FUNZIONALITÀ DEI MALWARE

- Identificare il tipo di malware in base alle chiamate di funzione utilizzate. Evidenziare le chiamate di funzione principali aggiungendo una descrizione per ognuna di essa.
- Identificare il metodo utilizzato dal Malware per ottenere la persistenza sul 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();	

Questa frazione di codice è presa da un keylogger, lo possiamo capire dalla chiamata alla funzione SetWindowsHook. Questa funzione installa un metodo, chiamato appunto “hook”, che monitora le azioni di una periferica, in questo caso del mouse. Ogni azione viene poi salvata in un file di log che l'attaccante potrà accedere per carpire le informazioni derivate dalle azioni della periferica.

Per ottenere persistenza, il malware usa il metodo “startup folder”; il malware carica nel suo registro il path alla cartella di startup, per poi copiarvi il codice malevolo tramite la funzione CopyFile. In questo modo il malware sarà avviato ogni volta che il sistema operativo verrà avviato.