

SOLUTION **ACCELERATORS**

Act faster. Go further.

Malware Removal Starter Kit

How to Combat Malware Using Windows PE

Version 1.0

Published: July 2007

For the latest information, please see

microsoft.com/technet/SolutionAccelerators

Microsoft

Copyright © 2007 Microsoft Corporation. All rights reserved. Complying with the applicable copyright laws is your responsibility. By using or providing feedback on this documentation, you agree to the license agreement below.

If you are using this documentation solely for non-commercial purposes internally within YOUR company or organization, then this documentation is licensed to you under the Creative Commons Attribution-NonCommercial License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc/2.5/> or send a letter to Creative Commons, 543 Howard Street, 5th Floor, San Francisco, California, 94105, USA.

This documentation is provided to you for informational purposes only, and is provided to you entirely "AS IS". Your use of the documentation cannot be understood as substituting for customized service and information that might be developed by Microsoft Corporation for a particular user based upon that user's particular environment. To the extent permitted by law, MICROSOFT MAKES NO WARRANTY OF ANY KIND, DISCLAIMS ALL EXPRESS, IMPLIED AND STATUTORY WARRANTIES, AND ASSUMES NO LIABILITY TO YOU FOR ANY DAMAGES OF ANY TYPE IN CONNECTION WITH THESE MATERIALS OR ANY INTELLECTUAL PROPERTY IN THEM.

Microsoft may have patents, patent applications, trademarks, or other intellectual property rights covering subject matter within this documentation. Except as provided in a separate agreement from Microsoft, your use of this document does not give you any license to these patents, trademarks or other intellectual property.

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious.

Microsoft, Windows, BitLocker, Internet Explorer, Windows Live, and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

You have no obligation to give Microsoft any suggestions, comments or other feedback ("Feedback") relating to the documentation. However, if you do provide any Feedback to Microsoft then you provide to Microsoft, without charge, the right to use, share and commercialize your Feedback in any way and for any purpose. You also give to third parties, without charge, any patent rights needed for their products, technologies and services to use or interface with any specific parts of a Microsoft software or service that includes the Feedback. You will not give Feedback that is subject to a license that requires Microsoft to license its software or documentation to third parties because we include your Feedback in them.

Overview

Many small- and medium-sized organizations use antivirus software, and yet new viruses, worms, and other forms of malicious software (*malware*) continue to infect large numbers of computers in these organizations. Malware proliferates at alarming speed and in many different ways, which makes it particularly widespread today.

This guide is intended for IT Generalists who want information and recommendations that they can use to effectively address and limit malware that infects computers in small- and medium-sized organizations. This guidance provides a set of tasks that licensed Windows® users can perform at no cost to create the Malware Removal Starter Kit. Recommendations for free malware-scanning tools are included. You can use these tools in combination with the kit to conduct scans, detect problems, and remove malware from your computer.

This guidance includes the following sections:

- [Overview](#)
- [Planning Your Response](#)
- [How to Determine if You Have a Problem](#)
- [Dealing with an Infection](#)
- [Summary](#)

Note The guidance for this kit is intended for use with other anti-malware tools. This kit is not a replacement for other malware prevention methods.

Malware Threats

The first step toward containing the spread of malware is to understand the various technologies and techniques that malware authors can use to attack your computer. Malware threats directly target both users and computers. However, it is also important to know that the majority of threats come from malware that targets the user rather than the computer. If a user with administrator-level user rights can be tricked into launching an attack, the malicious code has more power to perform its tasks. Such an attack can frequently cause more damage than one that has to rely on a security hole or vulnerability in an application or the operating system.

The "Planning Your Response" section of this starter kit focuses on the ways in which your computer can be at risk to malware attacks, and how you can prepare to address a malware attack by using the Windows Preinstallation Environment (Windows PE) kit that this guidance recommends in combination with other free anti-malware programs.

Note The recommendations and prescriptive information in this guidance are not intended for complex environments that require Infrastructure Specialists. For more comprehensive information about this subject, see the [Antivirus Defense-in-Depth Guide](#).

How Does Malware Get In?

Malware uses many different methods to try and replicate among computers. The following table lists common malware threats to organizations and provides examples of tools that you can use to mitigate them.

Table 1: Malware Threats and Mitigations

Threat	Description	Mitigation
E-mail	E-mail is the transport mechanism of choice for many malware attacks.	<ul style="list-style-type: none"> • Spam filters • Real-time antivirus and antispayware scanners • User education
Phishing	Phishing attacks try to trick people into revealing personal details such as credit card numbers or other financial or personal information. Although these attacks are rarely used to deliver malware, they are a major security concern because of the information that may be disclosed.	<ul style="list-style-type: none"> • Spam filters • Pop-up blockers • Antiphishing filters • User education
Removable media	This threat includes floppy disks, CD-ROM or DVD-ROM discs, Zip drives, USB drives, and memory (media) cards, such as those used in digital cameras and mobile devices.	<ul style="list-style-type: none"> • Real-time antivirus and antispayware scanners • User education
Internet downloads	Malware can be downloaded directly from Internet Web sites such as social networking sites.	<ul style="list-style-type: none"> • Browser security • Real-time antivirus and antispayware scanners • User education
Instant messaging	Most instant messaging programs let users share files with members of their contact list, which provides a means for malware to spread. In addition, a number of malware attacks have targeted these programs directly.	<ul style="list-style-type: none"> • Real-time antivirus and antispayware scanners • Personal firewall • Restrict unauthorized programs • User education

Threat	Description	Mitigation
Peer-to-peer (P2P) networks	To start file sharing, the user first installs a client component of the P2P program through an approved network port, such as port 80. Numerous P2P programs are readily available on the Internet.	<ul style="list-style-type: none"> • Real-time antivirus and antispyware scanners • Restrict unauthorized programs • User education
File shares	A computer that is configured to allow files to be shared through a network share provides another transport mechanism for malicious code.	<ul style="list-style-type: none"> • Real-time antivirus and antispyware scanners • Personal firewall • User education
Rogue Web sites	Malicious Web site developers can use the features of a Web site to attempt to distribute malware or inappropriate material.	<ul style="list-style-type: none"> • Browser security • Pop-up blockers • Antiphishing filters • User education
Remote exploit	Malware might attempt to exploit a particular vulnerability in a service or application to replicate itself. Internet worms often use this technique.	<ul style="list-style-type: none"> • Security updates • Personal firewall
Network scanning	Malware writers use this mechanism to scan networks for vulnerable computers that have open ports or to randomly attack IP addresses.	<ul style="list-style-type: none"> • Software updates • Personal firewall
Dictionary attack	Malware writers use this method of guessing a user's password by trying every word in the dictionary until they are successful.	<ul style="list-style-type: none"> • Strong password policy • User education

From a security perspective, it would seem best to block all these malware transport methods, but this would significantly limit the usefulness of the computers in your organization. It is more likely that you will need to allow some or all of these methods, but also to restrict them. There is no single anti-malware solution that will fit all organizations, so evaluate the computer requirements and risks for your organization, and then decide how best to defend against malware that attempts to exploit them.

Microsoft remains strongly committed to securing its software and services by working with partners to combat malware threats. Recent Microsoft efforts to reduce the impact of malware threats include:

- Developing defense tools such as Windows Defender, Microsoft Forefront, Windows Live™ OneCare safety scanner, the Malicious Software Removal Tool, and other resources available through the Windows Security Center. For more information about these and other security tools, see the [TechNet Security Center](#) or the [Security at Home](#) page on Microsoft.com.
- The [Microsoft Malware Protection Center](#) that provides the latest information on top desktop and e-mail threats to computers running Windows.
- The [Microsoft Security Response Alliance](#), which provides information about the Microsoft Virus Initiative (MVI), the Virus Information Alliance (VIA), and other member organizations.
- Supporting legislation to eliminate spam and working with law enforcement officials and Internet service providers (ISPs) to help prosecute spam operations. For information about an alliance dedicated to this effort, see [America Online, Microsoft and Yahoo! Join Forces Against Spam](#).

Planning Your Response

Planning cannot be considered complete until you have planned for the worst. If all your defenses are compromised by an attack, you need to ensure that the staff you work with know what to do. Your ability to mount a rapid response can make a big difference when an attack is severe.

As you plan your response, it is important to understand that overreacting to a malware problem can cause almost as much disruption as dealing with a real outbreak! Plan your response to be rapid but measured to minimize its effect on coworkers.

Create an Incident Response Plan

Creating an incident response plan that describes what should happen in the event of a suspected malware outbreak is an important preparation step for your organization. The plan should help instruct all affected staff on the best course of action when a malware outbreak occurs. It should aim to minimize the impact of the attack and communicate a documented incident response process that staff can follow. For example, a well-designed plan would be capable of managing the sequence of events for a typical incident such as the following:

1. A staff member calls an in-house support resource after noticing something strange appear on her computer screen.
2. The support resource checks the computer and calls a support number.
3. A support technician responds to complete a short diagnostic test, and then either cleans or rebuilds the system depending in the severity of the problem.

The entire response process could take hours to complete, so having a plan in place that helps minimize the risk of the malware spreading further until the process is complete is

important. For example, if the support resource is trained to run antivirus software on the computer and then remove the network cable from the suspect computer until a support technician arrives, this initial response eliminates the chance of the computer infecting other computers.

When planning your incident response plan, there are typically two scenarios that you need to consider:

- **Individual infection.** This scenario, which is by far the most common, occurs when malware infects a single computer.
- **Mass outbreak.** This scenario is thankfully much less common. A mass outbreak has the potential to cause serious disruption in the organization. Typically this scenario will only become apparent after the staff reports a number of individual infections that have similar symptoms.

Your incident response plan can cover both of these scenarios because the response process for an outbreak is an extension of the response to an individual infection. Typically the outbreak response will require you to temporarily isolate the organization's network to stop the attack from spreading further, and to give the support staff time to clean the infected systems. In some cases, it may be necessary to notify the network administrator or the person performing that role to change the firewall or router settings before the computers in the organization can be reconnected to the network. For example, if the malware uses a specific network port to infect computers, blocking this port at the firewall can prevent re-infection while allowing other network communications to continue.

Important If you still detect the presence of malware after using the kit to clean your computer, we recommend turning the computer off and not using it for five to 10 business days, or until your antivirus provider issues a virus signature update. You can then use the kit to download the latest signature files and rescan your computer to more effectively address the problem.

For more information about how to organize and develop an incident response plan, see the following resources:

- The [Antivirus Defense-in-Depth Guide](#).
- The [Responding to IT Security Incidents](#) page on Microsoft TechNet.
- Chapter 3, "Understanding the Security Risk Management Discipline" of the [Securing Windows 2000 Server Guide](#) for incident response information only.
- The [Service Management Functions Incident Management](#) section of the [Microsoft Operations Framework \(MOF\)](#).
- The [Windows Security Resource Kit](#), Second Edition from Microsoft Press.

Prepare a Kit for Offline Scanning

This section provides recommendations, support specifications, and a short set of tasks and instructions that you can use to prepare a Windows Preinstallation Environment (Windows PE) kit. You can then combine the kit with a set of tools to conduct offline scans for malware on the computers in your organization.

Windows PE provides powerful preparation and installation tools for Windows operating systems. With Windows PE, you can start Windows from a removable disk, which provides resources to troubleshoot Windows on the client computer. For more information about Windows PE, download the [Windows Preinstallation Environment Technical Overview](#).

Unsupported Tools and Technologies

Windows PE does not support the following tools and technologies:

- Internet Explorer® 7.
- Applications that use Microsoft Windows Installer (.msi files).

Prerequisites

The following are operating system and feature requirements for preparing a Windows PE kit:

- Windows Vista® or Windows XP® with Service Pack 2 (SP2).
- DVD burner and software to write to a CD-ROM.
- 992 MB of free space on the computer's hard drive disk to download the Windows PE .img file.

Note An additional 800 MB of space is required for the boot image on drive C of the computer when using the default script for the kit.

- Microsoft .NET Framework version 2.0 and MSXML to run Windows Installer.

You can use the following resources to meet these requirements:

- [Microsoft .NET Framework Version 2.0 Redistributable Package \(x86\)](#).
- [Microsoft Core XML Services \(MSXML\) 6.0](#).

For more information about 32-bit and 64-bit system requirements, see the:

- [Windows Preinstallation Environment Overview](#).

Task Overview

Complete the following tasks to prepare your Malware Removal Starter Kit to conduct offline scans:

- Task 1: Install the Windows Automated Installation Kit (AIK)
- Task 2: Download the malware-scanning tools and utilities
- Task 3: Create the Malware Removal Starter Kit CD-ROM
- Task 4: Use the Malware Removal Starter Kit to scan your computer

Task 1: Install the Windows Automated Installation Kit (AIK)

The first task in this process is to obtain the Windows Automated Installation Kit (AIK). This kit includes Windows PE and other files for you to install on your computer. The kit installs by default as an image (*.img) file on any system drive that you choose.

Note The AIK supports both Windows Vista and Windows XP SP2.

To install the AIK on your computer:

1. Download the AIK from the [Windows Automated Installation Kit \(AIK\)](#) page on the Microsoft Download Center.
Note The size of .img file for the AIK is 992 megabytes (MB). For this reason, you may require extended time to download the file, depending on your connection speed to the Microsoft Download Center.
2. Burn the .img file for the AIK to a DVD.
Note If your DVD-burning software does not recognize ".img" files, in the **Save As** dialog for the download, expand the **Save as type** drop-down list, change the file type to **All Files** and the file name extension from **.img** to **.iso** and then retry burning the information to a DVD.
3. On the AIK DVD that you created, double-click **StartCD.exe** to install the AIK on your computer.

Task 2: Download the Malware-Scanning Tools and Utilities

You will need to identify the tools that you want to use with Windows PE to perform malware scans on your computer. Windows PE does not support tools that use .msi packages to install on your computer. In addition, the amount of random access memory (RAM) on your computer can constrain what scanning tools you can use.

There are a number of anti-malware tools available for free that require no installation that you can run as program files in the Windows PE environment. You can also run these tools from a USB device.

Download the malware-scanning tools that you want to use to a temporary location on your computer.

Important Some anti-malware tools require network access to run. For this reason, only use anti-malware tools that are available to use offline when you use this guidance to create your Malware Removal Starter Kit CD-ROM. We recommend reading the installation instructions for all of the offline scanning tools that you choose to use. Some tools may not be compatible with all Windows operating systems.

At the time this guidance was written, the following tools ran with Windows PE on a computer running Windows XP SP2 or Windows Vista with at least 512 MB of RAM:

- [avast! Virus Cleaner](#) from Alwil Software. This tool is available for offline use. The signature files for the tool will be as current as the download date listed.
- [McAfee AVERT Stinger](#), a stand-alone virus scanner from McAfee. This tool is available for offline use. The signature files for the tool will be as current as the download date listed.
- [Malicious Software Removal Tool](#) from Microsoft. This tool is available for offline use. The signature files for the tool will be as current as the download date listed.
- [Spybot - Search & Destroy](#) from Spybot Search and Destroy.

Note Before you can use this tool, you must first install it on the computer you want to scan, and then download the latest signature file detection updates from Spybot. After the tool is installed, it will start by default from X:\Program Files\Spybot – Search & Destroy\spybotsd unless you specified a different path during the installation. The signature files for the tool will be as current as the download date listed. For more information about using this tool, see the [Tutorial](#) page of the Spybot Web site.

The following utilities are designed to help you manage your computer while you are in the process of removing malware from it:

- [Drive Manager](#) from the [Freeware Utilities by Alex Nolan](#) Web site. This tool identifies different drive types, such as hard drives, CD/DVD drives, USB drives, network drives, and lists their properties for analysis. This tool is available for offline use.
- [System Spec](#) from the [Freeware Utilities by Alex Nolan](#) Web site provides information about the current hardware on the computer. This tool may be useful if you are required to provide detailed information about the hardware while the computer is being serviced. This tool is available for offline use.

Task 3: Create the Malware Removal Starter Kit CD-ROM

Creating the Malware Removal Starter Kit CD-ROM requires you to produce a Windows PE image for the kit, modify the base Windows PE image by adding the tools to it, change the size of the disk cache to provide some additional space for RAM, and then build an .iso image file to burn the changed image to a CD-ROM. Periodically, you will need to download the latest virus signature updates for the offline scanning tools on the CD-ROM to keep them as effective as possible to detect malware.

Important After you start creating the Windows PE image, it is important to complete all of the steps in this task without interruption. If you have already downloaded the tools you plan to use, this process should take about 30 minutes to complete, depending on your system's performance and if you follow the steps in this task exactly as prescribed. You will need about 800 MB of free space on your C drive to complete this procedure. Ensure that you update all drive letter references as needed.

To create the Malware Removal Starter Kit CD-ROM:

1. Log on to the computer as an administrator, click **Start**, click **All Programs**, click **Microsoft Windows AIK**, and then click **Windows PE Tools Command Prompt**.
Note This step applies to Windows XP. If you are running Windows Vista on your computer, right-click **Windows PE Tools Command Prompt**, click **Run as administrator**, and then click **Continue**.
2. At the command prompt, type the following and then press ENTER to create a copy of the x86 image of Windows PE and set up a working folder directory on your computer:
copy x86 c:\WinPE
3. At the command prompt in the new directory c:\WinPE, type the following and then press ENTER to mount the WinPE.wim image so that you can change it:
imagex /mountrw winpe.wim 1 c:\WinPE\Mount
4. At the command prompt, type the following and then press ENTER to access the following registry subkey:
**reg load HKLM\WinPE_SYSTEM
c:\WinPE\Mount\windows\system32\config\system**
5. At the command prompt, type the following and then press ENTER to create a 96 MB disk cache of RAM:
**reg add HKLM\WinPE_SYSTEM\ControlSet001\Services\FBWF /v
WinPECacheThreshold /t REG_DWORD /d 96 /f**
6. At the command prompt, type the following and then press ENTER to exit this registry key:
reg unload HKLM\WinPE_SYSTEM
7. Create a directory for the malware-scanning tools under the Mount folder (for example, you could use the name "Tools" for this folder).
mkdir c:\WinPE\mount\Tools
8. Copy the tool files that you downloaded in Task 2 to the tools directory that you just created. Example:
copy <tools from the Task 2 directory> c:\WinPE\mount\Tools.
9. At the command prompt, type the following, press ENTER, and then type **Yes** and press ENTER again to continue the process:
peimg /prep c:\WinPE\Mount
10. At the command prompt, type the following and then press ENTER to save your changes:
imagex /unmount c:\WinPE\Mount /commit
11. At the command prompt, copy the following, press ENTER, and then type **Yes** to overwrite the existing file:
copy c:\WinPE\WinPE.wim c:\winpe\ISO\sources\boot.wim

- At the command prompt, type the following and then press ENTER to create an .iso file of the Windows PE image:

```
oscdimg -n -bc:\WinPE\etfsboot.com c:\WinPE\ISO c:\WinPE\WinPE_Tools.iso
```

- Burn the .iso file located at c:\WinPE\WinPE_Tools.iso to a CD-ROM and test the Windows PE image to verify that it runs all of the malware-scanning tools correctly.

Note You also can use [Microsoft Virtual PC 2007](#) to test the image.

The CD-ROM for your Malware Removal Starter Kit is now ready. If you require more frequent virus signature updates for your environment, we recommend maintaining the scanning tools you choose to use on a USB device to obtain the latest updates.

Task 4: Use the Malware Removal Starter Kit to Scan Your Computer

Now you are ready to use the Windows PE image and the tools you selected to scan your computer for malware.

To use the Windows PE CD-ROM and tools to scan your computer:

- Place the new CD-ROM in the computer's CD drive or DVD drive and then ensure that you start the computer from this drive according to your computer's startup order.

Option: Insert the USB device in a slot on the computer to ensure that the device is loaded when you start the operating system.

Note For more information about starting your computer from a Windows PE CD-ROM startup disk, see the [Windows Preinstallation Environment Overview](#) on Microsoft.com. This resource provides information about configuring your basic input/output system (BIOS) settings for the startup order of the computer, and other BIOS settings that may prevent you from starting the computer from the CD drive.

- Run the malware-scanning tools that you selected. If you used the default configuration information in Task 3 to build the Windows PE image, you will find the tools located at X:\Tools. You can run the listed tools by typing the name of the program file for each one at the command prompt.

Option: If you inserted a USB device to provide updated signatures or tools, and you are unsure of the drive letter that the USB device is using, you can determine the drive letter using Drive Manager, which is located at X:\Tools.

Note To run Spybot, refer to Spybot's installation instructions, and ensure that the definition program file runs after you install this tool on the computer.

Caution Running malware-scanning tools on an infected computer may damage the computer's ability to start properly. If key boot files are infected by malware, the cleaning process may prevent the operating system from working. For this reason, it is important to regularly back up all important information files on your computer. In addition, after restoring these files to the computer from your backup resource, we recommend rescanning the computer to detect any malware that may be present in your backup files.

How to Determine if You Have a Problem

Malware will often target a computer's operating system. The Windows operating system has been a significant target for a number of years due to its popularity. However, more recently malicious software that specifically targets other operating systems has been on the rise. In addition, many malware programs also target Microsoft and third-party applications, and in some cases even antivirus software. For these reasons, it is important to keep both the operating system and the applications that you use up to date.

Although most malware attacks are aimed at personal computers, they are not the only targets. Mobile devices such as personal digital assistants (PDAs), portable game systems, and even cell phones have become targets.

Some malware requires the installation of a particular application on the target computer before it can work. A huge number of Internet scams and phishing attacks have made the user of the computer a target to install such applications. In many cases it is easier to trick a user into running a piece of malware than it is to develop an automatic mechanism. For this reason it is important to invest time in training staff and managers to recognize likely Internet scams and phishing attempts.

Check for Performance Issues

Your computer should already have real-time antivirus and antispyware programs running on it to alert you with a message if they detect an infection. However, if you notice unusual behavior or your system slows down, at any time you can run a full system scan.

The following are a few primary performance issues that could indicate that your computer might be infected:

- Your computer runs more slowly than normal.
- Your computer often stops responding to program or system commands.
- Your computer fails and requires you to restart it frequently.
- Your computer restarts on its own and then fails to run normally.
- You cannot correctly run applications on your computer.
- You cannot access disks or disk drives on your computer.
- You cannot print correctly.
- You receive unusual error messages or popup windows.
- You see distorted menus and dialog boxes.
- Your Internet browser's home page unexpectedly changes.
- You cannot access administrator shares on the computer.
- You notice an unexplained loss of disk space.

Although this is not a complete list, it describes the types of unusual behavior that might suggest that malware is present on your computer. If you encounter any of these performance issues, you can run a full scan to better determine if you have a malware problem.

Note Not every computer that experiences these issues may have a malware problem. Misconfigured applications or software bugs can also cause such issues. To avoid false indications of a malware attack, ensure that your operating system and applications have the latest security updates and service packs, and that the computer has adequate RAM to run your applications.

Dealing with an Infection

In any organization, malicious software is an ever present threat. This section of the guide assumes that you have good reason to believe that an infection is present in your computer or other computers in your organization. You can use the 4-stage process that this section describes to help determine the nature of the problem, limit its spread, remove it using free malware-scanning tools from Microsoft and other third-party sources, verify that the malware is removed, and proceed with next steps as required.

Due to the changing nature of malware, no single antivirus or antispyware solution can guarantee to protect against all attacks. If, after following the stages in this section, you need more help with malware-related issues, contact Microsoft Product Support Services:

- For support within the United States and Canada, call toll-free (866) PCSAFETY (866) 727-2338.
- For support outside the United States and Canada, visit the "[Security Help and Support for IT Professionals](#)" Web page.

Stage 1: Initiate Your Response

As soon as you arrive at the computer that has the malware problem, if you cannot run antivirus software on the computer, disconnect the computer from the network, turn the computer off, and refer directly to "Stage 3, Run an Offline Scan Using the Kit."

Gather information. If possible, gather answers from the user who discovered the problem by asking the following questions:

- What happened when the problem started?
- How was the computer being used just prior to the problem?
- What (if anything) did the local antivirus program report?
- Does the computer contain any important data that is not backed up?
- What Web sites did the system recently visit?
- Are there processes running on the computer that are different from the standard processes?

After you have gathered as much information as you can about the infection, the next stage is to start the cleaning process.

Note It can be very helpful to obtain a list of suspicious process or file names that you can then research on the Internet to determine if they are malware.

Stage 2: Scan the Computer for Malware

Use the following steps in the prescribed order to most effectively use anti-malware software installed on the computer, and run online and offline scans for malware:

1. Run antivirus and antispyware software on the computer.
2. Run an online scan tool.
3. Run an online scan tool using the networked option in safe mode.

Step 1: Run Antivirus and Antispyware Software on the Computer

The method for launching a full scan of a computer for virus infections depends on the antivirus application. Check the program's Help resources to learn how to conduct a full virus scan.

Scanning for spyware is similar to scanning for viruses. Your computer should have real-time spyware-scanning software running on it. Windows Defender is available free of charge for computers running Windows XP. If you are running Windows Vista, Windows Defender is included with the operating system. To launch Windows Defender, click **Start**, click **All Programs**, click **Windows Defender** to open the program, and then click **Scan**. Allow the program to perform a full scan.

For more information about how Windows Defender works, see the [Windows Defender Technical Overview](#) on TechNet.

Step 2: Run an Online Scan Tool

Run an online scan, using a tool such as the [Windows Live OneCare safety scanner](#), to ensure that the computer has been checked against the latest antivirus and antispyware signatures, as well as other potentially unwanted software.

Other online scan software providers include:

- [Kaspersky Online Scanner](#)
- [McAfee FreeScan](#)
- [Symantec Security Check](#)
- [Trend Micro HouseCall](#)

In addition, several online software tools provide specialty scanning, such as [VIRUSTOTAL](#), which you can use to scan individual files for malware.

Step 3: Run an Online Scan Tool Using the Networked Option in Safe Mode

After completing an online scan, if you still suspect that malware is present on the computer, restart your computer in safe mode, and run the online scan again. After completing another online scan in safe mode, you can use offline scanning tools such as those that the guidance recommends using with this kit.

For more information about how to start your computer in safe mode, see:

- ["A description of the Safe Mode Boot options in Windows XP"](#): Microsoft Knowledge Base article 315222.
- [Advanced startup options \(including safe mode\)](#) for Windows Vista.

Stage 3: Run an Offline Scan Using the Kit

To use the Malware Removal Starter Kit, you start the computer from the CD-ROM, and then use offline scanning tools to repair the primary hard disk drive while it is "offline." In this way, you do not use the hard disk drive on the computer to start the computer or scan it. Running an online scan requires you to start the computer using the normal boot sequence, which loads files from the computer's hard disk drive that the operating system locks during this sequence. To access and remove malware that has altered or corrupted these normally locked system files requires using an offline process like the one this guidance prescribes.

Important You cannot scan a disk for malware if it has been encrypted with a tool such as BitLocker™, if the disk is managed as part of a RAID volume, or if the disk is damaged. In these cases or if you are unsure of the state of the disk, consult a specialist to determine its state.

Due to the ever-changing nature of malware, no process can be considered 100 percent effective for cleaning malware from a computer. The process described in the section, "Prepare a Kit for Offline Scanning," has been tested at Microsoft and should be considered a best effort solution. The tasks in the "Planning Your Response" section of this guidance provide instructions about how to create a Windows PE kit that uses free tools you can obtain online so that you can scan for malware on computers running Windows XP SP2 or Windows Vista in your organization.

Stage 4: Next Steps

If, after using the guidance in this kit, malware appears to still be compromising the computer, you may choose to use System Restore to return the computer to a known good state. System Restore takes a "snapshot" of critical system files and some program files, and saves this information at a Restore Point on the computer's hard disk drive. You can then use the Restore Point to return the operating system to a previous state. For more information about System Restore, see the following resources:

- [How to restore the operating system to a previous state in Windows XP](#).
- [Windows Backup and Restore Center](#) for Windows Vista.

If, at this point, the computer still shows signs of malicious software-related issues, you have two options:

- Get specialized help.
- Rebuild the computer.

If the malicious software has managed to avoid the malware-scanning capabilities of the Windows PE kit that this guide prescribes, it is very likely that you will need to seek specialized help to remove the malware. Because specialized help is likely to require time and money, a quicker and cheaper option is usually to delete the files on the hard drive of the computer, and then reinstall the operating system and software programs.

If you choose to rebuild the computer, ensure that you only use trusted media for that process. Rebuild the computer, and ensure that all updates and antivirus software is applied to the computer before bringing it back on to the network in case a virus is still propagating.

Summary

This aim of the Malware Removal Starter Kit is to provide reactive guidance and prescriptive steps to help you recover a computer that has been exposed to malicious software. It is important to understand that no process can guarantee a full recovery from the damage that malicious software can do. For this reason, there is no substitute for solid defenses and reliable backup and recovery processes. In this way, if the worst does happen and you have to rebuild the computer, the impact will be minimized.

If you do use the recovery steps in this guide, we recommend spending some time after the computer is fixed to investigate how the malicious software was introduced to it. This effort should attempt to learn how the problem was introduced rather than trying to find something or someone to blame. If the weakness was with a technical defense measure, such as a firewall or antivirus program, you can review it and update the measure as required. If the problem was introduced because of the actions of staff, additional training may be required to ensure the problem is not repeated. Remember the golden rule: "Prevention is better than cure."

Finally, while this guide is specifically written to help IT Generalists repair computers attacked by malware in small- to medium-sized organizations, much of this information is valuable for protecting the home computers that belong to you and your staff. For more information about protecting home computers, visit the [Microsoft Security at Home](#) Web site.

Feedback

Please direct questions and comments about this guidance to [Security Solutions Questions & Feedback](#).

Acknowledgments

The Solution Accelerators – Security and Compliance group (SA-SC) would like to acknowledge and thank the team that produced the Malware Removal Starter Kit. The following people were either directly responsible or made a substantial contribution to the writing, development, and testing of this solution.

Authors, Contributors, and Writers

John Cobb - *Wadeware LLC*

Mike Danseglio

Charles Denny

Richard Harrison – *Content Master Ltd*

Frank Simorjay

Editor

Jennifer Kerns - *Wadeware LLC*

Product Managers

Alain Meeus

Jim Stuart

Program Manager

Bomani Siwatu

Release Manager

Karina Larson

Testers

Gaurav Singh Bora

Saurabh Garg - *Infosys Technologies Ltd*

Sumit Parikh - *Infosys Technologies Ltd*

Reviewers

Cindy Agnew - *Fife School District*, Dr. Barbara Endicott-Popovsky, Joseph Kessler, Thom Nesbitt, Sterling Reasor

Reviewers (Microsoft)

Rebecca Black, Anthony Blumfield, Derick Campbell, Chase Carpenter, Shiroy Choksey, Bret Clark, Steve Clark, Jeremy Croy, Fidelis Ekezue, Joe Faulhaber, Karl Grunwald, Kumi Hilwa, Bashar Kachachi, Jimmy Kuo, Greg Lenti, Mark Miller, Adam Overton, Max Uritsky, Jeff Williams, Lee Yan