UNITÀ 3 SETTIMANA 3
COMPITO 4

Tipo di malware:

Basandosi sulle chiamate di funzione utilizzate, sembra che il malware stia facendo un hook alla funzione del mouse utilizzando `SetWindowsHook()`. Questo tipo di comportamento è spesso associato a malware di tipo keylogger, che registrano le azioni dell'utente, tra cui la pressione dei tasti e i movimenti del mouse.

Chiamate di funzione principali

`SetWindowsHook()`: Questa funzione è utilizzata per installare un hook di sistema o globale. Nel contesto del malware, è probabile che venga utilizzata per intercettare gli eventi del mouse.

Metodo per ottenere la persistenza:

Il malware sembra copiare se stesso in una cartella di avvio del sistema operativo, probabilmente per ottenere la persistenza. Questo è evidenziato dalle istruzioni:

`mov ecx, [EDI]`: Carica il percorso della cartella di avvio del sistema in ECX.

`mov edx, [ESI]`: Carica il percorso del malware in ESI.

`push ecx`: Passa il percorso della cartella di avvio del sistema come parametro.

`push edx`: Passa il percorso del malware come parametro.

Analisi a basso livello delle istruzioni:

`push eax`, `push eax`, `push eax`: Queste istruzioni spingono i registri EAX, EBX e ECX nello stack.

`pushWH_Mouse`: Questa istruzione sembra indicare l'hook del mouse, ma non è una chiamata di funzione standard. Potrebbe essere un'indicazione personalizzata dell'autore del malware.

`XOR ECX,ECX`: Effettua un'operazione di XOR tra ECX e se stesso, impostando ECX a 0.

`mov ecx, [EDI]`: Carica il contenuto di [EDI] (presumibilmente il percorso della cartella di avvio del sistema) in ECX.

`mov edx, [ESI]`: Carica il contenuto di [ESI] (presumibilmente il percorso del malware) in EDX.

`push cx`, `push edx`: Queste istruzioni spingono i valori di ECX e EDX nello stack, presumibilmente per passarli come parametri alla funzione di copia del file.

CONCLUSIONE

In conclusione, il malware sembra essere un keylogger che intercetta gli eventi del mouse utilizzando un hook di sistema e si installa nella cartella di avvio del sistema per ottenere la persistenza.