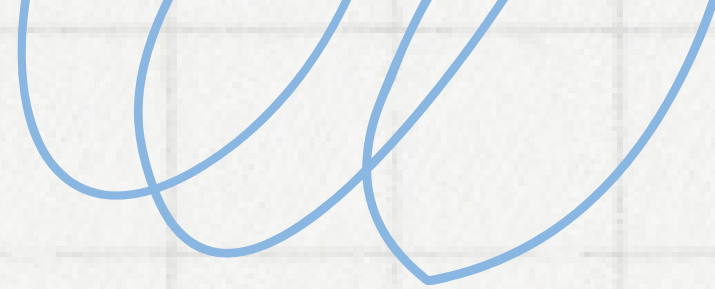


# Consegna S10/L2

di Giuseppe Lupoi



# Indice

03. Traccia

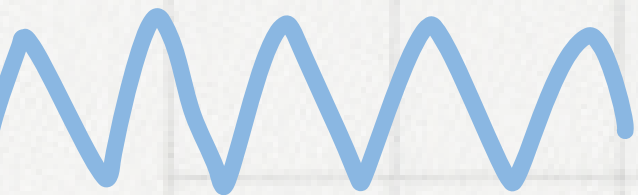
04. Lo scan di Process Monitor

05. Filtri e individuazione

06. Keylogger txt

07. Individuazione Thread

08. Profilazione del Malware



# Traccia

Nella lezione teorica del mattino, abbiamo visto come recuperare informazioni su un malware tramite l'analisi dinamica basica.

Con riferimento al file eseguibile contenuto nella cartella «**Esercizio\_Pratico\_U3\_W2\_L2**» presente sul desktop della vostra macchina virtuale dedicata all'analisi dei malware, rispondere ai seguenti quesiti:

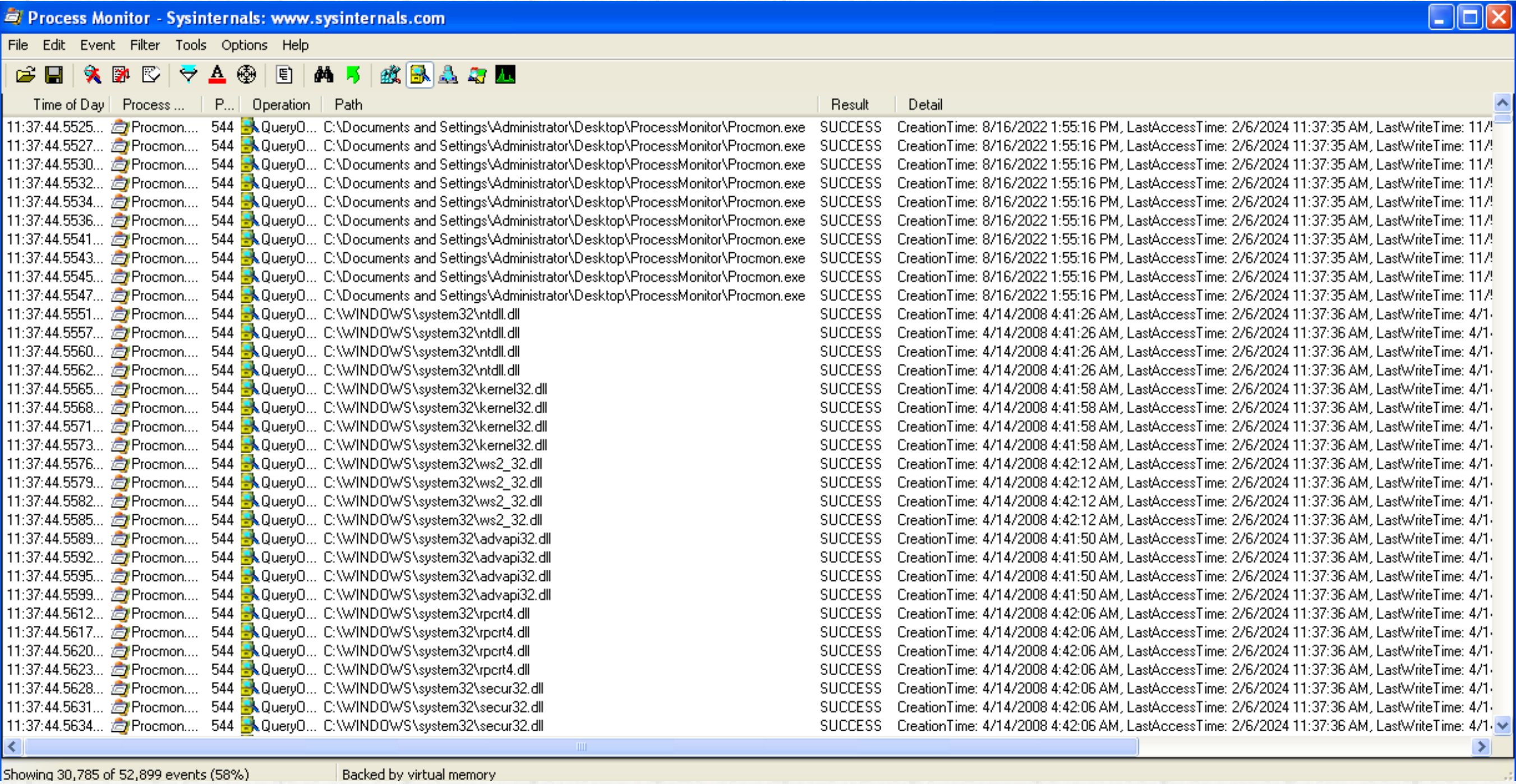
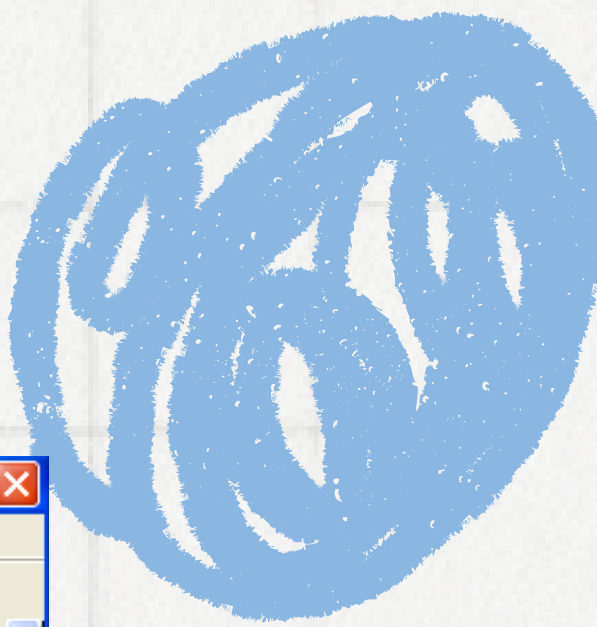
- Identificare eventuali azioni del malware sul file system utilizzando Process Monitor
- Identificare eventuali azioni del malware su processi e thread utilizzando Process Monitor
- Provare a profilare il malware in base alla correlazione tra «operation» e Path.

## Suggerimento:

Per quanto riguarda le attività dal malware sul file system, soffermatevi con particolare interesse sulle chiamate alla funzione create File su path noti (ad esempio il path dove è presente l'eseguibile del malware).



Per lo svolgimento della traccia di oggi, partendo dal primo punto, una volta avviata la macchina per l'analisi dei malware avvieremo **Process Monitor** dalla sua cartella per analizzare il malware contenuto nella cartella "Esercizio\_Pratico\_U3\_W2\_L2". Quindi avviando una prima scansione con tutti i filtri originali di Process Monitor e dopo aver avviato anche l'eseguibile del malware avremo una situazione come quella in figura qui sotto.



The screenshot shows the Process Monitor application window with the title bar "Process Monitor - Sysinternals: www.sysinternals.com". The menu bar includes File, Edit, Event, Filter, Tools, Options, and Help. The toolbar contains various icons for file operations, filters, and settings. The main display area is a table with columns: Time of Day, Process, PID, Operation, Path, Result, and Detail. The table lists numerous "QueryOpen" operations performed by "Procmon.exe" on various system files, all with a "SUCCESS" result. The status bar at the bottom indicates "Showing 30,785 of 52,899 events (58%)" and "Backed by virtual memory".

Time of Day	Process	PID	Operation	Path	Result	Detail
11:37:44.5525...	Procmon...	544	QueryOpen	C:\Documents and Settings\Administrator\Desktop\ProcessMonitor\Procmon.exe	SUCCESS	CreationTime: 8/16/2022 1:55:16 PM, LastAccessTime: 2/6/2024 11:37:35 AM, LastWriteTime: 11/...
11:37:44.5527...	Procmon...	544	QueryOpen	C:\Documents and Settings\Administrator\Desktop\ProcessMonitor\Procmon.exe	SUCCESS	CreationTime: 8/16/2022 1:55:16 PM, LastAccessTime: 2/6/2024 11:37:35 AM, LastWriteTime: 11/...
11:37:44.5530...	Procmon...	544	QueryOpen	C:\Documents and Settings\Administrator\Desktop\ProcessMonitor\Procmon.exe	SUCCESS	CreationTime: 8/16/2022 1:55:16 PM, LastAccessTime: 2/6/2024 11:37:35 AM, LastWriteTime: 11/...
11:37:44.5532...	Procmon...	544	QueryOpen	C:\Documents and Settings\Administrator\Desktop\ProcessMonitor\Procmon.exe	SUCCESS	CreationTime: 8/16/2022 1:55:16 PM, LastAccessTime: 2/6/2024 11:37:35 AM, LastWriteTime: 11/...
11:37:44.5534...	Procmon...	544	QueryOpen	C:\Documents and Settings\Administrator\Desktop\ProcessMonitor\Procmon.exe	SUCCESS	CreationTime: 8/16/2022 1:55:16 PM, LastAccessTime: 2/6/2024 11:37:35 AM, LastWriteTime: 11/...
11:37:44.5536...	Procmon...	544	QueryOpen	C:\Documents and Settings\Administrator\Desktop\ProcessMonitor\Procmon.exe	SUCCESS	CreationTime: 8/16/2022 1:55:16 PM, LastAccessTime: 2/6/2024 11:37:35 AM, LastWriteTime: 11/...
11:37:44.5541...	Procmon...	544	QueryOpen	C:\Documents and Settings\Administrator\Desktop\ProcessMonitor\Procmon.exe	SUCCESS	CreationTime: 8/16/2022 1:55:16 PM, LastAccessTime: 2/6/2024 11:37:35 AM, LastWriteTime: 11/...
11:37:44.5543...	Procmon...	544	QueryOpen	C:\Documents and Settings\Administrator\Desktop\ProcessMonitor\Procmon.exe	SUCCESS	CreationTime: 8/16/2022 1:55:16 PM, LastAccessTime: 2/6/2024 11:37:35 AM, LastWriteTime: 11/...
11:37:44.5545...	Procmon...	544	QueryOpen	C:\Documents and Settings\Administrator\Desktop\ProcessMonitor\Procmon.exe	SUCCESS	CreationTime: 8/16/2022 1:55:16 PM, LastAccessTime: 2/6/2024 11:37:35 AM, LastWriteTime: 11/...
11:37:44.5547...	Procmon...	544	QueryOpen	C:\Documents and Settings\Administrator\Desktop\ProcessMonitor\Procmon.exe	SUCCESS	CreationTime: 8/16/2022 1:55:16 PM, LastAccessTime: 2/6/2024 11:37:35 AM, LastWriteTime: 11/...
11:37:44.5551...	Procmon...	544	QueryOpen	C:\WINDOWS\system32\ntdll.dll	SUCCESS	CreationTime: 4/14/2008 4:41:26 AM, LastAccessTime: 2/6/2024 11:37:36 AM, LastWriteTime: 4/1...
11:37:44.5557...	Procmon...	544	QueryOpen	C:\WINDOWS\system32\ntdll.dll	SUCCESS	CreationTime: 4/14/2008 4:41:26 AM, LastAccessTime: 2/6/2024 11:37:36 AM, LastWriteTime: 4/1...
11:37:44.5560...	Procmon...	544	QueryOpen	C:\WINDOWS\system32\ntdll.dll	SUCCESS	CreationTime: 4/14/2008 4:41:26 AM, LastAccessTime: 2/6/2024 11:37:36 AM, LastWriteTime: 4/1...
11:37:44.5562...	Procmon...	544	QueryOpen	C:\WINDOWS\system32\ntdll.dll	SUCCESS	CreationTime: 4/14/2008 4:41:26 AM, LastAccessTime: 2/6/2024 11:37:36 AM, LastWriteTime: 4/1...
11:37:44.5565...	Procmon...	544	QueryOpen	C:\WINDOWS\system32\kernel32.dll	SUCCESS	CreationTime: 4/14/2008 4:41:58 AM, LastAccessTime: 2/6/2024 11:37:36 AM, LastWriteTime: 4/1...
11:37:44.5568...	Procmon...	544	QueryOpen	C:\WINDOWS\system32\kernel32.dll	SUCCESS	CreationTime: 4/14/2008 4:41:58 AM, LastAccessTime: 2/6/2024 11:37:36 AM, LastWriteTime: 4/1...
11:37:44.5571...	Procmon...	544	QueryOpen	C:\WINDOWS\system32\kernel32.dll	SUCCESS	CreationTime: 4/14/2008 4:41:58 AM, LastAccessTime: 2/6/2024 11:37:36 AM, LastWriteTime: 4/1...
11:37:44.5573...	Procmon...	544	QueryOpen	C:\WINDOWS\system32\kernel32.dll	SUCCESS	CreationTime: 4/14/2008 4:41:58 AM, LastAccessTime: 2/6/2024 11:37:36 AM, LastWriteTime: 4/1...
11:37:44.5576...	Procmon...	544	QueryOpen	C:\WINDOWS\system32\ws2_32.dll	SUCCESS	CreationTime: 4/14/2008 4:42:12 AM, LastAccessTime: 2/6/2024 11:37:36 AM, LastWriteTime: 4/1...
11:37:44.5579...	Procmon...	544	QueryOpen	C:\WINDOWS\system32\ws2_32.dll	SUCCESS	CreationTime: 4/14/2008 4:42:12 AM, LastAccessTime: 2/6/2024 11:37:36 AM, LastWriteTime: 4/1...
11:37:44.5582...	Procmon...	544	QueryOpen	C:\WINDOWS\system32\ws2_32.dll	SUCCESS	CreationTime: 4/14/2008 4:42:12 AM, LastAccessTime: 2/6/2024 11:37:36 AM, LastWriteTime: 4/1...
11:37:44.5585...	Procmon...	544	QueryOpen	C:\WINDOWS\system32\ws2_32.dll	SUCCESS	CreationTime: 4/14/2008 4:42:12 AM, LastAccessTime: 2/6/2024 11:37:36 AM, LastWriteTime: 4/1...
11:37:44.5589...	Procmon...	544	QueryOpen	C:\WINDOWS\system32\advapi32.dll	SUCCESS	CreationTime: 4/14/2008 4:41:50 AM, LastAccessTime: 2/6/2024 11:37:36 AM, LastWriteTime: 4/1...
11:37:44.5592...	Procmon...	544	QueryOpen	C:\WINDOWS\system32\advapi32.dll	SUCCESS	CreationTime: 4/14/2008 4:41:50 AM, LastAccessTime: 2/6/2024 11:37:36 AM, LastWriteTime: 4/1...
11:37:44.5595...	Procmon...	544	QueryOpen	C:\WINDOWS\system32\advapi32.dll	SUCCESS	CreationTime: 4/14/2008 4:41:50 AM, LastAccessTime: 2/6/2024 11:37:36 AM, LastWriteTime: 4/1...
11:37:44.5599...	Procmon...	544	QueryOpen	C:\WINDOWS\system32\advapi32.dll	SUCCESS	CreationTime: 4/14/2008 4:41:50 AM, LastAccessTime: 2/6/2024 11:37:36 AM, LastWriteTime: 4/1...
11:37:44.5612...	Procmon...	544	QueryOpen	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	CreationTime: 4/14/2008 4:42:06 AM, LastAccessTime: 2/6/2024 11:37:36 AM, LastWriteTime: 4/1...
11:37:44.5617...	Procmon...	544	QueryOpen	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	CreationTime: 4/14/2008 4:42:06 AM, LastAccessTime: 2/6/2024 11:37:36 AM, LastWriteTime: 4/1...
11:37:44.5620...	Procmon...	544	QueryOpen	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	CreationTime: 4/14/2008 4:42:06 AM, LastAccessTime: 2/6/2024 11:37:36 AM, LastWriteTime: 4/1...
11:37:44.5623...	Procmon...	544	QueryOpen	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	CreationTime: 4/14/2008 4:42:06 AM, LastAccessTime: 2/6/2024 11:37:36 AM, LastWriteTime: 4/1...
11:37:44.5628...	Procmon...	544	QueryOpen	C:\WINDOWS\system32\secur32.dll	SUCCESS	CreationTime: 4/14/2008 4:42:06 AM, LastAccessTime: 2/6/2024 11:37:36 AM, LastWriteTime: 4/1...
11:37:44.5631...	Procmon...	544	QueryOpen	C:\WINDOWS\system32\secur32.dll	SUCCESS	CreationTime: 4/14/2008 4:42:06 AM, LastAccessTime: 2/6/2024 11:37:36 AM, LastWriteTime: 4/1...
11:37:44.5634...	Procmon...	544	QueryOpen	C:\WINDOWS\system32\secur32.dll	SUCCESS	CreationTime: 4/14/2008 4:42:06 AM, LastAccessTime: 2/6/2024 11:37:36 AM, LastWriteTime: 4/1...

Applichiamo dei filtri per poterci concentrare meglio sulle attività del malware e soprattutto cerchiamo di capire cosa fa.

Nella barra degli strumenti in alto su **Process Monitor** clicchiamo su **Filter** ed andiamo ad aggiungere un filtro con il nome del malware che ci interessa per restringere la ricerca.

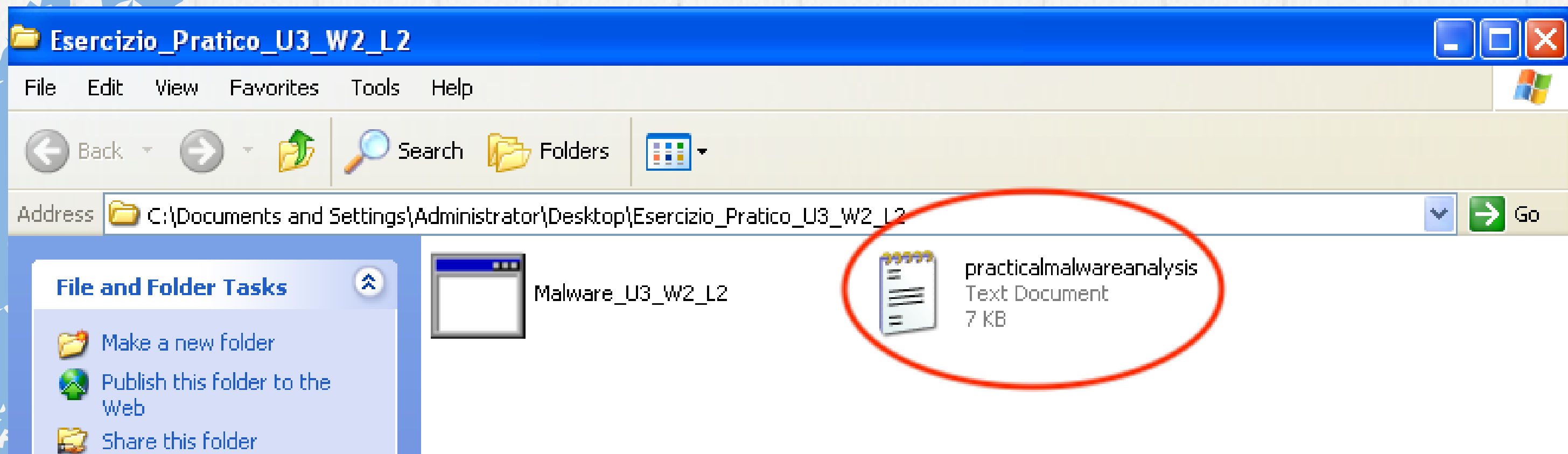
Notiamo in una riga particolare che il malware in questione è andato a creare un file nella cartella dove risiede.

1:30:59.66517...	Explorer.EXE	268	CloseFile	C:\Documents and Settings\Administrator\...	SUCCESS	
1:30:59.86936...	Explorer.EXE	268	CreateFile	C:\Documents and Settings\Administrator\Desktop	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Attributes: n/a, S...
1:30:59.86962...	Explorer.EXE	268	QueryDirectory	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS	Filter: Esercizio_Pratico_U3_W2_L2, 1: Esercizio_Pratico_U3_W2_L2, FileInformationClass: FileBothDirectoryInformation
1:30:59.86975...	Explorer.EXE	268	CloseFile	C:\Documents and Settings\Administrator\Desktop	SUCCESS	
1:30:59.86994...	Explorer.EXE	268	CreateFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Attributes: n/a, S...
1:30:59.87009...	Explorer.EXE	268	QueryDirectory	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS	Filter: practicalmalwareanalysis.log, 1: practicalmalwareanalysis.log, FileInformationClass: FileBothDirectoryInformation
1:30:59.87023...	Explorer.EXE	268	CloseFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS	
1:30:59.87164...	Explorer.EXE	268	CreateFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Non-Directory File, Attributes: n/a, ShareMode: Read, AllocationSize: n/a, Ope...
1:30:59.87175...	Explorer.EXE	268	FileSystemControl	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS	Control: FSCTL_REQUEST_FILTER_OPLOCK
1:30:59.87190...	Explorer.EXE	268	CreateFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: , Attributes: N, ShareMode: Read, Write, Delete, AllocationSize: n/a, OpenRes...
1:30:59.87206...	Explorer.EXE	268	QueryBasicInformationFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS	0: ::\$DATA
1:30:59.87219...	Explorer.EXE	268	QueryBasicInformationFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS	CreationTime: 2/6/2024 11:45:58 AM, LastAccessTime: 2/6/2024 4:30:12 PM, LastWriteTime: 2/6/2024 4:30:12 PM, ChangeTime: 2/6/2...
1:30:59.87235...	Explorer.EXE	268	ReadFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS	Offset: 0, Length: 24
1:30:59.87261...	Explorer.EXE	268	CreateFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log\Raec25ph4su... NAME NOT FOUND		Desired Access: Generic Read, Disposition: Open, Options: , Attributes: N, ShareMode: Read, Write, Delete, AllocationSize: n/a

268	CreateFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS
-----	------------	---	---------



Infatti andando poi a controllare nella cartella dov'è presente il malware è stato appunto creato un nuovo file di testo assente in precedenza, come possiamo notare dall'immagine



Andremo ora ad analizzare l'impatto del malware sui processi e thread, come possiamo vedere dall'immagine sottostante è stato creato un processo con successo direttamente sul file system sotto un nome innocuo perciò più difficile da individuare.

Process Monitor - Sysinternals: <a href="http://www.sysinternals.com">www.sysinternals.com</a>						
File Edit Event Filter Tools Options Help						
Time of Day	Process Name	PID	Operation	Path	Result	Detail
1:55:23.95666...	Malware_U3_W2_L2.exe	2132	Process Start		SUCCESS	Parent PID: 240, Command line: "C:\Documents and Settings\Administrator\Desktop\Esercizio_
1:55:23.95666...	Malware_U3_W2_L2.exe	2132	Thread Create		SUCCESS	Thread ID: 2136
1:55:23.95790...	Malware_U3_W2_L2.exe	2132	Load Image	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	Image Base: 0x400000, Image Size: 0xd000
1:55:23.95808...	Malware_U3_W2_L2.exe	2132	Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Image Base: 0x7c900000, Image Size: 0xaf000
1:55:23.98833...	Malware_U3_W2_L2.exe	2132	Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Image Base: 0x7c800000, Image Size: 0xf6000
1:55:23.99939...	Malware_U3_W2_L2.exe	2132	Load Image	C:\WINDOWS\system32\apphelp.dll	SUCCESS	Image Base: 0x77b40000, Image Size: 0x22000
1:55:24.00364...	Malware_U3_W2_L2.exe	2132	Load Image	C:\WINDOWS\system32\version.dll	SUCCESS	Image Base: 0x77c00000, Image Size: 0x8000
1:55:24.01180...	Malware_U3_W2_L2.exe	2132	Load Image	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Image Base: 0x77dd0000, Image Size: 0x9b000
1:55:24.01202...	Malware_U3_W2_L2.exe	2132	Load Image	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	Image Base: 0x77e70000, Image Size: 0x92000
1:55:24.01228...	Malware_U3_W2_L2.exe	2132	Load Image	C:\WINDOWS\system32\secur32.dll	SUCCESS	Image Base: 0x77fe0000, Image Size: 0x11000
1:55:24.02286...	Malware_U3_W2_L2.exe	2132	Process Create	C:\WINDOWS\system32\svchost.exe	SUCCESS	PID: 2140, Command line: "C:\WINDOWS\system32\svchost.exe"
1:55:25.02357...	Malware_U3_W2_L2.exe	2132	Thread Exit		SUCCESS	Thread ID: 2136, User Time: 0.0000000, Kernel Time: 0.0468750
1:55:25.02434...	Malware_U3_W2_L2.exe	2132	Process Exit		SUCCESS	Exit Status: 0, User Time: 0.0156250 seconds, Kernel Time: 0.0468750 seconds, Private Bytes:

Possiamo dunque confermare dalle analisi fatte in precedenza e dopo la visione del nuovo file di testo creato che abbiamo a che fare con un malware di tipo **keylogger**.

Un keylogger è un tipo di software progettato per registrare e monitorare le tastiere di un computer, al fine di catturare tutte le informazioni digitate dall'utente. Questo tipo di software può essere utilizzato a fini legittimi, come il monitoraggio dell'attività dell'utente su un computer o la registrazione di informazioni di login per scopi di sicurezza. Tuttavia, è spesso associato a utilizzi malevoli quando viene installato senza il consenso dell'utente per rubare informazioni sensibili come password, dati finanziari o altre informazioni personali.

```
practicalmalwareanalysis - Notepad
File Edit Format View Help

[window: Esercizio_Pratico_U3_W2_L2]
[window: Esercizio_Pratico_U3_W2_L2]
[window: Esercizio_Pratico_U3_W2_L2]
[window: Esercizio_Pratico_U3_W2_L2]
[window: Process Monitor Filter]
[window: Process Monitor Filter]
[window: Process Monitor Filter]
[window: Process Monitor Filter]
eeeeessseeeerrrrccccciiiizzzziiiiooooommmmmmmBACKSPACE BACKSPACE BACKSPACE BACKSPACE mmmmaaaa1111wwwaaaaarrreeeee BACKSPACE BACKSPACE
KSPACE BACKSPACE BACKSPACE BACKSPACE ppprrrrraaaattttiiiccckooo'''uuuu3333'''www2222'''11112222mmmmaaaa1111wwwaaaaarrreeeeeBACKSPACE
[window: Process Monitor Filter]
mmmmaaaaa11111wwwaaaaarrreeeee BACKSPACE BACKSPACE BACKSPACE BACKSPACE BACKSPACE BACKSPACE (((((((((BACKSPACE BACKSPACE BACKSPACE BAC
[window: Process Monitor Filter]
[window: Process Monitor Filter]
mmmmmmmaaaaaa1111111wwwawwaaaaaaarrrrrrrreeeeeeeuuuuuuuu3333333wwwwww2222222BACKSPACE BACKSPACE BACKSPACE BACKSPACE BACKSPACE
[window: Esercizio_Pratico_U3_W2_L2]
[window: Esercizio_Pratico_U3_W2_L2]
[window: Esercizio_Pratico_U3_W2_L2]
[window: Esercizio_Pratico_U3_W2_L2]
[window: Esercizio_Pratico_U3_W2_L2]
[window: Esercizio_Pratico_U3_W2_L2]
[window: Esercizio_Pratico_U3_W2_L2]
[window: Esercizio_Pratico_U3_W2_L2]
[window: Process Monitor Filter]
[window: Process Monitor Filter]
[window: Process Monitor Filter]
[window: Process Monitor Filter]
[window: Process Monitor Filter]
```