# The Increasing Complexity of Spam

**Jesse Dougherty**

Director of Development
Sophos

# A spam campaign is a marketing campaign

- Marketing campaigns have:
  - Incentives (in the content)
  - Calls to action (the links in the message)
  - A source – the sender IP

# Spammers want leads

- Spammers want to get leads, but stay unaccountable for their theft of resources, so they innovate…

# Content

- Modify the content of the message to avoid filtering (signature, keyword, etc.)
  - Obfuscations (v1agra, \ /iagra)
  - Word salad (tiger, forehead, tomato…)

# Is spam effective?

- Is it effective? Obvious scam
- Less porn, more pills
- More high margin, low cost of delivery products to gain profit
- Target insecurities and biases

# Sources

- Hide the actual source of the message to avoid accountability and blocking
- Open proxies provide great cover
- Spread by worm outbreaks
- Multi-Level-Marketing sender programs (VirtualMDA)
- Hijacked network blocks (bgp spoofing)

# What’s next?

- Asymetric routing for IP spoofing

# Destinations

- Http, dns even on infected machines
- Rolling through domains very quickly
  - Over 500,000 domains being tracked currently

# Summary

- People buy from spammers
- Spammers generate revenue
- Revenue drives innovation
- Innovation drives exploit economy

# HP WORLD 2004

Solutions and Technology Conference & Expo

Co-produced by:

interex

shared knowledge • shared power

encompass

AN HP USER GROUP