EPICODE

CS0124

REPORT PROGETTO S11L4

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();
```

Il malware utilizza la funzione whmouse ,ovvero un keylogger che anziche’ legarsi alla tastiera si lega al mouse dell’end point target , per mantenere attiva la persistenza il malware si avviera’ sempre all’avvio del dispositivo.Successivamente gli input del mouse verranno salvati in una cartella di log accessibile dall’attaccante

GRAZIE!