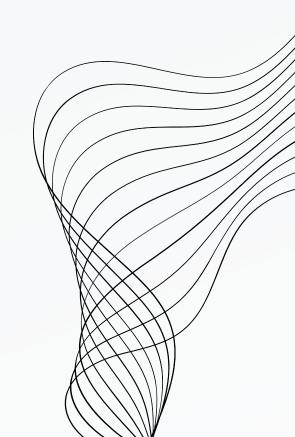


BUSINESS PROJECT

WWW.REALLYGREATSITE.COM



.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();	

Dalle funzioni mostrate si evince che il malware in questione è un Keylogger

.text: 0040101C push WH_Mouse ; hook to Mouse
.text: 0040101F call SetWindowsHook()

La chiamata alla funzione SetWindowsHook non fa che creare un "Hook" al monitoraggio degli eventi di una data periferica

.text: 00401044	mov ecx, [EDI]	EDI = «path to startup_folder_system»
.text: 00401048	mov edx, [ESI]	ESI = path_to_Malware

Lo startup_folder è un metodo di persistenza con cui il malware cerca di rimanere all'interno della macchina vittima, in questo caso copia il suo eseguibile all'interno della cartella startup, che sia generica o dedicata a un utente specifico.

.text: 00401048

.text: 0040104C

mov edx, [ESI]

......

push ecx

.text: 0040104F

push edx

.text: 00401054

call CopyFile();

ESI = path_to_Malware

; destination folder

; file to be copied

Con la chiamata CopyFile il Malware copierà gli input della periferica presa di mira in una determinata cartella