

# 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:

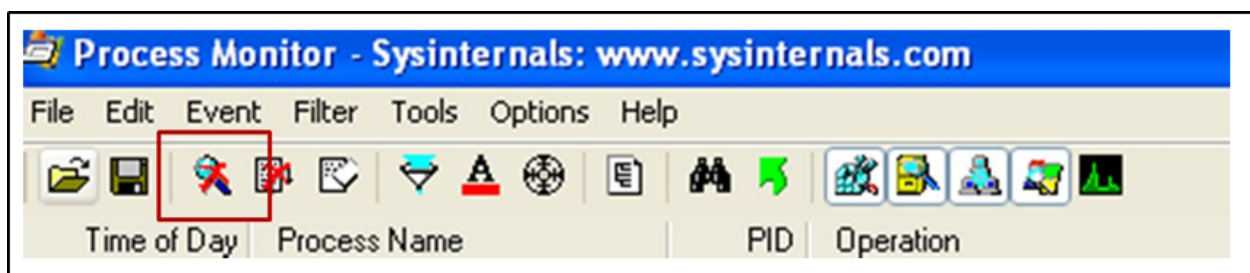
- Identify any malware actions on the file system using **Process Monitor (procmon)**
- Identify any malware actions on processes and threads using **Process Monitor**
- Registry changes after malware (**the differences**)
- Try to profile the malware based on the correlation between "**operation**"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

## Solution

### Identify actions on File system of the Malware

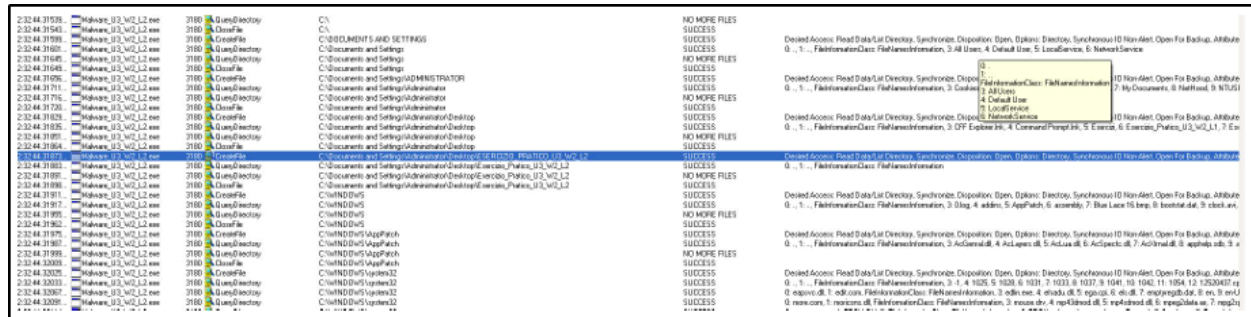
First, we start **Procmon** before running the malware, then we start the malware and after a time lapse of about 1 minute we stop Procmon capture by clicking on the lens-shaped icon in the red rectangle in the figure.

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.



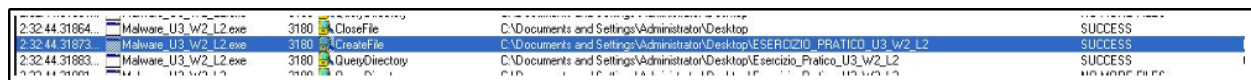
We enter the filter as seen in theory to show only the activities of the process named **"Malware\_U3\_W2\_L2.exe"**.

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.



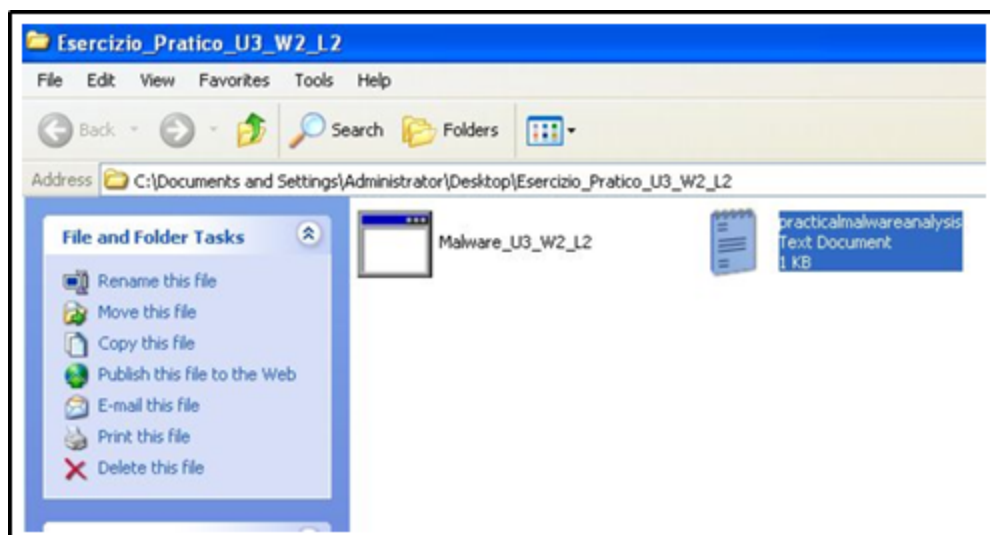
Time	Process	Operation	Path	Result
2:32:44.31538	Malware_U3_W2_L2.exe	QueryDirectory	C:\	NO MORE FILES
2:32:44.31543	Malware_U3_W2_L2.exe	CloseFile	C:\	SUCCESS
2:32:44.31598	Malware_U3_W2_L2.exe	CloseFile	C:\DOCUMENTS AND SETTINGS	SUCCESS
2:32:44.31601	Malware_U3_W2_L2.exe	CloseFile	C:\Documents and Settings	SUCCESS
2:32:44.31645	Malware_U3_W2_L2.exe	QueryDirectory	C:\Documents and Settings	NO MORE FILES
2:32:44.31648	Malware_U3_W2_L2.exe	CloseFile	C:\Documents and Settings	SUCCESS
2:32:44.31706	Malware_U3_W2_L2.exe	CloseFile	C:\Documents and Settings\ADMINISTRATOR	SUCCESS
2:32:44.31711	Malware_U3_W2_L2.exe	CloseFile	C:\Documents and Settings\Administrator	SUCCESS
2:32:44.31716	Malware_U3_W2_L2.exe	CloseFile	C:\Documents and Settings\Administrator	NO MORE FILES
2:32:44.31720	Malware_U3_W2_L2.exe	CloseFile	C:\Documents and Settings\Administrator	SUCCESS
2:32:44.31723	Malware_U3_W2_L2.exe	CloseFile	C:\Documents and Settings\Administrator\Desktop	SUCCESS
2:32:44.31805	Malware_U3_W2_L2.exe	CloseFile	C:\Documents and Settings\Administrator\Desktop	NO MORE FILES
2:32:44.31807	Malware_U3_W2_L2.exe	CloseFile	C:\Documents and Settings\Administrator\Desktop	SUCCESS
2:32:44.31854	Malware_U3_W2_L2.exe	CloseFile	C:\Documents and Settings\Administrator\Desktop	SUCCESS
2:32:44.31864	Malware_U3_W2_L2.exe	CreateFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS
2:32:44.31883	Malware_U3_W2_L2.exe	CloseFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS
2:32:44.31885	Malware_U3_W2_L2.exe	CloseFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	NO MORE FILES
2:32:44.31886	Malware_U3_W2_L2.exe	CloseFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS
2:32:44.31911	Malware_U3_W2_L2.exe	CloseFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS
2:32:44.31917	Malware_U3_W2_L2.exe	CloseFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	NO MORE FILES
2:32:44.31920	Malware_U3_W2_L2.exe	CloseFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS
2:32:44.31962	Malware_U3_W2_L2.exe	CloseFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	NO MORE FILES
2:32:44.31978	Malware_U3_W2_L2.exe	CloseFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS
2:32:44.31987	Malware_U3_W2_L2.exe	CloseFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS
2:32:44.31998	Malware_U3_W2_L2.exe	CloseFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	NO MORE FILES
2:32:44.32009	Malware_U3_W2_L2.exe	CloseFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS
2:32:44.32026	Malware_U3_W2_L2.exe	CloseFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS
2:32:44.32033	Malware_U3_W2_L2.exe	CloseFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS
2:32:44.32067	Malware_U3_W2_L2.exe	CloseFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS
2:32:44.32098	Malware_U3_W2_L2.exe	CloseFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS

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



Time	Process	Operation	Path	Result
2:32:44.31864	Malware_U3_W2_L2.exe	CloseFile	C:\Documents and Settings\Administrator\Desktop	SUCCESS
2:32:44.31873	Malware_U3_W2_L2.exe	CreateFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS
2:32:44.31883	Malware_U3_W2_L2.exe	CloseFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS
2:32:44.31885	Malware_U3_W2_L2.exe	CloseFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	NO MORE FILES

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**.

```
practicalmalwareanalysis - Notepad
File Edit Format View Help

[window: Save As]
cattura 20[ENTER]
[window: BinaryCollection]
*
[window: Run]
regedit0[ENTER]
[window: Registry Editor]
((((((((((((((((('((((((((('((((((((('((((((((('(((((((w'((( '((((((((((((((((((((((((((((
[window: WINDOWS]
p
[window: Prefetch]
*
[window: Confirm File Delete]
BACKSPACE 0[ENTER]
```

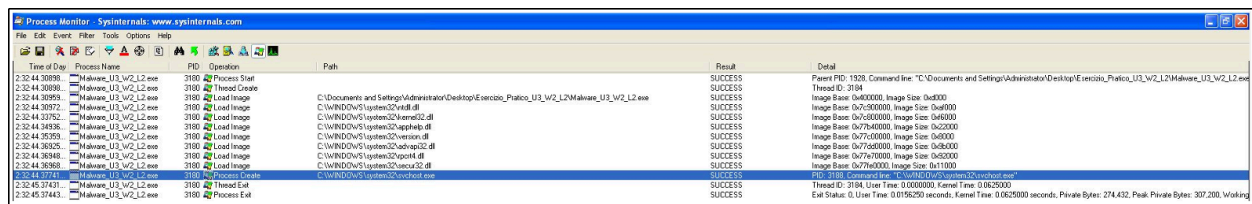
## Identifying Actions on Processes and Threads

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.

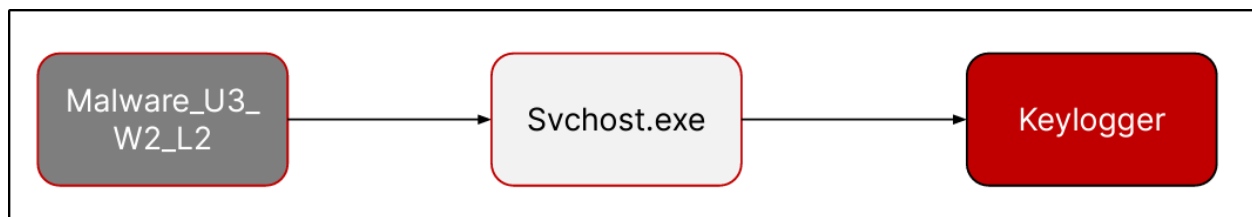
This is another frequent behavior of malware, trying to disguise their execution under a process with a valid name to evade any **antivirus/anti-malware**.



Time of Day	Process Name	PID	Operation	Path	Result	Detail
12:44:30898	Malware_U3_W2_L2.exe	3180	Process Start		SUCCESS	Parent PID: 1920, Command line: "C:\Documents and Settings\Administrator\Desktop\Esercizio_Protection_U3_W2_L2\Malware_U3_W2_L2.exe"
12:44:30898	Malware_U3_W2_L2.exe	3180	Thread Create		SUCCESS	Thread ID: 3184
12:44:30939	Malware_U3_W2_L2.exe	3180	Load Image	C:\Documents and Settings\Administrator\Desktop\Esercizio_Protection_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	Image Base: 0x400000, Image Size: 0x4000
12:44:30972	Malware_U3_W2_L2.exe	3180	Load Image	C:\Windows\System32\kernel.dll	SUCCESS	Image Base: 0x77D80000, Image Size: 0x4000
12:44:31752	Malware_U3_W2_L2.exe	3180	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x77D80000, Image Size: 0x4000
12:44:34936	Malware_U3_W2_L2.exe	3180	Load Image	C:\Windows\System32\user32.dll	SUCCESS	Image Base: 0x77D80000, Image Size: 0x4000
12:44:35259	Malware_U3_W2_L2.exe	3180	Load Image	C:\Windows\System32\GDI32.dll	SUCCESS	Image Base: 0x77D80000, Image Size: 0x4000
12:44:36325	Malware_U3_W2_L2.exe	3180	Load Image	C:\Windows\System32\ole32.dll	SUCCESS	Image Base: 0x77D80000, Image Size: 0x4000
12:44:36348	Malware_U3_W2_L2.exe	3180	Load Image	C:\Windows\System32\RPCRT4.dll	SUCCESS	Image Base: 0x77D80000, Image Size: 0x4000
12:44:36368	Malware_U3_W2_L2.exe	3180	Load Image	C:\Windows\System32\USER32.dll	SUCCESS	Image Base: 0x77D80000, Image Size: 0x4000
12:44:36368	Malware_U3_W2_L2.exe	3180	Process Create	C:\Windows\System32\svchost.exe	SUCCESS	Parent PID: 3180, Command line: "C:\Windows\System32\svchost.exe -k LocalSystemNetworkDiagnostics"
12:45:37431	Malware_U3_W2_L2.exe	3180	Thread Exit		SUCCESS	Thread ID: 3184, User Time: 0.000000 seconds, Kernel Time: 0.062000 seconds
12:45:37443	Malware_U3_W2_L2.exe	3180	Process Exit		SUCCESS	Exit Status: 0, User Time: 0.0156200 seconds, Kernel Time: 0.062000 seconds, Private Bytes: 274,432, Peak Private Bytes: 307,200, Working

## 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.



---