Internet spam – invading privacy and overloading systems

Report by Eugene Oscapella

HARVESTING ROBOTS are now trawling the Internet, posing as regular surfers while they collect huge quantities of information, including e-mail addresses.

Canada's *National Post* reported on February 19th that these "harvesting robots" are a piece of software that surfs the Internet, searching for strings of characters containing the @ symbol, which normally indicates an e-mail address. The e-mail addresses can then be sold to marketers who will then use them to send "spam" (unsolicited e-mail) messages.

The same day, the online news service, *Wirednews*, reported that Western "spammers" are exploiting Asian mail servers, using them to relay unsolicited mail. In response, an increasing number of systems administrators are now blocking all e-mail originating from Asia, in an attempt to stop a flood of spam from China, Taiwan and Korea. Some suggest that this blocking activity may soon become a diplomatic issue. It may also interfere with normal business conducted over the Internet.

According to the *Wirednews* report, many systems administrators and spam-fighters said that apart from blocking all e-mail from Asian Internet service providers, there does not seem to be any way to stop all the spam originating from or being routed through Asian e-mail servers. Apparently, China Telecom receives more than 50,000 spam complaints a day from Europe and North America, but ignores them all.

Blocking the spam-sending Internet Service Providers (ISPs) has not resolved all problems, says *Wirednews*. "Refusing massive amounts of attempted connections also puts a strain on servers, in some cases bogging the system down in much the same way as a sustained denial-of-service attack."

In a September 17th 2001 report, *Wirednews* quoted Tom Geller of the SpamCon Foundation, who said that the idea of having a "do not e-mail" list similar to the "do not call" lists available to deter telemarketers is totally hopeless: "Some e-mail addresses have hundreds of people, and some people have hundreds of addresses. It's impossible to build such a list, and no one is going to obey it anyway."

AUSTRALIA TACKLES SPAM

The Australian government has begun to investigate the apparently increasing volume of spam. In a media release dated February 18th, the federal Minister for Communications, Information Technology and the Arts spoke of the government's concern about unwanted e-mail messages. Senator Richard Alston cited an estimate by the Coalition Against Unsolicited Bulk E-mail that Internet users in Australia received six times as much e-mail in 2001 as they did in 2000.

Of particular concern to the Minister were unsolicited messages containing illegal, offensive or deceptive content, or those incorporating personal information collected or used in breach of the recent extensions of the Privacy Act to business. This material, he said, was often pornographic.

The Minister's media release also described several regulatory, self-regulatory and consumer awareness mechanisms already in place in Australia to counter intrusive spam:

• extension of the Privacy Act to place some spam-related restrictions on business;

• provisions in the Broadcasting Services Act for handling complaints about illegal and offensive material online;

• prohibitions in the Interactive Gambling Act of certain forms of online gambling and of advertising those services;

• measures in the Crimes Act to prevent a person being menaced, harassed or offended;

• consumer protection provisions in the Trade Practices Act; and

• the Internet Industry Association (IIA) codes of practice which prohibit IIA member Internet Service Providers from sending direct marketing messages without the recipient's permission and which require service providers to advise consumers on how to minimise spam problems.

i

For further information:
www.newsbytes.com/news/
02/174581.html