	Salva il valore del registro edx nello stack.
push edx	edx	Salva il valore del registro edx nello stack.
call CopyFile()	CopyFile()	Copia il EDX nella cartella startup_folder_system