Foto slide del codice del **virus**

.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();	

Le chiamate sono evidenziate nella slide Call SetWindowsHook() e Call CopyFile()

Il metodo che usa per la persistenza è girare alcuni registiri e cartelle di windows per ottenere il contorllo attraverso il mouse e altri programmi utente.

L'analisi di basso livello:

Le prime 4 e le altr con push stringhe e le stringhe indicano che viene messo in memoria il seguente registro, e nella 4 indica che quel programma viene messo in memoria.

La stringa call in tutte e 2 indica la funzione che si vuole eseguire per esempio call copyfile copia un file

Mov ecx e mov edx sono usate per copiare l'attributo di quel registro in questo caso Edi perché bisonga entrare nellla cartella per copiare.