The War Against Spam

by

Chris Baker

Topics

- How much of a problem is it?
- Who are they?
- How do they operate?
- What can we do?
- Who is fighting and who is not?
- Why should we fight?

Why Spam?

Spam is unsolicited bulk commercial e-mail (UCE or UBE)

- **Cheaper than postal mail**
- **Less labor intensive than telemarketing**
- **Most of the work is done by computers**
- **Because it is so cheap, it is essentially sent to people at random**

Statistics

- Studies vary, but some estimate that spam is now the majority of all e-mail traffic
- Jupiter Research estimates the average e-mail account received 2,200 spam messages last year
- Brightmail Inc. estimates nearly 40 percent of all Internet e-mail is unwanted, an increase of 8 percent from 2001

You Have Been Drafted

- Unless you have absolutely no Internet connectivity, you are in the war against spam, like it or not
- If you do not protect yourself, you could unknowingly be helping the enemy
- If we all work together, we can win

Spammer Profile

- ***Detroit Free-Press*** **profiled Alan Ralsky:** ***www.freep.com/money/tech/mwend22_20021122.htm***
- **"I'll never quit. I like what I do. This is the greatest business in the world."**
- **Served jail time**
- **Lost license to sell insurance**

How They Get Addresses

- Harvest from web sites
- Sign-up and opt-in lists
- Exchange with other spammers
- Monitor e-mail lists
- Usenet and chat rooms
- “Dictionary attacks”
- Domain name registries

Web Sites

- E-mail addresses can be encoded in web pages using Javascript
- Use forms on-line that don’t show addresses

Em@ilEncoder

- Automatically writes Javascript e-mail links for web sites
- Freeware, available from Tucows

Source Code and Text

- View in Browser:

  Click here to e-mail me.
- Source Code:

  <SCRIPT language=JavaScript type=text/javascript> <!-- document.write('Click here to e-mail me.');

  // --> </SCRIPT>

What Users Can Do

- Have multiple e-mail addresses or give out phony or throw-away addresses
- NEVER “click here to remove” NEVER

Blocking Mail from IP Addresses

- Most e-mail servers can do this now
- Most hosting companies also block e-mail
- Many can be configured to import from block lists
- Can also block by domain

Block lists or black lists

- Spamcop, *www.spamcop.net*
- SPEWS, *www.spews.org*
- Open Relay Database, *www.ordb.org*
- Distributed Server Boycott List, *www.dsbl.org*
- Spamhaus, *www.spamhaus.org*
- MAPS Realtime Blackhole List, www.*mail-abuse.org/rbl*

Are Block Lists Worse than the Disease?

- Some “victims” of block lists include British Telecom and Adelphia Cable
- IP Addresses change frequently
- How do you get off the lists if you are not a spammer?

Do System Administrators Care?

- At the beginning of 2002, a local university in my area was still running an open mail relay, for example
- About half of all spams come from open relays
- Open relays can be set up by accident

Do Producers of Spam-vertised Products Care?

- Pfizer Company, Viagra
- Symantec, Norton software
- Are they trying to keep their products in legitimate distribution channels?

Spam Advertising Other "Legitimate" Products and Services

- Devry University
- *Wall Street Journal*

Aggressive Anti-Spam Tactics

- Teergrubing
- Phony e-mail addresses

Teergrubes

- Set up a fake MTA to accept an SMTP connection
- Hold connections for a long time if they are spammers
- Require a lot of resources and maybe a dedicated machine

Phony E-mail Addresses

- Setting up a web site which generates fake e-mail addresses
- Foils harvest bots

Technical Solutions

- New SMTP and TCP/IP protocols
- Address resolution
- Whitelists
- Challenge response

New Protocols

- Old protocols outdated, designed for a much different and smaller Internet
- Old protocols make it easy to “cover the tracks”

Address Resolution

- Attempt to validate recipient's e-mail address automatically
- Resource intensive?
- How reliable is it?

Whitelists

- Accept mail only from approved addresses, domains, or IP addresses
- Extremely inconvenient

Challenge Response

- Sends message to sender asking him to validate himself
- Sender responds
- Inconvenient and impractical and defeats the main purpose for using e-mail
- Now offered by Earthlink

Legitimate E-mail Marketing

- Yes, there is such a thing
- Employs a “double opt-in” system
- User is sent e-mail asking him to opt-in
- If user does not opt-in, he no longer receives e-mail
- Different from spammers who ask users to opt-out
- Legitimate marketers hate spam, too

We Can Win the War

- Possibly 150-200 people are responsible for 90% of spam
- Hundreds of millions don’t want spam
- Out of a thousand that receive spam, less than one person takes the bait
- The many benefits of e-mail are too important to sacrifice to the spammers