MALWARE ANALYSIS

FUNZIONALITÁ DEL MALWARE

04-06-2023

Frammento codice 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();
```

In base alle funzioni contenute nel codice del malware possiamo capire che si tratta di un tipo Keylogger che prende l'input dal mouse e lo salva in un documento di testo, oltre a questo il malware ha anche delle funzioni classiche dei Worm dato che si duplica spostandosi nella cartella di startup di Windows facendo si che ogni volta che il sistema operativo viene avviato il virus in questione si avvii di conseguenza fornendo un'accesso persistente all'interno della macchina vittima, probabilmente il continuo di questo codice include funzioni per la trasmissioni dei dati raccolti verso la macchina dell'attaccante o un server sotto il suo controllo quindi andando avanti con la lettura ci si potrebbe imbattere in librerie per la rete, l'ultima chiamata di funzione potrebbe far pensare ad un malware che richiede un'accesso fisico alla macchina vittima sfruttando l'avvio automatico delle chiavette USB.

ANALISI LINEA PER LINEA

Le prime tre righe servono per inizializzare lo stack.

Questo push serve a impostare il parametro di cattura della funzione successiva.

Questa chiamata di funzione serve ad iniziare la cattura del mouse.

Nelle successive due righe viene pulito e subito rimpiazzato il registro ecx.

Nelle ultime quattro righe il path del malware viene salvato così come quello della cartella di destinazione e successivamente i due parametri serviranno a popolare i campi dell' ultima funzione.

```
.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();
```