Nobody’s Anonymous
Tracking Spam

Dr. Curtis Kret
Secure Science Corporation
http://www.securescience.net
Preface: We All Hate Spam...

- Spam is a problem.
  - “Problems” cannot be resolved until they are identified and classified.

- This presentation:
  - Describes methods for identifying, classifying, and tracking Spam
  - Identifying individual Spammers & purpose
  - Provides real-world examples
Contents

• Background
  – How Email Works (in under 3 minutes!)
  – Tracing Headers
• Organizing Spam
  – Identification, Classification, Tracking
• Covert Channels
  – Full-disclosure case study
• Conclusion & Questions
How Email Works

(A very brief overview)
Email Format

• Meta Header
  – field: value
    • TO: me@company.com
    • FROM: you@company.com

• Blank line (separates sections)

• Content
  – Usually plain text
Mail Forwarding and Delivery

1. Create the data
   Specify content subject, recipient

2. Local Mail System
   Populate header

3. Mail relays
   Apply more headers, route data

4. Recipient system
   Save to user’s box

5. Recipient Repository

6. Mail Reader
   View the mail

DNS: Used to identify mail servers
Okay. Much tedious time later, the RECEIPT and PURCHASE tables are repaired, *except*:

- I had to create new PURCHASE table entries for the 7 purchases
About Forging...

- “SMTP” not designed for security
  - Email is trivial to forge
  - Forged email passed easily to mail delivery agent
  - Most spammers forge email

Can Forge...
- Subject, Date, Message-ID
- Recipients: From, To, CC
- Other headers
- Content (body)
- Initial “Received” headers

Cannot Forge...
- Final “Received” headers
- “Originator”
  - IP address
  - Subsequent timestamps
Return-Path: <thicker@myself.com>
Received: from FUSMTA02-LRS ([62.172.195.247]) by server.company.com
     (InterMail vM.4.01.03.37 201-229-121-137-20020806) with ESMTP
     id <20021029142748.LLMT1493.server.company.com@FUSMTA02-LRS>
     for <neil@company.com>; Tue, 29 Oct 2002 14:27:48 +0000
Received: from [217.39.203.112] (helo=inverglen.co.uk)
     by FUSMTA02-LRS with esmtp (Exim 4.05)
     id 186XLB-0000Pi-00; Tue, 29 Oct 2002 14:27:33 +0000
Received: from 10.0.0.1 ([202.164.182.76]) by inverglen.co.uk with
     Microsoft SMTPSVC(5.0.2195.5329); Tue, 29 Oct 2002 14:28:53 +0000
Message-ID: <NWRMPLKIHGFQQLYMKLCYJHATAVFFL@10.0.0.1>
From: "Martin Williams" <thicker@myself.com>
To: nealedwards@webtv.net
X-MS-JQU: BCWXNXCDXQN
Date: Tue, 29 Oct 02 06:26:15 Eastern Standard Time
Content-Type: multipart/mixed;
       boundary=WC_MAIL_PaRt_BoUnDaRy_05151998
Subject: New Pill guranteed to give you a thicker larger penis!
Forged Header Clues

- “Received” - mismatched “From” and “By”
  - “HELO” name does not match IP address
- Non-standard headers
- Wrong or “different” format
  - Date
  - Received
  - Message-ID
  - Header labels
Organizing Spam
Organizing By Content
Organizing By Headers

- Spammer Tools act consistently
  - Same headers, same inconsistencies
  - Hash Busters: same format/locations
    - Unique subject/content strings bypass Spam filters

- Spammers are PEOPLE
  - People act consistently (until they need to change)
    - Tools not changed until becomes ineffective
  - Cheap: Most write their own tools; some share
## All Spam (Unorganized)

<table>
<thead>
<tr>
<th>Date</th>
<th>Sender</th>
<th>(Lines)</th>
<th>Subject</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aug 29</td>
<td><a href="mailto:lloihg@yahoo.com">lloihg@yahoo.com</a></td>
<td>43</td>
<td>Russian Girls Looking for men</td>
</tr>
<tr>
<td>Aug 29</td>
<td>Lorene2284f66@mult</td>
<td>104</td>
<td>You missed this investment last time, didn’t you? 0054qbVf1-834EQnE-16</td>
</tr>
<tr>
<td>Aug 29</td>
<td>latestnews7205g838</td>
<td>51</td>
<td>We Have a FREE Euro For You!</td>
</tr>
<tr>
<td>Aug 29</td>
<td><a href="mailto:bdrake18user@aol.com">bdrake18user@aol.com</a></td>
<td>57</td>
<td>Huge Profit on eBay</td>
</tr>
<tr>
<td>Aug 29</td>
<td><a href="mailto:bbballjac@hotmail.com">bbballjac@hotmail.com</a></td>
<td>174</td>
<td>Attn: SYSTEM WORKS CLEARANCE SALE ONLY $29.99</td>
</tr>
<tr>
<td>Aug 29</td>
<td>Mason</td>
<td>49</td>
<td>Spend More Time With Your Kids! Work at Home &amp; Make Great Money!</td>
</tr>
<tr>
<td>Aug 29</td>
<td><a href="mailto:cezauser@aol.com">cezauser@aol.com</a></td>
<td>58</td>
<td>Make a fortune on eBay - FREE Info</td>
</tr>
<tr>
<td>Aug 29</td>
<td>Jeremiah</td>
<td>51</td>
<td>Spend More Time With Your Kids! Work at Home &amp; Make Great Money!</td>
</tr>
<tr>
<td>Aug 29</td>
<td><a href="mailto:loras@atncorp.com">loras@atncorp.com</a></td>
<td>300</td>
<td>NIGHT VISION NZT-1 Just $99!</td>
</tr>
<tr>
<td>Aug 28</td>
<td><a href="mailto:ccxcfgdz@yahoo.com">ccxcfgdz@yahoo.com</a></td>
<td>93</td>
<td>300 percent boost for cellphone</td>
</tr>
<tr>
<td>Aug 28</td>
<td><a href="mailto:ccxcfgdz@yahoo.com">ccxcfgdz@yahoo.com</a></td>
<td>35</td>
<td>Want a Home Improvement Loan</td>
</tr>
<tr>
<td>Aug 29</td>
<td>Halina7538y28@iris</td>
<td>53</td>
<td>You won’t believe this! 1368Uige3-287Rw-14</td>
</tr>
<tr>
<td>Aug 29</td>
<td>kickboxthequeen</td>
<td>1931</td>
<td>Welcome to my hometown</td>
</tr>
<tr>
<td>Aug 29</td>
<td>Akilah2006w31@yahoo</td>
<td>66</td>
<td>The decision is yours 6526Ecu8-485ktQ-15</td>
</tr>
<tr>
<td>Aug 28</td>
<td>Christopher_Chasel</td>
<td>92</td>
<td>Money Manager Site</td>
</tr>
<tr>
<td>Aug 27</td>
<td><a href="mailto:lurchpa@hotmail.co">lurchpa@hotmail.co</a></td>
<td>174</td>
<td>PROTECT YOUR INFORMATION AND YOUR COMPUTER!</td>
</tr>
<tr>
<td>Aug 27</td>
<td><a href="mailto:nnetwork@bubfet.co">nnetwork@bubfet.co</a></td>
<td>149</td>
<td>Adv: Reduce your term on your mortgage.</td>
</tr>
<tr>
<td>Aug 27</td>
<td>a56772176y450lycos</td>
<td>46</td>
<td>** Your -approval- **</td>
</tr>
<tr>
<td>Aug 27</td>
<td><a href="mailto:jbroder@netzero.ne">jbroder@netzero.ne</a></td>
<td>197</td>
<td>Extended Auto Warranties Here</td>
</tr>
<tr>
<td>Aug 27</td>
<td><a href="mailto:zeroaday@idir.net">zeroaday@idir.net</a></td>
<td>188</td>
<td>Baby Boomers, Get Your Youth Back Now</td>
</tr>
<tr>
<td>Aug 26</td>
<td>a10in983118x050lyc</td>
<td>42</td>
<td>** Your -approval- **</td>
</tr>
<tr>
<td>Aug 26</td>
<td><a href="mailto:bbssw2@yahoo.com">bbssw2@yahoo.com</a></td>
<td>132</td>
<td>Need a good lawyer cheap</td>
</tr>
<tr>
<td>Aug 27</td>
<td><a href="mailto:mnytzen@bubfet.com">mnytzen@bubfet.com</a></td>
<td>86</td>
<td>Adv: Reach Million of Opt-In Customers Now!</td>
</tr>
<tr>
<td>Aug 27</td>
<td><a href="mailto:momentous@bubfet.com">momentous@bubfet.com</a></td>
<td>93</td>
<td>Adv: Generate Wealth on Wall Street</td>
</tr>
<tr>
<td>Aug 26</td>
<td>Julie29933746post</td>
<td>110</td>
<td>Browse Lovely Young Mail Order Brides for FREE (17-29 y/o)</td>
</tr>
<tr>
<td>Aug 26</td>
<td><a href="mailto:lloihg@yahoo.com">lloihg@yahoo.com</a></td>
<td>43</td>
<td>Healthcare you can afford</td>
</tr>
</tbody>
</table>

Copyright 2003 Secure Science Corp.
From: alice149@hotmail.com
Reply-To: alice149@hotmail.com
To: oblaga@hotmail.com, piasono2@hotmail.com
Cc: raver77@hotmail.com, narcisse@eccw.com
Message-ID: <000056361fbd$00006231$000047fa@copywriterl.ls>
Subject: Re: BE healthy with this BREAKTHROUGH product!
Date: Thu, 05 Sep 2002 07:54:28 -1600

Cap Letters
Cap Letters with TZ “-1600”

<table>
<thead>
<tr>
<th>Date</th>
<th>Username</th>
<th>Email Address</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sep 09</td>
<td>corbinjim@...</td>
<td>(171)</td>
<td>Attn: This is NO JOKE! Speed up your CPU for under $30!</td>
</tr>
<tr>
<td>Sep 09</td>
<td>corbinjim@...</td>
<td>(171)</td>
<td>Attn: This is NO JOKE! Speed up your CPU for under $30!</td>
</tr>
<tr>
<td>Sep 06</td>
<td>bbarber612@...</td>
<td>(167)</td>
<td>PROTECT YOUR INFORMATION AND YOUR COMPUTER! EZBCYT</td>
</tr>
<tr>
<td>Sep 05</td>
<td>alice149@...</td>
<td>(157)</td>
<td>Re: BE healthy with this BREAKTHROUGH product!</td>
</tr>
<tr>
<td>Sep 04</td>
<td>bconst3442@...</td>
<td>(91)</td>
<td>actually work?”NWWR</td>
</tr>
<tr>
<td>Sep 02</td>
<td>connie.1_1@...</td>
<td>(170)</td>
<td>Fw: PROTECT YOUR COMPUTER AGAINST HARMFUL VIRUSES!</td>
</tr>
<tr>
<td>Sep 01</td>
<td>binder39@...</td>
<td>(168)</td>
<td>Fw: NORTON SYSTEMWORKS CLEARANCE SALEONLY $29.99!</td>
</tr>
<tr>
<td>Aug 30</td>
<td>breaks26@...</td>
<td>(167)</td>
<td>Fw: DON'T LET A COMPUTER VIRUS RUIN YOUR DAY!</td>
</tr>
<tr>
<td>Aug 29</td>
<td>bballjac@...</td>
<td>(173)</td>
<td>Attn: SYSTEMWORKS CLEARANCE SALE ONLY $29.99!</td>
</tr>
<tr>
<td>Aug 25</td>
<td>bbkke861@...</td>
<td>(160)</td>
<td>Fw: PROTECT YOUR COMPUTER, YOU NEED SYSTEMWORKS!</td>
</tr>
<tr>
<td>Aug 20</td>
<td>blueguy13@...</td>
<td>(175)</td>
<td>Re: Discount Prices + FREE Shipping = #1 Service!</td>
</tr>
<tr>
<td>Aug 20</td>
<td>blueguy13@...</td>
<td>(175)</td>
<td>Re: Discount Prices + FREE Shipping = #1 Service!</td>
</tr>
<tr>
<td>Aug 12</td>
<td>bcook61@...</td>
<td>(151)</td>
<td>Attn: PROTECT YOUR COMPUTER, YOU NEED SYSTEMWORKS!ROOZ</td>
</tr>
<tr>
<td>Aug 11</td>
<td>breedde@...</td>
<td>(170)</td>
<td>Aren’t these things overpriced??XPQXLVE</td>
</tr>
<tr>
<td>Aug 09</td>
<td>barednek@...</td>
<td>(74)</td>
<td>Free Consultation, Buy Viagra Online !KK</td>
</tr>
<tr>
<td>Aug 09</td>
<td>barednek@...</td>
<td>(74)</td>
<td>Free Consultation, Buy Viagra Online !KK</td>
</tr>
<tr>
<td>Aug 07</td>
<td>bjorne59@...</td>
<td>(93)</td>
<td>Attn: Want to LOSE Weight FAST?WNSJDBZD</td>
</tr>
<tr>
<td>Aug 07</td>
<td>bcoole2@...</td>
<td>(91)</td>
<td>Lose 80lbs In A Wk? #1 Diet Pill! Wholesale!!JI</td>
</tr>
<tr>
<td>Aug 07</td>
<td>bbarrf@...</td>
<td>(60)</td>
<td><strong>Your Free Club membership!</strong>** DRZFP</td>
</tr>
<tr>
<td>Aug 07</td>
<td>bbarker6@...</td>
<td>(91)</td>
<td>Lose 19 Pounds In 10 Days!</td>
</tr>
<tr>
<td>Jul 30</td>
<td>dafrican@...</td>
<td>(141)</td>
<td>Re: Can’t Stand the Cost of Ink Cartridges? VGMURR</td>
</tr>
<tr>
<td>Jul 28</td>
<td>el186@...</td>
<td>(225)</td>
<td>Re: Men &amp; Women, Spruce up your life!</td>
</tr>
<tr>
<td>Jul 17</td>
<td>dagnyh@...</td>
<td>(88)</td>
<td>Lose 14 Pounds In 10 Days</td>
</tr>
<tr>
<td>Jul 09</td>
<td>cwood83@...</td>
<td>(97)</td>
<td>Make your prints beautiful &amp; SAVE BIG!</td>
</tr>
<tr>
<td>Jul 09</td>
<td>cwood83@...</td>
<td>(97)</td>
<td>Make your prints beautiful &amp; SAVE BIG!</td>
</tr>
<tr>
<td>Jul 04</td>
<td>contactroxy@...</td>
<td>(138)</td>
<td>Welcome to the Modern Way to Improve your Budget! XVITRZY</td>
</tr>
</tbody>
</table>
Cap Letters with TZ “-1700”

Dec 07 * ttyrew21@yahoo.com (101) Get better reception on your cell phoneSBCZFIHRN
Dec 07 * kkjhq65@yahoo.com (101) Boost your cell phone receptionKP
Dec 07 * minir221@yahoo.com (83) Need to be revitalizedVC
Dec 07 * ggdsr2@yahoo.com (83) Want to look youngerIAT
Dec 06 * vdsd221@yahoo.com (108) FW: HOT New Toy for Christmas 2002!KEDMIXBV
Dec 06 * ccvdc21@yahoo.com (108) FW: HOT New Toy for Christmas 2002!HQZGA
Dec 06 * rrewe21@yahoo.com (132) Protect your pc from hackersJQZI
Dec 06 * ppiou66@yahoo.com (133) Keep the hackers off your computerJDLIKTMS
Dec 05 * ljkjy56@yahoo.com (41) Automated Life Insurance quotes,JOBQ
Dec 05 * zxxas21@yahoo.com (42) We can save you thousands on life insuranceAMKG
Dec 04 * erw221@yahoo.com (107) HOT New Toy for Christmas 2002! J
Dec 04 * ggwss2@yahoo.com (108) FW: Remote Controlled Mini Matchbox Cars CI
Dec 04 * ytytr453@yahoo.com (46) Mortgage Rates are going lower
Dec 04 * mmmj543@yahoo.com (46) Mortgage Rates are going lowerUHW
Dec 03 * opioi78@yahoo.com (101) Tired of Dropped Cell CallsMS
Dec 03 * ccxsd2@yahoo.com (100) Get crystal reception on your cell phoneFBPNO
Dec 02 * bcvbcv32@yahoo.com (107) RE: Remote Controlled Mini Matchbox CarsQNM
Dec 02 * vvdsv2122@yahoo.com (107) FW: MINI RADIOCONTROLLED CARS ARE SOLD OUT IN STORES
Dec 02 * cxxzxo12@yahoo.com (78) Look and feel 30 years youngerXRDRJBAOSW
Dec 02 * cxxzxo12@yahoo.com (78) Look and feel 30 years youngerABCT
Dec 01 * vbcx21@yahoo.com (58) Enlarge your packageGTGIL
Dec 01 * vvds21@yahoo.com (59) Feeling SmallLPMEIV
Nov 30 * bcvcv32@yahoo.com (53) Refinance today and save thousandsJAL
Nov 30 * bcvcv32@yahoo.com (53) Want a Home Improvement LoanZQJAG
Nov 28 * ngtr32@yahoo.com (45) Want a Home Improvement LoanZETLCJYI
Nov 27 * nqmr3@yahoo.com (107) FW: MINI RADIOCONTROLLED CARS ARE SOLD OUT IN STORES

Thanksgiving: Thu Nov 28, 2002

Copyright 2003 Secure Science Corp.
Organizing Methods Summary

• Ignore **Contents** and **Subject**
  – Text changes too easily
  – Contents may be “borrowed”

• Focus on **Headers** and **Signatures**
  – Identify common inconsistencies (fingerprints)

• Organize by common features
Defining Spam

Identifying major categories
Every Definition is Different

MAIL ABUSE PREVENTION SYSTEM
Definition of "spam"

STANDARD:

An electronic message is "spam" IF: (1) the recipient's personal identity and context are irrelevant because the message is equally applicable to many other potential recipients; AND (2) the recipient has not verifiably granted deliberate, explicit, and still-revocable permission for it to be sent; AND (3) the transmission and reception of the message appears to the recipient to give a disproportionate benefit to the sender.
What is “Spam”? 

- “Spam” defined as “Undesirable Email”
- Classifications by intended purpose
  - Most common classes:
    1. Unsolicited Commercial Email
    2. Non-responsive Commercial Email
    3. List Makers
    4. Scams
    5. Covert Messages camouflaged as Spam
True Commercial Categories

The Spam Minority
1. Unsolicited Commercial Email

- **Purpose**
  - Actual companies contact *existing* customers
  - Actual companies contact *potential* customers

- **Identification**
  - No forged mail headers
  - Only 1 recipient: You.
  - "From:" matches "Reply-To:", other ID, and contact methods
  - Multiple contact methods
  - Does not ask to be forwarded
  - Frequently personalized, polite, to the point

True UCE is RARE!
UCE Example

SMART CLOCK

SHUTS OFF WITH A WAVE OF YOUR HAND!

American Technologies Network Corp.
20 S.Linden Ave. Unit 1B
South San Francisco, CA 94080
888-447-4946, 650-872-1278, FAX 650-875-0129
2. Non-responsive Commercial Email

• Purpose
  – Actual companies contact previous customers

• Identification
  – NCE looks like UCE

• Key differences from UCE
  – User initiated contact (non-transferable opt-in)
  – User opted-out from future communications
  – NCE violates “do not contact” requests
Subject: Holiday Gift Ideas and Free Shipping from Comcast's Shopping Channel!
Date: Sun, 7 Dec 2003 15:00:01 -0700

Shopping.Comcast.net

Holiday shopping has never been so much fun or easy!

Find great bargains and last minute gift ideas at the Shopping Channel on Comcast.net-your ultimate holiday shopping resource. With access to over 5 million products and 3,500 merchants, we're your one-stop store for the greatest gifts and the best deals.

...Not sure why you've received this e-mail?

Privacy Statement - http://www.comcast.net/privacy/?CM.src=eml031205

Terms of Service - http://www.comcast.net/terms/?CM.src=eml031205

© 2003 Comcast Cable Communications, Inc. All rights reserved.
My Comcast Preferences...

Comcast E-mail Contact Preferences

Be the first to hear about special offers, promotions, or features and the latest products and services from Comcast.

E-mail Address  xxxxxxxx@comcast.net

Zip Code  94011

☐ I'd like to receive e-mail from Comcast High-Speed Internet about special offers, promotions, or features. Note: If you opt out of receiving Comcast High-Speed Internet e-mails for special offers, promotions, or features, Comcast may still send Service and account-related e-mails to you.

☐ I'd like to receive e-mail from Comcast Cable about special offers, promotions, or features related to Comcast's Cable TV products and services and upcoming TV shows.
Other NCE Companies

• Besides Comcast...
• Other known NCE providers
  – Amazon.com
  – Angelfire/Lycos/Tripod Productions
  – Barns & Noble University
  – Hewlett-Packard
Non-Commercial Categories

The vast majority of Spam
3. List Makers

• Purpose
  – Make money by gathering & selling addresses
  – Three types of address lists
    • Grade “A”: Known good (someone replied)
    • Grade “B”: Probably good (no reply)
    • Grade “C”: Known bad (bounced)
List Makers: Validation

- Harvest addresses
- Send out a “test” message to addresses
  - Large variety of test messages
- Watch for reply
  - Bounced? Grade “C”
  - Nothing? Grade “B”
  - Reply? Grade “A”!
List Maker: Mark9

I Want to Get Started!
Here's How To Get Started Now!

We're ready to RUSH you - by return email - the complete, step-by-step Getting Started instructions, and REMEMBER!

YOU do NOT have to pay the $49.95 ACCESS FEE for all of the TOOLS, INSTRUCTIONS, and UPDATES until YOU have tried them for a FULL 30 DAYS and can see for yourself that it WORKS!

Your $19.95 US one-time payment will get you all of the SOFTWARE and TOOLS you need to get started making money NOW, and includes:

- Complete step-by-step set up instructions - Plan to spend one full day setting everything up to run automatically.
- All the Software you Need to run this business on autopilot.
- 650 opt-in email lists with HALF A MILLION people on them who have SUBSCRIBED, with hundreds more added daily.
- Access to autoresponder, and the instructions for setting them up so you COULD be...
106,056 may19b
72,992 may19c
106,056 may19d
54,195 names.txt
14,979,785 total.txt
5,013 opportunity_seekers
208,225 removes
27,812 Removes2

15,560,134 total addresses
15,454,078 total unique addresses
List Makers: Identification

• Common identification methods
  – Forged headers
  – Valid “From” and “Reply-To”: May not match content
  – HTML attachment
    • Web bugs for validation
    • One recipient with unique ID
    • Valid URLs (lots of them! lots of sites!)
  – Contact via web/email; No phone/address information
  – Huge address lists (in the “10-million or larger” range)

• Many spammers make lists… Even UCE
4. Scams

• Purpose
  – Acquire valuable assets from people
    • Money
    • Personal Information
    • Computer resources (worms & viruses)
  – Misrepresentation
Scams: Identification

- Usually forged headers
- “Subject” may not match message content
- Not a legitimate company
  - “From” and “Reply-To” do not match contact info
  - Many recipients: “To:”, “CC:”, and “BCC:”
- Justification for contact and methods
  - “You requested this” or a sad story
- And of course: reads like a scam
  - Pyramid, easy promises/quick wins
  - Money-related
  - Contact by phone/post office OR web/email (not both)
Dear Sir,

Ref.No.pro-hosiery-cor3-1of8
Jul.16,03.

We learnt your e-mail address through internet.

We would like to co-operate with you as supplying lady's "fishnet" panty hose(tight), stocking, compression hosiery and general panty hose(tight) in EXTRA LARGE sizes to you with sincerity.

Because for some reasons, at the beginning, it is not proper for us to reveal our real e-mail address and website, so if you response to us, please be sure to use "Fax" AND MENTION OUR Ref No. because the sender's e-mail address is virtual (we can't receive your response if you e-mail is via this virtual e-mail address).

...
Case Study: Gone Phishing
Dear Citibank Member,

This email was sent by the Citibank server to verify your e-mail address. You must complete this process by clicking on the link below and entering in the small window your Citibank ATM/Debit Card number and PIN that you use on ATM. This is done for your protection because some of our members no longer have access to their email addresses and we must verify it.

To verify your e-mail address and access your bank account, click on the link below. If nothing happens when you click on the link (or if you use AOL), copy and paste the link into the address bar of your web browser.

http://www.citibank.com:ac=piUq3027qcHw003nfuJ2@sd96V.pIsEm.NET/3/?3X6CMW2I2uPOVQW

Thank you for using Citibank!

---------------------------------------------
Russian URL

Your E-Mail Address Was Successful Verified.

Thank you.
### Сводная статистика IP адресов посетителей

**Статистика с 8.8.2003 по 15.8.2003**

Подобно

Распределение IP адресов (всего): 10

<table>
<thead>
<tr>
<th>№</th>
<th>Адрес</th>
<th>Количество</th>
<th>Среднее в день</th>
<th>Процент в группе</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>68.82.62.191</td>
<td>8</td>
<td>1</td>
<td>80.00%</td>
</tr>
<tr>
<td>2</td>
<td>12.5.1.207</td>
<td>1</td>
<td>0.12</td>
<td>10.00%</td>
</tr>
<tr>
<td>3</td>
<td>208.141.219.205</td>
<td>1</td>
<td>0.12</td>
<td>10.00%</td>
</tr>
</tbody>
</table>

### Таблица посещений

<table>
<thead>
<tr>
<th>День</th>
<th>Хиты</th>
</tr>
</thead>
<tbody>
<tr>
<td>08.08.2003</td>
<td>3</td>
</tr>
<tr>
<td>09.08.2003</td>
<td>0</td>
</tr>
<tr>
<td>10.08.2003</td>
<td>0</td>
</tr>
<tr>
<td>11.08.2003</td>
<td>5</td>
</tr>
<tr>
<td>12.08.2003</td>
<td>0</td>
</tr>
<tr>
<td>13.08.2003</td>
<td>1</td>
</tr>
<tr>
<td>14.08.2003</td>
<td>1</td>
</tr>
<tr>
<td>15.08.2003</td>
<td>1</td>
</tr>
<tr>
<td>16.08.2003</td>
<td>107274</td>
</tr>
<tr>
<td>17.08.2003</td>
<td>91503</td>
</tr>
<tr>
<td>18.08.2003</td>
<td>584</td>
</tr>
<tr>
<td>19.08.2003</td>
<td>209</td>
</tr>
<tr>
<td>20.08.2003</td>
<td>0</td>
</tr>
</tbody>
</table>

Итого: 199581
Phishing Header

Received: from host70-72.pool80117.interbusiness.it ([80.117.72.70])
    by mailserver with SMTP
    id <20030929021659s1200646q1e>; Mon, 29 Sep 2003 02:17:00 +0000
Received: from sharif.edu [83.104.131.38] by host70-
72.pool80117.interbusiness.it (Postfix) with ESMTP id EAC74E21484B for <e-
response@securescience.net>; Mon, 29 Sep 2003 11:15:38 +0000
Date: Mon, 29 Sep 2003 11:15:38 +0000
From: Verify <verify@citibank.com>
Subject: Citibank E-mail Verification: test@securescience.net
To: Test <test@securescience.net>
References: <F5B12412EAC2131E@securescience.net>
In-Reply-To: <F5B12412EAC2131E@securescience.net>
Message-ID: <EC2B7431BE0A6F48@citibank.com>
Reply-To: Verify <verify@citibank.com>
Sender: Verify <verify@citibank.com>
MIME-Version: 1.0
Content-Type: text/plain
Content-Transfer-Encoding: 8bit
# Related by Message-ID

<table>
<thead>
<tr>
<th>Great Spam Archive Date</th>
<th>Message-ID</th>
<th>Subject</th>
</tr>
</thead>
<tbody>
<tr>
<td>24 Apr 2003 13:01:55</td>
<td><a href="mailto:0JJ9H7JGA03EI8A7I@att.net">0JJ9H7JGA03EI8A7I@att.net</a></td>
<td>Rich, Hello! My name is John Turner....</td>
</tr>
<tr>
<td>15 Jun 2003 12:41:00</td>
<td><a href="mailto:D4CI74IDH3FKH13D@att.net">D4CI74IDH3FKH13D@att.net</a></td>
<td>Dear Rich! I've been scammed over...</td>
</tr>
<tr>
<td>07 Jul 2003 07:43:51</td>
<td><a href="mailto:2EF98ADD2HG3CJ54@att.net">2EF98ADD2HG3CJ54@att.net</a></td>
<td>Rich, Any software just for 15$ - 40$</td>
</tr>
<tr>
<td>17 Jul 2003 10:39:28</td>
<td><a href="mailto:76E7A5HFJIIHK63C@e-loan.com">76E7A5HFJIIHK63C@e-loan.com</a></td>
<td>[Ftpserver] Re: Your E-Loan Refinance..</td>
</tr>
<tr>
<td>17 Jul 2003 10:46:08</td>
<td><a href="mailto:6J76H1B289HCC313@e-loan.com">6J76H1B289HCC313@e-loan.com</a></td>
<td>Re: Your E-Loan Refinance Application..</td>
</tr>
<tr>
<td>22 Jul 2003 01:21:52</td>
<td><a href="mailto:77EGJ4AGC1F3AIB5@wellsfargo.com">77EGJ4AGC1F3AIB5@wellsfargo.com</a></td>
<td>Re: Wells Fargo Bank New Business... Newsletter</td>
</tr>
<tr>
<td>26 Jul 2003 09:43:59</td>
<td><a href="mailto:JFHAL1CJIB78IFFA8@security.org">JFHAL1CJIB78IFFA8@security.org</a></td>
<td>The Great E-Gold Giveaway!</td>
</tr>
<tr>
<td>26 Jul 2003 23:00:46</td>
<td><a href="mailto:H8HFB0BB06232180@e-gold.com">H8HFB0BB06232180@e-gold.com</a></td>
<td>Rich, software for you</td>
</tr>
<tr>
<td>29 Jul 2003 18:39:15</td>
<td><a href="mailto:4K63GFHLE8FJ1GK7@utp.edu.co">4K63GFHLE8FJ1GK7@utp.edu.co</a></td>
<td>I want to introduce Stock Cruiser</td>
</tr>
<tr>
<td>30 Jul 2003 19:03:38</td>
<td><a href="mailto:3FHG03G0I213JJ92@yahoo.com">3FHG03G0I213JJ92@yahoo.com</a></td>
<td>new mail</td>
</tr>
<tr>
<td>31 Jul 2003 05:26:44</td>
<td><a href="mailto:J9D9GK1H1IJ47920@hotmail.com">J9D9GK1H1IJ47920@hotmail.com</a></td>
<td>p1QwvfpX</td>
</tr>
<tr>
<td>02 Aug 2003 10:21:12</td>
<td><a href="mailto:BG5L3CAI6J586EK0@headgear.org">BG5L3CAI6J586EK0@headgear.org</a></td>
<td>Rich, Want sex &lt;rndmx&gt;</td>
</tr>
<tr>
<td>09 Aug 2003 11:59:24</td>
<td><a href="mailto:J9D9GK1H1IJ47920@hotmail.com">J9D9GK1H1IJ47920@hotmail.com</a></td>
<td>Ċęęęεiůé îůäůů</td>
</tr>
<tr>
<td>17 Aug 2003 07:58:36</td>
<td><a href="mailto:2J73600018ECI75J@virtualitas.net">2J73600018ECI75J@virtualitas.net</a></td>
<td>Re: mail</td>
</tr>
<tr>
<td>17 Aug 2003 17:49:39</td>
<td><a href="mailto:FBE6962ED2FJFK58@hotmail.com">FBE6962ED2FJFK58@hotmail.com</a></td>
<td>e4AXAvl8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Re: mail</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3CPVQp5E</td>
</tr>
</tbody>
</table>
## Related: Scams

<table>
<thead>
<tr>
<th>Great Spam Archive Date</th>
<th>Message-ID</th>
<th>Subject</th>
</tr>
</thead>
<tbody>
<tr>
<td>24 Apr 2003 13:01:55</td>
<td><a href="mailto:0JJ9H7JGA03EI8A71@att.net">0JJ9H7JGA03EI8A71@att.net</a></td>
<td>Rich, Hello! My name is John Turner....</td>
</tr>
<tr>
<td>15 Jun 2003 12:41:00</td>
<td><a href="mailto:D4CI74IDH3FKH13D@att.net">D4CI74IDH3FKH13D@att.net</a></td>
<td>Dear Rich! I've been scammed over...</td>
</tr>
<tr>
<td>07 Jul 2003 07:43:51</td>
<td><a href="mailto:2EF98ADD2HG3CJ54@att.net">2EF98ADD2HG3CJ54@att.net</a></td>
<td>Rich, Any software just for 15$ - 40$</td>
</tr>
<tr>
<td>17 Jul 2003 10:39:28</td>
<td><a href="mailto:76E7A5HFJHIHK63C@e-loan.com">76E7A5HFJHIHK63C@e-loan.com</a></td>
<td>[Ftpserver] Re: Your E-Loan Refinance..</td>
</tr>
<tr>
<td>17 Jul 2003 10:46:08</td>
<td><a href="mailto:6J76H1B289HCC313@e-loan.com">6J76H1B289HCC313@e-loan.com</a></td>
<td>Re: Your E-Loan Refinance Application..</td>
</tr>
<tr>
<td>22 Jul 2003 01:21:52</td>
<td><a href="mailto:77EGJ4AGC1F3Al5B5@wellsfargo.com">77EGJ4AGC1F3Al5B5@wellsfargo.com</a></td>
<td>Re: Wells Fargo Bank New Business...</td>
</tr>
<tr>
<td>26 Jul 2003 09:43:59</td>
<td><a href="mailto:JFHAL1CJIB78I8A8@security.org">JFHAL1CJIB78I8A8@security.org</a></td>
<td>Newsletter</td>
</tr>
<tr>
<td>26 Jul 2003 23:00:46</td>
<td><a href="mailto:H8HFB0BB06232180@e-gold.com">H8HFB0BB06232180@e-gold.com</a></td>
<td>The Great E-Gold Giveaway!</td>
</tr>
<tr>
<td>29 Jul 2003 18:39:15</td>
<td><a href="mailto:4K63GFHLE8FJ1GK7@utp.edu.co">4K63GFHLE8FJ1GK7@utp.edu.co</a></td>
<td>Rich, software for you</td>
</tr>
<tr>
<td>30 Jul 2003 19:03:38</td>
<td><a href="mailto:3FHG03G0I213JJ92@yahoo.com">3FHG03G0I213JJ92@yahoo.com</a></td>
<td>I want to introduce Stock Cruiser</td>
</tr>
<tr>
<td>31 Jul 2003 05:26:44</td>
<td><a href="mailto:BG5L3CAI6J586EK0@headgear.org">BG5L3CAI6J586EK0@headgear.org</a></td>
<td>new mail                p1QwvfpX</td>
</tr>
<tr>
<td>02 Aug 2003 10:21:12</td>
<td><a href="mailto:J9D9GK1H1IJ47920@hotmail.com">J9D9GK1H1IJ47920@hotmail.com</a></td>
<td>Rich, Want sex  &lt;rndmx&gt;</td>
</tr>
<tr>
<td>09 Aug 2003 11:59:24</td>
<td><a href="mailto:50LJ6D9B4EK320HD@annexia.org">50LJ6D9B4EK320HD@annexia.org</a></td>
<td>ï€ï€šï¿½ï¿½ï¿½ï¿½</td>
</tr>
<tr>
<td>17 Aug 2003 07:58:36</td>
<td><a href="mailto:2J736000184C175J@virtualitas.net">2J736000184C175J@virtualitas.net</a></td>
<td>Re: mail                   e4AXAVl8</td>
</tr>
<tr>
<td>17 Aug 2003 17:49:39</td>
<td><a href="mailto:FBE6962ED2FJFK58@hotmail.com">FBE6962ED2FJFK58@hotmail.com</a></td>
<td>Rich, Instant Pleasures,</td>
</tr>
<tr>
<td>20 Aug 2003 19:37:45</td>
<td><a href="mailto:A60I9A7D890FL51L@cbhost-68-111-42-31.sbccox.net">A60I9A7D890FL51L@cbhost-68-111-42-31.sbccox.net</a></td>
<td>Re: mail                   3CPVQp5E</td>
</tr>
</tbody>
</table>
## Related: Phishing

<table>
<thead>
<tr>
<th>Great Spam Archive Date</th>
<th>Message-ID</th>
<th>Subject</th>
</tr>
</thead>
<tbody>
<tr>
<td>24 Apr 2003 13:01:55</td>
<td><a href="mailto:0JJ9H7JGA03E18A71@att.net">0JJ9H7JGA03E18A71@att.net</a></td>
<td>Rich, Hello! My name is John Turner....</td>
</tr>
<tr>
<td>15 Jun 2003 12:41:00</td>
<td><a href="mailto:D4CI74IDH3FKH13D@att.net">D4CI74IDH3FKH13D@att.net</a></td>
<td>Dear Rich! I've been scammed over...</td>
</tr>
<tr>
<td>07 Jul 2003 07:43:51</td>
<td><a href="mailto:2EF98ADD2HG3CJ54@att.net">2EF98ADD2HG3CJ54@att.net</a></td>
<td>Rich, Any software just for 15$ - 40$</td>
</tr>
<tr>
<td>17 Jul 2003 10:39:28</td>
<td><a href="mailto:76E7A5HFIJIIHK63C@e-loan.com">76E7A5HFIJIIHK63C@e-loan.com</a></td>
<td>[Ftpserver] Re: Your E-Loan Refinance..</td>
</tr>
<tr>
<td>17 Jul 2003 10:46:08</td>
<td><a href="mailto:6J76H1B289HCC313@e-loan.com">6J76H1B289HCC313@e-loan.com</a></td>
<td>Re: Your E-Loan Refinance Application..</td>
</tr>
<tr>
<td>22 Jul 2003 01:21:52</td>
<td><a href="mailto:77EGJ4AGC1F3AlB5@wellsfargo.com">77EGJ4AGC1F3AlB5@wellsfargo.com</a></td>
<td>Re: Wells Fargo Bank New Business...</td>
</tr>
<tr>
<td>26 Jul 2003 09:43:59</td>
<td><a href="mailto:JFHAL1CJIB781FA8@security.org">JFHAL1CJIB781FA8@security.org</a></td>
<td>Newsletter</td>
</tr>
<tr>
<td>26 Jul 2003 23:00:46</td>
<td><a href="mailto:H8HFB0BB06232180@e-gold.com">H8HFB0BB06232180@e-gold.com</a></td>
<td>The Great E-Gold Giveaway!</td>
</tr>
<tr>
<td>29 Jul 2003 18:39:15</td>
<td><a href="mailto:4K63GFHLE8FJ1GK7@utp.edu.co">4K63GFHLE8FJ1GK7@utp.edu.co</a></td>
<td>Rich, software for you</td>
</tr>
<tr>
<td>30 Jul 2003 19:03:38</td>
<td><a href="mailto:3FHG03G0I213JJ92@yahoo.com">3FHG03G0I213JJ92@yahoo.com</a></td>
<td>I want to introduce Stock Cruiser</td>
</tr>
<tr>
<td>31 Jul 2003 05:26:44</td>
<td><a href="mailto:BG5L3CAI6J586EK0@headgear.org">BG5L3CAI6J586EK0@headgear.org</a></td>
<td>new mail p1QwvfpX</td>
</tr>
<tr>
<td>02 Aug 2003 10:21:12</td>
<td><a href="mailto:J9D9GK1H1J47920@hotmail.com">J9D9GK1H1J47920@hotmail.com</a></td>
<td>Rich, Want sex &lt;rndmx&gt;</td>
</tr>
<tr>
<td>09 Aug 2003 11:59:24</td>
<td><a href="mailto:50LJ6D9B4EK320HD@annexia.org">50LJ6D9B4EK320HD@annexia.org</a></td>
<td>ï€‌ï€‌ï€‌ï€‌ ið‌aûô</td>
</tr>
<tr>
<td>17 Aug 2003 07:58:36</td>
<td><a href="mailto:2J73600018ECI75J@virtualitas.net">2J73600018ECI75J@virtualitas.net</a></td>
<td>Re: mail e4AXAvl8</td>
</tr>
<tr>
<td>17 Aug 2003 17:49:39</td>
<td><a href="mailto:FBE6962ED2FJK58@hotmail.com">FBE6962ED2FJK58@hotmail.com</a></td>
<td>Rich, Instant Pleasures,</td>
</tr>
<tr>
<td>20 Aug 2003 19:37:45</td>
<td><a href="mailto:A60IA7D89OFL51L@cbhost-68-111-42-31.sbcocx.net">A60IA7D89OFL51L@cbhost-68-111-42-31.sbcocx.net</a></td>
<td>Re: mail 3CPVQp5E</td>
</tr>
</tbody>
</table>
## Related: Malware

<table>
<thead>
<tr>
<th>Date</th>
<th>Message-ID</th>
<th>Subject</th>
</tr>
</thead>
<tbody>
<tr>
<td>24 Apr 2003</td>
<td><a href="mailto:0JJ9H7JGA03EI8A7I@att.net">0JJ9H7JGA03EI8A7I@att.net</a></td>
<td>Rich, Hello! My name is John Turner...</td>
</tr>
<tr>
<td>15 Jun 2003</td>
<td><a href="mailto:D4CI74IDD3FKH13D@att.net">D4CI74IDD3FKH13D@att.net</a></td>
<td>Dear Rich! I've been scammed over...</td>
</tr>
<tr>
<td>07 Jul 2003</td>
<td><a href="mailto:2EF98ADD2G3CJ54@att.net">2EF98ADD2G3CJ54@att.net</a></td>
<td>Rich, Any software just for 15$ - 40$</td>
</tr>
<tr>
<td>17 Jul 2003</td>
<td><a href="mailto:76E7A5HFIJHIK63C@e-loan.com">76E7A5HFIJHIK63C@e-loan.com</a></td>
<td>[Ftpserver] Re: Your E-Loan Refinance..</td>
</tr>
<tr>
<td>17 Jul 2003</td>
<td><a href="mailto:6J76H1B289HCC313@e-loan.com">6J76H1B289HCC313@e-loan.com</a></td>
<td>Re: Your E-Loan Refinance Application..</td>
</tr>
<tr>
<td>22 Jul 2003</td>
<td><a href="mailto:77EGJ4AGC1F3AIB5@wellsfargo.com">77EGJ4AGC1F3AIB5@wellsfargo.com</a></td>
<td>Re: Wells Fargo Bank New Business...</td>
</tr>
<tr>
<td>26 Jul 2003</td>
<td><a href="mailto:JFHAL1CJIB78IFA8@security.org">JFHAL1CJIB78IFA8@security.org</a></td>
<td>Newsletter</td>
</tr>
<tr>
<td>26 Jul 2003</td>
<td><a href="mailto:H8HFB0BB06232180@e-gold.com">H8HFB0BB06232180@e-gold.com</a></td>
<td>The Great E-Gold Giveaway!</td>
</tr>
<tr>
<td>29 Jul 2003</td>
<td><a href="mailto:4K63GFHLE8F1JGK7@utp.edu.co">4K63GFHLE8F1JGK7@utp.edu.co</a></td>
<td>Rich, software for you</td>
</tr>
<tr>
<td>30 Jul 2003</td>
<td><a href="mailto:3FHG03G0I213JJ92@yahoo.com">3FHG03G0I213JJ92@yahoo.com</a></td>
<td>I want to introduce Stock Cruiser</td>
</tr>
<tr>
<td>31 Jul 2003</td>
<td><a href="mailto:BG5L3CAI6J586EK0@headgear.org">BG5L3CAI6J586EK0@headgear.org</a></td>
<td>new mail p1Qwvfpx</td>
</tr>
<tr>
<td>02 Aug 2003</td>
<td><a href="mailto:J9D9GK1H1IJ47920@hotmail.com">J9D9GK1H1IJ47920@hotmail.com</a></td>
<td>Rich, Want sex &lt;rndmx&gt;</td>
</tr>
<tr>
<td>09 Aug 2003</td>
<td><a href="mailto:50LJ6D9B4E320HD@annexia.org">50LJ6D9B4E320HD@annexia.org</a></td>
<td>ï€‘ï€œï€ îœœú­úœ</td>
</tr>
<tr>
<td>17 Aug 2003</td>
<td><a href="mailto:2J73600018EC175J@virtualitas.net">2J73600018EC175J@virtualitas.net</a></td>
<td>Re: mail e4AXAvI8</td>
</tr>
<tr>
<td>17 Aug 2003</td>
<td><a href="mailto:FBE6962ED2FJK58@hotmail.com">FBE6962ED2FJK58@hotmail.com</a></td>
<td>Rich, Instant Pleasures,</td>
</tr>
<tr>
<td>20 Aug 2003</td>
<td><a href="mailto:A60I9A7D890FL51L@cbhost-68-111-42-31.sbc">A60I9A7D890FL51L@cbhost-68-111-42-31.sbc</a> Cox.net</td>
<td>Re: mail 3CPVQp5E</td>
</tr>
</tbody>
</table>
Use of Malware

• Trojan.Download.Berbew
  – Captures passwords
• Exploit-Codebase
  – 26-Jul-2003
• Malware consistencies:
  – Written in C, same compiler
  – Old exploit techniques
# And Related Scams...

<table>
<thead>
<tr>
<th>Date</th>
<th>E-Loan</th>
<th>E-Gold</th>
<th>Yahoo</th>
<th>eBay</th>
<th>PayPal</th>
<th>Wells Fargo</th>
<th>Citibank</th>
<th>One-time Financial Targets</th>
</tr>
</thead>
<tbody>
<tr>
<td>17-Jul-2003</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21-Jul-2003</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>26-Jul-2003</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16-Aug-2003</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Security.org (M)</td>
</tr>
<tr>
<td>3-Sep-2003</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>17-Sep-2003</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>19-Sep-2003</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>23-Sep-2003</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>25-Sep-2003</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>28-Sep-2003</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>30-Sep-2003</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>2-Oct-2003</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>4-Oct-2003</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>5-Oct-2003</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>9-Oct-2003</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>18-Oct-2003</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>20-Oct-2003</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>419 (Nigerian scam)</td>
</tr>
<tr>
<td>21-Oct-2003</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>25-Oct-2003</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>Barclays Bank</td>
</tr>
<tr>
<td>26-Oct-2003</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>Halifax, Nationwide Banks</td>
</tr>
<tr>
<td>27-Oct-2003</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Lloyds Bank</td>
</tr>
<tr>
<td>9-Nov-2003</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>13-Nov-2003</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>15-Nov-2003</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>20-Nov-2003</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>22-Nov-2003</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>26-Nov-2003</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>419</td>
</tr>
</tbody>
</table>

**M:** Use of email with a hostile/malware attachment.

**X:** Use of email requesting information by email or hostile web site.
Phishing Summary

• Serial Phishing Group
  – Unique bulk-mailing tool
  – Primarily target: Citibank and eBay
  – Members
    • At least one in Tybouts Corner, Delaware
    • Some members in Europe
  – Dabbled in malware (email Trojans)
    • Comfortable with web impersonations
5. Covert Messages

• Purpose
  – Secret communication

• Why spam as a covert channel?
  – Hiding in plain sight
  – Forged email sources makes it hard to trace
    • Proxies can obscure path; Sender is anonymous
  – Spam is broadcast -- Recipient is anonymous
  – Do not need to be “on-line”
  – Plausible deniability
Covert Messages: Identification

• Not: UCE, NCE, Scam, List Maker
  – Multiple email lists; multiple members
  – Email designed to be caught by spam filters!
• “Not random” text in headers, contents, or signature
• Reuse spam messages!
  – Reused from multiple sources (not one specific spammer)
  – Usually not porn or scams
    • Do not want casual recipients looking too closely
  – HTML frequently contains invalid/broken links
  – (List Maker) Everyone receives same “unique ID” or web-bug
Case study: Hang-Outers

lee7 gR00P
(Elite Group)
Received: from yahoo.com ([210.248.69.67]) by server.company.com
   (InterMail vM.4.01.03.27 201-229-121-127-20010626) with SMTP
   id <20020502121549.NUAJ6753.server.company.com@yahoo.com>;
   Thu, 2 May 2002 12:15:49 +0000
Received: from unknown (HELO rly-xr01.mx.aol.com) (237.236.94.228)
   by rly-xw01.mx.aol.com with local; Tue, 30 Apr 2002 18:15:24 -1000
Received: from [32.230.106.82] by smtp013.mail.yahoo.com with local; Mon, 29 Apr 2002
   07:13:00 +1200
Received: from 79.224.119.189 ([79.224.119.189]) by a231242.upc-a.chello.nl with asmtp;
   Sat, 27 Apr 2002 20:10:36 +0400
Received: from mta05bw.bigpond.com ([127.219.131.43])
   by sydint1.microthin.com.au with QMQP; Fri, 26 Apr 2002 09:08:12 -0400
Reply-To: <75573.270cQDiR7@earthlink.net>
Message-ID: <EBBB6252-3E87-43CE-B214-FE4A5C940DE5@FP1na3ty>
From: <75573.270cQDiR7@earthlink.net>
To: <pandt@company.com>
Subject: HEY!     w941Q
MIME-Version: 1.0
Content-Type: multipart/mixed;
   boundary="=_NextPart_000_00P6_57S68U9W.X3811A11"
X-Priority: 3 (Normal)
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 5.50.4133.2400
Importance: Normal
Date: Thu, 2 May 2002 12:15:52 +0000
About the Content...

- Reused content
- Script to prevent viewing page source:

```html
...<SCRIPT>
function noRightClick(evnt) { var userAgent = window.navigator.userAgent; if (userAgent.indexOf("MSIE") > 0) { if (event.button == 2) { alert("Not enough system memory to display source."); return false; } }
else { if (evt.which == 3) { alert("Not enough system memory to display source."); return false; } }
}
document.onmousedown = noRightClick;
</SCRIPT>
```

[gvjr Fov-ka1AsHb3-oOGlgZSseoUJF]

[gvjr Fov-ka1AsHb3-oOGlgZSseoUJF]
[Governor of - class B - oh gee I guess UJF]
Chris025

Hang-outers' e-mails
Please inform us if you would like your email add to be posted here.
Right now we are still in the process of asking permission... blah blah blah...

<table>
<thead>
<tr>
<th>Name</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>hci</td>
<td><a href="mailto:hci@mail.com">hci@mail.com</a></td>
</tr>
<tr>
<td>Anferme</td>
<td></td>
</tr>
<tr>
<td>angelface</td>
<td></td>
</tr>
<tr>
<td>beatlebum</td>
<td><a href="mailto:skidrow_gail@mailcity.com">skidrow_gail@mailcity.com</a></td>
</tr>
<tr>
<td>CyBerSad*</td>
<td><a href="mailto:cybersad04@yahoo.com">cybersad04@yahoo.com</a></td>
</tr>
<tr>
<td>Czarina*</td>
<td><a href="mailto:czarina@pacific.net.ph">czarina@pacific.net.ph</a></td>
</tr>
<tr>
<td>DATA*</td>
<td><a href="mailto:chris025@hotmail.com">chris025@hotmail.com</a></td>
</tr>
<tr>
<td>DoC_SpOky*</td>
<td></td>
</tr>
<tr>
<td>Fay^</td>
<td><a href="mailto:duchessfay@hotmail.com">duchessfay@hotmail.com</a></td>
</tr>
</tbody>
</table>
Linking...

- uic.globe.com.ph
  - University of Immaculate Conception, Philippines
- Cutting...

Hacked by CNHonker – Lion H.U.C. Welcome to http://www.cnhonker.com Goodluck!
Lion H.U.C.

- Honker = Political/patriotic hacker
- Lion H.U.C. = 1i0n Internet Worm (March 2001)
- www.cnhonker.com
  - Forwards to www.cnhonker.net
- www.cnhonker.net
  - Hosted at unixs1-g1.chinadns.com
  - ChinaDNS.com: Registrar for global top-level domain names (gTLDs)
红客联盟公告

- 红客联盟严正声明
- 关于中国红客网络技术联盟
- 关于红客联盟邮件列表
- 红客联盟网站更新脚本全部完成, 今天将开始更新!
- 红客联盟网站重新开放!

最新文档更新

- [新手上路] Telnet命令模式 07-26 艰苦
- [文档资料] 封包探测器 (Sniffer) 07-26 艰苦
- [文档资料] 基于80端口后门的实现 07-26 freeshell
- [文档资料] 利用008查找socket 07-25 bbhll
- [安全公告] Windows 2000实用程序管理器 07-14 墨斗鱼
- [安全公告] SMB数据包过滤缺陷允许 07-14 墨斗鱼
- [安全公告] HTML转换器缓冲区溢出导致黑 07-14 墨斗鱼
- [漏洞利用] D3S-mnogo.pl 07-14 墨斗鱼
- [文档资料] 没有电脑的入侵深人浅出社 07-12 gouyi2kaJokul
- [文档资料] 没有电脑的入侵深人浅出社 07-11 gouyi2kaJokul

邮件列表

- [联盟IRC] host: irc.sunnet.org
  port: 6667
  #cnhonker
  Web入口
  download: KIRC

最新软件更新

- [扫描工具] WebDAVScan.rar 03-22 ubhhuy
- [扫描工具] ntscan.zip 03-18 ubhhuy
- [扫描工具] nscans.zip 03-18 ubhhuy
- [扫描工具] MSscan V1.20 03-10 ubhhuy
- [后门工具] HFilter V0.10 01-28 lion
- [扫描工具] InfoScan.exe 01-27 ubhhuy
- [攻击工具] KGod V0.51 01-16 lion
- [扫描工具] MSscan v1.01 01-08 ubhhuy
Back to the Hang-Outers...

Received: from yahoo.com ([200.50.193.133]) by server.company.com (InterMail vM.4.01.03.27 201-229-121-127-20010626) with SMTP id <20020702032202.QXDO26984.server.company.com@yahoo.com>
  Tue, 2 Jul 2002 03:22:02 +0000
Received: from n7.groups.yahoo.com ([125.81.113.162])
  by m10.grp.snv.yahoo.com with QMQP; Sun, 30 Jun 2002 12:29:41 -0400
Received: from 173.75.125.16 ([173.75.125.16]) by mailout2-eri1.midsouth.rr.com with QMQP; Sat, 29 Jun 2002 01:27:17 -0000
Received: from [220.70.138.123] by rly-xl05.mx.aol.com with esmtp; Thu, 27 Jun 2002 14:24:53 -0300
Reply-To: <SabrinasTVTsi@stud.uni-muenchen.de>
Message-ID: <93BBAC09-8D33-11D6-9430-00E07D95FE3E@3f2HBQUM>
From: <SabrinasTVTsi@stud.uni-muenchen.de>
To: <coolkat00@company.com>
Subject: >> Aquire a new credit card! LblBrLeiE
Importance: Normal
Date: Tue, 2 Jul 2002 03:22:10 +0000

... [wyC3gAuFd54-Adia4Sb6koQr-ERYjQaRvqHCDp]
Sabrina To Cy...

Address: http://members.tripod.com/addiks/members.html

The happy people interested in joining the JOIN IN button below to our addiks members have us brief detail a greatly appreciate (peg format please).
HOME BASED POSITIONS:

ASSEMBLERS, CRAFTERS, COMPUTER WORK, ART WORK, MYSTERY SHOPPING, FREELANCE WRITING, SEWING, PLUS MUCH MORE......

Thu, 15 Aug 2002 03:31:21
Reply-To: <homejobsourcesagYNaB@netzero.com>
Message-ID: <A83A2EF3-AF7F-11D6-AAE6-444553540000@O5ZFCbmK>
From: "Susan Whaley" <homejobsourcesagYNaB@netzero.com>
Subject: Jobs at Home
tyou96Xkn

Thu, 15 Aug 2002 04:06:53
Reply-To: <homejobsourceslDot78@netzero.com>
Message-ID: <A83A333F-AF7F-11D6-AAE6-444553540000@XpfEaTRG>
From: "Susan Whaley" <homejobsourceslDot78@netzero.com>
Subject: Jobs at Home
FVOa7-JAuj-NfasGb

HOME BASED POSITIONS:

ASSEMBLERS, CRAFTERS, COMPUTER WORK, ART WORK, MYSTERY SHOPPING, FREELANCE WRITING, SEWING, PLUS MUCH MORE......

[pi5BUpBP9-tXKKHllffs-xBrTv1YFIM]
Data Analysis

Mon, 1 Apr 2002 18:25:27
Thu, 2 May 2002 12:15:49
Tue, 14 May 2002 08:06:01
Wed, 15 May 2002 08:05:23
Tue, 21 May 2002 16:09:46
Sat, 8 Jun 2002 13:47:31
Thu, 13 Jun 2002 16:50:53
Thu, 13 Jun 2002 16:00:49
Wed, 26 Jun 2002 20:23:59
Fri, 28 Jun 2002 10:25:39
Tue, 2 Jul 2002 03:22:02
Thu, 15 Aug 2002 03:31:21
Thu, 15 Aug 2002 04:06:53
Mon, 19 Aug 2002 19:30:37
Wed, 28 Aug 2002 21:10:31
Wed, 4 Sep 2002 03:26:05
Fri, 6 Sep 2002 17:19:45
Tue, 10 Sep 2002 18:41:33
Thu, 12 Sep 2002 01:21:48
Fri, 27 Sep 2002 07:06:44
Mon, 30 Sep 2002 07:01:48
Wed, 9 Oct 2002 01:11:38
Fri, 11 Oct 2002 02:28:25
Fri, 11 Oct 2002 06:39:35
Fri, 25 Oct 2002 07:53:08
Sun, 27 Oct 2002 07:58:42
Wed, 6 Nov 2002 10:02:29
Tue, 19 Nov 2002 03:06:02
Tue, 19 Nov 2002 07:54:46
Tue, 26 Nov 2002 03:59:48
Tue, 31 Dec 2002 01:24:50
# Volume Analysis

## Hour when messages were received

<table>
<thead>
<tr>
<th>GMT+0</th>
<th>01</th>
<th>02</th>
<th>03</th>
<th>04</th>
<th>06</th>
<th>07</th>
<th>08</th>
<th>10</th>
<th>12</th>
<th>13</th>
<th>16</th>
<th>17</th>
<th>18</th>
<th>20</th>
<th>21</th>
</tr>
</thead>
<tbody>
<tr>
<td>GMT+8</td>
<td>09</td>
<td>10</td>
<td>11</td>
<td>12</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td>18</td>
<td>20</td>
<td>21</td>
<td>00</td>
<td>01</td>
<td>02</td>
<td>04</td>
<td>05</td>
</tr>
<tr>
<td>Volume</td>
<td>3</td>
<td>1</td>
<td>7</td>
<td>1</td>
<td>2</td>
<td>5</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>GMT</th>
<th>Sun</th>
<th>Mon</th>
<th>Tue</th>
<th>Wed</th>
<th>Thu</th>
<th>Fri</th>
<th>Sat</th>
</tr>
</thead>
<tbody>
<tr>
<td>+0</td>
<td>1</td>
<td>3</td>
<td>8</td>
<td>7</td>
<td>6</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>+8</td>
<td>1</td>
<td>1</td>
<td>9</td>
<td>6</td>
<td>6</td>
<td>7</td>
<td>2</td>
</tr>
</tbody>
</table>
Example Match

Example Match

http://www.cis.edu.ph/about_us/student_profile.html

Cebu International School

IMPORTANT NOTES:

• This is NOT necessarily the only match.
• NO indication that the school is linked to the spammers.
• NO indication that the school was used for the spamming.

Match only suggests that the spammers are likely school age and a 4-day school week in the Philippians is not improbable.
Hang-Outers Summary

• Filipino IRC group
  – World-wide: Philippines, Canada, USA, France
  – Communicates over IRC
    • Augment communications with covert spam
    • Not all members are involved. (Only a few.)
    • Spam: Inactive for over a year

• Demonstrates:
  – Active covert channels in Spam
Conclusion
Not all “Spam” is “Spam”

• Topics covered:
  – How email and Mail headers work
  – Tracking Techniques for Email and Spam
  – Spam Identification & Classification

• Questions?

Dr. Curtis Kret
Secure Science Corporation
http://www.securescience.net/
Acknowledgements

- Members of the Covert Channels in Spam mailing list
- ÅGZØ®Z, aggies hacking aggies
- Members of the Honeynet Project
- Many anonymous individuals