S11L4

Traccia:identificare Il tipo di Malware in base alle chiamate di funzione utilizzate.
Funzioni: call SetWindowsHook() e call CopyFile(),possiamo capire che si tratta di un keylogger.

Traccia: Evidenziate le chiamate di funzione principali aggiungendo una descrizione per ognuna di essa.
Funzioni: call SetWindowsHook() e call CopyFile().
SetWindowsHook(): è una funzione dell'API del sistema operativo Windows che consente di installare una procedura hook nel sistema. Questa procedura hook può monitorare o intercettare vari tipi di eventi o messaggi.
CopyFile():è una funzione dell'API di Windows utilizzata per copiare un file da una posizione a un'altra sullo stesso sistema o su un altro supporto di memorizzazione.

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

.text: 00401044	mov ecx, [EDI]	EDI = «path to startup_folder_system»

In questo modo il malware va a inserirsi nella cartella di avvio di windows che si trova in C:\Windows\System32.

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

Comando	Spiegazione
push eax	Mette il valore del registro EAX nello stack.
push ebx	Mette il valore del registro EBX nello stack.
push ecx	Mette il valore del registro ECX nello stack.
pushWH_Mouse	Mette il valore "hook to Mouse" nello stack.
call SetWindowsHook	Chiama la funzione SetWindowsHook() per installare un hook di Windows.
XOR ECX, ECX	azzera ECX.
mov ecx, [EDI]	Sposta il contenuto della memoria all'indirizzo EDI nel registro ECX.
mov edx, [ESI]	Sposta il contenuto della memoria all'indirizzo ESI nel registro EDX.
push ecx	Mette il valore del registro ECX nello stack.
push edx	Mette il valore del registro EDX nello stack.
call CopyFile()	Chiama la funzione CopyFile() per copiare un file da una posizione all'altra.