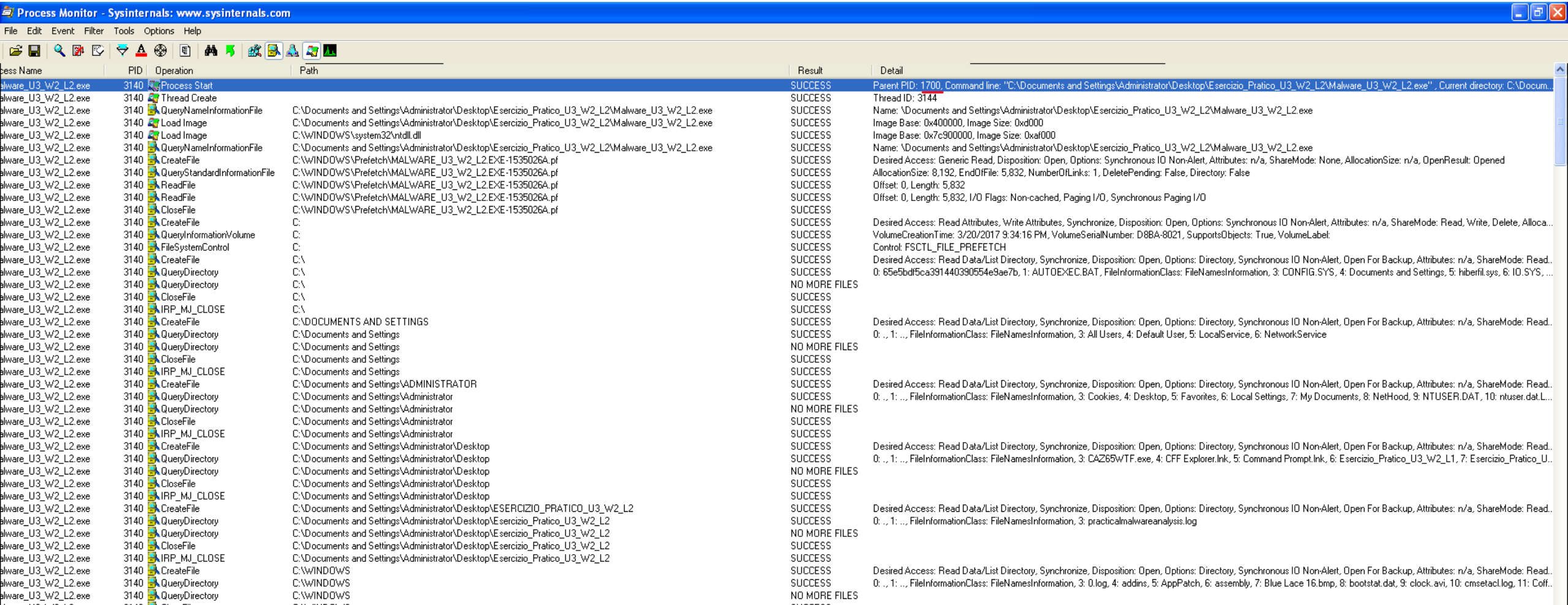
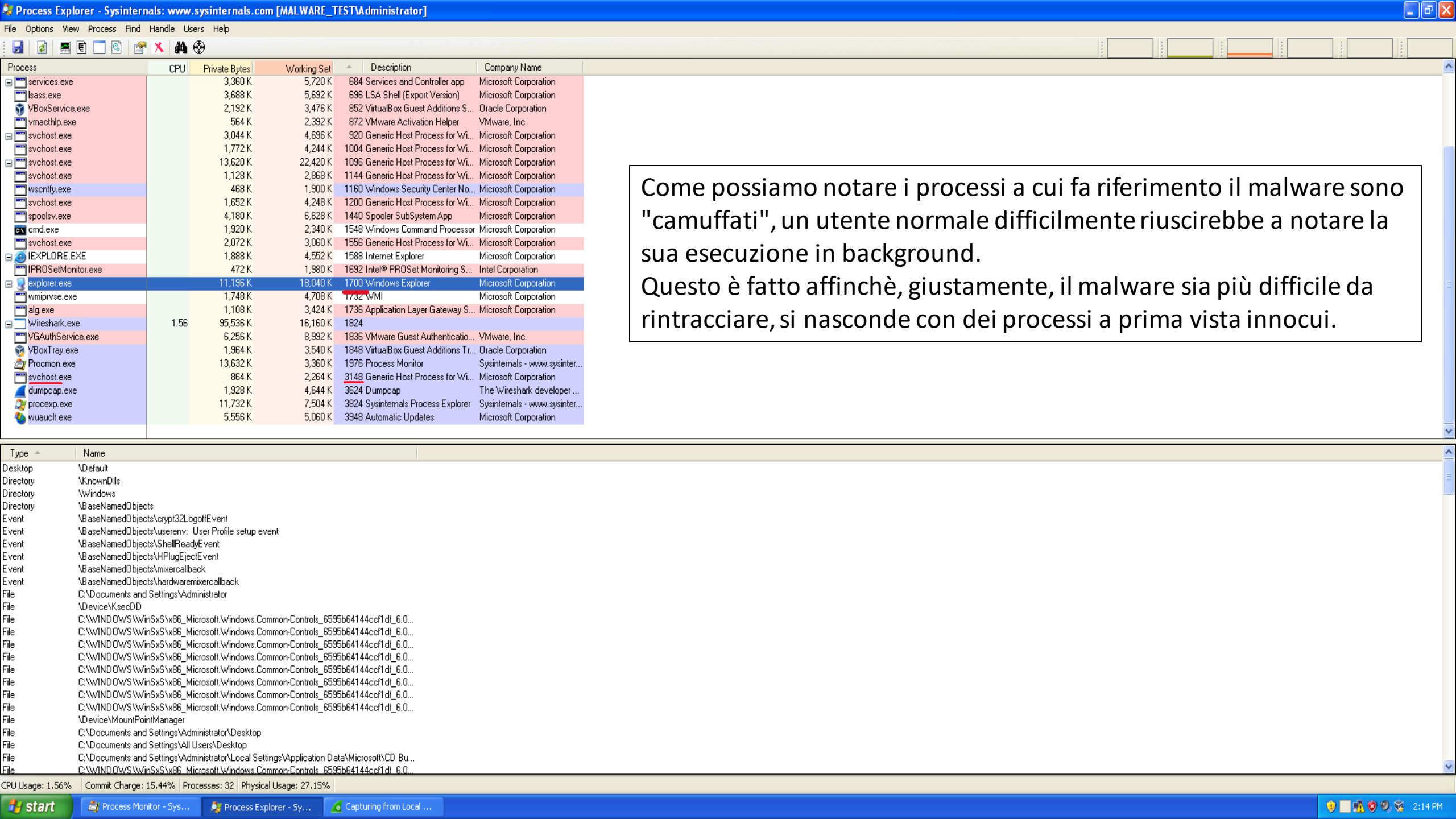
In questo esercizio andremo a fare una scansione dinamica basica di un malware. Andremo ad utilizzare process monitor (come di seguito) per verificare le azioni del malware sul file system, sui processi e sui thread. Successivamente analizzeremo eventuale traffico su WireShark e creeremo due istantanee delle chiavi di registro tramite Regshot, una prima ed una dopo aver eseguito il malware.
Possiamo subito notare che il programma fa riferimento a determinati PID (Process ID), li andremo ad individuare tramite il Process Explorer. Possiamo anche notare che il malware va a creare svariati file, il primo posto dove dovremmo guardare è la cartella in cui è installato il malware.



Process Name	PID	Operation	Path	Result	Detail
alware_U3_W2_L2.exe	3140	Process Start		SUCCESS	Parent PID: 1700, Command line: "C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe" , Current directory: C:\Docum...
alware_U3_W2_L2.exe	3140	Thread Create		SUCCESS	Thread ID: 3144
alware_U3_W2_L2.exe	3140	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_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe
alware_U3_W2_L2.exe	3140	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
alware_U3_W2_L2.exe	3140	Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Image Base: 0x7c900000, Image Size: 0xaf000
alware_U3_W2_L2.exe	3140	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_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe
alware_U3_W2_L2.exe	3140	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/a, OpenResult: Opened
alware_U3_W2_L2.exe	3140	QueryStandardInformationFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf	SUCCESS	AllocationSize: 8,192, EndOfFile: 5,832, NumberOfLinks: 1, DeletePending: False, Directory: False
alware_U3_W2_L2.exe	3140	ReadFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf	SUCCESS	Offset: 0, Length: 5,832
alware_U3_W2_L2.exe	3140	ReadFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf	SUCCESS	Offset: 0, Length: 5,832, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O
alware_U3_W2_L2.exe	3140	CloseFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf	SUCCESS	
alware_U3_W2_L2.exe	3140	CreateFile	C:	SUCCESS	Desired Access: Read Attributes, Write Attributes, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert, Attributes: n/a, ShareMode: Read, Write, Delete, Alloca...
alware_U3_W2_L2.exe	3140	QueryInformationVolume	C:	SUCCESS	VolumeCreationTime: 3/20/2017 9:34:16 PM, VolumeSerialNumber: D8BA-8021, SupportsObjects: True, VolumeLabel:
alware_U3_W2_L2.exe	3140	FileSystemControl	C:	SUCCESS	Control: FSCTL_FILE_PREFETCH
alware_U3_W2_L2.exe	3140	CreateFile	C:\	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup, Attributes: n/a, ShareMode: Read...
alware_U3_W2_L2.exe	3140	QueryDirectory	C:\	SUCCESS	0: 65e5bdf5ca391440390554e9ae7b, 1: AUTOEXEC.BAT, FileInformationClass: FileNamesInformation, 3: CONFIG.SYS, 4: Documents and Settings, 5: hiberfil.sys, 6: IO.SYS, ...
alware_U3_W2_L2.exe	3140	QueryDirectory	C:\	NO MORE FILES	
alware_U3_W2_L2.exe	3140	CloseFile	C:\	SUCCESS	
alware_U3_W2_L2.exe	3140	IRP_MJ_CLOSE	C:\	SUCCESS	
alware_U3_W2_L2.exe	3140	CreateFile	C:\DOCUMENTS AND SETTINGS	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup, Attributes: n/a, ShareMode: Read...
alware_U3_W2_L2.exe	3140	QueryDirectory	C:\Documents and Settings	SUCCESS	0: ., 1: .., FileInformationClass: FileNamesInformation, 3: All Users, 4: Default User, 5: LocalService, 6: NetworkService
alware_U3_W2_L2.exe	3140	QueryDirectory	C:\Documents and Settings	NO MORE FILES	
alware_U3_W2_L2.exe	3140	CloseFile	C:\Documents and Settings	SUCCESS	
alware_U3_W2_L2.exe	3140	IRP_MJ_CLOSE	C:\Documents and Settings	SUCCESS	
alware_U3_W2_L2.exe	3140	CreateFile	C:\Documents and Settings\ADMINISTRATOR	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup, Attributes: n/a, ShareMode: Read...
alware_U3_W2_L2.exe	3140	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: NTUSER.DAT, 10: ntuser.dat.L...
alware_U3_W2_L2.exe	3140	QueryDirectory	C:\Documents and Settings\Administrator	NO MORE FILES	
alware_U3_W2_L2.exe	3140	CloseFile	C:\Documents and Settings\Administrator	SUCCESS	
alware_U3_W2_L2.exe	3140	IRP_MJ_CLOSE	C:\Documents and Settings\Administrator	SUCCESS	
alware_U3_W2_L2.exe	3140	CreateFile	C:\Documents and Settings\Administrator\Desktop	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup, Attributes: n/a, ShareMode: Read...
alware_U3_W2_L2.exe	3140	QueryDirectory	C:\Documents and Settings\Administrator\Desktop	SUCCESS	0: ., 1: .., FileInformationClass: FileNamesInformation, 3: CAZ65WTF.exe, 4: CFF Explorer.lnk, 5: Command Prompt.lnk, 6: Esercizio_Pratico_U3_W2_L1, 7: Esercizio_Pratico_U...
alware_U3_W2_L2.exe	3140	QueryDirectory	C:\Documents and Settings\Administrator\Desktop	NO MORE FILES	
alware_U3_W2_L2.exe	3140	CloseFile	C:\Documents and Settings\Administrator\Desktop	SUCCESS	
alware_U3_W2_L2.exe	3140	IRP_MJ_CLOSE	C:\Documents and Settings\Administrator\Desktop	SUCCESS	
alware_U3_W2_L2.exe	3140	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, Open For Backup, Attributes: n/a, ShareMode: Read...
alware_U3_W2_L2.exe	3140	QueryDirectory	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS	0: ., 1: .., FileInformationClass: FileNamesInformation, 3: practicalmalwareanalysis.log
alware_U3_W2_L2.exe	3140	QueryDirectory	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	NO MORE FILES	
alware_U3_W2_L2.exe	3140	CloseFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS	
alware_U3_W2_L2.exe	3140	IRP_MJ_CLOSE	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS	
alware_U3_W2_L2.exe	3140	CreateFile	C:\WINDOWS	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup, Attributes: n/a, ShareMode: Read...
alware_U3_W2_L2.exe	3140	QueryDirectory	C:\WINDOWS	SUCCESS	0: ., 1: .., FileInformationClass: FileNamesInformation, 3: 0.log, 4: addins, 5: AppPatch, 6: assembly, 7: Blue Lace 16.bmp, 8: bootstat.dat, 9: clock.avi, 10: cmsetacl.log, 11: Coff...
alware_U3_W2_L2.exe	3140	QueryDirectory	C:\WINDOWS	NO MORE FILES	



Come possiamo notare i processi a cui fa riferimento il malware sono "camuffati", un utente normale difficilmente riuscirebbe a notare la sua esecuzione in background.
Questo è fatto affinchè, giustamente, il malware sia più difficile da rintracciare, si nasconde con dei processi a prima vista innocui.

```
     6 337.997764 0.0.0.0          255.255.255.255     DHCP      345 DHCP Discover - Transaction ID 0x82d80960
     7 345.997779 0.0.0.0          255.255.255.255     DHCP      345 DHCP Discover - Transaction ID 0x82d80960
     8 361.998800 0.0.0.0          255.255.255.255     DHCP      345 DHCP Discover - Transaction ID 0x82d80960
     9 470.404354 169.254.115.89   169.254.255.255     BROWSER   216 Get Backup List Request
    10 470.404494 169.254.115.89   169.254.255.255     NBNS       92 Name query NB WORKGROUP<1b>
    11 471.155007 169.254.115.89   169.254.255.255     NBNS       92 Name query NB WORKGROUP<1b>
    12 471.903969 169.254.115.89   169.254.255.255     NBNS       92 Name query NB WORKGROUP<1b>
    13 474.653983 169.254.115.89   169.254.255.255     BROWSER   216 Get Backup List Request
    14 474.654092 169.254.115.89   169.254.255.255     NBNS       92 Name query NB WORKGROUP<1b>
    15 475.403960 169.254.115.89   169.254.255.255     NBNS       92 Name query NB WORKGROUP<1b>
    16 476.154984 169.254.115.89   169.254.255.255     NBNS       92 Name query NB WORKGROUP<1b>
    17 478.904010 169.254.115.89   169.254.255.255     BROWSER   216 Get Backup List Request
    18 478.904119 169.254.115.89   169.254.255.255     NBNS       92 Name query NB WORKGROUP<1b>
    19 479.654882 169.254.115.89   169.254.255.255     NBNS       92 Name query NB WORKGROUP<1b>
    20 480.403967 169.254.115.89   169.254.255.255     NBNS       92 Name query NB WORKGROUP<1b>
    21 483.154849 169.254.115.89   169.254.255.255     NBNS       92 Name query NB WORKGROUP<1e>
    22 483.903987 169.254.115.89   169.254.255.255     NBNS       92 Name query NB WORKGROUP<1e>
    23 484.653957 169.254.115.89   169.254.255.255     NBNS       92 Name query NB WORKGROUP<1e>
    24 632.888380 169.254.115.89   169.254.255.255     BROWSER   243 Host Announcement MALWARE_TEST, Workstation, Server, NT Workstation
    25 691.999612 0.0.0.0          255.255.255.255     DHCP      345 DHCP Discover - Transaction ID 0x3fcb8b43
    26 697.000895 0.0.0.0          255.255.255.255     DHCP      345 DHCP Discover - Transaction ID 0x3fcb8b43
    27 703.998056 0.0.0.0          255.255.255.255     DHCP      345 DHCP Discover - Transaction ID 0x3fcb8b43
```

~res-x86_0011 - Notepad

File Edit Format View Help

```
Regshot 1.9.0 x86 Unicode
Comments:
Datetime: 2023/11/28 13:40:37   ,   2023/11/28 13:49:11
Computer: MALWARE_TEST , MALWARE_TEST
Username: Administrator , Administrator

------------------------------------
Values deleted: 1
------------------------------------
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\Folder\2:  45 00 73 00 65 00 72 00 63 00 69 00 7A 00 69 00 6F 00 5F 00 50 00 72 00 61 00 74 00 69 00 63 00 6F 00 5F 00 55 00 3

------------------------------------
Values added: 36
------------------------------------
HKLM\SYSTEM\ControlSet001\Services\kmixer\Enum\0: "SW\{b7eafdc0-a680-11d0-96d8-00aa0051e51d}\{9B365890-165F-11D0-A195-0020AFD156E4}"
HKLM\SYSTEM\CurrentControlSet\Services\kmixer\Enum\0: "SW\{b7eafdc0-a680-11d0-96d8-00aa0051e51d}\{9B365890-165F-11D0-A195-0020AFD156E4}"
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\Folder\9:  45 00 73 00 65 00 72 00 63 00 69 00 7A 00 69 00 6F 00 5F 00 50 00 72 00 61 00 74 00 69 00 63 00 6F 00 5F 00 55 00 3
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Bags\106\Shell\MinPos1920x977(1).x: 0xFFFFFFFF
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Bags\106\Shell\MinPos1920x977(1).y: 0xFFFFFFFF
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Bags\106\Shell\MaxPos1920x977(1).x: 0xFFFFFFFF
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Bags\106\Shell\MaxPos1920x977(1).y: 0xFFFFFFFF
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Bags\106\Shell\WinPos1920x977(1).left: 0x00000042
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Bags\106\Shell\WinPos1920x977(1).top: 0x00000057
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Bags\106\Shell\WinPos1920x977(1).right: 0x00000362
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Bags\106\Shell\WinPos1920x977(1).bottom: 0x000002AF
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Bags\106\Shell\ScrollPos1920x977(1).x: 0x00000000
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Bags\106\Shell\ScrollPos1920x977(1).y: 0x00000000
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Bags\58\Shell\MinPos1920x977(1).x: 0xFFFFFFFF
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Bags\58\Shell\MinPos1920x977(1).y: 0xFFFFFFFF
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Bags\58\Shell\MaxPos1920x977(1).x: 0xFFFFFFFF
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Bags\58\Shell\MaxPos1920x977(1).y: 0xFFFFFFFF
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Bags\58\Shell\WinPos1920x977(1).left: 0x00000042
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Bags\58\Shell\WinPos1920x977(1).top: 0x00000057
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Bags\58\Shell\WinPos1920x977(1).right: 0x00000362
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Bags\58\Shell\WinPos1920x977(1).bottom: 0x000002AF
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Bags\58\Shell\ScrollPos1920x977(1).x: 0x00000000
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Bags\58\Shell\ScrollPos1920x977(1).y: 0x00000000
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\MUICache\@explorer.exe,-7005: "Opens your e-mail program so you can send or read a message."
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\MUICache\@C:\WINDOWS\system32\SHELL32.dll,-32517: "Taskbar and Start Menu"
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\MUICache\@C:\WINDOWS\system32\SHELL32.dll,-22985: "Folder Options"
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\MUICache\@C:\WINDOWS\system32\icardres.dll.mui,-4097: "Windows CardSpace"
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\MUICache\@C:\WINDOWS\system32\SHELL32.dll,-22981: "Fonts"
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\MUICache\@C:\WINDOWS\system32\SHELL32.dll,-22982: "Administrative Tools"
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\MUICache\@C:\WINDOWS\system32\mstask.dll,-3408: "Scheduled Tasks"
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\MUICache\@C:\WINDOWS\system32\wiashext.dll,-331: "Scanners and Cameras"
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\MUICache\@C:\WINDOWS\system32\netshell.dll,-1201: "Connects to other computers, networks, and the Internet."
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\MUICache\C:\WINDOWS\system32\taskmgr.exe: "Windows TaskManager"
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\MUICache\C:\Program Files\Wireshark\Wireshark.exe: "Wireshark"
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\MUICache\C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe: "Malware_U3_W2_L2"
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\MUICache\@shdoclc.dll,-880: "Internet Explorer"
```

Comparativa delle chiavi di registro

Come già detto prima, dovremmo indagare prima nella cartella originaria del malware. In questo caso si tratta di un keylogger, possiamo notarlo dal file di testo che è stato creato nella cartella principale del malware. Il notepad viene aggiornato ogni volta che immettiamo qualcosa da tastiera.