a
ir

CNN.com

technology > computing

Editions | myCNN | Video | Audio | Headline News Brief | Feedback

MAINPAGE
WORLD
U.S.
WEATHER
BUSINESS
SPORTS
TECHNOLOGY *
computing
personal technology
SPACE
HEALTH
ENTERTAINMENT
POLITICS
LAW
CAREER
TRAVEL
FOOD
ARTS & STYLE
BOOKS
NATURE
IN-DEPTH
ANALYSIS
LOCAL

EDITIONS:
CNN.com Europe

change default edition

MULTIMEDIA:
video
video archive
audio
multimedia showcase
more services

E-MAIL:
Subscribe to one of our news e-mail lists.
Enter your address:
go

DISCUSSION:
chat
feedback

Analysis: How to secure your Windows environment

From...
PC World

July 27, 2000
Web posted at: 8:39 a.m. EDT (1239 GMT)

by Lenny Bailes

(IDG) -- By now, you've probably succumbed to the nagging and have installed antivirus software to protect your PC. That's good, but not good enough.

Generally, antivirus packages can only protect you after a major virus outbreak, not during one. Even if you regularly update your software to spot the latest strains, that might not help you should a new virus arrive on the scene. In the wake of the "ILove You" virus, major vendors made antivirus patches, but they were too late in most cases -- the damage had already been done.

"ILove You" and many other recent Windows viruses and worms exploit newly discovered weaknesses in the operating system and in popular e-mail clients. For a couple of years now, most widespread viruses have traveled around the world via e-mail, moving on the Net as attachments to messages.

MESSAGE BOARD
Operating systems

ALSO
Microsoft security executive promises improvements

For awhile, things started getting better because Net users learned not to open attachments from strangers, and they became wary of certain types of files, such as .exe program files and .doc Word files. But lately, matters have worsened again, for two reasons: Virus writers have begun using unfamiliar file types that people don't yet equate with danger (.vbs script files are the best example), and they've also learned to exploit some "features" in Windows that can mask a file's true nature.

In this article I'll show you how to close the points of entry in Windows and batten down its hatches. All you'll need to spend is a few minutes to make some minor Windows configuration adjustments.

CNN Sites

Search
CNN.com

Find

TECHNOLOGY
TOP STORIES

Consumer group: Online privacy protections fall short

Guide to a wired Super Bowl

Debate opens on making e-commerce law consistent

(MORE)

TOP STORIES

More than 11,000 killed in India quake

Mideast negotiators want to continue talks after Israeli elections

(MORE)

BUSINESS
Playing for Iraq's jackpot

Coke & smoke bite Dow

Sun Microsystems posts tiny profit

(MORE)

MARKETS 4:30pm ET, 4/16

DJIA	144.70	8257.60
NAS	3.71	1394.72
S&P	10.90	879.91

CNN WEB SITES:
CNN Websites
CNNfyi.com
CNN.com
Europe
AsiaNow
Spanish
Portuguese
German
Italian
Danish
Japanese
Chinese
Headlines
Korean
Headlines

TIME INC. SITES:
Go To ...

CNN NETWORKS:
Networks image
CNN anchors
transcripts
Turner
distribution

SITE INFO:
help
contents
search
ad info
jobs

WEB SERVICES:

Windows vulnerabilities

Recent e-mail-borne viruses have been successful at spreading themselves far and wide in part because Microsoft leaves your PC open to intruders. Preconfigured defaults in the operating systems and in Windows applications (most notably, Outlook and Outlook Express) give other programs easy access. Microsoft claims that its customers prefer it that way.

The "ILove You" virus took advantage of a feature of Windows 98 called the Windows Scripting Host, which is intended to give programmers and admins the ability to perform behind-the-scenes tasks with very simple code. The problem with the Windows Scripting Host is that lowlifes--such as the creator of "ILove You" -- have found it just as useful as the rest of us.

When files look like other files

Most folks have learned over time that unknown programs -- files with an .exe extension -- that arrive via e-mail are dangerous. Many users have also gotten used to the fact that Microsoft Office files (especially .doc files) are susceptible to so-called macro viruses. Other types of files -- such as VBScript files that sport the .vbs extension -- are dangerous, but unknown to most users. To make matters worse, virus spreaders have begun taking advantage of settings in Windows that can mask filename extensions, making a dangerous .vbs file look like an innocuous .txt text file.

The gotcha is that the full file name of the attachment is actually something like "Love-letter-for-you.txt**.vbs**". By default, Windows hides the .vbs file extension from view.

When you open a .vbs file, it doesn't appear in Notepad. Instead, Windows fires up the Windows Scripting Host, which in turn begins to execute any instructions contained inside the attached file. Bad news.

If you have a sharp eye, you might have detected this deception by noticing that the attachment has an unusual icon -- different from regular text files. To make these sorts of files easier to spot, change the Windows 98 display defaults. The real file extensions for most registered file types will then appear in Windows Explorer and in your e-mail program.

Hatch Number 1

1. Open Windows Explorer (usually found at Start, Programs, Windows Explorer.)
2. Choose View, Folder Options.
3. Click the View tab in the Folder Options window.
4. Under "Advanced settings," click the "Show all files" radio button and remove the check mark next to "Hide file

[SI.com] SPORTS
Jordan says farewell for the third time

Shaq could miss playoff game for child's birth

Ex-USOC official says athletes bent drug rules

(MORE)

> All Scoreboards

WEATHER
US Zip go All cities

WORLD

Quake help not fast enough, says Indian PM

U.S.

Bush: No help from Washington for California power crunch

POLITICS

Bush signs order opening 'faith-based' charity office for business

LAW

Prosecutor says witnesses saw rap star shoot gun in club

ENTERTAINMENT

Can the second 'Survivor' live up to the first?

HEALTH

Heart doctors debate ethics of testing super-aspirin

TRAVEL

Nurses to aid ailing airline passengers

extensions for known file types."

Voila! The same attachment we saw before will now show its true .vbs colors.

Scraps: Wolves clothed by Microsoft

Since some folks (and antivirus vendors) are hip to attacks from VBScript attachments, hackers have recently switched their focus by slipping a different disguised attachment type into their counterfeit e-mail messages. The Stages worm contains the customary come-on in the message text urging the user to click a "text file" attachment. This time, the attachment is really a Microsoft Scrap Object (a .shs file) with a hidden extension. Scrap Objects can work their black magic just like infected Word documents, executing destructive macros when loaded.

Unfortunately, Windows hides .shs extensions even after you've turned off extension hiding, as described above. The only way to override this foul behavior is to hack the system Registry. Here's how:

Hatch Number 2

1. Open the Windows Registry Editor: Click Start, Run, type Regedit in the field, and click OK.

2. Click the plus symbol to expand the HKEY_CLASSES_ROOT entry in the left pane and then scroll and select the ShellScrap key. (If you can't find ShellScrap, make sure you're scrolling far enough down: The alphabetization restarts after you get past the entries that start with a period.)

3. With the ShellScrap key highlighted, click the NeverShowExt string value in the right pane. Press the Delete key.

4. Close Regedit.

Hobbling VBScripts entirely

Due to the onslaught of e-mail viruses that use VBScript attachments, Microsoft has recently issued a patch for Outlook 98 and 2000 (see link below). This patch addresses the problem by forbidding Outlook 98 and 2000 to *open or save any executable file attachments at all* (including legitimate applications or scripts that users might actually want to transmit and run).

If this remedy is too drastic, here's another way to nullify malicious .vbs attachments. (This trick works for Outlook Express and Outlook 97 as well as Outlook 98/2000 and other e-mail packages.) You can divert VBScript files to open in the harmless Notepad (which will simply display them) rather than invoking the Windows Scripting Host (which will run them).

Hatch Number 3

1. Open Windows Explorer.

FOOD

Texas cattle quarantined after violation of mad-cow feed ban

ARTS & STYLE

Ceramist Adler adds furniture to his creations

(MORE HEADLINES)

2. Choose View, Folder Options.

3. Click the File Types tab in the Folder Options dialog, scroll down to and choose "VBScript Script File" in the "Registered file types" list, and click the Edit button to the right of the window.

4. In the Edit File Type window, select the Edit action under the Actions list. Then click the Set Default button. The Edit action should now be highlighted in bold type.

5. Click Close twice.

6. From now on, if you launch a .vbs file in Windows Explorer or from your e-mail program, it will appear as a text file in a Notepad window. You can still execute a legitimate VBScript file by saving it to a folder, right-clicking the file in Windows Explorer, and choosing Open from the pop-up menu.

Vulnerabilities in applications

As in Windows 98, there are "open hatches" that you can close in the configuration settings of Microsoft's Outlook, Outlook Express, and some third-party e-mail programs.

Attachment security

If you use Outlook for e-mail, the first thing you should do is download and install the appropriate attachment security patch for your version. Once that's done, follow the directions below to enable additional safety measures.

• Download Outlook 2000's e-mail attachment security patch from FileWorld

• Download Outlook 98's e-mail attachment patch from FileWorld

Microsoft's Outlook and Outlook Express have an "attachment security" option that will display a warning message on the screen before allowing you to launch a file attachment or save it to disk.

Hatch Number 4

To enable this warning in Outlook 97, 98, or 2000, choose Tools, Options, click the Attachments tab (in Outlook 2000, choose the Security tab, and then click the Attachment Security button), and select "Security Method: High." When you double-click an attachment's file icon in a message window (Outlook 97) or select the paperclip at the upper right of the message and click the attachment icon (Outlook 98/2000) a pop-up message will ask you to confirm that the file is trustworthy before prompting you to launch the file or save it to disk.

In Outlook Express 4 or 5 this warning message comes up automatically as a program default when you attempt to open a file attachment.

All of the Outlooks include an "Always ask before opening" check mark in the pop-up warning. If you remove the check mark for a specific file type (such as a Microsoft Word attachment), the default action for that file type again becomes to launch it directly.

If you enable the high security option and remove the "Always ask" check mark for one file type, other file types will continue to trigger the warning unless you specifically disable it for each one.

If you inadvertently disable Outlook's pop-up warning for a specific attachment type, you can easily get it back. For example, to reenable the warning for Microsoft Word documents:

1. Open Windows Explorer.
2. Choose View, Folder Options.
3. Click the File Types tab in the Folder Options window, scroll down, highlight the Microsoft Word Document file type, and click the Edit button.
4. Under the Actions list, place a check mark in the box marked "Confirm open after download."
5. Click OK twice to close the Folder Options dialog box.

More Outlook security

Rogue file attachments are not the only way that hackers can attack your PC through your e-mail. It's fun to be able to receive messages with full HTML formatting and embedded pictures, but associated JavaScript and ActiveX capabilities permit modern e-mail programs to run more forms of destructive code.

As we prepared this story, Microsoft announced the discovery of yet another new potential threat to users of Outlook and Outlook Express. A security flaw in the engine that underlies those products can permit hackers to control your computer simply by sending an e-mail message -- even if you don't open it or run an attachment. Fortunately, a cure already exists, but you may not like it: Download and install the latest version of Outlook, Outlook Express, or Internet Explorer 5.

• Download Internet Explorer 5.01 Service Pack 1 update from FileWorld. • Download Internet Explorer 5.5 from FileWorld.

Microsoft has established security settings for Internet Explorer 4 and 5 that apply to JavaScript and ActiveX content in the various Outlooks as well. To guard against destructive scripts embedded in the HTML content of an e-mail message, you can reconfigure your Internet Explorer Security Zone settings.

Hatch Number 5

1. Open the IE Internet Settings. You can always do this by launching the Internet Options applet in the Windows Control Panel. (Some of the Outlooks contain menu options to access the Internet Settings and some don't).

2. Click the Security tab and select the Internet zone.

3. Now click the Custom Level button. In the Security Settings dialog box, change the setting for each of the following options from Enable to either Disable or Prompt: "Script ActiveX controls marked safe for scripting," "Run ActiveX controls and plugins," "Active Scripting," and "Scripting of Java applets."

4. Click OK to return to the Security tab on the Internet Properties window, and then click the OK button to save your changes.

5. If you're running Outlook 97, 98, or 2000, you should also check in occasionally at Microsoft's Office Update site and download and install any patches that are appropriate for your computing environment. Outlook Express 4 or 5 users should visit the Windows 98 Update site for the latest information and patches.

Keep your guard up with Eudora

PC attacks through hostile code embedded in HTML are not limited to Microsoft's Outlooks. Qualcomm's Eudora is vulnerable to a trick that embeds false Windows shortcut links into an e-mail message.

Hatch Number 6

If you're a user of Eudora 3 or 4, open Notepad (Start, Programs, Accessories, Notepad), load the Eudora.ini file from your Eudora folder, and add the following line to the [Settings] section:

• WarnLaunchExtensions=exe com bat cmd pif htm do xl reg lnk

Avoiding Word Macro viruses

Microsoft Word Macro viruses are a little bit passe (and most scanners these days can easily spot them), but they still make the rounds, and they can still do damage.

Hatch Number 7

If your word processor of choice is Microsoft Word, there's always the possibility that some new macro virus will find you before your antivirus vendor issues an update. Although sophisticated macro viruses can slip past Word's built-in macro protection feature, you don't have anything to lose by turning it on. (Word 97: Choose Tools, Options from the pull-down menu, click the General tab, place a check mark next to "Macro virus protection." Word 2000: Choose Tools, Macro, Security and set the Security Level at Medium or High.) Enabling this option causes Word to display a warning dialog box whenever you open a macro-bearing .dot template disguised as an ordinary document.

If you've already created or obtained most of the macros you need for your word processing tasks, you can write-protect your existing Word document templates. Choose Start, Find, Files or Folders, enter *.dot in the Named field, choose My Computer in

the "Look in" list, and click the Find Now button. When the search is complete, select one of the Word templates in the Results field, press Ctrl-A, right-click any of the selected files, and choose Properties. Then place a check mark next to "Read-only" in the resulting dialog box. If a new, infected document slips onto your hard drive, the steps you've taken will stop it from spreading its destructive macros to your other templates.

Trouble on the network

As if viruses that spread through e-mail attachments, hostile Web scripts, and Microsoft Word documents weren't enough to worry about, your PC may also be vulnerable to attacks over the Internet if you share files on a local network. Viruses such as the infamous 911 can gain access to your hard disk through the default Windows link between the File and Print Sharing Service and the TCP/IP Internet protocol.

Internet Explorer 4 and 5 provide protection against this weakness in some Windows configurations by offering to disable File Sharing over TCP/IP when you open the Web browser. But if you connect to the Internet manually through Dial-Up Networking or a dedicated LAN, your PC may still be visible and accessible to any hacker who traces your computer name or IP address.

Fortunately, if you don't get the Internet Explorer warning, unlinking File Sharing from Windows Dial-Up Networking is pretty easy.

Hatch Number 8

1. Right-click the Network Neighborhood icon on the Desktop and click Properties.

2. If you use Dial-Up Networking, scroll down in the network components list and select the instance of TCP/IP bound to the Dial-Up Adapter. (If your computer doesn't have a dedicated network card, only one instance of TCP/IP may appear.) Click the Properties button under the components list and click OK if a TCP/IP Properties warning appears.

3. In the TCP/IP Properties window, select the Bindings tab. If you see a check mark next to "File and printer sharing for Microsoft Networks," remove it. Leave any other bindings on the screen alone. Then click OK to return to the Network Configuration tab.

If you connect to the Internet through a network card or a digital subscriber line adapter, you can guard your computer by unbinding the device's TCP/IP protocol from File and Print Sharing services. Follow the steps outlined above, but instead of looking for TCP/IP bound to the Dial-Up Adapter in step one, look for a line naming TCP/IP and your network device. One catch: You'll lose the ability to share files on a local network unless another network protocol (such as NETBEUI) is installed on your LAN.

As an alternative, if you connect to the Internet through a dedicated network or DSL, you should consider a network firewall. ZoneAlarm is a free software package that does a nice job of shielding your PC from attacks the on Internet. The

program can be tricky to set up, so check our tutorial on installing and configuring it.

Above all, keep in mind that computing in the Internet age is not the same as booting up was ten years ago, when personal computers were still stand-alone devices. A connected PC is caught in a sea of danger, but by battening down Windows' hatches, you've increased your chances of safely sailing through any storm you encounter.

RELATED STORIES:

Microsoft scrambling to fix new Outlook security hole
July 21, 2000
How to protect your network
July 4, 2000
IT pros debate security of Linux and Unix
June 8, 2000
Outlook patch called overkill
May 23, 2000
Top 10 security utilities
May 22, 2000

RELATED IDG.net STORIES:

Microsoft exec promises security
(*Computerworld*)
Lloyd's of London backs insurance against hackers
(*IDG.net*)
Network security threats are growing
(*IDG.net*)
New intrusion-detection devices debut
(*Network World Fusion*)
Cyberdefense mired in Cold War
(*FCW*)
WebAgain can undo hacker damage
(*PC World Online*)
Is Linux a security risk?
(*Computerworld Australia*)
Should you hack back?
(*Network World Fusion*)

RELATED SITES:

Microsoft patch for Outlook 98 and 2000

Back to the top

Note: Pages will open in a new browser window
External sites are not endorsed by CNN Interactive.
