In the last article in this short series about the implications of the CodeRed family of worms, I looked at the new variant called CodeRedII. In this article, I review some of the defenses that can help to fight infection by these malicious agents.

I was interested in three of press releases that came my way in the wake of the CodeRed news. The first was from my former employer, TruSecure Corporation <http://www.trusecure.com>. The news was that with an estimated 650,000 infected systems worldwide, not a single TruSecure customer was infected. The company explained this result by pointing out that their clients were warned of the IIS buffer overflow vulnerability a year ago; that the TruSecure process involves repeated testing to identify continued vulnerability and that the vulnerable customers were nagged to update their systems using the right patches. Now, even though I own stock in the TruSecure Corporation, I hope I am not biased in thinking that they’re doing it right for their clients.

The next press release that caught my eye was from PatchLink Corporation <http://www.patchlink.com>, which makes what sounds like a useful product for managing software patches. Patchlink Update 3.0 is currently in beta-test (should be available in the production version later this year) but is reported to have protected its users against the CodeRed worms. The product scans for patches appropriate for a system, downloads the right patches, and then reports on its findings to system administrators so they can decide whether and when to deploy the patches. It’s about time: we have the same kind of automated service from some of our antivirus products (mine checks for updates several times an hour because I have a new persistent connection to the Internet via a satellite link) and many other products (e.g., McAfee OilChange automatically looks for updates to a wide variety of programs).

Finally, a press release from Ubizen <http://www.ubizen.com> stated that its MultiSecure DMZ/Shield protected a customer against infection by the CodeRed worm(s). “MultiSecure DMZ/Shield protects the area between a company's Webserver and firewall, an area referred to as the 'demilitarized zone', or DMZ. The shield works as a scanner, checking all requests sent to the Webserver before passing the data onto the web applications. In essence, DMZ/Shield analyzes all http traffic for content not trusted, not expected, and not known by the Web servers. This process guarantees protection against unknown Web server security bugs and is the reason even new and tweaked versions of the Code Red Worm did not infect the [client] site.”

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mkabay@compuserve.com>. He invites inquiries about his information security and operations management courses and consulting services.

Copyright © 2001 M. E. Kabay. All rights reserved.
Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.