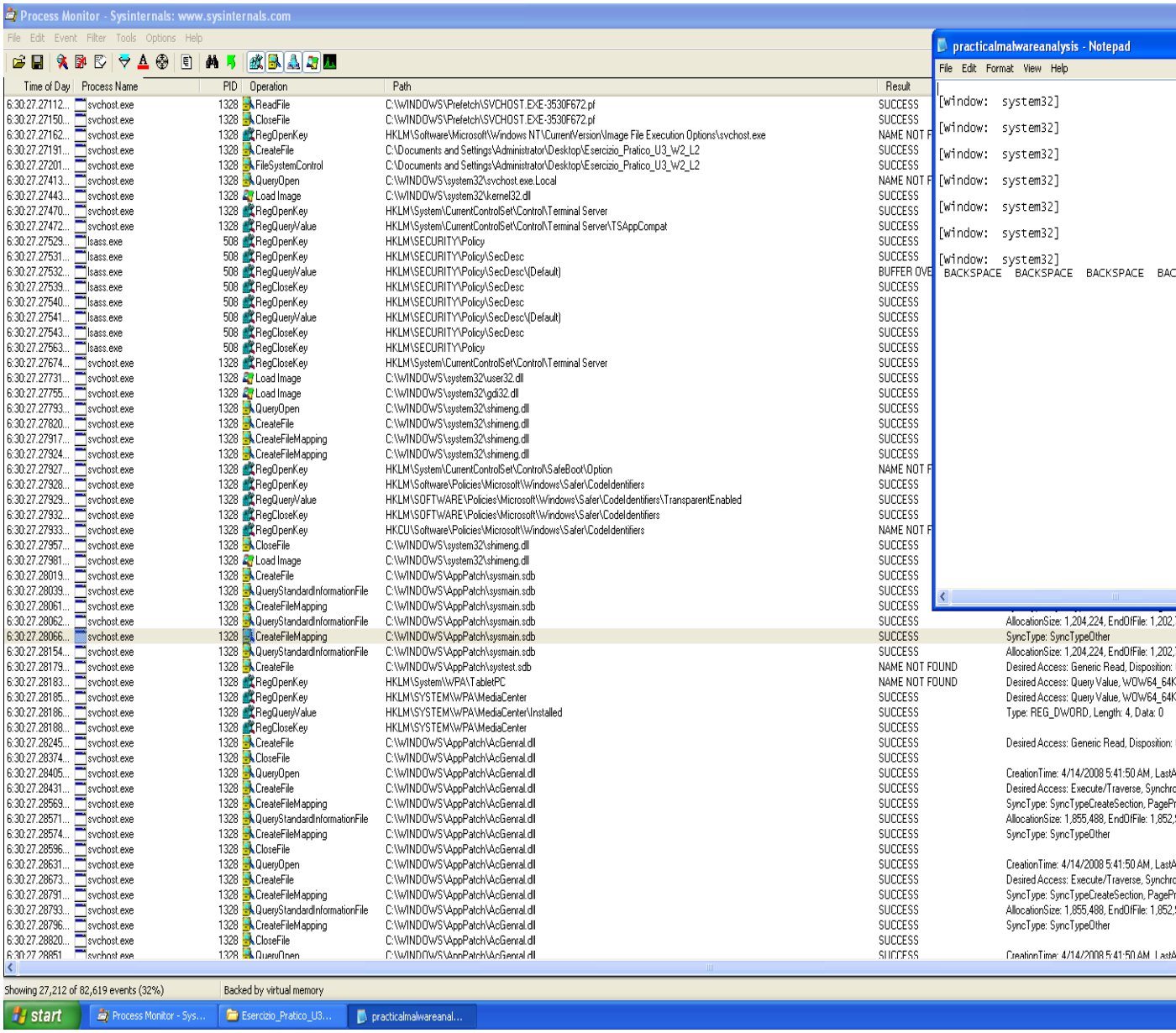
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time of Day | Process Name | PID | Operation | Path | Result
6:30:27.27112... svchost.exe 1328 ReadFile C:\WINDOWS\Prefetch\SVCHOST.EXE-3530F672.pf SUCCESS
6:30:27.27150... svchost.exe 1328 CloseFile C:\WINDOWS\Prefetch\SVCHOST.EXE-3530F672.pf SUCCESS
6:30:27.27162... svchost.exe 1328 RegOpenKey HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\svchost.exe NAME NOT F
6:30:27.27191... svchost.exe 1328 CreateFile C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2 SUCCESS
6:30:27.27201... svchost.exe 1328 FileSystemControl C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2 SUCCESS
6:30:27.27413... svchost.exe 1328 QueryOpen C:\WINDOWS\system32\svchost.exe.Local NAME NOT F
6:30:27.27443... svchost.exe 1328 Load Image C:\WINDOWS\system32\kernel32.dll SUCCESS
6:30:27.27470... svchost.exe 1328 RegOpenKey HKLM\System\CurrentControlSet\Control\Terminal Server SUCCESS
6:30:27.27472... svchost.exe 1328 RegQueryValue HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat SUCCESS
6:30:27.27529... lsass.exe 508 RegOpenKey HKLM\SECURITY\Policy SUCCESS
6:30:27.27531... lsass.exe 508 RegOpenKey HKLM\SECURITY\Policy\SecDesc SUCCESS
6:30:27.27532... lsass.exe 508 RegQueryValue HKLM\SECURITY\Policy\SecDesc\(Default) BUFFER OVE
6:30:27.27539... lsass.exe 508 RegCloseKey HKLM\SECURITY\Policy\SecDesc SUCCESS
6:30:27.27540... lsass.exe 508 RegOpenKey HKLM\SECURITY\Policy\SecDesc SUCCESS
6:30:27.27541... lsass.exe 508 RegQueryValue HKLM\SECURITY\Policy\SecDesc\(Default) SUCCESS
6:30:27.27543... lsass.exe 508 RegCloseKey HKLM\SECURITY\Policy\SecDesc SUCCESS
6:30:27.27563... lsass.exe 508 RegCloseKey HKLM\SECURITY\Policy SUCCESS
6:30:27.27674... svchost.exe 1328 RegCloseKey HKLM\System\CurrentControlSet\Control\Terminal Server SUCCESS
6:30:27.27731... svchost.exe 1328 Load Image C:\WINDOWS\system32\user32.dll SUCCESS
6:30:27.27755... svchost.exe 1328 Load Image C:\WINDOWS\system32\gdi32.dll SUCCESS
6:30:27.27793... svchost.exe 1328 QueryOpen C:\WINDOWS\system32\shimeng.dll SUCCESS
6:30:27.27820... svchost.exe 1328 CreateFile C:\WINDOWS\system32\shimeng.dll SUCCESS
6:30:27.27917... svchost.exe 1328 CreateFileMapping C:\WINDOWS\system32\shimeng.dll SUCCESS
6:30:27.27924... svchost.exe 1328 CreateFileMapping C:\WINDOWS\system32\shimeng.dll SUCCESS
6:30:27.27927... svchost.exe 1328 RegOpenKey HKLM\System\CurrentControlSet\Control\SafeBoot\Option NAME NOT F
6:30:27.27928... svchost.exe 1328 RegOpenKey HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers SUCCESS
6:30:27.27929... svchost.exe 1328 RegQueryValue HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers\TransparentEnabled SUCCESS
6:30:27.27932... svchost.exe 1328 RegCloseKey HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers SUCCESS
6:30:27.27933... svchost.exe 1328 RegOpenKey HKCU\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers NAME NOT F
6:30:27.27957... svchost.exe 1328 CloseFile C:\WINDOWS\system32\shimeng.dll SUCCESS
6:30:27.27981... svchost.exe 1328 Load Image C:\WINDOWS\system32\shimeng.dll SUCCESS
6:30:27.28019... svchost.exe 1328 CreateFile C:\WINDOWS\AppPatch\sysmain.sdb SUCCESS
6:30:27.28039... svchost.exe 1328 QueryStandardInformationFile C:\WINDOWS\AppPatch\sysmain.sdb SUCCESS
6:30:27.28061... svchost.exe 1328 CreateFileMapping C:\WINDOWS\AppPatch\sysmain.sdb SUCCESS
6:30:27.28062... svchost.exe 1328 QueryStandardInformationFile C:\WINDOWS\AppPatch\sysmain.sdb SUCCESS AllocationSize: 1,204,224, EndOfFile: 1,202,
6:30:27.28066... svchost.exe 1328 CreateFileMapping C:\WINDOWS\AppPatch\sysmain.sdb SUCCESS SyncType: SyncTypeOther
6:30:27.28154... svchost.exe 1328 QueryStandardInformationFile C:\WINDOWS\AppPatch\sysmain.sdb SUCCESS AllocationSize: 1,204,224, EndOfFile: 1,202,
6:30:27.28179... svchost.exe 1328 CreateFile C:\WINDOWS\AppPatch\systest.sdb NAME NOT FOUND Desired Access: Generic Read, Disposition:
6:30:27.28183... svchost.exe 1328 RegOpenKey HKLM\System\WPA\TabletPC NAME NOT FOUND Desired Access: Query Value, WOW64_64K
6:30:27.28185... svchost.exe 1328 RegOpenKey HKLM\SYSTEM\WPA\MediaCenter SUCCESS Desired Access: Query Value, WOW64_64K
6:30:27.28186... svchost.exe 1328 RegQueryValue HKLM\SYSTEM\WPA\MediaCenter\Installed SUCCESS Type: REG_DWORD, Length: 4, Data: 0
6:30:27.28188... svchost.exe 1328 RegCloseKey HKLM\SYSTEM\WPA\MediaCenter SUCCESS
6:30:27.28245... svchost.exe 1328 CreateFile C:\WINDOWS\AppPatch\AcGenral.dll SUCCESS Desired Access: Generic Read, Disposition:
6:30:27.28374... svchost.exe 1328 CloseFile C:\WINDOWS\AppPatch\AcGenral.dll SUCCESS
6:30:27.28405... svchost.exe 1328 QueryOpen C:\WINDOWS\AppPatch\AcGenral.dll SUCCESS CreationTime: 4/14/2008 5:41:50 AM, LastA
6:30:27.28431... svchost.exe 1328 CreateFile C:\WINDOWS\AppPatch\AcGenral.dll SUCCESS Desired Access: Execute/Traverse, Synchro
6:30:27.28569... svchost.exe 1328 CreateFileMapping C:\WINDOWS\AppPatch\AcGenral.dll SUCCESS SyncType: SyncTypeCreateSection, PagePr
6:30:27.28571... svchost.exe 1328 QueryStandardInformationFile C:\WINDOWS\AppPatch\AcGenral.dll SUCCESS AllocationSize: 1,855,488, EndOfFile: 1,852,
6:30:27.28574... svchost.exe 1328 CreateFileMapping C:\WINDOWS\AppPatch\AcGenral.dll SUCCESS SyncType: SyncTypeOther
6:30:27.28596... svchost.exe 1328 CloseFile C:\WINDOWS\AppPatch\AcGenral.dll SUCCESS
6:30:27.28631... svchost.exe 1328 QueryOpen C:\WINDOWS\AppPatch\AcGenral.dll SUCCESS CreationTime: 4/14/2008 5:41:50 AM, LastA
6:30:27.28673... svchost.exe 1328 CreateFile C:\WINDOWS\AppPatch\AcGenral.dll SUCCESS Desired Access: Execute/Traverse, Synchro
6:30:27.28791... svchost.exe 1328 CreateFileMapping C:\WINDOWS\AppPatch\AcGenral.dll SUCCESS SyncType: SyncTypeCreateSection, PagePr
6:30:27.28793... svchost.exe 1328 QueryStandardInformationFile C:\WINDOWS\AppPatch\AcGenral.dll SUCCESS AllocationSize: 1,855,488, EndOfFile: 1,852,
6:30:27.28796... svchost.exe 1328 CreateFileMapping C:\WINDOWS\AppPatch\AcGenral.dll SUCCESS SyncType: SyncTypeOther
6:30:27.28820... svchost.exe 1328 CloseFile C:\WINDOWS\AppPatch\AcGenral.dll SUCCESS
6:30:27.28851... svchost.exe 1328 QueryOpen C:\WINDOWS\AppPatch\AcGenral.dll SUCCESS CreationTime: 4/14/2008 5:41:50 AM, LastA
Showing 27,212 of 82,619 events (32%)
Backed by virtual memory
practicalmalwareanalysis - Notepad
File Edit Format View Help
[window: system32]
[window: system32]
[window: system32]
[window: system32]
[window: system32]
[window: system32]
[window: system32]
BACKSPACE BACKSPACE BACKSPACE BAC
start
Process Monitor - Sys...
Esercizio_Pratico_U3...
practicalmalwareanal...