

# THE GLOBE AND MAIL

CANADA'S NATIONAL NEWSPAPER

## CYBERSPACE

# Crackdown cans spam – for now

California Web-hosting company was gateway for junk e-mail

BY MATT HARTLEY  
TECHNOLOGY REPORTER

Internet users who noticed a decline in the amount of junk mail piling up in their e-mail inboxes this week should enjoy the respite while they can, because experts say it's unlikely the reprieve will last.

The amount of e-mail sent around the globe dipped substantially this week after a pair of Internet service providers pulled the plug on a U.S. Web-hosting company that observers believe acted as a distribution gateway for cybercriminals running some of the largest spamming operations in the world.

It was just after 1:30 p.m. PST on Tuesday when Nilesh Bhandari, a product manager for e-mail security firm IronPort Systems in San Bruno, Calif., noticed that the amount of spam – unwanted junk e-mails – travelling through the Internet was dropping, and fast.

When he dug a little deeper, he realized the decline in spam traffic coincided with the unplugging of a San Jose, Calif., company named McColo Corp., which was identified in an article by The Washington Post this week as acting as a host for organizations engaged in everything from sending spam to controlling compromised computers around the world and selling knock-off pharmaceuticals.

"We saw a major reduction in the spam volume," Mr. Bhandari said. "And it co-ordinated perfectly with the shutdown of McColo."

In the seven days before Nov. 11, an average of about 154 billion spam e-mails were sent every day, according to Senderbase.com, IronPort's spam-monitoring service, which scans about 30 per cent of the world's e-mail and Internet traffic. By Nov. 12, that total had dropped to 112 billion. Yesterday, about 64 billion spam messages were sent.

The website for McColo remained offline yesterday and calls to the company's head office were not immediately returned.

The problem is that experts don't expect the lull to last. If the spammers are the equivalent of narcotics producers and distributors, McColo was only a pusher or middleman; and while law-enforcement officials in the United States may eventually press charges against McColo, it is more difficult for authorities to shut down spam producers.

It is likely that the spammers using McColo's gateway will simply look for another Web-hosting company in a region of the world where cybercrime laws are more lax, such as Eastern Europe or Africa.

"I would bet that [McColo] will soon be replaced with other so-called bulletproof hosters," said David Poellhuber, founder and chief executive officer of Montreal's Zerospam Security Inc.

"But we're getting further up the food chain and that's good, because the higher up we get, the harder we can hit them," said Mr. Poellhuber, whose firm operates a service

that filters spam for organizations such as Elections Quebec.

"You may not get the bad guys, and they can always start up another operation, but you've hurt their economics. In the end, it's going to cost them more money to rebuild their infrastructure."

## Glossary

» **Spam:** Unsolicited junk e-mails that are sent en masse to millions of computer inboxes every day. Some advertise discount or counterfeit pharmaceuticals, some pose as legitimate institutions such as banks and ask for a user's personal information, while others deliver viruses and other harmful software.

» **Malware:** Short for malicious software. Malware is a catch-all term that describes any software that installs itself on a user's computer for illegal or unwanted activities and includes everything from conventional viruses and spyware to Trojan Horses and bots.

» **Botnet:** A bot is a piece of malware that infects a computer, which then sends information or spam messages to other computers, usually without the user's knowledge. A botnet is a network of bots that connect and can sometimes receive and relay information back to a central "command and control" server operated by the spammers or cyber criminals.

» Source: IronPort Systems, Industry Canada