

Windows XP Professional Security TechProGuide 1: Viruses, Worms and Spyware

Table of contents

Overview	3
Planning	4
Setup & Configuration.....	5
TechProGuide Checklist: Spyware	10
Optimization	11
Troubleshooting	13
TechProGuide Checklist: Virus software.....	18

Credits

Executive Editor,
Books and Subscriptions
Erik Eckel

Senior Editors
John Sheesley
Jim Wells

Copy Editor
Selena Frye

Graphic Artist
Natalie Eckerle

Overview

Hardly a day goes by when you don't read about a new virus or worm spreading its way across the Internet. In a constantly escalating battle, virus authors find new ways of attacking machines as antivirus vendors try to find new ways to prevent viruses. As an IT Professional, you find yourself caught in the crossfire, trying to strike a balance between keeping your users safe while also not inhibiting their productivity.

Viruses and worms are two distinct, but related afflictions. Viruses are usually spread with the help of a third-party program such as Outlook. The virus will come in an e-mail and when a user double-clicks an attachment, the virus launches, doing its damage and replicating itself. Examples of viruses include:

- Melissa
- SoBig
- Arcam
- Karga

A worm on the other hand doesn't need the help of a third party program. Once launched by the hacker, a worm self-replicates. It searches for vulnerabilities in a system and exploits them. After it "burrows" into a computer, it launches attacks to other computers, searching for the same vulnerabilities that it used to infect the host computer. Examples of common worms include:

- Sasser
- MSBlast
- NetSky
- MyDoom

A final class of malware that falls within the virus realm is the Trojan. Just like its namesake the Trojan horse, the Trojan masquerades as a legitimate program. When a user executes the Trojan,

it then reveals its true nature, causing damage to the user's computer. Examples of common Trojans include:

- Flipe
- Bing
- Blank.A
- Upbit

As if regular viruses and worms weren't bad enough, the new bane of the IT Professional is spyware and its cousin, adware. These programs usually come as a part of legitimate shareware, but hide themselves in such a way that you don't always know when they're being installed. They just sit in the background and drain system resources, either displaying advertisements or reporting back system activity to a central location. Marketers use information gathered from these programs to target pop-up ads and spam.

Spyware does more than just send information. Because it's usually poorly written, often times it causes programs like Internet Explorer to crash. It can also take over the settings of programs to display ads or redirect Web pages. Because spyware runs in the background, it can also degrade overall system performance, especially on workstations that are already near the base system requirements of an operating system.

Spyware doesn't always take the form of a separate program. Sometimes it can be a simple tracking cookie used by a Web site or e-mail. Common spyware includes:

- BonziBuddy
- Alexa
- WildTangent
- OpaServ
- AdMonitor ◆

Planning

Because virus authors are constantly changing their tactics, prevention planning can be very difficult. At a bare minimum, you need to make sure you have antivirus software installed on all of your workstations. As an added layer of defense, you may also want to make sure that you have antivirus software installed on your e-mail and file servers as well. Antivirus software should be a basic part of your workstation configuration, as important—if not more important—as application software.

Make sure that you schedule your antivirus software to update itself on a regular basis. Outdated antivirus software is worse than not having antivirus software at all because it lulls you into a false sense of security.

Ensure that your antivirus software scans your workstation in the background. Although this may place a drag on system performance, it will allow the antivirus software to immediately squash a virus if it encounters one. You should also schedule the antivirus software to do a complete system scan on a regular basis, preferably during off hours. This will catch any viruses that may have snuck past the background scan.

Because many worms take advantage of open ports on workstations and servers, a good firewall is as important as antivirus software in today's net-

working environment. You should provide firewall protection in-depth as well, placing a firewall not only between your network and the Internet, but also between your workstations and the network.

Often overlooked in IT environments is antispymware software. Viruses get all of the attention because they do damage, but having software that defends against spyware as well as viruses is also important. Like antivirus software, good spyware programs can run in the background and protect against spyware on the fly. You need to make sure you keep it up to date as well, as new versions of spyware crop up almost as fast as viruses.

One important part of planning goes beyond simple technology. You should have a clear Internet policy for your organization that spells out how to avoid spyware and viruses. Educate your users on how viruses and spyware are spread, and how to identify suspected infections. You may want to create a notification system to warn users when critical outbreaks happen.

Don't forget to also warn users about the existence of hoaxes. Just because their Aunt Esmerelda e-mails them about the "newest" virus, it doesn't mean that the virus is real. You want your users to be aware of legitimate threats, not acting like a bunch of Chicken Littles. ◆

Setup & Configuration

Configuring your workstation with security in mind is easy. Pick the proper defense mechanism, install it, and make sure you keep it up to date. Many vendors are offering complete antivirus/antispyware/firewall combinations such as:

- McAfee Internet Security
- Symantec Norton Internet Security
- Panda Platinum Internet Security
- PC-cillin Internet Security

We're not going to go into all of the iterations and combinations of software that you can and should use on your workstations. They're all pretty much the same, although some do a better job than others. Rather than recommend an individual product and walk you through its particulars, we've chosen two separate antivirus and antispyware packages to show you how to configure and use them in your battle. •

AVG AntiVirus offers a low-cost antivirus alternative

Protecting your network from viruses and Trojans isn't cheap, but it's significantly cheaper than losing employee productivity or mission-critical data due to a virus outbreak. One option to help trim your security costs is to use one of the low-cost alternatives. Many organizations are reluctant to try these alternatives because they consider them to be less reliable and less secure than the name-brand products. Nonetheless, there are low-cost solutions that might work well enough for you to consider, depending on the size of your shop and your security needs.

One such alternative is Grisoft Inc.'s AVG AntiVirus. Grisoft was founded in 1998 as a holding company for Czech Republic-based Grisoft, s.r.o., a company that specializes in antivirus software. Grisoft makes its AVG antivirus solution available free to home users.

The Enterprise version of AVG is split into two different versions—one for servers, the other for

workstations—and includes an admin module to make it easy to deploy the program to the network and to manage virus updating and other features. Performing the network install for the admin module can be a little complicated because it requires manually creating some directories on the server and copying required setup and other files to those directories. The manual work is a little annoying, but it's not overly difficult.

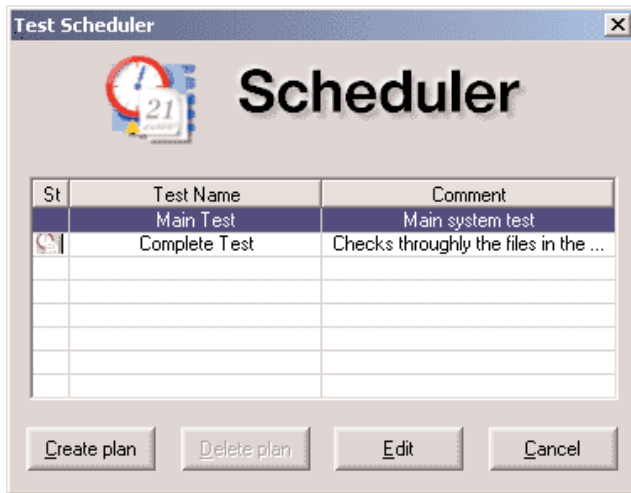
One of the steps involves creating the folder that workstation installs of AVG will use to communicate with the server and to obtain updates. You can use this folder, for example, to automatically deploy the latest definition files to the network. You can then configure the server edition to automatically connect to the AVG Web site on a regular basis to check for updates and download them to the communication folder. The workstation component will then communicate at regular intervals with the server to obtain updates. If you'd prefer, you can also configure the workstations to go directly to the AVG site for updates.

Setting up AVG for network use requires creating the communication folder and connecting to it in the interface from the workstation installs, so it's a critical component for interaction between the different pieces of the program. You'll also use the network connections between the workstations and server to schedule scans on network drives. These can also be scheduled locally, but if you want to have more control over network scans, AVG allows you to manage them centrally via the admin module.

A wizard in the admin module walks you through creating a network install script for AVG, and after you install the product itself, another wizard launches to step you through setting up basic program options. After that, you're on your own as far as configuring the Update Manager and Scheduler (see [Figure A](#)) features, which automate the definition updates and scanning.

Once the installation finished, the first thing I noticed was AVG's outdated and rather unattractive GUI. The interface looks like a throwback to the Windows 3.1 days, and you'll encounter some occa-

Figure A



sional misspellings. In the manual I downloaded with the program in PDF format, I noticed the screen captures displayed were actually taken from the Czech version of the program. This isn't a big issue compared to actual performance, but I think it reflects the level of polish you might expect to get out of a budget product. After all, that's what budget alternatives are all about—fulfilling a certain promise without a lot of bells and whistles.

Pros and cons

Like an economy car, AVG gets you from point A to point B without a lot of luxury features. If you're looking to save some money on your commute and don't care about luxury features like heated leather seats, then the economy model is just what you need.

AVG is a good fit for smaller organizations or SOHO users who want no-frills antivirus protection. Enterprises however should probably choose a more robust product with a more streamlined installation, a friendlier user interface, and better product support.

For those who think AVG is right for them or their organization: AVG Server starts at \$38 for up to two licenses and costs \$300 for 30 licenses. AVG Server runs on Windows NT/2000 servers and MS Exchange 5.0/5.5/2000, Lotus Domino, Tiny Mail, and Mail602 e-mail servers. AVG Professional Multilicense, which runs on Windows 95/98/Me/NT/2000/XP, starts at \$63 for up to two licenses and costs \$370 for 20 licenses. This is roughly half what you'd pay for the big-name antivirus suites, and with AVG, the updates are free. •

Protect against spyware and adware with Spybot

By simply visiting a Web site, or installing shareware, your users may be installing other software, cookies, or applications that are able to monitor and log Internet activity. This category of software is generally referred to as spyware. Adware is normally associated with shareware that generates pop-up ads, or displays banner ads. Spybot is a freeware tool to detect and remove spyware and adware from your system, and it performs this job remarkably well.

Installing Spybot

Spybot is donation-ware from Spybot S&D. That means that you don't have to pay for it, but that the organization does take donations to support future development. You can obtain the latest version of Spybot from [the Spybot Web site](#). Download the installation file, currently `Spybotsd12.exe`, to a temporary directory on your hard drive and you're ready to go.

To install Spybot, double-click on the self-extracting archive, and follow the prompts in the Setup Wizard. Spybot installs like every other Windows program you've ever used, with no confusing prompts or gotchas during the wizard. Once the installation is complete, you're ready to start running Spybot.

Running Spybot

To start Spybot, double-click on the desktop icon. The first action to take when Spybot runs is to check for updates by clicking the Search For Updates button. This will ensure that the spyware signatures used by Spybot, and the program itself, are up to date. If there are any updates, click the Download Updates button and let them download and install.

The default for Spybot is to run in Easy Mode. In this mode, Spybot searches for problems using a predefined configuration. Easy Mode is a good way to run Spybot if you want to run a quick check for cookies and other items that can identify you and report your Internet activity to a third party, but running Spybot in Advanced Mode provides more configuration options. To run Spybot in Advanced Mode, use the following procedure:

1. Right-click on the desktop icon for Spybot.
2. In the menu, left-click on properties.
3. The target executable for Spybot will be:
“C:\Program Files\Spybot - Search & Destroy\SpybotSD.exe” /easymode
4. Change the executable target to:
“C:\Program Files\Spybot - Search & Destroy\SpybotSD.exe”
5. Double-click on the icon to run Spybot in Advanced Mode.

All configuration changes are made through the menus contained in the Settings tab. There are five menus available under the Settings tab:

- Language
- File sets
- Settings
- Directories
- Skins
- Setting the Language

To set the language used with Spybot, left-click on the language menu. When the list of available languages appears, just click on the language you want to use. •

Main Settings

- **Save all settings:** This allows Spybot to be used with the same configuration for every scan.
- **Create backups of fixed spyware problems:** Some programs associated with Spyware will not function after the spyware component is removed. If you must use a program with a spyware component, the ability to recover the spyware will eliminate the need to reinstall the entire program.
- **Create backups of removed usage tracks:** Creating a backup of usage trackers allows you to view these trackers, and examine which Web sites are trying to monitor your activity.

- **Create backups of fixed system internals:** Any registry inconsistencies fixed by Spybot may cause problems for your system. Using this option the registry to be restored to the state it was in before the Spybot scan.
- **Ignore if single detections in include files need a new program version:** Activate this option.
- **Display confirmation changes before doing critical changes:** Using this option will ensure you are aware that changes are about to be made and prompt you for confirmation.
- **Scan priority:** Most users will normal scan priority. •

Automation settings

Spybot has the ability to run whenever the system is booted and to detect and fix any problems automatically. Enable the following settings under the Automation section of the Settings tab:

- Run Check On Program Start
- Fix All Programs On Program Start
- Rerun Checks After Fixing Problems
- Immunize On Program If Program Has Been Updated.
- Search The Web For New Versions At Each Program Start
- Download Updated Included Files If Available Online
- Expert Settings

The Expert Settings menu activates the Secure Shredder to run automatically when Spybot removes files. Because the Secure Shredder permanently deletes removed files, this tool should not be used automatically.

Selecting File Sets

To make it easier to select file sets, go to the Settings tab. Under the Expert Settings menu, enable the following settings:

- Show Expert Buttons In Results List
- Show Expert Buttons In Recovery List

These settings activate a drop-down list in the Search & Destroy screen. This list contains an easy-to-understand description of the types of scans available.

The Directories tab

The Directories tab is used to specify where downloaded files are stored. Spybot will then scan this directory whenever a check is run. The software in the specified directory will be scanned to see if any spyware or Trojans will be installed with the downloaded software.

To add a directory to the list, right-click in the blank under the Download Directory heading and select Add A Directory To This List. Browse for the folder you want to add to the list. At the bottom of the screen, select the Check Also Subdirectories Of The Above checkbox. Repeat the procedure for any additional folders you want checked by Spybot.

Running a Spybot scan

After configuring Spybot with the options you want, the next step is to run the scan of your system. To run a Spybot scan, click on the Spybot-S&D tab and click Search And Destroy.

Next, click on the File Sets button and select the type of scan to run. For this example, a Minimal Spyware Check was run. Click Check For Problems.

When the scan is complete, Spybot will display the results. Problems are divided into three categories. Red entries indicate spyware. Spyware problems are always selected to be fixed by Spybot. Green entries indicate usage trackers. You probably won't cause any problems by removing these from your system. Black entries are system internals. Make sure you know exactly what areas of your system will be affected before removing any of these entries.

Spybot automatically selects spyware problems to be fixed, so the next step is to click on the button marked Fix Selected Problems. If there are any problems that cannot be fixed because a program is in use, Spybot will attempt to correct the program automatically the next time the system is rebooted, before the spyware program is started.

Next, click on the File Sets button, and select Usage Tracks Check Only for the next scan. Click on Check For Problems and Spybot will run a check for Internet usage trackers.

To remove individual trackers from your system, click on the checkbox next to the tracker in the results, then click on the Fix Selected Problems button. Spybot will remove the selected trackers from your system. To remove all usage trackers, click Select All Items, then click on Fix Selected Problems.

The same procedure applies when Spybot runs a check on your system internals. This check is looking for registry inconsistencies, broken desktop links, and bad paths to executables. When a check on system internals is run, make sure you understand the output. Removing reported registry problems, and other entries related to system performance, can cause problems for your system.

Other Spybot tools

The Tools menu controls several tools associated with Internet Explorer and services run at startup. One of the programs you'll notice here is the Resident tool. The Resident tool is a continuously running security program. Presently, the Resident tool section provides a browser application for Internet Explorer that prevents downloads of known malicious software, such as spyware installers. To activate the Resident tool program, click on the Install button at the top of the screen.

The ActiveX menu displays a list of ActiveX controls currently installed on your system. ActiveX controls are categorized by color. Green entries are legitimate ActiveX controls. Red entries mark controls related to spyware. Black entries are not known to the Spybot database.

The BHOs tab displays information about Browser Helper Objects (BHOs). BHOs are small programs—often ActiveX controls—that extend Internet Explorer's capabilities. Because they are integrated with your browser, BHOs have access to each Web site you visit. Green entries are legitimate BHOs. Red entries are associated with spyware. Black entries are unknown to Spybot.

If you have any concerns about a BHO in this list, you can easily disable it. Click on the BHO to be disabled. At the top of the BHO window, click

on the toggle button. Disabled BHOs will then appear grayed out in the BHO list.

On the Brower Pages tab, Spybot also provides protection against browser-hijacking agents that can reset the start or search page in Internet Explorer. If your browser start page or search page is changed and cannot be reset through IE, the new URL will probably show up in this list.

To reset the offending URL, and ensure the URL is added to the next Spybot update, click on the URL your browser has been redirected to. At the top of the screen, click on the Change button. Enter the new URL. After changing the URL, mail the offending address to detections@spybot.info. The URL will be added to the list of known bad URLs.

Spybot comes with its own hosts file that contains an extensive list of Web sites known for spyware that you can view on the Hosts File tab. When this file is installed, no content from any of the sites in it will be displayed. To install the Spybot hosts file, click on the Hosts File tab.

At the top of the Hosts File screen, click on Add Spybot-S&D Hosts List. The Spybot Hosts File will now be used instead of your default Hosts File. To remove the Spybot Hosts File, click on Remove Spybot-S&D Hosts List.

The Process List tab displays all processes running on your system. Although any process may be killed (stopped) through this menu, it is intended primarily as information for Technical support, and to be included in a system report.

To kill a process in this list, select the process you want to kill from the list. At the top of the Process list window, click on the button marked Kill. Spybot will then stop the process.

System Startup

The System Startup menu lists all programs that are started when Windows is started. This menu allows the user to change the path to a Startup program, or change the command used to execute the program. You can also delete any program from Startup or insert a program to be started with Windows.

To view any item in the System Startup list, select the item, and click on the info button at the top of the System Startup screen. To disable a program run at startup, or to allow a disabled program in this list to start with Windows, select the program and

click on the Toggle button at the top of the screen. To change the path to a program run at startup, or to change the command options run with the program, select the program from the System Startup list, and click on the Change button at the top of the screen.

One good feature of this menu is the ability to add and configure new startup programs. To add a new program to the Startup list, click on the Insert button at the top of the screen. Make the program available to All Users On Startup, or only to the Present User. Select how the program will be run. There are three selections available:

- Run the program as a normal program
- Run the program as a service
- Create an autostart group link
- Provide a name for the registry entry and select the path to the executable file. A new entry with the value you enter will be added to the list of programs run at System Startup.

View Report

The View Report menu is used to generate a report of your system configuration, including the configuration used for Spybot. The results from a Spybot scan can also be included with this report.

Using Spybot Immunization

The Spybot Immunization Function is controlled through the Spybot-S&D tab. It provides four very useful functions:

- Permanently immunizing Internet Explorer from spyware
- Preventing Internet Explorer from downloading known spyware installers
- Preventing spyware from making changes to Internet Explorer configuration
- Locking the Hosts File

To provide immunity for your browser and Hosts File, click on the icon labeled Immunize under the Spybot-S&D tab. In the first configuration panel, titled Permanent Internet Explorer Immunity, click on the Immunize button to immunize Internet Explorer. The next panel is labeled

Percent Running Bad Download Blocker For Internet Explorer. In the drop-down list, select Block All Bad Pages Silently. Click on Install.

In the third panel, labeled Recommended Miscellaneous Protections, click in each of the three

checkboxes available to lock the Hosts File and to prevent spyware from reconfiguring Internet Explorer when immunization is activated. Spybot blocks all entries that are in its database. ◆

TechProGuide Checklist: Spyware

Rating system

- 1 = Does not
- 2 = Somewhat
- 3 = Mostly
- 4 = Completely

What your score means

- 31 - 40 = Your spyware detection software is excellent
- 21 - 30 = Your spyware detection software is adequate
- 11 - 20 = Your spyware detection software is substandard
- 0 - 10 = Your spyware detection software should be replaced

Does your spyware...

Rating

- | Does your spyware... | Rating |
|---|--------|
| 1. Quarantine identified spyware | |
| 2. Check and remove spyware from registry and start-up locations | |
| 3. Report all activities to a central log file | |
| 4. Download and install updates automatically | |
| 5. Automatically prevent spyware cookies from entering the system | |
| 6. Support command line switches for customizable installations | |
| 7. Scan memory for active spyware | |
| 8. Scan selected file types, including inside archives | |
| 9. Include the threat level of discovered spyware | |
| 10. Work with current antivirus, firewall, and IDS installations | |

Your score is:

Optimization

There's a lot you can do to optimize your workstations to make them virus-resistant. Microsoft has identified dozens of security holes in Windows XP and released patches for them. You should make sure that as soon as you finish installing Windows XP that you immediately apply all of the critical patches. This will go a long way to blocking some of the most common virus threats. You can also protect your workstation from attacks by disabling a common virus target, DCOM. •

Increase workstation security with DCOMbobulator

Many Internet worms such as MSBlaster take advantage of Windows XP-based workstations by using a little used and little known feature of these operating systems known as DCOM. Even though Microsoft has released many patches for DCOM, many systems remain unpatched and vulnerable to DCOM attacks. Here's how you can quickly find out if your workstation is subject to attack by using DCOMbobulator.

What's DCOM?

DCOM stands for Distributed Component Object Model. Because Windows itself is based on objects, Microsoft thought it would be a good idea to create objects that could be distributed, i.e., reused by computers across a network. This would allow computers to more easily share resources across a network, making the overall network more powerful. Using RPC (Remote Procedure Calls) over TCP/IP port 135, Computer A could use DCOM to execute applications on Computer B, freeing Computer A's storage and processor resources for other things, while taking advantage of the pre-installed program on Computer B.

The only drawback to this strategy was that very few programs actually make use of DCOM. If your users are using standard office or Internet applications, they'll never make use of DCOM. Unfortunately however, Microsoft turned DCOM on by default in Windows XP. This fact, along with several vulnerabilities in DCOM, leaves your system

wide open to hacker attack. The same components meant to share your computer with legitimate network users can be used by hackers to take over your machine.

Microsoft released updates and patches that were supposed to make DCOM more secure. Hopefully you've deployed the patches on your workstation. Even so, if DCOM is still available, even if patched, it can become a target. To make your network more secure, you should disable DCOM. DCOMbobulator can help.

What does DCOMbobulator do and how do I get it?

DCOMbobulator tests a workstation for the presence of DCOM, DCOM's status on the system, and whether or not DCOM has been patched. It's a freeware program by Steven Gibson, the author of SpinRite and the famous Shields Up! Web site.

You can obtain DCOMbobulator from the [DCOMbobulator Web site](#). In an age of multi-megabyte programs, long downloads, and Setup Wizards, DCOMbobulator is amazing. When you click the Download link, you'll download a tiny 29 KB program. You can choose to save it to your hard drive, and from there distribute it to others, or you can just run it directly from the Web site. •

Running DCOMbobulator

When DCOMbobulator starts, you'll see three tabs and an information pane in the middle of the screen. DCOMbobulator's information window displays everything you ever wanted to know about DCOM's vulnerabilities and what you should do about it. To test your system, click the Am I Vulnerable tab and then click Load DCOM Test. When you do, you'll see the results as shown in [Figure B](#).

As you can see in the figure, this machine is vulnerable to attack. DCOMbobulator will point you to the appropriate Microsoft Web site to obtain patches for a vulnerable system.

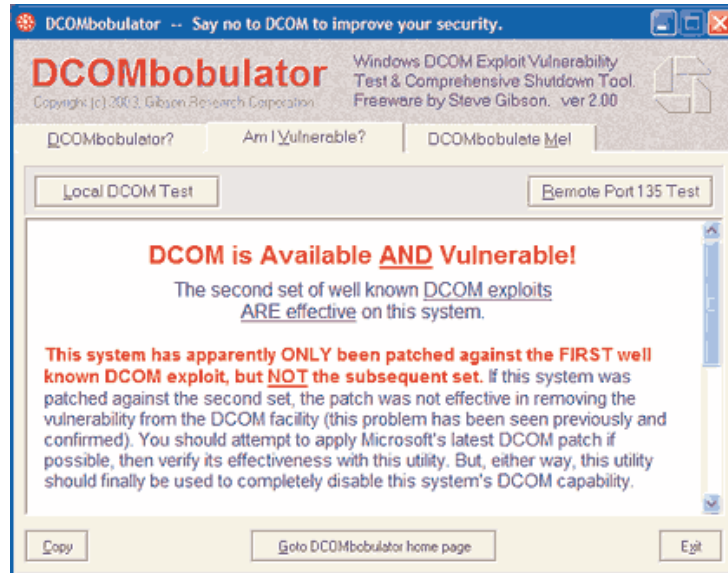
Even if all of the patches have been applied, you may want to disable DCOM. To do so, click the DCOMbobulate Me tab. Click Disable DCOM to turn DCOM off. If you find that you later need

DCOM, you can rerun the program and click Enable DCOM on this same tab.

That's all there is to it. Once you've applied the patches to your system, or better yet, simply

disabled DCOM, you're done. Your system is then immune to DCOM-based attacks like the MSBlaster worm. ♦

Figure B



DCOMbobulator tests your system's DCOM status.

Troubleshooting

Today's PC viruses, Trojan Horses, worms, and blended threats can cause run-of-the-mill Windows or application problems, out-of-memory errors, intermittent failures to fully start up, or installation or operation problems with applications. But these problems could also be caused by your typical hardware or software malfunction. Here's how to determine whether the culprit in question is indeed a virus.

You probably have a virus if...

The symptoms in the bulleted list below are rarely caused by anything except a virus, so if you detect any of these issues on an end user's PC, you should strongly suspect virus infection.

- The user received an e-mail with an odd attachment and opened it, with unexpected results—such as the appearance of odd dialog boxes or a sudden degradation in system performance.
- There is a double extension on an attachment that the user recently opened, such as .jpg.vbs.
- An antivirus program will not install on the PC (or appears to install, but then will not run), but other programs will.
- Odd dialog boxes or messages appear onscreen.
- Several files are missing, especially those of a common type. For example, some viruses have a side effect of deleting all graphic files of a particular type.
- Someone tells the user they have recently received strange e-mails from them containing random attached files or a virus.
- The PC starts performing actions seemingly on its own, like moving the mouse pointer, opening or closing windows, running programs, or opening and closing the CD tray. This is a symptom of someone actually using a back door to operate the PC, rather than a symptom of the existence of the back door.
- You notice the presence of new users with full security permissions that you know you did not

create, or you notice inappropriate permissions assigned to existing users. Again, this is more often a symptom of back door hacking than virus infection.

- The mouse pointer changes to some different graphic.
- Odd icons appear on the desktop that the user did not place there, although the user has not installed any new applications lately that could have placed them there.
- Strange sounds or music plays from the speakers for no apparent reason.
- File sizes or date/time stamps have changed on files that the user knows he or she did not alter.
- A program that was used successfully recently has disappeared, and the user knows that he or she did not uninstall it.

You might have a virus if...

A virus infection could also cause some of the following symptoms. Keep in mind that these symptoms are also typical of ordinary Windows system problems, so they cannot be definitively viral symptoms without running a complete virus scan with updated definitions.

- Windows will not start at all, even though the user has made no system changes, installed or removed any programs, or made any Registry edits since the last time it started successfully.
- Windows will not start because certain critical system files are missing (and you see an error message listing those files), and the user is confident that he or she did not accidentally delete them.
- The PC starts up normally sometimes, but at other times will hang before the desktop icons and taskbar appear.
- The PC runs very slowly and/or takes a long time to start up.

- Out-of-memory error messages appear, even though the PC has plenty of RAM.
- Viewing the system processes via Task Manager shows that an unknown process is consuming a high percentage of the CPU time.
- From the Task Manager view, you notice programs or processes running that you do not recognize, even after shutting down all running programs and system tray utilities.
- New applications will not install properly.
- Windows spontaneously reboots for no apparent reason.
- Applications that used to run normally are now crashing frequently. Removing and reinstalling them does not solve the problem.
- A disk utility such as Scandisk reports multiple serious disk errors.
- A partition completely disappears.

The key to distinguishing virus-related system problems from ordinary ones is often situational. What did the user do right before the problem started? It never hurts to ask. If possible, check the user's e-mail box to see whether an e-mail containing a virus might still be hanging around there. Check his or her Deleted Items and Sent Items folders as well to see if the virus may have been spread to others.

For definitive virus detection, you must turn to an antivirus program with updated definitions. If a reputable antivirus program will install, run, and complete a check successfully, and if its definitions have been updated within the last 24 hours, you can be fairly confident that the problem is not a virus. Otherwise, virus infection is still a credible suspect.

Are the definitions up to date?

Updated virus definitions are essential; otherwise, performing a complete system scan for a virus is a waste of time. And these days, new viruses are discovered almost every day, so definitions updated within the last 24 hours are preferable.

Most antivirus programs can't detect viruses that they don't know about. There are exceptions, such as programs that monitor the file sizes and dates of

essential system files and warn you if they are about to be changed. However, the vast majority of threats circulating today are not true viruses because they do not actively infect your existing .exe files or boot sector. Instead, they are Trojan horses, back door programs, or worms, whose behaviors won't normally trigger that kind of proactive detection. Therefore, updated definition files are your only reliable line of defense against new virus threats.

Norton AntiVirus, for example, checks for new definitions on the company's server and installs them automatically. Be warned, however, that some services (such as Symantec's Live Update) update their servers only once a week except during peak periods of virus problems, so you might not always get the latest updates by running Live Update. Going manually to the company's Web site and comparing the date of the most recently posted definitions to the date shown in your software is one way to ensure you have the latest stuff, but that can be a little taxing. Symantec offers an Intelligent Updater service that updates virus definitions every business day, which is a great alternative for administrators with mission-critical PCs to support.

Do a full system scan

Assuming your virus definitions are up to date, you can be reasonably certain that if an antivirus program successfully completes a full system scan and tells you there is no virus, there probably is no virus. If you remain skeptical, check one of the major virus security Web sites after 24 hours; it's possible that a brand-new variant has slipped in. If that's the case, other people should be reporting it and it should be all over the virus community's news within 24 hours.

If your antivirus program won't run, or won't do a full system scan, or if you buy a new copy and it won't install, this is a significant sign there is a virus infection. For example, many varieties of the W32.Klez.mm mass-mailing worm include commands that disable your antivirus software and make it difficult or impossible to install new antivirus software.

Avoiding future infections

End users seem prone to fall for every hoax and every encouragement to "click here," which makes it

especially difficult for support professionals to protect those PCs. Here are some tips geared toward safeguarding your users against their own gullibility and protecting your servers against virus attacks.

- Tell your end users not to open attachments unless they are expecting them, and not to run programs they download from the Internet unless they have been scanned for viruses.
- Encourage end users to keep Windows and Internet Explorer updated with the latest security patches. Simply visiting a Web site can cause infection if certain patches are not installed, so if possible, set up automatic updates for Windows and IE.
- By default, many operating systems (especially server versions) install with extra services that you don't need, such as an FTP server, telnet, and a Web server. Remove any that are not critical so a virus has fewer avenues of attack.
- Be quick to disable or block access to network services when a blended threat exploits one of them, and keep it sealed off until you can apply a fix.
- Keep patch levels up to date, especially on computers that host public services and are accessible through the firewall, such as HTTP, FTP, Mail, and DNS services.
- Use strong passwords yourself, and enforce an aggressive password policy that requires complex passwords and frequent changes. This helps limit the damage in the event that a computer is compromised through a back door.
- Configure your e-mail server to block or remove e-mail that contains file attachments that are commonly used to spread viruses, such as VBS, BAT, EXE, PIF, and SCR files. Recommend to users that they send any files that legitimately need to be mailed in those formats in compressed archives (ZIP files).
- Frequently check the security advisories provided by the makers of antivirus software to find out what the latest threats are. An excellent one is the Security Advisories list from Symantec. •

Sasser.a and Sasser.b prevention and cure

Sasser and its variations are network-aware worms that do not require e-mail or user interaction to spread. The worms use a bootstrap effect by infecting new machines first, then downloading the full code from a previously infected machine. Sasser (w32.sasser.a) and Sasser.b (w32.sasser.b) are both 15,872 bytes long, and they randomly scan local networks and the Internet to look for additional systems to infect.

This scanning could slow normal traffic on the Internet. Vulnerable systems include Windows 2000 and Windows XP that have not had the [Microsoft Security Bulletin patch MS04-011](#) installed and that are not running desktop firewall software. Sasser does not affect any other version of Windows, nor Linux, Unix, Mac OS, or any other operating system.

Sasser takes advantage of a buffer-overflow flaw in the Local Security Authority Subsystem (LSASS), which allows an attacker to gain control of infected systems. Sasser adds a copy of itself to the Windows directory under the name:

- Sasser.a AVSERVE.EXE
- Sasser.b AVSERVE2.EXE

It adds the following to the system Registry file:

Sasser.a: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run avserve.exe = c:\Windows\avserve.exe

Sasser.b: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run avserve2.exe = c:\Windows\avserve2.exe

This change to the Registry allows the worm to run once the machine reboots.

Sasser starts an FTP server on TCP port 5554. Meanwhile, it uses TCP port 445 to search random chunks of the Internet for additional Windows 2000 and Windows XP that have not patched the LSASS flaw.

Sasser then launches 128 threads to scan the random IP addresses and listens on successive ports starting with TCP port 1068. Microsoft reports that the worms also use TCP port 139 as well. Ports 139 and 445 are both used by the Windows file-sharing protocol.

If the Sasser worm finds a vulnerable machine on a local network or the Internet, the worm sends a specially crafted packet to cause a buffer-overflow in lsass.exe. The overflow contains instructions in a script file, cmd.ftp, on the newly infected machine to open TCP port 9996 and instructions to download a copy of itself from TCP port 5554 on the previously infected machine as [some random number]_up.exe.

The file cmd.ftp is then erased. Sasser.a creates a win.log in the root directory of the newly infected machine that contains the number of remote systems currently infected and the IP address of the last infected system. Sasser.b creates a file called win2.log.

Prevention

Microsoft has created [a special page](#) on how to prevent a Sasser infection. Basically, a desktop firewall should protect vulnerable systems until the Microsoft security patch can be downloaded. If you do not have a personal firewall, you should install one first to limit the effects of the Sasser worm. You should also make sure you've obtained and installed [Microsoft Security Bulletin patch MS04-011](#).

Removal

Most antivirus-software companies have updated their signature files to include this worm. This will stop the infection upon contact and in some cases will remove an active infection from your system. However, simply removing the Sasser worm infection is not enough; an infected system will remain vulnerable to attack until the LSASS vulnerability itself has been patched. •

Virus hoaxes can drain IT resources and wreak network havoc

“WARNING: XYZ virus will wipe your drive! Click here for help!!!! Warn your FRIENDS – This is URGENT!!”

More than likely, you have gotten an e-mail with a message similar to this one. Of course, being security aware, you probably know that these kinds of messages are always hoaxes, since viruses and worms are never legitimately brought to our atten-

tion by random e-mailers on some kind of mercy mission.

Nevertheless, hoaxes can be a major drain on an IT department's resources. The U.S. Department of Energy's Computer Incident Advisory Capability office said, “At CIAC, we find that we spend much more time debunking hoaxes than handling real virus and Trojan incidents.” When you realize that CIAC actively solicits new virus code and maintains a laboratory to investigate viruses and worms, that's a telling statement.

Many hoaxes are simply time-wasting pranks intended to make fun of novice or clueless users, but others include instructions that, if followed, will wreak havoc on a personal system or even a network. And many of the hoax e-mails that don't contain malicious payloads or damaging directions are used by spammers to collect new victims' addresses.

Don't ignore the threat from these time-wasters. Not only will they get you on spam lists, the original hoax can be hijacked and turned into a malicious attack. As McAfee points out on its hoax site, this is exactly what happened with the AOL4FREE hoax when a Trojan was added to the originally harmless hoax.

That hoax was a good example of the social engineering used to get by people's natural skepticism. AOL4FREE didn't purport to send users free AOL service; rather, it pretended to warn them that they shouldn't fall for a nonexistent free AOL letter and solicited their help in eliminating the phony virus by forwarding the warning to all their friends.

What do you do about hoaxes?

As usual, educating users is the best way to combat these threats. You need a detailed usage policy that all users have to read and follow. Part of this guide should be a brief explanation of the basic threats and problems faced by businesses using the Internet.

A brief introductory talk to staff and new workers covering the following topics should suffice for most employees:

- Virus threats are not announced by e-mails. These are always hoaxes and the IT department is usually notified about new viruses long before you could get an e-mail warning.

- E-mail addresses can be hijacked. If a message appears to be from someone you trust but the message seems somehow odd, it is probably a fake message that was automatically forwarded by a virus.
- Never open any unexpected e-mail attachments.
- Never forward any virus threat e-mails or attempt to deal with the supposed threat by following instructions contained in an e-mail. Contact the IT department if you have a concern, and it will take any necessary actions.

Managing e-mail access

You can cut the number of incidents that you have to respond to by forbidding users to access outside e-mail accounts from work. This is usually done via Web mail, Outlook Express, or even users who've loaded AOL software on their work computers. You'll get a lot of complaints about this policy at first, but you should point out that this is akin to the normal ban on personal phone calls at work, except for emergencies or other urgent incidents.

If you decide on this policy, you will also have to remind workers that their company e-mail account is not private, and they should never use it for any nonbusiness purpose. Make sure they understand that it's for business use only, and that their account may be routinely accessed by others in the company for legitimate reasons, such as when they are out sick or on vacation.

A policy banning access to personal e-mail accounts, complete with rigorously enforced sanctions against violators, will not only eliminate many of the threats from time-wasting hoax e-mails, but will also help mitigate a cause of real virus and worm infections: Employees opening infected attachments disguised as everything from lottery tips to nude photos of some actress or actor.

How to recognize a hoax

Most e-mail hoaxes (and almost all of the really successful ones) come in several recognizable categories:

- **The technical warning.** Many successful hoaxes use highly technical language to describe a threat. The description is often complete nonsense.

- **The Good Samaritan ploy.** Hoaxes don't just warn you of a mythical threat, they play on your desire to help your friends, or to appear important, and cajole you into sending the fake warning to everyone you know. This lends the warning an air of authenticity because it comes from someone users know.
- **The too-good-to-be-true offer.** Among other common ploys are those get rich quick schemes that clearly sound too good. They're usually pretty stupid, but people fall for them every day.

The e-mail hoax is just the technological equivalent of the chain letter and follows the age-old three-part pattern of all successful cons:

#1: The hook

First, there will be an appeal to greed or compassion or the chance to show off by being the first to warn your friends. The hook is the virus warning, the dying child announcement, the offer to make Big Money at Home While Sleeping, or a similar catchy subject line that is expanded in the first several paragraphs if you open the e-mail.

#2: The threat or warning

The message will quickly move on to warn of severe damage that could occur to your computer (or some other dire consequences that might befall you) if you don't take a certain action.

#3: The action

Although a few hoaxes will simply rely on your inherent desire to share good or bad news, nearly all of them will include a final plea to send copies of the original message to as many people as you can.

Certainly the most easy-to-identify feature shared by all hoaxes is this: They come in an e-mail, not from a trusted Web site or a mailing list you have subscribed to, but from an untrusted source. That should be such a gigantic red flag that no other warning is needed.

Hoax resources

Internet hoaxes are so common that virtually every security company or antivirus vendor maintains a Web page just for this problem. Here are some of the most useful sites:

- McAfee's site has details on about 50 major hoaxes.
- Symantec has an even longer list of hoaxes.
- Another interesting site is provided by F-Secure. This site focuses on the ones that include malicious code but still lists too many hoaxes to count.

- The CIAC has its own HoaxBusters site, which includes some useful tips on recognizing and combating hoaxes, as well as a helpful list of other legitimate sites that list hoaxes.
- In particular, CIAC recommends Rob Rosenberger's independent Vmyths site, in part because it's not sponsored by any of the antivirus software vendors. ◆

TechProGuide Checklist: Virus software

Rating system

- 1 = Does not
- 2 = Somewhat
- 3 = Mostly
- 4 = Completely

What your score means

- 31 - 40 = Your spyware detection software is excellent
- 21 - 30 = Your spyware detection software is adequate
- 11 - 20 = Your spyware detection software is substandard
- 0 - 10 = Your spyware detection software should be replaced

Does your virus software...	Rating
1. Scan instant message attachments	
2. Include centralized network auditing capabilities	
3. Provide outbound e-mail worm heuristics	
4. Provide Internet e-mail attachment scanning	
5. Provide automated virus damage cleanup	
6. Identify blended threat attack sources that spread via open file shares	
7. Ensure machines not connected to the network store and forward event data to administrators after reconnecting	
8. Handle IT antivirus policy enforcement	
9. Provide console monitoring	
10. Detect and terminate suspect processes in memory	
Your score is:	