

Malware analysis

Sommario

| | |
|---|---|
| Traccia S10/L2 | 1 |
| Analisi dei processi e del file system..... | 1 |

Traccia S10/L2

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

Per svolgere questo esercizio utilizzerò vari tool tra cui:

- Process Explorer, un tool che permette l'analisi dettagliata di tutti i processi in esecuzione su un sistema.
- Process Monitor, permette di monitorare i processi ed i thread attivi, l'attività di rete, l'accesso ai file e le chiamate di sistema effettuate su un sistema operativo.

Analisi dei processi e del file system

Avviamo la cattura di process monitor e controlliamo process explorer prima dell'avvio del malware

Inizialmente la situazione dei processi è la seguente:

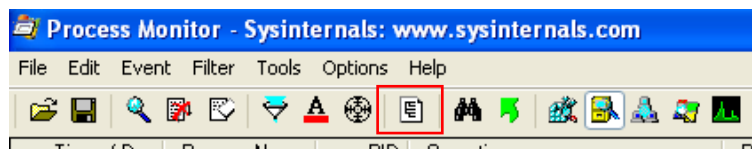
| Process Explorer - Sysinternals: www.sysinternals.com [MALWARE_TEST\Administrator] | | | | | | |
|--|--------|---------------|-------------|------|----------------------------------|--------------------------------|
| File Options View Process Find Handle Users Help | | | | | | |
| Process | CPU | Private Bytes | Working Set | PID | Description | Company Name |
| alg.exe | | 1,128 K | 3,436 K | 1104 | Application Layer Gateway S... | Microsoft Corporation |
| apateDNS.exe | | 19,220 K | 18,940 K | 1840 | Mandiant | Mandiant |
| cmd.exe | | 1,920 K | 2,348 K | 2040 | Windows Command Processor | Microsoft Corporation |
| cmd.exe | | 1,920 K | 2,348 K | 252 | Windows Command Processor | Microsoft Corporation |
| csrss.exe | | 1,836 K | 3,588 K | 652 | Client Server Runtime Process | Microsoft Corporation |
| dumpcap.exe | | 1,936 K | 4,656 K | 2452 | Dumpcap | The Wireshark developer ... |
| explorer.exe | | 12,288 K | 18,208 K | 696 | Windows Explorer | Microsoft Corporation |
| IEEXPLORE.EXE | | 1,812 K | 4,464 K | 172 | Internet Explorer | Microsoft Corporation |
| IPROSetMonitor.exe | | 472 K | 1,980 K | 156 | Intel® PROSet Monitoring S... | Intel Corporation |
| lsass.exe | | 3,880 K | 5,780 K | 732 | LSA Shell (Export Version) | Microsoft Corporation |
| Procmon.exe | | 7,060 K | 5,336 K | 2940 | Process Monitor | Sysinternals - www.sysinter... |
| Regshot-x86-Unicode.exe | | 728 K | 2,336 K | 284 | Regshot 1.9.0 x86 Unicode | Regshot Team |
| services.exe | | 1,644 K | 3,180 K | 720 | Services and Controller app | Microsoft Corporation |
| smss.exe | | 168 K | 388 K | 596 | Windows NT Session Mana... | Microsoft Corporation |
| spoolsv.exe | | 4,104 K | 6,484 K | 1384 | Spooler SubSystem App | Microsoft Corporation |
| svchost.exe | | 2,084 K | 3,064 K | 1968 | Generic Host Process for Wi... | Microsoft Corporation |
| svchost.exe | | 1,644 K | 4,248 K | 1292 | Generic Host Process for Wi... | Microsoft Corporation |
| svchost.exe | | 1,300 K | 3,464 K | 1236 | Generic Host Process for Wi... | Microsoft Corporation |
| svchost.exe | | 3,024 K | 4,672 K | 984 | Generic Host Process for Wi... | Microsoft Corporation |
| svchost.exe | | 1,744 K | 4,212 K | 1048 | Generic Host Process for Wi... | Microsoft Corporation |
| svchost.exe | | 13,700 K | 22,432 K | 1136 | Generic Host Process for Wi... | Microsoft Corporation |
| System | | 0 K | 236 K | 4 | | |
| VBoxService.exe | | 2,160 K | 3,436 K | 912 | VirtualBox Guest Additions S... | Oracle Corporation |
| VGAuthService.exe | | 6,264 K | 9,000 K | 264 | VMware Guest Authentica... | VMware, Inc. |
| vmacthlp.exe | | 564 K | 2,392 K | 932 | VMware Activation Helper | VMware, Inc. |
| winlogon.exe | | 6,800 K | 3,332 K | 676 | Windows NT Logon Applicat... | Microsoft Corporation |
| wmiprvse.exe | | 2,548 K | 6,496 K | 2080 | WMI | Microsoft Corporation |
| wmiprvse.exe | | 1,936 K | 4,748 K | 3060 | WMI | Microsoft Corporation |
| wscntfy.exe | | 468 K | 1,884 K | 1984 | Windows Security Center No... | Microsoft Corporation |
| wuauclt.exe | | 5,604 K | 5,088 K | 2004 | Automatic Updates | Microsoft Corporation |
| wuauclt.exe | | 6,464 K | 6,560 K | 1564 | Automatic Updates | Microsoft Corporation |
| Interrupts | < 0.01 | 0 K | 0 K | n/a | Hardware Interrupts and DPCs | |
| VBoxTray.exe | 0.75 | 1,964 K | 3,472 K | 340 | VirtualBox Guest Additions Tr... | Oracle Corporation |
| Wireshark.exe | 0.75 | 95,576 K | 72,480 K | 2036 | Wireshark | The Wireshark developer ... |
| procepx.exe | 1.49 | 10,476 K | 14,472 K | 3288 | Sysinternals Process Explorer | Sysinternals - www.sysinter... |
| System Idle Process | 97.01 | 0 K | 28 K | 0 | | |

Dopo l'avvio del malware possiamo notare un nuovo processo con PID 3680 camuffato con un nome generico di un processo Windows

Process Explorer - Sysinternals: www.sysinternals.com [MALWARE_TEST\Administrator]

| Process | CPU | Private Bytes | Working Set | PID | Description | Company Name |
|-------------------------|-------|---------------|-------------|------|----------------------------------|--------------------------------|
| alg.exe | | 1,128 K | 3,444 K | 1104 | Application Layer Gateway S... | Microsoft Corporation |
| apateDNS.exe | | 19,272 K | 19,016 K | 1840 | Mandiant | Mandiant |
| cmd.exe | | 1,920 K | 2,348 K | 2040 | Windows Command Processor | Microsoft Corporation |
| cmd.exe | | 1,920 K | 2,348 K | 252 | Windows Command Processor | Microsoft Corporation |
| dumpcap.exe | | 1,936 K | 4,656 K | 2452 | Dumpcap | The Wireshark developer ... |
| explorer.exe | | 12,156 K | 2,880 K | 696 | Windows Explorer | Microsoft Corporation |
| IEXPLORE.EXE | | 1,812 K | 4,488 K | 172 | Internet Explorer | Microsoft Corporation |
| IPROSetMonitor.exe | | 472 K | 1,980 K | 156 | Intel® PROSet Monitoring S... | Intel Corporation |
| lsass.exe | | 3,784 K | 5,760 K | 732 | LSA Shell (Export Version) | Microsoft Corporation |
| Procmon.exe | | 8,376 K | 3,500 K | 2940 | Process Monitor | Sysinternals - www.sysinter... |
| Regshot-x86-Unicode.exe | | 728 K | 2,336 K | 284 | Regshot 1.9.0 x86 Unicode | Regshot Team |
| services.exe | | 1,664 K | 3,204 K | 720 | Services and Controller app | Microsoft Corporation |
| smss.exe | | 168 K | 388 K | 596 | Windows NT Session Mana... | Microsoft Corporation |
| spoolsv.exe | | 4,064 K | 6,476 K | 1384 | Spooler SubSystem App | Microsoft Corporation |
| svchost.exe | | 2,084 K | 3,068 K | 1968 | Generic Host Process for Wl... | Microsoft Corporation |
| svchost.exe | | 1,644 K | 4,248 K | 1292 | Generic Host Process for Wl... | Microsoft Corporation |
| svchost.exe | | 1,276 K | 3,456 K | 1236 | Generic Host Process for Wl... | Microsoft Corporation |
| svchost.exe | | 3,024 K | 4,672 K | 984 | Generic Host Process for Wl... | Microsoft Corporation |
| svchost.exe | | 1,764 K | 4,224 K | 1048 | Generic Host Process for Wl... | Microsoft Corporation |
| svchost.exe | | 864 K | 2,200 K | 3680 | Generic Host Process for Wl... | Microsoft Corporation |
| svchost.exe | | 13,608 K | 22,324 K | 1136 | Generic Host Process for Wl... | Microsoft Corporation |
| System | | 0 K | 236 K | 4 | | |
| VBoxService.exe | | 2,160 K | 3,436 K | 912 | VirtualBox Guest Additions S... | Oracle Corporation |
| VBoxTray.exe | | 1,964 K | 3,472 K | 340 | VirtualBox Guest Additions Tr... | Oracle Corporation |
| VGAuthService.exe | | 6,264 K | 9,000 K | 264 | VMware Guest Authentica... | VMware, Inc. |
| vmacthlp.exe | | 564 K | 2,392 K | 932 | VMware Activation Helper | VMware, Inc. |
| winlogon.exe | | 6,272 K | 2,960 K | 676 | Windows NT Logon Applicat... | Microsoft Corporation |
| wmiprvse.exe | | 2,432 K | 6,448 K | 2080 | WMI | Microsoft Corporation |
| wmiprvse.exe | | 1,864 K | 4,744 K | 3060 | WMI | Microsoft Corporation |
| wscntfy.exe | | 468 K | 1,888 K | 1984 | Windows Security Center No... | Microsoft Corporation |
| wuauclt.exe | | 5,592 K | 5,080 K | 2004 | Automatic Updates | Microsoft Corporation |
| csrss.exe | 0.76 | 1,856 K | 3,624 K | 652 | Client Server Runtime Process | Microsoft Corporation |
| Wireshark.exe | 0.76 | 95,588 K | 72,496 K | 2036 | Wireshark | The Wireshark developer ... |
| Interrupts | 1.52 | 0 K | 0 K | n/a | Hardware Interrupts and DPCs | |
| procexp.exe | 1.52 | 11,472 K | 15,740 K | 3288 | Sysinternals Process Explorer | Sysinternals - www.sysinter... |
| System Idle Process | 95.45 | 0 K | 28 K | 0 | | |

Ora andiamo su process monitor e clicchiamo su process tree

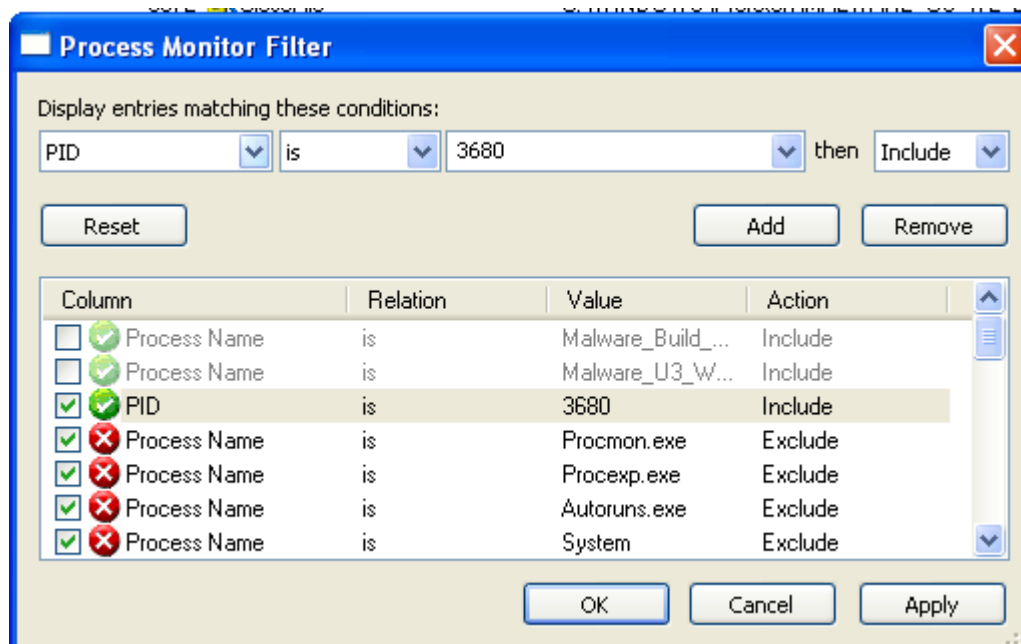


Possiamo notare che il processo svchost.exe è figlio del processo padre del malware. Notiamo anche i processi del blocco note, nonostante non sia mai stato avviato direttamente.

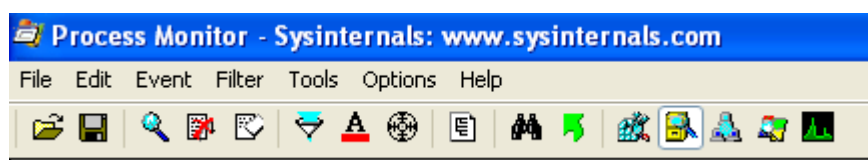
| Process | Description | Image Path | Life Time | Company | Owner | Command |
|-----------------------------------|-----------------------|--|-----------|-----------------------|------------------|-----------|
| svchost.exe (1048) | Generic Host Proc... | C:\WINDOWS\system32\svchost.exe | | Microsoft Corporat... | NT AUTHORITY\... | C:\WIND |
| cmd.exe (2040) | Windows Comma... | C:\WINDOWS\system32\cmd.exe | | Microsoft Corporat... | NT AUTHORITY\... | cmd /c st |
| Internet Explorer (172) | Internet Explorer | C:\Program Files\Internet Explorer\IEXPLORE.EXE | | Microsoft Corporat... | NT AUTHORITY\... | "C:\Progr |
| cmd.exe (252) | Windows Comma... | C:\WINDOWS\system32\cmd.exe | | Microsoft Corporat... | NT AUTHORITY\... | cmd /c st |
| Explorer.exe (696) | Windows Explorer | C:\WINDOWS\Explorer.EXE | | Microsoft Corporat... | MALWARE_TES... | C:\WIND |
| VBOTray.exe (340) | VirtualBox Guest ... | C:\WINDOWS\system32\VBOTray.exe | | Oracle Corporation | MALWARE_TES... | "C:\WIND |
| Regshot-x86-Unicode.exe (284) | Regshot 1.9.0 x86... | C:\Documents and Settings\Administrator\Desktop\Re... | | Regshot Team | MALWARE_TES... | "C:\Docu |
| Wireshark.exe (2036) | Wireshark | C:\Program Files\Wireshark\Wireshark.exe | | The Wireshark de... | MALWARE_TES... | "C:\Progr |
| dumpcap.exe (2452) | Dumpcap | C:\Program Files\Wireshark\dumpcap.exe | | The Wireshark de... | MALWARE_TES... | "C:\Progr |
| apateDNS.exe (1840) | Mandiant | C:\Documents and Settings\Administrator\Desktop\sdl... | | Mandiant | MALWARE_TES... | "C:\Docu |
| Procmon.exe (2940) | Process Monitor | C:\Documents and Settings\Administrator\Desktop\Pr... | | Sysinternals - ww... | MALWARE_TES... | "C:\Docu |
| proccp.exe (3288) | Sysinternals Proce... | C:\Documents and Settings\Administrator\Desktop\Pr... | | Sysinternals - ww... | MALWARE_TES... | "C:\Docu |
| Malware_U3_W2_L2.exe (367) | | C:\Documents and Settings\Administrator\Desktop\Es... | | | MALWARE_TES... | "C:\Docu |
| svchost.exe (3680) | Generic Host Proc... | C:\WINDOWS\system32\svchost.exe | | Microsoft Corporat... | MALWARE_TES... | "C:\WIND |
| NOTEPAD.EXE (432) | Notepad | C:\WINDOWS\system32\NOTEPAD.EXE | | Microsoft Corporat... | MALWARE_TES... | "C:\WIND |
| NOTEPAD.EXE (2524) | Notepad | C:\WINDOWS\system32\NOTEPAD.EXE | | Microsoft Corporat... | MALWARE_TES... | "C:\WIND |
| NOTEPAD.EXE (2568) | Notepad | C:\WINDOWS\system32\NOTEPAD.EXE | | Microsoft Corporat... | MALWARE_TES... | "C:\WIND |
| Idle (0) | Idle | | | | | |
| System (4) | System | | | | NT AUTHORITY\... | |
| smss.exe (596) | Windows NT Ses... | C:\WINDOWS\System32\smss.exe | | Microsoft Corporat... | NT AUTHORITY\... | \SystemF |
| csrss.exe (652) | Client Server Runt... | C:\WINDOWS\system32\csrss.exe | | Microsoft Corporat... | NT AUTHORITY\... | C:\WIND |
| winlogon.exe (676) | Windows NT Log... | C:\WINDOWS\system32\winlogon.exe | | Microsoft Corporat... | NT AUTHORITY\... | winlogon |
| services.exe (720) | Services and Cont... | C:\WINDOWS\system32\services.exe | | Microsoft Corporat... | NT AUTHORITY\... | C:\WIND |
| svchost.exe (984) | Generic Host Proc... | C:\WINDOWS\system32\svchost.exe | | Microsoft Corporat... | NT AUTHORITY\... | C:\WIND |
| wmiprvse.exe (20) | WMI | C:\WINDOWS\system32\wbem\wmiprvse.exe | | Microsoft Corporat... | NT AUTHORITY\... | C:\WIND |

Procediamo con l'analisi di questo processo. Andiamo su filtri e applichiamo un filtro per il processo con pid 3680

| Time of Day | PID | Operation |
|------------------|------|-----------|
| 4:02:42.60272... | 3672 | QueryNa |
| 4:02:42.60355... | 3672 | QueryNa |
| 4:02:42.60379... | 3672 | CreateFi |
| 4:02:42.60395... | 3672 | QuerySt |
| 4:02:42.60515... | 3672 | ReadFile |
| 4:02:42.60518... | 3672 | ReadFile |
| 4:02:42.60573... | 3672 | CloseFile |
| 4:02:42.60600... | 3672 | CreateFi |
| 4:02:42.60603... | 3672 | QueryInf |
| 4:02:42.60607... | 3672 | FileSyste |



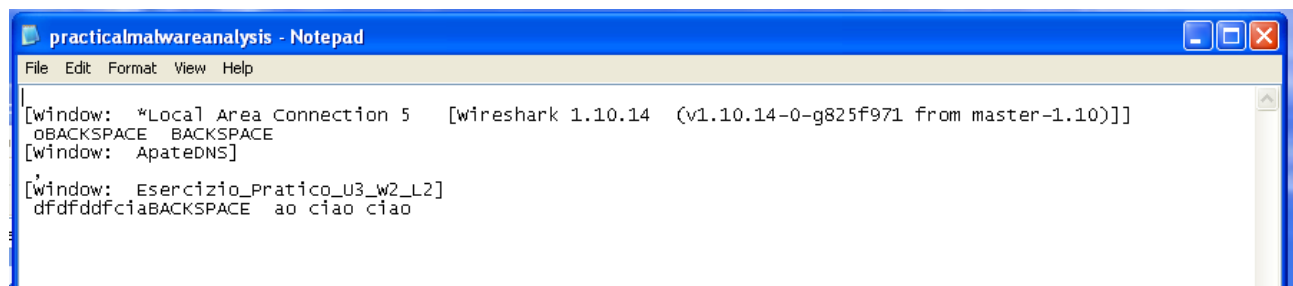
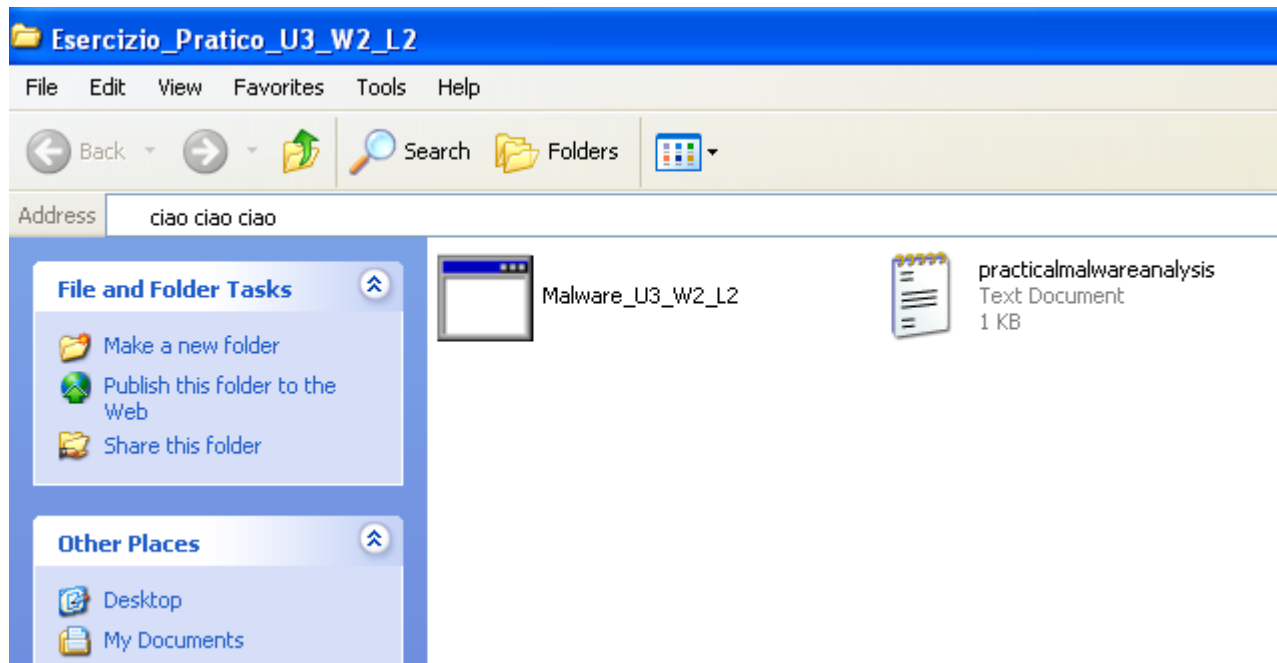
Selezioniamo il filtro per visualizzare solo le attività sul file system



Possiamo notare che questo processo figlio crea un log all'interno della cartella in cui è presente il malware

| Process Name | PID | Operation | Path | Result |
|--------------|------|------------------------------|---|---------|
| svchost.exe | 3680 | WriteFile | C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log | SUCCESS |
| svchost.exe | 3680 | CloseFile | C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log | SUCCESS |
| svchost.exe | 3680 | CreateFile | C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log | SUCCESS |
| svchost.exe | 3680 | QueryStandardInformationFile | C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log | SUCCESS |
| svchost.exe | 3680 | WriteFile | C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log | SUCCESS |
| svchost.exe | 3680 | CloseFile | C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log | SUCCESS |
| svchost.exe | 3680 | CreateFile | C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log | SUCCESS |
| svchost.exe | 3680 | QueryStandardInformationFile | C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log | SUCCESS |
| svchost.exe | 3680 | WriteFile | C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log | SUCCESS |
| svchost.exe | 3680 | CloseFile | C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log | SUCCESS |
| svchost.exe | 3680 | CreateFile | C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log | SUCCESS |
| svchost.exe | 3680 | QueryStandardInformationFile | C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log | SUCCESS |
| svchost.exe | 3680 | WriteFile | C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log | SUCCESS |
| svchost.exe | 3680 | CloseFile | C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log | SUCCESS |
| svchost.exe | 3680 | CreateFile | C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log | SUCCESS |
| svchost.exe | 3680 | QueryStandardInformationFile | C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log | SUCCESS |
| svchost.exe | 3680 | CloseFile | C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log | SUCCESS |
| svchost.exe | 3680 | CreateFile | C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log | SUCCESS |
| svchost.exe | 3680 | QueryStandardInformationFile | C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log | SUCCESS |

Infatti, andando nella cartella è stato creato un file txt con all'interno delle stringhe che sembrano gli input della tastiera.



A quanto pare ci troviamo davanti ad un keylogger!