To print: **Click here** *or* Select **File** and then **Print** from your browser's menu

---
This story was printed from Enterprise,
located at http://www.zdnet.com/enterprise.

Ban Outlook--now

By *Steven Vaughan-Nichols*, Enterprise
September 25, 2001 1:13 PM PT
URL:

The list of companies slugged by Nimda, the latest Outlook-transmitted disease (OTD), reads like a who's who in big business, with Sprint, AG Siemens, and Microsoft Japan topping the list. Nimda, known to professionals as W32.Nimda.A@mm, keeps growing and growing. And as I sit in my home in the Blue Ridge Mountains, looking over my NetScreen-10 Firewall Appliance log, I can see the number of attacks on my network rise above twenty--and that's just for today. Norton Anti-Virus for Gateways reports that three Nimda-infected messages have been blasted so far as they tried to reach my Ipswitch mail server. What a great day.

Nimda works in two ways. The first is that old OTD favorite: exploiting holes in how Internet Explorer and Outlook handle MIME attachments to access Microsoft e-mail address lists, and then spreading itself as an attachment to everyone on your address list.

The second is to use the more obscure Unicode Web Traversal exploit. This trick can be played on Internet Information Server 4.0 and 5.0. With it, the server can be fed a malformed URL that then lets the worm get at files and folders on the Web server's file folders' logical drive. From there, much more havoc can be done, but what Nimda does is set up its own Web page, which then prompts site visitors to download an Outlook Express (.eml) file with a fresh copy of the worm attached.

Want to know what makes this truly annoying? Microsoft had already released Nimda's cure. Nimda uses holes that were fixed long before the disease ever arrived. Web Traversal was fixed on October 17, 2000. The MIME exploit? Microsoft fixed that one in March, 2001. I recently suggested that network administrators update their server patches or be pink slipped. I'm still standing by my opinion.

Of course, that only takes care of the current crop. Outlook, with it deep hooks into the operating system, will *always* have security problems. So I'd like to propose a radical way to prevent OTDs: ban Outlook from corporate desktops. You think I'm kidding? I'm not.

Outlook is vulnerable by design. If you want all that power to trade data and code with other Microsoft programs like Excel and Word, security is the price you pay. Even when good users and administrators patch their software, this only closes the barn door after the

horses have fled. So it is that I think the best thing you can do to keep your company working--and not screaming--at their desktops is to drop Outlook now.

Want a replacement? I like Pegasus Mail--and it's free, guys! Eudora also still has its fans and can run on Windows PCs, Macs, and even Palms. Sure, your users can still get Nimda on their machines, but they can't spread it to anyone else via e-mail. I like this idea.

But though banning Outlook would be ideal, there's a problem with its aforementioned replacements. Though their latest versions have or are about to add group/individual scheduling and other personal information manager (PIM) features, this functionality isn't compatible with Outlook or Exchange's PIM features. If your people use Outlook exclusively for e-mail, switching them over to a Pegasus Mail really is the best solution. If they want more, though, you may be stuck with Outlook

So what can you do if your company is as addicted to Outlook? For starters, tell your users (again!) not to open unknown attachments, and not use the view pane in Outlook. Unfortunately, however, the attachment that spreads Nimda is named: *readme.exe*. Because only employees who've slept through Net security briefings would ever open a file with a name like that in the first place, there's not a lot a network administrator can do about them.

If you can't stop Outlook worms at the client level, what can you do at the desktop? Though it won't stop someone from clicking on an executable file, turning off the Windows Scripting Host (WSH) will stop Visual Basic Scripting worms like ILOVEYOU in their tracks. Of course, if your users are using Visual Basic scripting programs, it will stop those, too. But most users aren't doing so. As a result,you can pretty much turn WSH off without any qualms.

You should also turn off ActiveX in Outlook by going to Tool/Option/Security and set the security zone for Outlook HTML mail to Restricted Sites. Then, click on the Zone Setting button, and click your way through Custom and Settings to the Security Settings dialog box and disable all options for ActiveX Controls and plugins and Scripting.

Because worms are now clever enough to be activated simply by having their host message show up in the view panel, you should also disable the view panel. You can do this by going to View/Layout and make sure that Show Preview pane option is not checked on. Unfortunately, you can also expect some users to rise up in arms about losing their preview pane. And worse still, you're probably going to have to go to every workstation to reset those defaults. You might be better off just setting up a new model client setup and pushing it to all desktops with a migration/deployment tool such as the Altris eXpress Migration Toolkit.

So what else can you do if your users won't give up full Outlook functionality and you don't want the CEO calling you out on the carpet the next time the entire office goes on a 48-hour coffee break because the network is hosed? Well, everyone recommends PC-based antivirus programs--and so do I--but there's always one user who manages to turn his or her protection off or doesn't get viral identification files updated. As a result, you should also add viral protection at the mail server and or gateway levels.

By knocking worms and viruses out before Outlook even gets chance to be hit, you'll go a long way toward making sure that your network remains a contender--instead of flat on its

back.