FUNZIONALITA' DEL MALWARE

La figura nella slide successiva mostra un estratto del codice di un malware.

il tipo di Malware presente è un Keylogger, poichè dal punto di vista tecnico, questi Malware utilizzano un SetWindowsHookEx o un GetAsyncKeyState.

Nel nostro caso notiamo che la chiamata viene fatta con un SetWindowsHook. Dove "hook" non è altro che una funzione dedicata al monitoraggio degli eventi di una data periferica, in questo caso un mouse.

Il malware ottiene una persisenza al text 00401044, qui avviene un task pianificato, cioè l'esecuzione del malware all'avvio del sistema, controllando una cartella del sistema operativo stesso.

.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();	

Passo per passo cosa avviene?

Text 10/14/18	avviene la creazione dello stack.
Text 1C	viene inserita nello stack la funzione
Text 1F	viene chiamata la funzione
Text 40	Inizializza il registro
Text 44	Qua viene inserito il path da dove dovrà partire l'esecuzione
Text 48	Qui viene inserito il path di dove dovrà andare l'esecuzione
Text 4C/4F	Qui vengono pushati i parametri, in questo caso la cartella di destinazione e i file che devono essere copiati.
Text 54	Viene eseguita la funzione di copiatura dei files.