

Report Funzionalità Malware

Estratto del Codice:

.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();	

1. Possiamo individuare il tipo di Malware in base alle chiamate di funzione e dire che il Malware in questione è un **keylogger** il quale intercetta gli input inviati dal Mouse senza andare a mappare i movimenti del Mouse.
2. Nell'estratto soprastante possiamo evidenziare 2 chiamate di sistema, che sono:

.text: 00401010	push eax		Parametri e chiamata di funzione per intercettare gli input del mouse
.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	Parametri e chiamata di funzione per la copia di un file dato
.text: 0040104F	push edx	; file to be copied	
.text: 00401054	call CopyFile();		

1. **SetWindowsHook()**: Installa una procedura di hook definita dall'applicazione in una catena di hook. Si installa una procedura di aggancio per monitorare il sistema alla ricerca di determinati tipi di eventi. Questi eventi sono associati a un thread specifico o a tutti i thread dello stesso desktop del thread chiamante;
2. **CopyFile()**: La funzione **CopyFile()** offre due funzionalità aggiuntive. Può chiamare una funzione di **callback** specificata ogni volta che una parte dell'operazione di copia viene completata e **CopyFile()** può essere annullata durante l'operazione di copia.
3. Il metodo di questo Malware per ottenere la persistenza è quello di **Startup Folder** il quale consiste nel copiare il suo eseguibile in una cartella di startup;
4. Adesso, andiamo ad analizzare l'estratto del codice:
 - .text: 00401010 push eax Inserimento del parametro nel registro
eax
 - .text: 00401014 push ebx Inserimento del parametro nel registro
ebx
 - .text: 00401018 push ecx Inserimento del parametro nel registro
ecx
 - .text: 0040101C push WH_Mouse ; hook to Mouse
WH_MOUSE hook consente di monitorare i messaggi del mouse da restituire dalla funzione **GetMessage** o **PeekMessage**.
 - .text: 0040101F call SetWindowsHook() chiamata di funzione per la cattura e la creazione di un file in cui verranno inseriti i tasti catturati dal Mouse
 - .text: 00401040 XOR ecx, ecx Pulizia del registro ecx impostandolo a 0
 - .text: 00401044 mov ecx, [EDI] EDI = <<path to startup folder system>>

- | | | |
|-------------------|------------------|--|
| | | Copia nel registro ecx del percorso della cartella di startup |
| • .text: 00401048 | mov edx, [ESI] | ESI = path_to_Malware
Copia nel registro edx del percorso del percorso per il Malware |
| • .text: 0040104C | push ecx | ; destination folder
Inserimento del parametro per la cartella di destinazione nel registro ecx |
| • .text: 0040104F | push edx | ; file to be copied
Inserimento del parametro per la copia di un nuovo file nel registro ecx |
| • .text: 00401054 | call CopyFile(); | Chiamata di funzione per la copia di un file dato in una cartella data |

URL usati:

- <https://learn.microsoft.com/en-us/windows/win32/api/winuser/nf-winuser-setwindowshookexa>
- <https://learn.microsoft.com/en-us/windows/win32/api/winbase/nf-winbase-copyfile>
- https://learn.microsoft.com/it-it/windows/win32/winmsg/about-hooks#wh_mouse