LAB 2

Dynamic Malware Analysis

Under the direction of
Dr. Samuel Liles

Table of Contents

Abstract

This lab is focused on introducing new tools and getting familiar with it. The lab is going to use tools and application to do dynamic analysis of the malware while being isolated from the internet. The Practical Lab 3.1 to Lab 3.4 will be carried out to answer the questions provided.

The Computer Anti-virus was disabled as part of the instructions to enable the download and extract of the files being used. This lab is intended to lay grounds for further labs in the course.

Keywords: Digital Investigation, Forensic Evidence, Malware Analysis.

Lab 2 Dynamic Malware Analysis

Steps of the process

Preparing the LAB

The Computer was rebooted, anti-virus was disabled, and the appropriate files were downloaded. Different Images of VM were installed. Installation of different windows environment such as XP, 7 and 8.1. Programs needed have been downloaded and snapshots of the process have been taken.

LAB 3-1, 3-4

Applications & Tools

The following applications are used to forensically examine the files. The following descriptions have been captured from the developer's website and manuals.

PEiD," is an intuitive application that relies on its user-friendly interface to detect packers, cryptors and compilers found in PE executable files – its detection rate is higher than that of other similar tools since the app packs more than 600 different signatures in PE files" (Gröbert, 2010).

Resource Hacker,"is a freeware utility to view, modify, rename, add, delete and extract resources in 32bit & 64bit Windows executables and resource files (*.res). It incorporates an internal resource script compiler and decompiler and works on all (Win95 - Win7) Windows operating systems" (Johnson, 2011).

PE Explorer,"provides powerful tools for disassembly and inspection of unknown binaries, editing the properties of 32-bit executable files and customizing and translating their resources. Use this product to do reverse engineering, analyze the procedures and libraries an executable uses." (Heaventools Software, 2009).

Process Monitor, is an advanced monitoring tool for Windows that shows real-time file system, Registry and process/thread activity. It combines the features of two legacy Sysinternals utilities, Filemon and Regmon, and adds an extensive list of enhancements including rich and non-destructive filtering, comprehensive event properties such session IDs and user names, reliable process information, full thread stacks with integrated symbol support for each operation, simultaneous logging to a file, and much more. Its uniquely powerful features will make Process Monitor a core utility in your system troubleshooting and malware hunting toolkit (Russinovich & Cogswell, 2014).

ApateDNS, is a tool for controlling DNS responses though an easy to use GUI. As a phony DNS server, ApateDNS spoofs DNS responses to a user-specified IP address by listening on UDP port 53 on the local machine. It responds to DNS requests with the response set to any IP address you specify. The tool logs and timestamps any DNS request it receives. You may specify a number of non-existent domain (NXDOMAIN) responses to send before returning a valid response. ApateDNS also automatically sets the local DNS to localhost. By default, it will use either the set DNS or default gateway settings as an IP address to use for DNS responses. Upon exiting the tool, it sets back the original local DNS settings (Davis, 2011).

Regshot, is a small, free and open-source registry compare utility that allows you to quickly take a snapshot of your registry and then compare it with a second one - done after doing system changes or installing a new software product. The changes report can be produced in text or HTML format and contains a list of all modifications that have taken place between the two snapshots. In addition, you can also specify folders (with subfolders) to be scanned for changes as well (Regshot Team, 2013).

Issues or problems

VMware crashing while installing Windows 8.1 OS to an image. Low processing power on the Host PCs.

Conclusions

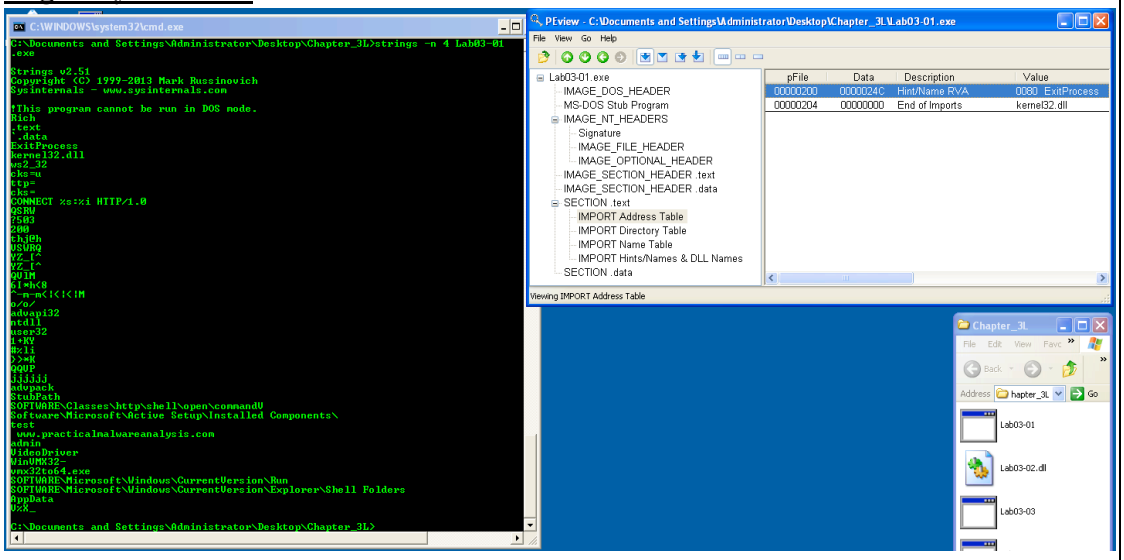
The Lab identified several programs that helps explore the malwares. The tools showed if the files being used are infected or packed. The tools used also showed the resources on the system that is being utilized such as privilege, CPU usage, Network communication.

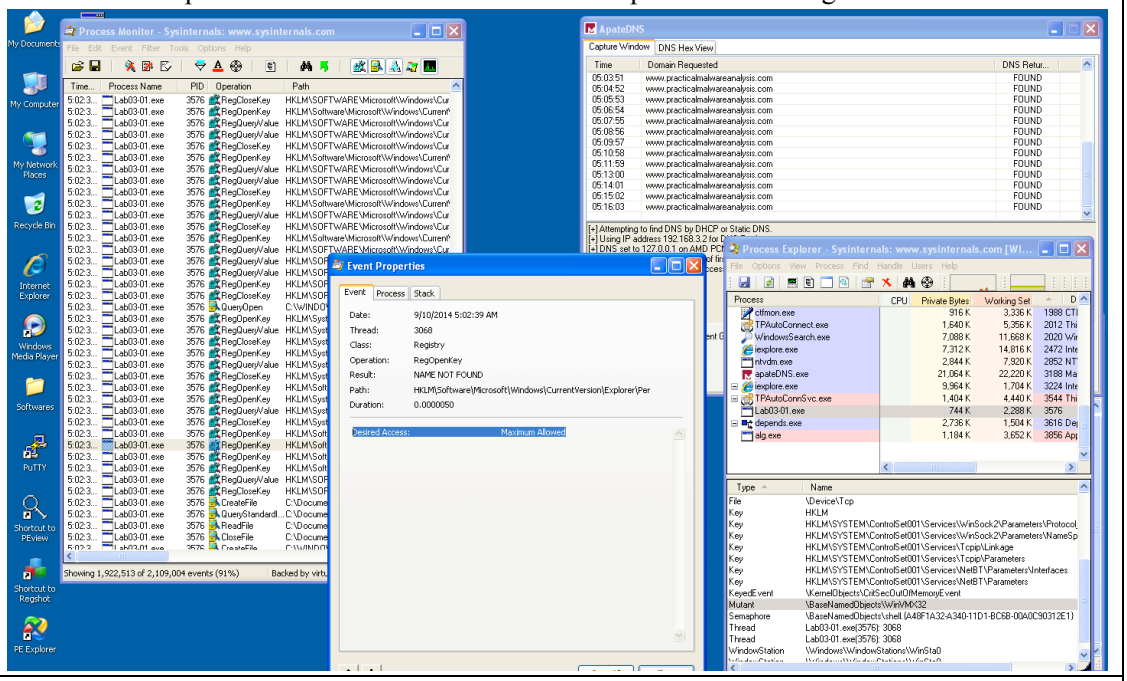
Case studies

No Case studies was given with this lab.

Review questions

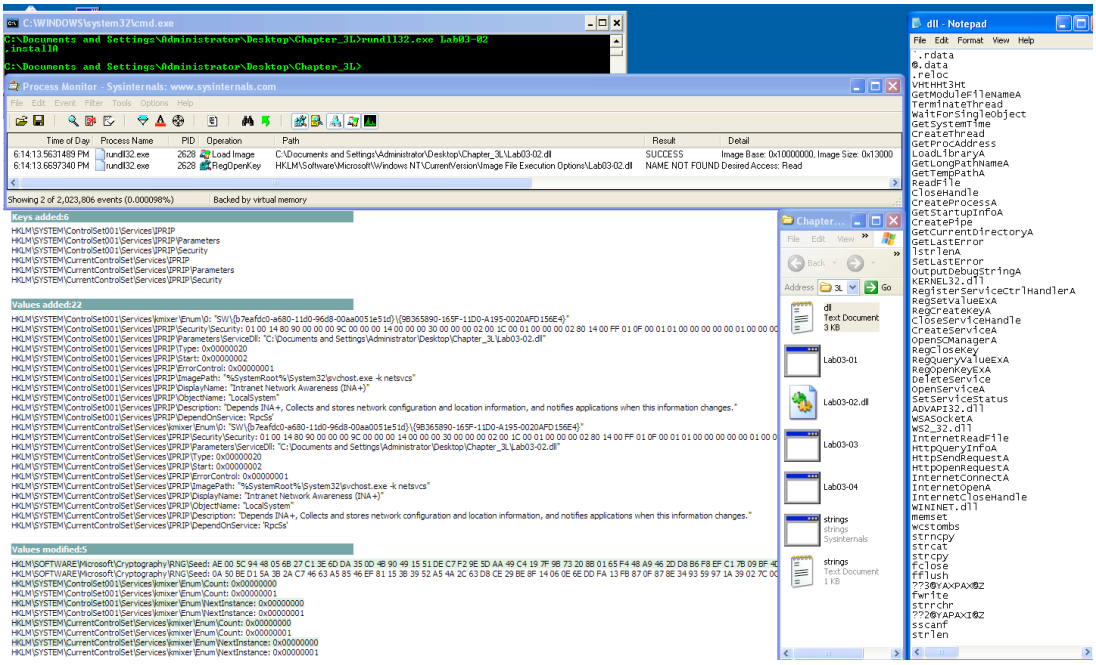
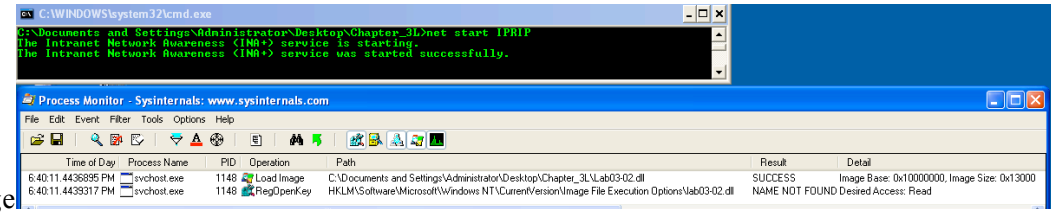
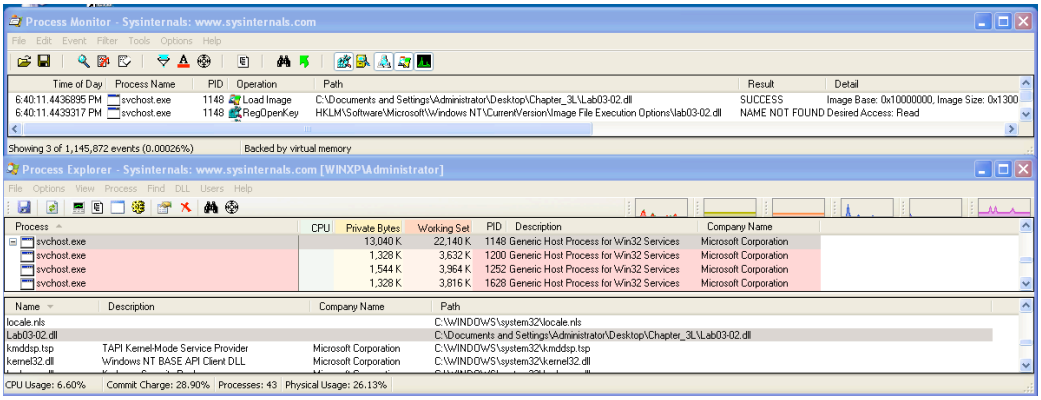
Lab 3-1

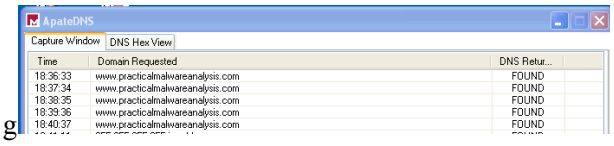
Answers	Lab03-01.EXE
1	The Address table in PEview shows that there is one imports function which is Exit Process. running the following command on the file strings -n 4 Lab03-01.exe > strings.txt produces lots of strings that are of interest such as: ExitProcess <------ **Malware Imports** kernel32.dll <------ **Only DLL library indecates it could be packaged** CONNECT %s:%i HTTP/1.0 StubPath SOFTWARE\Classes\http\shell\open\commandV <------ **Registery Location** Software\Microsoft\Active Setup\Installed Components\ <------ **Registery Location** test www.practicalmalwareanalysis.com <------ **Website** admin VideoDriver WinVMX32- vmx32to64.exe <------ **Exe File** SOFTWARE\Microsoft\Windows\CurrentVersion\Run <------ **Registery Location** SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders <------ **Registery Location** 
2	After running the malware lots of events started happening as shown on Procmon such as requesting maximum access privilege available on the explorer. It also mutated and

	created a new process vmx32 which was found as part of the strings available. 
3	Yes, using the ApateDNS we see the malware constantly sending packets to www.practicalmalwareanalysis.com

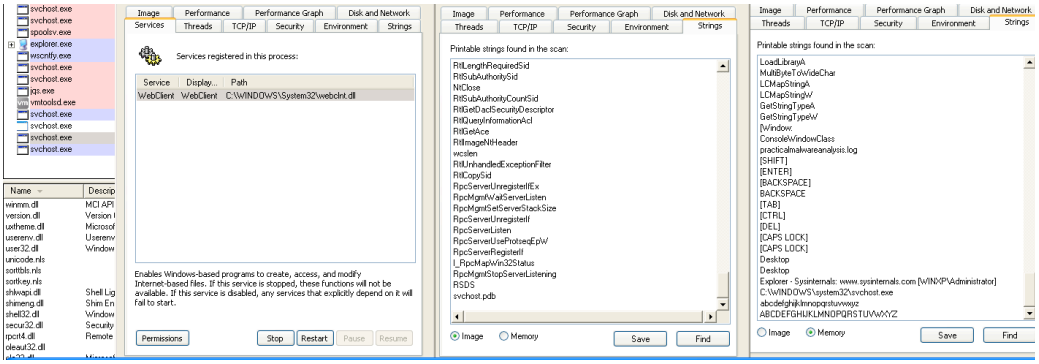
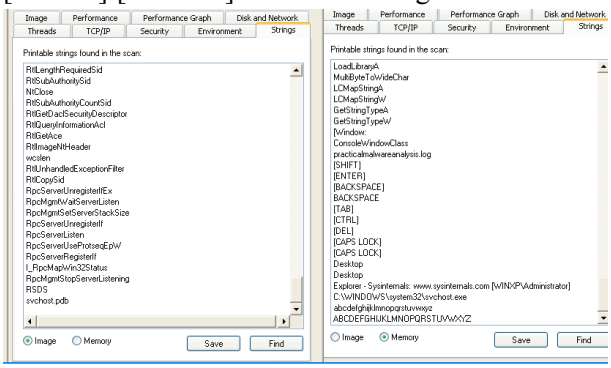
Lab 3-2

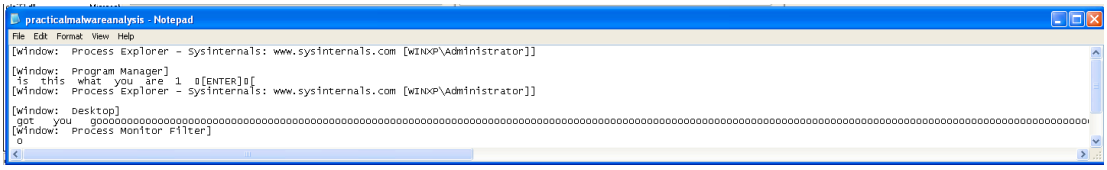
Answers	Lab03-02.Dll
1	After checking the PEview and since its a dll file its more likely the malware is designed to run as a service strings -n 5 Lab03-02.dll > dll.txt, the following are selected lines from the output file that gives another indication that the malware runs as service. CloseServiceHandle OpenServiceA ServiceMain CreateServiceA SetServiceStatus UninstallService DeleteService In order to install it we use the system file rundll32.exe on the DLL file Lab03-02.dll Calling the function available which is installA, the full command is rundll32.exe Lab03-02.dll,installA

	
2	After reviewing the registry keys we can see IPRIP has been installed in the Control set under services which can be used via running IPRIP which is a service that provide RIP information that helps in forwarding packets to subnetworks or remote host. The following command initiate the malware and put it in active mode. Net start IPRIP as shown in the image 
3	After seeing svchost.exe in Process Monitor application we use Process Explorer to look for the svchost.exe and analyze it looking for the malware and as seen in the picture the malware has used the svchost.exe to run. Since there are lots of svchost.exe instances running it was a clear indicator which one was abnormal when looking at the working Set values, all of them are bellow 4k except the one that had the Dll running it was 22k+. 
4	I can use the PID found in Process explorer to filter Procmon list which is 1148.

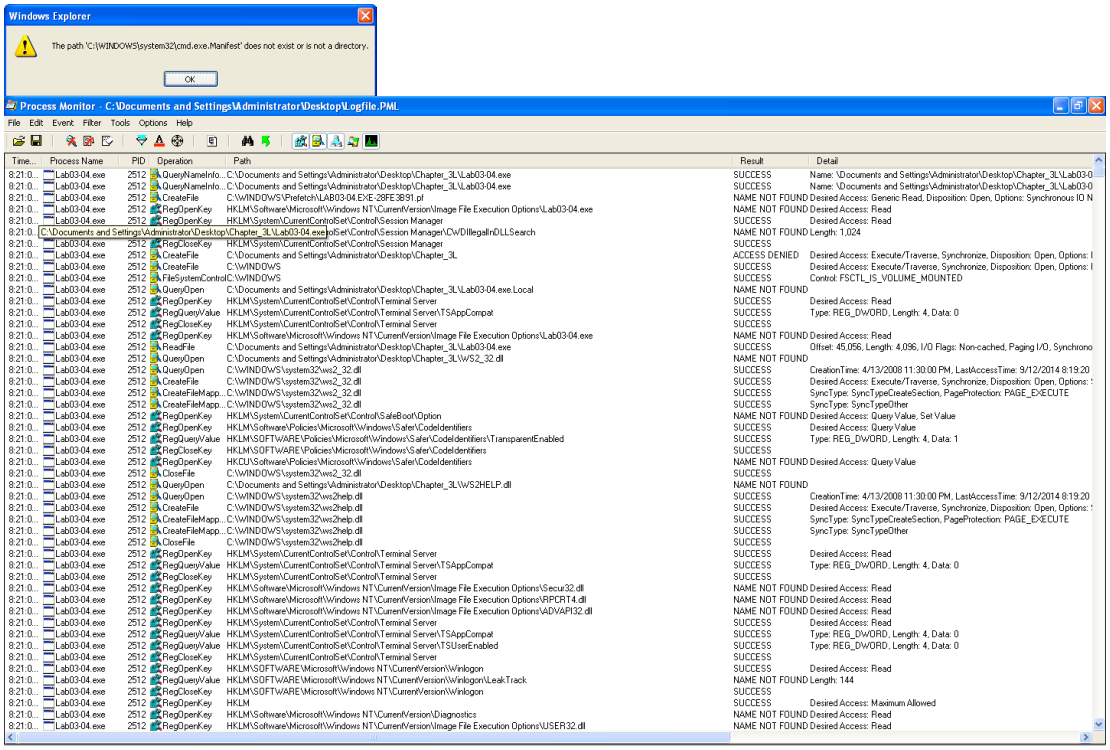
5	We Can see that the malware had added several registry files on the computer such as the first and last line in the bellow image. HKLM\SYSTEM\ControlSet001\Services\IPRIP\Parameters\ServiceDll: "C:\Documents and Settings\Administrator\Desktop\Chapter_3L\Lab03-02.dll" HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Parameters\ServiceDll: "C:\Documents and Settings\Administrator\Desktop\Chapter_3L\Lab03-02.dll" HKLM\SYSTEM\ControlSet001\Services\IPRIP\Parameters\ServiceDll: "C:\Documents and Settings\Administrator\Desktop\Chapter_3L\Lab03-02.dll" HKLM\SYSTEM\ControlSet001\Services\IPRIP\Type: 0x00000020 HKLM\SYSTEM\ControlSet001\Services\IPRIP\Start: 0x00000002 HKLM\SYSTEM\ControlSet001\Services\IPRIP\ErrorControl: 0x00000001 HKLM\SYSTEM\ControlSet001\Services\IPRIP\ImagePath: "%SystemRoot%\System32\svchost.exe -k netsvcs" HKLM\SYSTEM\ControlSet001\Services\IPRIP\DisplayName: "Intranet Network Awareness (INA+)" HKLM\SYSTEM\ControlSet001\Services\IPRIP\ObjectName: "LocalSystem" HKLM\SYSTEM\ControlSet001\Services\IPRIP\Description: "Depends INA+, Collects and stores network configuration and location information, and notifies HKLM\SYSTEM\ControlSet001\Services\IPRIP\DependOnService: 'RpcSs' HKLM\SYSTEM\CurrentControlSet\Services\mxer\Enum\0: "SW\{b7eafdc0-a680-11d0-96d8-00aa0051e51d}\{9B365890-165F-11D0-A195-0020AFD156E4 HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Security\Security: 01 00 14 80 90 00 00 00 9C 00 00 00 14 00 00 00 30 00 00 00 02 00 1C 00 01 00 00 0C HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Parameters\ServiceDll: "C:\Documents and Settings\Administrator\Desktop\Chapter_3L\Lab03-02.dll"
6	Looking at AdateDNS we can see that the malware is constantly asking for information almost every minute from www.practicalmalwareanalysis.com which can be used as a malware signuter. g 

Lab 3-3

Answers	Lab03-03.exe
1	From the Picture bellow we can see that the malware has attached itself to the process explorer. In the image we see 3 property windows. The first is a legitimate process scvhost.exe which is a child of Services. Where the other two property windows does not include Services Tab At all. 
2	From the Picture bellow we can see a discrepancy in the strings section of the file saved on the hard disk and the one running in memory. On the Right property image we see [SHIFT] [ENTER] and other things that are not stored in the file. 
3	The Following image of a notepad file called practicalmalwareanalysis.log was found in

	the same directory that included the malware. 
4	From the notepad created and the information in it. It looks like a key logger hijacking a svchost.exe process.

Lab 3-4

Answers	Lab03-04.exe
1	The file deletes itself.
2	Trying the command line failed probably because we do not have the proper arguments set up.
3	Using Right Click Run As was successful and Dynamic analysis could be done. The malware creates a threat, and a prefetch file under its name. It also injects itself into the registry. It also creates different DLL files such as comctl32.dll it has also created logs and such as software.LOG under windows\system32\config\ from the general look it seems like it is creating alternative streams in files to save its own information. Moreover, it is also using encryption and using the network to upload that information. A host based indicators is comctl32.dll as well as cmd.exe.Manifest 

References

Davis, S. (2011, October). *ApateDNS*. Retrieved from https://www.mandiant.com/blog/research-tool-release-apatedns/

Gröbert, F. (2010, 02 07). *PEiD*. Retrieved 02 18, 2014, from https://code.google.com/p/kerckhoffs/downloads/

Heaventools Software. (2009, 10 14). *Heaventools*. Retrieved from http://heaventools.com/download.htm

Johnson, A. (2011, 09 16). *Resource Hacker*. Retrieved from http://www.angusj.com/resourcehacker/

Regshot Team. (2013, August). *Regshot*. Retrieved from http://sourceforge.net/projects/regshot/

Russinovich, M., & Cogswell, B. (2014, March). *Process Monitor v3.1*. Retrieved from http://technet.microsoft.com/en-us/sysinternals/bb896645.aspx