

FTC & Spam

Howard Beales

Director, Bureau of Consumer Protection
U.S. Federal Trade Commission

The Problems with Spam

- Fraudulent and deceptive content
- High volume being sent
- Security issues
 - Service disruption
 - Viruses
- Cumulative economic damage
 - Estimate: \$10 billion to \$87 billion a year
- “Killing the Killer App”
 - Action needed to avert erosion of public confidence

Different From Other Marketing

- Anonymity: Spammers can easily cross international borders and hide their identity
 - False headers
 - Open relays and open proxies
- Cost: Spam is profitable
 - Even if response rate less than 0.0001%
(Testimony of bulk e-mailer at FTC Spam Forum)

Typical Spam Routing Headers

Return-Path: q0koco@aol.com

Received: from massena-2-81-57-128-46.fbx.proxad.net ([81.57.128.46]) by lakemtai08.cox.net (InterMail vM.5.01.06.05.201-253-122-130-105-20030824) with SMTP id <20040115161857.JKJM5944.lakemtai08.cox.net@massena-2-81-57-128-46.fbx.proxad.net>; Thu, 15 Jan 2004 14:18:57 -0500

Received: from [61.220.187.85] by massena-2-81-57-128-46.fbx.proxad.net id N1tbyb9rILTH; Thu, 15 Jan 2004 13:13:56 -0300

Message-ID: oj\$73un7\$p\$aI\$nx2617cbe0@wuy7.69oi.k2

From: "Chris Chamberlain" <q0koco@aol.com>

Reply-To: "Chris Chamberlain" <q0koco@aol.com>

To: dblumenthal@cox.net

Subject: Fwd:I need your help...

Date: Thu, 15 Jan 04 13:13:56 GMT

**Possibly
Forged**

Multinational Path

Received: from massena-2-81-57-128-46.fbx.proxad.net ([81.57.128.46]) by lakemtai08.cox.net

- Headers show route in reverse. The final destination is cox.net, a U.S. ISP. Cox.net received the message from proxad.net, a French ISP.

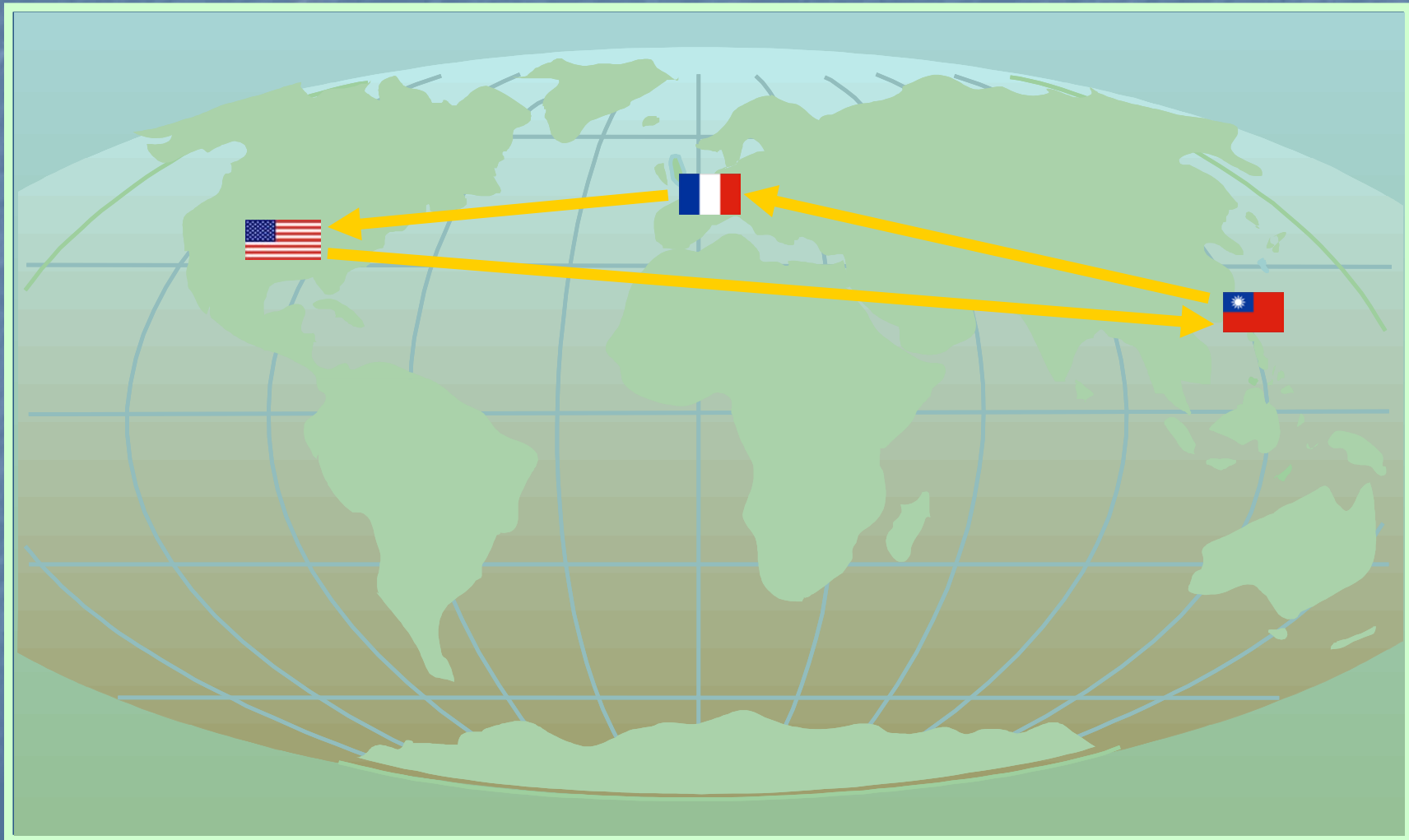
Received: from [61.220.187.85] by massena-2-81-57-128-46.fbx.proxad.net

- Proxad.net received the message from a server using IP number 61.220.187.85 - registered to a Taiwanese company - it was the first step in the routing process.

From: "Chris Chamberlain" q0koco@aol.com

- The message that showed its first step in Taiwan was from a U.S.-based ISP (although the address was spoofed in this case)

Multinational Path



What Is the FTC Doing About Spam?

- Research

- Studies, surfs

- Consumer and business education

- Forums, publications, Web sites

- Enforcement

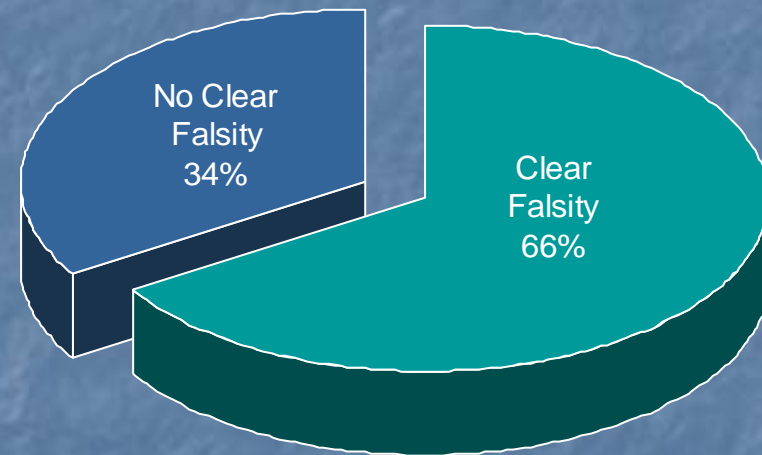
- Warning letters, cases

Research and Education

- “False Claims in Spam” Study
- “Remove Me” Surf
 - Do spammers honor requests to be removed from mailing lists?
- “Spam Harvest”
 - Where do spammers get email addresses?
- Spam Forum
- Operation Secure Your Server
 - Worldwide effort to close spammers’ access to anonymity

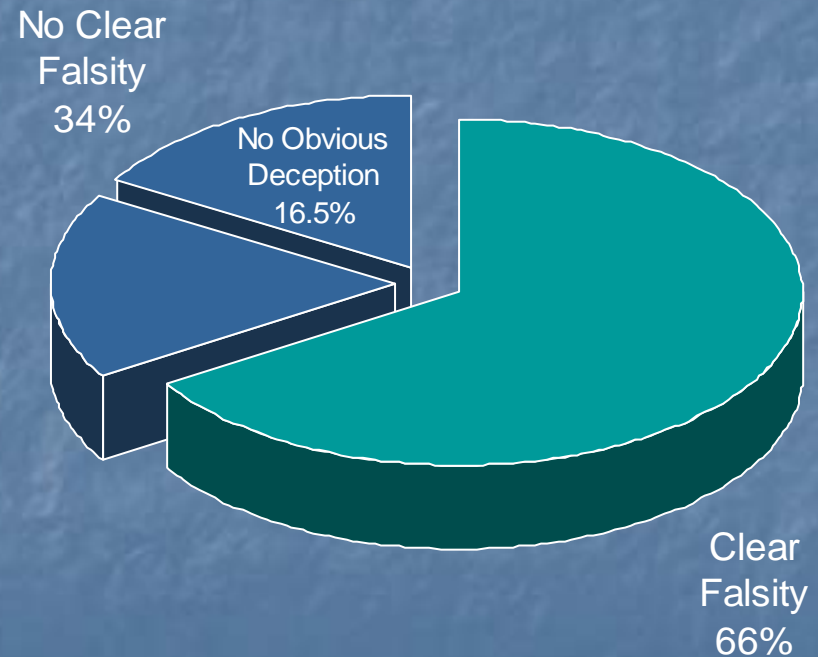
False Claims In Spam Study

- The FTC's study found that 66% of the spam sample contained signs of falsity in the from line, subject line, or text.



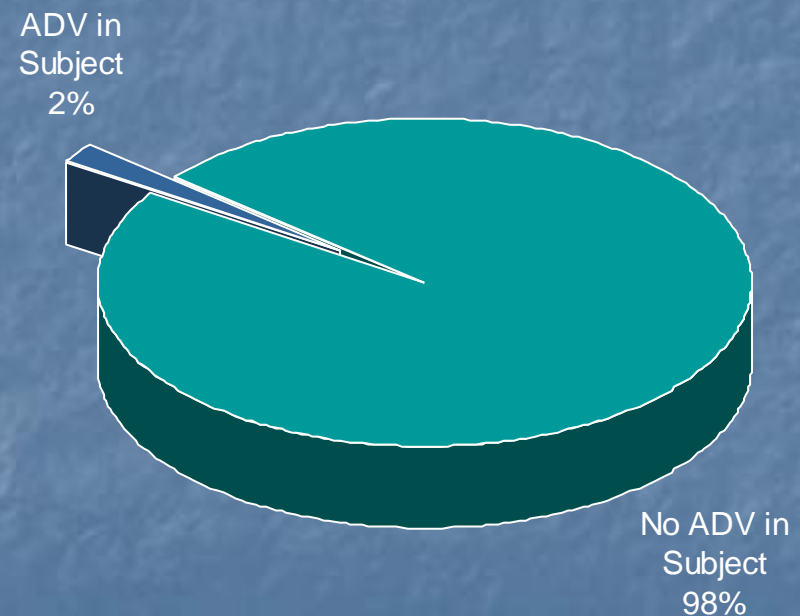
False Claims In Spam Study

- Only 16.5% of the spam did not sell an illegitimate product or service.
- We found no Fortune 500 companies and only one Fortune 1000 company among the websites connected to the spam by hyperlink.



False Claims In Spam Study

- Although several state laws required the use of “ADV” in the subject line of spam e-mail, only 2% of the spam actually complied with this requirement.

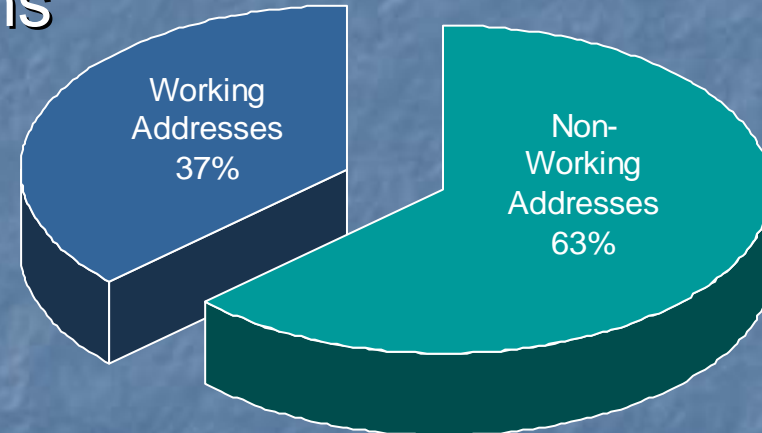


False Claims In Spam Study

- Falsity in the from line
 - Spammers mask their identity.
- Falsity in the subject line
 - Spammers mislead recipients to get them to open and read their messages.
- Falsity in the text
 - Spammers trick consumers into falling for worthless offers.

“Remove Me” Surf

- Tested 215 spam messages with “remove me” claims.
 - “Click here to be removed from mailing list.”
 - “Reply to this message with ‘unsubscribe’ in the subject.”
- 63% of links and reply options did not function.



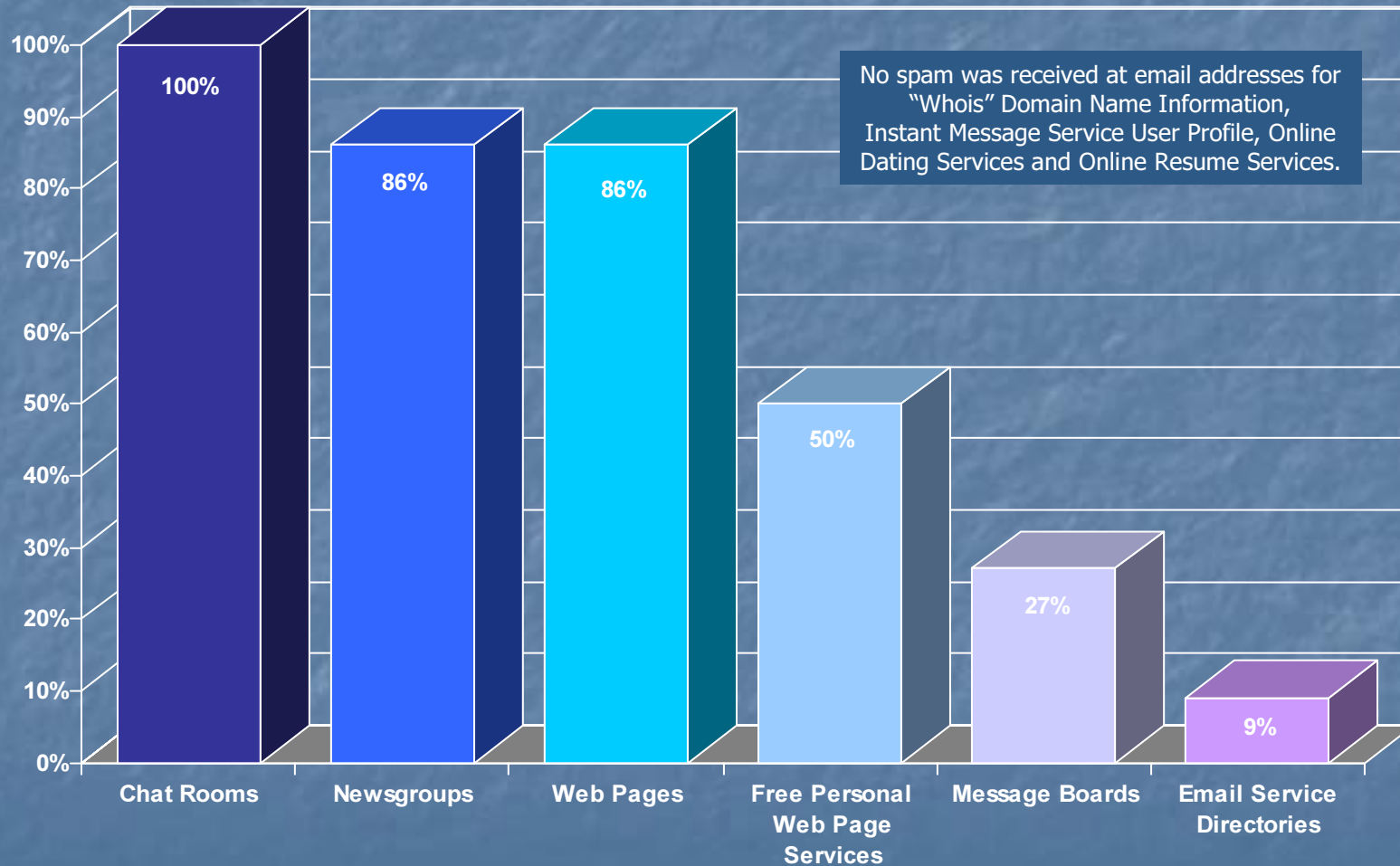
“Remove Me” Surf

- Opting out did *not* result in a greater volume of spam.
- Spammers making false “remove me” claims received a warning.

“Spam Harvest”

- Harvesting: Spammers use software to scan the Internet and capture email addresses
- The FTC placed unique email addresses throughout the Internet:
 - One address received spam only 8 minutes after it was used in a chat room.
 - 86% of addresses used on websites and newsgroups received spam, even though some weren't visible on the sites.

Email Address Harvesting



Source: Northeast Netforce Investigators seeded 175 different locations on the Internet with 250 new, undercover email addresses and monitored the addresses for six weeks.

Spam Forum

- Three days of discussions with 87 panelists
 - Advocates and opponents, marketers, technologists, law enforcement, and international regulators
- Emphasis
 - Mechanics and costs
 - Potential solutions
- Unique effort to gather all stakeholders in one room

Operation Secure Your Server

- International effort to notify owners of open relays and open proxies about how to protect their servers from abuse by spammers
- Spammers use these servers to send spam anonymously and avoid anti-spam filters
- 38 international government agencies from 28 countries are in the process of contacting tens of thousands open relay/proxy administrators

Operation Secure Your Server



Enforcement Against Spammers

- Despite anonymity, it *is* possible to find most spammers.
- FTC has filed over 55 spam-related cases.
 - Deceptive content
 - Deceptive and unfair spamming techniques
- The FTC wants spam
 - Forward spam to *uce@ftc.gov*

CAN-SPAM Act: New Violations

- False or misleading header information
- Deceptive subject lines
- Failure to include:
 - an opt-out method and honor opt-out requests
 - Sender's valid physical postal address
- New criminal violations for spam-related unauthorized access and spoofing, and false header and email account information
- Aggravated violations for spam plus:
 - Harvesting
 - Dictionary attack
 - Using someone else's computer without their authorization
 - Automated creation of multiple email accounts
- FTC may specify other aggravated violations to cover practices contributing to the spam problem

Solving the Spam Problem

- No “silver bullet” to limit spam
- Requires enhanced law enforcement tools *plus*
 - Technological developments
 - Business and consumer education
 - New business methods to reduce spam volume

FTC & Spam

www.ftc.gov/spam