August 4, 1998

Hacker Group Says Program Can Exploit Microsoft Security Hole

By MATT RICHTEL BIO

LAS VEGAS -- A group of computer hackers, one of whose members recently spoke to Congress about vulnerabilities in the national computer infrastructure, said they planned to release on Monday a program they say can be used to hack into and wreak havoc on machines that use the Windows operating systems.

Members of the hacker group, known as "Cult of the Dead Cow," said they are releasing the program to encourage Microsoft Corp. to pay closer attention to computer security issues.

However, a Microsoft spokesman said the company is not concerned about the program and that it does not expose or create any new vulnerabilities. "This is not a tool we should take seriously, or our customers should take seriously," said Edmund Muth, who oversees security for Microsoft's enterprise marketing group.

He said Microsoft has not yet seen the program, but that it is working with a computer security company that has seen it. The company, Atlanta-based Internet Security Systems Inc., said it is working with Microsoft to develop software so companies can determine if the program has been installed on one of their computers.

Related Articles
The Hacker Myth Crumbles at Convention (August 2, 1998)

Hacker Convention Takes On a Corporate Tone (July 31, 1998)

CyberTimes Special
HackStock: A Reporter's Fact-Finding Mission

Other computer security consultants acknowledged the program does not expose any new vulnerabilities in Microsoft operating systems. However, they said it makes it much easier to exploit those holes, meaning that computer running Windows 95 or 98 could be vulnerable to a wider group of those with ill intentions.

"It's not going to change the balance of power overnight," said Robert J. Stratton, a consultant for Security Design International in Falls Church, Va. "But it could be disconcerting if people decide to employ it."

The program is called "Back Orifice," which is meant as a play on words parodying Microsoft's Office suite. Members of the hacker group said that an outsider who gains access to a computer using their program would be able to control the computer and its software just as if they were sitting at the actual terminal.

In other words, the remote user would be able to see what's on the screen, install and download files, delete or edit text and view or manipulate databases and spreadsheets.

TODAY IN TECHNOLOGY

Business Technology
Ascend to Acquire Stratus for $822 Million

Software Makers Offer to Help ... Themselves

Spanish Phone Utility Extends Its Latin American Leadership

Kodak to Acquire Medical Imaging Business From Imation

According to Microsoft, programs that allow this type of access already exist for use within networks by company system administrators. However, the hackers, and some computer security consultants, say this is the first time such a tool has been widely and freely distributed to the public.

"Once it is installed, a remote administrator has more control over the computer than the person sitting at the console," said DilDog, a hacker who helped write some of the Dead Cow group's coding. He said the reason the remote user would have more control is because they would have access to base-level commands, enabling them to manipulate more information than if they used the Windows graphical user interface.

There is at least one factor that may limit how much damage the program can cause. In order for a person to take control of a computer using Back Orifice, they must first install a copy of the program on the target computer. This could be done by physically loading the program, or by sending an e-mail attachment or other electronic file that would have to be downloaded and opened.

Stratton, the security consultant, said that one way companies can further guard against any attacks is to make sure they don't leave their "file sharing" program open to the Internet. When that particular program is open, it permits employees to freely exchange files over the Internet, but also makes it possible for outside users to send in unwanted files.

Stratton said it may also be possible for companies to modify their virus scanners to look for and block incoming files that contain the program.

Allan Bailey, a product operations engineer for the search service Excite, described the program as a "very, very bad exploit." "It means we're going to have to batten down the hatches and make secure our PC networks."

At the same time, he said he believes some good could come of the program because it will force Microsoft to pay closer attention to network security. He said Microsoft has been criticized for not reacting quickly enough to vulnerabilities, "and this could force the issue."

Cult of the Dead Cow members said it took a year to write the program, which was created predominately by Josh Buchbinder, a hacker who goes by the name "Sir Dystic." They said the program is meant as a viable network tool but also as a way to raise awareness about security problems with Microsoft programs.

Some computer security professionals questioned that motivation. Ira S. Winkler, president of Information Security Advisors Group, and someone who is close to the hacker community, said the Cult of the Dead Cow has identified and glorified a problem without offering a solution.

Also, he said that even if the hacker group is managing to force Microsoft's hand, it is doing so at the expense of innocent corporations and individuals who use Windows operating systems. "They're extorting Microsoft by torturing innocent victims," he said.

Christoper Klaus, the founder of Internet Security Systems -- the company Microsoft is consulting on this issue -- said the release of the program might be valuable in raising the awareness of system administrators about threats to their network security.

Related Sites

Following are links to the external Web sites mentioned in this article. These sites are not part of The New York Times on the Web, and The Times has no control over their content or availability. When you have finished visiting any of these sites, you will be able to return to this page by clicking on your Web browser's "Back" button or icon until this page reappears.

- Microsoft Corp.
- Internet Security Systems
- Security Design International
- Excite

Matt Richtel at mrichtel@nytimes.com welcomes your comments and suggestions.
