7 Aug 96
w/ geek

PACKET

Simson Garfinkel
TECH

Can That Spam

If junk email drowns the Net, it will be our fault

Electronic mail was the Internet's first killer app. Thanks to electronic junk mail, it could be the Net's last killer app as well.

Direct marketing professionals bristle at the words "junk mail." Roy Schwedelson, CEO of Florida-based Worldata Inc. - one of the nation's largest mailing list brokers - nearly hung up on me when I uttered the dreaded phrase in an interview. The reason is simple: Traditional marketers really don't want to send mail to people who don't want to receive it. It typically costs a marketer 50 cents to rent a person's name and address, print an advertisement, then send it to them. As one prominent direct marketer said, "There is no such thing as junk mail, only junk people."

But the Net's crazy economics changed all that. On the Net, it's just as cheap to send a hundred emails as it is to send ten. And if you're in the bulk mail business, it's just as easy to send ten million pieces of mail as it is to send a million. All you need is a list of email addresses, a connection, and some garden-variety robots and programs.

There are no fundamental technical or economic reasons for marketers not to flood the world's mailboxes. So that's what we're starting to see. Every day, five to ten pieces of spam hit my mailbox.

And it's getting worse, to the point where some people believe that if the trend continues unchecked, spam will overrun their mailboxes. This won't destroy the Net, but will make mail unusable for most people.

Already, a growing number of individuals and companies are spamming for hire. Following the lead from Jeff Slaton (aka the Spam King), these companies offer

"Some people believe that if the trend continues

unchecked, spam will overrun their mailboxes. It won't destroy the Net, but it will make mail unusable for most people."

spams-for-hire. They thrive on shady businesses that don't know the first thing about getting online themselves.

I called one such company, Cyber Promotions, in Philadelphia, Pennsylvania, and was told that they charge US$149 for a five-line advertisement. This ad is bundled with 20 to 30 others and sent to the company's mailing list of 900,000 names. You can have your own "full-page ad" for $995.

Meanwhile, Jeff Slaton has gone from spamming to selling his own spamware. Doing business as Unix Etcetera - "We are Unix geeks with an attitude" - he is selling a program called Lightning Bolt. This package gleans email addresses from Usenet, collects them in a large database, then sends out the junk mail. Another piece of spamware out there is Floodgate: "The ultimate in email programs. Open the floodgates and let the email flow NOW!" blares the company's Web page.

Don't shoot the postmaster!

Talk spam strategy, in Packet Chat: Subscribe to PacketFlash, for Packet news.

Ian Kaplan, a programmer in California, recently contacted me to let me know what Slaton was up to. Kaplan's upset that folks like Slaton and Floodgate are distributing the tools that will let thousands of spammers flower on the Net. But he's also kind of pissed that these folks are making money with what are essentially trivial programs.

Fundamentally, there are three ways to put an end to technical, economic, and legal spamming.

Technical solutions can be implemented at the user's mailbox. But any anti-spamming program needs to have some way of distinguishing between welcome email and spams. And that of course assumes that there aren't some spams that the user genuinely wants to see. You can create a simple Eudora filter with a set of keywords (like transfer any message with a to: header containing "@cyberpromotions.com" to the Trash). The problem is, of course, what to do with the email messages that don't match any of the rules.

I've been thinking a lot about what sort of robot guard could protect me against unwanted email. The robot could be written as a perl script and run on the Unix computer that acts as my mailbox.

Ideally, the script would have two modes of operation:

1. A training mode, when the robot would simply collect the names of my regular correspondents. I would run it this way for a month or so. You would probably set this up with some sort of .forward file like this:

```
 % cat ~/.forward
"|/usr/home/simsong mail-robot -t /var/mail/simsong"

%
```

2. Incoming mail would be delivered to the script and either returned to sender, flushed, or put in my mail spoolfile (/var/mail/simsong) until I picked it up via POP.

A file in my home directory would specify the basic mail rules. It would be rigged so that mail from some addresses was automatically flushed, mail addressed to some of my favorite mailing lists automatically accepted, and other mail interactively filtered. The rules might look something like this:

```
From: @cyberpromotions.com                  FLUSH
From: IP-ONLY (no matching domain name)     FLUSH
To: cwd@cyberwerks.com                      KEEP
To: vtw-announce@vtw.org                    KEEP
From: @mit.edu                              KEEP
From: *                                     FILTER
```

The Filter directive solves the problem of what to do with mail that doesn't match any of your other rules. In my ideal implementation, the Filter command would first calculate a unique message authorization code ($MAC) for this message in question. (Base it on the MD5 hash of the From: address and a user-definable password, perhaps.) If the $MAC code was in the Subject: field, the message would be kept. If it wasn't, the robot would send the message back to the sender with note saying something to the effect, "your message has been bounced by my mail filtering robot. If you are a human, and not a spammer, then just send this message back to me with the keyword $MAC in the header." This is elegant, stateless, and relatively easy to implement.

The economic solution would be to make spammers pay "postage" for their spams. But I'm not holding my breath. Today, I can send out a million email messages for less than $5 over a weekend using a Netcom "netcruiser" account. Any system for charging users a token fee for delivering email is a long ways off.

One way to implement the postage would be to rig the Internet's backbones so that TCP/IP packets destined for port 25 weren't carried unless they included some sort of cryptographic authentication. That authentication could be Chaum-like digital cash that would debit the sender's account - or transfer money from the sender's account into the recipient's.

I'm less sanguine about this solution than the mail robot, however. One reason is that, even with the growth in spamming, the percentage of Net traffic that's the result of email is fast declining - and it's likely to be infinitesimal as soon as the Internet starts being used for routine video conferences.

Some people are looking for legal solutions. After all, they worked in the 1980s with unsolicited faxes. Title 47 of the US Code, Section 227 allows recipients of unwanted faxes to sue for $500 in damages per occurrence. The statute is written broadly enough that email probably qualifies, although as far as I know, no such suits have yet been filed.

Even if legal solutions worked within this country, US law doesn't reach overseas. While it's prohibitively expensive to send faxes from the Asia or Europe to the US, it is just as cheap to email spams from Japan as from anywhere else. That's why I'm pinning my hopes on technical fixes at the user's mailbox.

In order to be effective, such a technical fix will need to be widespread throughout the Internet. That means it's got to be free. Who'd like to write it?

Send mail to Simson Garfinkel at simsong@hotwired.com

Illustration by Dave Plunkert

webmonkey SURF CENTRAL

Previously in Garfinkel ...