

# The New York Times



---

December 6, 2006

## Spam Doubles, Finding New Ways to Deliver Itself

By BRAD STONE

Hearing from a lot of new friends lately? You know, the ones that write “It’s me, Esmeralda,” and tip you off to an obscure stock that is “poised to explode” or a great deal on prescription drugs.

You’re not the only one. Spam is back — in e-mail in-boxes and on everyone’s minds. In the last six months, the problem has gotten measurably worse. Worldwide spam volumes have doubled from last year, according to Ironport, a spam filtering firm, and unsolicited junk mail now accounts for more than 9 of every 10 e-mail messages sent over the Internet.

Much of that flood is made up of a nettlesome new breed of junk e-mail called image spam, in which the words of the advertisement are part of a picture, often fooling

traditional spam detectors that look for telltale phrases. Image spam increased fourfold from last year and now represents 25 to 45 percent of all junk e-mail, depending on the day, Ironport says.

The antispam industry is struggling to keep up with the surge. It is adding computer power and developing new techniques in an effort to avoid losing the battle with the most sophisticated spammers.

It wasn't supposed to turn out this way. Three years ago, Bill Gates, Microsoft's chairman, made an audacious prediction: the problem of junk e-mail, he said, "will be solved by 2006." And for a time, there were signs that he was going to be proved right.

Antispam software for companies and individuals became increasingly effective, and many computer users were given hope by the federal Can-Spam Act of 2003, which required spam senders to allow recipients to opt out of receiving future messages and prescribed prison terms for violators.

According to the Federal Trade Commission, the volume of spam declined in the first eight months of last year.

But as many technology administrators will testify, the respite was short-lived.

"At the beginning of the year spam was off our radar," said Franklin Warlick, senior messaging systems administrator at Cox Communications in Atlanta.

"Now employees are stopping us in the halls to ask us if we turned off our spam filter," Mr. Warlick said.

Mehran Sabbaghian, a network engineer at the Sacramento Web hosting company Lanset America, said that last month a sudden Internet-wide increase in spam clogged his firm's servers so badly that the delivery of regular e-mail to customers was delayed by hours.

To relieve the pressure, the company took the drastic step of blocking all messages from several countries in Europe, Latin America and Africa, where much of the spam was originating.

This week, Lanset America plans to start accepting incoming mail from those countries again, but Mr. Sabbaghian said the problem of junk e-mail was “now out of control.”

Antispam companies fought the scourge successfully, for a time, with a blend of three filtering strategies. Their software scanned each e-mail and looked at whom the message was coming from, what words it contained and which Web sites it linked to. The new breed of spam — call it Spam 2.0 — poses a serious challenge to each of those three approaches.

Spammers have effectively foiled the first strategy — analyzing the reputation of the sender — by conscripting vast networks of computers belonging to users who unknowingly downloaded viruses and other rogue programs. The infected computers begin sending out spam without the knowledge of their owners. Secure Computing, an antispam company in San Jose, Calif., reports that 250,000 new computers are captured and added to these spam “botnets” each day.

The sudden appearance of new sources of spam makes it more difficult for companies to rely on blacklists of known junk e-mail distributors. Also, by using other people’s computers to scatter their e-mail across the Internet, spammers vastly increase the number of messages they can send out, without having to pay for the data traffic they generate.

“Because they are stealing other people’s computers to send out the bad stuff, their marginal costs are zero,” said Daniel Drucker, a vice president at the antispam company Postini. “The scary part is that the economics are now tilted in their favor.”

The use of botnets to send spam would not matter as much if e-mail filters could still make effective use of the second spam-fighting strategy: analyzing the content of an incoming message. Traditional antispam software examines the words in a text message and, using statistical techniques, determines if the words are more likely to make up a legitimate message or a piece of spam.

The explosion of image spam this year has largely thwarted that approach. Spammers have used images in their messages for years, in most cases to offer a peek at a pornographic Web site, or to illustrate the effectiveness of their miracle drugs. But as more of their text-based messages started being blocked, spammers searched for new methods and realized that putting their words inside the image could frustrate text

filtering. The use of other people's computers to send their bandwidth-hogging e-mail made the tactic practical.

"They moved their message into our blind spot," said Paul Judge, chief technology officer of Secure Computing.

Antispam firms spotted the skyrocketing amount of image spam this summer. A technology arms race ensued. The filtering companies adopted an approach called optical character recognition, which scans the images in an e-mail and tries to recognize any letters or words. Spammers responded in turn by littering their images with speckles, polka dots and background bouquets of color, which mean nothing to human eyes but trip up the computer scanners.

Spammers have also figured out ways to elude another common antispam technique: identifying and blocking multiple copies of the same message. Pioneering antispam companies like the San Francisco-based Brightmail, which was bought two years ago year by the software giant Symantec, achieved early victories against spam by recognizing unwanted e-mail as soon as it hit the Internet, noting its "fingerprint" and stopping every subsequent copy. Spammers have defied that technique by writing software that automatically changes a few pixels in each image.

"Imagine an archvillain who has a new thumbprint every time he puts his thumb down," said Patrick Peterson, vice president for technology at Ironport. "They have taken away so many of the hooks we can use to look for spam."

But don't spammers still have to link to the incriminating Web sites where they sell their disreputable wares? Well, not anymore. Many of the messages in the latest spam wave promote penny stocks — part of a scheme that antispam researchers call the "pump and dump." Spammers buy the inexpensive stock of an obscure company and send out messages hyping it. They sell their shares when the gullible masses respond and snap up the stock. No links to Web sites are needed in the messages.

Though the scam sounds obvious, a joint study by researchers at Purdue University and Oxford University this summer found that spam stock cons work. Enough recipients buy the stock that spammers can make a 5 percent to 6 percent return in two days, the study concluded.

The Securities and Exchange Commission has brought dozens of cases against such fraudsters over the years. But as a result of the Can-Spam Act, which forced domestic e-mail marketers to either give up the practice or risk jail, most active spammers now operate beyond the reach of American law enforcement. Antispam researchers say the current spam hot spots are in Russia, Eastern Europe and Asia.

While spammers are making money, companies are clearly spending more of it to fight the surge. Postini says that the costs for companies trying to fight spam on their own have tripled, mostly because of increased bandwidth costs to handle bulky image spam and lost employee productivity.

The estimates should be taken with a grain of salt, since antispam companies are eager to hawk their expensive filtering systems, which can cost around \$20,000 a year for a company of 1,000 employees. But the onslaught of junk e-mail does affect business operations, even if the impact is difficult to quantify.

At the headquarters of the Seattle Mariners this summer, the topic of the worsening spam problem came up regularly in executive meetings, and the team's top brass began pressuring the technology staff to fix the problem. Ben Nakamura, the Mariners' network manager, said he tried to tighten spam controls and inadvertently began blocking the regular incoming press notes from opposing teams.

Two weeks ago, the situation grew so dire that the team switched from software provided by Computer Associates, whose suite of security programs sat on the team's internal server, to a dedicated antispam server from Barracuda Networks, which gets regular updates from Barracuda's offices in Silicon Valley.

Mr. Nakamura said the new system had greatly improved the situation. On a single day last week, the team received 5,000 e-mail messages and the Barracuda spam appliance blocked all but 300. Still, some employees continue to see two or three pieces of spam in their in-boxes each day.

Some antispam veterans are not optimistic about the future of the spam battle. "As an industry I think we are losing," Mr. Peterson of Ironport said. "The bad guys are simply outrunning most of the technology out there today."