REPORT

Dato il codice riportato di seguito qui sotto, verrano analizzati ed identificati:

- La tipologia di malware in base alle chiamate utilizzate, evidenziando le chiamate di funzione principali.

- Il metodo con il quale il malware ottiene persistenza sul sistema vittima

.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();	

Evidenziamo innanzitutto l'utilizzo di un Hook, ossia un meccanismo tramite il quale un'applicazione può intercettare degli eventi come azioni del mouse o sequenze di tasti digitati sulla tastiera, tramite utillizzo di hook è anche possibile agire sull'evento stesso, modificandolo o eliminandolo.

Avviene quindi l'inserimento del Parametro "WH_Mouse", che installa appunto una procedura di Hook per il monitoraggio delle azioni del mouse, alla chiamata di funzione "SetWindowsHook()" della libreria "User32.dll"

A questo punto la funzione "SetWindowsHookex" installerà una Hook routine specifica che si attiverà ogni volta che il tipo di evento (parametro) che è stato inserito nella funzione sarà utilizzato, in questo caso il monitoraggio di eventi del mouse.

Una volta settata funzione e parametro, sposta tutto in un registro di "Destination Index" , EDI, copiando dati da una destinazione (EDI) ad un'altra (Registro ESI, Registro indirizzo sorgente) .

Muove quindi il contenuto del registro EDI in ECX. (Mov ECX, [EDI])

Inserendo come destinazione “ Path to startup_folder_system” , uno speciale folder dei sistemi Windows, i programmi qui inseriti sono eseguiti durante il log on dello user, senza bisogno di interazione esterna, fornendo quindi al malware quella che viene definita “persistenza”, la capacità del malware di resistere ai reboot e di eseguirsi in automatico.

Copiando da registro sorgente il path (percorso del malware) per inserirlo nello startup folder

Muove quindi il contenuto del registro ESI in EDX. (Mov ECX, [ESI])

A questo punto sposta entrambi i parametri per effettuare una chiamata alla funzione “CopyFile” inserendo definitivamente il malware nel folder di start up windows.

Dalle funzioni utilizzate si può ipotizzare che il malware ricada nella categoria dei Keylogger.