



Virus-like attack slows Web traffic



Nightly News

Infection interferes with Web browsing, e-mail even ATMs

Computer experts around the world are trying to figure out who is responsible for an Internet 'worm' that slowed down Web and e-mail traffic early Saturday morning. NBC's Pete Williams reports.

By Bob Sullivan
MSNBC

Jan. 26 — Many Internet users experienced a sharp slowdown in traffic during Saturday's early morning hours, as a fast-spreading Internet worm overwhelmed the world's digital pipelines. The worm, which is being called both "Slammer" and "Sapphire" doesn't attack typical home computers — instead it attacks machines running database software from Microsoft called SQL Server. At one point, the worm attack was so bad it caused most of Bank of America's ATM machines to go offline, the company said.



THE OUTBREAK WAS so severe that while it infected only back-end Internet computers, general e-mail use and Web browsing were slowed by its effects. The worst of the attack seems over, experts said, but groggy-eyed Internet workers were spending the day Saturday and Sunday cleaning up from the effects of the outbreak.

Many compared the outbreak to Code Red, another network-based worm which infected thousands of computers worldwide. Code Red also temporarily stumped Internet traffic.

But even Code Red wasn't blamed for ATM outages.

Bank of America Corp. said Saturday that customers at a majority of its 13,000 automatic teller machines were unable to process customer transactions after a malicious computer worm nearly froze Internet traffic worldwide.

Bank of America spokeswoman Lisa Gagnon said that many, if not a majority of the No. 3 U.S. bank's ATMs were back online and that their automated banking network would recover by late Saturday.

"We have been impacted, and for a while customers could not use ATMs and customer services could not access customer information," Gagnon said.

Gagnon said that the worm, which slows down computer networks by replicating rapidly and spreading to other servers, did not cause any damage to customer information, but slowed down or blocked access to that sensitive information, making transactions difficult.

In South Korea, systems engineers raced on Sunday to repair Internet networks ahead of the start of the working week, after the country's system crashed under a global weekend attack by the fast-spreading computer worm that reportedly shut down most Internet services. Millions of Internet users were disconnected when computers at Korea Telecom Freetel and SK Telecom failed.

South Korea, considered the world's most wired country, said its Internet companies would boost security spending to try to prevent a repeat of the outage that paralyzed broadband and mobile services on Saturday afternoon.

"The problem is not completely resolved and we will have to have more of a sense of the importance of security," Information and Communication Minister Lee Sang Chul said.

25,000 MACHINES HIT IN HOURS

The attack began shortly after midnight ET on

The virus-like attack sought out vulnerable computers on the Internet to infect using a known flaw in popular database software from Microsoft Corp., called 'SQL Server 2000.'

Saturday. Within a few hours, 25,000 back-end database servers had been infected, said Oliver Friedrichs, senior manager with Symantec Corp.'s security response team. At the height of the outbreak, between 3 and 5 a.m. ET, all those computers were flooding the Internet with traffic, looking for other computers to infect. It was enough traffic to slow down the entire Internet, he said, and certainly enough to completely clog up entire companies.

"It's been an all night operation here," said Matt Pilla, Microsoft Corp. spokesman. Slammer attacks a relatively old flaw in Microsoft's SQL Server, one found by researchers in July. But many systems were still unpatched when the worm began spreading late Friday night. Adding to Microsoft's headaches: The clogs in Internet traffic were still limiting access to Microsoft's Web site on Saturday, preventing some engineers from patching infected systems.

Microsoft on Saturday was still trying to determine the best advice for customers; the company could not confirm that the free patch issued in July was enough to protect systems against Slammer. Instead, the company was recommending a free service pack upgrade instead. Service Packs are far more time consuming to download and install. (MSNBC is a Microsoft-NBC joint venture.)

Baltimore train wreck (July 18-19, 2001): Keynote Systems found significant Internet backbone slowdowns in the aftermath of the CSX train derailment in Baltimore, probably due to damage to fiber optic lines in the tunnel. Web sites measured from East Coast cities on affected backbones showed severely degraded response times.

Presidential election (Nov. 7-8, 2000): Web sites for major news organizations, political parties and other election-related groups suffered severe performance degradations, with some sites reachable less than 60 percent of the time and page load times longer than 30 seconds in some cases.

Denial-of service attacks (February 2000): The performance of the Internet overall degraded by as much as 26.8 percent during business hours. From Feb. 7 to 9, Yahoo, eBay, Buy.com, CNN, Amazon, ZDNet, eTrade, Excite were all attacked.

ILOVEYOU virus scare (May 2000): As users flocked to security software sites in the face of the ILOVEYOU virus, their performance and availability suffered. The performance of Symantec.com dropped to 72.24 seconds until the site became unavailable for about five hours the morning of May 4. McAfee.com's availability fell to 47 percent.

Starr report (September 1998): The online availability of the Starr report had minimal effect on overall Internet performance; however, Web sites that made the report available were significantly affected. CNN.com experienced 68 percent availability; MSNBC.com 47 percent, according to Keynote's statistics. Availability of the U.S. House of Representatives's Web site, where the full text of the Starr report was posted, was only 11 percent.

[Printable version](#)

Source: Keynote Systems, Inc.

WORST OVER BY MORNING

Still, the worst of the attack was over before most U.S. users awoke Saturday morning, said Mike Bradshaw, spokesman for Symantec Corp. By 4 a.m. ET, traffic generated by the worm had dropped 60 percent, as Internet Service Providers began filtering out traffic generated by the worm.

Also limiting the trouble caused by the worm: It infects only Microsoft SQL Servers, which number far fewer than Microsoft-powered Web servers, which were the target of 2001's Code Red attacks, when some experts say hundreds of thousands of machines were

infected.

“Sometime this morning, it reached saturation point, and there really were no more computer to infect,” Friedrichs said.

Still, Slammer slowed Net traffic even more than Code Red, according to Matrix Systems Inc., which measures Internet outages. The firm’s Web site indicates nearly 20 percent of Internet traffic was lost during the frantic morning attack, compared to about 10 percent during the height of the Code Red attack.

Vincent Gullotto, spokesman for Networks Associates Inc., said impact from the outbreak could have been worse if the worm were released during a business day. And there might be additional problems from the worm on Monday morning, when office employees get back to work.

“There will probably be many, many SQL servers that won’t be cleaned up,” he said.

ASIAN COMPUTERS CUT OFF

Problems caused by Slammer were global; In addition to the major problems in South Korea, Japan’s NHK television reported heavy data traffic swamped some of the country’s Internet connections, and Finnish phone operator TeliaSonera reported some problems.

But Howard Schmidt, President Bush’s No. 2 cyber-security adviser, said impact on U.S. government computers was limited.

“Everybody seems to be getting it under control,” Schmidt said. “They were fighting for bandwidth just like everybody else.

The departments of State, Agriculture, Commerce and some units within the Defense Department appeared hardest hit within the government, according to Matrix NetSystems Inc., a monitoring firm in Austin, Texas.

Schmidt said the FBI’s National Infrastructure Protection Center and private experts at the CERT Coordination Center were monitoring the attacks.

“This reinforces the fact that we just have got to pay attention to these vulnerabilities,” Schmidt said. “Here’s a classic example where there’s a patch out there, but still we see something that causes degradation of the Internet.”

PATCHING NOT SO EASY

While a patch which would have stopped the virus in its tracks has been freely available since July, Microsoft was criticized Saturday because that particular patch was more cumbersome to install than most, said Mikko Hypponen, spokesman for F-secure

Corp. Most patches require a simple download and restart of the computer. But this patch required manual editing of critical system files, something many administrators just aren't comfortable doing.

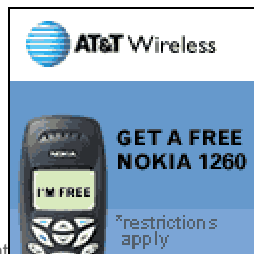
"It isn't that easy," Hypponen said. So many likely waited for the next completely updated version of the software to arrive, what's called a "service pack" in the industry. The full service pack which would have stopped Slammer just became available Jan. 17. That gave administrators who didn't want to deal with the patch less than a week to install the full service pack before the Slammer worm hit. That bad timing likely contributed to the worm's spread.

And the service pack installation isn't easy either, said Ruben Bybee, general manager of Blue Mountain Internet.

"This process takes between 15 minutes and a couple of hours depending on the speed of your Internet connection and the size of the SQL database," he said.

Bybee also said there might be additional problem when the Monday workday begins, because some networks use the Microsoft database product to manage logins for all employees. Companies that haven't addressed the problem by Monday — companies which haven't managed to install the service pack — won't be able to let their employees connect to their network.

The latest attack was likely to revive debate within the technology industry about the need for an Internet-wide monitoring center, which the Bush administration has proposed. Some Internet industry executives and lawyers said they would raise serious civil liberties concerns if the U.S. government, not an industry consortium, operated such a powerful monitoring center.



Advertisement



Add local news and weather to the MSNBC home page.

The Associated Press and Reuters contributed to this report.