NET TIPS
E-MAIL SECURITY
Mailbox: www.sciencemag.org/dmail.cgi?53844

E-mail Trojan Horses

E-mail is the most common Internet application used at home and at work. Literally millions of users rely on this way to communicate on a daily basis (*1*). Just imagine a week without the technology of e-mail to see how essential it is to today's scientist.

E-mail has become so ubiquitous that you can now get free e-mail accounts from numerous Web sites, and Web browsers have bundled in free programs as add-on components. Recently, however, some bad news has hit many popular e-mail applications. Security flaws were discovered in late July in the mail programs bundled in Microsoft Explorer and Netscape Communicator. One week later, another security flaw was discovered in Eudora Pro. With literally millions of copies of these flawed programs out there, the potential for disaster is great, and users need to be aware of the flaws as well as the fixes that are available. Additional information about these security flaws in MIME (multipurpose Internet mail extension) buffers are further described in the external bulletins on the Web site of the Australian Computer Emergency Response Team (AusCERT; www.auscert.org.au).

The security issue discovered in Internet Explorer and Netscape Communicator is caused by improper handling of file attachments with very long file names (that is, 200 characters or more). This vulnerability was identified first in July by Finnish testers at the University of Oulu. If you receive an e-mail attachment with a very long file name and read your e-mail using the e-mail reader bundled in these browsers, the long file name will cause the application to shut down unexpectedly. A sophisticated hacker could use this flaw to run malicious code that might wreak havoc in your system. Basically, a buffer overrun could occur, and this vulnerability can be exploited to force programs to execute arbitrary commands with the privileges of the user running the program. Also, attempting to open the corrupted file within the browser might lead to the execution of harmful code.

For Microsoft products, the flaw affects Outlook 98 and Outlook Express that were shipped with Microsoft Internet Explorer 4.0 or 4.01 on Windows 98, Windows 95, Windows NT 4.0, and Windows NT for DEC Alpha, Macintosh, or UNIX. Users are advised to download a security patch that is available at the company's Web site (www.microsoft.com/ie/security).

For Netscape products, the mail and news components of Netscape Communicator versions 4.0 through 4.05 and Netscape Communicator 4.5 Preview Release 1 on the Windows 3.1, 95, 98, and NT platforms could be compromised. This vulnerability does not affect the Macintosh or Unix versions of Communicator. Comunicator 4.06, as well as a new version of Communicator 4.5 Preview Release 1, contains a fix for this bug, so users are advised to download upgrades for these browsers from the company's site (http://home.netscape.com/products/security/resources/bugs/longfile.html).

For Eudora Pro, the security flaw is different. Hackers could use the ability of Eudora to render hypertext links within an e-mail message. By linking to hostile applets or scripts in an e-mail message, an executable program could be launched by merely clicking on what seems to be an innocent hypertext link. The versions of the software affected include Eudora Pro 4.0 for Windows and Eudora Pro e-mail 4.0.1 for Windows. The problem does not affect Eudora Pro 4.0 for Macintosh. A patch is available from the company's Web site (http://eudora.qualcomm.com/security.html).

Without a central way to correct the flaws (because millions of copies of these programs are already in use), users need to take charge. Anyone using the versions affected should download and install the fixes immediately. Before doing this, however, make sure you back up your system—something you should do regularly anyway and definitely before installing any new software.

—RICHARD PETERS AND ROBERT SIKORSKI

Reference

1. R. Peters and R. Sikorski, *J. Am. Med. Assoc.* **277**, 1258 (1997).

SITEFINDER
SECURITY ADVISORIES

www.auscert.org.au/Information/advisories.html

For anyone interested in keeping up with security flaws in software and hardware, the Australian Computer Emergency Response Team (AusCERT) Web site publishes advisories and alerts in the field of computer security. These bulletins are organized by date of publication and report on security flaws in operating systems, applications, or hardware. Each bulletin consists of a description of the flaw, its impact, recommended solutions, and "workarounds."

www.mednav.com/zone/science

If computer security is important to you, it is well worth your time to check out this site at least once a month to find out what type of new flaws have been reported. In addition, we have collected a list of security resources on our Web site.

Tech.Sight is published in the third issue of each month. Contributing editors: Robert Sikorski and Richard Peters, Medsite Communications, Boston, MA, USA. Send your comments by e-mail to techsight@aaas.org or via the Web to the mailbox URL with each item.

TECHSIGHTING
ENZYMOLOGY TECHNIQUE
Mailbox: www.sciencemag.org/dmail.cgi?53842a

Two-Hybridzyme

The two-hybrid system, a technique developed in the yeast research community, is widely used. Armed with a couple of plasmids, yeast strains, and toothpicks, the cardiologist, neurobiologist, and immunologist can use the two-hybrid technique to screen clone libraries for novel proteins that bind to any given target. This straightforward technique often leads researchers into very fertile frontiers.

The two-hybrid system has steadily evolved over the past few years to allow formation of diverse types of complexes (one-hybrid, three-hybrid, and so forth). It has also adapted to the ever-increasing knowledge of protein structure, so that the required fusion protein constructs can be made more intelligently. Nevertheless, enzymologists seem to have avoided the technique, because enzyme-substrate complexes have not been byproducts of two-hybrid studies, until now.

The Tsugimoto group from Japan (*1*) has recently succeeded in tweaking the two-hybrid system so that it can be used by researchers looking for candidate protein substrates for a specific enzyme. The authors set out to find the substrates for the enzyme caspase-3, a complex of two polypeptide subunits of 10 and 20 kilodaltons (kD). Caspase-3 is a protease that, in many cell types, cleaves target proteins in a cascade that ultimately leads to cell death by apoptosis. There is great interest in these downstream targets for general study and for possible therapeutic strategies.

Applying the two-hybrid method to the problem of caspase-3 binding partners required careful design of the enzyme fusion proteins and modification of the active site of the enzyme. The crystallographic structure of