Email Address Harvest Techniques

Doug McLean
VP Marketing

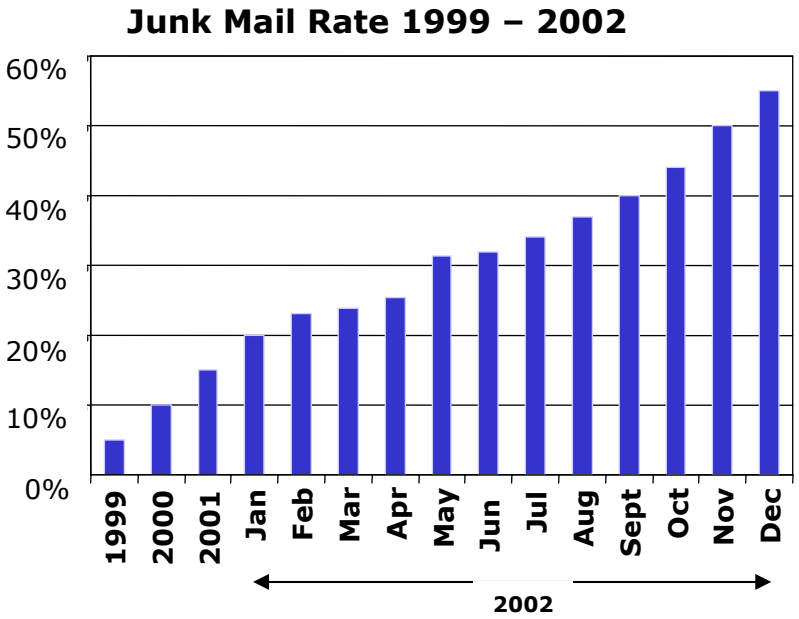
Postini: The Email Security Leader

- The Company
  - Largest email security services provider
  - Offering email security services since 1999
  - 1,000+ corporate and network service provider customers
  - 4M+ end-users
  - Process 60-70M emails per day; 9B in 2002

- Perspective on Spam
  - Sits in the email flow (SMTP layer)
  - Observes spammer behavior in real time
  - “See” attacks illuminate across thousands of email domains
  - Blocks spam, viruses, and harvest attacks from reaching customers’ networks

Spam: A Growing and Persistent Problem

- Postini recorded a 150% increase in spam traffic in 2002
- Average spam capture rate across customer base is now 60%; individual rates range from 20% to 80%
- Spammers are aggressively changing tactics to defeat current solutions
- Directory Harvest Attacks (DHAs) fundamentally change how spammers operate



* % of Total. Source: 6 billion total messages processed by Postini

postini

Observed Spammer Tactics

	Before 2002	2002 and Beyond
Content	➢Flat text	➢Flat text ➢Graphics ➢HTML ➢JavaScript
Address Sources	➢Websites ➢Newsgroups	➢**Directory Harvest Attacks**
Profitability Variables	➢Volume delivery ➢List Cleaning	➢Volume delivery ➢Volume address acquisition ➢Anti-filter tactics

Directory Harvest Attack

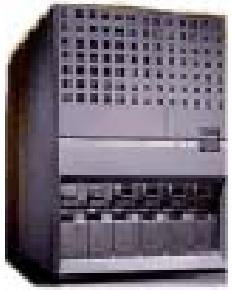
Common Names

- Bill
- Steve
- Gates
- Smith
- Levy
- Chung

Spammer's Servers

To: bill@acme.com

550 error: invalid address



Acme Widgets Corporate Mail Server

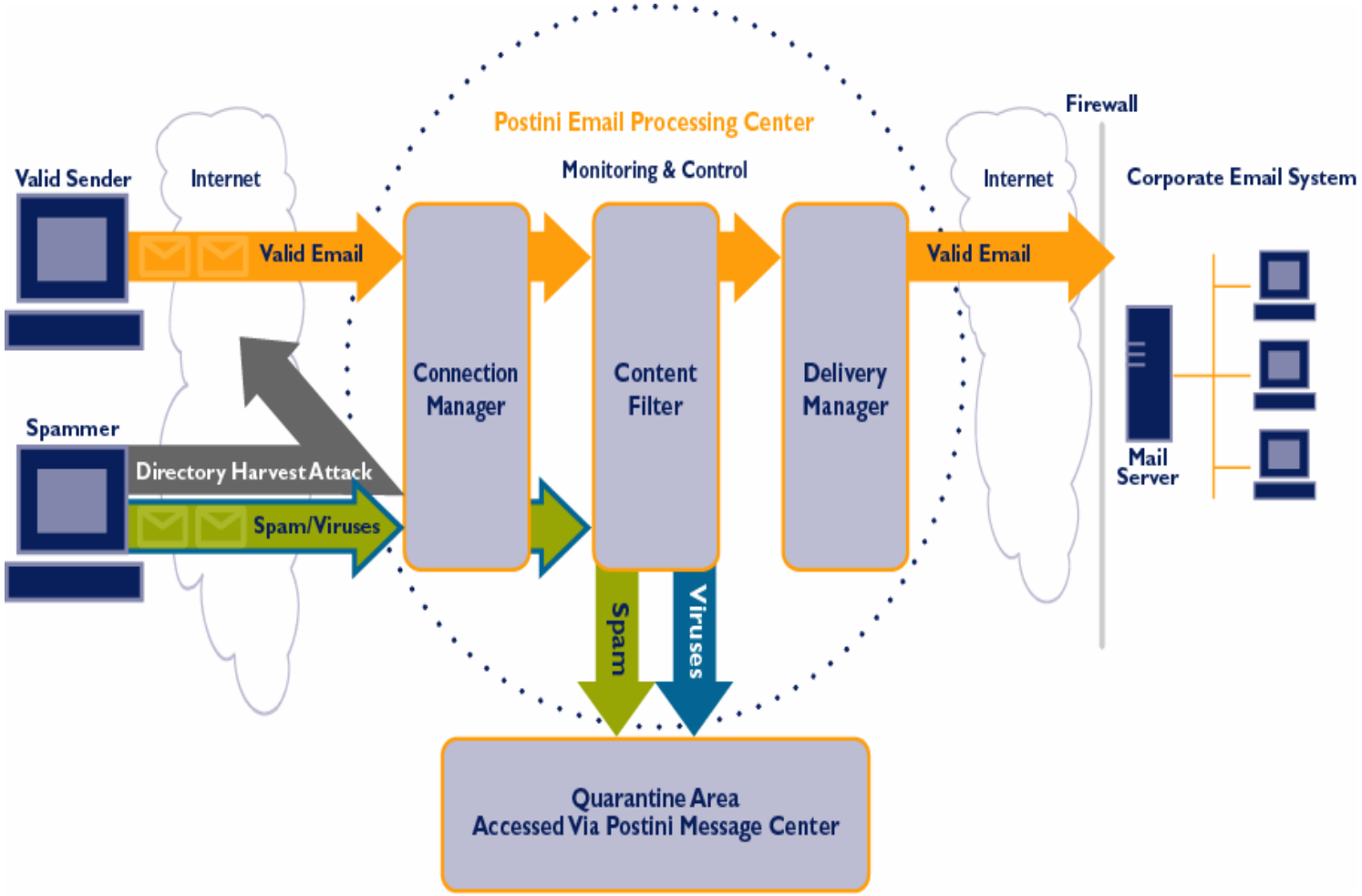
To: bgates@acme.com

Open SMTP Session

Valid Addresses

- bgates@acme.com
- al_levy@acme.com
- bgates@acme.com

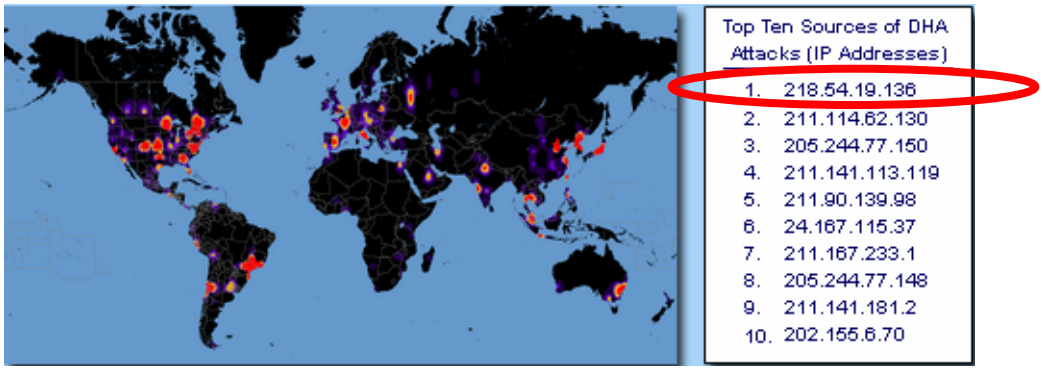
Postini Service Architecture



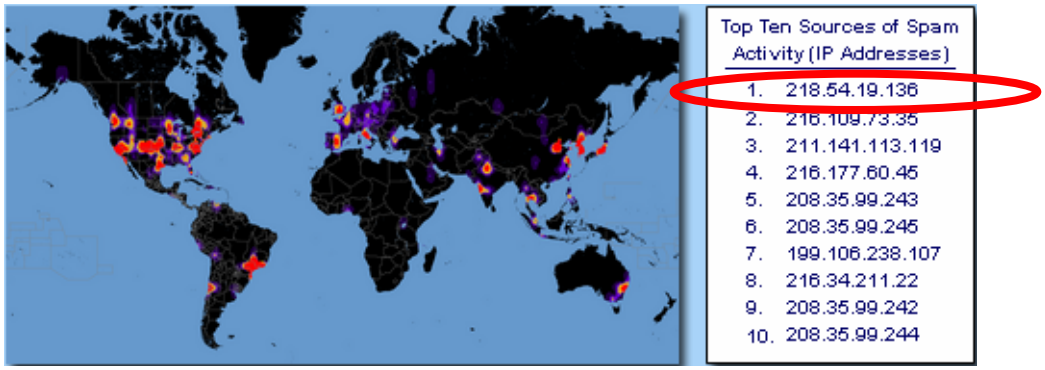
Specific Correlation of Attacks

- Postini 24hr processing snapshot
  - **40 million messages**
  - **19,300 DHAs, 16 million delivery attempts**
  - **Over 20 million spams**

First the Directory Harvest Attack…



…then the spam attack

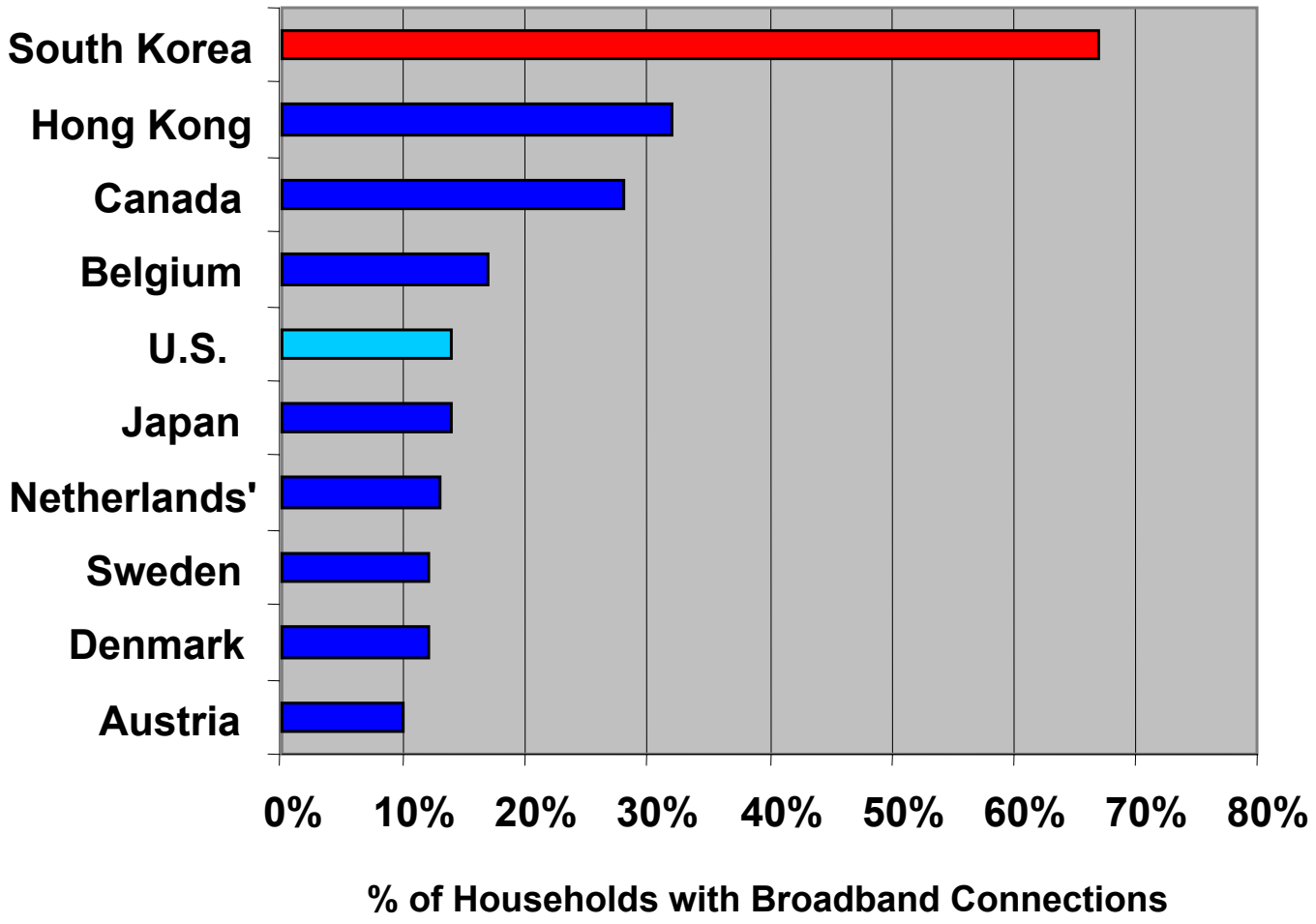


Directory attacks happen in real-time and target specific organizations

Effective solutions need to block the attacker *before* they spam

postini

Broadband Connection Penetration



Source: Yankee Group, 2002

Directory Harvest Attack Demonstration