Funzionalità dei Malware

1. *Il tipo di malware in base alle chiamate di funzione utilizzate:*

.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();	

SetWindowsHook: utilizzato dai **keylogger**, un malware che cattura ciò che viene digitato dell'utente, ad esempio la pressione dei tasti o la movimentazione del mouse, viene installato il metodo **hook** che monitora gli eventi di una periferica, in questo caso il **mouse**.

https://learn.microsoft.com/it-it/windows/win32/api/winuser/nf-winuser-setwindowshookexa
https://learn.microsoft.com/en-us/windows/win32/winmsg/about-hooks#wh_mouse_ll
https://learn.microsoft.com/en-us/windows/win32/winmsg/lowlevelmouseproc

2. *Evidenziate le chiamate di funzione principali aggiungendo una descrizione per ognuna di esse.*

.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();	

SetWindowsHook: installa un hook di sistema per il mouse utilizzando il valore "WH_Mouse". Il metodo hook verrà allertato ogni volta che l'utente userà la periferica indicata e salverà le informazioni su un file di log.
CopyFile: copia nell'indirizzo dalla variabile EDI, il file dell'indirizzo assoluto dalla variabile ESI.

https://learn.microsoft.com/it-it/windows/win32/api/winbase/nf-winbase-copyfile

3. *Il metodo utilizzato dal Malware per ottenere la persistenza sul sistema operativo*

Tramite la funzione **CopyFile**
Path_to_startup_folder_system: fa riferimento alla cartella di avvio del sistema, che è una directory in cui vengono collocati i programmi o gli script che devono essere eseguiti all'avvio del sistema operativo.
Path_to_Malware: indica il path del Malware che verrà copiato nella directory precedente.

4. Bonus: effettuare un'analisi basso livello

I primi 3 PUSH inseriscono i valori contenuti in EAX, EBX e ECX in cima allo stack,

PUSH WH_MOUSE: installa il metodo **hook** tramite il valore WH_Mouse

CALL SETWINDOWSHOOK: chiamata della funzione SetWindowsHook per monitorare il sistema per determinati tipi di eventi, in questo caso l'hook/aggancio del mouse.

XOR ECX, ECX: azzera il valore del registro ecx.

MOV: i contenuti degli indirizzi di memoria [EDI] e [ESI] vengono copiati rispettivamente nei registri ecx e edx, ora saranno l'indirizzo di destinazione e l'indirizzo assoluto del file che si vuole copiare.

I 2 PUSH inseriscono i valori contenuti in ECX e EDX in cima allo stack,

CALL COPYFILE: chiamata della funzione CopyFile