



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
notepad.exe		916 K	392 K	2528	Notepad	Microsoft Corporation
Procmon.exe		7,488 K	2,272 K	2416	Process Monitor	Sysinternals - www.sysinter...
Regshot-x86-Unicode.exe		54,792 K	536 K	2320	Regshot 1.9.0 x86 Unicode	Regshot Team
services.exe		1,628 K	3,508 K	720	Services and Controller app	Microsoft Corporation
smss.exe		168 K	388 K	588	Windows NT Session Mana...	Microsoft Corporation
spoolsv.exe		3,996 K	6,488 K	1392	Spooler SubSystem App	Microsoft Corporation
svchost.exe		1,348 K	3,544 K	1232	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		1,644 K	4,264 K	1296	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		1,688 K	4,216 K	1052	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		2,084 K	3,068 K	1972	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		13,056 K	22,272 K	1140	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		864 K	2,256 K	4060	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		3,036 K	4,688 K	984	Generic Host Process for Wi...	Microsoft Corporation
System		0 K	236 K	4		
VBoxService.exe		2,200 K	3,488 K	912	VirtualBox Guest Additions S...	Oracle Corporation
VBoxTray.exe		1,968 K	3,532 K	1128	VirtualBox Guest Additions Tr...	Oracle Corporation
VGAuthService.exe		6,268 K	9,000 K	780	VMware Guest Authentication...	VMware, Inc.
vmacthlp.exe		564 K	2,392 K	932	VMware Activation Helper	VMware, Inc.

  

Type	Name
Desktop	\Default
Directory	\KnownDlls
Directory	\Windows
Directory	\BaseNamedObjects
Event	\BaseNamedObjects\userenv: User Profile setup event
File	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2
File	\Device\KsecDD
File	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0...
Key	HKLM
Key	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32
Key	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32
KeyedEvent	\KernelObjects\CritSecOutOfMemoryEvent
Mutant	\BaseNamedObjects\SHIMLIB_LOG_MUTEX
Semaphore	\BaseNamedObjects\shell.{A48F1A32-A340-11D1-8C6B-00A0C90312E1}
WindowStation	\Windows\WindowStations\WinSta0
WindowStation	\Windows\WindowStations\WinSta0

Se filtriamo il pid 4060 notiamo che viene scritto continuamente un file “practicemalwareanalysis” che si trova nella stessa cartella del malware, aprendo questo file vediamo che compare il pid che avevo inserito, quindi si presuppone che sia un keylogger, cioè un malware che prende tutto quello che digito.