# Advanced Malware Cleaning Techniques for the IT Professional

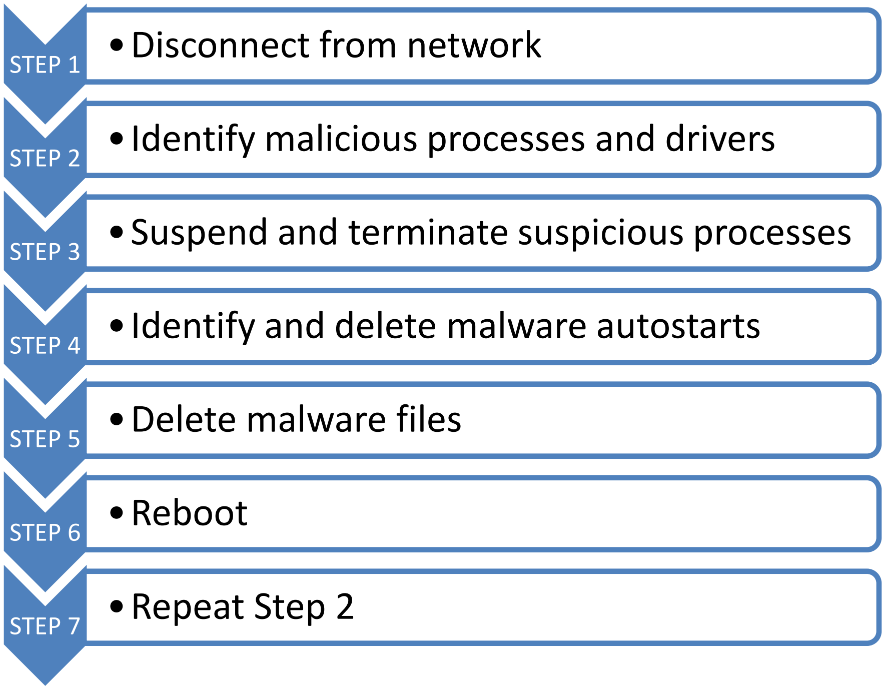
***Mark Russinovich***
***Microsoft Technical Fellow***

This section of the *Microsoft Security Intelligence Report* provides information and guidance for IT professionals about investigating, analyzing, and—when possible—removing malware from an infected computer.

Except in special situations, Microsoft recommends the use of antimalware software tools, such as Microsoft Forefront Endpoint Protection (for organizations) and Microsoft Security Essentials (for individuals), for keeping computers free from malware, rather than the manual techniques described in this section. This guidance is intended for advanced users who possess a good understanding of the inner workings of computers and Windows, and who wish to understand the disinfection process—how malware can be removed without the aid of antimalware software. It is designed to help IT professionals understand the impact of malware, understand how malware operates, learn how to use some specific software tools, and create a rudimentary roadmap for cleaning infected computers in special situations.

This guidance involves the use of several Windows Sysinternals tools. Sysinternals is a suite of advanced diagnostics and troubleshooting utilities for the Windows platform that is available for download at no charge from the Microsoft Download Center. See technet.microsoft.com/sysinternals for more information about the Sysinternals utilities.

Figure 60. A seven-step process for removing malware


STEP 1
- Disconnect from network

STEP 2
- Identify malicious processes and drivers

STEP 3
- Suspend and terminate suspicious processes

STEP 4
- Identify and delete malware autostarts

STEP 5
- Delete malware files

STEP 6
- Reboot

STEP 7
- Repeat Step 2

## Step 1: Disconnect from the Network

Disconnecting the infected computer or computers from the network is an essential part of the malware removal process, because it ensures that infected computers do not spread malware to other computers on the network. This step can be performed by physically disconnecting or disabling the network cable or card from each computer (including disabling wireless networking via hardware switch if possible), or by disabling all networking functions from the BIOS configuration screen (instructions for performing this task vary for different computers and motherboards).

## Step 2: Identify Malicious Processes and Drivers

After an infected computer is disconnected from the network, the next step in the disinfection process is to identify any malicious processes. This step involves looking for telltale signs such as:

- Processes without custom icons.

- Processes that have no description or company name associated with them.

- Files that represent themselves as being from Microsoft, but don't have digital signatures.

- Unfamiliar processes running from the Windows directory.

- Files that are *packed*, which means that they have been compressed or encrypted. Most malware files are packed by their distributors in an effort to make them more difficult for security software to identify.

- Strange URLs in strings embedded in files.

- Processes with open TCP/IP endpoints.

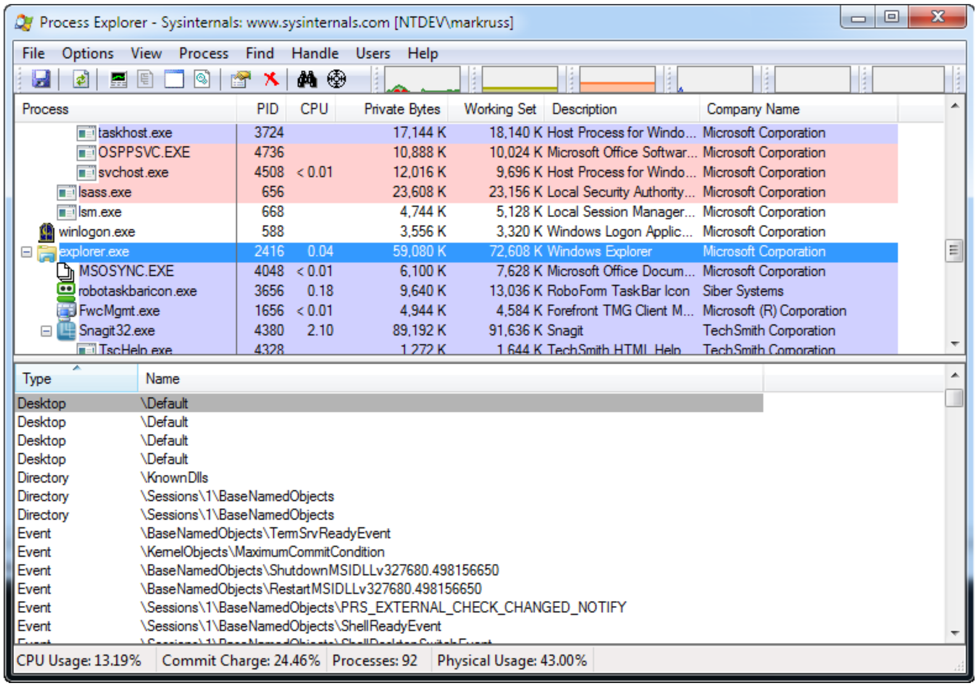
- Processes that host suspicious dynamic-link libraries (DLLs) or services.

By themselves, these signs do not conclusively indicate a malicious process. For example, many legitimate executables and other files are packed, and many legitimate processes run without custom icons. Also, not all malware files and processes exhibit all the signs listed here. However, these signs generally serve as useful clues for detecting malware on an infected computer. A Sysinternals tool called Process Explorer can help a troubleshooter spot malicious processes.

## Using Process Explorer

Process Explorer is a kind of "super Task Manager" that provides a variety of general troubleshooting capabilities, including the discovery of DLL versioning problems, handle leaks, and locked file information; performance troubleshooting; and detailing hung processes.

Figure 61. The Process Explorer main window


Process Explorer - Sysinternals: www.sysinternals.com [NTDEV\markruss]
File
Options
View
Process
Find
Handle
Users
Help

| Process | PID | CPU | Private Bytes | Working Set | Description | Company Name |
|---|---|---|---|---|---|---|
| taskhost.exe | 3724 | | 17,144 K | 18,140 K | Host Process for Windo... | Microsoft Corporation |
| OSPPSVC.EXE | 4736 | | 10,888 K | 10,024 K | Microsoft Office Softwar... | Microsoft Corporation |
| svchost.exe | 4508 | < 0.01 | 12,016 K | 9,696 K | Host Process for Windo... | Microsoft Corporation |
| lsass.exe | 656 | | 23,608 K | 23,156 K | Local Security Authority... | Microsoft Corporation |
| lsm.exe | 668 | | 4,744 K | 5,128 K | Local Session Manager... | Microsoft Corporation |
| winlogon.exe | 588 | | 3,556 K | 3,320 K | Windows Logon Applic... | Microsoft Corporation |
| explorer.exe | 2416 | 0.04 | 59,080 K | 72,608 K | Windows Explorer | Microsoft Corporation |
| MSOSYNC.EXE | 4048 | < 0.01 | 6,100 K | 7,628 K | Microsoft Office Docum... | Microsoft Corporation |
| robotaskbaricon.exe | 3656 | 0.18 | 9,640 K | 13,036 K | RoboForm TaskBar Icon | Siber Systems |
| FwcMgmt.exe | 1656 | < 0.01 | 4,944 K | 4,584 K | Forefront TMG Client M... | Microsoft (R) Corporation |
| Snagit32.exe | 4380 | 2.10 | 89,192 K | 91,636 K | Snagit | TechSmith Corporation |
| TscHelp.exe | 4328 | | 1,272 K | 1,644 K | TechSmith HTML Help | TechSmith Corporation |

| Type | Name |
|---|---|
| Desktop | \Default |
| Desktop | \Default |
| Desktop | \Default |
| Desktop | \Default |
| Directory | \KnownDlls |
| Directory | \Sessions\1\BaseNamedObjects |
| Directory | \Sessions\1\BaseNamedObjects |
| Event | \BaseNamedObjects\TermSrvReadyEvent |
| Event | \KernelObjects\MaximumCommitCondition |
| Event | \BaseNamedObjects\ShutdownMSIDLLv327680.498156650 |
| Event | \BaseNamedObjects\RestartMSIDLLv327680.498156650 |
| Event | \Sessions\1\BaseNamedObjects\PRS_EXTERNAL_CHECK_CHANGED_NOTIFY |
| Event | \Sessions\1\BaseNamedObjects\ShellReadyEvent |
| Event | \Sessions\1\BaseNamedObjects\ShellDesktopSwitchEvent |

CPU Usage: 13.19% Commit Charge: 24.46% Processes: 92 Physical Usage: 43.00%

The Process Explorer main window provides a simple paneled display of information about the processes that are running on the computer. Although there are superficial similarities between this view and the **Processes** tab in Windows Task Manager, Process Explorer provides a great deal more information about each process. Each row in the process list represents a process object running on the computer that has its own virtual address space and one or more threads that could conceivably execute code at some point.

The names of malicious processes often mimic the names of legitimate processes, which can make them difficult to identify in Task Manager. Using Process Explorer makes it easier to identify processes that run from suspicious locations, or that display suspicious characteristics. By default, processes are listed in a hierarchical view called the process tree, which shows parent/child relationships between processes. Columns display a range of properties for each process, including the name of the company that published the image, a brief description, version information, and more.

When investigating an infection, pay attention to the **Company Name**, **Description**, and **Version** columns. Legitimate software publishers usually provide values for some or all of these columns, but malware authors sometimes neglect them. To display more columns or hide columns already in the display, click the **View** menu, and then click **Select Columns**.

Rows can be highlighted in different colors, which provides additional information:

- Blue indicates that the process is running in the same security context as Process Explorer. Generally, this means that it's running under the active user account, rather than a system or service account.

- Pink indicates that the process is hosting one or more Windows services. Services can run on their own, or as part of the services DLL inside a Svchost.exe process.

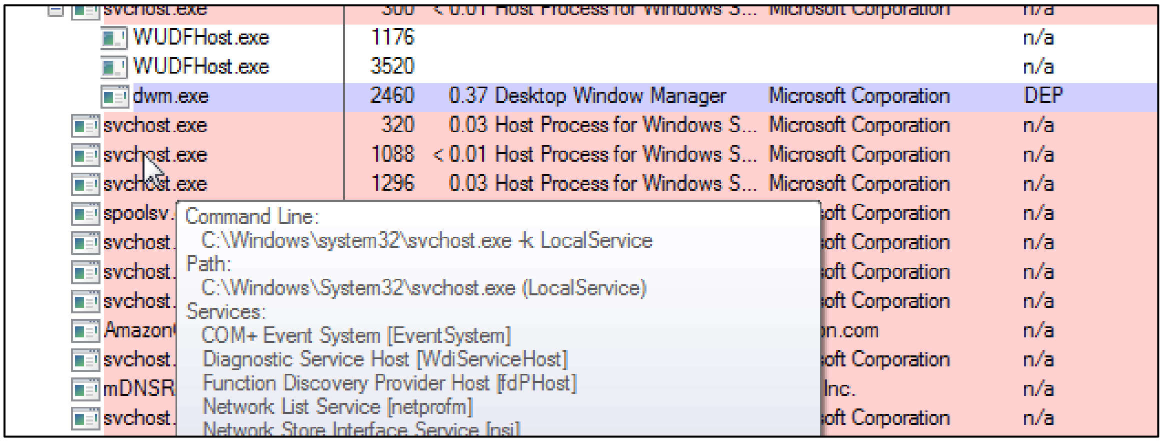
- Purple indicates that the image has been packed (compressed or encrypted).

- Green and red indicates that the process has just started or exited, respectively. By default, rows are only highlighted green or red for 1 second, which can make them difficult to track. You can change this default length by clicking **Difference Highlight Duration** in the **Options** menu.

Other colors indicate different process types, but the ones in the preceding list are the important ones that can help you locate and remove malware.

Moving the mouse pointer over a row displays a tooltip with information about the process, such as the full path to the process image, which can help you identify processes running from unusual or suspicious locations. Tooltips also provide additional information for system processes, such as DLLs hosted by Rundll32.exe, services hosted by Svchost.exe and other service processes, and COM server information for Dllhost.exe. Malware often attempts to disguise its presence by attaching itself to system processes such as these, so pay attention to tooltips when investigating the source of an infection.

Figure 62. Tooltips provide additional information about processes



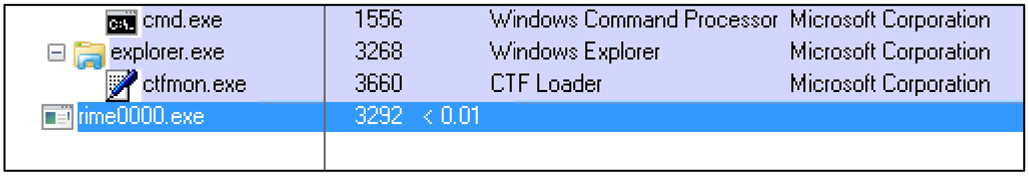
| | | | | | |
|---|---|---|---|---|---|
| svchost.exe | 300 | < 0.01 | Host Process for Windows S... | Microsoft Corporation | n/a |
| WUDFHost.exe | 1176 | | | | n/a |
| WUDFHost.exe | 3520 | | | | n/a |
| dwm.exe | 2460 | 0.37 | Desktop Window Manager | Microsoft Corporation | DEP |
| svchost.exe | 320 | 0.03 | Host Process for Windows S... | Microsoft Corporation | n/a |
| svchost.exe | 1088 | < 0.01 | Host Process for Windows S... | Microsoft Corporation | n/a |
| svchost.exe | 1296 | 0.03 | Host Process for Windows S... | Microsoft Corporation | n/a |
| spoolsv. | | | | oft Corporation | n/a |
| svchost. | | | | oft Corporation | n/a |
| svchost. | | | | oft Corporation | n/a |
| svchost. | | | | oft Corporation | n/a |
| Amazon | | | | n.com | n/a |
| svchost. | | | | oft Corporation | n/a |
| mDNSR | | | | Inc. | n/a |
| svchost. | | | | oft Corporation | n/a |

```
Command Line:
   C:\Windows\system32\svchost.exe -k LocalService
Path:
   C:\Windows\System32\svchost.exe (LocalService)
Services:
   COM+ Event System [EventSystem]
   Diagnostic Service Host [WdiServiceHost]
   Function Discovery Provider Host [fdPHost]
   Network List Service [netprofm]
   Network Store Interface Service [nsi]
```

To research a process you don't recognize, select **Search Online** from the **Process** menu or press Ctrl+M to search for the process name using the configured browser and search engine. Malware sometimes uses random or semi-random strings for process and file names, so even if you can't locate affirmative evidence that a process is a malicious one, a search that produces no results at all for a process name can sometimes indicate that the process is suspicious.

Figure 63 shows a malicious process created by a variant of the worm family Win32/Rimecud. This process has no icon, company name, or description, and a name that produces no results in an Internet search.

Figure 63. A malicious process in Process Explorer

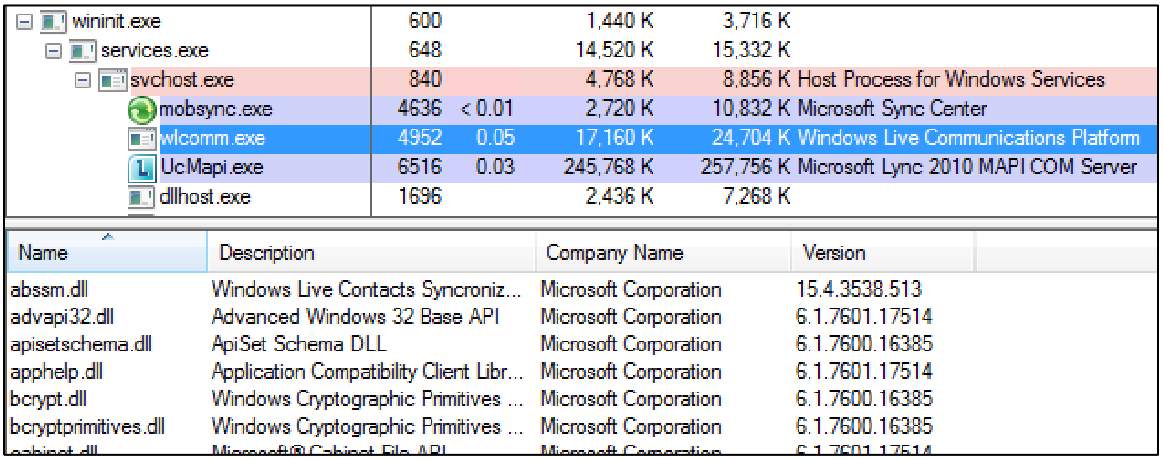


| | | | | |
|---|---|---|---|---|
| cmd.exe | 1556 | | Windows Command Processor | Microsoft Corporation |
| explorer.exe | 3268 | | Windows Explorer | Microsoft Corporation |
| ctfmon.exe | 3660 | | CTF Loader | Microsoft Corporation |
| rime0000.exe | 3292 | < 0.01 | | |

## DLL View

Malware can hide inside a legitimate process as a DLL, using a technique called DLL injection. Process Explorer's lower pane (which can be displayed by clicking the **Show Lower Pane** button on the toolbar or pressing Ctrl+L) lets you list the contents of the process selected in the upper pane. The lower pane can be configured to display in either DLL view or Handle view. DLL view lists all the DLLs and other files mapped into the process' address space, and Handle view lists all the kernel objects opened by the process. Pressing Ctrl+D opens DLL view.

Figure 64. DLL view lists the DLLs and other files used by a process



| | | | | | |
|---|---|---|---|---|---|
| wininit.exe | 600 | | 1,440 K | 3,716 K | |
| services.exe | 648 | | 14,520 K | 15,332 K | |
| svchost.exe | 840 | | 4,768 K | 8,856 K | Host Process for Windows Services |
| mobsync.exe | 4636 | < 0.01 | 2,720 K | 10,832 K | Microsoft Sync Center |
| wlcomm.exe | 4952 | 0.05 | 17,160 K | 24,704 K | Windows Live Communications Platform |
| UcMapi.exe | 6516 | 0.03 | 245,768 K | 257,756 K | Microsoft Lync 2010 MAPI COM Server |
| dllhost.exe | 1696 | | 2,436 K | 7,268 K | |

| Name | Description | Company Name | Version |
|---|---|---|---|
| abssm.dll | Windows Live Contacts Syncroniz... | Microsoft Corporation | 15.4.3538.513 |
| advapi32.dll | Advanced Windows 32 Base API | Microsoft Corporation | 6.1.7601.17514 |
| apisetschema.dll | ApiSet Schema DLL | Microsoft Corporation | 6.1.7600.16385 |
| apphelp.dll | Application Compatibility Client Libr... | Microsoft Corporation | 6.1.7601.17514 |
| bcrypt.dll | Windows Cryptographic Primitives ... | Microsoft Corporation | 6.1.7600.16385 |
| bcryptprimitives.dll | Windows Cryptographic Primitives ... | Microsoft Corporation | 6.1.7600.16385 |
| cabinet.dll | Microsoft® Cabinet File API | Microsoft Corporation | 6.1.7601.17514 |

In DLL view, each row in the lower pane lists information about a DLL, executable file, or other memory-mapped file that is being used by the process. For the System process, DLL view lists the image files mapped into kernel memory, including Ntoskrnl.exe and all the loaded device drivers. As with processes, any packed files are highlighted in purple.

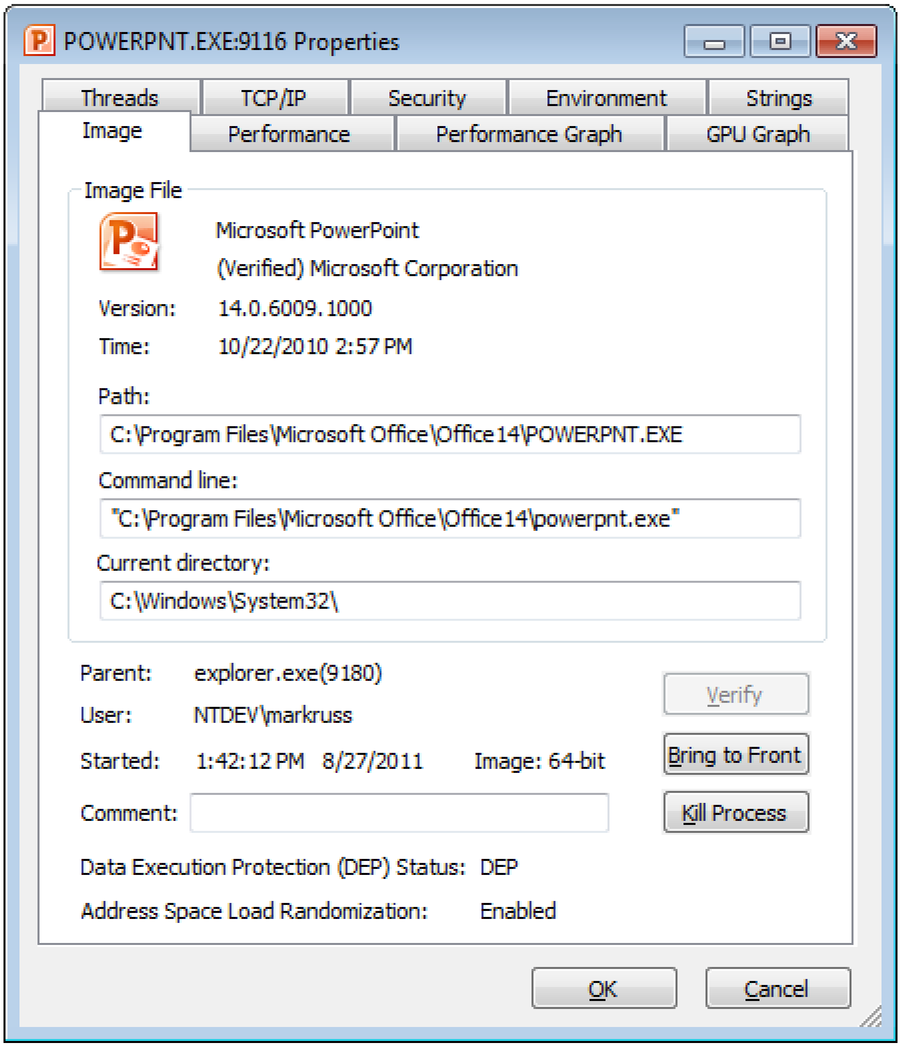
Double-clicking a row displays a **Properties** dialog with information about the file, including any strings found in the file on disk and in memory (see page 104). DLL view also supports the same Search Online functionality that the Process view does.

DLL view is empty for the System Idle Process and Interrupts pseudo-processes. You need to run Process Explorer with administrative rights to list DLLs loaded in processes running as a different user, but administrative rights are not required to list the images loaded in the System process.

## Process Properties

Double-clicking a process launches the **Properties** dialog, which is shown in Figure 65.

Figure 65. The Properties dialog



POWERPNT.EXE:9116 Properties

Image File

Microsoft PowerPoint

(Verified) Microsoft Corporation

Version: 14.0.6009.1000

Time: 10/22/2010 2:57 PM

Path:

C:\Program Files\Microsoft Office\Office14\POWERPNT.EXE

Command line:

"C:\Program Files\Microsoft Office\Office14\powerpnt.exe"

Current directory:

C:\Windows\System32\

Parent: explorer.exe(9180)

User: NTDEV\markruss

Started: 1:42:12 PM 8/27/2011 Image: 64-bit

Comment:

Data Execution Protection (DEP) Status: DEP

Address Space Load Randomization: Enabled

This dialog provides detailed process information, much of which can be useful when investigating malware. Process information is arranged on a number of tabs, including:

- **Image.** This tab displays information about the executable file that launched the process, including the path to the file, the command-line argument used to launch it, the user account under which it is running, the creation time of the file, and the time the process was started.

- **Services.** This tab provides detailed information about the services registered in the process. This information includes the name used to identify the service in the registry, the display name of the service, an optional description, and (for Svchost.exe DLLs) the DLL path.

- **Strings.** This tab lists any Unicode strings found in the executable file. Look for suspicious URLs, names, or debug strings—malware binaries are often "signed" by their creators, or include URLs for command-and-control (C&C) or download servers. Process Explorer allows you to view strings in the file's address space in memory as well as on disk, which can be helpful in the investigation of packed files. (Strings.exe, another Sysinternals utility, provides a command-line interface for extracting strings from a file.) Clicking the **Memory** option button causes Process Explorer to list the strings visible in the file's memory mapping, which can reveal strings that might be encrypted in the on-disk version of the file.

### Image Verification

A malware author who takes the trouble to do so can easily add the name of a legitimate company, such as Microsoft, to the Company field of an executable file. Therefore, to provide assurance that their products are genuine, legitimate software vendors digitally sign most of the program files they publish. A digital signature can be used to verify that a file has been signed by the vendor using a private key and that the file has not been modified since being signed.

Process Explorer allows you to automatically verify the signature of a signed executable or DLL file. By default, verification is performed only on demand, and can be performed for individual files or for all running processes. In the **Properties** dialog for both processes and DLLs, the **Image** tab contains a **Verify** button that can be used to verify the digital signature for the associated file. Clicking the button causes Process Explorer to check the Certificate Revocation List (CRL) for the certificate to ensure that it is valid, and to check the cryptographic hash of the file to verify that it has not been tampered with since being signed. (Validating certificates requires reconnecting the computer to the Internet, which should only be considered if the risk of additional exfiltration or infection is low.)

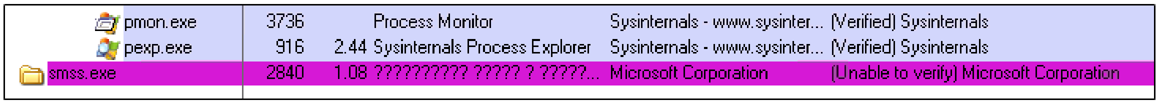
To configure Process Explorer to automatically verify the signatures for all running processes and files, click the **Options** menu, and then click **Verify Image Signatures**.

The Verified Signer field, which displays next to the file icon in the **Properties** dialog and as a column that can be shown in the process list and DLL View, indicates the status of any signature check that has been performed. If Process

Explorer is able to verify the signature, the field displays “(Verified)”, followed by the subject name from the certificate. (Note that the name on the signing certificate might not be the same as the name in the Company Name field. For example, most executable files that ship as part of Windows display “Microsoft Corporation” as the company name but are signed with a “Microsoft Windows” certificate.)

If signature verification has not been attempted, or if the selected file is not an executable file type, the field is blank or displays “(Not verified)” followed by the company name from the file’s version resource. “(Unable to verify)” followed by the company name indicates that the file is not signed or that a signature check has failed. You can also use the command-line Sysinternals Sigcheck tool to verify signatures on specific files as well as view detailed version information and their MD5, SHA1, and SHA256 hashes.

Figure 66. Autorun.A, masquerading as a system process but failing signature verification



| | | | | | |
|---|---|---|---|---|---|
| pmon.exe | 3736 | | Process Monitor | Sysinternals - www.sysinter... | (Verified) Sysinternals |
| pexp.exe | 916 | 2.44 | Sysinternals Process Explorer | Sysinternals - www.sysinter... | (Verified) Sysinternals |
| smss.exe | 2840 | 1.08 | ?????????? ????? ? ?????... | Microsoft Corporation | (Unable to verify) Microsoft Corporation |

## Investigating Loaded Drivers

Some malicious files are designed to load as device drivers, so it’s important to investigate drivers as well. Click the **System** row in the process list to display all the currently loaded drivers in DLL View. From this display, you can inspect the same properties that are available for DLLs and other files, such as the path to the driver file, the verified signer, strings found in the file on disk or in memory, and so on.

When investigating a 64-bit installation of Windows, note that two drivers, Hal.dll and Ntoskrnl.exe, are highlighted in purple, the color used to indicate packed files. These two files are actually not packed, but they exhibit some of the characteristics Process Explorer uses to classify files as compressed or encrypted. By itself, the fact that these two drivers are highlighted should not be considered evidence of infection.

In addition to Process Explorer, a number of utilities ship with Windows that can be used to provide different views of running processes:

- The System Information tool provides information about system drivers, including name, description, path and file name, driver type, and more. To run System Information:

  - In Windows XP, click **Start**, click **Run**, type **msinfo32.exe**, and then press Enter.
  - In Windows Vista, click **Start**, click in the **Start Search** box, type **msinfo32.exe**, and then press Enter.
  - In Windows 7, click **Start**, click in the **Search programs and files** box, type **msinfo32.exe**, and then press Enter.

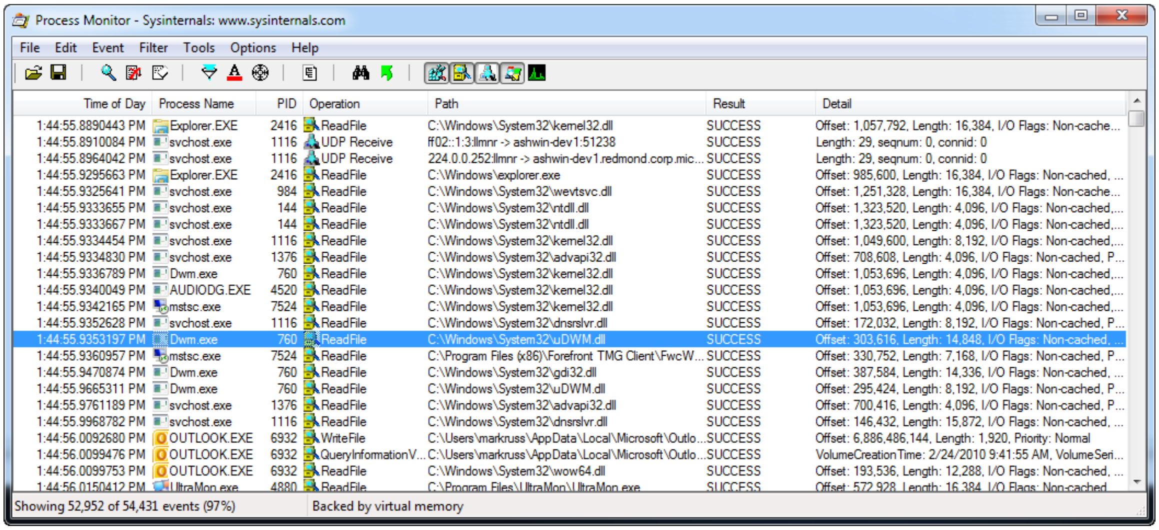
  To display the list of system drivers, in the navigation pane, click **Software Environment**, and then click **System Drivers**.

- Sc.exe is a command line program used to communicate with the Service Control Manager and services. To display a list of drivers, at the command prompt type **sc query type= driver** and press Enter.
- In Device Manager, click the **View** menu, and then click **Show Hidden Devices** to display a list of devices that are normally hidden from view.

## Tracing Malware

The list of active processes on a typical computer changes constantly, which can sometimes make it difficult to spot suspicious activity. In fact, if a malicious process starts and exits faster than Process Explorer's refresh rate, it may never show up in Process Explorer at all. You can use another Sysinternals tool, Process Monitor, to examine events in detail, including error messages and short-lived processes.

Figure 67. The Process Monitor main window



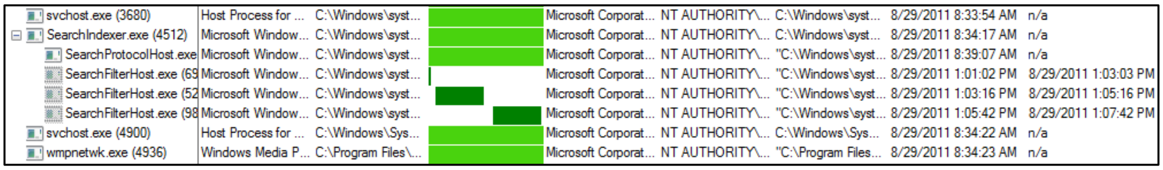
| Time of Day | Process Name | PID | Operation | Path | Result | Detail |
|---|---|---|---|---|---|---|
| 1:44:55.8890443 PM | Explorer.EXE | 2416 | ReadFile | C:\Windows\System32\kernel32.dll | SUCCESS | Offset: 1,057,792, Length: 16,384, I/O Flags: Non-cache... |
| 1:44:55.8910084 PM | svchost.exe | 1116 | UDP Receive | ff02::1:3:llmnr -> ashwin-dev1:51238 | SUCCESS | Length: 29, seqnum: 0, connid: 0 |
| 1:44:55.8964042 PM | svchost.exe | 1116 | UDP Receive | 224.0.0.252:llmnr -> ashwin-dev1.redmond.corp.mic... | SUCCESS | Length: 29, seqnum: 0, connid: 0 |
| 1:44:55.9295663 PM | Explorer.EXE | 2416 | ReadFile | C:\Windows\explorer.exe | SUCCESS | Offset: 985,600, Length: 16,384, I/O Flags: Non-cached, ... |
| 1:44:55.9325641 PM | svchost.exe | 984 | ReadFile | C:\Windows\System32\wevtsvc.dll | SUCCESS | Offset: 1,251,328, Length: 16,384, I/O Flags: Non-cache... |
| 1:44:55.9333655 PM | svchost.exe | 144 | ReadFile | C:\Windows\System32\ntdll.dll | SUCCESS | Offset: 1,323,520, Length: 4,096, I/O Flags: Non-cached,... |
| 1:44:55.9333667 PM | svchost.exe | 144 | ReadFile | C:\Windows\System32\ntdll.dll | SUCCESS | Offset: 1,323,520, Length: 4,096, I/O Flags: Non-cached,... |
| 1:44:55.9334454 PM | svchost.exe | 1116 | ReadFile | C:\Windows\System32\kernel32.dll | SUCCESS | Offset: 1,049,600, Length: 8,192, I/O Flags: Non-cached,... |
| 1:44:55.9334830 PM | svchost.exe | 1376 | ReadFile | C:\Windows\System32\advapi32.dll | SUCCESS | Offset: 708,608, Length: 4,096, I/O Flags: Non-cached, P... |
| 1:44:55.9336789 PM | Dwm.exe | 760 | ReadFile | C:\Windows\System32\kernel32.dll | SUCCESS | Offset: 1,053,696, Length: 4,096, I/O Flags: Non-cached,... |
| 1:44:55.9340049 PM | AUDIODG.EXE | 4520 | ReadFile | C:\Windows\System32\kernel32.dll | SUCCESS | Offset: 1,053,696, Length: 4,096, I/O Flags: Non-cached,... |
| 1:44:55.9342165 PM | mstsc.exe | 7524 | ReadFile | C:\Windows\System32\kernel32.dll | SUCCESS | Offset: 1,053,696, Length: 4,096, I/O Flags: Non-cached,... |
| 1:44:55.9352628 PM | svchost.exe | 1116 | ReadFile | C:\Windows\System32\dnsrslvr.dll | SUCCESS | Offset: 172,032, Length: 8,192, I/O Flags: Non-cached, P... |
| 1:44:55.9353197 PM | Dwm.exe | 760 | ReadFile | C:\Windows\System32\uDWM.dll | SUCCESS | Offset: 303,616, Length: 14,848, I/O Flags: Non-cached, ... |
| 1:44:55.9360957 PM | mstsc.exe | 7524 | ReadFile | C:\Program Files (x86)\Forefront TMG Client\FwcW... | SUCCESS | Offset: 330,752, Length: 7,168, I/O Flags: Non-cached, P... |
| 1:44:55.9470874 PM | Dwm.exe | 760 | ReadFile | C:\Windows\System32\gdi32.dll | SUCCESS | Offset: 387,584, Length: 14,336, I/O Flags: Non-cached, ... |
| 1:44:55.9665311 PM | Dwm.exe | 760 | ReadFile | C:\Windows\System32\uDWM.dll | SUCCESS | Offset: 295,424, Length: 8,192, I/O Flags: Non-cached, P... |
| 1:44:55.9761189 PM | svchost.exe | 1376 | ReadFile | C:\Windows\System32\advapi32.dll | SUCCESS | Offset: 700,416, Length: 4,096, I/O Flags: Non-cached, P... |
| 1:44:55.9968782 PM | svchost.exe | 1116 | ReadFile | C:\Windows\System32\dnsrslvr.dll | SUCCESS | Offset: 146,432, Length: 15,872, I/O Flags: Non-cached, ... |
| 1:44:56.0092680 PM | OUTLOOK.EXE | 6932 | WriteFile | C:\Users\markruss\AppData\Local\Microsoft\Outlo... | SUCCESS | Offset: 6,886,486,144, Length: 1,920, Priority: Normal |
| 1:44:56.0099476 PM | OUTLOOK.EXE | 6932 | QueryInformationV... | C:\Users\markruss\AppData\Local\Microsoft\Outlo... | SUCCESS | VolumeCreationTime: 2/24/2010 9:41:55 AM, VolumeSeri... |
| 1:44:56.0099753 PM | OUTLOOK.EXE | 6932 | ReadFile | C:\Windows\System32\wow64.dll | SUCCESS | Offset: 193,536, Length: 12,288, I/O Flags: Non-cached, ... |
| 1:44:56.0150412 PM | UltraMon.exe | 4880 | ReadFile | C:\Program Files\UltraMon\UltraMon.exe | SUCCESS | Offset: 572,928, Length: 16,384, I/O Flags: Non-cached |

Showing 52,952 of 54,431 events (97%) Backed by virtual memory

Process Monitor records many different kinds of activity as it runs; each row represents a specific event. Events tracked by Process Monitor include process starts and exits, thread starts and exits, network events, registry events, and many more. Each row gives a selection of information about the associated process, such as the operation performed, the path to the associated file or registry key, time information, and additional details.

To see short-lived processes in Process Monitor, open the Process Tree window by clicking the **Tools** menu and then clicking **Process Tree**, or by pressing Ctrl+T. The Process Tree window displays a list of all processes that have run since Process Monitor was launched, including processes that have exited.

Figure 68. The Process Tree View in Process Monitor shows details for current and exited processes

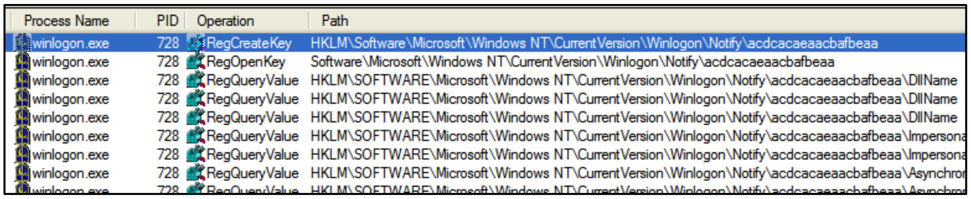


| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| svchost.exe (3680) | Host Process for ... | C:\Windows\syst... | 🟩 | Microsoft Corporat... | NT AUTHORITY\... | C:\Windows\syst... | 8/29/2011 8:33:54 AM | n/a |
| ⊟ SearchIndexer.exe (4512) | Microsoft Window... | C:\Windows\syst... | 🟩 | Microsoft Corporat... | NT AUTHORITY\... | C:\Windows\syst... | 8/29/2011 8:34:17 AM | n/a |
| SearchProtocolHost.exe | Microsoft Window... | C:\Windows\syst... | 🟩 | Microsoft Corporat... | NT AUTHORITY\... | "C:\Windows\syst... | 8/29/2011 8:39:07 AM | n/a |
| SearchFilterHost.exe (69 | Microsoft Window... | C:\Windows\syst... | 🟩 | Microsoft Corporat... | NT AUTHORITY\... | "C:\Windows\syst... | 8/29/2011 1:01:02 PM | 8/29/2011 1:03:03 PM |
| SearchFilterHost.exe (52 | Microsoft Window... | C:\Windows\syst... | 🟩 | Microsoft Corporat... | NT AUTHORITY\... | "C:\Windows\syst... | 8/29/2011 1:03:16 PM | 8/29/2011 1:05:16 PM |
| SearchFilterHost.exe (98 | Microsoft Window... | C:\Windows\syst... | 🟩 | Microsoft Corporat... | NT AUTHORITY\... | "C:\Windows\syst... | 8/29/2011 1:05:42 PM | 8/29/2011 1:07:42 PM |
| svchost.exe (4900) | Host Process for ... | C:\Windows\Sys... | 🟩 | Microsoft Corporat... | NT AUTHORITY\... | C:\Windows\Sys... | 8/29/2011 8:34:22 AM | n/a |
| wmpnetwk.exe (4936) | Windows Media P... | C:\Program Files\... | 🟩 | Microsoft Corporat... | NT AUTHORITY\... | "C:\Program Files... | 8/29/2011 8:34:23 AM | n/a |

Double-clicking a row displays a **Properties** dialog with all of the available information about the event, including the *call stack*—the hierarchical list of nested function calls that led to the event. By examining the call stack of a malicious event, you can determine which function directly invoked it, which may alert you to the presence of additional malware. You can integrate Process Monitor with Debugging Tools for Windows, which are available for download at no charge from the Microsoft Download Center, to make it easier to interpret the function calls in the stack.

Figure 69 shows events generated by a variant of the worm family Win32/Swimnag, in the form of repeated queries of a registry key with a suspicious name. The DllName value of the suspicious key points to a malicious file in the system32 directory.

Figure 69. Malicious events in Process Monitor



| Process Name | PID | Operation | Path |
|---|---|---|---|
| winlogon.exe | 728 | RegCreateKey | HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\acdcacaeaacbafbeaa |
| winlogon.exe | 728 | RegOpenKey | Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\acdcacaeaacbafbeaa |
| winlogon.exe | 728 | RegQueryValue | HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\acdcacaeaacbafbeaa\DllName |
| winlogon.exe | 728 | RegQueryValue | HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\acdcacaeaacbafbeaa\DllName |
| winlogon.exe | 728 | RegQueryValue | HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\acdcacaeaacbafbeaa\DllName |
| winlogon.exe | 728 | RegQueryValue | HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\acdcacaeaacbafbeaa\Imperson |
| winlogon.exe | 728 | RegQueryValue | HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\acdcacaeaacbafbeaa\Imperson |
| winlogon.exe | 728 | RegQueryValue | HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\acdcacaeaacbafbeaa\Asynchro |
| winlogon.exe | 728 | RegQueryValue | HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\acdcacaeaacbafbeaa\Asynchro |

For more information, visit the Process Monitor page at technet.microsoft.com/sysinternals/bb896645.

## Step 3: Terminate Malicious Processes

After you locate the malicious processes, record the full path to each malicious file so you can remove them after terminating their processes.

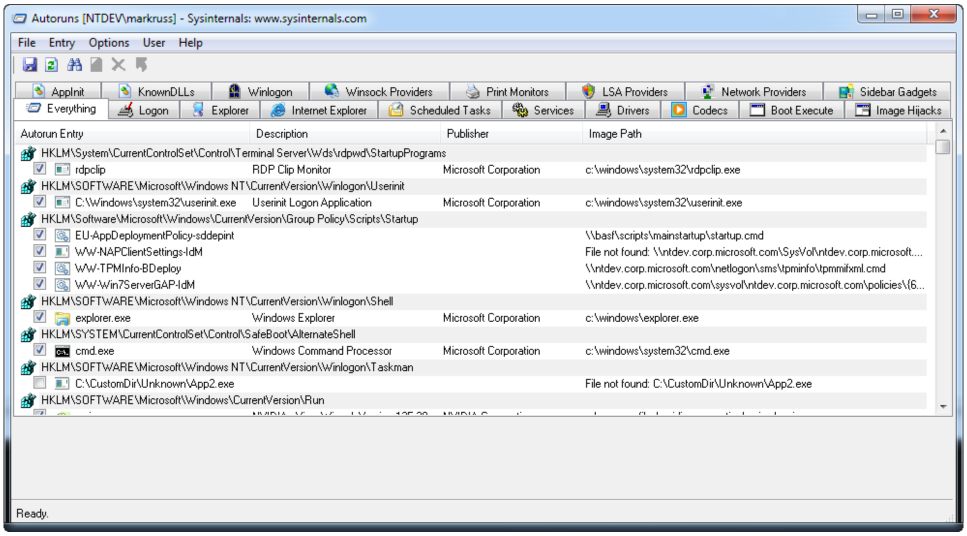
In an effort to resist removal, many malware infections include multiple processes, each of which monitors the others and restarts them when they are terminated. Instead of simply terminating malicious processes one by one, therefore, begin by suspending each process you've identified, and then terminate all of them. (Note that suspending Svchost.exe and other core system processes might cause parts of the system to become nonresponsive.) To suspend a process in Process Explorer, click the appropriate row in the process list, click the **Process** menu, and then click **Suspend**.

When terminating processes, watch for any newly started or restarted processes in the list (identified by green highlighting). If terminating malicious processes causes others to restart, it could be an indication that you're overlooking one or more sources of infection.

## Step 4: Identify and Delete Malware Autostarts

Malware persists on an infected computer by configuring itself to run when Windows starts, or when a user logs in. The System Configuration utility (Msconfig.exe, sometimes called “Msconfig”) that ships with Windows displays a list of programs that load at startup, among other information. Although this utility can be useful for general troubleshooting purposes, Msconfig is often inadequate for dealing with a malware infection: it doesn’t check all of the *autostart extensibility points* (ASEPs), or the places that processes can automatically start from, and it doesn’t provide certain information that can be useful when investigating an infection. A better malware detection tool than Msconfig is another Sysinternals tool, Autoruns.

Figure 70. Autoruns shows which programs run when Windows starts



| Autorun Entry | Description | Publisher | Image Path |
|---|---|---|---|
| HKLM\System\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\StartupPrograms | | | |
| ☑ rdpclip | RDP Clip Monitor | Microsoft Corporation | c:\windows\system32\rdpclip.exe |
| HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit | | | |
| ☑ C:\Windows\system32\userinit.exe | Userinit Logon Application | Microsoft Corporation | c:\windows\system32\userinit.exe |
| HKLM\Software\Microsoft\Windows\CurrentVersion\Group Policy\Scripts\Startup | | | |
| ☑ EU-AppDeploymentPolicy-sddepint | | | \\basf\scripts\mainstartup\startup.cmd |
| ☑ WW-NAPClientSettings-IdM | | | File not found: \\ntdev.corp.microsoft.com\SysVol\ntdev.corp.microsoft.... |
| ☑ WW-TPMInfo-BDeploy | | | \\ntdev.corp.microsoft.com\netlogon\sms\tpminfo\tpmmifxml.cmd |
| ☑ WW-Win7ServerGAP-IdM | | | \\ntdev.corp.microsoft.com\sysvol\ntdev.corp.microsoft.com\policies\{6... |
| HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell | | | |
| ☑ explorer.exe | Windows Explorer | Microsoft Corporation | c:\windows\explorer.exe |
| HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell | | | |
| ☑ cmd.exe | Windows Command Processor | Microsoft Corporation | c:\windows\system32\cmd.exe |
| HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Taskman | | | |
| ☐ C:\CustomDir\Unknown\App2.exe | | | File not found: C:\CustomDir\Unknown\App2.exe |
| HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run | | | |

### Using Autoruns

When you launch Autoruns, it immediately begins filling its display with entries collected from known ASEPs. Each shaded row represents an ASEP location in either the file system or the registry. The rows beneath a shaded row indicate entries configured in that ASEP. Each row shows the item’s description, publisher, and path. Click a row to display more information about the item at the bottom of the Autoruns window, including file size, version number, and any command-line arguments used to launch the item. Double-clicking an item in the list displays the item in either Regedit or an Explorer window, depending on whether the item is a registry entry or a file on disk. For registry entries, you can also open the folder that contains the file associated with the selected entry by clicking the **Entry** menu and then clicking **Jump to**.

On most computers, Autoruns is likely to display hundreds of entries for startup items. To reduce the number of items you have to investigate, enable the **Hide Microsoft and Windows Entries** and **Verify Code Signatures** items in the **Options** menu, and then click **Refresh** on the toolbar to filter out items with verified Microsoft signatures.

Autoruns can also be used to display autostart entries for other profiles, and for offline computers (for example, an offline virtual machine, or a physical computer booted into a preloader environment with Autoruns installed). To display entries for another profile, click the **User** menu, and then click the user account you want to check. To check an offline computer, click the **File** menu, and then click **Analyze Offline System**.

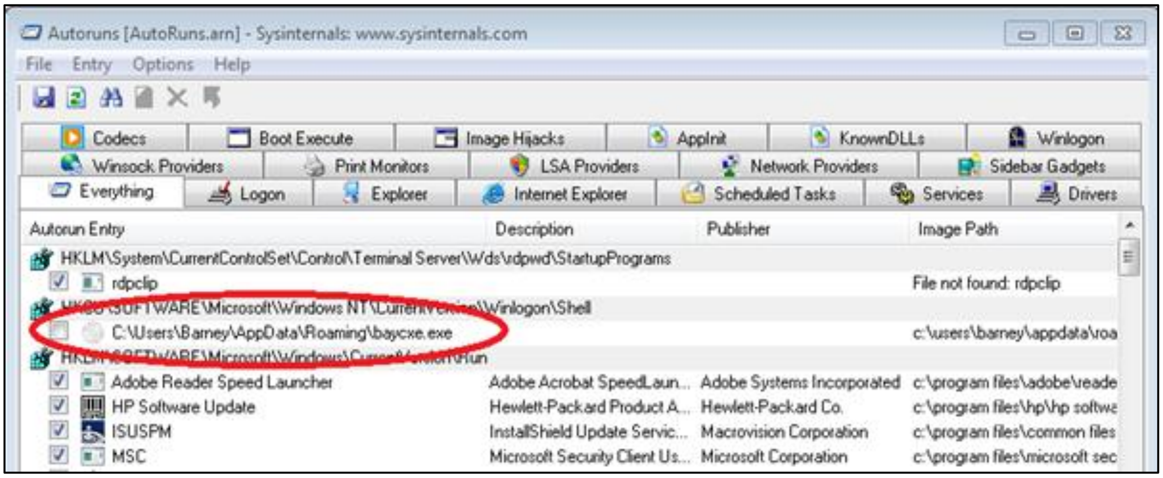
The Autoruns download package includes a command-line version of the tool, Autorunsc.exe. See technet.microsoft.com/sysinternals/bb963902 for usage instructions.

### Identifying Malware Autostarts

Suspicious autostart items can often be identified by many of the same characteristics listed on page 97: look for files with no icon, entries with blank Description and Publisher fields, files with unusual or random-seeming names, files that can't be verified, and files in unexpected locations, among others. To quickly search for information about a filename online, click the **Entry** menu and then click **Search Online**, or press Ctrl+M.

Figure 71 shows a malicious autostart entry created by a variant of Win32/FakePAV, a rogue security software program. This entry has blank Description and Publisher fields, has a random-seeming name with no obvious meaning, and comes from a location in the registry that usually points to Explorer.exe.

Figure 71. A malicious entry in Autoruns



| Autorun Entry | Description | Publisher | Image Path |
|---|---|---|---|
| HKLM\System\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\StartupPrograms | | | |
| ☑ rdpclip | | | File not found: rdpclip |
| HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell | | | |
| □ C:\Users\Barney\AppData\Roaming\baycxe.exe | | | c:\users\barney\appdata\roa |
| HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run | | | |
| ☑ Adobe Reader Speed Launcher | Adobe Acrobat SpeedLaun... | Adobe Systems Incorporated | c:\program files\adobe\reade |
| ☑ HP Software Update | Hewlett-Packard Product A... | Hewlett-Packard Co. | c:\program files\hp\hp softwa |
| ☑ ISUSPM | InstallShield Update Servic... | Macrovision Corporation | c:\program files\common files |
| ☑ MSC | Microsoft Security Client Us... | Microsoft Corporation | c:\program files\microsoft sec |

### Deleting Autostarts

To delete a selected autostart entry, click the **Entry** menu and then click **Delete**, or press Ctrl+D. To disable an entry without deleting it, clear the check box at the left end of the row. Before deleting any entries, record the full path to each malicious file, so you can remove them later.

After deleting or disabling suspicious autostarts, refresh the list by clicking the **Refresh** button on the toolbar or pressing F5. If you overlooked any malicious processes, they may monitor the autostart list and recreate any entries you delete. If this happens, return to Step 2 and use Process Explorer and Process Monitor to find and eliminate the responsible processes.

## Step 5: Delete Malware Files

After terminating malicious processes and deleting autostart entries, the next step is to remove the malicious files themselves by visiting the file locations you recorded during the investigation, locating the malicious files, and deleting them.

## Steps 6 and 7: Reboot and Repeat

To verify that you've eliminated the malware, reboot the computer and start the process over with step 1. Some malware families expend considerable effort to avoid detection, and repeating the investigation process a few times may help you uncover malicious processes and files that you missed earlier.

## Conclusion

Unfortunately, the process of eliminating malware from a computer is likely to become much harder in the next few years. Malware has become a lucrative business for the criminals who create and distribute it, and they have a financial incentive to find new ways to evade detection and make malicious files and processes harder to remove.

Therefore, understanding how malware spreads, operates, and defends itself at a fundamental level should be considered a prerequisite for IT professionals charged with protecting their users from attack and containing outbreaks when they occur. However, the best guidance is that which helps prevent malware infection from ever occurring. For more information about how to prevent malware infection, see the Microsoft Malware Protection Center at www.microsoft.com/security/portal.