Worm Infects Millions of Computers Worldwide

By JOHN MARKOFF
Published: January 22, 2009

A new digital plague has hit the Internet, infecting millions of personal and business computers in what seems to be the first step of a multistage attack. The world's leading computer security experts do not yet know who programmed the infection, or what the next stage will be.

In recent weeks a worm, a malicious software program, has swept through corporate, educational and public computer networks around the world. Known as Conficker or Downadup, it is spread by a recently discovered Microsoft Windows vulnerability, by guessing network passwords and by hand-carried consumer gadgets like USB keys.

Experts say it is the worst infection since the Slammer worm exploded through the Internet in January 2003, and it may have infected as many as nine million personal computers around the world.

Worms like Conficker not only ricochet around the Internet at lightning speed, they harness infected computers into unified systems called botnets, which can then accept programming instructions from their clandestine masters. "If you're looking for a digital Pearl Harbor, we now have the Japanese ships steaming toward us on the horizon," said Rick Wesson, chief executive of Support Intelligence, a computer security consulting firm based in San Francisco.

Many computer users may not notice that their machines have been infected, and computer security researchers said they were waiting for the instructions to materialize, to determine what impact the botnet will have on PC users. It might operate in the background, using the infected computer to send spam or infect other computers, or it might steal the PC user's personal information.

“I don’t know why people aren’t more afraid of these programs,” said Merrick L. Furst, a computer scientist at Georgia Tech. “This is like having a mole in your organization that can do things like send out any information it finds on machines it infects.”

Microsoft rushed an emergency patch to defend the Windows operating systems against this vulnerability in October, yet the worm has continued to spread even as the level of warnings has grown in recent weeks.

Earlier this week, security researchers at Qualys, a Silicon Valley security firm, estimated that about 30 percent of Windows-based computers attached to the Internet remain vulnerable to infection because they have not been updated with the patch, despite the fact that it was made available in October. The firm’s estimate is based on a survey of nine million Internet addresses.

Security researchers said the success of Conficker was due in part to lax security practices by both companies and individuals, who frequently do not immediately install updates.

A Microsoft executive defended the company’s security update service, saying there is no single solution to the malware problem.

“I do believe the updating strategy is working,” said George Stathakopoulos, general manager for Microsoft’s Security Engineering and Communications group. But he added that organizations must focus on everything from timely updates to password security.

“It’s all about defense in depth,” Mr. Stathakopoulos said.

Alfred Huger, vice president of development at Symantec’s security response division, said, “This is a really well-written worm.” He said security companies were still racing to try to unlock all of its secrets.

Unraveling the program has been particularly challenging because it comes with encryption mechanisms that hide its internal workings from those seeking to disable it.

Most security firms have updated their programs to detect and eradicate the software, and a variety of companies offer specialized software programs for detecting and removing it.

The program uses an elaborate shell-game-style technique to permit someone to command it remotely. Each day it generates a new list of 250 domain names. Instructions from any one of these domain names would be obeyed. To control the botnet, an attacker would need only to register a single domain to send instructions to the botnet globally, greatly complicating the task of law enforcement and security companies trying to intervene and block the activation of the botnet.

Computer security researchers expect that within days or weeks the bot-herder who controls the programs will send out commands to force the botnet to perform some as yet unknown illegal activity.

Several computer security firms said that although Conficker appeared to have been written from scratch, it had parallels to the work of a suspected Eastern European criminal gang that has profited by sending programs known as “scareware” to personal computers that seem to warn users of an infection and ask for credit card numbers to pay for bogus antivirus software that actually further infects their computer.

One intriguing clue left by the malware authors is that the first version of the program checked to see if the computer had a Ukrainian keyboard layout. If it found it had such a keyboard, it would not infect the machine, according to Phillip Porras, a security investigator at SRI International who has disassembled the program to determine how it functioned.

The worm has reignited a debate inside the computer security community over the possibility of eradicating the program before it is used by sending out instructions to the botnet that provide users with an alert that their machines have been infected.

“Yes, we are working on it, as are many others,” said one botnet researcher who spoke on the grounds that he not be identified because of his plan. “Yes, it’s illegal, but so was Rosa Parks sitting in the front of the bus.”

This idea of stopping the program in its tracks before it has the ability to do damage was challenged by many in the computer security community.

“It’s a really bad idea,” said Michael Argast, a security analyst at Sophos, a British computer security firm. “The ethics of this haven’t changed in 20 years, because the reality is that you can cause just as many problems as you solve.”

More Articles in Technology » **A version of this article appeared in print on January 23, 2009, on page A12 of the New York edition.**