InfoWorld. LEAD WITH KNOWLEDGE

SEARCH: [   ] [News ▼] [GO]

Google

Home // News // Article

NEWS

PRINT ARTICLE   EMAIL ARTICLE

IE flaw exploited for MSN Messenger worm

By Joris Evers
February 14, 2002 9:29 am PT

A NEW WORM that uses Microsoft's instant messenger application MSN Messenger to propagate has been spotted by several antivirus software vendors.

The worm arrives in an instant message that contains text telling the recipient to go to one of several Web sites. The text says either "URGENT -- go to (url) now," or "ATTeNT!oN -- go to (url) now." Clicking on the URL (Uniform Resource Locator) link in the message opens a Web page with malicious JavaScript code that sends instant messages advertising the Web page, or other Web pages with the code, to all the MSN Messenger users on the user's contacts list, Symantec and F-Secure said in advisories Thursday.

Dubbed "JS.Menger.Worm" by Symantec and "Coolnow" by F-Secure, the worm sends instant messages, but does no damage to a user's system, the antivirus software vendors said. F-Secure is trying to shut down the sites hosting the malicious code before it becomes very widespread, the company said.

The JavaScript code takes control of MSN Messenger by exploiting a known flaw in Microsoft's Internet Explorer (IE) Web browser. An example of how to stage such an attack was published last weekend by two European experts. That example was used to craft the worm, according to the experts.

"The worm is a modified version of our example code. We never intended for anybody to copy the code, although we kind of expected it would happen," said Thor Larholm, one of the two Europeans who demonstrated how specially crafted code on a Web page could take over MSN Messenger. "We published the example to put pressure on Microsoft to patch vulnerabilities that they are fully aware of."

Microsoft on Monday released a bundle of patches for IE that fixes the flaw used by the MSN Messenger worm, Larholm and the antivirus software vendors said.

Still, a PC with IE is all but secure, according to Larholm.

"The patch doesn't fix all the problems in IE. It fixes a lot, Microsoft deserves kudos for that, but there are still publicly known vulnerabilities, some two

months old, that allow an attacker to read any local file and execute arbitrary commands on a user's system," Larholm said. The Danish Internet programmer maintains a list of unplugged holes on his Web site (http://jscript.dk/unpatched/).

Both Symantec and F-Secure have updated their antivirus products so they can detect the worm. No one at Microsoft was immediately available to comment.

Joris Evers is an Amsterdam correspondent for the IDG News Service, an InfoWorld affiliate.

RELATED ARTICLES
▶ Microsoft security patch said ineffective
▶ Microsoft battles old, new security holes with IE patch

RELATED SUBJECTS
▶ Security
▶ Web Technologies

SUBSCRIBE TO: ▶ E-mail Newsletters ▶ InfoWorld
Mobile ▶ InfoWorld Magazine

Home // News // Article

PRINT ARTICLE   EMAIL ARTICLE

BACK TO TOP   DISCUSS ARTICLE

ABOUT INFOWORLD | SITE MAP | EMPLOYMENT | PRIVACY | CONTACT US