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 S10/L2

Track:

Configure the virtual machine for dynamic analysis (malware will actually be executed).

With reference to the executable file contained in the "**Exercise_Practice_U3_W2_L2**" folder on the desktop of your virtual machine dedicated to malware analysis, answer the following questions:

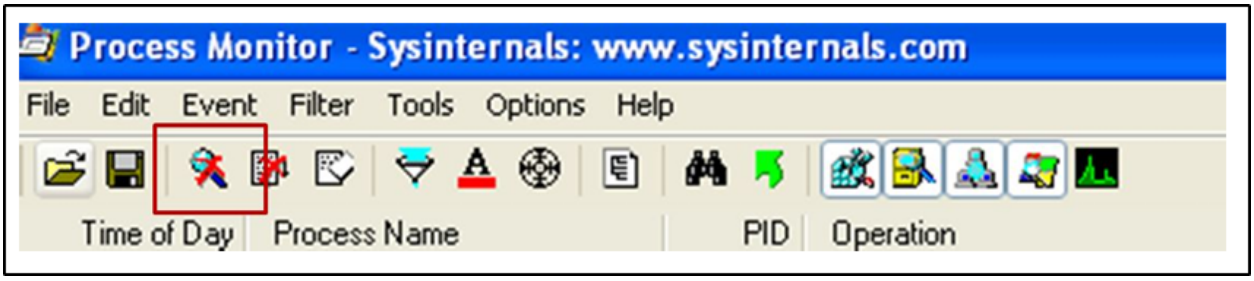
- Identify any malware actions on the file system using **Process Monitor** (**procmon**)
- Identify any malware actions on processes and threads using **Process Monitor**
- Registry changes after malware (**the differences**)
- Try to profile the malware based on the correlation between "**operation**" and **Path**.

Solution

Identify actions on File system of the Malware

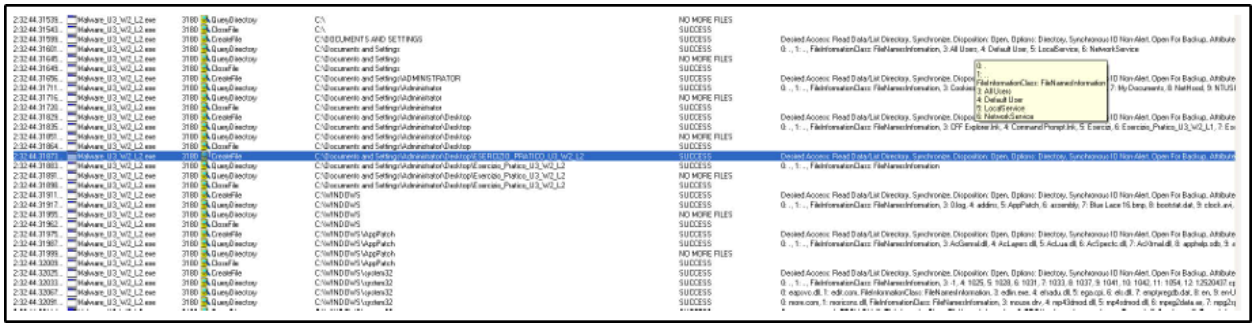
First, we start **Procmon** before running the malware, then we start the malware and after a time lapse of about 1 minute we stop Procmon capture by clicking on the lens-shaped icon in the red rectangle in the figure.

Be careful, when as in the figure there is a red "X" on the icon it means that the capture is stopped and procmon is not monitoring events. When the red "X" is not present, then the capture is in progress.



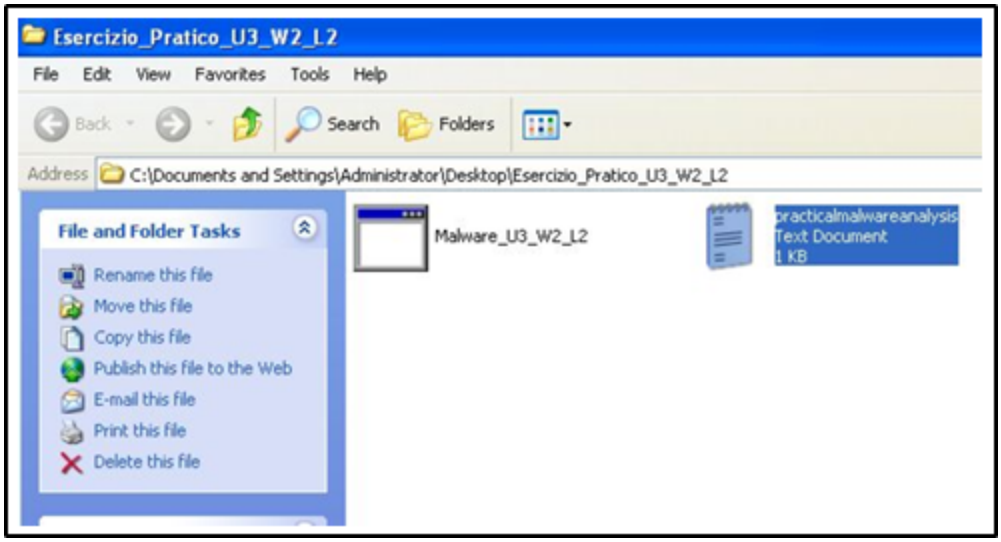
We enter the filter as seen in theory to show only the activities of the process named "**Malware_U3_W2_L2.exe**".

We immediately see from the procmon report that there are some functions reported in the "operation" column that are very interesting such as "**Create File**", "**Read file**" and "**Close File**" with respective path.

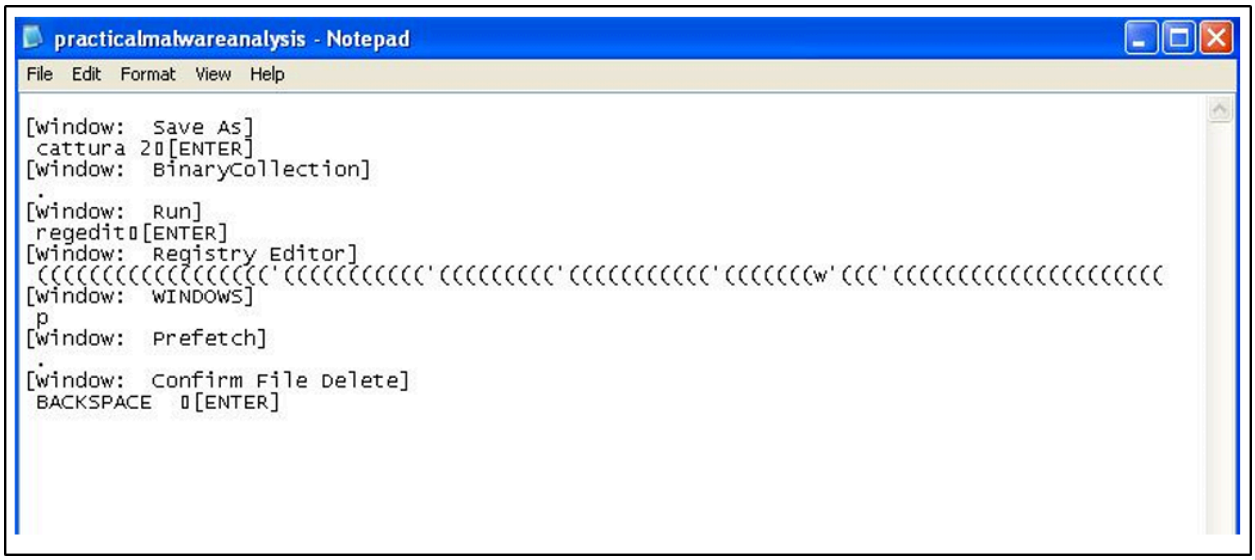


Very interesting is the line below - **Procmon** tells us that a **.txt file** has been created in the folder where the Malware resides.

We open the folder on the desktop where the malware executable resides to confirm that indeed the malware has created a file named "**practicalmalwareanalysis**"



We open the file (the contents of your file may be different) to notice that the file has acquired some of the keyboard characters used during the malware execution-this behavior is quite usual of **Keylogger malware**.



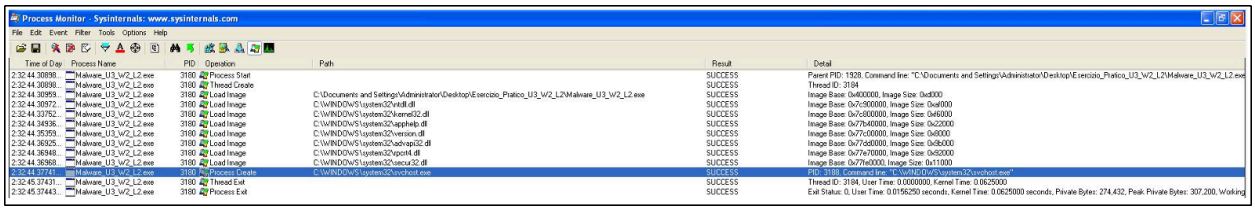
Identifying Actions on Processes and Threads

Using the same **Procmon capture**, we use icons to filter on events regarding processes and threads.

We see some very interesting functions such as Load Image which is used to "load" for execution the malware and the necessary **libraries (.dll)**, and then we see "**Process Create**" which is used to create a process.

It appears that our malware is creating a process called "**svchost.exe**" which is generally a valid Windows process.

This is another frequent behavior of malware, trying to disguise their execution under a process with a valid name to evade any **antivirus/anti-malware**.



Final conclusions

Therefore, we can assume that our malware when executed first tries to disguise itself by creating a new process called "**svchost.exe**", then launches its main functionality that is a **keylogger** that saves the characters typed by the user in the file "**practicalmalwareanalysis**" specially created in the folder where the executable is located.