

Windows weakness can lead to network traffic hijacks

By Joris Evers

http://news.com.com/Windows+weakness+can+lead+to+network+traffic+hijacks/2100-1002_3-6170229.html

Story last modified Mon Mar 26 12:38:31 PDT 2007

WASHINGTON--A problem in the way Windows PCs obtain network settings could let attackers hijack traffic, security researchers said Saturday.

The problem occurs because of a design bug in the system used by Windows PCs to obtain proxy settings, researchers with security firm [IOActive](#) said at the ShmooCon hacker conference here. As a result, an attacker with access to a network at a corporation, for example, could insert a malicious proxy and [see all the traffic](#), the researchers said.

"The upshot of it is that I can become your proxy server without you knowing about it," Chris Paget, director of research and development at IOActive, said in an interview after his presentation on the problem. "I can put up the equivalent of a detour sign on your network and redirect all the traffic."

An attacker can set up that "detour sign" because Internet Explorer on Windows PCs by default searches for a proxy server using the [Web Proxy Autodiscovery Protocol](#), or WPAD, Paget said. It turns out that an attacker can easily register a proxy server on a network using the [Windows Internet Naming Service](#), or WINS, and other network services including the [Domain Name System](#), or DNS, he said.

"When IE starts up, it will ask the network where its proxy server is," Paget said. "It is really easy to put up your hand and say: 'Here I am.'"

Microsoft acknowledged the problem in a [support article published Saturday](#) on its TechNet Web site. "If an entity can surreptitiously register a WPAD entry in DNS or in WINS clients may be able to route their Internet traffic through a malicious proxy server," Microsoft said in its support article.

If an attack is successful, all traffic on a network will flow through the attacker's proxy. This means the attacker can access all the data, redirect and manipulate it and carry out all kinds of other nefarious acts, Paget said.

Still, the proxy problem isn't a critical security issue, Paget and fellow IOActive security expert Dan Kaminsky said. An attack is possible only with access to the target network, not from the Internet, they noted. "The biggest risk inside a corporation would come from a malicious insider," Paget said. "This is not worthy of mass panic or critical advisories."

That doesn't remove the need to fix the problem. Insider threats are real. Also, the proxy problem may be appealing to attackers who find it increasingly hard to exploit other vulnerabilities, Kaminsky said.

"Buffer overflows and other bugs have gotten a lot harder to do, so design issues like this have gotten a lot more interesting for attackers," he said.

Problems with WPAD aren't new. Seven years ago Microsoft patched IE 5 because the browser would search for a proxy server on the Internet if it failed to find one on its local network. That let a malicious hacker give settings to the browser that would facilitate a broader attack.

Such a problem was exploited by somebody who registered the domain name "wpad.org.uk" and served a "wpad.dat" file with proxy information to Windows PCs looking for it. As a result the people using those PCs ended up on an online auction Web site regardless of the address they typed into their browser.

In its [support article](#), Microsoft lists steps for network administrators to address the WPAD problem. The steps reserve static WPAD DNS host names and to reserve WPAD WINS name records. As a result, an attacker's malicious WPAD name will no longer work, which will foil the malicious proxy trick, Paget said.

[Copyright](#) ©1995-2007 CNET Networks, Inc. All rights reserved.



Credit: Joris Evers/CNET News.com
Chris Paget, director of research and development at IOActive, during his ShmooCon presentation.

Now on News.com:

- [At Kink.com, making a fetish of HD](#)
- [Newsmaker: For Chicago chef, it's prepare, print, serve](#)
- [Newsmaker: Solar as a service? SunEdison thinks so](#)
- [Extra: More on the Sonic/Mario Olympics game](#)