

Lack of Security Processes Keeps Sending Enterprises to 'Code Red'

John Pescatore

Predictably, the Code Red worm did not live up to its hype. The episode illustrates that panic ensues when a virus emerges because many enterprises fail to establish processes for keeping their IT security up to date.

NEWS ANALYSIS

Event

On 1 August 2001, security experts estimated that the Code Red worm had done relatively little damage, although the final assessment would take some time. One research firm, Computer Economics, estimated that enterprises worldwide spent \$1.2 billion fixing vulnerabilities in their IT systems that Code Red could exploit. The worm propagates itself over TCP/IP connections and exploits a weakness in Microsoft's Internet Information Server (IIS) software, which runs on the Windows NT and 2000 operating systems. The worm directs infected PCs on the last day of the month to launch a denial-of-service (DOS) attack against the Web site of the U.S. White House.

Analysis

DOS attacks send floods of data packets to target servers to make them crash or at least use up all available bandwidth and block legitimate access to the server. Emerging during a slow news cycle, the Code Red worm caused a massive DOS attack of another kind as the media made proclamations about Code Red's impact and unleashed a tsunami of e-mail alerts, press releases and predictions of the Internet's collapse. The bandwidth and attention consumed by this hype greatly outweighed the impact of the Code Red worm itself.

Code Red will undoubtedly spur more government infrastructure protection committees, more investigations and more press releases. However, Gartner believes that this and similar incidents, which seem to occur monthly, really beg two simple questions:

- Why do Microsoft's software products continue to provide easily exploited openings for such attacks?
- Why do enterprises that use Microsoft's software fail to deploy the patches Microsoft releases to close those openings?

Microsoft's Windows NT and 2000 — and particularly the IIS Web server program included with them — have had a continuing stream of security vulnerabilities exposed. Gartner has published a number of notes advising enterprises to take extra security precautions (see *Gartner FirstTake* FT-13-6734 "Another Windows 2000 Flaw Exposes Microsoft Security Weaknesses"). Enterprises should recognize that any use of IIS in Internet-connected applications requires constant vigilance for security alerts, continual application of security patches, and the use of additional security products and services that quickly detect vulnerabilities and attacks against the numerous security holes in IIS.

Above all, enterprises should establish processes to make sure they promptly apply all security patches to all Internet-exposed systems and replace with more secure products those that continually have vulnerabilities exposed. As long as enterprises continue to use free software and expect to get more security than they paid for, attacks like Code Red will have a high probability of either succeeding in direct attacks or eating up attention and resources as hype makes enterprises suddenly realize their vulnerability.

Analytical Source: John Pescatore, Information Security Strategies

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Level 7, 40 Miller Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Latin America Headquarters
Av. das Nações Unidas 12.551
9 andar—WTC
04578-903 São Paulo SP
BRAZIL
+55 11 3443 1509