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.

TIPO DI MALWARE

Si può dedurre che questo frammento di codice stia configurando alcuni hook per gli eventi del mouse e quindi stia eseguendo operazioni legate ai percorsi dei file, probabilmente per copiare un file in una cartella di destinazione. I dettagli specifici dipendono dal contesto e dal resto del codice disassemblato.

CODICE RIGA PER RIGA

.text: 00401010 push eax ; Questa istruzione mette il valore del registro eax nello stack.
.text: 00401014 push ebx ; Questa istruzione mette il valore del registro ebx nello stack.
.text: 00401018 push ecx ; Questa istruzione mette il valore del registro ecx nello stack.
.text: 0040101C pushWH_Mouse ; hook al Mouse

.text: 0040101F call SetWindowsHook(); Questa istruzione chiama la funzione SetWindowsHook().

.text: 00401040 XOR ECX, ECX ; Questa istruzione effettua un'operazione XOR sul registro ECX con se stesso, azzerandolo.

.text: 00401044 mov ecx, [EDI] EDI = «percorso della cartella di avvio del sistema»

.text: 00401048 mov edx, [ESI] ESI = percorso del Malware

.text: 0040104C push ecx ; cartella di destinazione

.text: 0040104F push edx ; file da copiare

.text: 00401054 call CopyFile(); ; Questa istruzione chiama la funzione CopyFile().

Si può dedurre che questo frammento di codice stia configurando alcuni hook per gli eventi del mouse e quindi stia eseguendo operazioni legate ai percorsi dei file, probabilmente per copiare un file in una cartella di destinazione. I dettagli specifici dipendono dal contesto e dal resto del codice disassemblato.

PERSISTENZA

Il passaggio:

.text: 00401044 mov ecx, [EDI]
.text: 00401048 mov edx, [ESI]
.text: 0040104C push ecx
.text: 0040104F push edx
.text: 00401054 call CopyFile();

Sembra indicare che il malware sta copiando se stesso (o una parte di esso) in una cartella specifica. Questo è un comune metodo utilizzato dai malware per ottenere persistenza nel sistema operativo. Una volta che il malware è stato copiato nella cartella di avvio del sistema o in un'altra posizione rilevante, può essere eseguito all'avvio del sistema o in risposta ad altri eventi specifici, garantendo la sua persistenza nel sistema.
Tuttavia, la persistenza può essere ottenuta in vari modi, e il codice disassemblato fornito potrebbe rappresentare solo una parte delle attività del malware. Altri metodi comunemente utilizzati per ottenere persistenza includono la creazione di voci di registro, l'installazione di servizi di sistema, l'aggiunta di collegamenti nel menu di avvio e così via.