From ENTmag.com:

News

print article

More News

- Yukon's Broad Beta Slated for Second Half of 2002
- Microsoft Tool to Tighten .NET-SQL Server Bond
- Exchange SP2 Enhances Outlook Web Access
- Compaq Offers Windows Systems Based on Oracle Clustering
- Goner Mass-Mailing Worm Makes the Rounds

Sticking it Out on IIS

by Stephen Swoyer

11/15/2001 — The success of attack worms like Code Red, Code Blue and Nimda prompted some industry watchers to suggest that enterprise users should reconsider their use of Microsoft's IIS Web hosting platform.

Several IIS users ENT spoke with, however, say that such caution is misplaced. Some cite the difficulties associated with migrating from IIS to another platform. Still others maintain that IIS isn't any more or less secure than Sun-Netscape's iPlanet or the open source Apache Web servers. Most seem disinclined even to consider alternatives to their existing IIS deployments.

"It's only due to its popularity that [IIS] is the prime target for exploits. If everyone moved to Netscape, the focus would only shift to that platform," explains Simon Jones, an IIS administrator with a UK-based telecommunications giant.

After the appearance of the Nimda virus in early September, at least one prominent analyst, Gartner Group's John Pescatore, stated that IT organizations needed to think about investigating alternatives to IIS.

"Gartner recommends that enterprises hit by both Code Red and Nimda immediately investigate alternatives to IIS, including moving Web applications to Web server software from other vendors, such as iPlanet and Apache," he wrote in a Gartner advisory bulletin.

Appearing in early November, U.K.-based research outfit Netcraft's Web server survey for the month of October seemed to suggest that IT organizations were taking Pescatore's advice to heart. In its October survey, Netcraft found that 131,417 of the sites that had once hosted IIS were now running some other Web server, mostly Apache. Netcraft noted that 1,709 former IIS sites had moved to iPlanet, while 1,506 were running the open source Zeus Web server platform.

Netcraft later updated its report to show that *more* sites had switched from other platforms *to* IIS in the same month -- 148,000. iPlanet/Netscape-Enterprise lost three times as many sites to IIS as it gained from Microsoft's server in its high-profile migration promotion, according to Netcraft.

And Russ Cooper, editor of the Windows NT Bugtraq mailing list and a security analyst with TruSecure Corp., the Netcraft numbers also show that IIS grew its overall share of sites (to 29 percent, representing about 9.6 million sites) in October –- while Apache actually lost a little ground. As a result of this, Cooper contends, the Netcraft numbers probably don't tell the whole story.

"One has to wonder how many IIS sites were taken off the Net simply because they weren't supposed to be accessible in the first place," he speculates, noting that, as a result of Code Red, some broadband service providers cut off access to Web services hosted by their residential customers on DSL or cable modem connections. "I think that Code Red and Nimda demonstrated that a lot of IIS services were exposed that should not have been accessible, and I know that a lot of internal sites had

to get rid of IIS running on desktop machines."

Still, the Netcraft numbers indicate 65 times as many sites switched from IIS to other platforms in October as did the switch in September (131,000 versus 2,000).

For the most part, Cooper and other analysts say that users won't rip and replace IIS because the move would probably require replacing Windows NT 4.0 or Windows 2000, as well. After all, analysts point out, IIS' security is ultimately dependent upon the integrity of its Window NT 4.0 or Windows 2000 base.

"It is a ludicrous assumption to say that people are going to trivially switch from IIS to anything else for anything that's in production, although they may well be reconsidering development plans," Cooper says. "But remember, it's simply not trivial to take a strategy that involved Microsoft products and then try to understand what the compatible bits and pieces are for use in another environment."

Besides, says Dan Kusnetzky, director of worldwide operating environments for IDC, IT managers almost never rip and replace solutions that work.

"IT management almost never rips out something which is largely working and replaces it with something else. One of the key mottos of the IT executive is to use things until they fall apart. They don't throw things away," he says.

John Stemper, an IIS administrator with direct sales vendor Antioch Publishing, says that his IT organization's operations were impacted to some extent by Code Red, primarily as a result of the frenetic network traffic that the attack worm generated as it searched the Internet for additional hosts to infect.

"Our network administrators are very diligent about applying patches so most of our machines were already protected," he says. "The remaining machines were patched in a few hours. The ease of obtaining the patches from Microsoft made the issue much less of a problem than it could have been."

Because of this, Stemper says, he hasn't given much thought to replacing IIS with another Web server platform. Besides, he confesses, his IT organization already moved once from another platform – Apache – to IIS. "We used to be an all-Apache shop. We had a very difficult time finding the detailed help that we needed when issues arose," he avers, adding: "We were affected more by hacking attempts and cracks then than we ever have been with IIS."

John Catalano, an IIS administrator with Atlanta-based Internet service provider 323 Interactive, says that his IT organization was affected during the very first wave of Code Red attacks – before the worm was even identified as such by Microsoft and by members of the security community.

In spite of his close scrape with Code Red, Catalano claims that he hasn't given any thought to replacing IIS in his environment. "We feel that this is a very functional part of hosting and that we just need to attempt to monitor our equipment as best we can to help ensure its security," he comments, noting that his IT organization was able to patch its systems against Code Red within hours after it was first attacked.

Don Lester, an IIS administrator with Clinitech Information Resources, says that he doesn't agree with analysts who suggest that companies should consider replacing IIS with other Web server platforms.

"Microsoft IIS is a popular target because it is a popular platform," he

points out. “If 5 percent of the market used IIS, there would not be as many threats because they wouldn't be as productive for those who are writing the programs to infect and compromise them.”

At the same time, Lester grants, Microsoft has done an adequate job helping IT administrators secure their IIS systems. “Following the instructions Microsoft has in place and using their existing tools will go a long way toward securing IIS. Unfortunately, those tools are not very practical for an extremely large network,” he remarks, citing hotfix management as a particularly burdensome task.

Stephen Swoyer is a contributing editor at ENT and a freelance IT reporter. You can contact Stephen about "Sticking it Out on IIS" at stephen.swoyer@shakespeareandcompany.net.

back to previous page