FUNZIONALITA’ DEI MALWARE

FRANCESCO PERSICHETTI

Traccia:

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

1. Il tipo di Malware in base alle chiamate di funzione utilizzate.
2. Evidenziate le chiamate di funzione principali aggiungendo una **descrizione** per ognuna di essa
3. Il metodo utilizzato dal Malware per ottenere la **persistenza** sul sistema operativo
4. BONUS: Effettuare anche un’analisi basso livello delle singole istruzioni

Estratto del codice del malware da analizzare:

.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.
Tramite la chiamata di funzione che il malware fa, posso dedurre che il malware in questione sia un “keylogger” il quale intercetta gli input inviati dal mouse senza andare a mappare i movimenti del mouse.

2.
Le chiamate di funzione principali sono 2:

.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. Installa una procedura hook definita dall'applicazione in una catena hook. Installo una procedura hook per monitorare il sistema per determinati tipi di eventi. Questi eventi sono associati a un thread specifico o a tutti i thread nello stesso desktop del thread chiamante.
2. La funzione CopyFile() serve appunto a copiare il file che servirà poi per immettere un file di persistenza nel registro

3.
Il metodo per ottenere la persistenza da parte del malware è quello di “Startup Folder” il quale copia il proprio eseguibile all’interno della cartella di startup della macchina vittima

4.

CODICE	SPIEGAZIONE
.text: 00401010 push eax	Inserisce il parametro nel registro eax
.text: 00401014 push ebx	Inserisce il parametro nel registro ebx
.text: 00401018 push ecx	Inserisce il parametro nel registro ecx
.text: 0040101C push WH_Mouse	**L'WH_MOUSE** hook consente di monitorare i messaggi del mouse da restituire dalla funzione **GetMessage** o **PeekMessage**. È possibile **usare l'WH_MOUSE** hook per monitorare l'input del mouse pubblicato in una coda di messaggi.
.text: 0040101F call SetWindowsHook()	Chiamata di funzione per registrare gli input del mouse
.text: 00401040 XOR ecx, ecx	Pulizia del registro ecx, impostandolo a 0 con lo XOR
.text: 00401044 mov ecx, [EDI]	EDI = <<path to startup_folder_system>> Copia nell'ecx il file di startup
.text: 00401048 mov edx, [ESI]	ESI = path_to_Malware Copia in edx il file del malware
.text: 0040104C push ecx	Cartella di destinazione
.text: 0040104F push edx	File da copiare
.text: 00401054 call CopyFile();	Funzione che copia il file