CMP United Business Media
CRN Vital Information for VARs and Technology Integrators

August 15, 2003
Network & Security Technologies

NEWS: THE AFTERMATH

Blaster: What's Next?

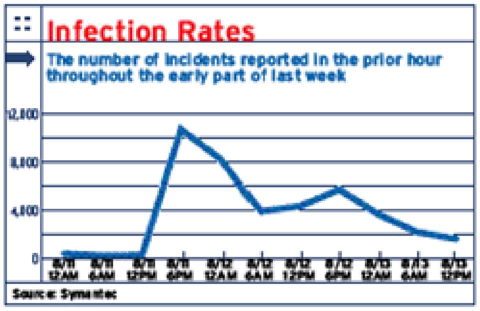
As worm winds down, solution providers fear there's more to come

By Marcia Savage
CRN

- 5:17 PM EST Fri., Aug. 15, 2003

Security solution providers said they fear the worst is yet to come in the wake of last week's Blaster worm, which ripped through the Internet and crashed thousands of systems worldwide by exploiting a known vulnerability in Microsoft Windows.

Gary Morse, president of Razorpoint Security Technologies, a New York-based security services firm, described the self-propagating Blaster,also called Lovsan and MSBlast,as "a very efficient exploitation device." A relatively inexperienced hacker could easily add functionality to Blaster that makes its payload more dangerous, he added.


Infection Rates
The number of incidents reported in the prior hour throughout the early part of last week

Source: Symantec

Although Blaster caused systems to reboot, it didn't destroy files.

While the rate of new Blaster infections appeared to slow by midweek, users need to remain vigilant about patching their systems, said Charles Kaplan, senior director of research at Guardent, a managed security provider in Waltham, Mass.

Discussions among hacker groups on the Internet indicate that other code that exploits the same vulnerability could be in the works, he said.

Blaster exploits a buffer overflow in a component of the Remote Procedure Call (RPC) protocol used by Windows. It scans random ranges of IP addresses on port 135 for vulnerable systems and directs those systems to download the MSBlast.exe file via TFTP.

Microsoft issued an alert and patch for the flaw July 16. It affects Windows NT 4.0, 2000, XP and Server 2003.

Blaster was programmed to launch a distributed denial-of-service attack against Microsoft's Windows Update site on Aug. 16. Antivirus vendors identified variants of the worm last week, but they didn't appear to be as widespread as the original.

Adam Lipson, president and CEO of Network & Security Technologies, a Pearl River, N.Y.-based consulting firm, said Blaster caught many users off guard because it spreads through Internet connections, not e-mail, as past attacks have done. The worm illustrates the problem with patches, Lipson said.

Lipson: Blaster caught many off guard because of the way it spreads.

"There's been a general feeling in the business community that the onslaught of patches hasn't helped, and [that] in some cases, they have caused more problems than they solve," he said.

While patches are part of the security process, customers need to implement an overall defense-in-depth strategy that secures internal networks in addition to locking down the perimeter, Lipson said.

Razorpoint advises customers to be proactive instead of reactive in waiting for the next patch, Morse said. Proactive steps include hardening operating systems, segmenting the network and installing firewalls that are more intelligent about applications, he said.