DOMANDA 1

Il codice sembra essere coinvolto nell'installazione di un keylogger, che è un tipo di malware progettato per registrare le battute di tastiera dell'utente e inviare le informazioni a un attaccante. Ma notiamo alla riga .text push WH_Mouse ; hook to Mouse ci fa pensare che registri non la tastiera bensi' il mouse

DOMANDA 2 + BONUS

push eax: Inserisce il valore del registro eax nello stack.

push ebx: Inserisce il valore del registro ebx nello stack.

push ecx: Inserisce il valore del registro ecx nello stack.

push WH_Mouse: Inserisce il valore della costanteWH_Mousenello stack. Questa costante viene utilizzata come parametro per la funzioneSetWindowsHook, che installa un hook per il mouse.

call SetWindowsHook(): Chiama la funzioneSetWindowsHook, che installa un hook per il mouse. Questo hook viene utilizzato per intercettare gli input del mouse.

XOR ECX,ECX: Esegue un'operazione di XOR tra i registriecxeecx, impostando il registroecxa zero.

mov ecx, [EDI]: Muove il valore contenuto nella memoria all'indirizzo contenuto nel registroedinel registroecx.EDIcontiene il percorso della cartella di avvio di sistema.

mov edx, [ESI]: Muove il valore contenuto nella memoria all'indirizzo contenuto nel registroesinel registroedx.ESIcontiene il percorso del malware.

push ecx: Inserisce il percorso della cartella di avvio di sistema nello stack.

push edx: Inserisce il percorso del malware nello stack.

call CopyFile(): Chiama la funzioneCopyFile, che copia il file specificato dal percorso di origine al percorso di destinazione. In questo caso, il malware viene copiato nella cartella di avvio di sistema.

DOMANDA 3

Il malware copia se stesso in una cartella di avvio del sistema, in modo che venga eseguito ogni volta che il sistema viene avviato. In questo modo ottiene la persistenza