Port 25: The Gaping Hole in the Firewall

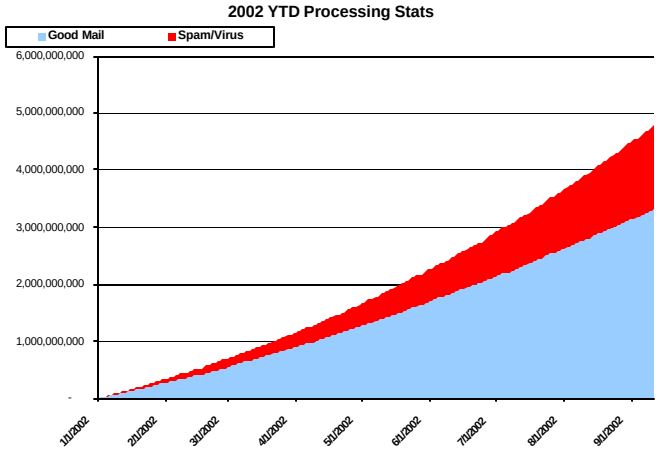
ACSAC Conference

December 12, 2002

Scott Petry
VP Products & Engineering
spetry@postini.com

Postini: The Email Security Leader

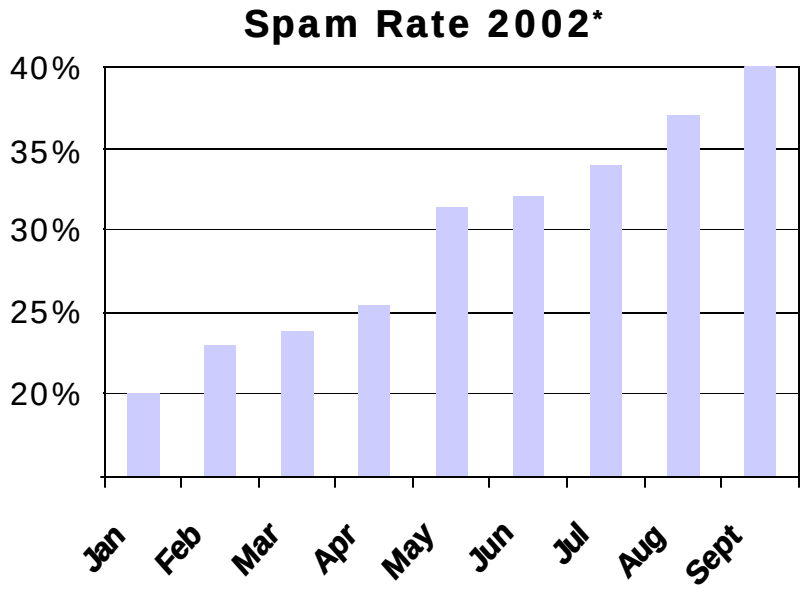
- Email Security and Systems Management functionality for 1000 corporations and service providers
  - Customers rely on Postini for
    - Spam and Virus blocking
    - SMTP connection security
    - System-wide visibility and resource management
    - Disaster recovery solutions



- Management and Security at network *perimeter*
- Postini processes ~ 1.5 billion messages per month
  - Zero detectable latency

Spam Is a Growing Corporate Problem

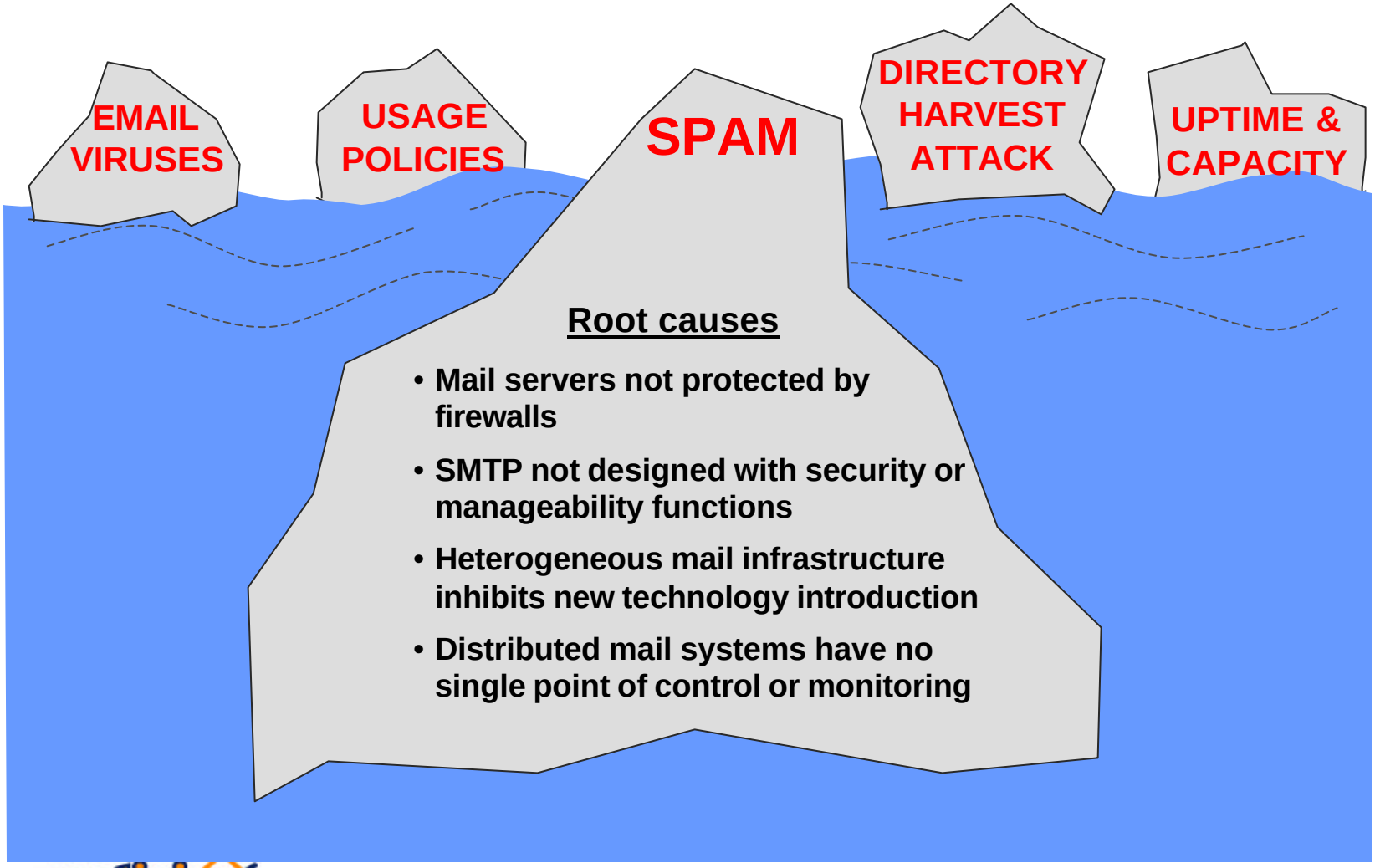
- Spam volume increasing
  - Postini average spam capture rate doubled between January and September, 2002
  - Current spam capture rates across customer base range from 20% to 70%, with an overall average of about 40%
- Spam Costs IT
  - Overruns server capacity
  - Opens workplace liabilities
  - Interrupts productivity
  - Adds unnecessary workload to over-burdened IT support staff
- With growth unchecked, email becomes unusable by 2004



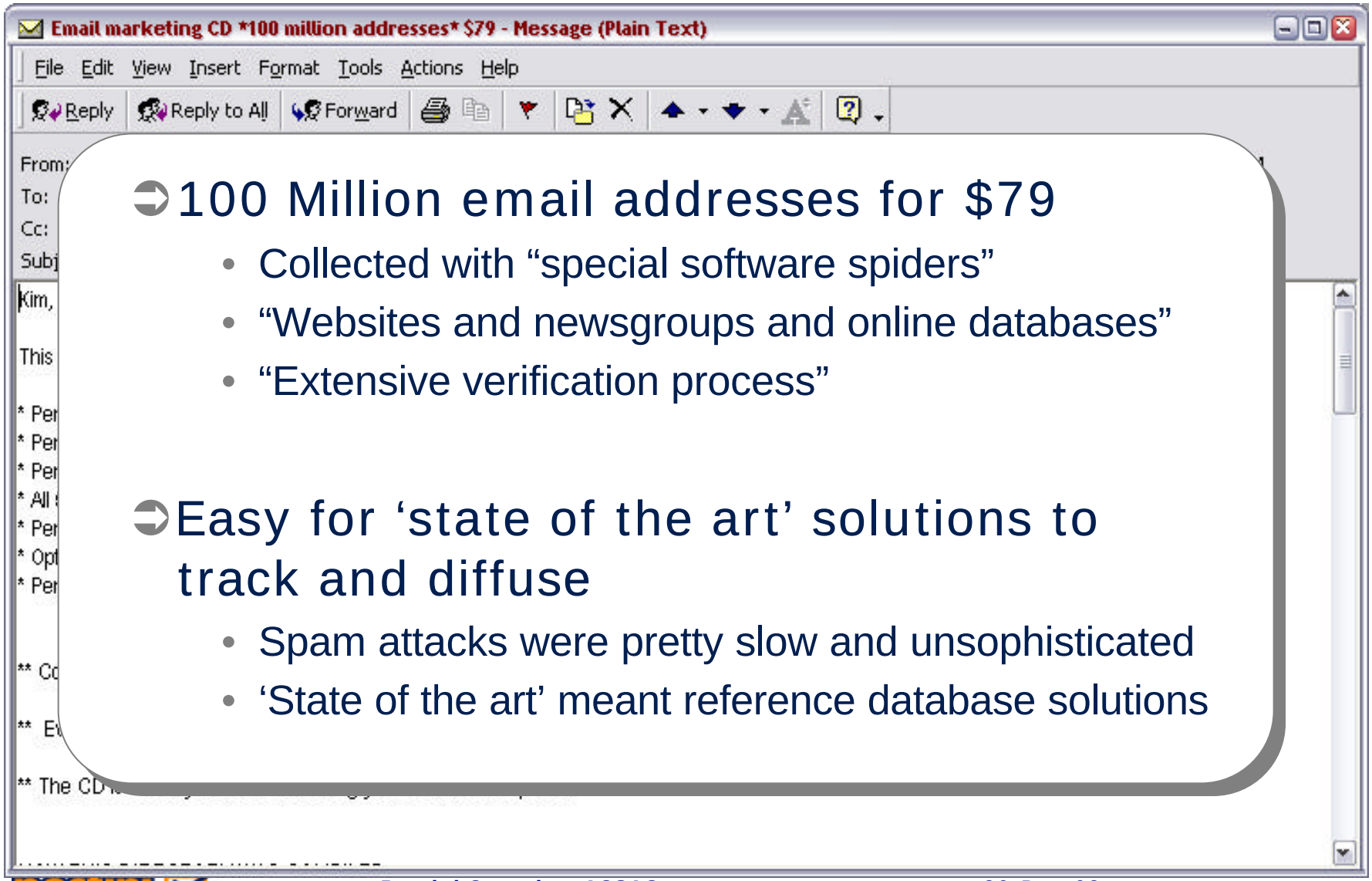
* % of Total. Source: 6 billion total messages processed by Postini

Spam Is Major Symptom

Larger Email Systems Vulnerability Issue



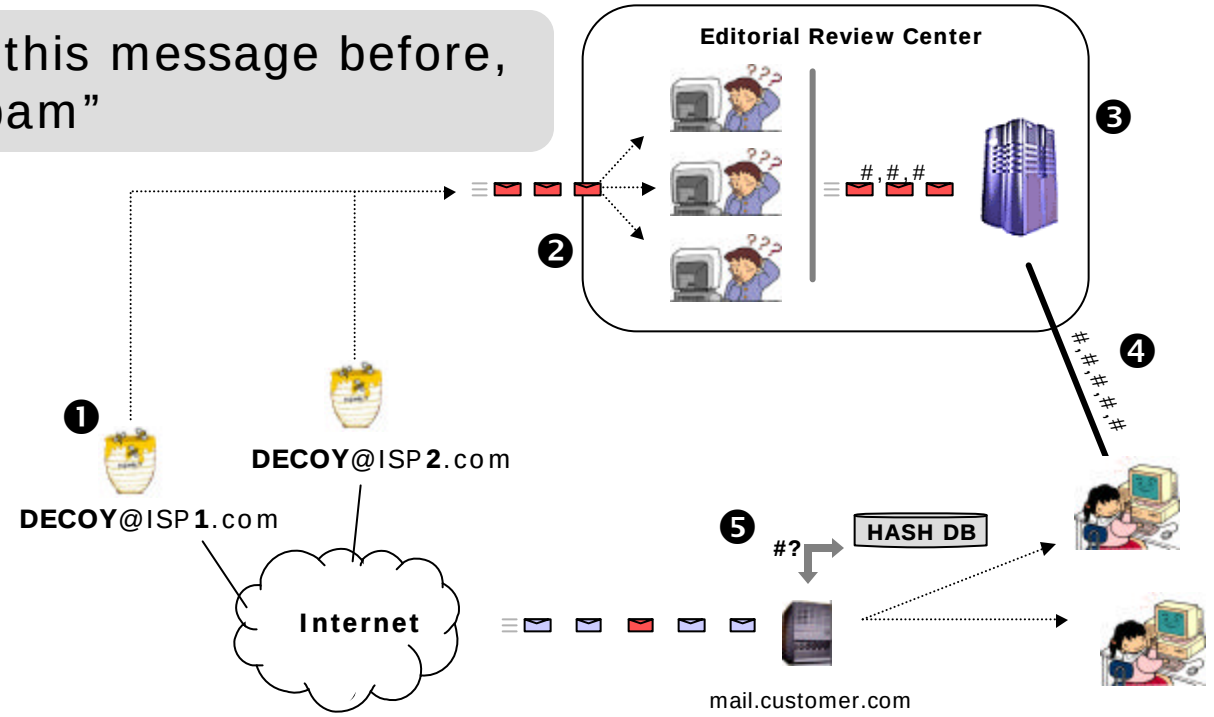
The Old World: Dumb Bombs



- 100 Million email addresses for $79
  - Collected with “special software spiders”
  - “Websites and newsgroups and online databases”
  - “Extensive verification process”
- Easy for ‘state of the art’ solutions to track and diffuse
  - Spam attacks were pretty slow and unsophisticated
  - ‘State of the art’ meant reference database solutions

The Spam Reference Database Solution

"I've seen this message before, and it is spam"



❶ - Decoy ' Honey Pot' email addresses are populated around the Internet. These act as spam collectors

❷ - Spam is forwarded to an editorial review center, where each message is reviewed by a human editor

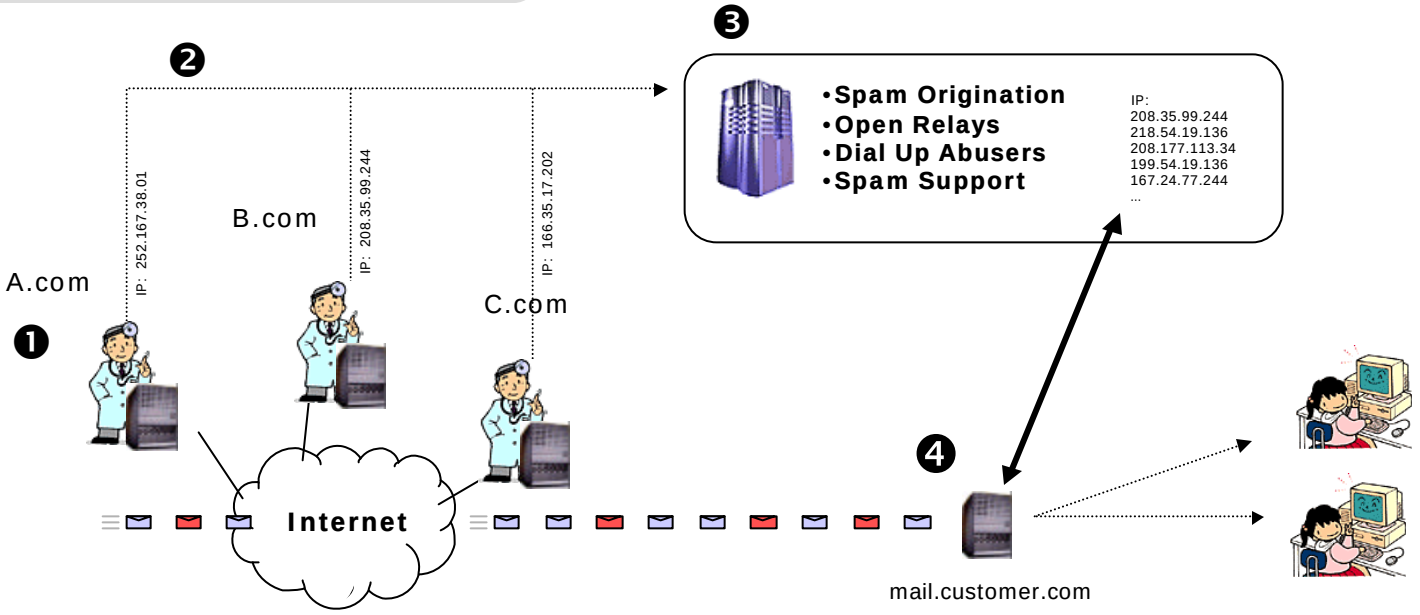
❸ - Spam is catalogued, a hash pattern is created and stored in a database

❹ - Hash pattern updates are pushed to customer DB

❺ - Each message is hashed, and the value is compared against the database

The Abuse IP Database Solution

"I've seen this IP before, and it sends spam"



❶ - Admins monitor server performance and message actvity

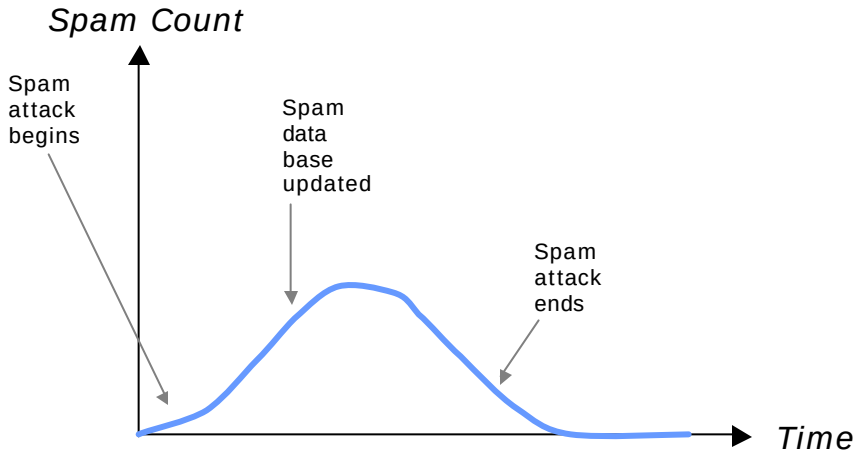
❷ - Admins submit IP addresses of abusers to controlling body

❸ - Database of abusers is updated

❹ - Subscribers of Abuse DB validates incoming requests against 'known' abusers

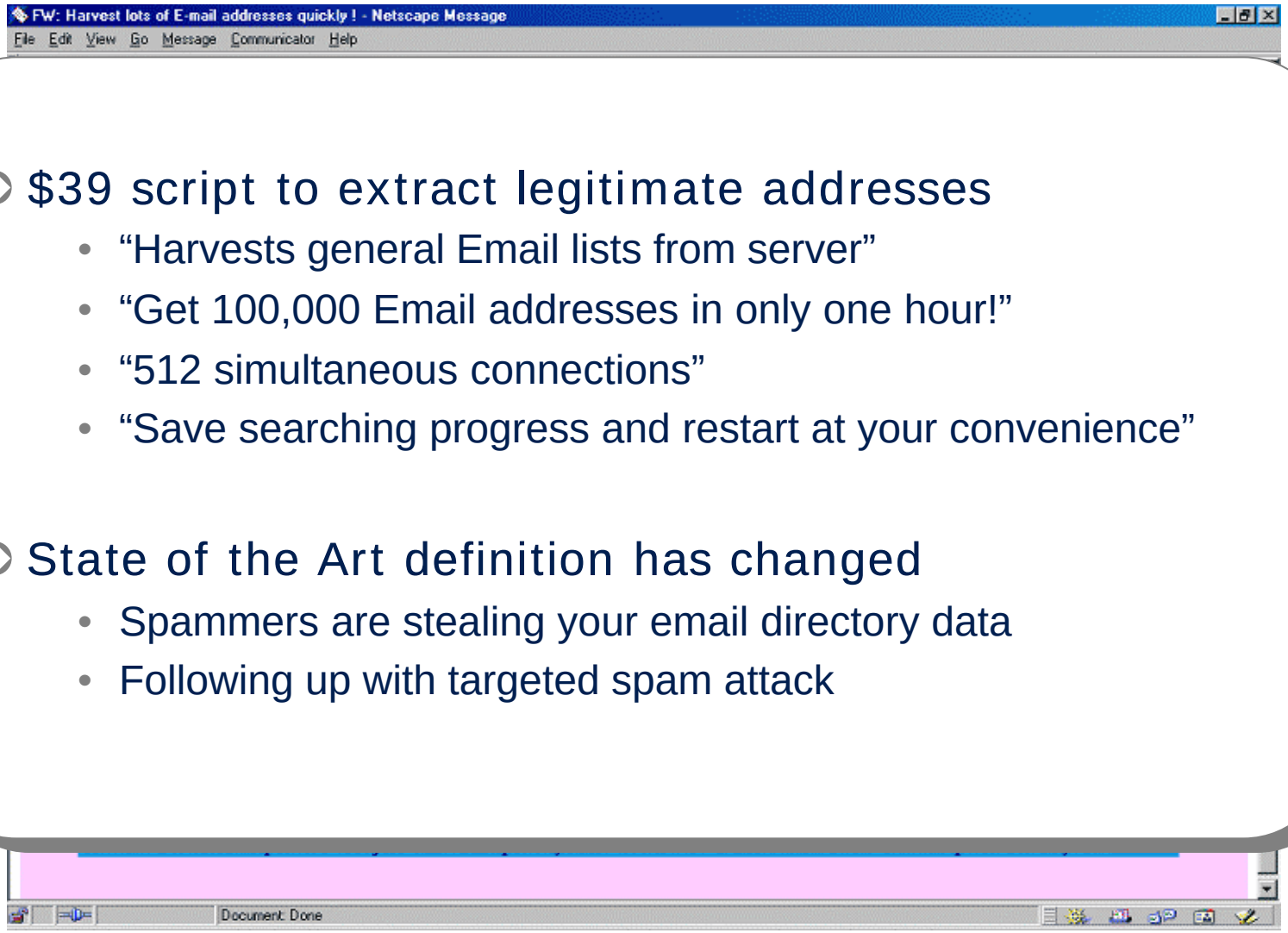
Databases: Appropriate at the Time

- Slow, long-rolling spam attacks give DB solutions time to propagate signature files



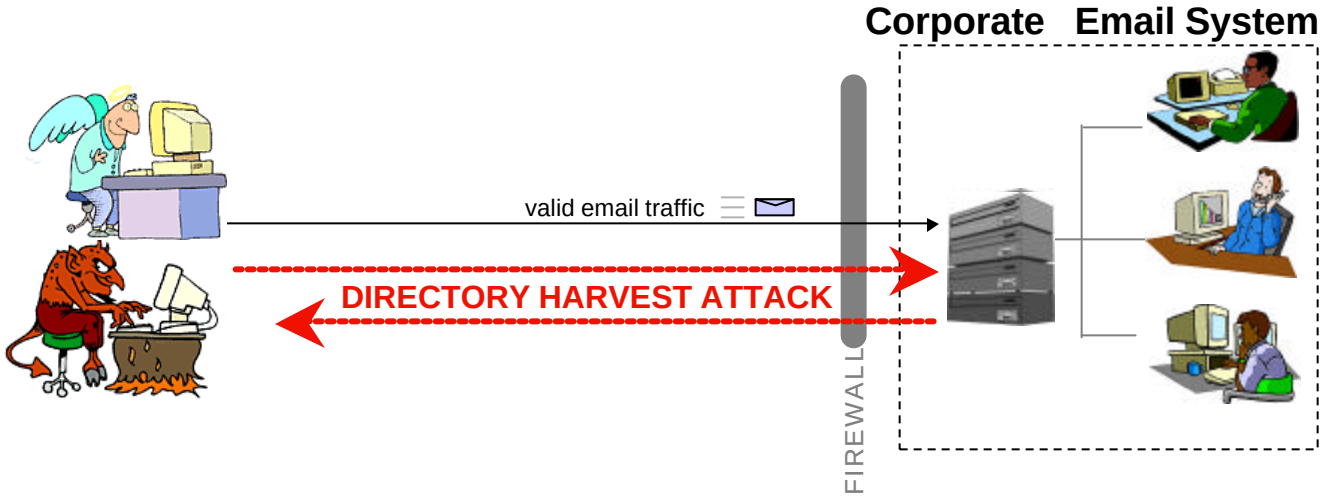
- Spammers targeted ISPs, high penetration of Honey Pot addresses at ISPs
- Regional ISPs participated in the contribution efforts
- Spam was obvious by its signature
  - Consumer sensitivity to false positives was low
- Database solutions address the symptom: "Is this message spam?"
  - Volume was low, admins could be reactive
  - Root cause analysis not required

The New World: Precision Munitions



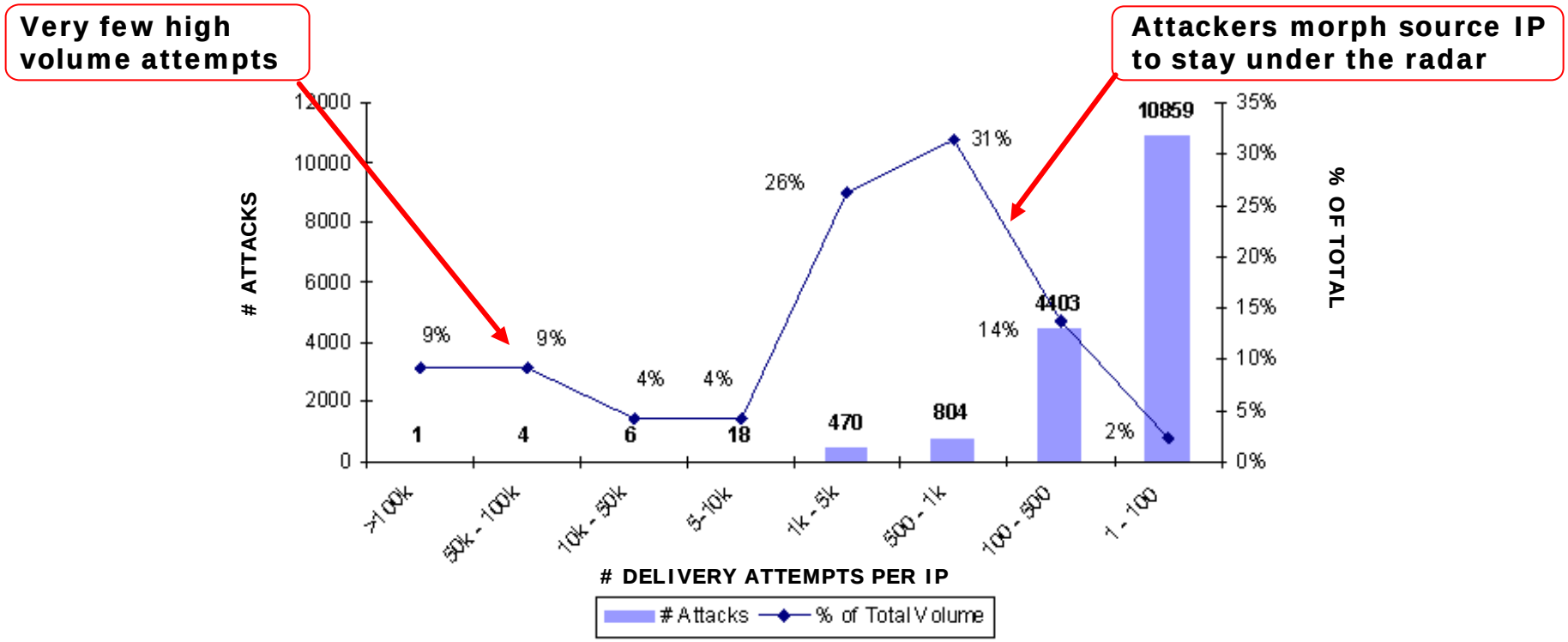
- $39 script to extract legitimate addresses
  - "Harvests general Email lists from server"
  - "Get 100,000 Email addresses in only one hour!"
  - "512 simultaneous connections"
  - "Save searching progress and restart at your convenience"
- State of the Art definition has changed
  - Spammers are stealing your email directory data
  - Following up with targeted spam attack

The Directory Harvest Attack



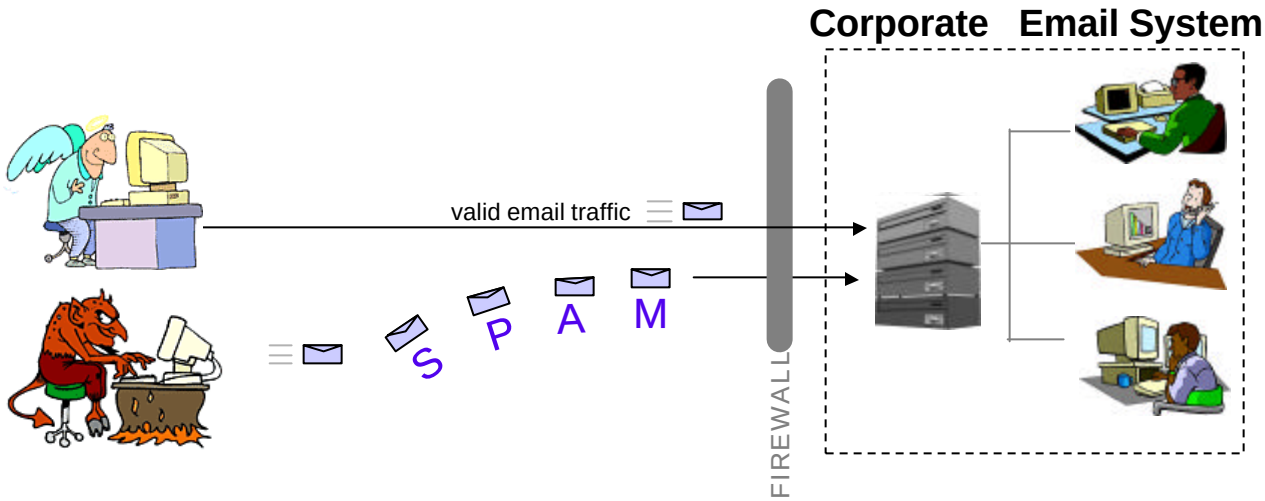
- Directory Harvest Attack
  - Scripted attempt to steal valid directory info from customer server
  - Exploits standard SMTP behavior
- High-volume delivery attempts in rapid-fire
  - John@company.com, JohnA@company.com, JohnB@company.com, etc.
- MTA handles delivery attempts as designed:
  - Rejects unknown addresses with 550 (standard UNIX emailers)
    - Until valid address is acknowledged, spammer collects and catalogs
  - Accepts EVERYTHING, bounces later (Exchange, Qmail)
    - Spammers interpret as 100% yield, volume increases geometrically

DHA Stealth Tactics



- Log file analysis does not uncover moving threats
- Even if identified in the logs, it's too late – attacker has moved to another IP

The Spam Follow-Up



- Harvester completes the mail merge….
  - Customizes the message
    - New header data
    - Random numbers in body
    - Re-sequence message text
- Targets valid recipients in organization
- Connects, delivers, leaves

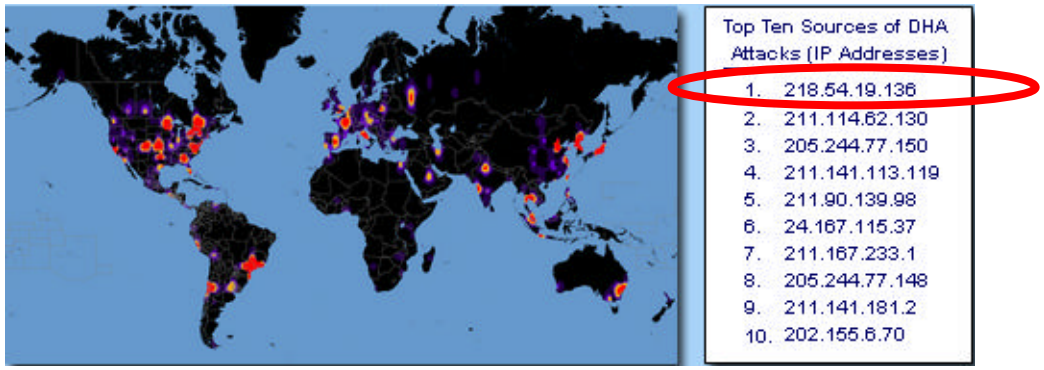
Specific Correlation of Attacks

- Postini 24hr processing snapshot
  - 40 million messages
  - 19,300 DHAs, 16 million delivery attempts
  - Over 20 million spams
- Consistent correlation of top 10 offenders

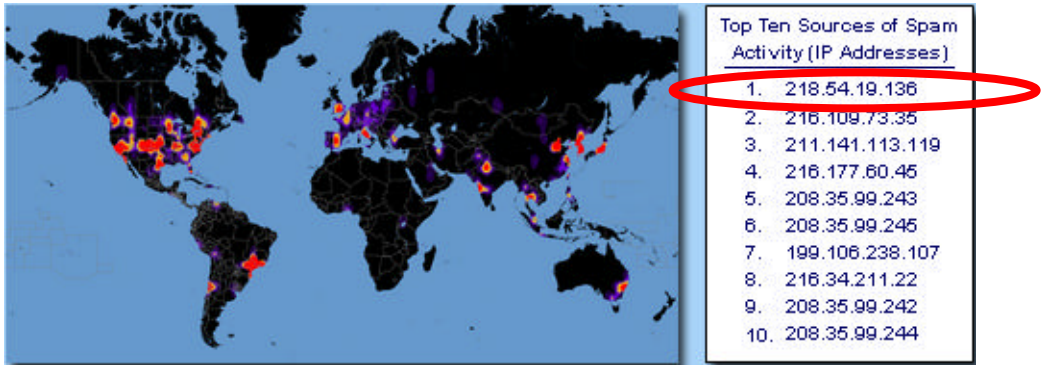
Spam attacks happen in real-time and target specific organizations

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

First the Directory Harvest Attack…

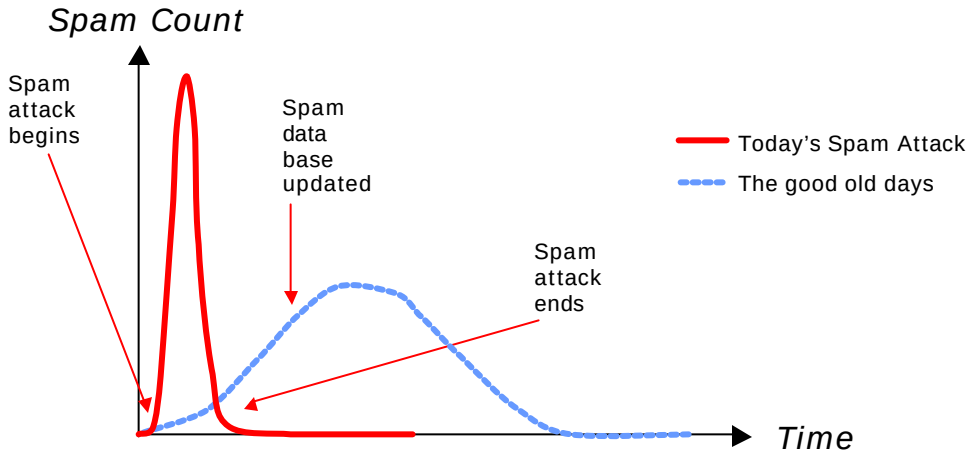


…then the spam attack



Databases: Appropriate at the Time…

- Database solutions require time to collect data and disseminate rules
  - Spam attacks are over before the DB update can propagate



- Databases require that attacks be identified *before* spammer targets customer system
  - Honey Pot addresses need to be at *every* installation
  - Contribution to Abuse DBs must be real-time, world-wide, 24x7
- Database solutions yield a binary result: 'Yes' or 'No'.
  - No context for policy-based or user-group provisioning thresholds
  - False positives is a major corporate concern, need probabilistic assessment
- Database solutions address the symptom: 'Is this spam?'
  - Do not deliver PROTECTION

Current Technology Not Keeping Current

Spammers modifying tactics to defeat existing technology

Technology	Evolving Spammer Tactic
REFERENCE DATABASE AND FINGERPRINTING SOLUTIONS	• Random character generation – inserted into both header and body • Text paragraph re-sequencing • Single use 'From:' address, no recycling
LEXICAL SCAN AND TEXT PROCESSING SOLUTIONS;	• HTML encoding • HTML comments inserted to split words • Mis-spell, add spaces within words, or replace letters with numbers
SIEVE, PROCMAIL AND OTHER HEADER ANALYSIS SOLUTIONS	• Not suppressing SMTP: From • Sending to single recipient • Frequently changing IPs within Net block

Detection vs. Protection

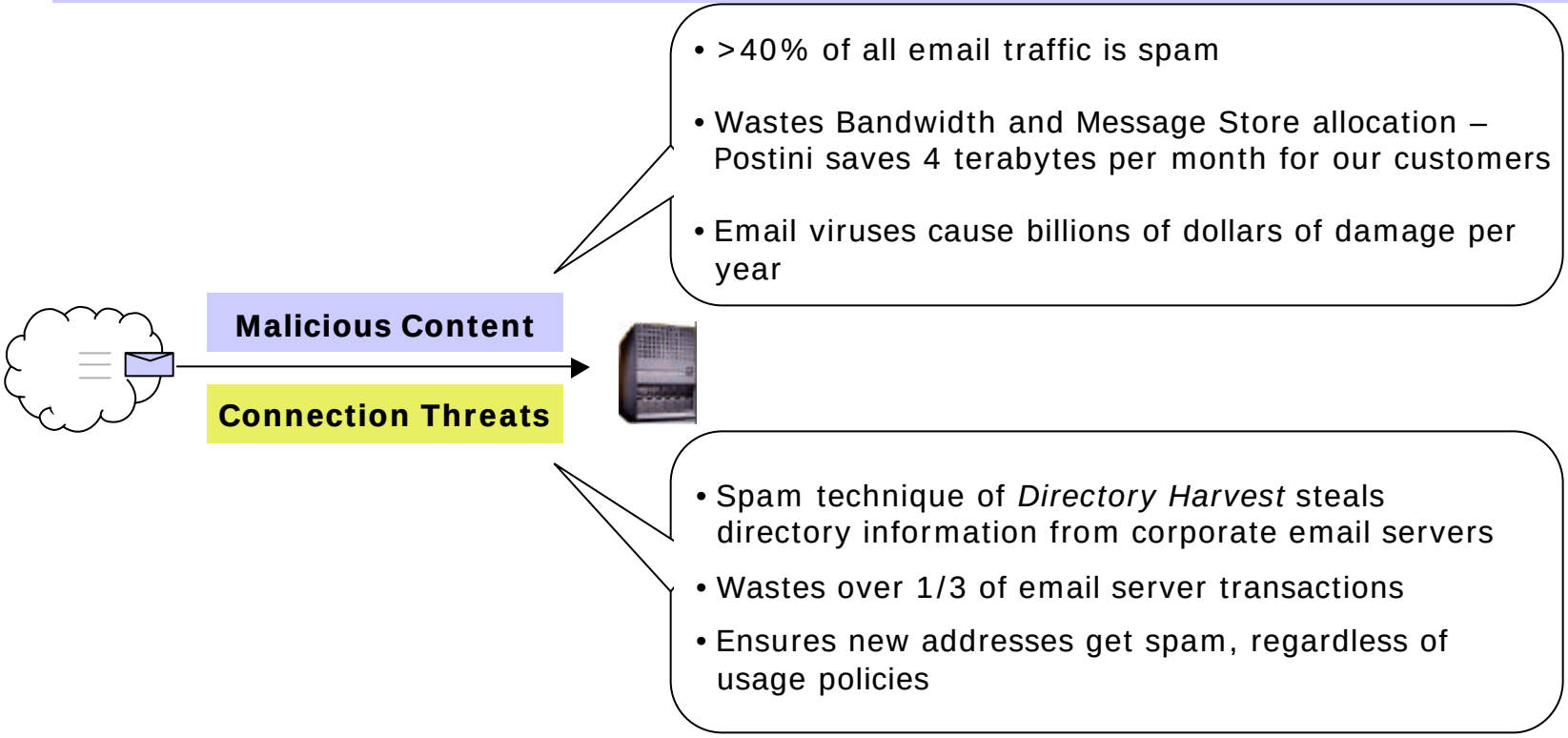
Identify Spam 'After the Fact'

- Is this spam?

Stop Attacks Outside the Network

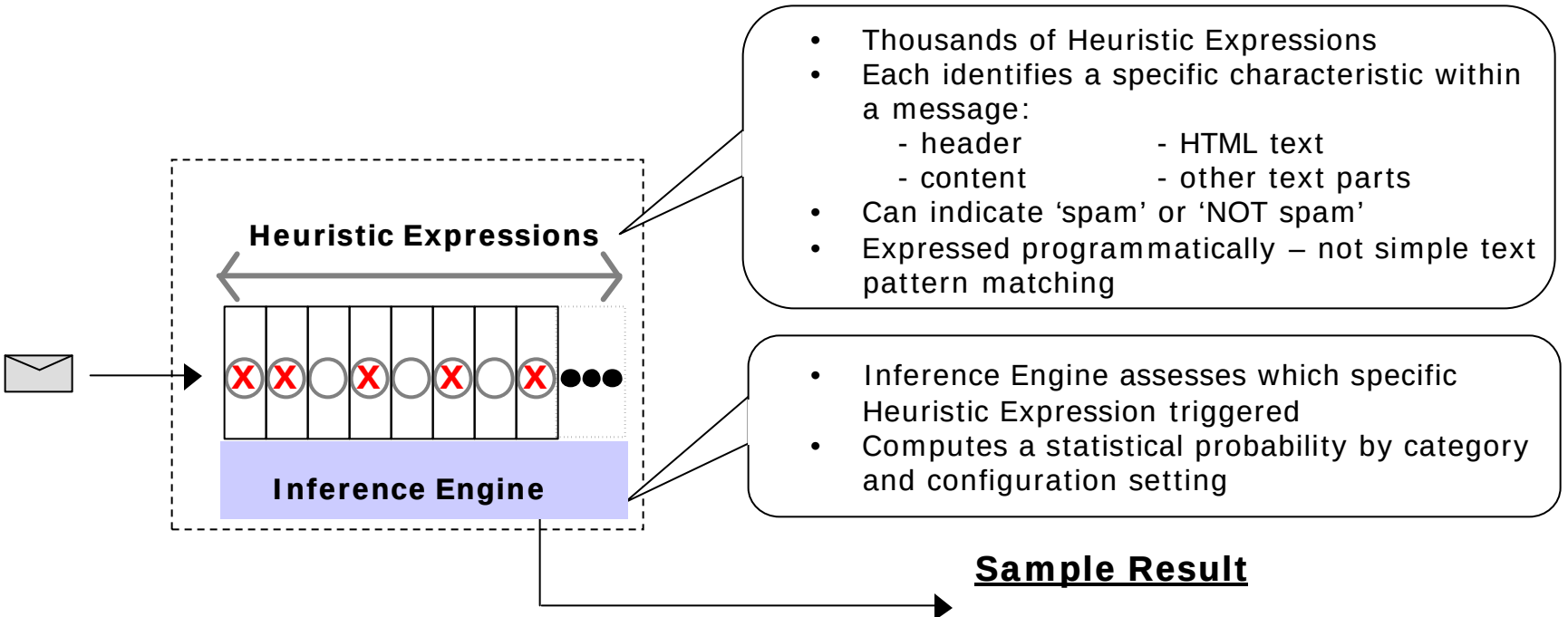
- Conditional SMTP access
- In-line statistical analysis
- Disposition prior to delivery

2-Tier Approach for Email System Security



- Over 50% of server resources wasted in processing erroneous messages
- An effective security solution must comprehend both aspects of SMTP data

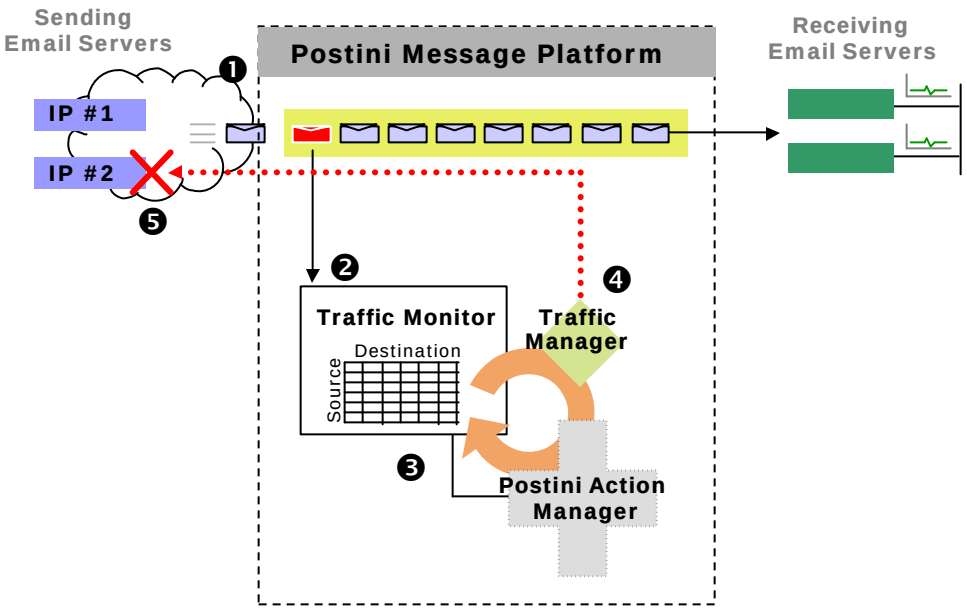
Postini Real-Time Heuristic Analysis



- Disposition determined by correlating score against configuration settings
- Supports granular configuration options: Sensitivity by category
- Automatically and incrementally modified as spammer tactics evolve

Postini Real-Time SMTP Analysis

- Postini sits between Internet and customer servers
- Identifies, resolves threats before hitting customer network
- Stateful inspection of SMTP connection and content data
  - Real-time Feedback loop
  - Conditional access to email server
  - Block or throttle at the IP level



1 - SMTP channel is instrumented. Connections and content data is collected in real time

2 - Real-time Traffic Monitor aggregates data

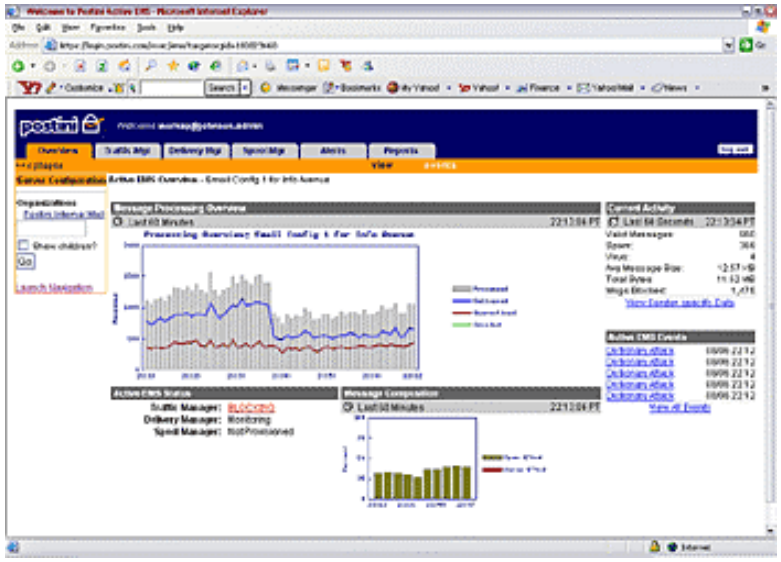
3 - Action Manager interprets Traffic Monitor data for conditions and threats, initiates action depending on customer configuration

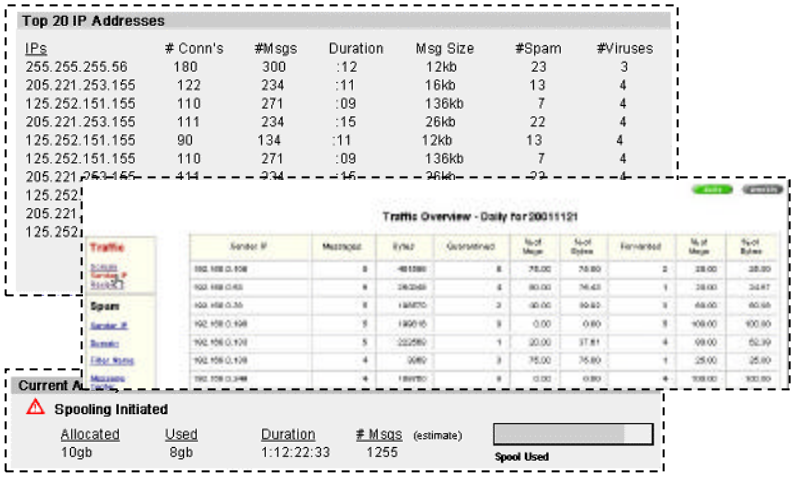
High incidence of 550 errors relative to valid message delivery suggests Email Harvest Attack

4 - Action Manager instructs Traffic Manager to block offending IP, halting further connection attempts from that address

5 - Email traffic from valid senders continues unabated

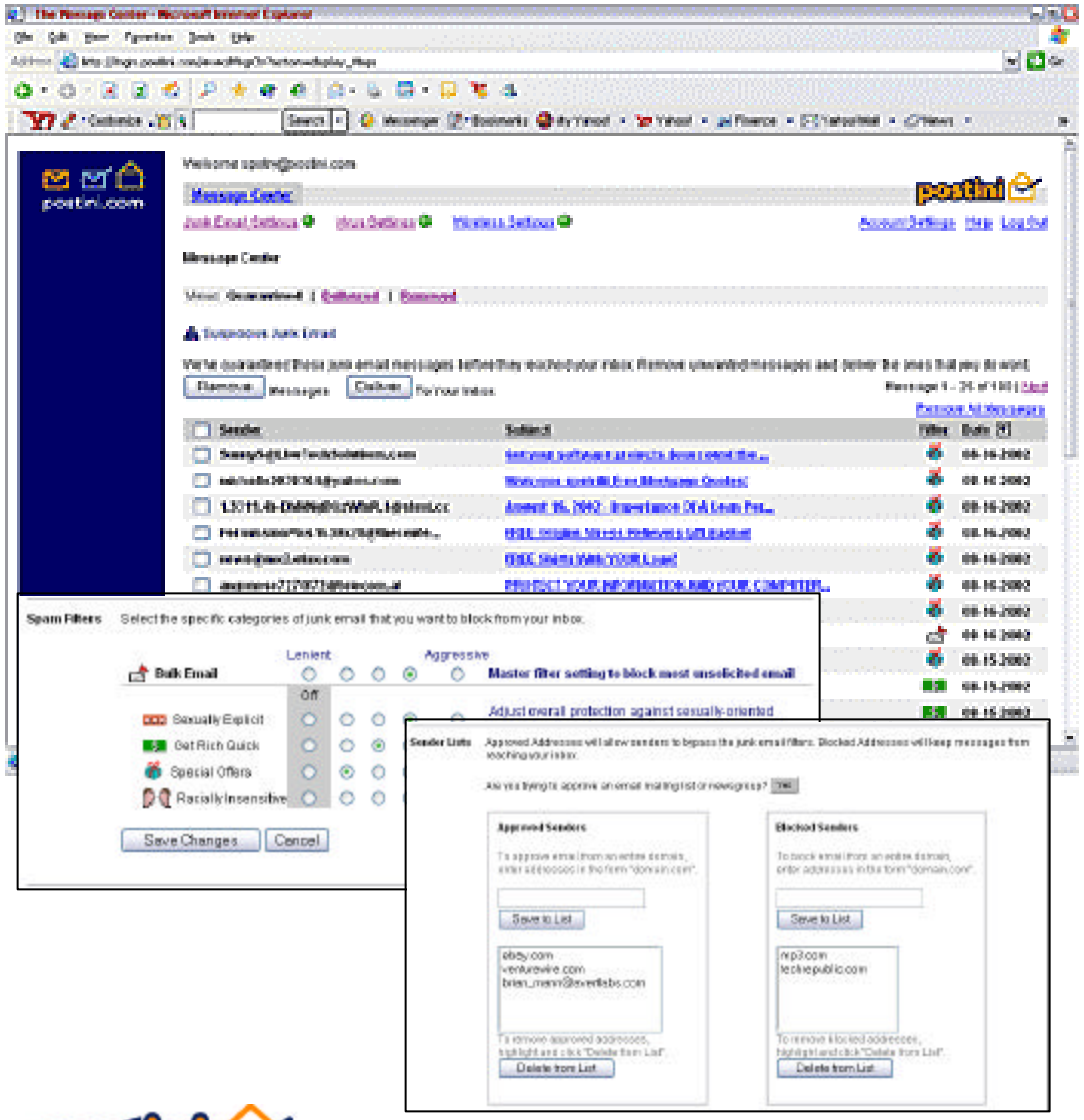
Admins Gain System-Wide Visibility





- Secure, consolidated management and administration of the ***entire email system***
- ***Policy-based*** application deployment on organization-wide or individual basis
- ***Deep visibility*** into usage statistics, traffic metrics, histogram, system responsiveness, etc.
- ***Improved reliability*** through system monitoring, administrator alerts, load balancing and email spooling

Statistical Analysis Enables Customization



- Most effective
  - 90-97% catch rate
  - .5 - .01% false quarantine
  - empirically validated
- Most Flexible
  - Quarantine for review
  - Sensitivity
  - Category type
- Policy-based provisioning
  - admin or user controlled
  - user/group settings

Postini Customers (CONFIDENTIAL)

PACKETEER

digitalfountain

FORRESTER

FOUNDATION CAPITAL

Interliant

DPR Construction Inc.

Voyager CAPITAL

Integral Capital Partners

TOSHIBA

LORAL Space & Communications

INVESCO

NEUBERGER BERMAN

BINGHAM McCUTCHEN

KEEN Your Personal Advisor

CANAAN PARTNERS

MORRISON & FOERSTER LLP

SEQUOIA CAPITAL

The American Society of Mechanical Engineers

COMPUTERWORLD

Draper International

Cornish & Carey Commercial

H&Q ASIA PACIFIC


end