Report U3 W11.4

Analisi estratto

La figura mostra un estratto del codice di un malware.

.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. Identificare il tipo di malware in base alle chiamate di funzioni utilizzate.

Il malware è un keylogger, installa un hook per monitorare gli eventi del mouse e copiare il file del malware nella cartella di avvio di sistema.

2. Evidenziare le chiamate di funzione principali aggiungendo una descrizione per ognuna di esse.

Vengono chiamate le funzioni **CopyFile** e **SetWindowsHook**. Quest'ultima viene utilizzata per catturare la digitazione utente installando un hook per monitorare gli eventi del mouse. La funzione CopyFile, invece, copia edx (percorso del malware) nella cartella ecx (percorso cartella startup).

3. Identificare il metodo utilizzato dal malware per ottenere la persistenza sul sistema operativo.

Copiando il file del malware nella cartella di avvio di sistema, il malware si assicura che verrà eseguito automaticamente ogni volta che il sistema operativo viene avviato.

4. Effettuare un'analisi di basso livello delle singole istruzioni.

push eax

push ebx

push ecx

Il valore dei registry eax, ebx, ecx viene salvato nello stack.

push WH_Mouse ; hook to Mouse

call SetWindowsHook()

Il valore Wh_Mouse viene salvato nello stack, questo è il parametro per la funzione SetWindowsHook.

XOR ECX, ECX

Azzera il registro ecx.

mov ecx, [EDI] **; EDI = <<path to startup_folder_system>>**

mov edx, [ESI] **; ESI = path_to_Malware**

Vengono copiati i percorsi agli indirizzi puntati.

push ecx **; cartella di destinazione**

push edx **; file da copiare**

Vengono salvati i parametri sullo stack per la funzione CopyFile()

call CopyFile() **;**

Esegue la copia del file.