S11L4

Rosario Z.

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

.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();	

Figura 1

Punto 1

Il tipo di Malware in base alle chiamate di funzione utilizzate.

Il tipo di malware è un keylogger per mouse, che si avvia insieme al computer infatti vediamo la funzione di richiamo ad avvio “path to startup_folder_system»” e che poi salva il dati rilevati in un file di testo che salva su “path_to_malware”

Punto 2

Evidenziate le chiamate di funzione principali aggiungendo una descrizione per ognuna di essa

.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();	

Figura 1 Bis

push WH_Mouse ; hook to Mouse
Questi comandi servono a settare i parametri di cattura delle informazioni riguardanti il mouse in quanto come già visto stiamo parlando di un Keylogger per mouse.
Un Keylogger è un malware che salva gli input forniti dall’utente su una determinata macchina.
EDI = <<path to startup_folder_system>>
Così il malware verrà avviato ogni volta che la macchina verrà messa in esecuzione.

Punto 3

Il metodo utilizzato dal Malware per ottenere la persistenza sul sistema operativo

EDI = «path to startup_folder_system» Questo è il metodo utile ad ottenere la persistenza sulla macchina in esecuzione in quanto così il malware verrà riavviato ad ogni avvio del pc vittima.

Punto 4

BONUS: Effettuare anche un'analisi basso livello delle singole istruzioni

L'istruzione push WH_Mouse carica il valore della costante WH_Mouse (codice per il hook del mouse) sullo stack.
L'istruzione call SetWindowsHook invoca la funzione SetWindowsHook con il codice del hook del mouse come parametro.

Recupero del percorso della cartella di avvio di sistema:

L'istruzione XOR ECX,ECX azzera il registro ECX.
L'istruzione mov ecx, [EDI] carica il valore puntato dal registro EDI nel registro ECX.
Si presume che EDI contenga l'indirizzo della variabile che memorizza il percorso della cartella di avvio di sistema.

Recupero del percorso del malware:

L'istruzione mov edx, [ESI] carica il valore puntato dal registro ESI nel registro EDX. Si presume che ESI contenga l'indirizzo della variabile che memorizza il percorso del malware.

Copia del malware nella cartella di avvio di sistema:

L'istruzione push ecx carica il valore del registro ECX (percorso della cartella di avvio di sistema) sullo stack.
L'istruzione push edx carica il valore del registro EDX (percorso del malware) sullo stack.
L'istruzione call CopyFile invoca la funzione CopyFile per copiare il file dal percorso specificato in EDX al percorso specificato in ECX.