PCWorld.com - Motives of Code Red Bug Hunters Questioned

Code Red's astonishing success at infecting computers has reignited a fierce debate about full disclosure--the practice of publishing information about security holes. The discussion has even led some to question the motives of those who discovered the hole in the Microsoft software that Code Red exploited.

At the center of the storm is eEye Digital Security, the company that uncovered and posted information about the .ida buffer overflow problem in Microsoft's Internet Information Server 5.

The company notified Microsoft of the problem in May 2001, and waited until June 18 for a patch before publishing its information on the hole. Despite the wait, critics have denounced the company, suggesting it published too many details about the vulnerability.

That information, says Richard L. Smith, chief technology officer of the Privacy Foundation, may have helped someone to create and unleash Code Red a month later.

Too Much Information

Smith says eEye showed "poor judgment" in releasing full details about the vulnerability and then publishing a detailed analysis about how the worm worked once it appeared.

That information let someone--perhaps Code Red's originator--tweak the worm four days later and create a second, more aggressive version that infected more computers than the first had, he says.

"The fact that [eEye] explained how the virus works, to the point of explaining how you execute the code that exploits it, was too much information," Smith says. "You'll find 10 to 20 other descriptions of Code Red on [antivirus] sites, but you won't find details of the internal operations of the virus."

Smith also questions eEye's motives. The company markets a product called Secure IIS that protects servers from malicious programs like Code Red.

"The more troubles there are for IIS, the more potential sales they can have for their Secure IIS product," Smith says.

Marc Maiffret, "chief hacking officer" of eEye, says the company behaved no differently than any other bug hunter who posts information on the Internet.

"The information we posted was enough so people would have the tools to make sure [Microsoft's] patch was actually working and so that organizations would be able to update their intrusion detection systems," he says.

Maiffret denies that eEye helped someone develop Code Red. In fact, he says, an earlier worm almost identical to Code Red appeared in February. That was long before eEye published its report, he says.

That worm, which appeared on systems belonging to Sandia National Laboratories, also attempted to launch a denial-of-service attack against the White House Web site. However, that worm was different in one crucial way: It affected .htr files in IIS 4.0. Microsoft released a patch to cover that vulnerability in June 1999.

"[It was] a worm written without any information from eEye," Maiffret says.

But while the .htr worm existed before eEye's June announcement, Tim Toole, one of two network security administrators at Sandia who found the .htr worm, notes that whoever wrote it seems to have adapted it for the .ida vulnerability once that became public.

In other words, Toole says, the author of Code Red simply waited for the announcement of a new, unpatched hole against which he or she could launch an already tested worm.

All of this raises chicken-and-egg questions about whether publishing information about vulnerabilities increases or reduces the chance of cyberattacks.

To Disclose or Not to Disclose?

The issue of full disclosure has long been a topic of contention between those who say that disclosure improves security on the Internet and those who say it hands crackers (criminal hackers) the tools they need to break into systems. Those in the former camp say that the embarrassment of public disclosure forces software vendors to patch faulty products.

It also raises awareness among the public of the need for better security and helps network administrators and consumers protect their systems by telling them about holes that crackers may already be exploiting.

But those opposed to disclosure say that crackers monitor online security discussions for talk about new vulnerabilities, then create exploits (malicious code) to attack those vulnerabilities.

A wide-range of groups track down security holes. Sometimes it's a security company like eEye; other times it might be an attentive system administrator that stumbles upon one. Occasionally white-hat hackers, who serve as informal watchdogs over software vendors, locate them; other times crackers find holes simply to exploit them.

Most bug hunters, including some hackers, contact a software vendor about a hole before posting information about it to an online security discussion list like BugTraq. This lets the vendor create and post a patch for the hole at the same time the vulnerability is announced.

But other bug hunters post with no warning, and some give vendors only a week's notice before posting. Georgi Guninski, a prolific bug sleuth out of Bulgaria who has discovered a number of vulnerabilities in Internet Explorer among other products, is apt to give vendors a mere 24 hours to fix a hole before reporting it. But he generally posts workaround solutions to help people deal with the hole until a proper patch comes out.