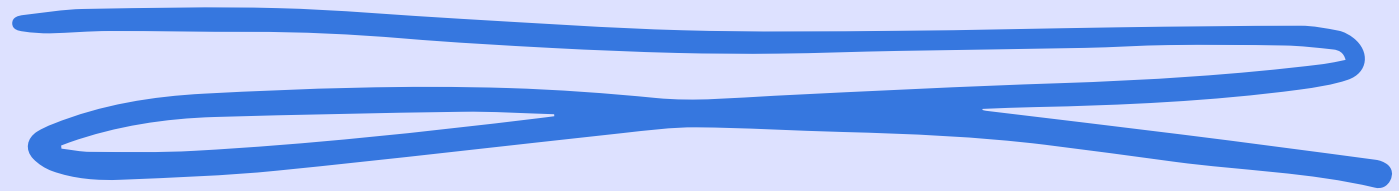


S11 L4



Analisi comportamentale
delle categorie dei
malware più note

Daniele Zizzi

Traccia:

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

- Il tipo di Malware in base alle chiamate di funzione utilizzate. Evidenziate le chiamate di funzione principali aggiungendo una descrizione per ognuna di essa
- Il metodo utilizzato dal Malware per ottenere la persistenza sul sistema operativo

Il malware in questione è un keylogger, dato che richiama la funzione “SetWindowsHook()”, che permette, appunto, di controllare un dispositivo. Poichè, l'ultimo parametro passato nella funzione è “WH_Mouse”, il malware registra solo l'input del mouse.

Figura 1:

.text: 00401010	push eax	
.text: 00401014	push ebx	
.text: 00401018	push ecx	
.text: 0040101C	push WH_Mouse	; hook to Mouse
.text: 0040101F	call SetWindowsHook()	

Il malware si copia nella cartella di avvio del sistema, pertanto ottiene la persistenza nell'host.

Viene inizializzato a 0 ECX, dopodichè, gli viene inserito il path della cartella di startup del sistema. Ad EDX, viene passato, invece, il path del malware.

Viene creato lo stack con i due push, poi viene richiamata la funzione CopyFile(), che va a copiare il malware nella cartella di avvio del sistema operativo.

.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();	