Progetto S11-L4

Studente: Simone Mininni

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. Evidenziate le chiamate di funzione principali aggiungendo una descrizione per ognuna di esse;
2) Il metodo utilizzato dal Malware per ottenere la persistenza sul sistema operativo;

Porzione di codice assembly x86:

```
-----------------------------------------------------------------------------------------
.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 chiamate:

- **SetWindowsHookex();**
- **CopyFile();**

Possiamo ipotizzare che si tratti di un keylogger persistente.
Infatti la funzione "**SetWindowsHookex()”** permette di monitorare determinati eventi e salvarli in un file di log, come ad esempio input di

tastiera, o in questo caso monitoring dei messaggi del mouse in quanto viene passato il parametro “WH_Mouse”.
Link Doc:
https://learn.microsoft.com/en-us/windows/win32/api/winuser/nf-winuser-setwindowshookexa

Mentre con la funzione **“CopyFile()”** copia un file in una destinazione specifica.
In questo caso il file del malware viene copiato nello startup folder di sistema comune a tutti gli utenti, al fine di avere persistenza cosicché il programma malevole può essere eseguito all’ avvio del sistema.
Link
Doc:https://learn.microsoft.com/en-us/windows/win32/api/winbase/nf-winbase-copyfile