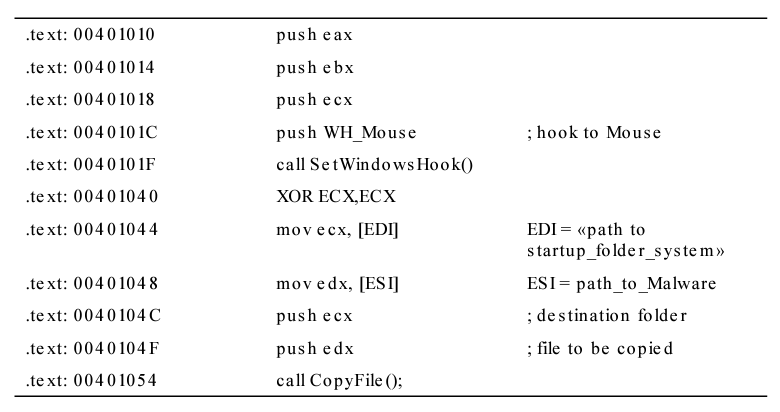
EPICODE

Esercizio 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



SOLUZIONE

1. Il tipo di Malware in base alle chiamate di funzione utilizzate.

- Il malware in questione è un keylogger che traccia le azioni del mouse, successivamente ottiene anche la persistenza.

2. Evidenziate le chiamate di funzione principali aggiungendo una descrizione per ognuna di essa

- Le chiamate di funzione principali sono:

* SetWindowsHook(). Questa funzione installa un “hook” dedicato al monitoraggio degli eventi di una data periferica, come in questo caso il mouse. Il metodo “hook” verrà allertato ogni qualvolta l’utente interagirà con il mouse e salverà le informazioni su un file di log.
* CopyFile(). Questa funzione permette di copiare un file. In questo specifico caso permette al malware di copiare il suo eseguibile all’interno della cartella “startup folder”. La «startup folder» è una particolare cartella del sistema operativo che viene controllata all’avvio del sistema, ed i programmi che sono al suo interno vengono eseguiti.

3. Il metodo utilizzato dal Malware per ottenere la persistenza sul sistema operativo

- Il metodo utilizzato dal malware per ottenere la persistenza è proprio quello di copiare il suo eseguibile all’interno della cartella “startup folder”. In questo modo il malware viene eseguito automaticamente all’avvio del sistema.

4. BONUS: Effettuare anche un’analisi basso livello delle singole istruzioni

- .text: 00401010 push eax

- .text: 00401014 push ebx

- .text: 00401018 push ecx

* Queste prime tre istruzioni mettono i registri eax, ebx, ecx sullo stack come parametri della prossima funzione chiamata.

- .text: 0040101C push WH\_Mouse ; hook to Mouse

* Un ulteriore parametro che fa riferimento al metodo “hook” per rilevare gli eventi del mouse.

- .text: 0040101F call SetWindowsHook()

* Chiama la funzione SetWindowsHook() in riferimento ai parametri passati precedentemente.

- .text: 00401040 XOR ECX,ECX

* Rinizializza ecx.

- .text: 00401044 mov ecx, [EDI] EDI = «path to startup\_folder\_system»

* Inserisce dentro ecx il percorso alla cartella “startup folder”.

- .text: 00401048 mov edx, [ESI] ESI = path\_to\_Malware

* Inserisce dentro edx il percorso al file del malware.

- .text: 0040104C push ecx ; destinationfolder

- .text: 0040104F push edx ; file to be copied

* Queste due istruzioni mettono i registri ecx (percorso della cartella “startup folder”) ed edx (percorso al file del malware) sullo stack. Sono i parametri della prossima funzione chiamata.

- .text: 00401054 call CopyFile();

* Quest’ultima istruzione chiama la funzione CopyFile() per copiare il file del malware nella cartella “startup folder” grazie ai parametri appena passati.