The Scope of the Spam Problem

Enrique Salem
Understanding Spam

Legal definition of spam: Anti-spam laws exist in a number of countries around the world
• Currently no universally accepted definition of ‘spam’
Spam Continues to Grow and Evolve

Spam Always Evolving

ASCII Simple Text
Ink - All Printer?
Brands - ?
No shipping charge

Mutations and Randomization
1nk - All Printer?
Br@nds !!!!!! ?
No shipping charge
xyysdy99394

HTML Vary message while maintaining the same look

URL Short messages with links to spam Web pages

Converging Threats (viruses and worms)
Check out this picture!!!
I hope you like it.
Bye

Phishing More damaging

Severity/Complexity

Spam as a percentage of all email

8%

2001 2004

65%
Claimed Region of Origin

North America 70.9%
Asia 14.7%
Europe 9.9%
South America 2.6%
Africa 0.1%

Note: Claimed region of origin indicates the region from which the message claims to originate.
Non-English Spam is not Insignificant

- Non-English: 16%
- English: 84%
Solution to Spam? Multi-Layered Approach

Multiple Anti-Spam Technologies

- Content Filters
- Allowed Senders List
- Blocked Senders List
- Brightmail Reputation Service
- Signatures
- URL Filters
- Language Identification
- Heuristic Filters

Brightmail Anti-Spam Technologies and Architecture

- Reputation Filtering
  - Trojan Sources
  - High Volume Spam Sources
  - Safe Sources

- URL Filters
  - Fraud URLs
  - Mail URLs
  - HTTP URLs
  - Adult URLs

- Heuristics
  - Header Analysis
  - Foreign Language
  - Content Analysis
  - Structural Analysis

- Signatures
  - Body Hash
  - Body Fuzzy Signatures
  - Attachment Signatures

- Anti-Spam Architecture
  - Probe Network
  - BLOC Technicians
  - Redundant Architecture
  - Real-time Filter Delivery
  - Fraud Detection
  - Automated QA

- Customer-Defined Filters
  - Personal Allow List
  - Personal Block List
  - Personal Language Filters
  - Content Filters
  - Allowed Senders List
  - Blocked Senders List

Available Actions:
- Deliver to Inbox
- Delete
- Folder
- Save to Disk
- Quarantine
- Forward
- Modify

Filter Managed by Brightmail
Filter Managed by Customers
Fraud is Bigger Threat than Spam to Email Security

<table>
<thead>
<tr>
<th></th>
<th>Spam</th>
<th>Fraud</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Range of Damage</strong></td>
<td>Internal</td>
<td>External</td>
</tr>
<tr>
<td><strong>Asset Attacked</strong></td>
<td>IT Resources</td>
<td>Brand</td>
</tr>
<tr>
<td><strong>Group Targeted</strong></td>
<td>Employees</td>
<td>Customers and potential customers</td>
</tr>
<tr>
<td><strong>Key Threat</strong></td>
<td>Ability to use email as a</td>
<td>Ability to do business online</td>
</tr>
<tr>
<td></td>
<td>communication medium</td>
<td></td>
</tr>
</tbody>
</table>

Symantec Confidential
Messages Are Deceptive

Email: Messages appear legitimate … except for fraudulent URLs

Dear Citibank customer,

We are letting you know, that you, as a Citibank checking account holder, must become acquainted with our new Terms & Conditions and agree to it.

Please, carefully read all the parts of our new Terms & Conditions and post your consent. Otherwise, we will have to suspend your Citibank checking account.

This measure is to prevent misunderstanding between us and our valued customers.

We are sorry for any inconvenience this may cause.

Click here to access our Terms & Conditions page and not allow your Citibank checking account suspension.

A 2003 Citibank, Citibank (West), FSB. Member FDIC. Citibank with Arc Design is a registered service mark of Citicorp.

citi.com
citigroup.com
Citicorp Privacy Promise
Terms & Conditions
Copyright @ 2003 Citicorp

---

Dear eBay User,

During our regular update and verification of the accounts, you could not verify your current information. Either your information has changed or it is incomplete.

Please update and verify your information by clicking here and signing into your account. If the account information is not updated to current information within 5 days then, your access to bid, buy or sell on eBay will be restricted.

Thank you

Accounts Management

Copyright 2003 eBay Inc. All Rights Reserved.

As outlined in our User Agreement, eBay will periodically send you information about site changes and enhancements. Visit our Privacy Policy and User Agreement if you have any questions.

Copyright 2003 eBay Inc. All Rights Reserved.

Designated trademarks and brands are the property of their respective owners. eBay and the eBay logo are trademarks of eBay Inc.

www.citibank.com/ac%398HAAA9UWDYAZJWVWAAAA9pYWwgc2l6ZT00PjxTVgc2l6ZT00PjxT3Aac%398HAAA9UWDYAZJWVWAAAA9pYWwgc2l6ZT00PjxTVgc2l6ZT00PjxT@211.155.234.84

http://205.214.89.85/ebay.html
Websites Are Also Deceptive

Websites: Fraudulent sites often look more “real” than the legitimate sites

Exploits Microsoft I.E. “%01” vulnerability to display a legitimate URL

Legitimate Site
(with warning)

Fraudulent Site
## Growth and Impact of Email Fraud

<table>
<thead>
<tr>
<th>Cost</th>
<th>Description</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>$60 Billion</td>
<td>Cost of Identity Theft in last 5 years in US</td>
<td>FTC</td>
</tr>
<tr>
<td>600 hours</td>
<td>Individual time spent recovering from Identity Theft</td>
<td>Identity Theft Resource Center</td>
</tr>
<tr>
<td>3.4%</td>
<td>US Population fallen victim to Identity Theft</td>
<td>Gartner</td>
</tr>
<tr>
<td>3%</td>
<td>Estimated number of people reporting fraud to FTC</td>
<td>FTC</td>
</tr>
<tr>
<td>3.5 million</td>
<td>Number of FDIC fraud messages caught by Brightmail in one week in January 2004</td>
<td>Brightmail</td>
</tr>
</tbody>
</table>

### High Profile Attacks

<table>
<thead>
<tr>
<th>Financial Services</th>
<th>Consumer</th>
<th>Service Provider</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citibank, Visa, Fleet Bank, Barclays Bank, NatWest, Lloyds TSB, Nationwide, Halifax, Bank One, Bank of America, Wells Fargo, Bank of Montreal, Schwab…</td>
<td>EBay, Best Buy, PayPal, Microsoft, Sony, Target, UPS, Fedex, British Airways, Monster.com, 1-800-Flowers.com…</td>
<td>Yahoo, Earthlink, AOL, AT&amp;T, MSN, MSNTV…</td>
</tr>
</tbody>
</table>