

**S11 / L4**

**ESERCITAZIONE**

# TRACCIA

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

**01** Il tipo di Malware in base alle chiamate di funzione utilizzate.

**02** Evidenziate le chiamate di funzione principali aggiungendo una descrizione per ognuna di essa

**03** Il metodo utilizzato dal Malware per ottenere la persistenza sul sistema operativo

**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<br>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 TIPO DI MALWARE IN BASE ALLE CHIAMATE DI FUNZIONE UTILIZZATE.

```
.text:00401010      push eax  
.text:00401014      push ebx  
.text:00401018      push ecx  
.text:0040101C      push WH_Mouse           ; hook to Mouse  
.text:0040101F      call SetWindowsHook()
```

La funzione chiamata in questo caso è

Call SetWindowsHook()

Esso è utilizzato nei Malware di tipo Keylogger:

Tipologia di Malware che vanno ad intercettare tutto ciò che l'utente della macchina va a digitare o cliccare.

## IL METODO UTILIZZATO DAL MALWARE PER OTTENERE LA PERSISTENZA SUL SISTEMA OPERATIVO

|                 |                  |                                       |
|-----------------|------------------|---------------------------------------|
| .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 metodo Utilizzato per avere la persistenza sul sistema è di copiare ed inserire la Path del Malware e la Path della cartella dell'avvio automatico all'interno dello stack**

**Chiamando la Funzione: [Call CopyFile\(\)](#) esegue il processo ogni volta che l'utente avvia il sistema.**

## EFFETTUARE ANCHE UN'ANALISI BASSO LIVELLO DELLE SINGOLE ISTRUZIONI

|                 |                       |   |
|-----------------|-----------------------|---|
| .text: 00401010 | push eax              | Inserisce <b>EAX</b> nello stack  |
| .text: 00401014 | push ebx              | Inserisce <b>EBX</b> nello stack  |
| .text: 00401018 | push ecx              | Inserisce <b>ECX</b> nello stack  |
| .text: 0040101C | push WH_Mouse         | ; hook to Mouse inserisce nello stack un parametro che rileva l' <b>input del Mouse</b> |
| .text: 0040101F | call SetWindowsHook() | <b>Chiama la funzione di tipo Keylogger e monitora/controlla il Mouse</b>               |
| .text: 00401040 | XOR ECX,ECX           | Azzera il valore di <b>ECX</b>  |
| .text: 00401044 | mov ecx, [EDI]        | EDI = «path to startup_folder_system»<br><b>Copia (EDI) all'interno di ECX</b>          |
| .text: 00401048 | mov edx, [ESI]        | ESI = path_to_Malware<br><b>Copia (ESI) all'interno di EDX</b>                          |
| .text: 0040104C | push ecx              | ; destination folder<br><b>Inserisce ECX (EDI) nello stack</b>                          |
| .text: 0040104F | push edx              | ; file to be copied<br><b>Inserisce EDX (ESI) nello stack</b>                           |
| .text: 00401054 | call CopyFile();      | <b>Chiama la funzione CopyFile() per ottenere la persistenza</b>                        |

## CONSIDERAZIONI FINALI

Come possiamo notare, il Software in questione può **monitorare e comandare l'input del mouse** della macchina vittima, ed attraverso il metodo di **persistenza** utilizzato, il malware interagisce con il sistema operativo per ottenere un controllo **prolungato e nascosto**.