

Traccia:

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.



Process Monitor - Sysinternals: www.	w.sysinternals.com			
File Edit Event Filter Tools Options Help				
9:25:23.3763194 AM Malware_U3_W2_L2.exe	3440 🍣 Process Start		SUCCESS	Parent PID: 1896, Command line: "C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.
9:25:23:37632 Malware_U3_W2_L2.exe	3440 🚉 Thread Create		SUCCESS	Thread ID: 3444
9:25:23.37655 Malware_U3_W2_L2.exe 9:25:23.37690 Malware_U3_W2_L2.exe	3440 🖳 QueryNameInformationFile 3440 🌊 Load Image	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	Name: \Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe Image Base: 0x400000, Image Size: 0xd000
9:25:23.37718 Malware_U3_W2_L2.exe	3440 ag Load Image 3440 ag Load Image	C:\WINDOWS\system32\ntdl.dll	SUCCESS	Image Base: 0x7c500000, Image Size: 0xal000
9:25:23.37723 Malware U3 W2 L2 exe	3440 QueryNameInformationFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	Name: \Documents and Settings\Administrator\Desktop\Esercizio_Prabico_U3_W2_L2\Malware_U3_W2_L2.exe
9:25:23:37755 Malware 113 W2 12 eve	3440 CreateFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Attributes: n/a, ShareMode: None, AllocationSize: n/
9-25-23 37790 Mahuara 113 W2 1.2 ava	3440 🖳 QueryStandardInformationFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf	SUCCESS	AllocationSize: 8,192, EndOfFile: 5,832, NumberOfLinks: 1, DeletePending: False, Directory: False
9:25:23.37799 Malware_U3_W2_L2.exe	3440 ReadFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf	SUCCESS	Offset: 0, Length: 5,832
9:25:23.37836 Malware_U3_W2_L2.exe 9:25:23.37844 Malware_U3_W2_L2.exe	3440 A CloseFile 3440 A CreateFile	C:\WINDOW\$\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf	SUCCESS	Project Advance Providents and Advance Contractor Providence Contractor Contractor (Parket and Advanced Contractor)
9:25:23.37844 Malware_U3_W2_L2.exe 9:25:23.37849 Malware_U3_W2_L2.exe	3440 Createrile 3440 QueryInformationVolume	C.	SUCCESS	Desired Access: Read Attributes, Write Attributes, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert, Attributes: n/a, Share VolumeCreationTime: 3/20/2017 9:34:16 PM, VolumeSerialNumber: D8BA-9021, Supports/Dbiects: True, VolumeLabel:
9:25:23.37853 Malware_U3_W2_L2.exe	3440 FileSystemControl	C	SUCCESS	Control FSCTL FILE PREFETCH
9:25:23:37860 Malware_U3_W2_L2.exe	3440 CreateFile	C/	SUCCESS	Desired Access: Read Dalar List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup
9:26:23:37866 Mahuare 113 W/2 1.2 eve	3440 - QueryDirectory	C/	SUCCESS	0: 65e5bdf5ca391440390554e9ae7b, 1: AUTOEXEC.BAT, FileInformationClass: FileNamesInformation, 3: CONFIG.SYS, 4: Documents and
9:25:23.37881 Malware_U3_W2_L2.exe	3440 QueryDirectory	C:/	NO MORE FILES	
9:25:23:37897 Mahuare II3 W2 I 2 eve	3440 CloseFile	C:/	SUCCESS	
9:25:23.37912 Malware_U3_W2_L2.exe	3440 CreateFile	C:\DOCUMENTS AND SETTINGS	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup
9:25:23.37917 Malware_U3_W2_L2.exe 9:25:23.37929 Malware_U3_W2_L2.exe	3440 A QueryDirectory 3440 QueryDirectory	C:\Documents and Settings C:\Documents and Settings	SUCCESS NO MORE FILES	0: ., 1:, FileInformationClass: FileNamesInformation, 3: All Users, 4: Default User, 5: LocalService, 6: NetworkService
9:25:23.37937 Malware_U3_W2_L2.exe	3440 CloseFile	C:\Documents and Settings C:\Documents and Settings	SUCCESS	
	3440 CreateFile	C:\Documents and Settings\ADMINISTRATOR	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous ID Non-Alert, Open For Backup
9:25:23:37961 Malware_U3_W2_L2.exe	3440 QueryDirectory	C:\Documents and Settings\Administrator	SUCCESS	0:1: FileInformationClass: FileNamesInformation, 3: Cookies, 4: Desktop, 5: Favorites, 6: Local Settings, 7: My Documents, 8: NetHood,
9:25:23.37970 Malware U3 W2 L2.exe	3440 QueryDirectory	C:\Documents and Settings\Administrator	NO MORE EUES	
		C. Oocuments and Settings Watministrator	NO MORE FILES	
9:25:23.37978 Malware_U3_W2_L2.exe	3440 🗟 CloseFile	C:\Documents and Settings\Administrator	SUCCESS	
9:25:23.39978 Malware_U3_W2_L2.exe 9:25:23.39018 Malware_U3_W2_L2.exe	3440 CloseFile 3440 CreateFile	C:\Documents and Settings\Administrator C:\Documents and Settings\Administrator\Desktop	SUCCESS SUCCESS	Desired Access: Read Data/List Directory, Synchronice, Disposition, Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup
9:25:23.39978 Malware_U3_W2_L2.exe 9:25:23.39018 Malware_U3_W2_L2.exe	3440 A CloseFile 3440 D CreateFile 3440 QueryDirectory	C:\Documents and Settings\Administrator C\\Documents and Settings\Administrator\Oesktop C:\Documents and Settings\Administrator\Oesktop	SUCCESS SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup 0:., 1:, FileInformation/Class: FileNamesInformation, 3: CFF Explored Ink, 4: Command Prompt Ink, 5: Esercizio_Pratico_U3_W2_L1, 6: Esercizio_
9:25:23.37978 Malware_U3_W2_L2.exe 9:25:23.39018 Malware_U3_W2_L2.exe 9:25:23.38032 Malware_U3_W2_L2.exe 9:25:23.38051 Malware_U3_W2_L2.exe 9:25:23.38071 Malware_U3_W2_L2.exe	3440 CloseFile 3440 QueryDirectory 3440 QueryDirectory 3440 QueryDirectory	C\Documents and Settings\Administrator C\Documents and Settings\Administrator\Desktop C\Documents and Settings\Administrator\Desktop C\Documents and Settings\Administrator\Desktop	SUCCESS SUCCESS SUCCESS NO MORE FILES	
9:25:23.37978 Malware_U3_W2_L2.exe 9:25:23.39018 Malware_U3_W2_L2.exe 9:25:23.38032 Malware_U3_W2_L2.exe 9:25:23.38051 Malware_U3_W2_L2.exe 9:25:23.38071 Malware_U3_W2_L2.exe	3440 A CloseFile 3440 D CreateFile 3440 QueryDirectory	C:\Documents and Settings\Administrator C:\Documents and Settings\Administrator\Desktop	SUCCESS SUCCESS	0:, 1:, FileInformation/Class: FileNamesInformation, 3: CFF Explorer Ink, 4: Command Prompt Ink, 5: Esercizio_Pratico_U3_W2_L1, 6: Eserc
9.252.337978 Malware, U.3, W.2, L2 exe. 9.252.338018 Malware, U.3, W.2, L2 exe. 9.252.338032 Malware, U.3, W.2, L2 exe. 9.252.338051 Malware, U.3, W.2, L2 exe. 9.252.338151 Malware, U.3, W.2, L2 exe.	3440 CloseFile 3440 QueyOlirectory 3440 QueyOlirectory 3440 QueyOlirectory 3440 CloseFile 3440 QueyOlirectory 3440 QueyOlirectory	C:\Documents and Settings\Administrator \C:\Documents and Settings\Administrator\Desktop C:\Documents and Settings\Administrator\Desktop\ESERCIZID_PRATICO_U3_\W2_L2 C:\Documents and Settings\Administrator\Desktop\Esercizio_\Pratico_U3_\W2_L2	SUCCESS SUCCESS NO MORE FILES SUCCESS SUCCESS SUCCESS	
9.25.23.39798. Malware, U3, W2, L2 exe 9.25.23.380318. Malware, U3, W2, L2 exe 9.25.23.38051 Malware, U3, W2, L2 exe	3440 CloseFile 3440 CloseFile 3440 QueyOriectory	C:\Documents and Settings\Administrator\ C:\Documents and Settings\Administrator\Desktop C:\Documents and Settings\Administrator\Desktop C:\Documents and Settings\Administrator\Desktop C:\Documents and Settings\Administrator\Desktop C:\Documents and Settings\Administrator\Desktop\EscERCIZIO_PRATICO_U3_W2_L2 C:\Documents and Settings\Administrator\Desktop\EscERCIZIO_PRATICO_U3_W2_L2 C:\Documents and Settings\Administrator\Desktop\Esceicio_Pratico_U3_W2_L2 C:\Documents and Settings\Administrator\Desktop\Esceicio_Pratico_U3_W2_L2	SUCCESS SUCCESS SUCCESS NO MORE FILES SUCCESS SUCCESS SUCCESS NO MORE FILES	0:, 1:, FileInformationClass: FileNamesInformation, 3: CFF Explorer.Ink, 4: Command Prompt.Ink, 5: Esercizio_Pratico_U3_W2_L1, 6: Eserc Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup
9.252.3 39798 Malware, U.3. W.2, L.2 exe 9.252.3 38019 Malware, U.3. W.2, L.2 exe 9.252.3 38051 Malware, U.3, W.2, L.2 exe 9.252.3 38071 Malware, U.3, W.2, L.2 exe 9.252.3 38071 Malware, U.3, W.2, L.2 exe 9.252.3 38115 Malware, U.3, W.2, L.2 exe 9.252.3 38140 Malware, U.3, W.2, L.2 exe 9.252.3 38161 Malware, U.3, W.2, L.2 exe 9.252.3 38161 Malware, U.3, W.2, L.2 exe	3440 CloseFile 3440 Curesterile 3440 Query Directory	C:Documents and Settings:\Administrator\ C\Documents and Settings:\Administrator\Desktop C:Documents and Settings:\Administrator\Desktop C:Documents and Settings:\Administrator\Desktop C:Documents and Settings:\Administrator\Desktop C:Documents and Settings:\Administrator\Desktop\EseRCIZID_PRATICO_U3_W2_L2 C:Documents and Settings:\Administrator\Desktop\Esectiop.\Patrico_U3_W2_L2	SUCCESS SUCCESS SUCCESS NO MORE FILES SUCCESS SUCCESS SUCCESS SUCCESS NO MORE FILES SUCCESS	0:, 1:, FileInformationClass: FileNamesInformation, 3: CFF Explorer.Ink, 4: Command Prompt.Ink, 5: Esercizio_Pratico_U3_W2_L1, 6: Esercizio_Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronius IO Non-Alert, Open For Backup 0: 1:, FileInformationClass: FileNamesInformation, 3: practicalmativareanalysis.log
9.252.3 3978 Malware, U.3, W.2, L.2 exe 9.252.3 80018 Malware, U.3, W.2, L.2 exe 9.252.3 80051 Malware, U.3, W.2, L.2 exe 9.252.3 80071 Malware, U.3, W.2, L.2 exe 9.252.3 80071 Malware, U.3, W.2, L.2 exe 9.252.3 81015 Malware, U.3, W.2, L.2 exe 9.252.3 81140 Malware, U.3, W.2, L.2 exe 9.252.3 8140 Malware, U.3, W.2, L.2 exe 9.252.3 83140 Malware, U.3, W.2, L.2 exe 9.252.3 83140 Malware, U.3, W.2, L.2 exe 9.252.3 83140 Malware, U.3, W.2, L.2 exe	3440 CloseFile 3440 CloseFile 3440 QueyOriectory	C:\Documents and Settings:\Administrator\ C:\Documents and Settings:\Administrator\Desktop C:\Documents and Settings:\Administrator\Desktop\Setcizio_PRATICO_U3_W2_L2 C:\NDNDUMS	SUCCESS SUCCESS NO MORE FILES SUCCESS SUCCESS NO MORE FILES SUCCESS NO MORE FILES SUCCESS SUCCESS	0:, 1:, FileInformation/Class: FileNamesInformation, 3: CFF Explorer Ink, 4: Command Prompt Ink, 5: Esercizio_Pratico_U3_W2_L1, 6: Esercizio Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup 0:, 1:, FileInformation/Class: FileNamesInformation, 3: practicalmalwareanalysis.log Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup
9.252.3 39798 Mahvare, U.3, W.2, L.2 exe 9.252.3 80018 Mahvare, U.3, W.2, L.2 exe 9.252.3 80051 Mahvare, U.3, W.2, L.2 exe 9.252.3 80051 Mahvare, U.3, W.2, L.2 exe 9.252.3 80051 Mahvare, U.3, W.2, L.2 exe 9.252.3 8115 Mahvare, U.3, W.2, L.2 exe 9.252.3 81140 Mahvare, U.3, W.2, L.2 exe 9.252.3 81261 Mahvare, U.3, W.2, L.2 exe 9.252.3 82161 Mahvare, U.3, W.2, L.2 exe 9.252.3 82361 Mahvare, U.3, W.2, L.2 exe	3440 CloseFile 3440 QueyOriectory	C:\Documents and Settings\Administrator\ C\Documents and Settings\Administrator\Desktop\ C\Documents and Settings\Administrator\Desktop\Escencia\Desktop\ C\Documents and Settings\Administrator\Desktop\Escencia\Desktop\Esce	SUCCESS SUCCESS NO MORE FILES SUCCESS SUCCESS NO MORE FILES SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS	0:, 1:, FileInformationClass: FileNamesInformation, 3: CFF Explorer.Ink, 4: Command Prompt Ink, 5: Esercizio_Pratico_U3_W2_L1, 6: Esercizio_Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronius IO Non-Alert, Open For Backup 0: 1:, FileInformationClass: FileNamesInformation, 3: practicalmalwareanalysis.log
9.252.3 39798 Mahvare, U.3, W.2, L.2 exe 9.252.3 80018 Mahvare, U.3, W.2, L.2 exe 9.252.3 80051 Mahvare, U.3, W.2, L.2 exe 9.252.3 80051 Mahvare, U.3, W.2, L.2 exe 9.252.3 80051 Mahvare, U.3, W.2, L.2 exe 9.252.3 8115 Mahvare, U.3, W.2, L.2 exe 9.252.3 81140 Mahvare, U.3, W.2, L.2 exe 9.252.3 81261 Mahvare, U.3, W.2, L.2 exe 9.252.3 82161 Mahvare, U.3, W.2, L.2 exe 9.252.3 82361 Mahvare, U.3, W.2, L.2 exe	3440 CloseFile 3440 CloseFile 3440 QueyOriectory	C:\Documents and Settings\Administrator\ C:\Documents and Settings\Administrator\Desktop C:\Documents and Settings\Administrator\Desktop C:\Documents and Settings\Administrator\Desktop C:\Documents and Settings\Administrator\Desktop C:\Documents and Settings\Administrator\Desktop\EseRICIZID_PRATICO_U3_W2_L2 C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2 C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2 C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2 C:\Univoluments and Settings\Univoluments and Settings\Univoluments and Settings\Univoluments and Settings\Univoluments and Settings\Univoluments and Settings\Univoluments and Settings\U	SUCCESS SUCCESS NO MORE FILES SUCCESS SUCCESS SUCCESS NO MORE FILES SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS NO MORE FILES	0:, 1:, FileInformationClass: FileNamesInformation, 3: CFF Explorer Ink, 4: Command Prompt Ink, 5: Esercizio_Pratico_U3_W2_L1, 6: Esercizio_U3_W2_L1, 6
9.252.3 37978 Malware, U.3, W.2, Le exe 9.252.3 38032 Malware, U.3, W.2, Le exe 9.252.3 38051 Malware, U.3, W.2, Le exe 9.252.3 38051 Malware, U.3, W.2, Le exe 9.252.3 38051 Malware, U.3, W.2, Le exe 9.252.3 38115 Malware, U.3, W.2, Le exe 9.252.3 38140 Malware, U.3, W.2, Le exe 9.252.3 38216 Malware, U.3, W.2, Le exe 9.252.3 38216 Malware, U.3, W.2, Le exe 9.252.3 38216 Malware, U.3, W.2, Le exe 9.252.3 38238 Malware, U.3, W.2, Le exe	3440 CloseFile 3440 QueyOriectory	C:\Documents and Settings\Administrator\ C\Documents and Settings\Administrator\Desktop\ C\Documents and Settings\Administrator\Desktop\Escencia\Desktop\ C\Documents and Settings\Administrator\Desktop\Escencia\Desktop\Esce	SUCCESS SUCCESS NO MORE FILES SUCCESS SUCCESS NO MORE FILES SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS	O:, 1:, FileInformationClass: FileNamesInformation, 3. CFF Explorer. Ink, 4: Command Prompt. Ink, 5: Esercizio_Pratico_U3_W2_L1, 6: Esercizio_U3_W2_L1
9.252.3 39798. Mahvare, U.3, W.2, L.2 exe 9.252.3 38032. Mahvare, U.3, W.2, L.2 exe 9.252.3 38032. Mahvare, U.3, W.2, L.2 exe 9.252.3 38051. Mahvare, U.3, W.2, L.2 exe 9.252.3 38051. Mahvare, U.3, W.2, L.2 exe 9.252.3 38140. Mahvare, U.3, W.2, L.2 exe 9.252.3 38140. Mahvare, U.3, W.2, L.2 exe 9.252.3 38216. Mahvare, U.3, W.2, L.2 exe 9.252.3 38236. Mahvare, U.3, W.2, L.2 exe 9.252.3 38336.	3440 CloseFile 3440 CloseFile 3440 QueyOriectory	C:\Documents and Settings\Administrator\ C:\Documents and Settings\Administrator\Desktop C:\Documents and Settings\Administrator\Desktop C:\Documents and Settings\Administrator\Desktop C:\Documents and Settings\Administrator\Desktop C:\Documents and Settings\Administrator\Desktop\Esercizio_PRATICO_U3_W2_L2 C:\United C:\Unite	SUCCESS SUCCESS NO MORE FILES SUCCESS SUCCESS NO MORE FILES SUCCESS	0:, 1:, FileInformation/Class: FileNamesInformation, 3: CFF Explorer Ink, 4: Command Prompt Ink, 5: Esercizio_Pratico_U3_W2_L1, 6: Esercizio Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup 0:, 1:, FileInformation/Class: FileNamesInformation, 3: practicalmalwareanalysis.log Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup
9.252.3 39798 Malware, U.3. W.2, L.2 exe 9.252.3 38051 Malware, U.3. W.2, L.2 exe 9.252.3 38051 Malware, U.3. W.2, L.2 exe 9.252.3 38071 Malware, U.3. W.2, L.2 exe 9.252.3 38071 Malware, U.3. W.2, L.2 exe 9.252.3 38151 Malware, U.3. W.2, L.2 exe 9.252.3 38161 Malware, U.3. W.2, L.2 exe 9.252.3 38161 Malware, U.3. W.2, L.2 exe 9.252.3 38264 Malware, U.3. W.2, L.2 exe 9.252.3 38263 Malware, U.3. W.2, L.2 exe 9.252.3 38361 Malware, U.3. W.2, L.2 exe 9.252.3 38341 Malware, U.3. W.2, L.2 exe 9.252.3 38341 Malware, U.3. W.2, L.2 exe 9.252.3 38341 Malware, U.3. W.2, L.2 exe 9.252.3 383431 Malware, U.3. W.2, L.2 exe 9.252.3 383431 Malware, U.3. W.2, L.2 exe 9.252.3 383431 Malware, U.3. W.2, L.2 exe 9.252.3 383341 Malware, U.3. W.2, L.2 exe 9.252.3 3833341 Malware, U.3. W.2, L.2 exe 9.252 Malware, U.3. W.2, L.	3440 CloseFile 3440 CloseFile 3440 QueyOriectory	C:\Documents and Settings\Administrator\ C\Documents and Settings\Administrator\Desktop C\Documents and Settings\Administrator\Desktop C:\Documents and Settings\Administrator\Desktop C:\Documents and Settings\Administrator\Desktop C:\Documents and Settings\Administrator\Desktop\EscERCIZIO_PRATICO_U3_W2_L2 C:\Documents and Settings\Administrator\Desktop\Esceizio_Pratico_U3_W2_L2 C:\Documents and Settings\Administrator\Desktop\Esceizio_Pratico_U3_W2_L2 C:\Documents and Settings\Administrator\Desktop\Esceizio_Pratico_U3_W2_L2 C:\Documents and Settings\Administrator\Desktop\Esceizio_Pratico_U3_W2_L2 C:\University C	SUCCESS SUCCESS NO MORE FILES SUCCESS SUCCESS NO MORE FILES SUCCESS	O:, 1:, FileInformation/Class: FileNamesInformation, 3: CFF Explorer Ink, 4: Command Prompt Ink, 5: Esercizio_Pratico_U3_W2_L1, 6: Esercizio Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous ID Non-Alert, Open For Backup O:, 1:, FileInformation/Class: FileNamesInformation, 3: practicalmativareanalysis: log Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous ID Non-Alert, Open For Backup O:, 1:, FileInformation/Class: FileNamesInformation, 3: 0.log, 4: addins, 5: AppPatch, 6: assembly, 7: Blue Lace 16 bmp, 8: bootstat dat, 9: c Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous ID Non-Alert, Open For Backup
9.252.3 39798 Malware, U.3, W.2, Le exe 9.252.3 80018 Malware, U.3, W.2, Le exe 9.252.3 80018 Malware, U.3, W.2, Le exe 9.252.3 80051 Malware, U.3, W.2, Le exe 9.252.3 80051 Malware, U.3, W.2, Le exe 9.252.3 80151 Malware, U.3, W.2, Le exe 9.252.3 80151 Malware, U.3, W.2, Le exe 9.252.3 80161 Malware, U.3, W.2, Le exe 9.252.3 80264 Malware, U.3, W.2, Le exe 9.252.3 80264 Malware, U.3, W.2, Le exe 9.252.3 80264 Malware, U.3, W.2, Le exe 9.252.3 80364 Malware, U.3, W.2, Le exe 9.252.3 80341 Malware, U.3, W.2, Le exe 9.252.3 803411 Malware, U.3, W.2, Le exe	3440 CloseFile 3440 CloseFile 3440 QueyOriectory	C:\Documents and Settings\Administrator\Col\Delta\top\Col\	SUCCESS SUCCESS NO MORE FILES SUCCESS SUCCESS NO MORE FILES SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS NO MORE FILES SUCCESS NO MORE FILES SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS	O:, 1:, FileInformationClass: FileNamesInformation, 3: CFF Explorer Ink, 4: Command Prompt Ink, 5: Esercizio_Pratico_U3_W2_L1, 6: Esercizio Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup O:, 1:, FileInformationClass: FileNamesInformation, 3: practicalmalwareanalysis.log Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup O:, 1:, FileInformationClass: FileNamesInformation, 3: O.log, 4: addins, 5: AppPatch, 6: assembly, 7: Blue Lace 16:bmp, 8: bootstat.dat, 9: Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup O:, 1:, FileInformationClass: FileNamesInformation, 3: AcGenral dll, 4: AcLayers dll, 5: AcLua dll, 6: AcSpecto. dll, 7: Ac/dmal. dll, 8: apphelp
9.252.3 39798 Malware, U.3, W.2, L.2 exe 9.252.3 38051 Malware, U.3, W.2, L.2 exe 9.252.3 38051 Malware, U.3, W.2, L.2 exe 9.252.3 38071 Malware, U.3, W.2, L.2 exe 9.252.3 38071 Malware, U.3, W.2, L.2 exe 9.252.3 38115 Malware, U.3, W.2, L.2 exe 9.252.3 38161 Malware, U.3, W.2, L.2 exe 9.252.3 38161 Malware, U.3, W.2, L.2 exe 9.252.3 38264 Malware, U.3, W.2, L.2 exe 9.252.3 38264 Malware, U.3, W.2, L.2 exe 9.252.3 38381 Malware, U.3, W.2, L.2 exe 9.252.3 3841 Malware, U.3, W.2, L.2 exe 9.252.3 3844 Malware, U.3, W.2, L.2 exe 9.252 Malware, U.3, W.2, L.2 exe 9.252.3 3844 Malware, U.3, W.2, L.2 exe 9.252.3 384	3440 CloseFile 3440 CloseFile 3440 QueyOriectory	C:\Documents and Settings\Administrator\ C:\Documents and Settings\Administrator\Desktop C:\Documents and Settings\Administrator\Desktop C:\Documents and Settings\Administrator\Desktop C:\Documents and Settings\Administrator\Desktop\Desktop C:\Documents and Settings\Administrator\Desktop\Deskt	SUCCESS SUCCESS NO MORE FILES SUCCESS SUCCESS SUCCESS NO MORE FILES SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS NO MORE FILES SUCCESS	O:, 1:, FileInformationClass: FileNamesInformation, 3: CFF Explorer Ink, 4: Command Prompt Ink, 5: Esercizio_Pratico_U3_W2_L1, 6: Esercizio Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup O:, 1:, FileInformationClass: FileNamesInformation, 3: practicalmalwareanalysis.log Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup O:, 1:, FileInformationClass: FileNamesInformation, 3: 0.log, 4: addins, 5: AppPatch, 6: assembly, 7: Blue Lace 16: bmp, 8: bootstat.dat, 9: c Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup O:, 1:, FileInformationClass: FileNamesInformation, 3: AcGenral dll, 4: AcLayers dll, 5: AcLua dll, 6: AcSpectc. dll, 7: Ac/Otmal.dll, 8: apphelp: Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup
9.252.3 39798 Malware, U.3, W.2, L.2 exe 9.252.3 38032 Malware, U.3, W.2, L.2 exe 9.252.3 38032 Malware, U.3, W.2, L.2 exe 9.252.3 38031 Malware, U.3, W.2, L.2 exe 9.252.3 38031 Malware, U.3, W.2, L.2 exe 9.252.3 38115 Malware, U.3, W.2, L.2 exe 9.252.3 38161 Malware, U.3, W.2, L.2 exe 9.252.3 38216 Malware, U.3, W.2, L.2 exe 9.252.3 38216 Malware, U.3, W.2, L.2 exe 9.252.3 38238 Malware, U.3, W.2, L.2 exe 9.252.3 38238 Malware, U.3, W.2, L.2 exe 9.252.3 38238 Malware, U.3, W.2, L.2 exe 9.252.3 38231 Malware, U.3, W.2, L.2 exe 9.252.3 38231 Malware, U.3, W.2, L.2 exe 9.252.3 38240 Malware, U.3, W.2, L.2 exe 9.252.3 38440 Malwa	3440 CloseFile 3440 CloseFile 3440 QueyOriectory	C:\Documents and Settings\Administrator\Desktop C:\Documents and Settings\Administrator\Desktop C:\Documents and Settings\Administrator\Desktop C:\Documents and Settings\Administrator\Desktop C:\Documents and Settings\Administrator\Desktop\Deskto	SUCCESS SUCCESS NO MORE FILES SUCCESS SUCCESS NO MORE FILES SUCCESS	O:, 1:, FileInformationClass: FileNamesInformation, 3: CFF Explorer Ink, 4: Command Prompt Ink, 5: Esercizio_Pratico_U3_W2_L1, 6: Esercizio_Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup O, 1:, FileInformationClass: FileNamesInformation, 3: practicalmalwareanalysis.log Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup O, 1:, FileInformationClass: FileNamesInformation, 3: O.log, 4: addins, 5: AppPatch, 6: assembly, 7: Blue Lace 16: bmp, 8: bootstat.dat, 9: c Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup O, 1:, FileInformationClass: FileNamesInformation, 3: AcGenral dtl, 4: AcLayers.dtl, 5: AcLua dtl, 6: AcSpectc.dtl, 7: Ac9tmal.dtl, 8: apphelp: Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup O, 1:, FileInformationClass: FileNamesInformation, 3: -1, 4: 1025, 5: 1028, 6: 1031, 7: 1033, 8: 1037, 9: 1041, 10: 1042, 11: 1054, 12: 125
9.252.3 39798 Malware, U.3, W.2, L.2 exe 9.252.3 38051 Malware, U.3, W.2, L.2 exe 9.252.3 38051 Malware, U.3, W.2, L.2 exe 9.252.3 38071 Malware, U.3, W.2, L.2 exe 9.252.3 38071 Malware, U.3, W.2, L.2 exe 9.252.3 38151 Malware, U.3, W.2, L.2 exe 9.252.3 38161 Malware, U.3, W.2, L.2 exe 9.252.3 38161 Malware, U.3, W.2, L.2 exe 9.252.3 38264 Malware, U.3, W.2, L.2 exe 9.252.3 38264 Malware, U.3, W.2, L.2 exe 9.252.3 38264 Malware, U.3, W.2, L.2 exe 9.252.3 38261 Malware, U.3, W.2, L.2 exe 9.252.3 38341 Malware, U.3, W.2, L.2 exe 9.252.3 38440 Malware, U.3, W.2, L.2 exe 9.252.3 38453 Malware, U.3, W.2, L.2 exe 9.252 Malware, U.3, W.2	3440 CloseFile	C:\Documents and Settings\Administrator\Cos\top\C\Documents and Settings\Administrator\Oes\top\C\Documents and Settings\Administrator\Oes\top\C\Documents and Settings\Administrator\Oes\top\C\Documents and Settings\Administrator\Oes\top\C\Documents\Oes\top\C\Documents and Settings\Administrator\Oes\top\C\Documents\Oes\top\C\D	SUCCESS SUCCESS NO MORE FILES SUCCESS NO MORE FILES SUCCESS	O:, 1:, FileInformationClass: FileNamesInformation, 3: CFF Explorer Ink, 4: Command Prompt Ink, 5: Esercizio_Pratico_U3_W2_L1, 6: Esercizio_Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup O, 1:, FileInformationClass: FileNamesInformation, 3: practicalmalwareanalysis.log Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup O, 1:, FileInformationClass: FileNamesInformation, 3: 0. log, 4: addins, 5: AppPatch, 6: assembly, 7: Blue Lace 16: bmp, 8: bootstat dat, 9: c Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup O, 1:, FileInformationClass: FileNamesInformation, 3: AcGenral dll, 4: AcLayers dll, 5: AcLua dll, 6: AcSpecic, dll, 7: AcVornal dll, 8: apphelp Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup O, 1:, FileInformationClass: FileNamesInformation, 3: -1, 4: 1025, 5: 1028, 6: 1031, 7: 1033, 8: 1037, 9: 1041, 10: 1042, 11: 1054, 12: 125 0: epsyred, dl. 1: edit.com, FileInformationClass: FileNamesInformation, 3: -1, 4: 1025, 5: 1028, 6: 1031, 7: 1033, 8: 1037, 9: 1041, 10: 1042, 11: 1054, 12: 125
9.522.3 9018. Mahvare, U.3, W.2, Le exe 9.522.3 80018. Mahvare, U.3, W.2, Le exe 9.523.3 80018. Mahvare, U.3, W.2, Le exe 9.522.3 80051. Mahvare, U.3, W.2, Le exe 9.522.3 80051. Mahvare, U.3, W.2, Le exe 9.522.3 80151. Mahvare, U.3, W.2, Le exe 9.522.3 80150. Mahvare, U.3, W.2, Le exe 9.522.3 80150. Mahvare, U.3, W.2, Le exe 9.522.3 80150. Mahvare, U.3, W.2, Le exe 9.522.3 80251. Mahvare, U.3, W.2, Le exe 9.522.3 80252. Mahvare, U.3, W.2, Le e	3440 CloseFile 3440 CloseFile 3440 QueyOirectory	C:\Documents and Settings\Administrator\Cesttop C:\Documents and Settings\Administrator\Desttop C:\Documents and Settings\Administrator\Desttop C:\Documents and Settings\Administrator\Desttop C:\Documents and Settings\Administrator\Desttop C:\Documents and Settings\Administrator\Desttop\Esercizo_PRATICO_U3_W2_L2 C:\UninDOWS C:\UninDOWS C:\UninDOWS C:\UninDOWS C:\UninDOWS C:\UninDOWS C:\UninDOWS\DepPatch C:\UninDOWS\DepPatch C:\UninDOWS\DepPatch C:\UninDOWS\DepPatch C:\UninDOWS\DepPatch C:\UninDOWS\DepPatch C:\UninDOWS\SuppPatch C:\UninnOWS\SuppPatch C:\UninnOWS\SuppPatch C:\UninnOWS\SuppPatch C:\UninnOWS\SuppPatch C:\UninnOWS\SuppPatch C:\Uni	SUCCESS SUCCESS NO MORE FILES SUCCESS SUCCESS SUCCESS NO MORE FILES SUCCESS SUCCESS NO MORE FILES SUCCESS	O:, 1:, FileInformationClass: FileNamesInformation, 3: CFF Explorer Ink, 4: Command Prompt Ink, 5: Esercizio_Pratico_U3_W2_L1, 6: Esercizio Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup O:, 1:, FileInformationClass: FileNamesInformation, 3: practicalmalwareanalysis. log Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup O:, 1:, FileInformationClass: FileNamesInformation, 3: 0.log, 4: addins, 5: AppPatch, 6: assembly, 7: Blue Lace 16: bmp, 8: bootstat.dat, 9: c Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup O:, 1:, FileInformationClass: FileNamesInformation, 3: AcGenral dll, 4: AcLayers dll, 5: AcLua dll, 6: AcSpectc.dll, 7: AcGranal dll, 8: apphelp Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup O:, 1:, FileInformationClass: FileNamesInformation, 3: -1, 4: 1025, 5: 1028, 6: 1031, 7: 1033, 8: 1037, 9: 1041, 10: 1042, 11: 1054, 12: 125 O: espayor, dll, 1: edit.com, FileInformationClass: FileNamesInformation, 3: editin exe, 4: etadu.dll, 5: ega.cpi, 6: eta.dl. 7: emptypegdo.ddl, 8: eg
9.522.3 9018. Mahvare, U.3, W.2, Le exe 9.522.3 80018. Mahvare, U.3, W.2, Le exe 9.523.3 80018. Mahvare, U.3, W.2, Le exe 9.522.3 80051. Mahvare, U.3, W.2, Le exe 9.522.3 80051. Mahvare, U.3, W.2, Le exe 9.522.3 80151. Mahvare, U.3, W.2, Le exe 9.522.3 80150. Mahvare, U.3, W.2, Le exe 9.522.3 80150. Mahvare, U.3, W.2, Le exe 9.522.3 80150. Mahvare, U.3, W.2, Le exe 9.522.3 80251. Mahvare, U.3, W.2, Le exe 9.522.3 80252. Mahvare, U.3, W.2, Le e	3440 CloseFile	C:\Documents and Settings\Administrator\Cos\top\C\Documents and Settings\Administrator\Oes\top\C\Documents and Settings\Administrator\Oes\top\C\Documents and Settings\Administrator\Oes\top\C\Documents and Settings\Administrator\Oes\top\C\Documents\Oes\top\C\Documents and Settings\Administrator\Oes\top\C\Documents\Oes\top\C\D	SUCCESS SUCCESS NO MORE FILES SUCCESS NO MORE FILES SUCCESS	O:, 1:, FileInformationClass: FileNamesInformation, 3: CFF Explorer Ink, 4: Command Prompt Ink, 5: Esercizio_Pratico_U3_W2_L1, 6: Esercizio Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup O:, 1:, FileInformationClass: FileNamesInformation, 3: practicalinalwareanalysis.log Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup O:, 1:, FileInformationClass: FileNamesInformation, 3: 0 log, 4: addins, 5: AppPatch, 6: assembly, 7: Blue Lace 16: bmp, 8: bootstat dat, 9: c Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup O:, 1:, FileInformationClass: FileNamesInformation, 3: AcGenral dll, 4: AcLayers dll, 5: AcLua dll, 6: AcSpect. dll, 7: Ac/Qtmal.dll, 8: apphelp Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup O:, 1:, FileInformationClass: FileNamesInformation, 3: -1, 4: 1025, 5: 1028, 6: 1031, 7: 1033, 8: 1037, 9: 1041, 10: 1042, 11: 1054, 12: 125 O: epsyved. dl. 1: ed.t.com, FileInformationClass: FileNamesInformation, 3: -1, 4: 1025, 6: 1028, 6: 1031, 7: 1033, 8: 1031, 7: 1034, 10: 1044, 10: 104, 10: 104
9.252.3 39798 Malware, U.3, W.2, Le exe 9.252.3 80032 Malware, U.3, W.2, Le exe 9.252.3 80032 Malware, U.3, W.2, Le exe 9.252.3 80031 Malware, U.3, W.2, Le exe 9.252.3 80031 Malware, U.3, W.2, Le exe 9.252.3 80151 Malware, U.3, W.2, Le exe 9.252.3 80151 Malware, U.3, W.2, Le exe 9.252.3 80151 Malware, U.3, W.2, Le exe 9.252.3 80251 Malware, U.3, W.2, Le exe 9.252.3 80254 Malware, U.3, W.2, Le exe 9.252.3 80254 Malware, U.3, W.2, Le exe 9.252.3 80254 Malware, U.3, W.2, Le exe 9.252.3 803541 Malware, U.3, W.2, Le exe 9.252.3 80351 Malware, U.3, W.2, Le exe 9.252.3 80551 Malware, U.3, W.2, Le exe 9.252.3 80550 Malware	3440 CloseFile	C:\Documents and Settings\Administrator\Collaboruments and Settings\Administrator\Cesttop C:\Documents and Settings\Administrator\Desttop C:\Documents and Settings\Administrator\Desttop C:\Documents and Settings\Administrator\Desttop C:\Documents and Settings\Administrator\Desttop\Cest	SUCCESS SUCCESS NO MORE FILES SUCCESS SUCCESS NO MORE FILES SUCCESS	O:, 1:, FileInformationClass: FileNamesInformation, 3: CFF Explorer Ink, 4: Command Prompt Ink, 5: Esercizio_Pratico_U3_W2_L1, 6: Esercizio_Pratico_U3
9.252.3 39798 Malware, U3, W2, L2 exe 9.252.3 39051 Malware, U3, W2, L2 exe 9.252.3 39051 Malware, U3, W2, L2 exe 9.252.3 39071 Malware, U3, W2, L2 exe 9.252.3 39071 Malware, U3, W2, L2 exe 9.252.3 39151 Malware, U3, W2, L2 exe 9.252.3 39140 Malware, U3, W2, L2 exe 9.252.3 39161 Malware, U3, W2, L2 exe 9.252.3 39264 Malware, U3, W2, L2 exe 9.252.3 39361 Malware, U3, W2, L2 exe 9.252.3 39361 Malware, U3, W2, L2 exe 9.252.3 39361 Malware, U3, W2, L2 exe 9.252.3 39450 Malware, U3, W2, L2 exe 9.252.3 39450 Malware, U3, W2, L2 exe 9.252.3 39553 Malware, U3, W2, L2 exe 9.252.3 39553 Malware, U3, W2, L2 exe 9.252.3 39555 Malware, U3, W2, L2 exe 9.252.3 39555 Malware, U3, W2, L2 exe 9.252.3 39558 Malware, U3, W2, L2 exe 9.252.3 39559 Malware, U3, W2, L2 exe 9.252.3 39559 Malware, U3, W2, L2	3440 CloseFile	C. Opocuments and Settings (Administrator C. Opocuments and Settings (Administrator Operation) C. Opocuments and Settings (Administrator O	SUCCESS SUCCESS NO MORE FILES SUCCESS	O:, 1:, FileInformationClass: FileNamesInformation, 3: CFF Explorer Ink, 4: Command Prompt Ink, 5: Esercizio_Pratico_U3_W2_L1, 6: Esercizio Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup O:, 1:, FileInformationClass: FileNamesInformation, 3: practicalinalwareanalysis.log Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup O:, 1:, FileInformationClass: FileNamesInformation, 3: 0.log, 4: addins, 5: AppPatch, 6: assembly, 7: Blue Lace 16: bmp, 8: bootstat dat, 9: c Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup O:, 1:, FileInformationClass: FileNamesInformation, 3: AcGenral dll, 4: AcLayers dll, 5: AcLua dll, 6: AcSpecit. dll, 7: AcVinnal dll, 8: apphelp Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup O:, 1:, FileInformationClass: FileNamesInformation, 3: 1, 4: 1025, 5: 1028, 6: 1031, 7: 1033, 8: 1037, 9: 1041, 10; 1.042, 11: 1044, 11: 1054, 12: 125 O: approxed, 11: edit.com, FileNamesInformation, 3: nouse dry, 4: mp43dmod dll, 5: mp43dmod dll, 6: mpegddata ax, 0; programar exe, 1: PROIND dll, FileInformationClass: FileNamesInformation, 3: mouse dry, 4: mp43dmod dll, 5: mp43dmod dll, 6: mpegddata ax, 0; programar exe, 1: PROIND dll, FileInformationClass: FileNamesInformation, 3: vmhpfs.dll, 4: VMUpgradeAtShutdownWAP.dll, 5: vmwogl32.dll, 6: vmw
9.252.3 39798 Malware, U.3, W.2, L.2 exe 9.252.3 38032 Malware, U.3, W.2, L.2 exe 9.252.3 38032 Malware, U.3, W.2, L.2 exe 9.252.3 38031 Malware, U.3, W.2, L.2 exe 9.252.3 38151 Malware, U.3, W.2, L.2 exe 9.252.3 38151 Malware, U.3, W.2, L.2 exe 9.252.3 38161 Malware, U.3, W.2, L.2 exe 9.252.3 38216 Malware, U.3, W.2, L.2 exe 9.252.3 38238 Malware, U.3, W.2, L.2 exe 9.252.3 38231 Malware, U.3, W.2, L.2 exe 9.252.3 38341 Malware, U.3, W.2, L.2 exe 9.252.3 38341 Malware, U.3, W.2, L.2 exe 9.252.3 3840 Malware, U.3, W.2, L.2 exe 9.252.3 3840 Malware, U.3, W.2, L.2 exe 9.252.3 38502 Malware, U.3, W.2, L.2 exe 9.252.3 38503 Malware, U.3, W.2, L.2 exe 9.252.3 38551 Malware, U.3, W.2, L.2 exe 9.252.3 38571 Malware, U.3, W.2, L.2 exe 9.252.3 38573 Malware, U.3, W.2, L.2 exe 9.252.3 3873 Malware, U.3	3440 CloseFile 3440 CloseFile 3440 QueyOriectory	C:\Documents and Settings\Administrator\Desktop C:\Documents and Settings\Administrator\Desktop C:\Documents and Settings\Administrator\Desktop C:\Documents and Settings\Administrator\Desktop C:\Documents and Settings\Administrator\Desktop\Deskto	SUCCESS SUCCESS NO MORE FILES SUCCESS SUCCESS NO MORE FILES SUCCESS	O:., 1:, FileInformationClass: FileNamesInformation, 3: CFF Explorer Ink, 4: Command Prompt Ink, 5: Esercizio_Pratico_U3_W2_L1, 6: Esercizio_Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup O, 1:, FileInformationClass: FileNamesInformation, 3: practicalmalwareanalysis.log Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup O, 1:, FileInformationClass: FileNamesInformation, 3: Olog, 4: addins, 5: AppPatch, 8: assembly, 7: Blue Lace 16: bmp, 8: bootstat.dat, 9: c Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup O, 1:, FileInformationClass: FileNamesInformation, 3: AcGenral dlt, 4: AcLayers dlt, 5: AcLua dlt, 6: AcSpectc.dlt, 7: AcOtmat dlt, 8: apphelp: Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup O, 1:, FileInformationClass: FileNamesInformation, 3: -1, 4: 1025, 5: 1028, 6: 1031, 7: 1033, 8: 1037, 9: 1041, 10: 1042, 11: 1054, 12: 125; 0: espayor.dll, 1: edit.com, FileInformationClass: FileNamesInformation, 3: edit.exe, 4: efsadu.dll, 5: eac.pc; 6: et. dl., 7: emptypegbb.ds, 8: et. 0. more com, 1: moriconal FileInformationClass: FileNamesInformation, 3: more dev. 4: impadend.dll, 5: mayediand.dll, 6: propheropol.dll, 6: propaga.dll, 6: propaga.dll, 7: 0. vjoy.dll, 1: vmGuestl.b.dll, FileInformationClass: FileNamesInformation, 3: -1, 10: 10: 4. VMUpgradeAlShutdowntv/Pr.dll, 5: vmwogi32.dll, 6: Desired Access: Read Data/List Directory, Read Altitibutes, Disposition: Open, Options: Non-Directory File, Altibutes: N., ShareMode: Read.
9.252.3 39798 Malware, U.3, W.2, L.2 exe 9.252.3 38051 Malware, U.3, W.2, L.2 exe 9.252.3 38051 Malware, U.3, W.2, L.2 exe 9.252.3 38071 Malware, U.3, W.2, L.2 exe 9.252.3 38071 Malware, U.3, W.2, L.2 exe 9.252.3 38151 Malware, U.3, W.2, L.2 exe 9.252.3 38161 Malware, U.3, W.2, L.2 exe 9.252.3 38161 Malware, U.3, W.2, L.2 exe 9.252.3 38161 Malware, U.3, W.2, L.2 exe 9.252.3 38264 Malware, U.3, W.2, L.2 exe 9.252.3 38264 Malware, U.3, W.2, L.2 exe 9.252.3 38361 Malware, U.3, W.2, L.2 exe 9.252.3 38361 Malware, U.3, W.2, L.2 exe 9.252.3 38341 Malware, U.3, W.2, L.2 exe 9.252.3 38531 Malware, U.3, W.2, L.2 exe 9.252.3 38531 Malware, U.3, W.2, L.2 exe 9.252.3 38551 Malware, U.3, W.2, L.2 exe 9.252.3 38553 Malwa	3440 CloseFile	C. Opcourrents and Settings (Administrator Collocuterity and Settings (Administrator Operation) C. Opcourrents and Settings (Administrator Operation) C. Opc	SUCCESS SUCCESS NO MORE FILES SUCCESS NO MORE FILES SUCCESS	O:, 1:, FileInformationClass: FileNamesInformation, 3: CFF Explorer Ink, 4: Command Prompt Ink, 5: Esercizio_Pratico_U3_W2_L1, 6: Esercizio_Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup O:, 1:, FileInformationClass: FileNamesInformation, 3: practicalmalwareanalysis.log Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup O:, 1:, FileInformationClass: FileNamesInformation, 3: 0.log, 4: addins, 5: AppPatch, 6: assembly, 7: Blue Lace 16 bmp, 8: bootstat.dat, 9: c Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup O:, 1:, FileInformationClass: FileNamesInformation, 3: AcGenral dt, 4: AcLayers dt, 5: AcLua dt, 6: AcSpectc.dt, 7: AcAtmal dt, 8: apphete Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup O:, 1:, FileInformationClass: FileNamesInformation, 3: -1, 4: 1025, 5: 1028, 6: 1031, 7: 1033, 8: 1037, 9: 1041, 10: 1042, 11: 1054, 12: 125 O: epspre.dt, 1: edit.com, FileInformationClass: FileNamesInformation, 3: addin exe, 4: efsadu dt, 5: egs.cp; 6: et. dt, 7: emptyregot.dst, 8: et. 0: more.com, 1: moricons.dt, FileInformationClass: FileNamesInformation, 3: mouse dtv, 4: mp43dmod dt, 5: mp43dmod dt, 6: mpeg2data ax, 0: prognams exe, 1: FRONIDib dt, FileInformationClass: FileNamesInformation, 3: vmhgfs.dt, 4: VMUpgradeAtShutdownWcP dt, 5: vmwogl32.dt, 6 Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read. Sync1 yee Csync1 yee Csy
9.252.3 39032. Malware, U.3, W.2, Le exe 9.252.3 38032. Malware, U.3, W.2, Le exe 9.252.3 38032. Malware, U.3, W.2, Le exe 9.252.3 38031. Malware, U.3, W.2, Le exe 9.252.3 38031. Malware, U.3, W.2, Le exe 9.252.3 38140. Malware, U.3, W.2, Le exe 9.252.3 38141. Malware, U.3, W.2, Le exe 9.252.3 38141. Malware, U.3, W.2, Le exe 9.252.3 38216. Malware, U.3, W.2, Le exe 9.252.3 38236. Malware, U.3, W.2, Le exe 9.252.3 38236. Malware, U.3, W.2, Le exe 9.252.3 38231. Malware, U.3, W.2, Le exe 9.252.3 38231. Malware, U.3, W.2, Le exe 9.252.3 38341. Malware, U.3, W.2, Le exe 9.252.3 38410. Malware, U.3, W.2, Le exe 9.252.3 38535. Malware, U.3, W.2, Le exe 9.252.3 38551. Malware, U.3, W.2, Le exe 9.252.3 385571. Malware, U.3, W.2, Le exe 9.252.3 385737. Malware, U.3, W.2, Le exe 9.252.3 38579. Malware, U.3,	3440 S. CloseFile 3440 LicesErife 3440 QueyOriectory	C:\Documents and Settings\Administrator\Desktop C:\Documents and Settings\Administrator\Desktop\Deskto	SUCCESS SUCCESS NO MORE FILES SUCCESS SUCCESS SUCCESS NO MORE FILES SUCCESS	O:., 1:, FileInformationClass: FileNamesInformation, 3: CFF Explorer Ink, 4: Command Prompt Ink, 5: Esercizio_Pratico_U3_W2_L1, 6: Esercizio_Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup O, 1:, FileInformationClass: FileNamesInformation, 3: practicalmalwareanalysis. log Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup O, 1:, FileInformationClass: FileNamesInformation, 3: 0.log, 4: addins, 5: AppPatch, 6: assembly, 7: Blue Lace 16 bmp, 8: bootstat dat, 9: c Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup O, 1:, FileInformationClass: FileNamesInformation, 3: AcGenral dll, 4: AcLayers dll, 5: AcLua dll, 6: AcSpectc dll, 7: AcOstnal dll, 8: apphelp Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup O, 1:, FileInformationClass: FileNamesInformation, 3: -1, 4: 1025, 5: 1028, 6: 1031, 7: 1033, 8: 1037, 9: 1041, 10: 1042, 11: 1054, 12: 125; 0: espayor, dll, 1: edit.com, FileInformationClass: FileNamesInformation, 3: editin exe, 4: etadu dll, 5: ega cpi, 6: et. dl. 7: emptyeegdo dat, 8: et Omero, on, 1: encoronal III. FileInformationClass: FileNamesInformation, 3: mbgls, dll, 4: VMUpgradeAtShutdownWvP dll, 5: vmwogl32 dll, 6: pubsase dll, 7: 0: vigo; dll, 1: vmGuestLib dll, FileInformationClass: FileNamesInformation, 3: mbgls, dll, 4: VMUpgradeAtShutdownWvP dll, 5: vmwogl32 dll, 6: Alexandra SyncType: SyncTy
9.252.3 39798 Malware, U.3, W.2, L.2 exe 9.252.3 38051 Malware, U.3, W.2, L.2 exe 9.252.3 38051 Malware, U.3, W.2, L.2 exe 9.252.3 38071 Malware, U.3, W.2, L.2 exe 9.252.3 38071 Malware, U.3, W.2, L.2 exe 9.252.3 38151 Malware, U.3, W.2, L.2 exe 9.252.3 38161 Malware, U.3, W.2, L.2 exe 9.252.3 38161 Malware, U.3, W.2, L.2 exe 9.252.3 38161 Malware, U.3, W.2, L.2 exe 9.252.3 38264 Malware, U.3, W.2, L.2 exe 9.252.3 38264 Malware, U.3, W.2, L.2 exe 9.252.3 38361 Malware, U.3, W.2, L.2 exe 9.252.3 38361 Malware, U.3, W.2, L.2 exe 9.252.3 38341 Malware, U.3, W.2, L.2 exe 9.252.3 38531 Malware, U.3, W.2, L.2 exe 9.252.3 38531 Malware, U.3, W.2, L.2 exe 9.252.3 38551 Malware, U.3, W.2, L.2 exe 9.252.3 38553 Malwa	3440 CloseFile	C. Opcourrents and Settings (Administrator Collocuterity and Settings (Administrator Operation) C. Opcourrents and Settings (Administrator Operation) C. Opc	SUCCESS SUCCESS NO MORE FILES SUCCESS NO MORE FILES SUCCESS	O:, 1:, FileInformationClass: FileNamesInformation, 3: CFF Explorer Ink, 4: Command Prompt Ink, 5: Esercizio_Pratico_U3_W2_L1, 6: Esercizio Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup O:, 1:, FileInformationClass: FileNamesInformation, 3: practicalmalwareanalysis.log Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup O:, 1:, FileInformationClass: FileNamesInformation, 3: 0.log, 4: addins, 5: AppPatch, 6: assembly, 7: Blue Lace 16: bmp, 8: bootstat.dat, 9: c Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup O:, 1:, FileInformationClass: FileNamesInformation, 3: AcGenral dtl, 4: AcLayers dtl, 5: AcLua dtl, 6: AcSpecit. dtl, 7: AcVirnal dtl, 8: apphelp Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup O:, 1:, FileInformationClass: FileNamesInformation, 3: -1, 4: 1025, 5: 1028, 6: 1031, 7: 1033, 8: 1037, 9: 1031, 10: 1042, 11: 1054, 12: 125 O: espayo.dtl, 1: edit.com, FileInformationClass: FileNamesInformation, 3: mouse dtv, 4: rep3dmod dtl, 5: mp4dmod dtl, 6: mpeg2ddata ax, 0: prognams ewe, 1: FRONIDib dtl, FileInformationClass: FileNamesInformation, 3: mouse dtv, 4: rep4dmod dtl, 5: mp4dmod dtl, 6: mpeg2ddata ax, 0: prognams ewe, 1: FRONIDib dtl, FileInformationClass: FileNamesInformation, 3: mmbgfs.dtl, 4: VMUpgradeAtShutdownWcP dtl, 5: wmwogl32 dtl, 5 Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-Directory File, Attributes: N. ShareMode: Read. Sync1ype: Sync1ype:GesteSection, PageProtection: PAGE_READ/WRITE

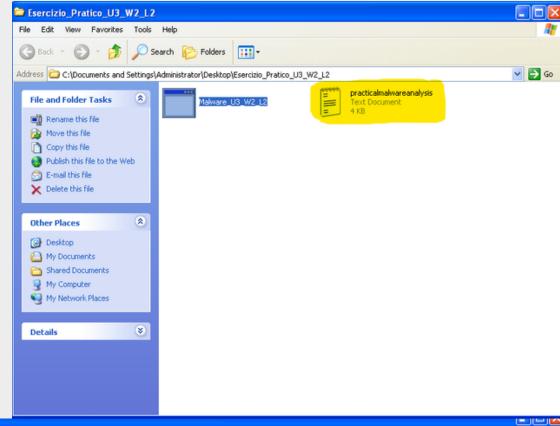
Utilizzando **Process monitor**possiamo controllare i
processi in esecuzione sulla
macchina.

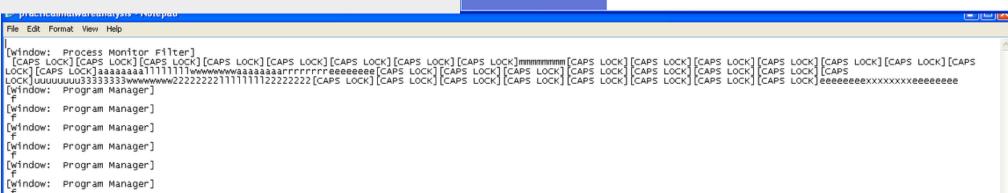
Avviando il malware notiamo un processo che crea un file di testo "praticalmalwareanalysis" nella stessa cartella del malware





Aprendo il file di testo creato,
possiamo vedere alcuni degli
input precedentemente
digitati sulla nostra tastiera,
chiaro segno che si tratta di un
keylogger.

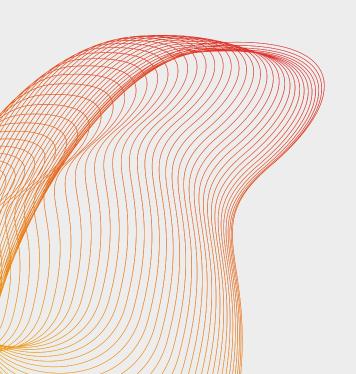




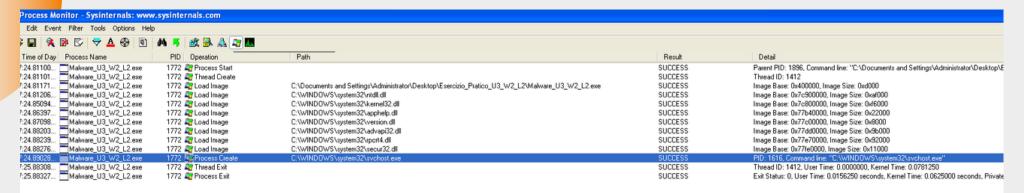


Approfondimento:

KeyLogger



Un keylogger è un tipo di software o dispositivo progettato per registrare e memorizzare le tastate effettuate su una tastiera del computer. La sua funzione principale è catturare le informazioni digitate dall'utente, inclusi username, password, messaggi di testo e altre informazioni sensibili.



Utilizzando la cattura precedente di ProcMon e cliccando sull'icona "Processi e Thread" andiamo a filtrare i processi che appartengono a quella categoria. Tra i processi trovati si trova
"Svchost.exe", nome di un processo
legittimo di Windows. Il malware è quindi
progettato per camuffarsi da processo
legittimo per passare inosservato