

Reprint from June 26, 2004 AOL News

Web Virus May Be Stealing Financial Data

New Scheme Causes Web Sites to Spread the Bug

By ANICK JESDANUN, AP

A computer virus designed to steal valuable information like passwords spread Friday through a new technique that converted popular Web sites into virus transmitters.

Though the impact of the "Scob" outbreak was mild compared with recent infections like "Sasser" and "Blaster," security experts worried about its method of delivery.

With Scob, virus writers have discovered yet another way – beyond e-mail and network techniques – of distributing their malicious code.

Talk About It

- Chat | Post Messages
- Top News Boards

Now that the exploit is out, it won't be long before others adapt it for spamming and for launching broad attacks to cripple the Internet, said Alfred Huger, senior director of engineering at security company Symantec Corp.

The infection, first discovered by Microsoft Corp. on Thursday, appears to take advantage of three separate flaws with Microsoft products and can be difficult to detect.

Stephen Toulouse, a security program manager at Microsoft, said software updates to fix two of them had been released in April, but the third flaw



was newly discovered and had no patch available yet.

He recommended that computer owners obtain the latest security updates for Microsoft products and their anti-virus and firewall programs. For the flaw that lacks a patch, he said, users should also turn up security settings on Microsoft's Internet Explorer browsers to the highest levels.

More on This Story

- [Microsoft Bulletin](#)
- [Anti-Virus Center](#)
- [AOL Computing](#)

Users could also turn off the "JavaScript" feature on their Microsoft browsers, though doing so could cripple functions on some sites.

The virus does not affect Macintosh versions of Internet Explorer, nor does it spread through non-Microsoft browsers like Mozilla and Opera.

Users can search their computers for the files "Kk32.dll" or "Surf.dat" to see if they are infected. Removal tools are available from major anti-virus vendors.

Experts said the infection was unusually broad but wasn't substantially interfering with Internet traffic.

The U.S. Computer Emergency Readiness Team warned that any Web site, even those trusted by users, might be a vector for spreading the virus.

Security experts worked Friday to pin down how hackers managed to infect hundreds and possibly thousands of Web sites. It appears to target at least one recent version of Microsoft software for operating Web sites, called Internet Information Server.

Hackers made subtle changes to the Web site so visitors get a piece of code that's designed to retrieve, from a Russian Web site, software that records a person's keystrokes.

Such data, which can include credit card numbers, bank accounts and passwords, are collected for remote delivery to hackers, experts say.

The virus, however, does not attempt to spread itself, helping to limit its

effect.

Web sites have been used before to spread a form of spyware called "browser hijackers." One, known as Qhosts, disables access to major search engines and resets the Internet Explorer browser home page to a little-known site.

But those typically have involved "users having been visiting shady sites," Chris Kraft, senior security analyst at Sophos Inc. Here, hackers plant the code on business, government and other everyday sites they do not normally con