Experts Race to Beat Computer Worm
U.S., Canada Try to Thwart Sobig by Disconnecting 17 Machines

By Brian Krebs
Special to The Washington Post
Saturday, August 23, 2003; Page A01

Computer-security experts working with law enforcement officials in the United States and Canada raced yesterday to contain the Sobig.F computer worm before it could launch a new attack as authorities reported progress on finding the source of the virus.

Security experts who cracked the worm’s code late Thursday night found that Sobig instructed infected computers to try to contact one of 20 other computers yesterday afternoon to download new instructions -- to do what is as yet unknown. But the worm either failed to seek those instructions or it was thwarted from doing so when security experts disconnected 17 of the 20 targeted computers before the anticipated 3 p.m. attack.

The computer worm was one of at least three viruses that have brought corporate, personal and government computer networks to a crawl over the past two weeks.

The FBI served a grand jury subpoena yesterday on EasyNews.com, a Phoenix-based Internet service provider whose network may have been used as a starting point for the Sobig worm.

The worm is thought to have been released originally on Usenet, a sort of Internet bulletin board, by someone who had an account at EasyNews.com, according to Michael Minor, the company’s co-owner. The account was paid for with a stolen credit card number and established minutes before the virus was released on the Internet on Monday, Minor said. He added that the company is cooperating with the FBI.

The account was apparently established from a computer in British Columbia, which experts said belongs to an unwitting home user whose computer appeared to be infected by a previous version of the virus. That version let Sobig’s author seize control of the computer.

The virus was disguised on Usenet as a pornographic photograph in an adult news group, Minor said. People who clicked on the photo had their PC infected with the virus, which then began to e-mail itself to every address on the infected computer’s e-mail address book.

FBI cyber division spokesman Bill Murray said the bureau and the Department of Homeland Security would do everything they could, including serving subpoenas, to track the source of the worm.

The Sobig.F worm, a variation of a virus that’s been around since January, quickly spread out of control this month. America Online Inc., the world’s largest online service, reported that nearly 60 percent of the 38 million attachments to e-mail messages that it filtered Thursday contained the Sobig.F virus.

Authorities hoped they had neutralized the worm by disconnecting most of the 20 targeted computers. But security experts did not know last night whether they really succeeded. The instructions in the worm’s code orders it to try to connect to 20 computer addresses, assigned to home computers in Canada, South Korea and the United States, every Friday and Sunday from 3 to 6 p.m. until Sept. 10, when the worm expires.

Computer-security experts scrambled to get those computers unplugged from the Internet before 3 p.m. yesterday. When the appointed time came, all the virus did was download an address for an adult Web site from one of the three remaining computers, said Vincent Weaver, security director at
Symantec Security Response.

But, just as this is the sixth version of the Sobig worm, there may be other variants that harbor other instructions.

"The idea is to eliminate the threat before it becomes even more of a problem," said Tony Magallanez, a San Jose-based systems engineer at F-Secure, a Finnish computer-security firm. F-Secure was one of the teams of private and government security experts that cracked the worm’s code.

The CERT Coordination Center, a government-funded computer-security watchdog group at Carnegie Mellon University in Pittsburgh, also said that initial analyses of the Sobig worm underestimated its threat. "New information indicates that this worm has additional capabilities that were not realized at the time it first began propagating," CERT said.

Computer-security experts advised users to keep safe from Sobig by updating or installing anti-virus programs, which should have the ability to remove the infection. Users also are encouraged to employ some sort of hardware or software firewall to keep intruders out and to prevent unauthorized programs that do get installed on a PC from gaining access to the Internet. Authorities encourage anyone with a computer that might be infected to turn it off between 3 and 6 p.m. on Fridays and Sundays until Sept. 10.

Based on the activity from five previous versions of the virus, experts worry that Sobig could instruct infected PCs to install back doors and programs designed to steal credit card numbers, user names and passwords. Previous versions of Sobig allowed hackers to seize control of infected computers and program them remotely to send unsolicited e-mail.

The attacks are "calculated, precise and intelligently designed, and it’s a given that the individual behind [Sobig] is an expert in anonymous surfing, making it extremely difficult to locate him," said Ken Dunham, malicious code intelligence manager at iDefense Inc., a Reston-based Internet-security firm.

Investigators do not know how many computers have been infected with Sobig so far, but several security and anti-virus companies have already labeled it the "fastest-spreading virus ever."

"If Sobig had been written by malicious programmers, it could have spread 10 times faster and brought down half-a-million machines," said Scott Bradner, senior technology consultant for Harvard University.

"Just one smart person sitting down and writing a virus can now set off effects that [create a] tremor through the Internet," said Jonathan Zittrain, a Harvard Law assistant professor. "Now one person really can change the world. But that’s also what’s terrifying."

When hackers three decades ago found they could get free calls on pay phones using a toy whistle that mimicked the phone’s network signals, they exploited the system’s vulnerabilities in much the same manner as today’s viruses, Zittrain said. Phone firms, though, were able to quickly change their network design. But the Internet is fundamentally a different type of technology.

"The lesson from pay phones is don’t have your channel of communication be the same as your channel of control -- never create a system where the user can break the network," Zittrain said. "But the Internet was designed explicitly as a platform for innovation that allows anyone, anywhere, to create something new and disseminate it instantly. That’s why it has been such a wild success."

Brian Krebs is a washingtonpost.com staff writer. Staff writer Charles Duhigg contributed to this report.

© 2003 The Washington Post Company