September 14, 1996

New York's Panix Service Is Crippled by Hacker Attack

By ROBERT E. CALEM

Public Access Networks Corporation, a Manhattan-based Internet service provider popularly known as Panix, wanted to shield its customers from the junk bulk e-mailers known as "spammers." So, two weeks ago Panix installed a system for blocking junk bulk e-mail to its users -- an effort similar to the one that will send America Online to court in November.

But now the company is facing a new threat to its users that may have no solution, short of pulling the plug on Panix itself, experts said Friday.

Beginning Sept. 6 and continuing through at least last Tuesday, a hacker intent on shutting Panix down successfully did just that, by bombarding the service provider's servers with a flood of phony connection requests that prevented real requests by legitimate customers from getting through.

Company Statement
Statement from Public Access Networks Corporation explaining to subscribers how the attack took place and how it affected service.

Speculation about the attacker's motive has focused on the company's newly installed system for locking out bulk e-mail spammers.

Okolo Schwinn-Clanton, director of corporate services at Panix, said that two weeks ago the ISP created a list of junk bulk e-mailers and a program that allows customers to instruct the company's mail servers to block all incoming messages from any sender on that list. Use of the blocking feature is entirely voluntary, Schwinn-Clanton emphasized. By editing their personal list, Panix subscribers can block sources of other e-mail they find annoying or restore sources from which they want to receive mail.

"In principle, most of the denial-of-service attacks we see have no solution."

Peter G. Neumann,
SRI International

Moreover, Simona Nass, a spokeswoman for Panix, said that the ISP did not automatically add any bulk e-mailer to the blacklist. But if any source of bulk e-mail is identified as a spammer by numerous customers, she said, Panix will exercise due diligence by contacting both the sender and the Internet provider that hosts the sender and request that the mass mailings be stopped.

Only then, if the junk bulk e-mail continues to flow, Schwinn-Clanton said, will all mail from the host site be blocked at Panix's gates -- whether it's from the accused sender or some other customer of the host.

Nass conceded that this solution might not be fair to the host server, which in all likelihood will have a number of other customers, all of whose e-mail will be blocked from Panix.

On the other hand, she said it was also "very unfair" for Panix customers "to have to spend time weeding through stuff."

As of Friday, Schwinn-Clanton said, Panix had 15 hosts on its blacklist, up from one, Moneyworld.com, two weeks ago. The second host to join the list was Capital Area Internet Service, or CAIS, whose downstream clients include Cyber Promotions, the junk bulk-emailer that is now also the focus of AOL's legal team. (Cyber Promotions is hosted by ServInt Corporation of McLean, Va., which buys its bandwidth from CAIS.) Cyber Promotions and AOL will meet in November in the United States Court of Appeals for the Third Circuit in Philadelphia.

Related Article

Judge Prevents AOL From Blocking E-Mail
(September 7)

Online Service Blocks 'Junk' E-Mail Aimed at Subscribers
(September 5)

Whether Panix's strategy for blocking junk bulk e-mailers will be affected by the outcome of the AOL-Cyber Promotions case cannot be known now, said David Phillips, associate general counsel for America Online in Vienna, Va. "If the court held AOL did not have the right to block," then it could have "implications" for Panix, Phillips said.

Phillips added, "I think it would be astonishing if there was a ruling that AOL would not have the right to protect the integrity of its network and its members against offensive mass junk e-mail."

No one at Cyber Promotions or CAIS could be reached for comment on Friday.

It has been speculated by experts outside Panix that the recent attack on the ISP was in fact a protest of its e-mail blocking. But Nass said that the connection wasn't certain. Panix also hosts some controversial Web sites, including Voters Telecommunications Watch, she noted. The site focuses on hotly debated First Amendment and privacy law issues.

"We have no definitive information, so we're not speculating," Nass said.

The kind of assault leveled on Panix is formally known as a "denial-of-service attack," said Peter G. Neumann, author of the book *Computer-Related Risks* and a principal scientist at SRI International in Menlo Park, Calif.

"These are growing pains on the Net. We'll fix this and move on to the next one."

Emmanuel Goldstein,
Editor of 2600 magazine

"In principle, most of the denial-of-service attacks we see have no solution," Neumann said. "The generic problem is basically unsolvable. It's an open-ended problem."

Nass said that the attacker sent "Syn packets," which request a connection to a machine, to Panix's mail, Web and news servers, as well as to the machines that manage its user logins and name servers, as often as 150 times every second. In addition, the source of the packets was forged so that it could not be easily traced, Nass said. As a result, she said, there is no defense against the

attack short of "major Internet backbone providers not accepting packets that don't identify their source correctly."

She added, "I'm not that optimistic about that happening because it relies on universal goodwill and universal competence."

Neumann explained that the method used to attack Panix was one of thousands of possible techniques to accomplish the same goal -- bringing a Web site to its knees -- and agreed that the only realistic solutions were too Draconian to be exercised. He offered a similar example to the one promulgated by Nass.

Instructions for pulling off the exact attack used against Panix were published in an article titled "Flood Warning" in the Summer 1996 issue of 2600, a quarterly magazine for hackers and people who want to learn their methods. The publication's editor, Emmanuel Goldstein, said Friday: "There's always going to be idiots that do bad things with information. These are growing pains on the Net. We'll fix this and move on to the next one."

But Neumann remains pessimistic. "Filtering is not a panacea," he asserted. Rather, it's "an attempt to saw off the top half of 1 percent of an iceberg." There's always more.

Related Sites

Following are links to the external Web sites mentioned in this article. These sites are not part of The New York Times on the Web, and The Times has no control over their content or availability. When you have finished visiting any of these sites, you will be able to return to this page by clicking on your Web browser's "Back" button or icon until this page reappears.

- Panix
- Cyber Promotions
- Capital Area Internet Service
- 2600 magazine
- Voters Telecommunications Watch
