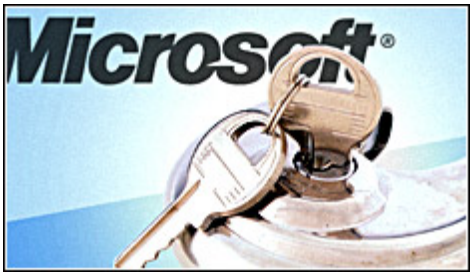
Site Updated: 12:56 AM/EST March 26, 2004

TOP STORIES



Microsoft Belatedly Starting its Engine

Microsoft chief Steve Ballmer conceded Thursday that the company's one big recent misstep was neglecting search technology. No more, as the company is gearing up for a battle in the search-engine market.

- MSN Altering Paid Search Listings
- Google Dives into Local Search
- Paid Inclusion Under Fire at Search-Engine Shindig
- Yahoo Stakes Out Paid Search Path
- Is Google Web Search at Risk?

News

VoIP's Open-Source Move

SIPfoundry, a nonprofit initiative, will be announced at next week's VON conference. The group hopes to spark open-source development for Internet telephony.

News

Speech Technology Making Enterprise Inroads

Leading speech vendors say the challenges now are to keep improving recognition and the usefulness of applications.

News

New Worms Stretching Across Web

New worms, Snapper and Mywife, moved in the wild Thursday. Although they're low-level threats, one has potential for widespread mischief.

More News >>

Windows

EU Hits Microsoft With Record Fine

eWEEK.com's special report follows the long road to this week's decision and looks at the chance of further legal actions against Microsoft.

EDITOR'S NOTE

Blogs and TalkBacks for eWEEK.com

Executive Editor Matthew Rothenberg cuts the ribbon on new features for reader interaction and lively analysis.

eWEEK TOPIC CENTERS

SECURITY MORE>

- Sarvega Appliance Inspects XML Traffic
- Web-based Mail Threat Looms
- Netsky.P Spreads Through Ancient Security Hole

LINUX & OPEN SOURCE MORE>

- Lotus Founder: Open Source is Route Worth Taking
- Augustin's 8 Simple Rules for Open-Source Business Strategy
- IBM Upgrades Speech Offerings, Plans Linux Support

BREAKING NEWS

3.25.2004
Cognos Names New CEO on Heels of Strong Quarter

3.25.2004
Pingtel Goes Open Source with IP Telephony Platform

3.25.2004
HP Sues Gateway for Patent Infringement

3.25.2004
'FlashMob' Networks PCs for Ad-Hoc Supercomputer

3.25.2004
Microsoft Concedes Misstep in Search Market

3.25.2004
Speech Making Enterprise Inroads, Top Vendors Say

3.25.2004
New Worms Stretching Across Web

View All >

WEBLOGS

David Coursey XML

Microsoft Didn't Fake Linux TCO Studies

Vendor-sponsored studies are always open to question, especially on controversial topics. So I was very interested to read about a new study comparing total cost of ownership for Linux vs. Windows servers.

Larry Seltzer XML

Full-Discord

As great as my own site may be, the cutting edge for security is in mailing lists, where researchers and other interested parties like me share information.

Steve Gillmor XML

Virtual Schmirtual

Security

New Worms Stretching Across Web

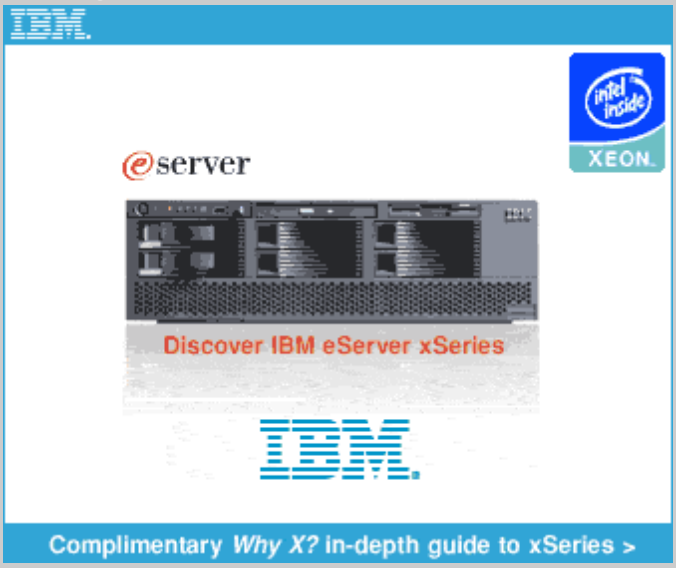
By Dennis Fisher

March 25, 2004

Two new low-threat worms are making the rounds on the Internet Thursday, continuing the plague of malware that began in January and has shown no signs whatsoever of abating.

eWEEK.com Special Report:
E-mail Worms 2004

Of the two worms, known as Mywife and Snapper, the former appears to be the more worrisome and have the greater potential for spreading widely, security services said. Mywife arrives in an e-mail with a spoofed sending address and any one of several vaguely pornographic subject lines, including, "very hot XXX" and "FW:RE: Hot Erotic." The body of the e-mail also varies and some of the messages are quite graphic.



The e-mail contains two attachments, one of which is simply a graphic file that displays a fake Norton AntiVirus 2004 logo, supposedly certifying that the other attachment is virus-free. The second attached file is compressed and can have any one of several names, including: Aprilgoostree, Parishilton, Rickymartin or a handful of profanities. The compressed file contains a third file with either an .exe or .scr extension, according to an analysis of the worm done by Panda Software Inc.

A second version of the virus-infected e-mail carries a fake virus warning, purportedly from antivirus vendor Symantec Corp., informing recipients that their machine is infected by the fictitious BlackWorm virus. This version has an attachment named either Scan.tge or Scan. zip.

The Mywife code also contains a jab at Microsoft Corp., although it is never displayed on the user's screen: "microsoft do u hear me? we gon kick u ass an *** u down u got my word **Black Worm**."

Once resident on a computer, Mywife goes to work removing the Windows registry entries for a variety of antivirus and security applications.

The Snapper worm is quite different from Mywife, and in fact resembles the last few variants of the Bagle virus that showed up last week. Instead of relying on the user to open an infected attachment, Snapper sends blank e-mails with spoofed sending addresses that contain code that automatically executes once the message is opened or viewed in the preview pane in Outlook. The code causes the local host computer to connect to a remote Web server located at 198.170.245.129 and try to download a file called HTMLhelp.cgi.

Click here to read more about the latest Bagle variants.

Like Bagle.Q and subsequent variants, Snapper exploits the object tag vulnerability in Internet Explorer to force the infected

machine to download the file. That file then runs a piece of VB Script code that creates and executes a DLL in the Windows directory. The DLL, called IEload.dll, is 8,704 bytes in size.

Snapper then sends itself to all of the addresses in the user's address book. However, the CGI file is not available on the remote Web server, making it unlikely that Snapper will spread very far, according to Network Associates Inc.'s McAfee Security unit.

Network Associates, based in Santa Clara, Calif., listed both Snapper and Mywife as low threats.

Check out eWEEK.com's Security Center at http://security.eweek.com for security news, views and analysis. Be sure to add our eWEEK.com security news feed to your RSS newsreader or My Yahoo page: XML add to My YAHOO!