EPICODE

CYBERSECURITY COURSE

BY MAX ALDROVANDI

17/05/2024

Web-site: https://epicode.com/it

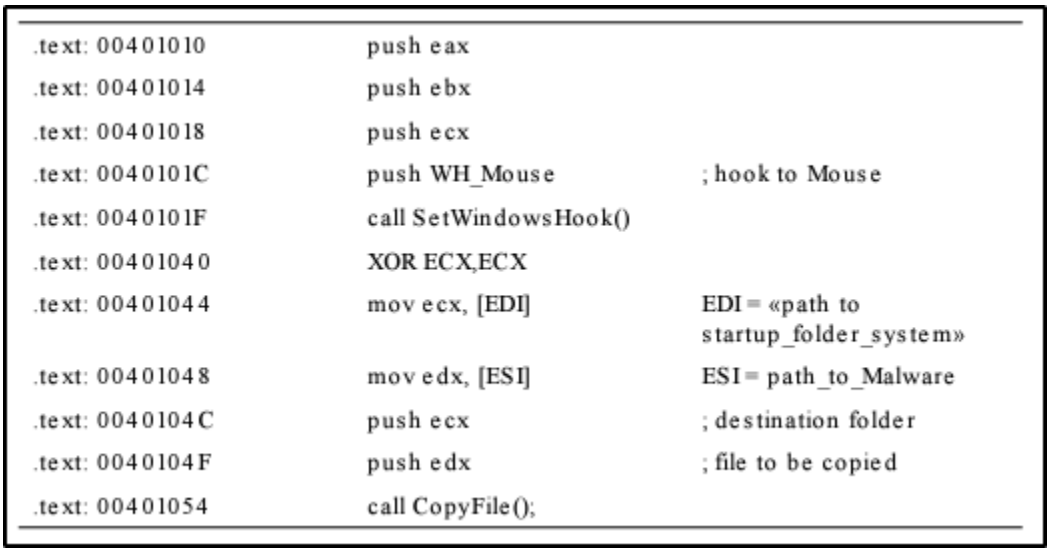
Locality:

Via dei Magazzini Generali,
6 Roma, Lazio 00154, IT

PRACTICE EXERCISE S11/L4

Track:

The figure shows an excerpt of a malware code.



```
.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();
```

Identify:

1. The type of Malware based on the function calls used. Exercise Functionality Malware

2. Highlight the main function calls by adding a description for each one

3. The method used by the Malware to achieve persistence on the operating system

4. **BONUS**: Also perform a low-level analysis of the individual instructions

Solution

Malware identification:

The code in the table below makes us think of a Keylogger-type Malware, in fact we see the use of the "**SetWindowsHook**" function, for installing a "**hook**" to **control a device**.

What we notice, however, is that unlike the code in the theoretical lesson, the last parameter passed on the stack is "**WH_MOUSE**."

This makes us think that the Malware **does not record** the typing of the user's keyboard keys, but rather the **typing of the mouse keys**!

.text: 00401010	push eax	
.text: 00401014	push ebx	
.text: 00401018	push ecx	
.text: 0040101C	push WH_Mouse	; hook to Mouse
.text: 0040101F	call SetWindowsHook()	

Malware Persistence:

The Malware obtains persistence by copying its executable into the "**operating system startup**" folder.

The code in the table starting with the instruction **00401040** first sets the **ECX register** to **zero**, then inserts the path to the "**startup_folder_system**" folder and the **Malware executable** into the **ECX** and **EDX registers**, respectively.

It then passes both registers to the **CopyFile() function** with the two instructions **push ECX** and **push EDX**. The **CopyFile() function** will then copy the contents of **EDX** (i.e., the Malware executable) to the **OS startup folder**.

.text: 00401044	mov ecx, [EDI]	EDI = «startup_folder_system»
.text: 00401048	mov edx, [ESI]	ESI = Malware_name
.text: 0040104C	push ecx	; destination folder
.text: 0040104F	push edx	; file name
.text: 00401054	call CopyFile();	