Preface: We All Hate Spam...

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

• This presentation:
  – Describes forensic and profiling techniques applied to spam
  – Methods to classify and track 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: you@company.com
    • FROM: me@company.com

• Blank line (separates sections)

• Content
  – Usually plain text
Mail Forwarding and Delivery

1. Create the mail
   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>;
    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: <NWRMPLKIHGFCQQLYMKLCYJHAZAVFFL@10.0.0.1>
From: "Martin Williams" <thicker@myself.com>
To: nealedwards@webtv.net
X-MS-JQU: BCWXNCDXQN
Date: Tue, 29 Oct 02 06:26:15 Eastern Standard Time
Content-Type: multipart/mixed;
    boundary=WC_MAIL_PaRt_BoUnDaRy_05151998
Subject: New Pill guaranteed 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
<table>
<thead>
<tr>
<th>Date</th>
<th>Sender</th>
<th>(Lines)</th>
<th>Subject</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aug 26</td>
<td><a href="mailto:lloihhg@yahoo.com">lloihhg@yahoo.com</a></td>
<td>(42)</td>
<td>Healthcare you can afford</td>
</tr>
<tr>
<td>Aug 26</td>
<td><a href="mailto:bbssw2@yahoo.com">bbssw2@yahoo.com</a></td>
<td>(131)</td>
<td>Need a good lawyer cheap</td>
</tr>
<tr>
<td>Aug 26</td>
<td><a href="mailto:neverlate21b@l12.n">neverlate21b@l12.n</a></td>
<td>(30)</td>
<td>ADV: Interest rates slashed! Don't wait!</td>
</tr>
<tr>
<td>Aug 27</td>
<td>smesmith7733r40@ho</td>
<td>(50)</td>
<td>Life Insurance Price Wars 120 8369VweC6-598-12</td>
</tr>
<tr>
<td>Aug 27</td>
<td><a href="mailto:momentous@bubfet.com">momentous@bubfet.com</a></td>
<td>(92)</td>
<td>Adv: Generate Wealth on Wall Street</td>
</tr>
<tr>
<td>Aug 26</td>
<td>Julie29593746@post</td>
<td>(109)</td>
<td>Browse Lovely Young Mail Order Brides for FREE (17-29 y/o)</td>
</tr>
<tr>
<td>Aug 27</td>
<td><a href="mailto:mnytzen@bubfet.com">mnytzen@bubfet.com</a></td>
<td>(85)</td>
<td>Adv: Reach Million of Opt-In Customers Now!</td>
</tr>
<tr>
<td>Aug 26</td>
<td><a href="mailto:mmester@bubfet.com">mmester@bubfet.com</a></td>
<td>(108)</td>
<td>Adv:ce Learn how to keep your money on Life Insurance!</td>
</tr>
<tr>
<td>Aug 27</td>
<td>a56772176y45@lycos</td>
<td>(45)</td>
<td>** Your -approval-. **</td>
</tr>
<tr>
<td>Aug 27</td>
<td><a href="mailto:zeroday@idir.net">zeroday@idir.net</a></td>
<td>(187)</td>
<td>Baby Boomers, Get Your Youth Back Now</td>
</tr>
<tr>
<td>Aug 27</td>
<td><a href="mailto:jbroder@netzero.ne">jbroder@netzero.ne</a></td>
<td>(196)</td>
<td>Extended Auto Warranties Here</td>
</tr>
<tr>
<td>Aug 27</td>
<td><a href="mailto:mnetwork@bubfet.co">mnetwork@bubfet.co</a></td>
<td>(148)</td>
<td>Adv: Reduce your term on your mortgage.</td>
</tr>
<tr>
<td>Aug 27</td>
<td><a href="mailto:lurchpa@hotmail.co">lurchpa@hotmail.co</a></td>
<td>(173)</td>
<td>PROTECT YOUR INFORMATION AND YOUR COMPUTER! 8777</td>
</tr>
<tr>
<td>Aug 28</td>
<td><a href="mailto:ccxcfcdxz@yahoo.com">ccxcfcdxz@yahoo.com</a></td>
<td>(34)</td>
<td>Want a Home Improvement Loan</td>
</tr>
<tr>
<td>Aug 28</td>
<td><a href="mailto:ccxcfcdxz@yahoo.com">ccxcfcdxz@yahoo.com</a></td>
<td>(92)</td>
<td>300 percent boost for cellphone QDQLIB</td>
</tr>
<tr>
<td>Aug 28</td>
<td>Christopher_ChaseU</td>
<td>(91)</td>
<td>Money Manager Site c3N33-gHt-jma</td>
</tr>
<tr>
<td>Aug 29</td>
<td>latestnews7205g83@</td>
<td>(50)</td>
<td>We Have a FREE Euro For You!</td>
</tr>
<tr>
<td>Aug 29</td>
<td>kickboxthequeen</td>
<td>(130)</td>
<td>Welcome to my hometown</td>
</tr>
<tr>
<td>Aug 29</td>
<td>Akilah2006w31@yahoo</td>
<td>(65)</td>
<td>The decision is yours 6526EeCu8-485ktQ-15</td>
</tr>
<tr>
<td>Aug 29</td>
<td>Halina7638y28@iris</td>
<td>(52)</td>
<td>You won't believe this! 1368Ugie3-287Rw-14</td>
</tr>
<tr>
<td>Aug 29</td>
<td>Lorene2284f64@mult</td>
<td>(103)</td>
<td>You missed this investment last time, didn't you? 0054qbVf1-834EeqE-16</td>
</tr>
<tr>
<td>Aug 29</td>
<td><a href="mailto:loras@atncorp.com">loras@atncorp.com</a></td>
<td>(299)</td>
<td>NIGHT VISION NZT-1 Just $99!</td>
</tr>
<tr>
<td>Aug 29</td>
<td>Jeremiah</td>
<td>(50)</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:cezazuser@aol.com">cezazuser@aol.com</a></td>
<td>(57)</td>
<td>Make a fortune on eBay - FREE Info</td>
</tr>
<tr>
<td>Aug 29</td>
<td><a href="mailto:bdrake16user@aol.c">bdrake16user@aol.c</a></td>
<td>(56)</td>
<td>Huge Profit on eBay</td>
</tr>
<tr>
<td>Aug 29</td>
<td><a href="mailto:lloihhg@yahoo.com">lloihhg@yahoo.com</a></td>
<td>(48)</td>
<td>Russian Girls Looking for men HHBV</td>
</tr>
<tr>
<td>Aug 29</td>
<td><a href="mailto:bballjac@hotmail.c">bballjac@hotmail.c</a></td>
<td>(173)</td>
<td>Attn: SYSTEMWORKS CLEARANCE SALE ONLY $29.99 ZENRT</td>
</tr>
</tbody>
</table>
Aug 21 ccxaq@yahoo.com    (108)    Copy DVD Movies to CD-R right now!                TO
Aug 22 xxxza22@yahoo.com  (48)   Russian Women seeking Western Men                PC
Aug 22 ttteersw@yahoo.com (91)   Get crystal reception on your cell phone                         LGAT
Aug 23 ttteersw@yahoo.com (65)   FREE HGH -Look Ten Years Younger in 3 Weeks                LUPWMSIMDR
Aug 25 bbkke861@hotmail.c (160)  Fw: PROTECT YOUR COMPUTER,YOU NEED SYSTEMWORKS!               WDKCJW
Aug 25 bbarelka@hotmail.c (164)  NORTON SYSTEMWORKS BLOWOUT!
Aug 26 lloihhg@yahoo.com  (42)   Healthcare you can afford                                 YCZHEBRCXTJN
Aug 26 bbssw2@yahoo.com   (131)  Need a good lawyer cheap                                MTCNDU
Aug 28 ccxcfdxz@yahoo.com (34)   Want a Home Improvement Loan                                P
Aug 28 ccxcfdxz@yahoo.com (92)  300 percent boost for cellphone                       QDQLIB
Aug 29 lloihhg@yahoo.com  (48)   Russian Girls Looking for men                           HHBV
Aug 29 bballjac@hotmail.c (173)  Attn: SYSTEMWORKS CLEARANCE SALE_ONLY $29.99             ZENRT
Aug 30 kjjhh (254)        (170)  Affordable Healthcare for families                    ZR
Aug 30 breaks26@hotmail.c (167)  Fw: DON'T LET A COMPUTER VIRUS RUIN YOUR DAY!                   CEUDG
Aug 31 lloihhg@yahoo.com  (48)   Dont pay to much for cigs                               UKMPC
Aug 31 bbssw2@yahoo.com   (70)   FREE HGH -Look Ten Years Younger in 3 Weeks                       CGU
Sep 01 binder39@hotmail.c (168)  Fw: NORTON SYSTEMWORKS CLEARANCE SALE_ONLY $29.99!              HTHIPNB
Sep 02 lloihhg@yahoo.com  (77)   Magical Laser Keychain                                  NNJODQ
Sep 02 ccxcfdxz@yahoo.com (34)   Save thousands rates are low                          ESLGW
Sep 03 asdw2@well-in.com  (41)   Affordable Healthcare                         FSX
Sep 03 ljhuy (71)        (71)   Discount Viagra                                         G
Sep 03 connie_1_1@hotmail (170)  Fw: PROTECT YOUR COMPUTER AGAINST HARMFUL VIRUSES!              GMKTPIW
Sep 03 zzxdw@festie.com   (91)   Get crystal reception on your cell phone                IZKQLO
Sep 04 bconst3442@hotmail (91)   actually work?                                      "NRWR
Sep 05 alice149@hotmail.com (157)  Re: BE healthy with this BREAKTHROUGH product!            XMUJL
Sep 06 bbabarber612@hotmail (167)  PROTECT YOUR INFORMATION AND YOUR COMPUTER!EZBCYT
Sep 06 vvcxzza@yahoo.com  (71)   FREE HGH -Look Ten Years Younger in 3 Weeks                LZKHF
Cap Letters with TZ “-1600”

Jun 28 daisy5136@hotmail. (137) Do You Use Your Printer Alot?
Jul 04 contactroxy@hotmail (141) Welcome to the Modern Way to Improve your Budget!
Jul 09 cwood83@hotmail.co (100) Make your prints beautiful & SAVE BIG!
Jul 17 dagnyh@hotmail.com (91) Lose 14 Pounds In 10 Days
Jul 28 el86@hotmail.com (229) Re: Men & Women, Spruce up your life!
Jul 30 dafricano@hotmail. (144) Re: Can't Stand the Cost of Ink Cartridges?
Aug 07 bbarff@hotmail.com (63) **Your Free Club membership!**
Aug 07 bcoole2@hotmail.co (94) Lose 80lbs In A Wk? #1 Diet Pill! Wholesale!!
Aug 07 barker6@hotmail.c (94) Lose 19 Pounds In 10 Days
Aug 07 bjorne59@hotmail.c (77) Attn: Want to LOSE Weight FAST?
Aug 09 bbarednek@hotmail. (77) Free Consultation. Buy Viagra Online !
Aug 09 bbarednek@hotmail. (77) Free Consultation. Buy Viagra Online !
Aug 11 breedde@hotmail.co (173) Aren't these things overpriced?
Aug 12 bcook61@hotmail.co (154) Attn: PROTECT YOUR COMPUTER, YOU NEED SYSTEMWORKS!
Aug 20 bblueguyl3@hotmail. (178) Re: Discount Prices + FREE Shipping = #1 Service!
Aug 20 bblueguyl3@hotmail. (178) Re: Discount Prices + FREE Shipping = #1 Service!
Aug 25 bbkke861@hotmail.c (163) FW: PROTECT YOUR COMPUTER, YOU NEED SYSTEMWORKS!
Aug 25 bchicka@hotmail.c (167) NORTON SYSTEMWORKS BLOWOUT!
Aug 29 bbballjac@hotmail.c (176) Attn: SYSTEMWORKS CLEARANCE SALE ONLY $29.99
Aug 30 bbreaks26@hotmail.c (170) FW: DON'T LET A COMPUTER VIRUS RUIN YOUR DAY!
Sep 01 binder39@hotmail.c (171) FW: NORTON SYSTEMWORKS CLEARANCE SALE ONLY $29.99!
Sep 02 connie_1_1@hotmail (173) FW: PROTECT YOUR COMPUTER AGAINST HARMFUL VIRUSES!
Sep 04 bconst3442@hotmail (94) actually work?"NRWR
Sep 05 alice149@hotmail.c (160) Re: BE healthy with this BREAKTHROUGH product!
Sep 06 bchicka@hotmail.c (167) PROTECT YOUR INFORMATION AND YOUR COMPUTER!
Sep 09 corbinjim@hotmail. (174) Attn: This is NO JOKE! Speed up your CPU for under $30!
Sep 09 corbinjim@hotmail. (174) Attn: This is NO JOKE! Speed up your CPU for under $30!
<table>
<thead>
<tr>
<th>Date</th>
<th>Sender Email</th>
<th>(Index)</th>
<th>Message Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nov 26</td>
<td><a href="mailto:vvds21@yahoo.com">vvds21@yahoo.com</a></td>
<td>(85)</td>
<td>Double your life insurance free. LAYKWR</td>
</tr>
<tr>
<td>Nov 27</td>
<td><a href="mailto:wjw3@yahoo.com">wjw3@yahoo.com</a></td>
<td>(107)</td>
<td>FW: MINI RADIO_CONTROLLED CARS ARE SOLD OUT IN STORES H</td>
</tr>
<tr>
<td>Nov 28</td>
<td><a href="mailto:nngtr32@yahoo.com">nngtr32@yahoo.com</a></td>
<td>(45)</td>
<td>Want a Home Improvement Loan ZETLCJYI</td>
</tr>
<tr>
<td>Nov 30</td>
<td><a href="mailto:bcvbcv32@yahoo.com">bcvbcv32@yahoo.com</a></td>
<td>(53)</td>
<td>Want a Home Improvement Loan ZQJAG</td>
</tr>
<tr>
<td>Nov 30</td>
<td><a href="mailto:bcvbcv32@yahoo.com">bcvbcv32@yahoo.com</a></td>
<td>(53)</td>
<td>Refinance today and save thousands JAL</td>
</tr>
<tr>
<td>Dec 01</td>
<td><a href="mailto:vvdsd21@yahoo.com">vvdsd21@yahoo.com</a></td>
<td>(59)</td>
<td>Feeling Small LPMVEDV</td>
</tr>
<tr>
<td>Dec 01</td>
<td><a href="mailto:vbcx21@yahoo.com">vbcx21@yahoo.com</a></td>
<td>(58)</td>
<td>Enlarge your package GTGIL</td>
</tr>
<tr>
<td>Dec 02</td>
<td><a href="mailto:cxxzca12@yahoo.com">cxxzca12@yahoo.com</a></td>
<td>(78)</td>
<td>Look and feel 30 years younger ABCT</td>
</tr>
<tr>
<td>Dec 02</td>
<td><a href="mailto:cxxzca12@yahoo.com">cxxzca12@yahoo.com</a></td>
<td>(78)</td>
<td>Look and feel 30 years younger XRDRAOSVW</td>
</tr>
<tr>
<td>Dec 02</td>
<td><a href="mailto:vvds2122@yahoo.com">vvds2122@yahoo.com</a></td>
<td>(107)</td>
<td>FW: MINI RADIO_CONTROLLED CARS ARE SOLD OUT IN STORES H</td>
</tr>
<tr>
<td>Dec 02</td>
<td><a href="mailto:bcvbcv32@yahoo.com">bcvbcv32@yahoo.com</a></td>
<td>(107)</td>
<td>RE: Remote Controlled Mini Matchbox Cars QNM</td>
</tr>
<tr>
<td>Dec 03</td>
<td><a href="mailto:ccxsd2@yahoo.com">ccxsd2@yahoo.com</a></td>
<td>(100)</td>
<td>Get crystal reception on your cell phone FBPNO</td>
</tr>
<tr>
<td>Dec 03</td>
<td><a href="mailto:opioi78@yahoo.com">opioi78@yahoo.com</a></td>
<td>(101)</td>
<td>Tired of Dropped Cell Calls MS</td>
</tr>
<tr>
<td>Dec 04</td>
<td><a href="mailto:mmjh543@yahoo.com">mmjh543@yahoo.com</a></td>
<td>(46)</td>
<td>Mortgage Rates are going lower UHW</td>
</tr>
<tr>
<td>Dec 04</td>
<td><a href="mailto:yytr453@yahoo.com">yytr453@yahoo.com</a></td>
<td>(46)</td>
<td>Mortgage Rates are going lower</td>
</tr>
<tr>
<td>Dec 04</td>
<td><a href="mailto:qwws3@yahoo.com">qwws3@yahoo.com</a></td>
<td>(108)</td>
<td>FW: Remote Controlled Mini Matchbox Cars CI</td>
</tr>
<tr>
<td>Dec 04</td>
<td><a href="mailto:erww221@yahoo.com">erww221@yahoo.com</a></td>
<td>(107)</td>
<td>HOT New Toy for Christmas 2002! J</td>
</tr>
<tr>
<td>Dec 05</td>
<td><a href="mailto:zxxas21@yahoo.com">zxxas21@yahoo.com</a></td>
<td>(42)</td>
<td>We can save you thousands on life insurance AMKG</td>
</tr>
<tr>
<td>Dec 05</td>
<td><a href="mailto:l1kjy56@yahoo.com">l1kjy56@yahoo.com</a></td>
<td>(41)</td>
<td>Automated Life Insurance quotes JOBQ</td>
</tr>
<tr>
<td>Dec 06</td>
<td><a href="mailto:ppiou66@yahoo.com">ppiou66@yahoo.com</a></td>
<td>(133)</td>
<td>Keep the hackers off your computer JDLIKTMS</td>
</tr>
<tr>
<td>Dec 06</td>
<td><a href="mailto:rrewe2@yahoo.com">rrewe2@yahoo.com</a></td>
<td>(132)</td>
<td>Protect your pc from hackers JQZI</td>
</tr>
<tr>
<td>Dec 06</td>
<td><a href="mailto:ccvds21@yahoo.com">ccvds21@yahoo.com</a></td>
<td>(108)</td>
<td>FW: HOT New Toy for Christmas 2002! HQZGA</td>
</tr>
<tr>
<td>Dec 06</td>
<td><a href="mailto:vdsd221@yahoo.com">vdsd221@yahoo.com</a></td>
<td>(108)</td>
<td>FW: HOT New Toy for Christmas 2002! KEDMIXBV</td>
</tr>
<tr>
<td>Dec 07</td>
<td><a href="mailto:ggd2a@yahoo.com">ggd2a@yahoo.com</a></td>
<td>(83)</td>
<td>Want to look younger IAT</td>
</tr>
<tr>
<td>Dec 07</td>
<td><a href="mailto:minir221@yahoo.com">minir221@yahoo.com</a></td>
<td>(83)</td>
<td>Need to be revitalized VC</td>
</tr>
<tr>
<td>Dec 07</td>
<td><a href="mailto:kkjhg65@yahoo.com">kkjhg65@yahoo.com</a></td>
<td>(101)</td>
<td>Boost your cell phone reception KP</td>
</tr>
<tr>
<td>Dec 07</td>
<td><a href="mailto:ttyrew21@yahoo.com">ttyrew21@yahoo.com</a></td>
<td>(101)</td>
<td>Get better reception on your cell phone SBCZFIHRN</td>
</tr>
</tbody>
</table>
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

Received: from power1.anything3d.com ([207.224.122.65]) by server.company.com (InterMail vM.4.01.03.27 201-229-121-127-20010626) with ESMTP id

<20020704025350.VHVJ11685.server.company.com@power1.anything3d.com>
for <TEST@SECURESCIENCE.NET>; Thu, 4 Jul 2002 02:53:50 +0000
Received: (from httpd@localhost)
    by power1.anything3d.com (8.11.4/8.11.4) id g642fd412182;
Date: Wed, 3 Jul 2002 19:53:39 -0700
Message-Id: <20020704025350.g642fd412182@power1.anything3d.com>
To: <TEST@SECURESCIENCE.NET>
Subject: SMART CLOCK Just $29.95!
From: loras@atncorp.com

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, 650-872-1276, FAX 650-875-0129

Copyright © 2004 Secure Science Corp.
UCE Example

Received: from guinness.cosaint.net (HELO cosaint.net) ([216.57.201.99])
  (envelope-sender <realname@cosaint.net>)
  by smtp-1-2b.secureserver.net (qmail-ldap-1.03) with SMTP
  for <web@securescience.com>; 25 Jan 2004 23:27:53 -0000
Received: by cosaint.net (CommuniGate Pro PIPE 4.1.5)
  with PIPE id 950413; Sun, 25 Jan 2004 15:23:52 -0800
To: web@securescience.com
Subject: HIPAA Security for Healthcare Staff - A New Course from Cosaint
From: realname@cosaint.net
Reply-To: realname@cosaint.net
Date: Sun, 25 Jan 2004 15:23:52 -0800
Message-ID: <auto-000000950411@cosaint.net>

To: Curtis Kret
...
<br real person name>
Business Development
Cosaint Inc.
T: 206 547 xxxx
C: 206 300 xxxx
mailto:realname@cosaint.net
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
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.
More Comcast

From: "Comcast Online Communications" <online.communications@comcast.net>
Subject: Important Information from Comcast High-Speed Internet about your Webmail
Date: Wed, 3 Mar 2004 06:24:27 -0700

Check out your new webmail at Comcast.net

On March 4th Comcast High-Speed Internet will launch its new and improved webmail.

Comcast High-Speed Internet customers like you have asked for some changes to their e-mail & and we've listened. Here is your sneak peek at just some of the improvements your e-mail is about to undergo.

You'll like our new look. You'll love our new features.

Starting soon your e-mail will not only look better, it will also feature improved navigation, easier use of attachments and sharper graphics with more enhancements planned for the coming months. And, to start using your new webmail there's nothing you need to do. Your stored e-mails and address book will automatically be transferred.

Be sure to check us out at www.comcast.net on March 4, 2004 and sign in when we unveil our great new look and all the features you've been waiting for.

THIS E-MAIL IS SERVICE RELATED.

Remember that Comcast will never ask for your password or billing information via e-mail.
Other NCE Companies

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

• If you don’t subscribe, you won’t get NCE
Non-Commercial Categories

The vast majority of Spam
3. List Makers

• Purpose
  – Make money by gathering & selling addresses
  – Manage lists for others
  – 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”!
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 autoresponders, 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
Not all lists are obvious...

Burglars target ‘out of office’ emails

Andy McCue, 04-12-2002

Thieves are using information contained in “out of office” auto-reply emails and cross-referencing it with publicly available personal information to target empty houses.

The warning comes from UK blue chip user group The Infrastructure Forum (Tif), which uncovered details of the scam from a meeting of its members.

Criminals are buying huge lists of email addresses over the internet and sending mass-mailings in the hope of receiving “out of office” auto-responses from workers away on holiday.

By cross-reference such replies with publicly available information from online directories such as 192.com or bt.com, the burglars can often discover the name, address and telephone number of the person on holiday.

Tif is advising users to warn their staff to be careful of the information they put in their “out of office” messages.

“You wouldn’t go on holiday with a note pinned to your door saying who you were, how long you were away for and when you were coming back, so why would you put this in an email?” said David Roberts, chief executive at Tif.

“Email is the most popular form of office communication but many people forget that the information contained in these messages can get into the wrong hands,” he added.
List Makers: Identification

• Common identification methods
  – Forged headers
  – Valid “From” & “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
  – Huge address lists ( “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)
Scam Example: Pro-Hosiery

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/?3X6CMW2IzupOVQW

---------------------------------------------

Thank you for using Citibank!

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

sign on to Citibank
with your Citibank® Banking Card

Card #/CIN

PIN

sign on

Thank you.

Your E-Mail Address Was Successful Verified.
## Russian Web Bug

### Detailed Statistics of IP Address Visits

<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></td>
</tr>
<tr>
<td>12.08.2003</td>
<td></td>
</tr>
<tr>
<td>13.08.2003</td>
<td></td>
</tr>
<tr>
<td>14.08.2003</td>
<td></td>
</tr>
<tr>
<td>15.08.2003</td>
<td></td>
</tr>
<tr>
<td>16.08.2003</td>
<td></td>
</tr>
<tr>
<td>17.08.2003</td>
<td></td>
</tr>
<tr>
<td>18.08.2003</td>
<td></td>
</tr>
<tr>
<td>19.08.2003</td>
<td></td>
</tr>
<tr>
<td>20.08.2003</td>
<td></td>
</tr>
</tbody>
</table>

### Summary Statistics of IP Address Visitors

<table>
<thead>
<tr>
<th>No</th>
<th>Адрес</th>
<th>Кол-во</th>
<th>Среднее в день</th>
<th>Процент в группе</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>68.82.62.191 [whois]</td>
<td>8</td>
<td>1</td>
<td>80.00%</td>
</tr>
<tr>
<td>2</td>
<td>12.5.1.207 [whois]</td>
<td>1</td>
<td>0.12</td>
<td>10.00%</td>
</tr>
<tr>
<td>3</td>
<td>208.141.219.205 [whois]</td>
<td>1</td>
<td>0.12</td>
<td>10.00%</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
    <test@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:0JJ9H7JGA03E18A7I@att.net">0JJ9H7JGA03E18A7I@att.net</a></td>
<td>Rich, Hello! My name is John Turner....</td>
</tr>
<tr>
<td>07 Jul 2003 07:43:51</td>
<td><a href="mailto:2EF98ADD2HG3CJ54@att.net">2EF98ADD2HG3CJ54@att.net</a></td>
<td>Dear Rich! I've been scammed over...</td>
</tr>
<tr>
<td>17 Jul 2003 10:46:08</td>
<td><a href="mailto:76E7A5HFIJHK63C@e-loan.com">76E7A5HFIJHK63C@e-loan.com</a></td>
<td>Rich, Any software just for 15$ - 40$</td>
</tr>
<tr>
<td>22 Jul 2003 01:21:52</td>
<td><a href="mailto:77EGJ4AGC1F3AIB5@wellsfargo.com">77EGJ4AGC1F3AIB5@wellsfargo.com</a></td>
<td>[Ftpserver] Re: Your E-Loan Refinance..</td>
</tr>
<tr>
<td>26 Jul 2003 09:43:59</td>
<td><a href="mailto:JFHAL1CJIB78IFA8@security.org">JFHAL1CJIB78IFA8@security.org</a></td>
<td>Re: Your E-Loan Refinance Application..</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>Re: Wells Fargo Bank New Business...</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>Newsletter</td>
</tr>
<tr>
<td>30 Jul 2003 19:03:38</td>
<td><a href="mailto:3FHG03G0I213JJ92@yahoo.com">3FHG03G0I213JJ92@yahoo.com</a></td>
<td>The Great E-Gold Giveaway!</td>
</tr>
<tr>
<td>31 Jul 2003 05:26:44</td>
<td><a href="mailto:BG5L3CAI6J586EK0@headgear.org">BG5L3CAI6J586EK0@headgear.org</a></td>
<td>Rich, software for you</td>
</tr>
<tr>
<td>02 Aug 2003 10:21:12</td>
<td><a href="mailto:J9D9GK1H1I1J47920@hotmail.com">J9D9GK1H1I1J47920@hotmail.com</a></td>
<td>I want to introduce Stock Cruiser</td>
</tr>
<tr>
<td>09 Aug 2003 11:59:24</td>
<td><a href="mailto:50LJ6D9B4EK320HDl@annexia.org">50LJ6D9B4EK320HDl@annexia.org</a></td>
<td>new mail p1QwvfpX</td>
</tr>
<tr>
<td>17 Aug 2003 07:58:36</td>
<td><a href="mailto:2J73600018ECI75J@virtualitas.net">2J73600018ECI75J@virtualitas.net</a></td>
<td>Rich, Want sex &lt;rndmx&gt;</td>
</tr>
</tbody>
</table>
| 17 Aug 2003 17:49:39   | FBE6962ED2FJFK58@hotmail.com | ^\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř\š\ř
| 20 Aug 2003 17:49:39   | 77EGJ4AGC1F3AIB5@wellsfargo.com | The Great E-Gold Giveaway! |
| 20 Aug 2003 19:37:45   | J9D9GK1H1I1J47920@hotmail.com | Rich, software for you |
| 20 Aug 2003 19:37:45   | 77EGJ4AGC1F3AIB5@wellsfargo.com | I want to introduce Stock Cruiser |
| 26 Aug 2003 09:43:59   | 50LJ6D9B4EK320HDl@annexia.org | new mail p1QwvfpX |
| 26 Aug 2003 23:00:46   | JFHAL1CJIB78IFA8@security.org | Rich, Want sex <rndmx> |

---

Copyright 2004 Secure Science Corp.
# 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:0JJ9H7JGA03E18A7I@att.net">0JJ9H7JGA03E18A7I@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:76E7A5HFIJHK63C@e-loan.com">76E7A5HFIJHK63C@e-loan.com</a></td>
<td>[Ftpsver] 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 Applicatio..</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:JFHAL1CJIB78IFA8@security.org">JFHAL1CJIB78IFA8@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:3FHG03G01213JJ92@yahoo.com">3FHG03G01213JJ92@yahoo.com</a></td>
<td>new mail p1QwvfpX</td>
</tr>
<tr>
<td>31 Jul 2003 05:26:44</td>
<td><a href="mailto:BG5L3CAI6J586EK0@headgear.org">BG5L3CAI6J586EK0@headgear.org</a></td>
<td>Rich,Want sex &lt;rndmx&gt;</td>
</tr>
<tr>
<td>02 Aug 2003 10:21:12</td>
<td><a href="mailto:J9D9GK1H11J47920@hotmail.com">J9D9GK1H11J47920@hotmail.com</a></td>
<td></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:0JJ9H7JGA03E18A7I@att.net">0JJ9H7JGA03E18A7I@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:D4C174IDH3FKH13D@att.net">D4C174IDH3FKH13D@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:2EF98ADD2HG3JC54@att.net">2EF98ADD2HG3JC54@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:76E7A5HFIJ1HK63C@e-loan.com">76E7A5HFIJ1HK63C@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:77EGJ4AGC1F3AI5B5@wellsfargo.com">77EGJ4AGC1F3AI5B5@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:JFHAL1CJIB78IDA8@security.org">JFHAL1CJIB78IDA8@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:4K63GFHE8FJ1IK7@utp.edu.co">4K63GFHE8FJ1IK7@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:3FHG03G01213JJ92@yahoo.com">3FHG03G01213JJ92@yahoo.com</a></td>
<td>new mail p1QwvfpX</td>
</tr>
<tr>
<td>31 Jul 2003 05:26:44</td>
<td><a href="mailto:BG5L3CAI6J586E0@headgear.org">BG5L3CAI6J586E0@headgear.org</a></td>
<td>Rich, Want sex &lt;rndmx&gt;</td>
</tr>
<tr>
<td>02 Aug 2003 10:21:12</td>
<td><a href="mailto:J9D9GK1H11J47920@hotmail.com">J9D9GK1H11J47920@hotmail.com</a></td>
<td></td>
</tr>
<tr>
<td>09 Aug 2003 11:59:24</td>
<td><a href="mailto:50LJ6D9B4EK320HD@annexia.org">50LJ6D9B4EK320HD@annexia.org</a></td>
<td></td>
</tr>
<tr>
<td>17 Aug 2003 07:58:36</td>
<td><a href="mailto:2J73600018EC175J@virtualitas.net">2J73600018EC175J@virtualitas.net</a></td>
<td></td>
</tr>
<tr>
<td>17 Aug 2003 17:49:39</td>
<td><a href="mailto:FBE6962ED2FJFK58@hotmail.com">FBE6962ED2FJFK58@hotmail.com</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td><a href="mailto:A60I9A7D090LE51L@cbshost-08-111-42-31.sbcx.net">A60I9A7D090LE51L@cbshost-08-111-42-31.sbcx.net</a></td>
<td></td>
</tr>
<tr>
<td>Great Spam Archive Date</td>
<td>Message-ID</td>
<td>Subject</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------</td>
<td>---------</td>
</tr>
<tr>
<td>24 Apr 2003 13:01:55</td>
<td><a href="mailto:0JJ9H7JGA03EJ8A7I@att.net">0JJ9H7JGA03EJ8A7I@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:76E7A5HFIJ1HK63C@e-loan.com">76E7A5HFIJ1HK63C@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:JFHAL1CJIB78IFA8@security.org">JFHAL1CJIB78IFA8@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 p1QwvfpX</td>
</tr>
<tr>
<td>31 Jul 2003 05:26:44</td>
<td><a href="mailto:BG5L3CAI6J586EK0@headgear.org">BG5L3CAI6J586EK0@headgear.org</a></td>
<td>Rich, Want sex &lt;rndmx&gt;</td>
</tr>
<tr>
<td>02 Aug 2003 10:21:12</td>
<td><a href="mailto:J9D9GK1H11J47920@hotmail.com">J9D9GK1H11J47920@hotmail.com</a></td>
<td></td>
</tr>
<tr>
<td>09 Aug 2003 11:59:24</td>
<td><a href="mailto:50LJ6D9B4EK320HD@annexia.org">50LJ6D9B4EK320HD@annexia.org</a></td>
<td></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 e4AXA1vl8</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></td>
<td><a href="mailto:A60I9A7D890IE01L@cbshost-us-111-42-31.sbcox.net">A60I9A7D890IE01L@cbshost-us-111-42-31.sbcox.net</a></td>
<td>Re: mail 3CPVQpsE</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>Targeted Financial Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>17-Jul-2003</td>
<td>E-Loan: M</td>
</tr>
<tr>
<td>21-Jul-2003</td>
<td>E-Gold: M, M</td>
</tr>
<tr>
<td>26-Jul-2003</td>
<td>X</td>
</tr>
<tr>
<td>16-Aug-2003</td>
<td>X</td>
</tr>
<tr>
<td>3-Sep-2003</td>
<td>X</td>
</tr>
<tr>
<td>17-Sep-2003</td>
<td>X</td>
</tr>
<tr>
<td>19-Sep-2003</td>
<td>X</td>
</tr>
<tr>
<td>23-Sep-2003</td>
<td>X</td>
</tr>
<tr>
<td>25-Sep-2003</td>
<td>X</td>
</tr>
<tr>
<td>28-Sep-2003</td>
<td>X</td>
</tr>
<tr>
<td>30-Sep-2003</td>
<td>X</td>
</tr>
<tr>
<td>2-Oct-2003</td>
<td>X</td>
</tr>
<tr>
<td>4-Oct-2003</td>
<td>X</td>
</tr>
<tr>
<td>5-Oct-2003</td>
<td>X</td>
</tr>
<tr>
<td>9-Oct-2003</td>
<td>X</td>
</tr>
<tr>
<td>18-Oct-2003</td>
<td>X</td>
</tr>
<tr>
<td>20-Oct-2003</td>
<td>X</td>
</tr>
<tr>
<td>21-Oct-2003</td>
<td>X</td>
</tr>
<tr>
<td>25-Oct-2003</td>
<td>X</td>
</tr>
<tr>
<td>26-Oct-2003</td>
<td>X</td>
</tr>
<tr>
<td>27-Oct-2003</td>
<td>X</td>
</tr>
<tr>
<td>9-Nov-2003</td>
<td>X</td>
</tr>
<tr>
<td>13-Nov-2003</td>
<td>X</td>
</tr>
<tr>
<td>15-Nov-2003</td>
<td>X</td>
</tr>
<tr>
<td>20-Nov-2003</td>
<td>X</td>
</tr>
<tr>
<td>22-Nov-2003</td>
<td>X</td>
</tr>
<tr>
<td>26-Nov-2003</td>
<td>X</td>
</tr>
</tbody>
</table>

*M*: Use of email with a hostile/malware attachment.
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) & 419
    • 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 Channel: 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” (web-bug)
Covert Message: Example

Return-Path: <jbCarisa_Gov8972@hotmail.com>
Received: from [211.251.155.129] ([211.242.88.140]) by server.company.com
   (InterMail vM.4.01.03.27 201-229-121-127-20010626) with SMTP
   id <20020526233820.LYAK17701.server.company.com@[211.251.155.129]>
   for <test@securescience.net>; Sun, 26 May 2002 23:38:20 +0000
Received: from ssymail.ssy.co.kr ([115.212.44.160]) by hd.regsoft.net with asmtp; May, 26
   2002 6:38:29 PM +0300
Received: from [137.155.98.192] by f64.law4.hotmail.com with QMQP; May, 26 2002 5:17:17 PM
   +0700
Received: from unknown (124.215.35.163) by rly-xw01.mx.aol.com with QMQP; May, 26 2002
   4:19:07 PM -0700
Received: from unknown (134.164.251.44) by mail.gmx.net with asmtp; May, 26 2002 3:40:15
   PM -0800
From: qojeCarisa <jbCarisa_Gov8972@hotmail.com>
To: test@securescience.net
Subject: Government Grants And Loansááááááááááááá wpo
Sender: qojeCarisa <jbCarisa_Gov8972@hotmail.com>
Date: Sun, 26 May 2002 18:41:37 -0400
X-Mailer: Microsoft Outlook Build 10.0.2627
Message-Id: <20020526233820.LYAK17701.server.company.com@[211.251.155.129]>
Case study: Hang-Outers

lee7 gR00P
(Elite Group)
The Header

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
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 (evnt.which == 3) { alert("Not enough system memory to display source."); return false; } } }
document.onmousedown = noRightClick;
</SCRIPT>
```

[gvjrFov-ka1AsHb3-oOGlgZSseoUJF]

[gvjr Fov - ka1AsH b3 - oO G I gZSseo UJF]
[Governor of - class B - oh gee I guess UJF]
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>Anfernee</td>
<td></td>
</tr>
<tr>
<td>angelface</td>
<td></td>
</tr>
<tr>
<td>beetlebum</td>
<td><a href="mailto:skidrow_gal@mailcity.com">skidrow_gal@mailcity.com</a></td>
</tr>
<tr>
<td>CyBeRSaD*</td>
<td><a href="mailto:cybersa04@yahoo.com">cybersa04@yahoo.com</a></td>
</tr>
<tr>
<td>Czarena*</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_SpOoKy*</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 HUC: 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)
unixs1-g1.chinadns.com
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 <200207020322202.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!       LblBrLeElE
Importance: Normal
Date: Tue, 2 Jul 2002 03:22:10 +0000

...
Sabrina To Cy...
HOME BASED POSITIONS:

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

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

Copyright 2004 Secure Science Corp.
Example Match

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 Philippines 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
Not all are kids...

News Analysis

21 January, 2004

US intelligence links 419s to terrorist attacks

Wayne Madsen

US intelligence sources have linked the ubiquitous Internet financial fraud spam emails, known as Advance Fee Fraud 419 (AFF 419) messages, to coded communications by terrorist groups and international organized crime syndicates.

According to the sources, who spoke on the condition of anonymity, the 419s have been used to clandestinely plan a number of terrorist actions, especially in Africa.

419 is the number of the section in the Nigerian penal code outlawing financial fraud. The coded transmissions are often found in sentences dealing with the assassinations of or coups d’etat against former African heads of state.

According to US intelligence, such messages have contained actual planning information for three actual events in West Africa: the March 2003 assassination in Abidjan of the Saudi ambassador to the Ivory Coast, the killing of former Ivory Coast leader Robert Guei in September 2002, and an attempted Ivory Coast coup in January 2001 that resulted in a number of deaths.
Case Study: Abuse-Tracking

“potential covert channel”
Abuse-Tracking

- Email
- Header analysis
- Contents analysis
  - Reuse
  - Sequences
Not interested in a loan? <A href="http://z9813817h83ld@www.healthproductsnow.net/human/index.php?id=720&0667a=1qv9">Click here for information on our HGH Enhancer!</A>
No Message-Id!
Base64(Base64)

- Encoded destination address
ZEdWemRFQnpaV04xY21WelkybGxibU5sTG01bGRB

Base64-decode:
dGVzdEBzZWN1cmVzY2llbmNlLm5ldA

Base64-decode: test@securescience.net
Contents

Not interested in a loan? <A href="http://z9813817h83ld@www.healthproductsnow.net/human/index.php?id=720&0667a=1qv9">Click here for information on our HGH Enhancer!</A>
Not interested in a loan? Click here for information on our HGH Enhancer!

To be removed from our mailing list Click Here

Copyright 2004 Secure Science Corp.
Content Reuse

- Daniel Ivans
  - healthproductsnow.net
  - Vary topics
  - No long hash-busters
  - Change IDs
    - List Maker
- mort888.com
greatssn3.com
  - China, List Makers

- These emails...
  - No content variety
  - Long hash-busters
  - Same IDs
  http://www.healthproductsnow.net/human/index.php?id=720
Same Contents, Different Strings

<br><img src="http://f2xczg5mk87v5@images.healthproductsnow.net/t.php?i=dGVzdEBzZWN1cmVzY2llbmN1Lm5ldA&z98138=17h831"><br><A HREF="http://d0667a1qv93b2fx@greatssn3.com/4/index.asp?RefID=396552&3ed790014=6i4cs6gw1192">b3156j405296ppi203r3921n</A><br><IMG SRC="http://5s09q4j2m3589v@mort888.com/pic_morta/1.gif?7o6t00442=t3y512604"
border="0"><br>Not interested in a loan? <A href="http://z9813817h83ld@www.healthproductsnow.net/human/index.php?id=720&0667a=1qv9">Click here for information on our HGH Enhancer!</A><br><br>To be removed from our mailing list <A HREF="http://904d25z0415j76@greatssn3.com/auto/index.htm?hg0013ju13=sf6j2z5r">Click Here</A>
Contents: Sequence Overlay

Click here for information on our HGH Enhancer!
Just the hash-busters

3921n5s09q4j2m3589v7o6t00442t3y512604851932u5474
f2xczg5mk87v5
z98138 17h831
d0667a1qv93b2fx
3ed790014 6i4csg6w1192
b3156j405296ppi203r3921n
5s09q4j2m3589v
7o6t00442 t3y512604
851932u5474f2xczg5mk87v5
z9813817h831d
0667a 1qv9
84x501ts1lpqu7b6449vd0tt m6q7v9068r9w3c886wq2823z
17994m65xx777in9g428pn76
y930856a44k97o11904d25z0 415j76hg0013ju13sf6j2z5r
a2e4580n84x501ts1lpqu7b6 449vd0ttm6q7v9068r9w3c88
6wq2823z17994m65xx777in9 g428pn76y930856a44k97o11
904d25z0415j76
hg0013ju13 sf6j2z5r
a2e4580n84x501ts1lpqu7b6
Repeated codes: 128 Bytes

3921n5s09q4j2m3589v7o6t00442t3y512604851932u5474f2xczg5mk87v5z9813817h831d0667a1qv93b2fx3ed7900146i4csg6w1192b3156j405296ppi203r

3921n5s09q4j2m3589v7o6t00442t3y512604851932u5474f2xczg5mk87v5z9813817h831d0667a1qv9

84x501tsllpqu7b6449vd0ttm6q7v9068r9w3c886wq2823z17994m65xx777in9g428pn76y930856a44k97o11904d25z0415j76hg0013ju13sf6j2z5ra2e4580n

84x501tsllpqu7b6449vd0ttm6q7v9068r9w3c886wq2823z17994m65xx777in9g428pn76y930856a44k97o11904d25z0415j76hg0013ju13sf6j2z5ra2e4580n

84x501tsllpqu7b6
Repeated Sequences

- Some emails contain 1 sequence
  - Repeated multiple times
- Many emails contain 2 sequences
  - Each repeated at least in part
  - No interlacing
Are they “random”?

• Characters: a-z, 0-9
  – Numbers always more frequent than letters
    • Each number = 5% to 10%
    • Each letter = 0.7% to 3%

• Phi-test $\Delta IC$
  – Index of Coincidence (IC) measures repeats
  – Random: $\Delta IC = 1.00$
  – English text: $\Delta IC = 1.50$ to 2.00
    • Centered at 1.73
Not random...

$\Delta I_C = 1.53$

$\Delta I_C = 1.38$

Consistently between 1.35 and 2.00
Duplicates?

#10 (20 Jul 2003)

5o16c0c63596748dgb337xz20iws58t257q731n9y7kg25h4s3e379bvl
u956168f77b4wyj0i642854444y123866218r1e408m26753565ve5311
4ao3326112i32p

#10 Rotated

54444y123866218r1e408m26753565ve53114ao3326112i32p5o16c0c
63596748dgb337xz20iws58t257q731n9y7kg25h4s3e379bvlu956168
f77b4wyj0i6428
Duplicates? Yes!

#10 (20 Jul 2003)
5o16c0c63596748dgb337xz20iws58t257q73ln9y7kg25h4s3e379bvlu956168f77b4wyj0i642854444y123866218r1e408m26753565ve53114ao3326112i32p

#10 Rotated
54444y123866218r1e408m26753565ve53114ao3326112i32p5o16c0c63596748dgb337xz20iws58t257q73ln9y7kg25h4s3e379bvlu956168f77b4wyj0i6428

#07 (17 Jul 2003)
54444z123867218r1e408m26753565vf53114ap3427212j32p5o16c0c63506748dgc437xz20jwt58t257q73ln9y7kg25h4s3e370bwmu986168g77b4wzj0i6524
Duplicates!

- #07 and #10
  - 83.59% match (21 characters different)
  - 19 of 21 characters are decrements
    - E.g., 9→8, c→b
- #03 (15 Jul 2003), #05 (16 Jul), #13 (22 Jul)
  #03,#05 = 52%  #03,#13 = 55%  #05,#13 = 35%

- All duplicates are from the 1st 128-byte sequence
Rapid Changes

Received: from attbi.com (aclermont-ferrand-102-1-1-66.w217-128.abo.wanadoo.fr[217.128.109.66])
    by rwcrmxc12.comcast.net (rwcrmxc12) with SMTP
    id <20030808153204r1200e59e1e>; Fri, 8 Aug 2003 15:32:05 +0000
Received: from Filipe [217.128.109.66] by attbi.com with MailMXPro2
    (2195.5658);
    ven., 08 août 2003 17:31:15 +0200
Message-ID: <082a01c35dc2$2092cca4$b400a8c0@Filipe>
From: "hott lips" <4test@aol.com>
To: <test@securescience.net>
Subject: Get total protection now...
Date: ven., 08 août 2003 17:31:15 +0200
MIME-Version: 1.0
Content-Type: multipart/alternative;
    boundary="-----_NextPart_7DF_E68E0521.D3C938A7"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: mxMAILPro 1.0
Return-Path: 4test@aol.com
Abuse2-Tracking: <dGVzdEBzZWN1cmVzY2llbmNlLm5ldA>

Copyright 2004 Secure Science Corp.
And more changes...

<table>
<thead>
<tr>
<th>Date</th>
<th>Observed Base64 ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>8-Aug-2003</td>
<td>Abuse2-Tracking</td>
</tr>
<tr>
<td>17-Oct-2003</td>
<td>ABC-Tracking</td>
</tr>
<tr>
<td>29-Oct-2003</td>
<td>Nex-Tracking</td>
</tr>
<tr>
<td>4-Nov-2003</td>
<td>Kel-Tracking</td>
</tr>
<tr>
<td>8-Nov-2003</td>
<td>Bel-Tracking</td>
</tr>
<tr>
<td>12-Nov-2003</td>
<td>Hel-Tracking</td>
</tr>
<tr>
<td>3-Dec-2003</td>
<td>X-Killa</td>
</tr>
<tr>
<td>3-Dec-2003</td>
<td>X-Kip</td>
</tr>
<tr>
<td>13-Dec-2003</td>
<td>X-Ki</td>
</tr>
</tbody>
</table>
Even Content Changes!

The money was subsidized to nothing when I made up a stupid sentence? I bridled Amber and made her obey me? 3G5p0PO9NCi3n8h9De5961069X46i0346PEk663j24A3

I bridled Amber and made her obey me?

We do the work for you. By submitting your information across to hundreds of Lenders, we can get you the best interest rates around. I bridled Amber and made her obey me?

Interest rates are lower than they have been in over 40 years, but it won't stay that way for long. Our simple form only takes a few moments, there is absolutely NO OBLIGATION, and it's 100% FREE. You have nothing to lose, and everything to gain?

Get a free mortgage quote today!

to be taken off our list, <a href="http://www.geniuseewxc.com/mout/">unsubscribe</a>.
Steganography or Spam?

Spam tool with bad random generator
- Non-standard headers
- Repeated sequences with minor variation days apart

Covert message with unknown encoding
- Content reuse
- Non-standard headers
- Non-random sequences in header and content
- Sequence duplication
  - ID, reply, or resend
  - Or key exchange
- Probable multiple individuals
Abuse-Tracking Summary

• “Interesting” spam group
  – Potential covert channel
    • Reuses content
    • Includes non-random repeated sequences
    • Multiple members
    • Rotates software rapidly
  – Still active today!
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

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