

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

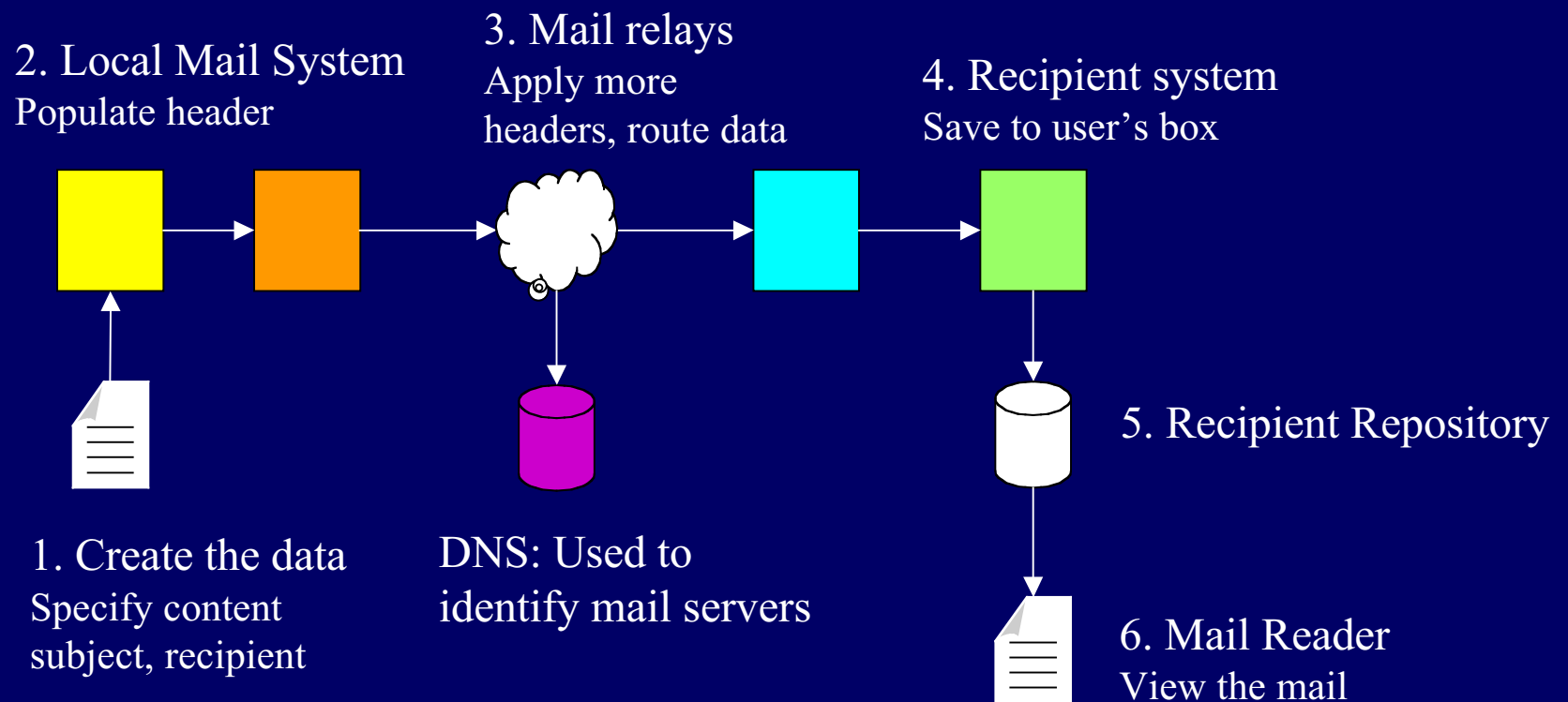
How Email Works

(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



Mail Format and Delivery

Received: from mail.company.com ([10.8.17.2]) by exchange.company.com with SMTP (Microsoft Exchange Internet Mail Service Version 5.5.2653.13) id J2DWGL96; Mon, 22 Apr 2002 16:50:39 -0400

Received: from safard.company.com (safard.company.com [10.2.23.20]) by mail.company.com (Postfix) with ESMTP id B54F2E00612; Mon, 22 Apr 2002 13:50:38 -0700 (PDT)

Received: (from bob@localhost) by safard.company.com (8.8.6 (PHNE_17135)/8.7.3 SMKit7.1.1 hp hp) id OAA10071 for ecom; Mon, 22 Apr 2002 14:48:46 -0600 (MDT)

From: Bob <bob@company.com>

Message-Id: <200204222048.OAA10071@safard.company.com>

Subject: PURCHASE repair

To: ecom@safard.company.com

Date: Mon, 22 Apr 2002 14:48:46 MDT

X-Mailer: Elm [revision: 212.4]

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

Non-standard Email

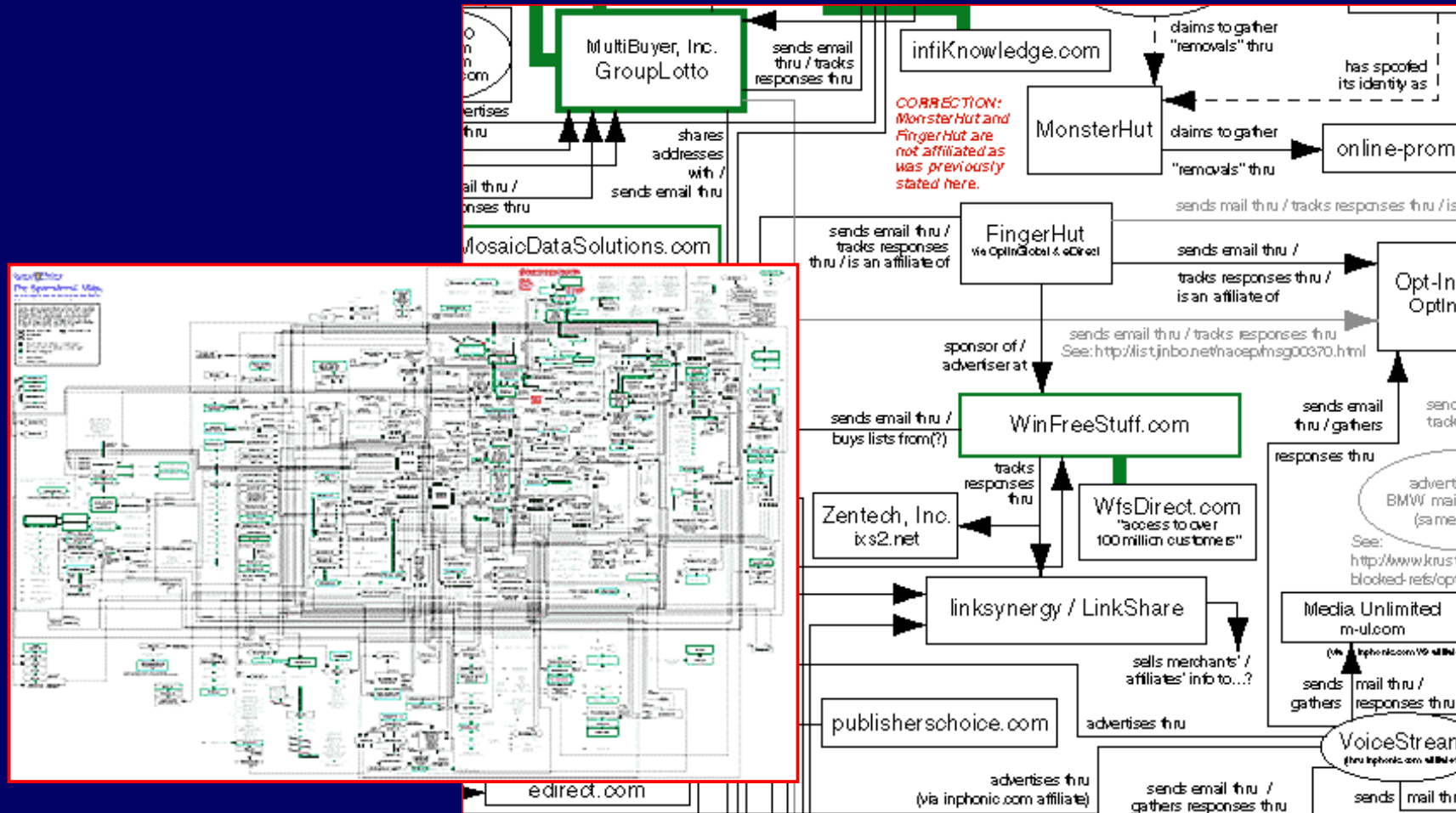
Return-Path: <thicker@myself.com>
Received: from FUSMTA02-LRS ([62.172.195.247]) by server.company.com
(InterMail vM.4.01.03.37 201-229-121-137-20020806) with ESMT
id <20021029142748.LLMT1493.server.company.com@FUSMTA02-LRS>
for <neil@company.com>; Tue, 29 Oct 2002 14:27:48 +0000
Received: from [217.39.203.112] (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: <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 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)

Date	Sender	(Lines)	Subject		
Aug 29	* lloihhg@yahoo.com	(49)	Russian Girls Looking for men	HHBV	
Aug 29	* Lorene2284f64@mult	(104)	You missed this investment last time, didn't you?	0054qbVf1-834EQnE-16	
Aug 29	* latestnews7205g83@	(51)	We Have a FREE Euro For You!		
Aug 29	* bdrake16user@aol.c	(57)	Huge Profit on eBay	16184	
Aug 29	* bballjac@hotmail.c	(174)	Attn: SYSTEMWORKS CLEARANCE SALE_ONLY \$29.99	ZENRT	
Aug 29	* Mason	(49)	Spend More Time With Your Kids! Work at Home & Make Great Money!		19249
Aug 29	* cezazuser@aol.com	(58)	Make a fortune on eBay - FREE Info	19530	
Aug 29	* Jeremiah	(51)	Spend More Time With Your Kids! Work at Home & Make Great Money!		20884
Aug 29	* loras@atncorp.com	(300)	NIGHT VISION NZT-1 Just \$99!		
Aug 28	* ccxcfdxz@yahoo.com	(93)	300 percent boost for cellphone	QDQLIB	
Aug 28	* ccxcfdxz@yahoo.com	(35)	Want a Home Improvement Loan	P	
Aug 29	* Halina7638y28@iris	(53)	You won't believe this! 1368Ugie3-287Rw-14		
Aug 29	* kickboxthequeen	(1931)	Welcome to my hometown		
Aug 29	* Akilah2006w31@yaho	(66)	The decision is yours 6526EeCu8-485ktQ-15		
Aug 28	* Christopher_ChaseU	(92)	Money Manager Site	c3N33-gHt-jma	
Aug 27	* lurchpa@hotmail.co	(174)	PROTECT YOUR INFORMATION AND YOUR COMPUTER!		8777
Aug 27	* mnetwork@bubfet.co	(149)	Adv: Reduce your term on your mortgage.		
Aug 27	* a56772176y45@lycos	(46)	** Your -approval-, **		
Aug 27	* jbroder@netzero.ne	(197)	Extended Auto Warranties Here		
Aug 27	* zeroday@idir.net	(188)	Baby Boomers, Get Your Youth Back Now		
Aug 26	* a10in983118x05@lyc	(42)	* * Your -approval-! * *		
Aug 26	* bbssw2@yahoo.com	(132)	Need a good lawyer cheap	MTCNDU	
Aug 27	* mnytzen@bubfet.com	(86)	Adv: Reach Million of Opt-In Customers Now!		
Aug 27	* momentous@bubfet.c	(93)	Adv: Generate Wealth on Wall Street		
Aug 26	* Julie29593746@post	(110)	Browse Lovely Young Mail Order Brides for FREE (17-29 y/o)		
Aug 26	* lloihhg@yahoo.com	(43)	Healthcare you can afford	YCZHEBRCXTJN	8/26/2002 11:13:44 PM

Cap Letters

```
Sep 06 * vvcxzza@yahoo.com (71) FREE HGH -Look Ten Years Younger in 3 Weeks LZKHF
Sep 06 * bbarber612@hotmail (167) PROTECT YOUR INFORMATION AND YOUR COMPUTER!EZBCYT
Sep 06 * zzsaw@yahoo.com (34) Mortgage Rates are going lower LYLSJE
Sep 05 * alice149@hotmail.c (157) Re: BE healthy with this BREAKTHROUGH product! XMUJL
Sep 04 * bconst3442@hotmail (91) actually work?"NRWR
Sep 03 * zzxdw@festie.com (91) Get crystal reception on your cell phone IZKQLO
Sep 03 * ljhuyt@chilly-bin. (71) Discount Viagra G
Sep 03 * asdw2@well-in.com (41) Affordable Healthcare FSX
Sep 02 * ccxcfdxz@yahoo.com (34) Save thousands rates are low ESLGW
Sep 02 * lloihhg@yahoo.com (77) Magical Laser Keychain NNJODQ
Sep 02 * connie_1_1@hotmail (170) Fw: PROTECT YOUR COMPUTER AGAINST HARMFUL VIRUSES! GMKTPIW
Sep 01 * binder39@hotmail.c (168) Fw: NORTON SYSTEMWORKS CLEARANCE SALE_ONLY $29.99! HTHIPNB
Aug 31 * bbssw2@yahoo.com (70) FREE HGH -Look Ten Years Younger in 3 Weeks CGU
Aug 31 * lloihhg@yahoo.com (41) Dont pay to much for cigs UKMPC
Aug 30 * [REDACTED] (157) Fw: PROTECT LET A COMPUTER VIRUS RUN YOUR [REDACTED] CEJPS
```

```
Aug 30 * From: alice149@hotmail.com
Aug 29 * Reply-To: alice149@hotmail.com
Aug 29 * To: oblaga@hotmail.com, piasono2@hotmail.com
Aug 28 * Cc: raver77@hotmail.com, narcisse@eccw.com
Aug 26 * Message-ID: <000056361fbd$00006231$000047fa@copywriter1.ls>
Aug 25 * Subject: Re: BE healthy with this BREAKTHROUGH product! XMUJL
Aug 22 * Date: Thu, 05 Sep 2002 07:54:28 -1600
Aug 22 * MIME-Version: 1.0
```

Cap Letters with TZ “-1600”

```

Sep 09 * corbinjim@hotmail. (171) Attn: This is NO JOKE! Speed up your CPU for under $30! G
Sep 09 * corbinjim@hotmail. (171) Attn: This is NO JOKE! Speed up your CPU for under $30! G
Sep 06 * bbarber612@hotmail (167) PROTECT YOUR INFORMATION AND YOUR COMPUTER!EZBCYT
Sep 05 * alicel49@hotmail.c (157) Re: BE healthy with this BREAKTHROUGH product! XMUJL
Sep 04 * bconst3442@hotmail (91) actually work?"NRWR
Sep 02 * connie_1_1@hotmail (170) Fw: PROTECT YOUR COMPUTER AGAINST HARMFUL VIRUSES! GMKTPIW
Sep 01 * binder39@hotmail.c (168) Fw: NORTON SYSTEMWORKS CLEARANCE SALE_ONLY $29.99! HTHIPNB
Aug 30 * breaks26@hotmail.c (167) Fw: DON'T LET A COMPUTER VIRUS RUIN YOUR DAY! CEUDG
Aug 29 * bballjac@hotmail.c (173) Attn: SYSTEMWORKS CLEARANCE SALE_ONLY $29.99 ZENRT
Aug 25 * bbkke861@hotmail.c (160) Fw: PROTECT YOUR COMPUTER, YOU NEED SYSTEMWORKS! WDKCJW
Aug 20 * blueguy13@hotmail. (175) Re: Discount Prices + FREE Shipping = #1 Service! EOQMIHFTO
Aug 20 * blueguy13@hotmail. (175) Re: Discount Prices + FREE Shipping = #1 Service! EOQMIHFTO
Aug 12 * bcook61@hotmail.co (151) Attn: PROTECT YOUR COMPUTER, YOU NEED SYSTEMWORKS!RUOZ
Aug 11 * breedde@hotmail.co (170) Aren't these things overpriced?KXPQXLVE
Aug 09 * bbarednek@hotmail. (74) Free Consultation. Buy Viagra Online !KK
Aug 09 * bbarednek@hotmail. (74) Free Consultation. Buy Viagra Online !KK
Aug 07 * bjorne59@hotmail.c (93) Attn: Want to LOSE Weight FAST?WNSJDBZD
Aug 07 * bcoole2@hotmail.co (91) Lose 80lbs In A Wk? #1 Diet Pill! Wholesale!!JI
Aug 07 * bbarff@hotmail.com (60) **Your Free Club membership!*** DRZFP
Aug 07 * bbarker6@hotmail.c (91) Lose 19 Pounds In 10 DaysI
Jul 30 * dafricano@hotmail. (141) Re: Can't Stand the Cost of Ink Cartridges?VGMURR
Jul 28 * el86@hotmail.com (226) Re: Men & Women, Spruce up your life! CKIDDB
Jul 17 * dagnyh@hotmail.com (88) Lose 14 Pounds In 10 Days VET
Jul 09 * cwood83@hotmail.co (97) Make your prints beautiful & SAVE BIG! Y
Jul 09 * cwood83@hotmail.co (97) Make your prints beautiful & SAVE BIG! Y
Jul 04 * contactroxy@hotmail (138) Welcome to the Modern Way to Improve your Budget!XVITRZY

```


Cap Letters with TZ “-1700”

```
Dec 07 * ttyrew21@yahoo.com (101) Get better reception on your cell phoneSBCZFIHRN
Dec 07 * kkjhg65@yahoo.com (101) Boost your cell phone receptionKP
Dec 07 * minir221@yahoo.com (83) Need to be revitalizedVC
Dec 07 * ggdsa2@yahoo.com (83) Want to look youngerIAT
Dec 06 * vdsd221@yahoo.com (108) FW: HOT New Toy for Christmas 2002!KEDMIXBV
Dec 06 * ccvds21@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 * llkjy56@yahoo.com (41) Automated Life Insurance quotes,JOBQ
Dec 05 * zxxas21@yahoo.com (42) We can save you thousands on life insuranceAMKG
Dec 04 * erww221@yahoo.com (107) HOT New Toy for Christmas 2002! J
Dec 04 * qqwss3@yahoo.com (108) FW: Remote Controlled Mini Matchbox Cars CI
Dec 04 * yytr453@yahoo.com (46) Mortgage Rates are going lower
Dec 04 * mmjh543@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 * vvsd2122@yahoo.com (107) FW: MINI RADIO_CONTROLLED CARS ARE SOLD OUT IN STORESH
Dec 02 * cxzxca12@yahoo.com (78) Look and feel 30 years youngerXRDRJBAOSVW
Dec 02 * cxzxca12@yahoo.com (78) Look and feel 30 years youngerABCT
Dec 01 * vbcx21@yahoo.com (58) Enlarge your packageGTGIL
Dec 01 * vvsd21@yahoo.com (59) Feeling SmallLPMVEDV
Nov 30 * bcvbcv32@yahoo.com (53) Refinance today and save thousandsJAL
Nov 30 * bcvbcv32@yahoo.com (53) Want a Home Improvement LoanZQJAG
Nov 28 * nngtr32@yahoo.com (45) Want a Home Improvement LoanZETLCJYI
Nov 27 * wqw3@yahoo.com (107) FW: MINI RADIO_CONTROLLED CARS ARE SOLD OUT IN STORESH
```

Thanksgiving: Thu Nov 28, 2002

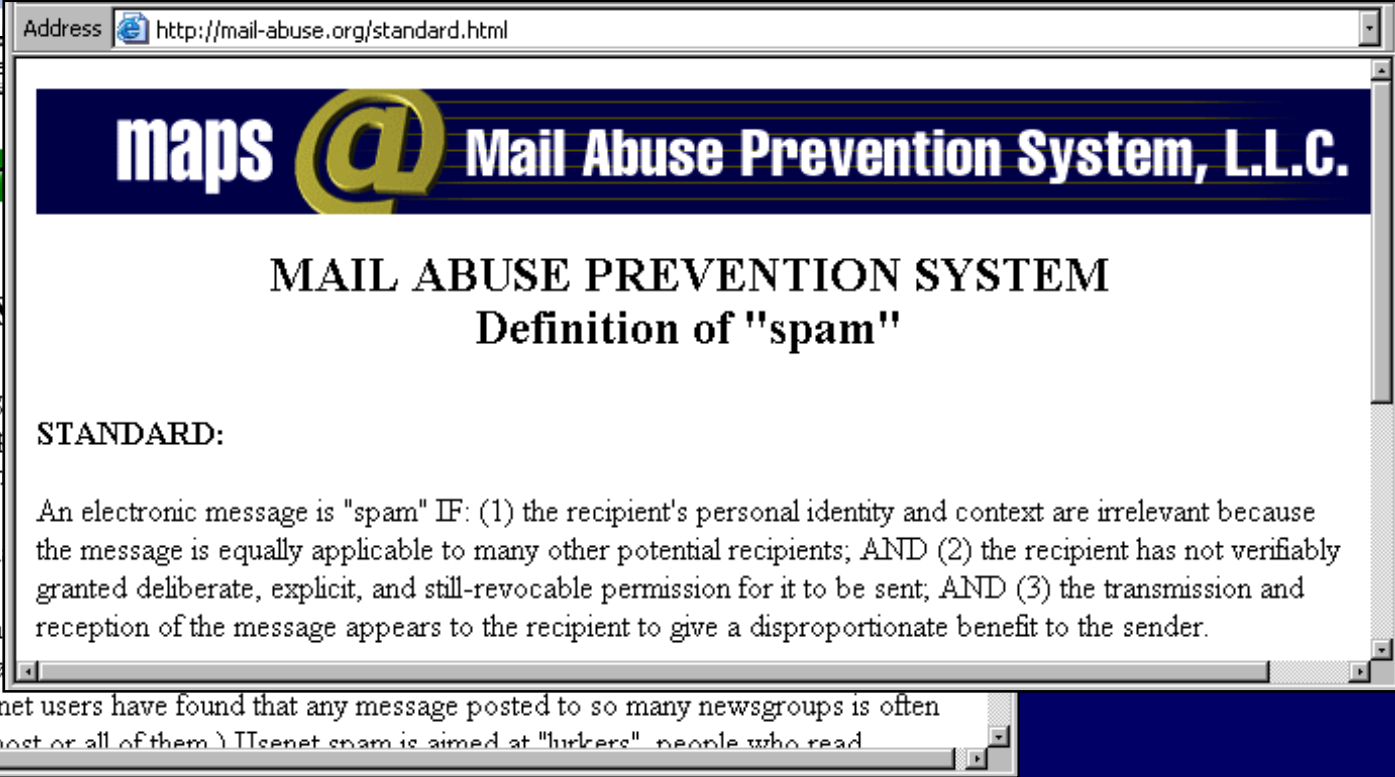
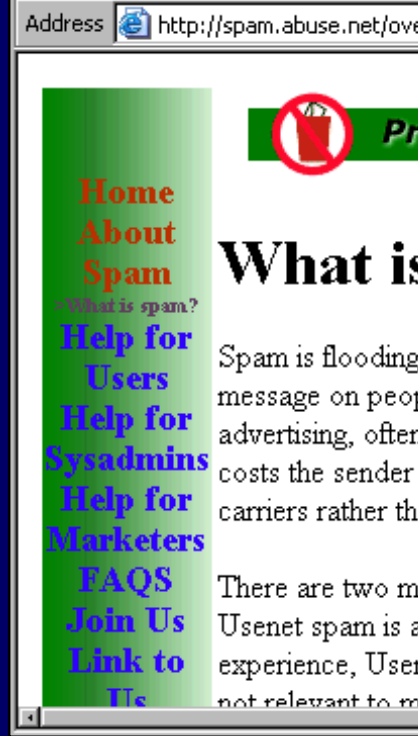
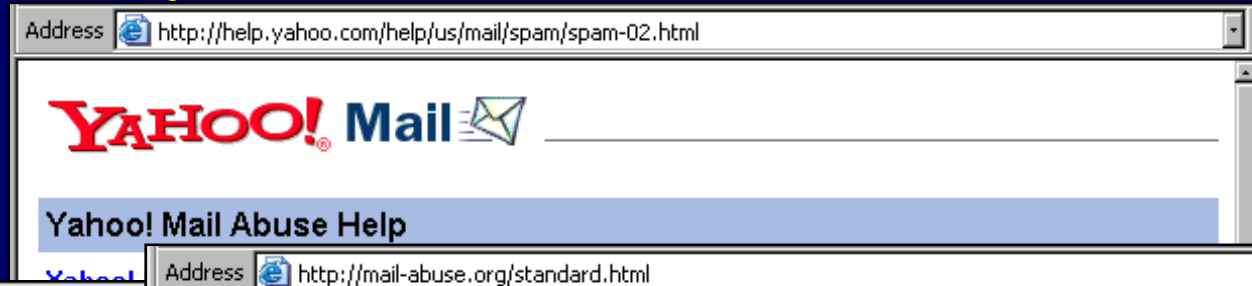
Organizing Methods Summary

- 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



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 forwarding
 - Includes “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;

Wed, 3 Jul 2002 19:53:39 -0700

Date: Wed, 3 Jul 2002 19:53:39 -0700

Message-Id: <200207040253.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, 650-872-1278, 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

NCE Example: Comcast

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?

Check your Comcast E-Mail Contact Preferences at

<http://www.comcast.net/signin.jsp?redirectUrl=http://www.comcast.net/CheckAuth?redirectUrl=http://online.comcast.net/preferences/index.html?CM.src=eml031205>.

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

Welcome to Comcast High-Speed Internet!

December 8, 2003

HOME PRODUCTS SHOPPING SEARCH ABOUT US

CHANNELS

- News
- Finance
- Sports
- Entertainment
- Games

TOOLBOX

- Mail
- Service Center
- Online Storage
- Personal Web Pages
- Photo Center

SERVICE CENTER

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 **xxxxxxx@comcast.net**

Zip Code*

- 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
 - Barnes & Noble University
 - Hewlett-Packard

Non-Commercial Categories

The vast majority of Spam

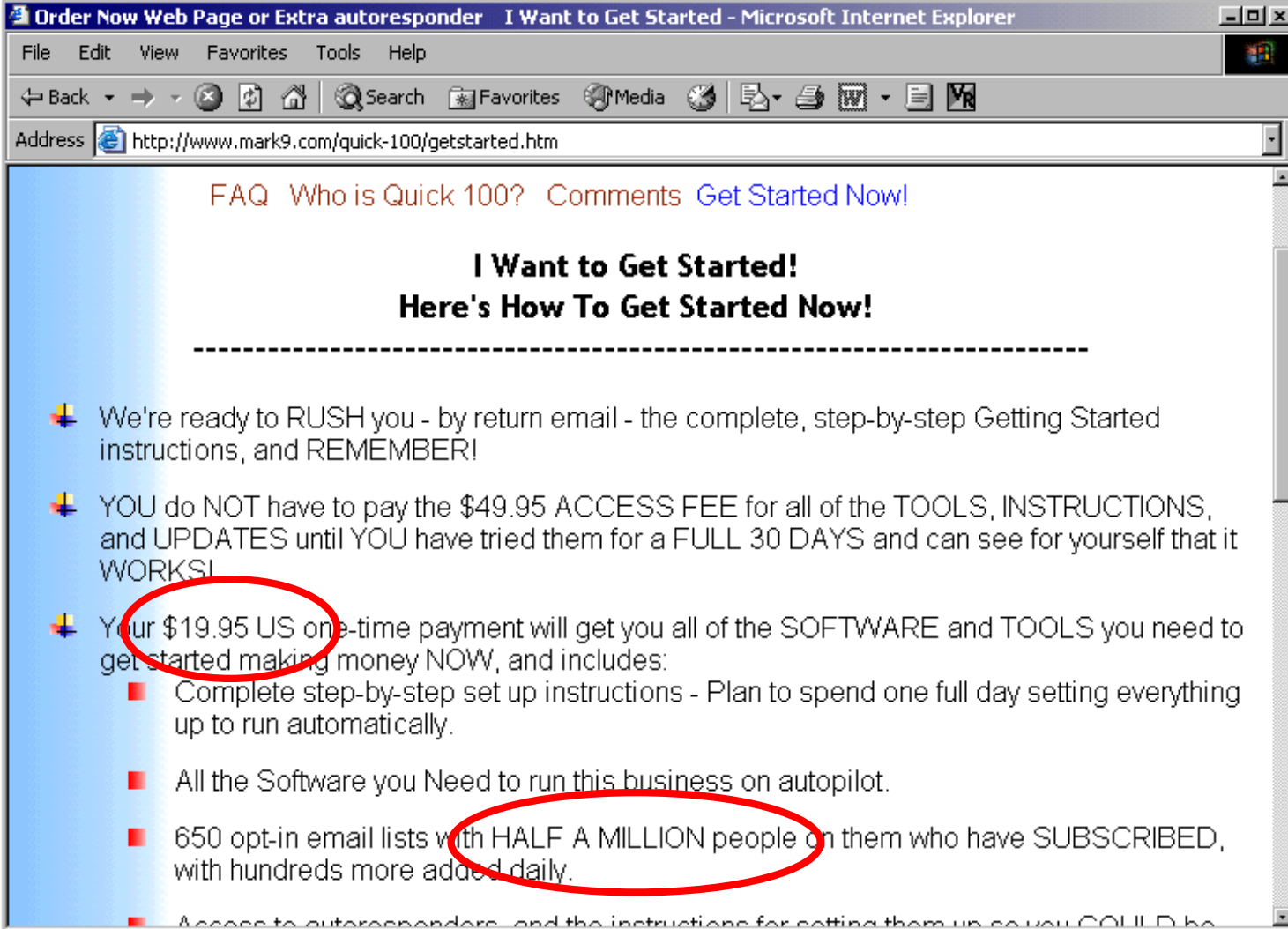
3. List Makers

- 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



Order Now Web Page or Extra autoresponder I Want to Get Started - Microsoft Internet Explorer

File Edit View Favorites Tools Help

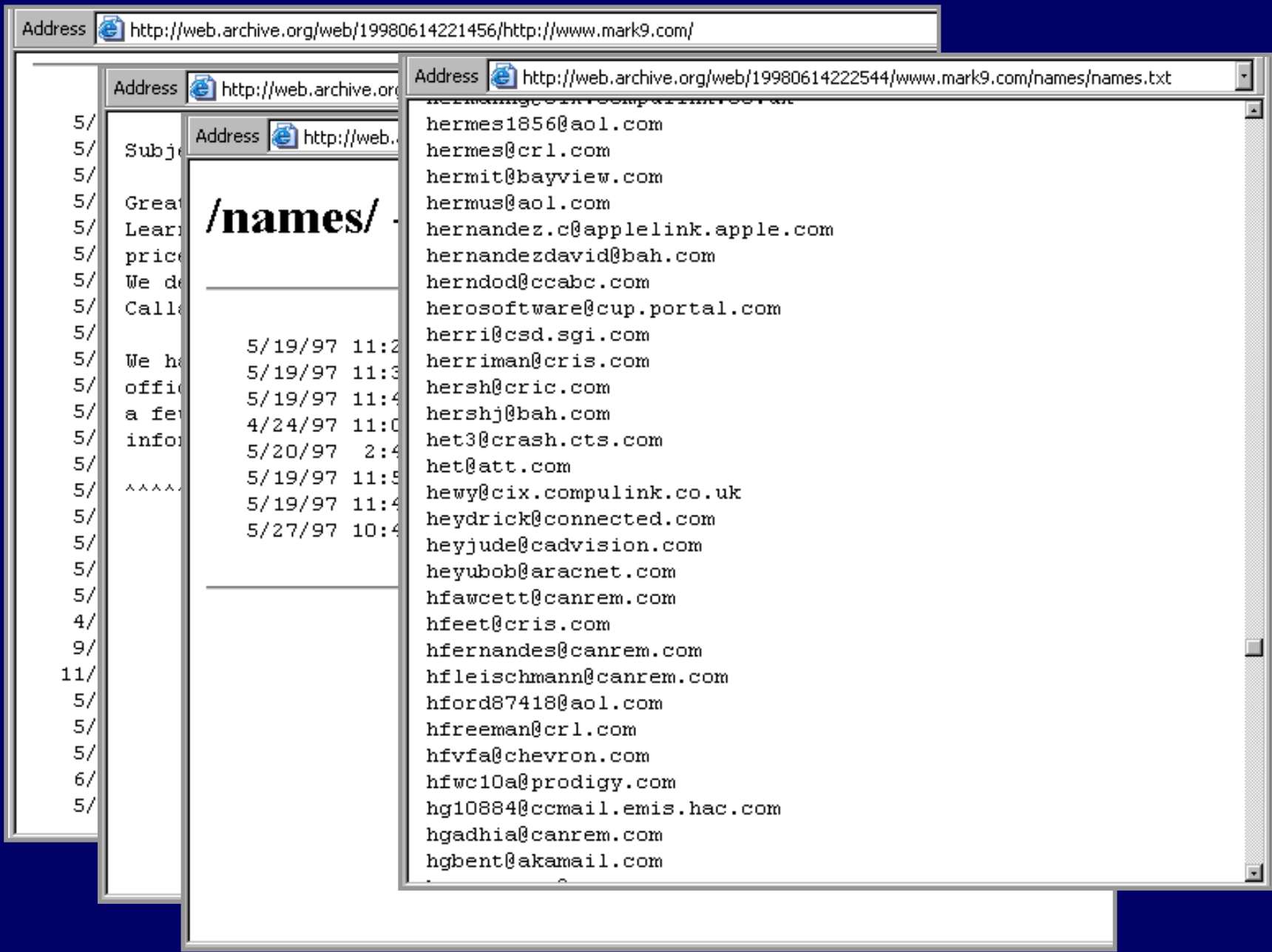
Back Forward Stop Home Search Favorites Media Print Mail

Address <http://www.mark9.com/quick-100/getstarted.htm>

[FAQ](#) [Who is Quick 100?](#) [Comments](#) [Get Started Now!](#)

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 autoresponders, and the instructions for setting them up so you COULD be...



Address <http://web.archive.org/web/19980614221456/http://www.mark9.com/>

Address <http://web.archive.org/web/19980614221832/www.mark9.com/90003/90003.TXT>

Address <http://web.archive.org/web/19980614221731/www.mark9.com/names/>

5/

5/ Subject

5/

5/ Great

5/ Learn

5/ price

5/ We de

5/ Call

5/

5/ We h

5/ offic

5/ a fe

5/ info

5/ *****

5/

5/

5/

5/

4/

9/

11/

5/

5/

5/

6/

5/

```

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)

Scam Example: Pro-Hosiery

Received: from **localhost** (218-163-8-137.hinet-ip.hinet.net[218.163.8.137])
by sccrmxc14.attbi.com (sccrmxc14) with SMTP
id <20030716092122s140071jkbe>; Wed, 16 Jul 2003 09:21:31 +0000

Message-ID: <000601c34b2f\$b3e3c220\$0300a8c0@selfassembled>

From: "pro-hosiery-cor3-1of8" <pro-hosiery-cor3-1of8@**pro-hosiery-cor3-1of8.com**>

To: test@seurescience.net

Subject: Supplying to you with ladies hosiery

Date: Wed, 16 Jul 2003 08:17:54 +0800

Dear Sir,
Jul.16,03.

Ref.No.pro-hosiery-cor3-1of8

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 **begining**,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

It's Citibank!

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 -t- 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)K, copy and paste the link into the address bar of your web browser.

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

y-----

Thank you for using Citibank!

C-----

Russian URL

E-mail Verification - Microsoft Internet ...

sign on to Citibank
with your Citibank® Banking Card

Card #/CIN

PIN

sign on

Your E-Mail Was Verified. - Microsoft In...

Your E-Mail Was Verified. - Mic

Thank you.

Your E-Mail Address Was
Successful Verified.

Welcome to Citibank - Microsoft Internet Explorer


File Edit View Favorites Tools Help

← Back → Home Media

Address <http://www.citibank.com/us/index.htm>

citi [sign on](#) [open account](#) [contact us](#) [search](#) [privacy](#) [citi.com](#)

PRODUCTS & SERVICES PLANNING & TOOLS INVESTING & MARKETS HELP DESK MY Citi



VARIABLE RATES
AS LOW AS
Prime minus
2.01%, currently
1.99% APR
for 4 months
Prime, currently
4.00% APR
thereafter

Welcome to Citibank

Ready to
Credit fr

sign on
to your accounts

Choose one

[learn more](#)
take a tour

[apply now](#)
open an account

Jump to

Small Business

Corporate

select a country

United States

look for a product or service

Choose one

learn about

Choose one

smartdeals

Get more mileage
out of your money

Get up to 10,000 AAdvantage® miles when you open a **Citibank** checking account online.

[details](#)

Need extra

from Citibank.

[get details](#)

0 APR* purchases for 6 months.

[*apply now](#)

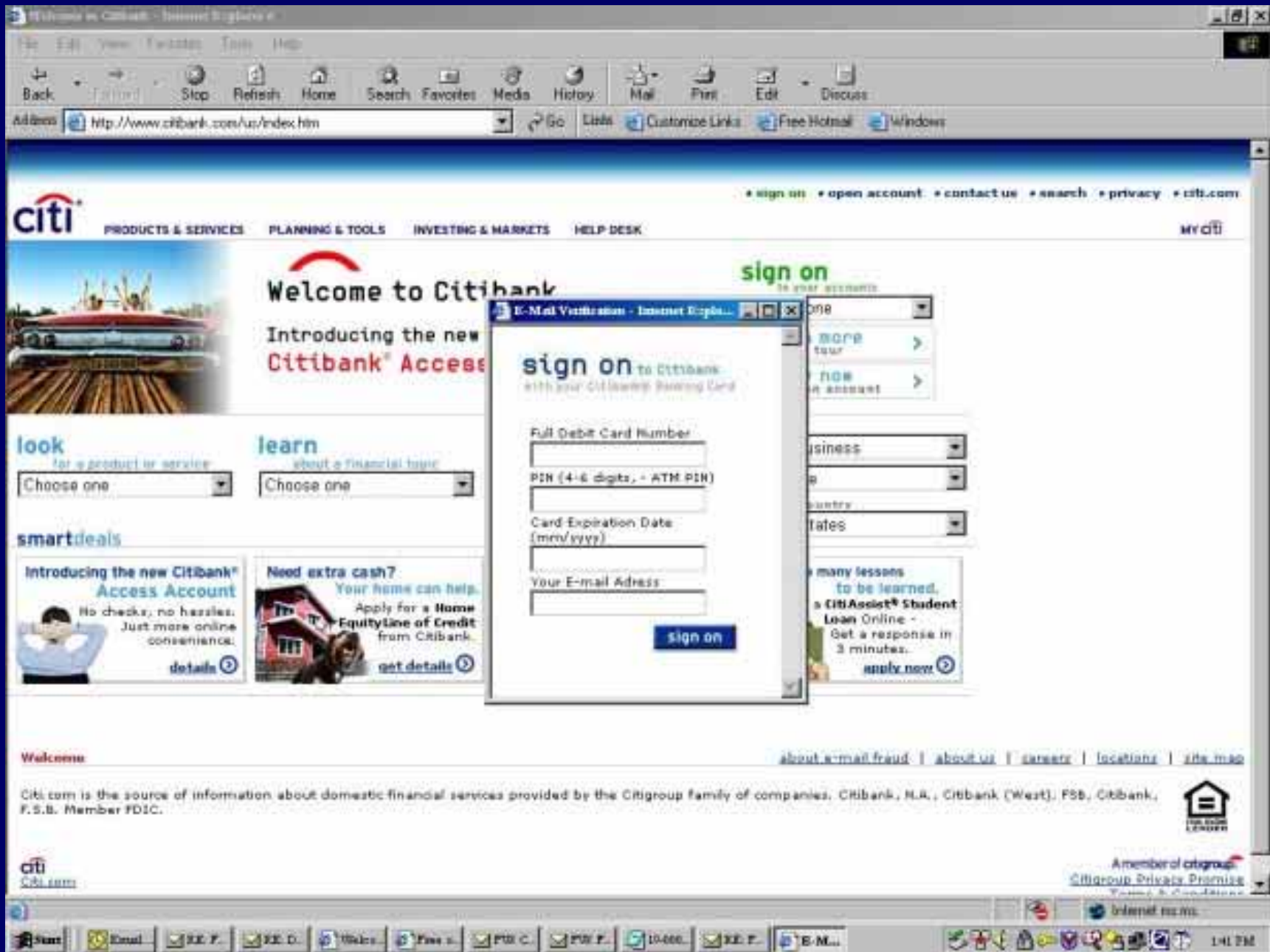
There are many lessons to be learned.

Apply for a **CitiAssist® Student Loan** Online - Get a response in 3 minutes.

[apply now](#)

sign on

Internet



Russian Web Bug

День	Хиты
08.08.2003	3
09.08.2003	0
10.08.2003	0
11.08.2003	5
12.08.2003	0
13.08.2003	1
14.08.2003	1
15.08.2003	1
16.08.2003	107274
17.08.2003	91503
18.08.2003	584
19.08.2003	209
20.08.2003	0
Итого:	199581

Сводная статистика IP адресов посетителей

Статистика с 8.8.2003 по 15.8.2003

[Подробнее](#)

Распределение IP адресов (всего): 10

№	Адрес	Кол-во	Среднее в день	Процент в группе
1	68.82.62.191 [whois]	8	1	80.00%
2	12.5.1.207 [whois]	1	0.12	10.00%
3	208.141.219.205 [whois]	1	0.12	10.00%

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@seurescience.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@seurescience.net
To: Test <test@seurescience.net>
References: <F5B12412EAC2131E@seurescience.net>
In-Reply-To: <F5B12412EAC2131E@seurescience.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

Great Spam Archive Date	Message-ID	Subject
24 Apr 2003 13:01:55	0JJ9H7JGA03EI8A7I@att.net	Rich, Hello! My name is John Turner...
15 Jun 2003 12:41:00	D4CI74IDH3FKH13D@att.net	Dear Rich! I've been scammed over...
07 Jul 2003 07:43:51	2EF98ADD2HG3CJ54@att.net	Rich, Any software just for 15\$ - 40\$
17 Jul 2003 10:39:28	76E7A5HFIJIHK63C@e-loan.com	[Ftpserver] Re: Your E-Loan Refinance..
17 Jul 2003 10:46:08	6J76H1B289HCC313@e-loan.com	Re: Your E-Loan Refinance Applicatio..
22 Jul 2003 01:21:52	77EGJ4AGC1F3AIB5@wellsfargo.com	Re: Wells Fargo Bank New Business...
26 Jul 2003 09:43:59	JFHAL1CJIB78IFA8@security.org	Newsletter
26 Jul 2003 23:00:46	H8HFB0BB06232180@e-gold.com	The Great E-Gold Giveaway!
29 Jul 2003 18:39:15	4K63GFHLE8FJ1GK7@utp.edu.co	Rich, software for you
30 Jul 2003 19:03:38	3FHG03G0I213JJ92@yahoo.com	I want to introduce Stock Cruiser
31 Jul 2003 05:26:44	BG5L3CAI6J586EK0@headgear.org	new mail p1QwvfpX
02 Aug 2003 10:21:12	J9D9GK1H11J47920@hotmail.com	Rich,Want sex <rndmx>
09 Aug 2003 11:59:24	50LJ6D9B4EK320HD@annexia.org	ÿæíúé îäüö
17 Aug 2003 07:58:36	2J73600018ECI75J@virtualitas.net	Re: mail e4AXAvl8
17 Aug 2003 17:49:39	FBE6962ED2FJFK58@hotmail.com	Rich, Instant Pleasures,
20 Aug 2003 19:37:45	A60I9A7D890FL51L@cbshost-68-111-42-31.sbcox.net	Re: mail 3CPVQp5E

Related: Scams

Great Spam Archive Date	Message-ID	Subject
24 Apr 2003 13:01:55	0JJ9H7JGA03EI8A7I@att.net	Rich, Hello! My name is John Turner...
15 Jun 2003 12:41:00	D4CI74IDH3FKH13D@att.net	Dear Rich! I've been scammed over...
07 Jul 2003 07:43:51	2EF98ADD2HG3CJ54@att.net	Rich, Any software just for 15\$ - 40\$
17 Jul 2003 10:39:28	76E7A5HFIJIHK63C@e-loan.com	[Ftpserver] Re: Your E-Loan Refinance..
17 Jul 2003 10:46:08	6J76H1B289HCC313@e-loan.com	Re: Your E-Loan Refinance Applicatio..
22 Jul 2003 01:21:52	77EGJ4AGC1F3AIB5@wellsfargo.com	Re: Wells Fargo Bank New Business...
26 Jul 2003 09:43:59	JFHAL1CJIB78IFA8@security.org	Newsletter
26 Jul 2003 23:00:46	H8HFB0BB06232180@e-gold.com	The Great E-Gold Giveaway!
29 Jul 2003 18:39:15	4K63GFHLE8FJ1GK7@utp.edu.co	Rich, software for you
30 Jul 2003 19:03:38	3FHG03G0I213JJ92@yahoo.com	I want to introduce Stock Cruiser
31 Jul 2003 05:26:44	BG5L3CAI6J586EK0@headgear.org	new mail p1QwvfpX
02 Aug 2003 10:21:12	J9D9GK1H11J47920@hotmail.com	Rich,Want sex <rndmx>
09 Aug 2003 11:59:24	50LJ6D9B4EK320HD@annexia.org	İëÿæíúé îòäüö
17 Aug 2003 07:58:36	2J73600018ECI75J@virtualitas.net	Re: mail e4AXAvl8
17 Aug 2003 17:49:39	FBE6962ED2FJFK58@hotmail.com	Rich, Instant Pleasures,
20 Aug 2003 19:37:45	A60I9A7D890FL51L@cbshost-68-111-42-31.sbcox.net	Re: mail 3CPVQp5E

Related: Phishing

Great Spam Archive Date	Message-ID	Subject
24 Apr 2003 13:01:55	0JJ9H7JGA03EI8A7I@att.net	Rich, Hello! My name is John Turner...
15 Jun 2003 12:41:00	D4CI74IDH3FKH13D@att.net	Dear Rich! I've been scammed over...
07 Jul 2003 07:43:51	2EF98ADD2HG3CJ54@att.net	Rich, Any software just for 15\$ - 40\$
17 Jul 2003 10:39:28	76E7A5HFIJIHK63C@e-loan.com	[Ftpserver] Re: Your E-Loan Refinance..
17 Jul 2003 10:46:08	6J76H1B289HCC313@e-loan.com	Re: Your E-Loan Refinance Applicatio..
22 Jul 2003 01:21:52	77EGJ4AGC1F3AIB5@wellsfargo.com	Re: Wells Fargo Bank New Business...
26 Jul 2003 09:43:59	JFHAL1CJIB78IFA8@security.org	Newsletter
26 Jul 2003 23:00:46	H8HFB0BB06232180@e-gold.com	The Great E-Gold Giveaway!
29 Jul 2003 18:39:15	4K63GFHLE8FJ1GK7@utp.edu.co	Rich, software for you
30 Jul 2003 19:03:38	3FHG03G0I213JJ92@yahoo.com	I want to introduce Stock Cruiser
31 Jul 2003 05:26:44	BG5L3CAI6J586EK0@headgear.org	new mail p1QwvfpX
02 Aug 2003 10:21:12	J9D9GK1H11J47920@hotmail.com	Rich,Want sex <rndmx>
09 Aug 2003 11:59:24	50LJ6D9B4EK320HD@annexia.org	İëÿæíúé îòäüö
17 Aug 2003 07:58:36	2J73600018ECI75J@virtualitas.net	Re: mail e4AXAvl8
17 Aug 2003 17:49:39	FBE6962ED2FJFK58@hotmail.com	Rich, Instant Pleasures,
20 Aug 2003 19:37:45	A60I9A7D890FL51L@cbshost-68-111-42-31.sbcox.net	Re: mail 3CPVQp5E

Related: Malware

Great Spam Archive Date	Message-ID	Subject
24 Apr 2003 13:01:55	0JJ9H7JGA03EI8A7I@att.net	Rich, Hello! My name is John Turner...
15 Jun 2003 12:41:00	D4CI74IDH3FKH13D@att.net	Dear Rich! I've been scammed over...
07 Jul 2003 07:43:51	2EF98ADD2HG3CJ54@att.net	Rich, Any software just for 15\$ - 40\$
17 Jul 2003 10:39:28	76E7A5HFIJIHK63C@e-loan.com	[Ftpserver] Re: Your E-Loan Refinance..
17 Jul 2003 10:46:08	6J76H1B289HCC313@e-loan.com	Re: Your E-Loan Refinance Applicatio..
22 Jul 2003 01:21:52	77EGJ4AGC1F3AIB5@wellsfargo.com	Re: Wells Fargo Bank New Business...
26 Jul 2003 09:43:59	JFHAL1CJIB78IFA8@security.org	Newsletter
26 Jul 2003 23:00:46	H8HFB0BB06232180@e-gold.com	The Great E-Gold Giveaway!
29 Jul 2003 18:39:15	4K63GFHLE8FJ1GK7@utp.edu.co	Rich, software for you
30 Jul 2003 19:03:38	3FHG03G0I213JJ92@yahoo.com	I want to introduce Stock Cruiser
31 Jul 2003 05:26:44	BG5L3CAI6J586EK0@headgear.org	new mail p1QwvfpX
02 Aug 2003 10:21:12	J9D9GK1H11J47920@hotmail.com	Rich,Want sex <rndmx>
09 Aug 2003 11:59:24	50LJ6D9B4EK320HD@annexia.org	İëÿæíúé îòäüö
17 Aug 2003 07:58:36	2J73600018ECI75J@virtualitas.net	Re: mail e4AXAvI8
17 Aug 2003 17:49:39	FBE6962ED2FJFK58@hotmail.com	Rich, Instant Pleasures,
20 Aug 2003 19:37:45	A60I9A7D890FL51L@cbshost-68-111-42-31.sbcox.net	Re: mail 3CPVQp5E

Use of Malware

- Trojan.Download.Berbew
 - 17-Jul-2003 & 22-Jul-2003
 - Captures passwords
- Exploit-Codebase
 - 26-Jul-2003
- Malware consistencies:
 - Written in C, same compiler
 - Old exploit techniques

And Related Scams...

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

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 asmtpt;
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

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 asmtpt;
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:

```
...  
<SCRIPT>  
function noRightClick(evt) { 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>
```

[gvjrFov-ka1AsHb3-oOGlgZSseoUJF]

[gvjr Fov - ka1AsH b3 - oO G I gZSseo UJF]

[Governor of - class B - oh gee I guess UJF]

Received: from yahoo.com ([211.250.18.161]) by server.company.com
(InterMail vM.4.01.03.27 201-229-121-127-20010626) with SMTP
id <20020521160946.TILS4787.server.company.com@yahoo.com>;
Tue, 21 May 2002 16:09:46 +0000

Received: from [233.76.29.183] by rly-yk05.mx.aol.com with esmtp; Mon, 20 May 2002
00:06:43 -0300

Received: from [27.70.42.37] by smtp013.mail.yahoo.com with local; Sat, 18 May 2002
13:04:19 +1200

Received: from 75.65.54.143 ([75.65.54.143]) by mx.rootsystems.net with asmt; Fri, 17 May
2002 02:01:55 +0400

Received: from 122.59.66.250 ([122.59.66.250]) by n7.groups.yahoo.com with asmt; Wed, 15
May 2002 14:59:31 +1000

Reply-To: <Chris0254sCaREn@earthlink.net>

Message-ID: <4185C208-DA36-4E94-8E43-9AA48332FED4@EcKc4Fag>

From: <Chris0254sCaREn@earthlink.net>

To: <neil@company.com>

Cc: <nethawk@company.com>, <niraj@company.com>

Subject: Do you want Financial Independence? K6eufcHWb

X-Priority: 3 (Normal)

X-MSMail-Priority: Normal

X-Mailer: Microsoft Outlook Express 5.00.2615.200

Importance: Normal

Date: Tue, 21 May 2002 16:09:49 +0000

...

[whQZsFOtOcY-AWw9fYuTUvLS-EBdh4gbj2Py5H]

Chris025

Yellow Pages - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Print

Address <http://uic.globe.com.ph/grimrod/hang-out/hci-miscell/hci-yellowpages.htm> Links

YELLOW PAGES

[home](#) | [omsnomm hang-out](#) | [u've got to c her](#) | [drumroll please](#) | [irc's most wanted](#) | [eyeball to eyeball](#) | [ur file is done](#) | [anything goes](#) | [linkathon](#) | [tadentry online](#)

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...

hci	hci@mail.com
Anfernee	
angelface	
beetlebum	skidrow_gal@mailcity.com
CyBeRSaD*	cybersad04@yahoo.com
Czarina*	czarina@pacific.net.ph
DATA*	chris025@hotmail.com
DoC_SpOoKy*	
Fay^	duchessfay@hotmail.com
...	

Done Internet

Linking...

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

<http://uic.globe.com.ph/grimrod/hang-out/hci-miscell/hci-yellowpages.htm>

<http://uic.globe.com.ph/grimrod/hang-out/hci-miscell/>

<http://uic.globe.com.ph/grimrod/hang-out/>

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)

unixsl-gl.chinadns.com

Address  http://www.cnhonker.net/index.php

. HVC .

- About
- Advisories
- Beginner
- Chat
- Checklist
- Documents
- Exploits
- Forums
- Projects
- Standard
- Tools

红客联盟公告



- 红客联盟严正声明 10-05 红客联盟
- 关于中国红客网络技术联盟 10-05 红客联盟
- 关于红客联盟邮件列表 09-23 lion
- 红客联盟网站更新脚本全部完成,今天将开始更新! 09-23 lion
- 红客联盟网站重新开放! 09-20 lion

[更多公告>>>](#)

最新文档更新

▶ [新手上路]	Telnet命令模式	07-26	艰苦
▶ [文档资料]	封包嗅探器(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OOB查找socket	07-25	bkbll
▶ [安全公告]	Windows 2000实用程序管理器...	07-14	墨斗鱼
▶ [安全公告]	SMB数据包边界过滤缺陷允许...	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]	DSR-mnogo.pl	07-14	墨斗鱼
▶ [文档资料]	没有电脑的入侵-深入浅出社...	07-12	gouy2k&Jokul
▶ [文档资料]	没有电脑的入侵-深入浅出社...	07-11	gouy2k&Jokul

[递交文章>>>](#) [更多文档>>>](#)

最新软件更新

▶ [扫描工具]	WebDAVScan.rar	03-22	uhhuhy
▶ [扫描工具]	ntscan.zip	03-18	uhhuhy
▶ [扫描工具]	HScan V1.20	03-10	uhhuhy
▶ [后门木马]	HFilter V0.10	01-28	lion
▶ [扫描工具]	Infoscan.exe	01-27	uhhuhy
▶ [攻击工具]	HGod V0.51	01-16	lion
▶ [扫描工具]	HScan v1.01	01-06	uhhuhy

邮件列表

邮箱地址

联盟IRC

host: irc.sunnet.org
port: 6667
#cnhonker
Web入口
download: HIRC

合作站点

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! LbIBrLeIE

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

MEMBERS

addikti populi...

THE BASICS AND ADDITIONS

- SabRina^
- Zarah
- Silverlove
- vogue
- CyBeRSaD
- Seagull
- SiKyo
- KurDaPya
- SabRina^
- MMV
- 'X-SeMiNaRiaN'
- Cuervo

The happy people interested in joining our community. Please click the JOIN IN button below to join our addiks members. We will provide you with a brief detail about our community. We greatly appreciate your contribution. (jpeg format please) addiks.zzn.com

Conversations

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

HOME B Thu, 15 Aug 2002 04:06:53

Reply-To: <homejobsourcesIDot78@netzero.com>

ASSEMBL Message-ID: <A83A333F-AF7F-11D6-AAE6-444553540000@XpfEaTRG>

ART WORK From: "Susan Whaley" <homejobsourcesIDot78@netzero.com>

WRITING Subject: Jobs at Home FVOa7-JAuj-NfasGb

...

[eUEVW HOME BASED POSITIONS:

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

...

[pi5BUpBP9-tXKKHlhffs-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
Wed, 16 Oct 2002 10:49:16
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															
GMT+0	01	02	03	04	06	07	08	10	12	13	16	17	18	20	21
GMT+8	09	10	11	12	14	15	16	18	20	21	00	01	02	04	05
Volume	3	1	7	1	2	5	2	3	1	1	3	1	2	2	1

GMT	Sun	Mon	Tue	Wed	Thu	Fri	Sat
+0	1	3	8	7	6	6	1
+8	1	1	9	6	6	7	2

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 Philipppians is not improbable.

10:15 - 11:45	Periods 4 & 5	90 minutes
11:45 - 12:45	Lunch Break	0 minutes
12:45 - 02:15	Period 6 & 7	90 minutes
Total Hours per week in class		7 Hours

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

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