S11L4,

BENVENUTI LUIGI

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

CODICE:

```
.text: 00401010    push eax
.text: 00401014    push ebx
.text: 00401018    push ecx
.text: 0040101C    push WH_Mouse              ;hook to Mouse
.text: 0040101F    call SetWindowsHook()
.text: 00401040    XOR ECX, ECX
.text: 00401044    mov ecx , [EDI]            ;EDI = «path to startup_folder_system»
.text: 00401048    mov edx , [ESI]            ;ESI = path_to_Malware
.text: 0040104C    push ecx                   ;destinationfolder
.text: 0040104F    push edx                   ;file to be copied
.text: 00401054    call CopyFile()
```

1 – Tipo di malware

Il malware chiama le funzioni SetWindowsHook() e CopyFile(). Si può dunque immaginare che esso sia un keylogger.

2 – Chiamate di funzione principali

Analizzando le chiamate di funzione principali, possiamo vedere che viene creato uno stack per la funzione SetWindowsHook() e vengono aggiunti i valori dei registri eax, ebx ed ecx; inoltre, viene eseguito un pull sullo stack di una variabile denominata Wh_Mouse, ovvero un metodo hook che viene allertato ogni volta che l'utente digita un input da mouse.

3 – Persistenza

Il malware ottiene persistenza copiando sé stesso nella cartella "Startup Folder System", ovvero quella cartella di Windows che contiene i programmi da eseguire all'avvio del sistema operativo.

4 – Bonus

.text: 00401010	push eax	;passaggio del contenuto di EAX sullo stack
.text: 00401014	push ebx	;passaggio del contenuto di EAX sullo stack
.text: 00401018	push ecx	;passaggio del contenuto di EAX sullo stack
.text: 0040101C	push WH_Mouse	;hook al mouse
.text: 0040101F	call SetWindowsHook()	;chiamata alla funzione SetWindowsHook()
.text: 00401040	XOR ECX, ECX	;inizializzazione a zero del registro ECX
.text: 00401044	mov ecx , [EDI]	;EDI contiene il path alla cartella startup_folder_system
.text: 00401048	mov edx , [ESI]	;ESI contiene il path al Malware
.text: 0040104C	push ecx	;push sullo stack della cartellla di destinazione
.text: 0040104F	push edx	;push sullo stack del file da replicare
.text: 00401054	call CopyFile()	;chiamata della funzione CopyFile()