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:

1/2. ----------|

Il codice presente nella tabella sottostante ci fa pensare ad un Malware di tipo **Keylogger**, infatti vediamo l'utilizzo della funzione *«SetWindowsHook»*, per l'installazione di un *«hook»,* utilizzati per intercettare eventi del sistema, come la pressione di un tasto, il movimento del mouse, ecc... Nello specifico, poiché l'ultimo parametro passato sullo stack è «WH_MOUSE», possiamo dedurre che il Malware registra la digitazione dei tasti del mouse:

.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	; destination folder
.text: 0040104F	push edx	; file to be copied
.text: 00401054	call CopyFile();	

3. ----------|

Il Malware ottiene la **persistenza** copiando il suo eseguibile nella cartella di «startup del sistema operativo». Il codice presente nella tabella a partire dall'istruzione 00401040, dapprima setta a zero il registro ECX, successivamente inserisce rispettivamente il path della cartella *«startup_folder_system»* e l'eseguibile del Malware nei registri ECX ed EDX. In seguito, passa entrambi i registri alla funzione *CopyFile()* con le due istruzioni *push ECX* e *push EDX*, che quindi copierà il contenuto di EDX (ovvero l'eseguibile del malware) nella cartella di startup del sistema operativo:

.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	; destination folder
.text: 0040104F	push edx	; file to be copied
.text: 00401054	call CopyFile();	