washingtonpost.com

'Good' Worm Fixes Infected Computers

By Brian Krebs
washingtonpost.com Staff Writer
Monday, August 18, 2003; 2:55 PM

A new Internet worm emerged today that is designed to seek out and fix any computer that remains vulnerable to "Blaster," the worm that attacked more than 500,000 computers worldwide last week.

The new worm scours the Internet for computers already infected with Blaster and deletes the "bad" worm, according to two anti-virus software vendors. The worm then fixes the computers with one of eight software patches developed by Microsoft Corp, and it uses infected computers as a base for searching the Internet for other vulnerable systems. Blaster and the new worm both target vulnerabilities in recent versions of Windows XP, Windows 2000 and Windows NT 4.0.

Even though the new worm is "good," it can cause plenty of trouble for computer users, said Oliver Friedrichs, senior manager at Symantec Security Response, an Internet security company based in Cupertino, Calif.

Once it infects a computer, it is programmed to remain there until Jan. 1, 2004, all the while scanning the Internet for other computers to infect. That activity saps an infected computer's processing power and Internet connection speed, Friedrichs said.

A Microsoft official declined to comment on the new worm.

The Blaster worm was first identified last Monday. It instructed infected computers to launch a denial-of-service attack on Microsoft's security Web site beginning on Saturday. That attack largely fizzled, however, after Microsoft disabled the targeted site.

The unprecedented media attention given to Blaster prompted millions of users to download the Microsoft patch that fixes the Windows vulnerability, but many computers remain unprotected. The new variant and others like it continue to infect roughly 3,000 new machines each hour, Symantec said.

Experts cautioned users to download the Microsoft security patches to ensure their computers are not infected with the new worm.

"The fact is, this thing will install stuff on your computer without your permission," said David Perry, global director of education for Cupertino, Calif.-based anti-virus software maker Trend Micro. "You don't know if these things are competent programs, and the fact is that more damage has been done to computers systems through viruses that were otherwise benign that messed something else up because they were poorly written."

Trend Micro and Symantec have released information to help customers detect and eliminate the new worm.

In its structure, Blaster is considered most similar to "Code Red," a worm that infected more than 300,000 computers in the summer of 2001, directing all PCs plagued with the bug to attack the White House Web site. As with Blaster, several variants followed the original Code Red, including a worm known as "Code Green," which attempted to fix computers tainted by Code Red.

Security experts have debated the merits of using so-called "good worms" to fight virulent worms and viruses since the early 1990s, particularly in situations when a fast-spreading infection might endanger critical information systems or cause widespread damage. Most experts say such activity has never been seriously considered because it is illegal under a 1986 computer crimes law.

"It's been discussed that if there were ever a really bad worm that might do semi-irreparable damage to the Internet, a good worm might be useful," said Richard Clarke, the Bush administration's former cybersecurity czar and a former member of the National Security Council. "But most sensible people realize it's probably illegal."

The new worm variant comes on the heels of a more insidious version that debuted last week. Dubbed "BlasterC," that version installed "backdoors" on infected machines that could allow intruders to steal or delete files.

Buried within the code of the new worm is the message: "I love my wife & baby :-)~~~ Welcome Chian~~~ Notice: 2004 will remove myself:-)~~ sorry."

The FBI and the Department of Homeland Security are investigating the source of the Blaster worm and all of its variations.