.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();	

FUNZIONI PRINCIPALI:

Le prime quattro istruzioni push inseriscono i registri eax, ebx, ecx e il valore WH_Mouse nello stack seguite dalla chiamata SetWindowsHook(), la quale permette di monitorare/registrare mouse, tastiera e altri eventi di sistema. L'istruzione XOR ECX, ECX imposta il registro ecx a zero.

PERSISTENZA:

Le istruzioni mov ecx, [EDI] e move edx, [ESI] caricano nei registri ecx e edx i valori contenuti negli indirizzi di memoria; in questo caso la directory di startup e il malware stesso.

Le istruzioni push ecx e push edx inseriscono i valori dei registri ecx e edx nello stack.

L'istruzione call CopyFile() richiama la funzione di sistema omonima, la quale copierà il malware nella directory di startup.

A questo punto il malware verrà eseguito ad ogni avvio del sistema.

SPIEGAZIONE:

Il malware preso in analisi installa un hook di sistema attraverso la funzione SetWindowsHook() per monitorare/registrare vari input di sistema. La funzione CopyFile() va a copiare il malware nel percorso di avvio del sistema operativo per garantirne l'esecuzione automatica. Da una veloce analisi si può ipotizzare che il malware in analisi sia un logger.