What Will Stop Spam?

Carl Hutzler
Director Anti-Spam Operations
America Online, Inc.

Fall 2004 NANOG

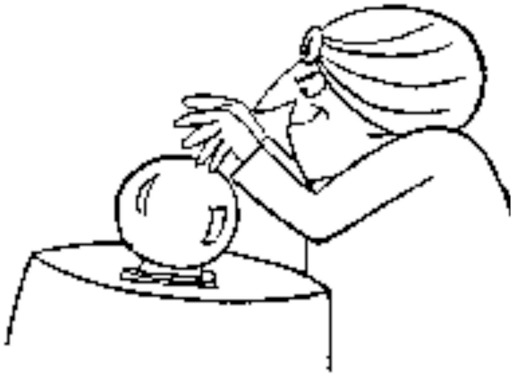
Agenda

- What do the new email identity technologies do?
- Will they stop spam?
- What will stop spam?

What do Email Identity Technologies Do?

- They provide some assurances that a domain is being used with permission
  - Citibank can control the use of their domain, but cit1bank.com will still be abused
  - Bounces can be analyzed to see if they are legitimate
  - Information can be analyzed on the responsible domain owners and their reputation/accreditation
- But remember, email identity technologies do not stop spammers!
  - They only force spammers into other behaviors, many of which are better for enforcement and controls.
  - <u>But without ISPs doing their part</u> to use these technologies wisely, <u>we will be no better off.</u>

AOL is a Crystal Ball



Report from 9/14/2004

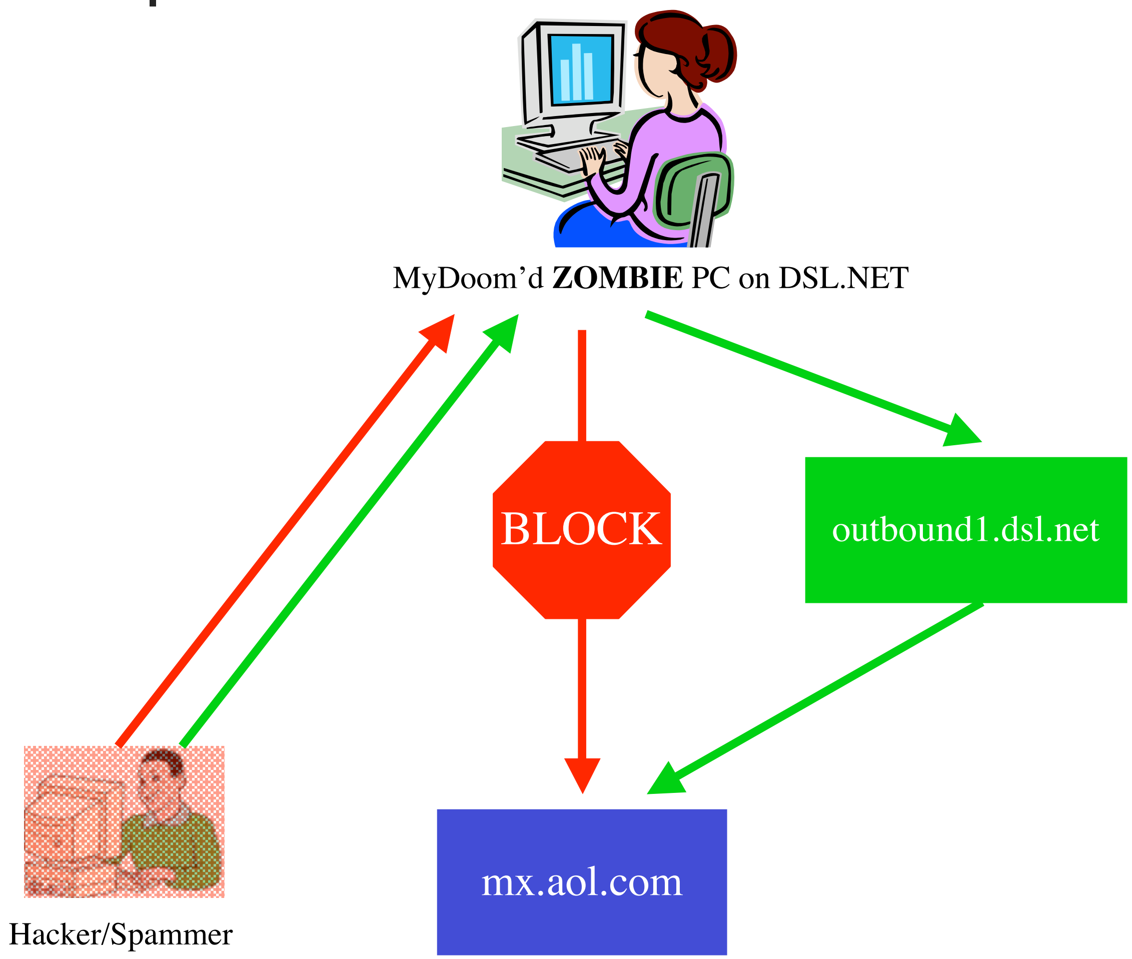
188841 hotmail.com
64543 x-mailer.co.uk
62757 shawcable.com
46312 concentric.net
32259 cnchost.com
32022 zero.ou.edu
23557 mail.atl.earthlink.net
22837 grp.scd.yahoo.com
21005 ucla.edu
17676 oemgrp.com
16849 mail.cornell.edu
16260 dejazzd.com
15764 mta01.tie.cl
15659 mrf.mail.rcn.net
14343 urbanhomesecurity.com
14280 mail.pas.earthlink.net
14246 smtp.nextra.cz
13646 mail.yahoo.com

Note1: Greyed domains have very low spam penetration due to very large number of emails sent which counters the total complaint statistic.

Note2: Italic domains were whitelisted and subsequently blocked for spamming.

- Bulk Mailers on AOL’s whitelist comprise 30-50% of our daily email volume but only 5-10% of complaints.
- >80% of AOL’s spam problem comes from other ISP’s main outbound MTAs and compromised web servers (CGI scripts)
- AOL began seeing this shift in Sept 2003
- The rest of the internet is beginning to see this now…
  - “We're the **biggest spammer** on the **Internet**," network engineer Sean Lutner, Comcast - source CNET.com, May 24, 2004

All spam will eventually come from ISP Networks



For example: AOL, BlackLists, and other organizations are getting really fast at blocking zombie machines

BUT…

The machines do not get un-infected
No SMTP AUTH

- Most ISPs "trust" internal networks

No Outbound Spam controls
No Rate controls

Results?
ISP mail servers act as forwarding MTAs for a network of open relay Zombie machines

Will SenderID, SPF, DomainKeys, etc stop spam?

- Simple answer, NO. Complex answer, NO.
- Why?
  - Most AOL spam obeys sender identity technologies TODAY!
  - Spammers send through the local MTA and use the local ISP’s domain as the FROM/Sender
- Identity Technologies can allow blacklists/whitelists to work from DOMAINs instead of IP addresses
  - Good from a not blocking innocents by IP address standpoint
  - Reputation/Accreditation systems will be key to success of Email Identity technologies
  - Without SMTP Authentication, we are only validating the DOMAIN and not the USER portion of the address (user@domain.com)

Bottom Line: If ISPs don’t get smart soon and control the sources of spam on their networks, the reputation for their domain (e.g., comcast.net) will be so poor that they will not have connectivity to other ISPs

Summary: What technologies will stop spam?

- ISPs and Network Providers “waking up” and working together to cut off the spammer’s oxygen supply:
  - Spammers need connectivity
  - Spammers need large numbers of high throughput IP addresses
- So what is the formula for success?
  - ISPs should monitor their networks for sources of spam LEAVING their network
    - Port25 is always the responsibility of the originating ISP
    - Shift some of the resources from inbound filtering to **OUTBOUND Controls**
  - Enforce strong authentication to authorize use of an ISPs MTAs
  - **Monitor customer sending patterns like a credit company monitors “fraudulent charges”**
  - **Monitor/Sign-up to receive complaints from AOL and other sources (spamcop, abuse@, etc)**
  - **Remove sources of spam within minutes (Zombie machines, insecure CGI scripts, bad customers, etc)**

Shameless Plug and Contact Info

- Plug into AOL to monitor your network for abuse!
  - MCI and Level3 do it. But they are the only ones who seem to care.
  - AOL may sever connectivity to your network if abuse continues.
  - AOL Feedback Loop can show you where spam is coming from within your network!
  - Sign-up Today at http://postmaster.aol.com/tools/fbl.html

- Contact AOL if you have any issues:
  - Carl Hutzler, cdhutzler@aol.com
  - AOL's 24x7 Postmaster, **703.265.6942** or **1.888.212.5537 (US only)**
    - Charles Stiles, Manager of the AOL PM Team (stilesch@aol.com)