SP(iced h)AM

presented by Eric Hughes for CSC 200, Spring 2004

Spammer's Tools:
How they Work,
Why they Work.

Spammers' Goals

- Ultimate Goal: To Make Money
- Supporting Goals:
  - Collect & use email addresses
    - Convince victims to buy legit. goods
    - Scam victims
    - Sell addresses to others who will do the above
  - Bypass filters/detection techniques
  - Avoid negative repercussions

E-mail

- Why is email the ideal way to spread spam?
- How do spammers collect addresses?
  - collected by forms on sites with registration
  - harvested by viruses, worms (eg. Bagle/Beagle, others)
  - assembled by web-crawling, etc.
  - purchased from others who do above
- How do spammers verify, tailor lists?
  - use web (registration) forms
  - above combined with cookies, clear gifs to reveal users' interests
  - "remove me from your list" links, replies

Circumvention of Anti-Spam

- Simple: fool users
  - Masquerade as contests, legit. companies.
  - Refer to (bogus) sponsorship from well-known companies
- Sneaky: use tricks to hide obvious spam text
  - Send graphics
  - Separate words with
  - Encode characters with numeric representation
  - Use tables to split the message into columns
  - Send HTML for user, text for anti-spam ("chaff"?)

Circumvention of Anti-Spam

- Sneaky: Foil/Spoil adaptive ("Bayesian") filters
  - Foiling Bayesian filters
    - add innocent text (from news, etc.), pref. invisibly
    - re-flavor the probability of ham message, tailored to individual.
      - Send several flavors
      - Use feedback (clear gif) to find users' flavor
  - Spoil ("poison") Bayesian filters
    - Add innocent text to have system filter out ham (false positives)
    - Hope user gets fed up with filter, goes unfiltered

Avoid Repercussions

- Header spoofing
  - Easy to do with SMTP
  - Easily caught by filters
  - Often tagged by servers
- Anon. Forwarding
- IP spoofing
  - Confounds traceroute, whois, etc.
- Trojaned systems
  - Use victims' systems to send mail
  - Use victims' systems to cover tracks

References:

- Sophos whitepapers (filter-bypassing, text tricks):
  - http://www.sophos.com/spaminfo/whitepapers/WP_PMFool_US.pdf
  - http://www.sophos.com/spaminfo/whitepapers/WP_PMSpam_US.pdf
- Wired News (spamming + hacking = spoofed, untraceable spam):
  - http://www.wired.com/news/business/0,1367,60747,00.html
- Spam.abuse.net
  - http://spam.abuse.net
- Paul Graham:
  - http://store.yahoo.com/paulgraham/