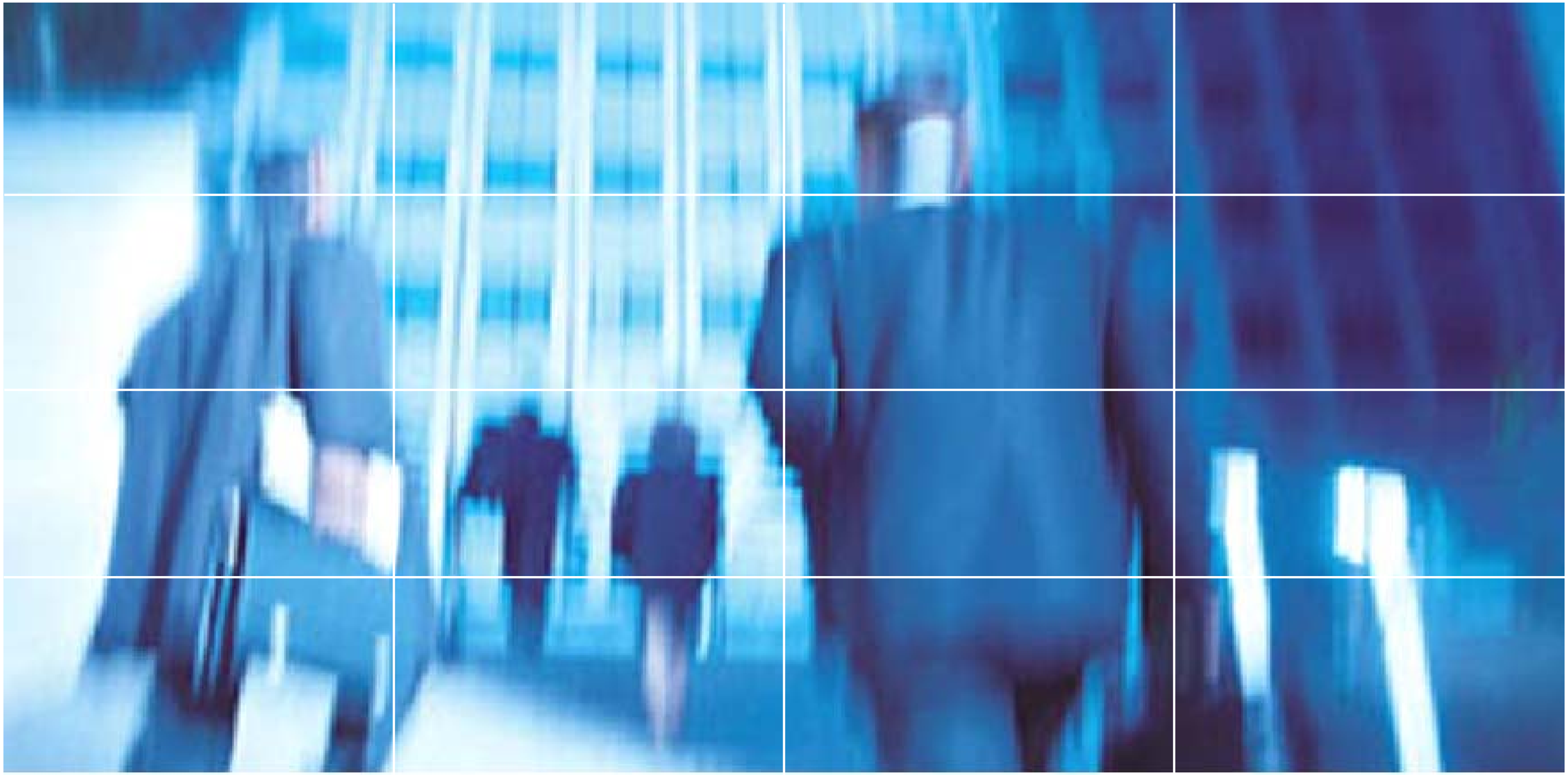


Botnets and spam: What we're doing to deal with the blended threat

Jim Lippard

FRnOG 6, April 1, 2005

Global Crossing®

AGENDA

1. Overview of the blended threat.
2. Some trends.
3. Rogue’s gallery.
4. Defense and attack strategies.
5. Our implementation and plans.
6. Help wanted.
7. Q&A.

Rise of the botnets

Early 1990s: IRC channel bots (e.g., eggdrop, mIRC scripts, ComBot, etc.).

Late 1990s: Denial of service tools (e.g., Trinoo, Tribal Flood Network, Stacheldraht, Shaft, etc.).

2000: Merger of DDoS tools, worms, and rootkits (e.g., Stacheldraht+t0rnkit+Ramen worm; Lion worm+TFN2K).

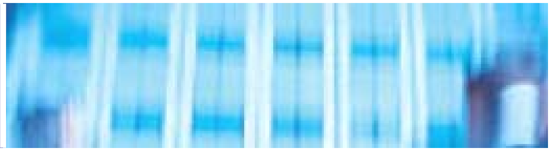
2002: IRC-controlled bots implementing DDoS attacks.

2003: IRC-controlled bots spread with worms and viruses, fully implementing DDoS, spyware, malware distribution activity.

(Dave Dittrich, “Invasion Force,” Information Security, March 2005, p. 30)

2003-2005: Botnets used as a criminal tool for extortion, fraud, identity theft, computer crime, spam, and phishing.

Botnets today



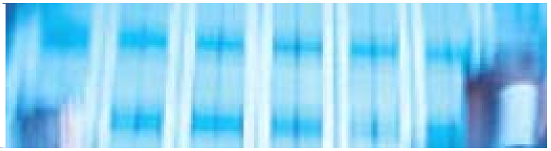
- Botnets are usually compromised Windows machines, usually controlled from a compromised Unix machine running ircd, sometimes with passwords, sometimes with encryption. Controllers are most often found on low-cost, high-volume web hosting providers. Bots are most often found on home machines of cable modem and DSL customers.

- Agobot/Phatbot is well-written, modular code supporting DoS attacks, spam proxying, ability to launch viruses, scan for vulnerabilities, steal Windows Product Keys, sniff passwords, support GRE tunnels, self-update, etc. Phatbot control channel is WASTE (encrypted P2P) instead of IRC.

- Approximately 70% of spam is sent via botnets. (MessageLabs, October 2004 Monthly Report)

- Bots refute the common argument that “there’s nothing on my computer that anyone would want” (usually given as an excuse not to bother securing the system).

Malicious traffic comparison



Unique Infected IPs, week ending March 28, 2005:

Entire Internet (unique IPs within each category; a single IP may have multiple problems)

Spam	1819518	71%
Bots	356211	14%
Phatbot	229270	9%
Beagle3	95141	4%
Slammer	22976	1%
Proxy	11814	0%
Dameware	11428	0%
Nachi	5823	0%
Beagle	4339	0%
Scanners	2744	0%
Scan445	2090	0%
Dipnet	1435	0%
Blaster	910	0%
Mydoom	551	0%
Sinit	376	0%
Phishing	252	0%
Bruteforce	10	0%
Total	2564888	

Malicious traffic trends

Spam, viruses, phishing are growing. Possible drop in DoS attacks.

Percentage of email that is spam:

2002: 9%. 2003: 40%. 2004: 73%. (received by GLBC Apr 2004-Mar 2005: 73%)

Percentage of email containing viruses:

2002: 0.5%. 2003: 3%. 2004: 6.1%. (received by GLBC Apr 2004-Mar 2005: 5%)

Number of phishing emails:

Total through September 2003: 273

Total through September 2004: >2 million

Monthly since September 2004: 2-5 million

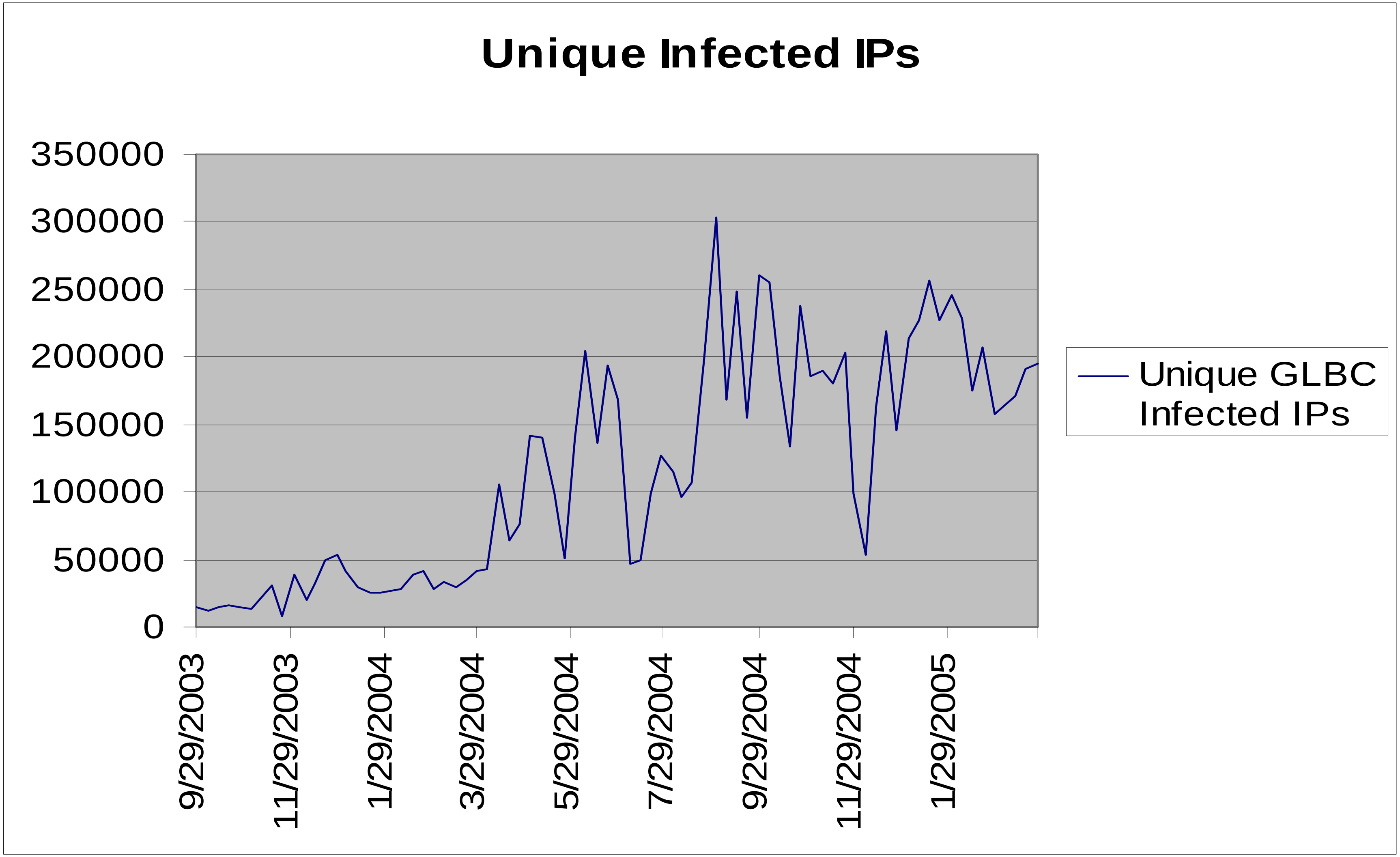
(Above from MessageLabs 2004 end-of-year report.)

Denial of Service Attacks (reported):

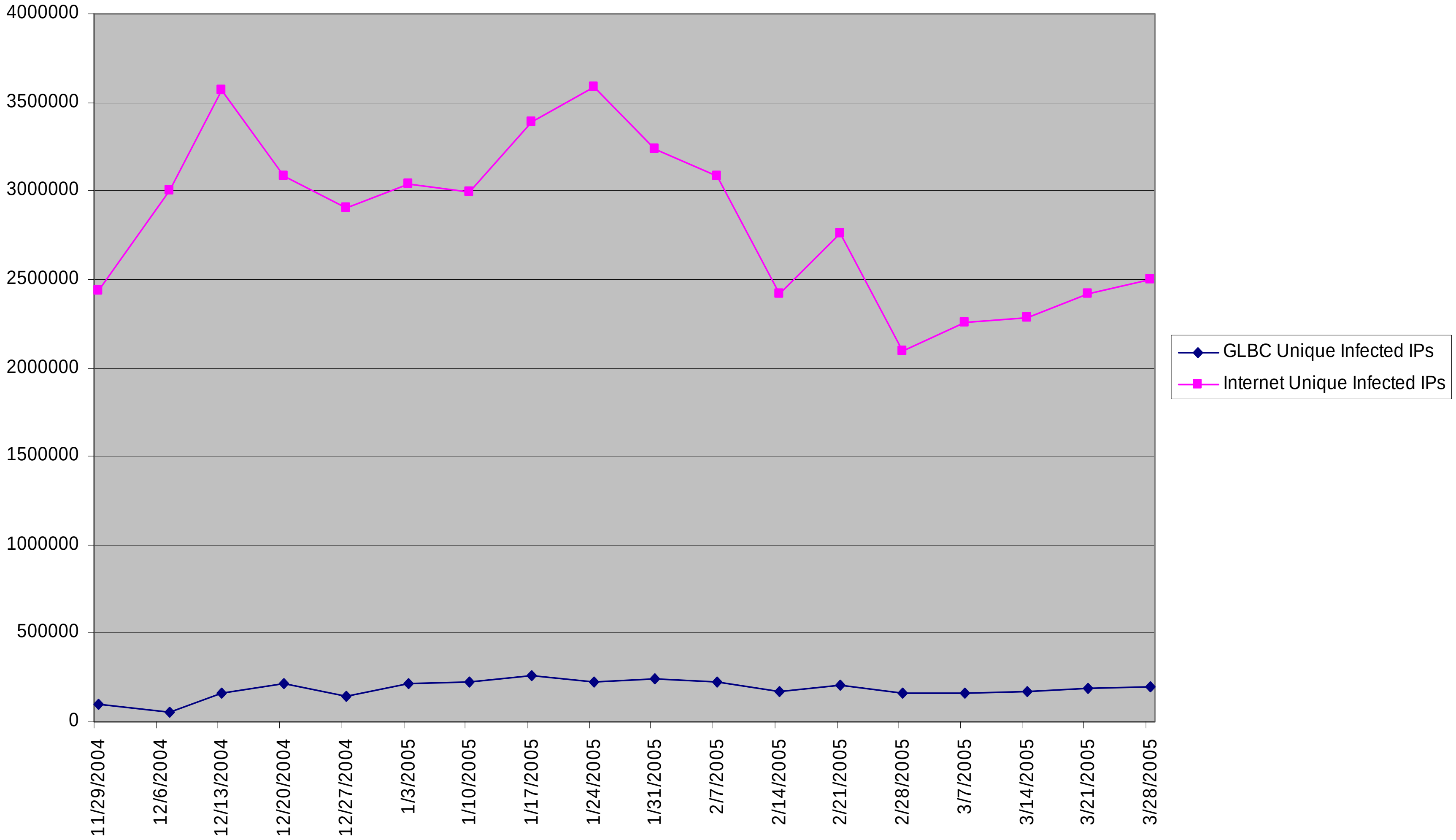
2002: 48 (16/mo). 2003: 409 (34/mo). 2004: 482 (40/mo). Jan. 1-Mar. 23, 2005: 74 (25/mo).

(Above from Global Crossing; 2002 is for Oct-Dec only.)

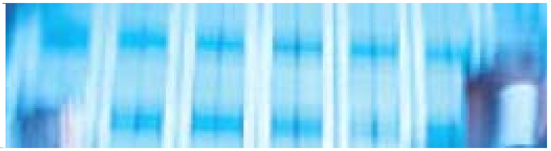
GLBC downstream malware-infected hosts



Infected hosts: Internet/GLBC downstreams



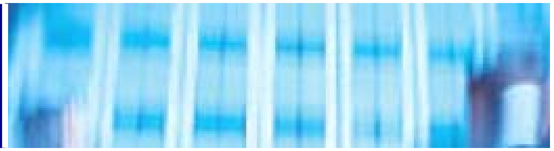
GLBC Infected Downstreams



Distribution by region for week ending March 28, 2005; unique infected IPs on AS's with more than 300 infected IPs, which accounts for 91% of unique infected IPs for the week.

Total	203521	
IPs for AS w/>300	184586	
Europe	66832	36%
South America	65516	35%
Asia	46592	25%
U.S.	5646	3%

Money is the main driver



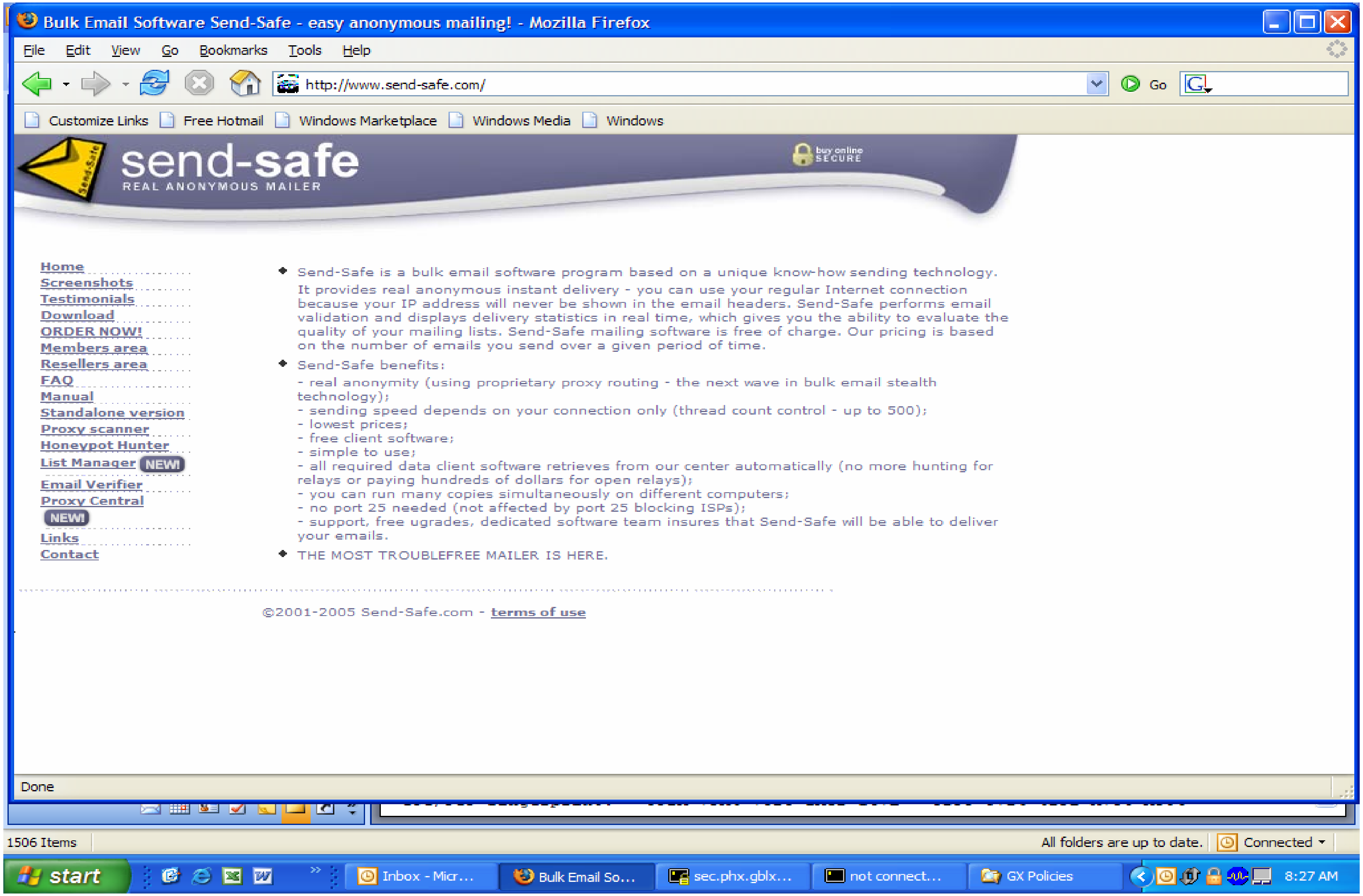
Most botnet-related abuse is driven by financial considerations:

•Viruses and worms are used to compromise systems to use as bots.

•Bots are used to send spam to sell products and services (often fraudulent), engage in extortion (denial of service against online gambling, credit card processors, etc.), send phishing emails to steal bank account access.

•Access to bots as proxies (“peas”) is sold to spammers, often with a very commercial-looking front end web interface.

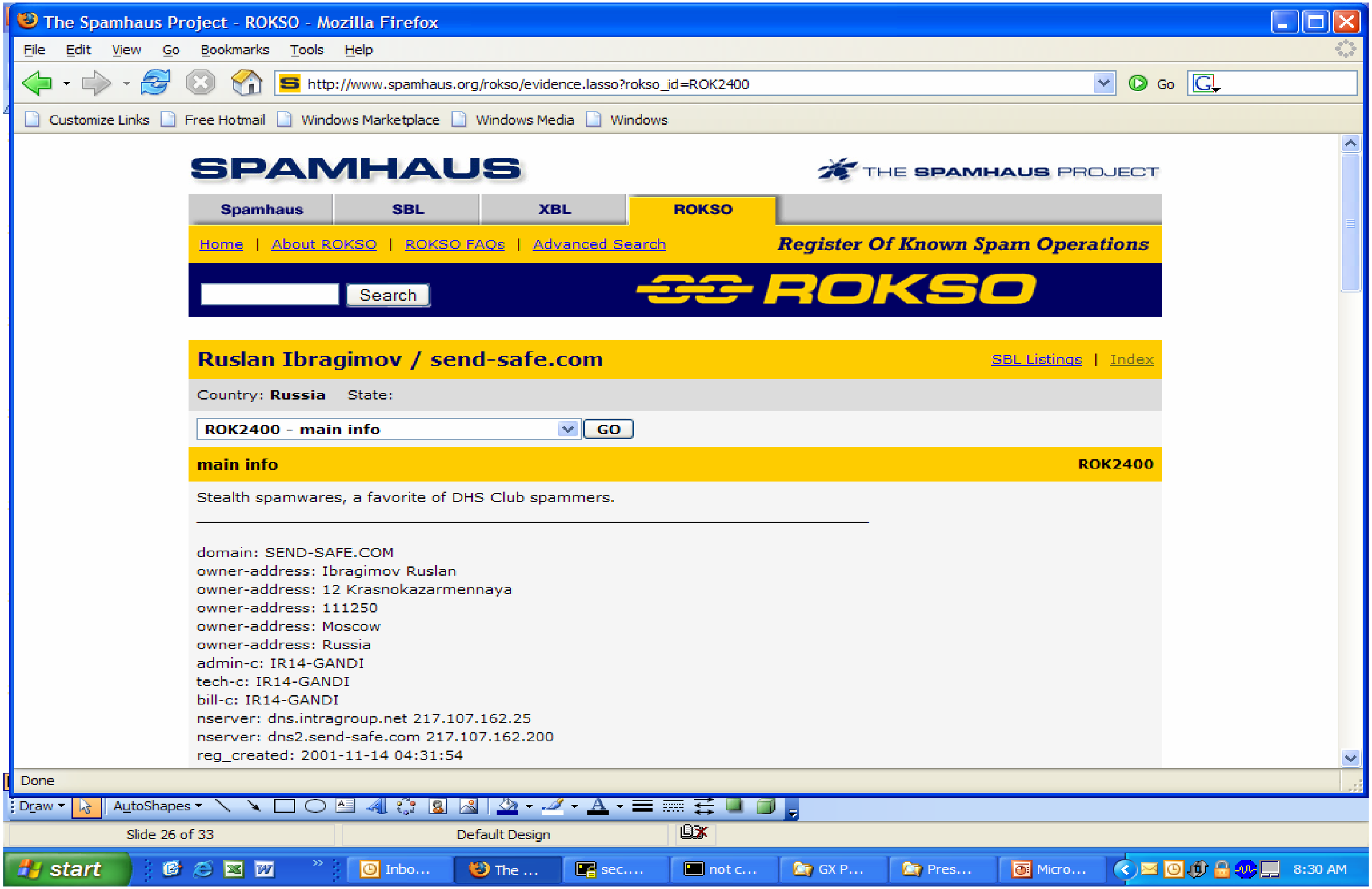
Ruslan Ibragimov/send-safe.com



- Send-Safe is a bulk email software program based on a unique know-how sending technology. It provides real anonymous instant delivery - you can use your regular Internet connection because your IP address will never be shown in the email headers. Send-Safe performs email validation and displays delivery statistics in real time, which gives you the ability to evaluate the quality of your mailing lists. Send-Safe mailing software is free of charge. Our pricing is based on the number of emails you send over a given period of time.
- Send-Safe benefits:
  - real anonymity (using proprietary proxy routing - the next wave in bulk email stealth technology);
  - sending speed depends on your connection only (thread count control - up to 500);
  - lowest prices;
  - free client software;
  - simple to use;
  - all required data client software retrieves from our center automatically (no more hunting for relays or paying hundreds of dollars for open relays);
  - you can run many copies simultaneously on different computers;
  - no port 25 needed (not affected by port 25 blocking ISPs);
  - support, free ugrades, dedicated software team insures that Send-Safe will be able to deliver your emails.
- THE MOST TROUBLEFREE MAILER IS HERE.

©2001-2005 Send-Safe.com - terms of use

Ruslan Ibragimov – ROKSO Record



Ruslan Ibragimov / send-safe.com

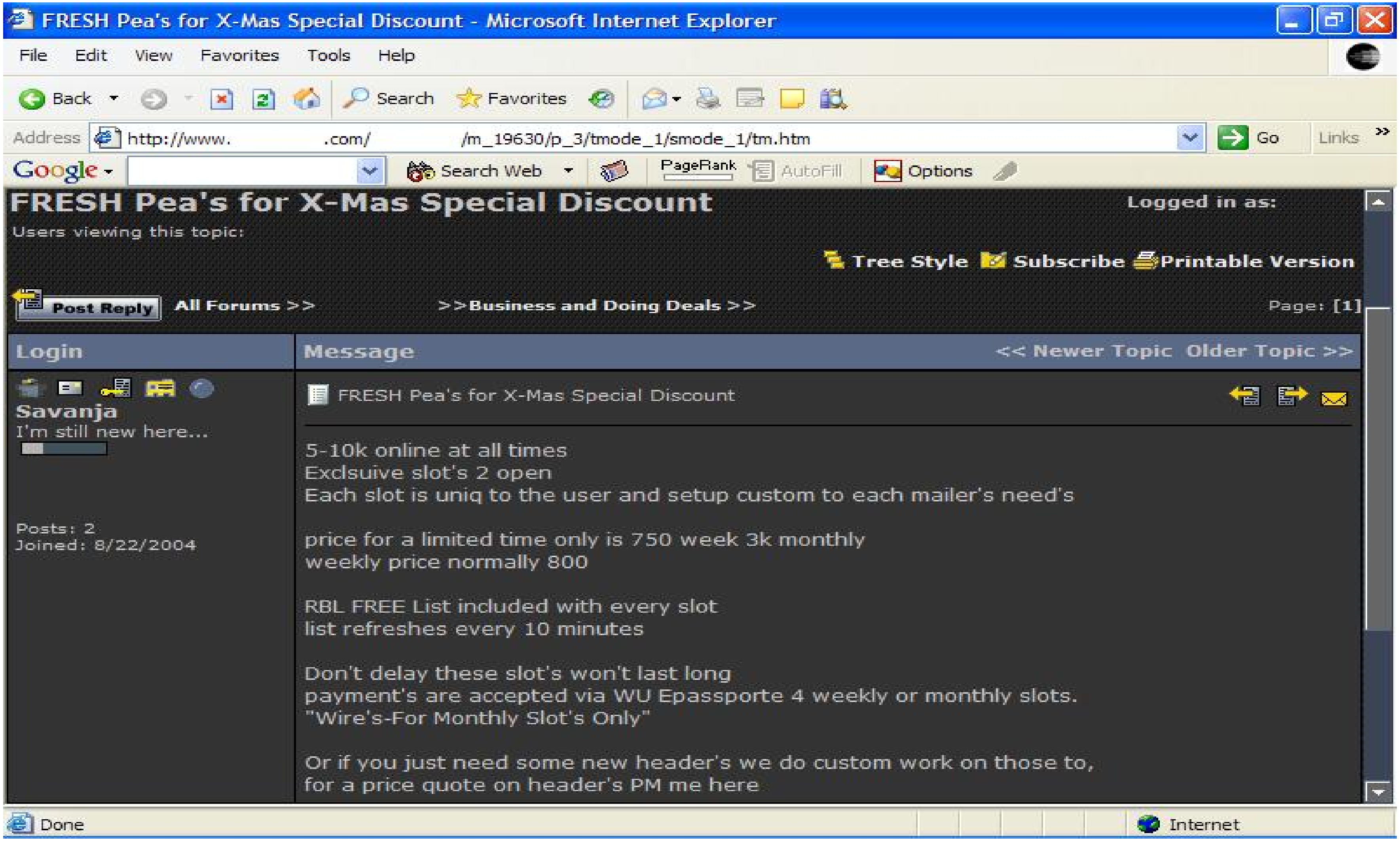
Country: **Russia** State:

main info ROK2400

Stealth spamwares, a favorite of DHS Club spammers.

```
domain: SEND-SAFE.COM
owner-address: Ibragimov Ruslan
owner-address: 12 Krasnokazarmennaya
owner-address: 111250
owner-address: Moscow
owner-address: Russia
admin-c: IR14-GANDI
tech-c: IR14-GANDI
bill-c: IR14-GANDI
nserver: dns.intragroup.net 217.107.162.25
nserver: dns2.send-safe.com 217.107.162.200
reg_created: 2001-11-14 04:31:54
```

“FRESH Pea’s for X-Mas Special Discount”


FRESH Pea's for X-Mas Special Discount - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.   .com/   /m_19630/p_3/tmode_1/smode_1/tm.htm
Go Links
Google Search Web PageRank AutoFill Options
Logged in as:
Users viewing this topic:
Tree Style Subscribe Printable Version
Post Reply
All Forums >>
>>Business and Doing Deals >>
Page: [1]
Login
Message
<< Newer Topic Older Topic >>
Done
Internet

FRESH Pea's for X-Mas Special Discount

Savanja
I'm still new here...

Posts: 2
Joined: 8/22/2004

FRESH Pea's for X-Mas Special Discount

5-10k online at all times
Exclsuive slot's 2 open
Each slot is uniq to the user and setup custom to each mailer's need's

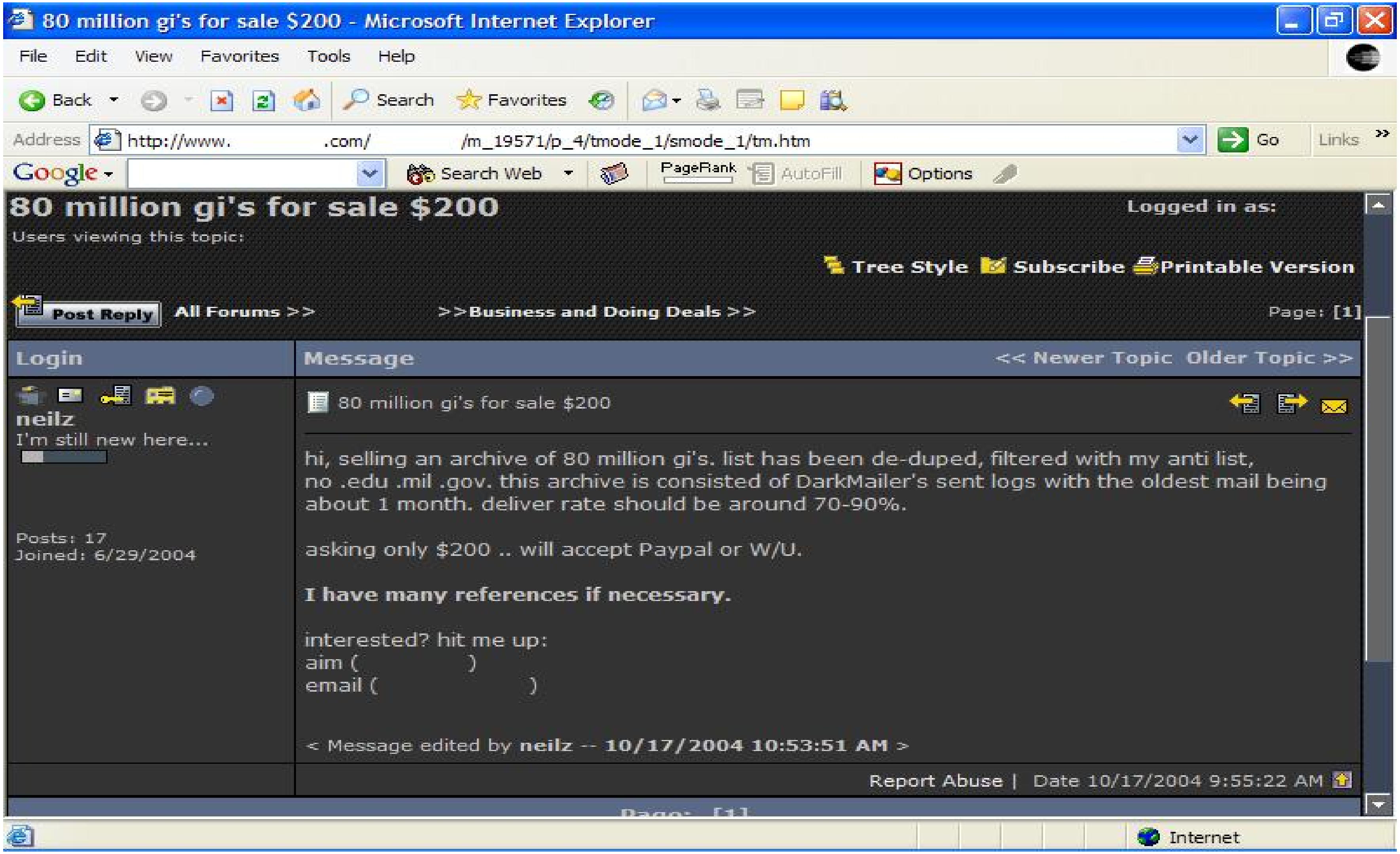
price for a limited time only is 750 week 3k monthly
weekly price normally 800

RBL FREE List included with every slot
list refreshes every 10 minutes

Don't delay these slot's won't last long
payment's are accepted via WU Epassporte 4 weekly or monthly slots.
"Wire's-For Monthly Slot's Only"

Or if you just need some new header's we do custom work on those to,
for a price quote on header's PM me here

General Interest emails for sale


80 million gi's for sale $200 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www. .com/ /m_19571/p_4/tmode_1/smode_1/tm.htm
Go Links
Google Search Web PageRank AutoFill Options
Internet

80 million gi's for sale $200

Logged in as:

Users viewing this topic:

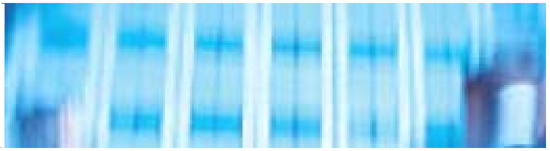
Tree Style Subscribe Printable Version

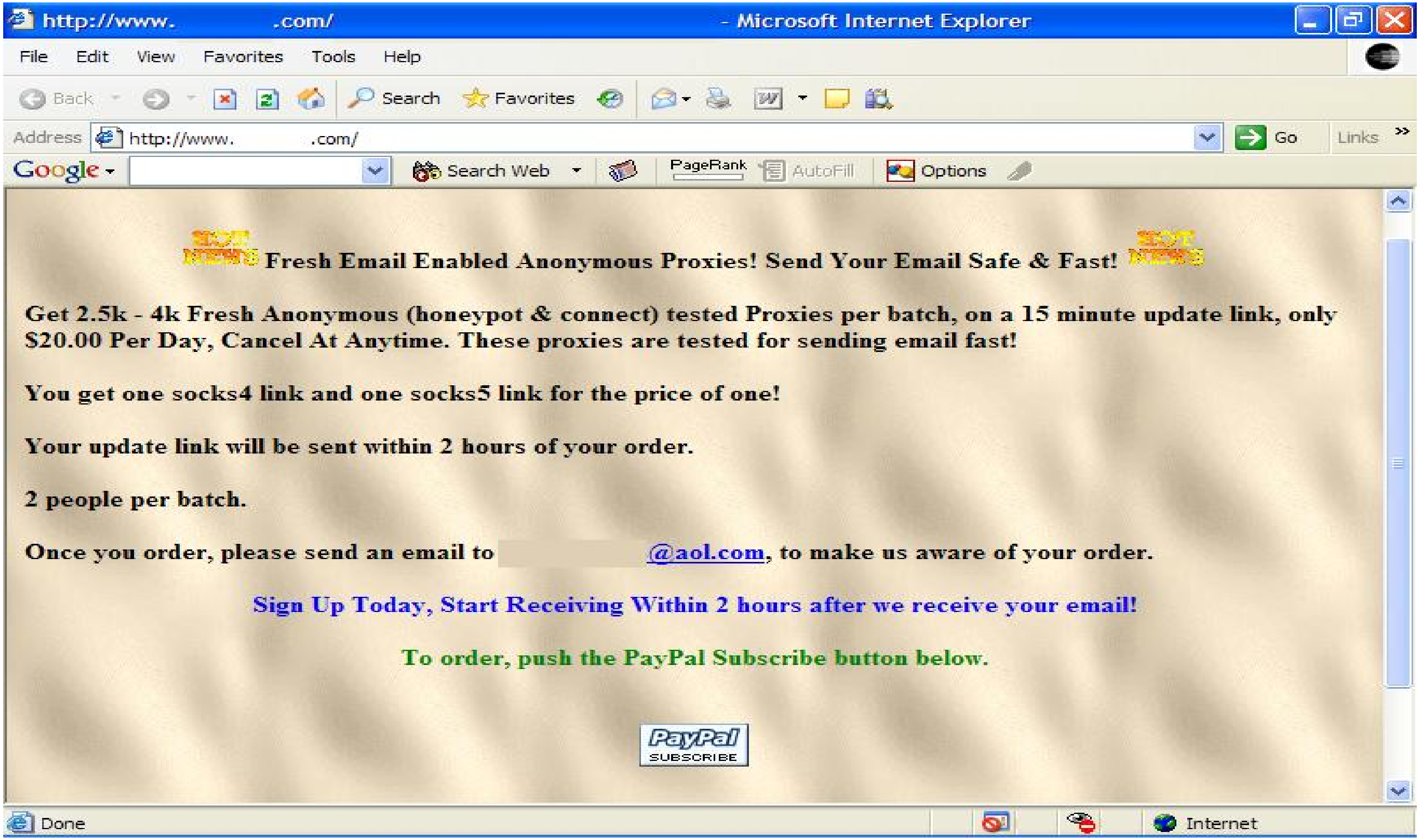
Post Reply All Forums >> >>Business and Doing Deals >> Page: [1]

Login	Message << Newer Topic Older Topic >>
neilz I'm still new here... Posts: 17 Joined: 6/29/2004	80 million gi's for sale $200 hi, selling an archive of 80 million gi's. list has been de-duped, filtered with my anti list, no .edu .mil .gov. this archive is consisted of DarkMailer's sent logs with the oldest mail being about 1 month. deliver rate should be around 70-90%. asking only $200 .. will accept Paypal or W/U. **I have many references if necessary.** interested? hit me up: aim ( ) email ( ) < Message edited by **neilz** -- **10/17/2004 10:53:51 AM** >
	Report Abuse | Date 10/17/2004 9:55:22 AM

Page: [1]

Proxies for Sale





HOT NEWS Fresh Email Enabled Anonymous Proxies! Send Your Email Safe & Fast! HOT NEWS

Get 2.5k - 4k Fresh Anonymous (honeypot & connect) tested Proxies per batch, on a 15 minute update link, only $20.00 Per Day, Cancel At Anytime. These proxies are tested for sending email fast!

You get one socks4 link and one socks5 link for the price of one!

Your update link will be sent within 2 hours of your order.

2 people per batch.

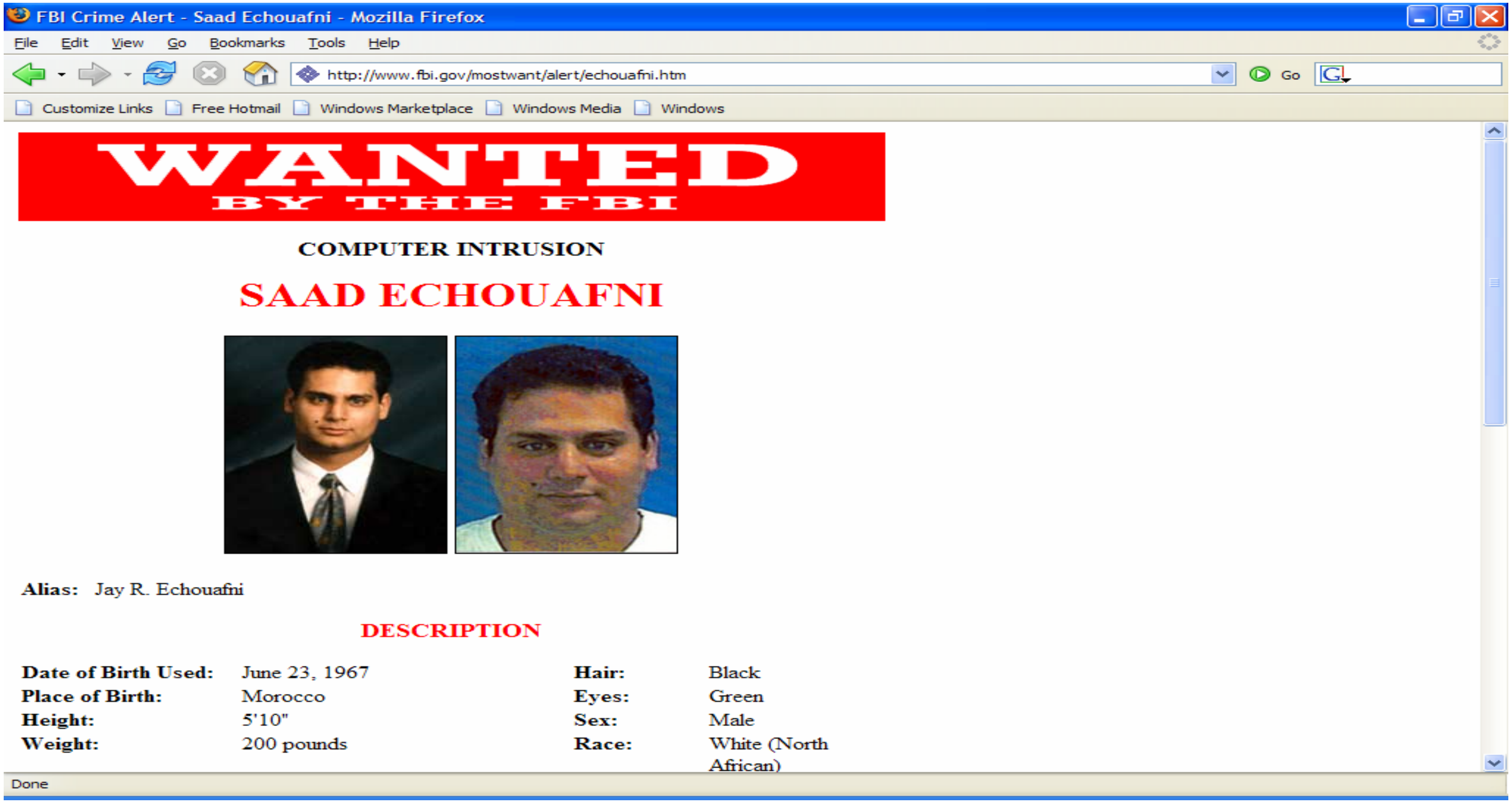
Once you order, please send an email to [redacted]@aol.com, to make us aware of your order.

Sign Up Today, Start Receiving Within 2 hours after we receive your email!

To order, push the PayPal Subscribe button below.

PayPal SUBSCRIBE

Jay Echouafni / Foonet



WANTED
BY THE FBI

COMPUTER INTRUSION

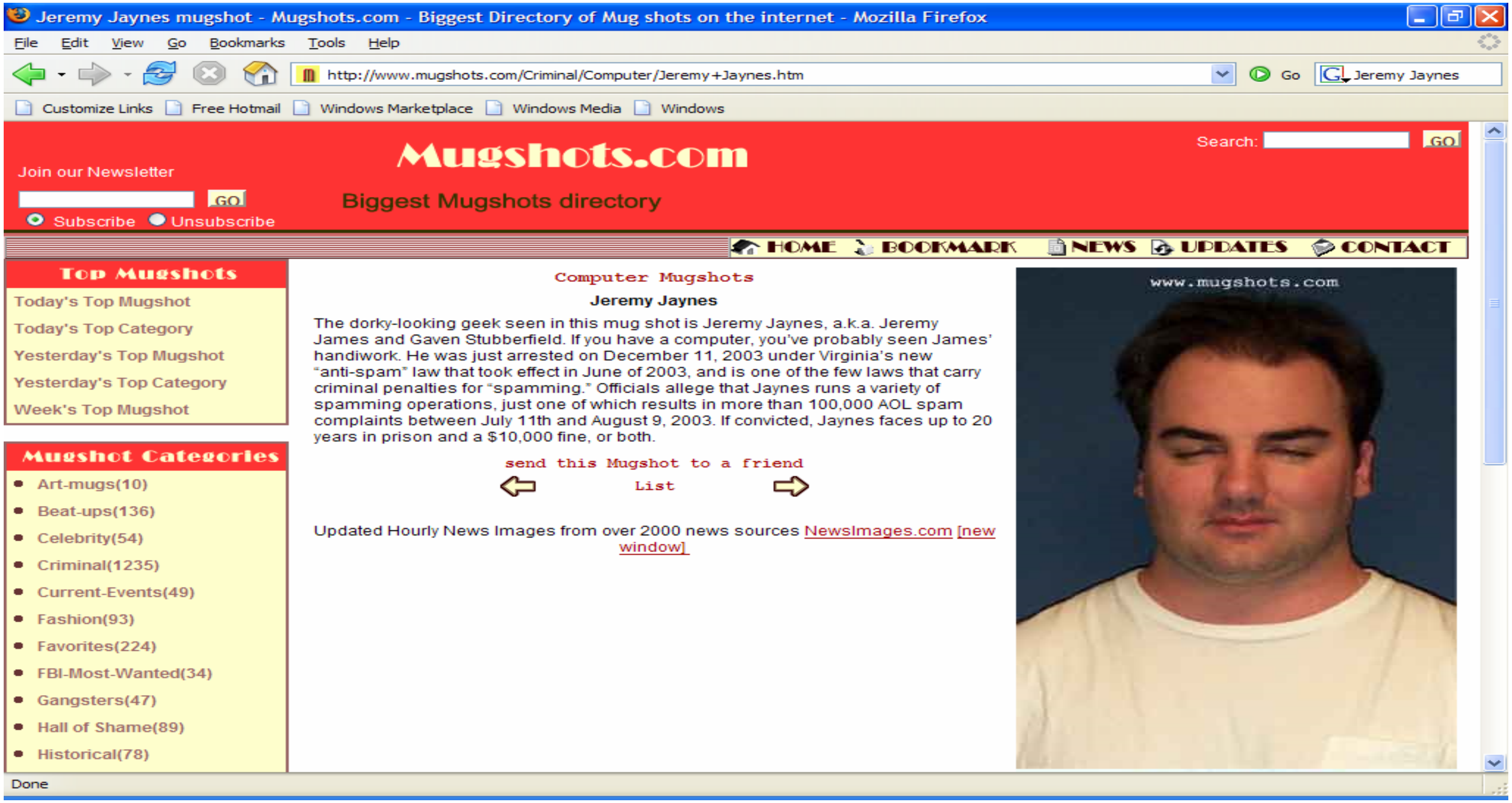
SAAD ECHOUAFNI

Alias: Jay R. Echouafni

DESCRIPTION

Date of Birth Used:	June 23, 1967	**Hair:**	Black
Place of Birth:	Morocco	**Eyes:**	Green
Height:	5'10"	**Sex:**	Male
Weight:	200 pounds	**Race:**	White (North African)

Jeremy Jaynes – 9 year prison sentence



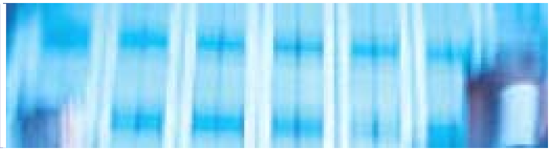
Computer Mugshots

Jeremy Jaynes

The dorky-looking geek seen in this mug shot is Jeremy Jaynes, a.k.a. Jeremy James and Gaven Stubberfield. If you have a computer, you've probably seen James' handiwork. He was just arrested on December 11, 2003 under Virginia's new "anti-spam" law that took effect in June of 2003, and is one of the few laws that carry criminal penalties for "spamming." Officials allege that Jaynes runs a variety of spamming operations, just one of which results in more than 100,000 AOL spam complaints between July 11th and August 9, 2003. If convicted, Jaynes faces up to 20 years in prison and a $10,000 fine, or both.

Updated Hourly News Images from over 2000 news sources NewsImages.com [new window]

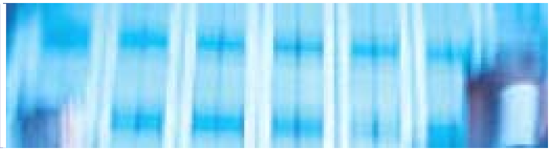
Other miscreants



Others:

- **Howard Carmack, the Buffalo spammer: $16 million judgment for Earthlink, 3.5-7 years on criminal charges from NY AG.**
- **Jennifer Murray, Ft. Worth spamming grandmother, arrested and extradited to VA.**
- **Ryan Pitylak, UT Austin philosophy student, sued by Texas AG.**
- **200+ spam lawsuits filed in 2004 by Microsoft (Glenn Hannifin, etc.)**
- **Robert Kramer/CIS Internet lawsuit in Iowa: $1 billion judgment.**
- **Long list of names at the Registry of Known Spam Operations (ROKSO): http://www.spamhaus.org**

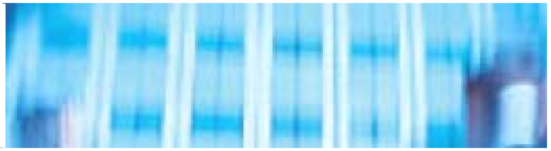
Weak points in need of defense



Weak points being exploited:

- **ISPs not vetting/screening customers—spammers set up shop in colo spaces at carriers worldwide.**
- **Poorly secured end user machines with high-bandwidth connections.**
- **Organizations failing to secure their networks and servers.**
- **NSPs/ISPs not monitoring for malicious traffic, not being aggressive to terminate abusers—spammers operating for months or years on major carriers sending proxy spam.**
- **Law enforcement not having the right resources or information to catch/prosecute offenders.**

Defense and attack strategies for NSPs/ISPs



- Screen prospective customers against ROKSO and other publicly available information sources.

- Strengthen AUPs and contracts to allow rapid removal of miscreants (and filtering or nullrouting of specific problems prior to termination).

- Secure company end-user machines with endpoint security.

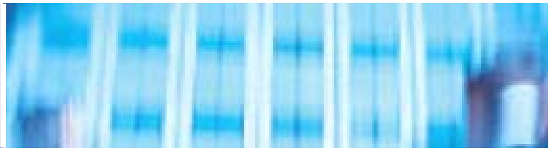
- Monitor for malicious traffic (or interact with security researchers or upstreams who monitor); notify downstreams and escalate if they fail to act.

- Filter and terminate abusers.

- Nullroute bot controllers and phishing websites.

- Collect actionable intelligence and notify law enforcement.

Global Crossing’s implementation



External customer-facing components

- **AUP provisions**

Global Crossing reserves the right to deny or terminate service to a Customer based upon the results of a security/abuse confirmation process used by Global Crossing. Such confirmation process uses publicly available information to primarily examine Customer's history in relation to its prior or current use of services similar to those being provided by Global Crossing and Customer's relationship with previous providers.

If a Customer has been listed on an industry-recognized spam abuse list, such Customer will be deemed to be in violation of Global Crossing's Acceptable Use Policy.

- **Customer screening**

Policy Enforcement/Compliance department reviews new orders for known publicly reported abuse incidents, suspicious contact information (e.g., commercial mail drops, free email addresses, cell phone as only contact).

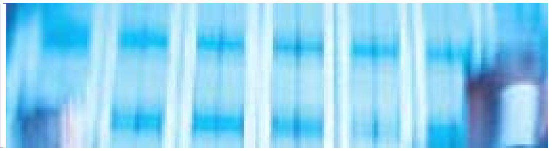
- **Network monitoring and customer notification**

We use Arbor Peakflow to detect and mitigate DoS attacks and engage in regular information exchange with peers and security researchers. We have automated processes for sending daily reports to customers of detected issues.

- **Regular review of spam block lists and taking action**

Reduced Spamhaus SBL listings from 43 in January 2004 to 6 at end of 2004. Currently (25 March 2005) at 11; several removal actions in process.

Global Crossing’s implementation



- **Law enforcement interaction**

Participation in the FBI’s Operation Slam Spam, which has collected data since September 2003. We are hoping to see major prosecutions in 2005.

Internal components

- **Comprehensive Enterprise Security Program Plan (ESPP)**

Physical and Information Security merged into single organization; reports directly to Security Committee of corporate board of directors under Network Security Agreement with U.S. government agencies (a public document obtainable at www.fcc.gov).

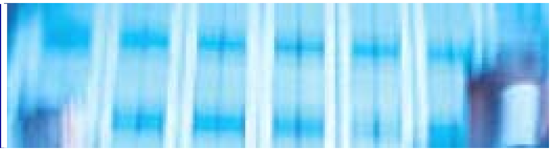
- **Endpoint security**

Sygate Enforcer at corporate VPN access points; Sygate Agent on all corporate laptops (and being deployed to all corporate workstations). Sygate Agent acts as PC firewall, IDS, file integrity checker, and enforces compliance on patch levels and anti-virus patterns; it reports back to a central management station. The IDS functionality makes every individual’s machine into an IDS sensor.

- **Antispam/antivirus**

Corporate mail servers use open source SpamAssassin plus Trend Micro VirusWall.

Future Plans



- **Partially automated escalation**

Automated testing of botnet controllers and phishing websites; ticket generation, customer notification, nullrouting (with human intervention step).

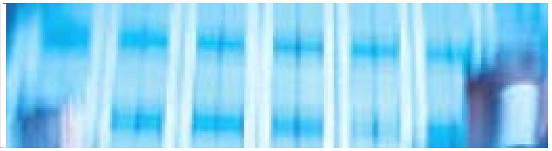
- **More creative monitoring and analysis of Netflow data**

To automate detection of proxy spamming and botnet activity.

- **More creative monitoring and analysis of DNS queries**

To spot cache poisoning and “pharming” attacks, detection of bots by DNS lookups of botnet controllers; possibly use passive DNS replication to view historical data or find FQDNs associated with botnet controllers where the IP has no rDNS.

Help wanted



Peers:

Similar implementations: screen customers, strengthen and enforce AUPs, nullroute botnet controllers and phishing websites. Share additional ideas; coordination of defenses.

OS/Application vendors:

More securely written software, with secure-by-default configurations. Automated, digitally-signed update capability, turned on by default for home users.

ISPs with end user customers:

Better filtering/quarantining of infected customer systems—automation and self-service point-and-click tools needed. Any solution that requires end users to become expert system administrators is doomed to failure.

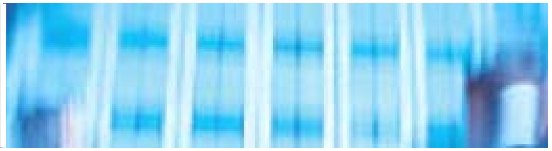
Organizations on the Internet:

Use firewalls and endpoint security solutions, use spam and anti-virus filtering. Block email from known infected systems using the Composite Blocking List (CBL), cbl.abuseat.org.

Law enforcement and prosecutors:

Undercover investigations to follow the money and capture the criminals profiting from spam, phishing, denial of service, and the use of botnets. Follow up civil litigation from large providers like AOL, Earthlink, and Microsoft with criminal charges.

Conclusion



An effective response to botnets, spam, phishing, and denial of service requires a combination of policies and procedures, technology, and legal responses from network providers, ISPs, organizations on the Internet, and law enforcement and prosecutors. All of these components need to respond and change as the threats continue to evolve.

Further Information

Composite Blocking List: http://cbl.abuseat.org

Registry Of Known Spam Operations (ROKSO): http://www.spamhaus.org

Bot information: http://www.lurhq.com/research.html

http://www.honeynet.org/papers/bots/

Message Labs 2004 end-of-year report:

http://www.messagelabs.com/binaries/LAB480_endofyear_v2.pdf

CAIDA Network Telescope: http://www.caida.org/analysis/security/telescope/

Team Cymru DarkNet: http://www.cymru.com/Darknet/

Internet Motion Sensor: http://ims.eecs.umich.edu/

Passive DNS Replication: http://cert.uni-stuttgart.de/stats/dns-replication.php

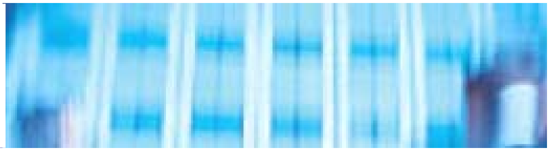
Brian McWilliams, *Spam Kings*, 2004, O’Reilly and Associates.

Spammer-X, *Inside the Spam Cartel*, 2004, Syngress. (Read but don’t buy.)

Jim Lippard

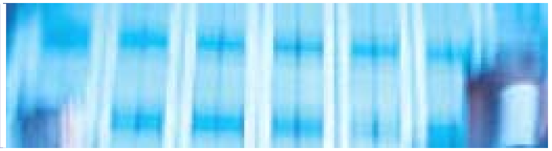
james.lippard@globalcrossing.com

Appendix: Global Crossing notifications



```
The following is a list of IP addresses on your network which we have
good reason to believe may be compromised systems engaging in
malicious activity.  Please investigate and take appropriate action to
stop any malicious activity you verify.

The following is a list of types of activity that may appear in this
report:
    BEAGLE     BEAGLE3    BLASTER    BOTNETS    BOTS       BRUTEFORCE
    DAMEWARE   DIPNET     DNSBOTS    MYDOOM     NACHI      PHATBOT
    PHISHING   SCAN445    SINIT      SLAMMER    SPAM

Open proxies and open mail relays may also appear in this report.
Open proxies are designated by a two-character identifier (s4, s5, wg,
hc, ho, hu, or fu) followed by a colon and a TCP port number.  Open
mail relays are designated by the word "relay" followed by a colon and
a TCP port number.

A detailed description of each of these may be found at
   https://security.gblx.net/reports.html

NOTE: IPs identified as hosting botnet controllers or phishing
websites (marked with BOTNETS or PHISHING, respectively) may be null
routed by Global Crossing following a separately emailed notice.

This report is sent on weekdays, Monday through Friday.  If you would
prefer a weekly report, sent on Mondays, please contact us by replying
to this email to request it.  We would prefer, however, that you
receive and act upon these reports daily.

Unless otherwise indicated, timestamps are in UTC (GMT).

3549 | 208.50.20.164/32 | 2005-01-10 23:23:36 BOTNETS | GBLX Global Crossing Ltd.
3549 | 209.130.174.106/32 | 2005-02-03 15:58:06 tokeat.4two0.com TCP 13222 BOTNETS | GBLX Global Crossing Ltd.
3549 | 146.82.109.130 | 2005-03-24 10:01:30 BEAGLE3 | GBLX Global Crossing Ltd.
3549 | 195.166.97.130 | 2005-03-24 08:40:03 SPAM | GBLX Global Crossing Ltd.
3549 | 206.132.221.37 | 2005-03-24 01:56:13 PHATBOT | GBLX Global Crossing Ltd.
3549 | 206.132.93.5 | 2005-03-23 22:13:40 NACHI | GBLX Global Crossing Ltd.
3549 | 206.165.142.184 | 2005-03-23 09:35:53 SLAMMER | GBLX Global Crossing Ltd.
3549 | 206.165.192.5 | 2005-03-24 12:35:53 SPAM | GBLX Global Crossing Ltd.
```

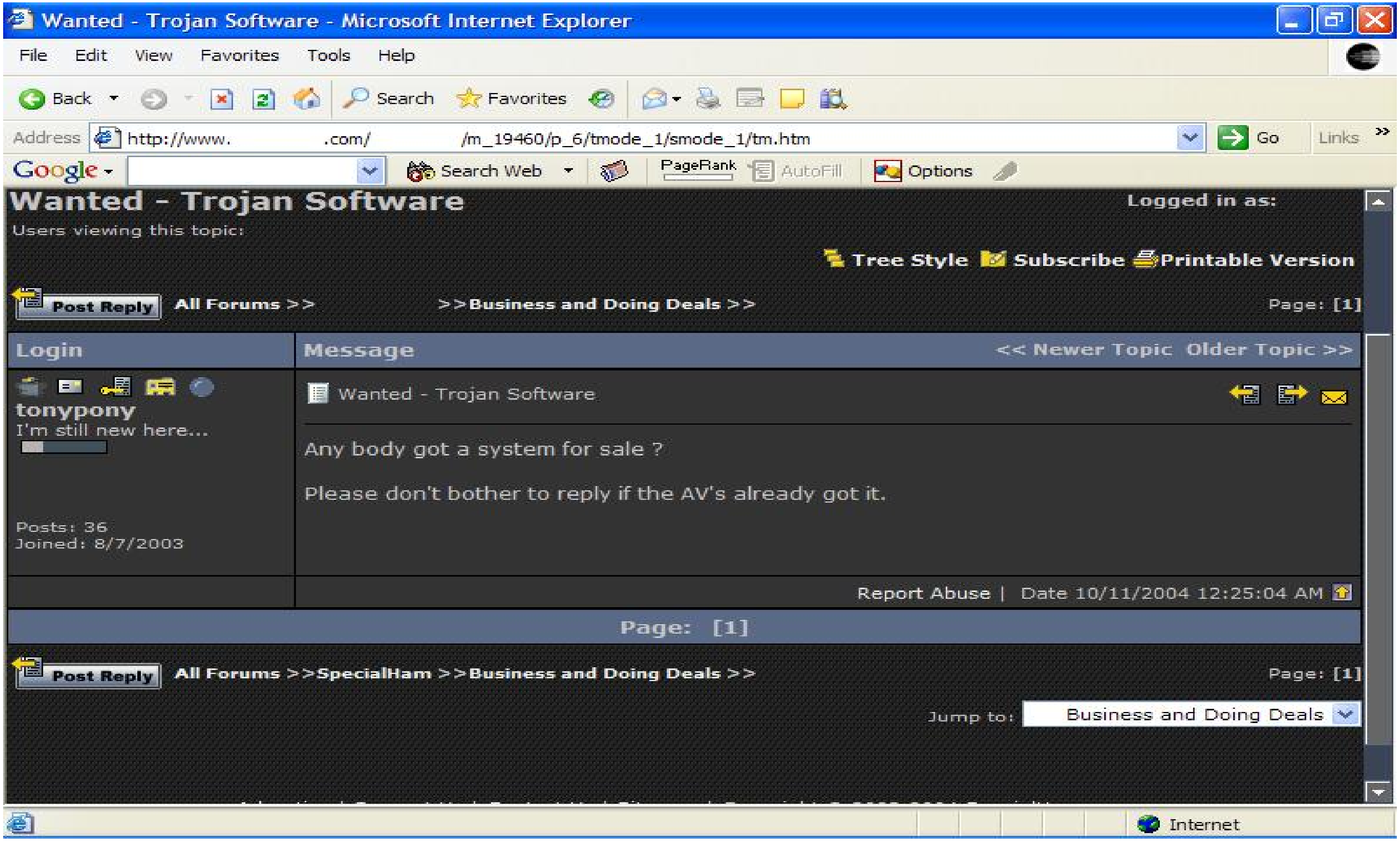
Appendix: Phatbot functionality



Phatbot command list (from LURHQ)

bot.command runs a command with system()
bot.unsecure enable shares / enable dcom
bot.secure delete shares / disable dcom
bot.flushdns flushes the bots dns cache
bot.quit quits the bot
bot.longuptime If uptime > 7 days then bot will respond
bot.sysinfo displays the system info
bot.status gives status
ot.rndnick makes the bot generate a new random nick
bot.removeallbut removes the bot if id does not match
bot.remove removes the bot
bot.open opens a file (whatever)
bot.nick changes the nickname of the bot
bot.id displays the id of the current code
bot.execute makes the bot execute a .exe
bot.dns resolves ip/hostname by dns
bot.die terminates the bot
bot.about displays the info the author wants you to see
shell.disable Disable shell handler
shell.enable Enable shell handler
shell.handler FallBack handler for shell
commands.list Lists all available commands
plugin.unload unloads a plugin (not supported yet)
plugin.load loads a plugin
cvar.saveconfig saves config to a file
cvar.loadconfig loads config from a file
cvar.set sets the content of a cvar
cvar.get gets the content of a cvar
cvar.list prints a list of all cvars
inst.svcdel deletes a service from scm
inst.svcadd adds a service to scm
inst.asdel deletes an autostart entry
inst.asadd adds an autostart entry
logic.ifuptime exec command if uptime is bigger than specified
mac.login logs the user in
mac.logout logs the user out
ftp.update executes a file from a ftp url
ftp.execute updates the bot from a ftp url
ftp.download downloads a file from ftp
http.visit visits an url with a specified referrer
http.update executes a file from a http url
http.execute updates the bot from a http url
http.download downloads a file from http
rsl.logoff logs the user off
rsl.shutdown shuts the computer down
rsl.reboot reboots the computer
pctrl.kill kills a process
pctrl.list lists all processes
scan.stop signal stop to child threads
scan.start signal start to child threads
scan.disable disables a scanner module
scan.enable enables a scanner module
scan.clearnetranges clears all netranges registered with the scanner
scan.resetnetranges resets netranges to the localhost
scan.listnetranges lists all netranges registered with the scanner
scan.delnetrange deletes a netrange from the scanner
scan.addnetrange adds a netrange to the scanner
ddos.phatwonk starts phatwonk flood
ddos.phaticmp starts phaticmp flood
ddos.phatsyn starts phatsyn flood
ddos.stop stops all floods
ddos.httpflood starts a HTTP flood
ddos.synflood starts an SYN flood
ddos.udpflood starts a UDP flood
redirect.stop stops all redirects running
redirect.socks starts a socks4 proxy
redirect.https starts a https proxy
redirect.http starts a http proxy
redirect.gre starts a gre redirect
redirect.tcp starts a tcp port redirect
harvest.aol makes the bot get aol stuff
harvest.cdkeys makes the bot get a list of cdkeys
harvest.emailshttp makes the bot get a list of emails via http
harvest.emails makes the bot get a list of emails
waste.server changes the server the bot connects to
waste.reconnect reconnects to the server
waste.raw sends a raw message to the waste server
waste.quit
waste.privmsg sends a privmsg
waste.part makes the bot part a channel
waste.netinfo prints netinfo
waste.mode lets the bot perform a mode change
waste.join makes the bot join a channel
waste.gethost prints netinfo when host matches
waste.getedu prints netinfo when the bot is .edu
waste.action lets the bot perform an action
waste.disconnect disconnects the bot from waste

Appendix: Trojan software wanted


Wanted - Trojan Software - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.   .com/   /m_19460/p_6/tmode_1/smode_1/tm.htm
Go Links
Google Search Web PageRank AutoFill Options
Internet

Wanted - Trojan Software

Logged in as:

Users viewing this topic:

Tree Style Subscribe Printable Version

Post Reply All Forums >> >>Business and Doing Deals >> Page: [1]

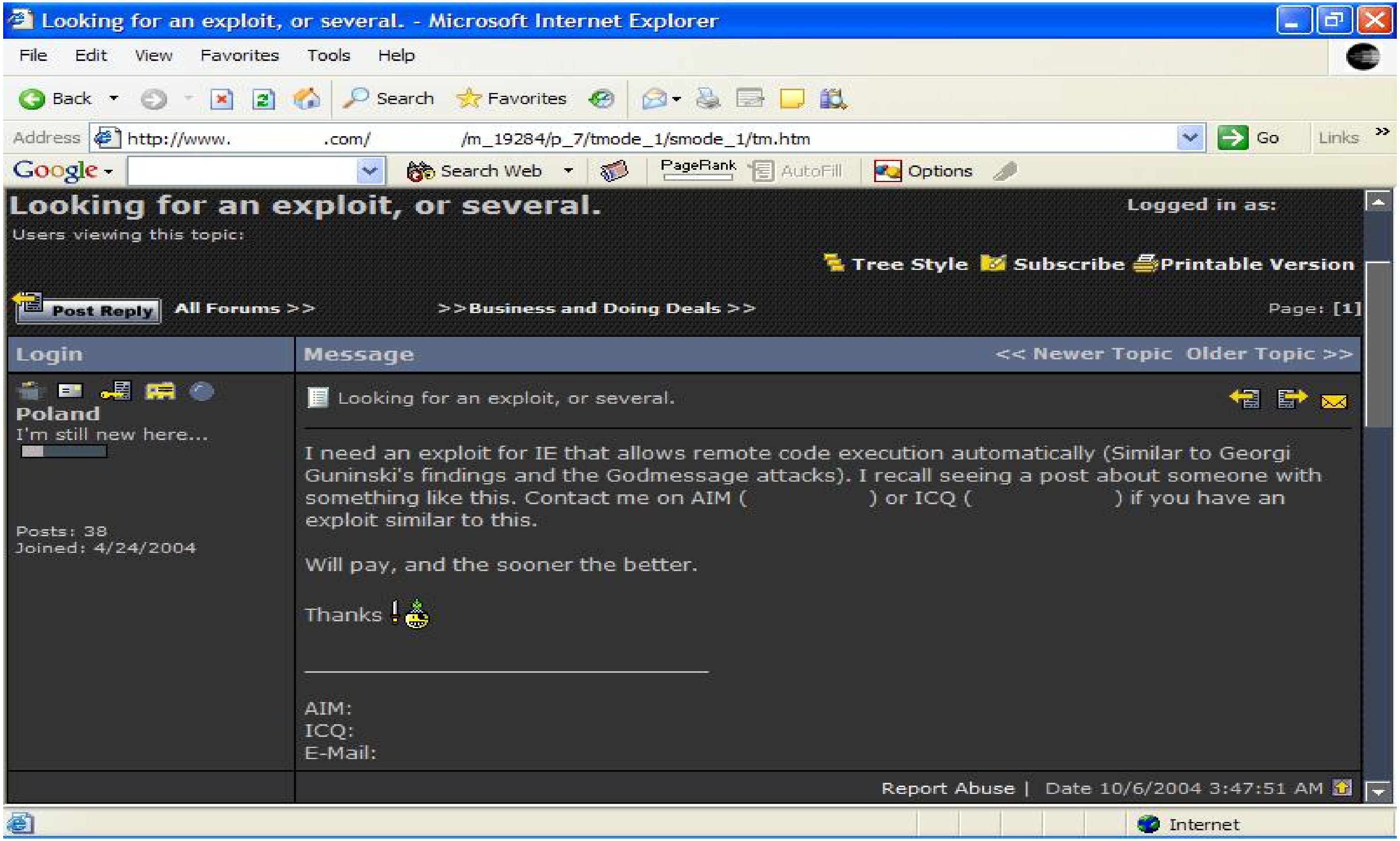
Login	Message << Newer Topic Older Topic >>
tonypony I'm still new here... Posts: 36 Joined: 8/7/2003	Wanted - Trojan Software Any body got a system for sale ? Please don't bother to reply if the AV's already got it.
	Report Abuse | Date 10/11/2004 12:25:04 AM

Page: [1]

Post Reply All Forums >>SpecialHam >>Business and Doing Deals >> Page: [1]

Jump to: Business and Doing Deals

Appendix: Looking for an Exploit



http://www.   .com/   /m_19284/p_7/tmode_1/smode_1/tm.htm

Looking for an exploit, or several.

Logged in as:

Users viewing this topic:

All Forums >>   >>Business and Doing Deals >>

Page: [1]

Poland
I'm still new here...

Posts: 38
Joined: 4/24/2004

Looking for an exploit, or several.

I need an exploit for IE that allows remote code execution automatically (Similar to Georgi Guninski's findings and the Godmessage attacks). I recall seeing a post about someone with something like this. Contact me on AIM (   ) or ICQ (   ) if you have an exploit similar to this.

Will pay, and the sooner the better.

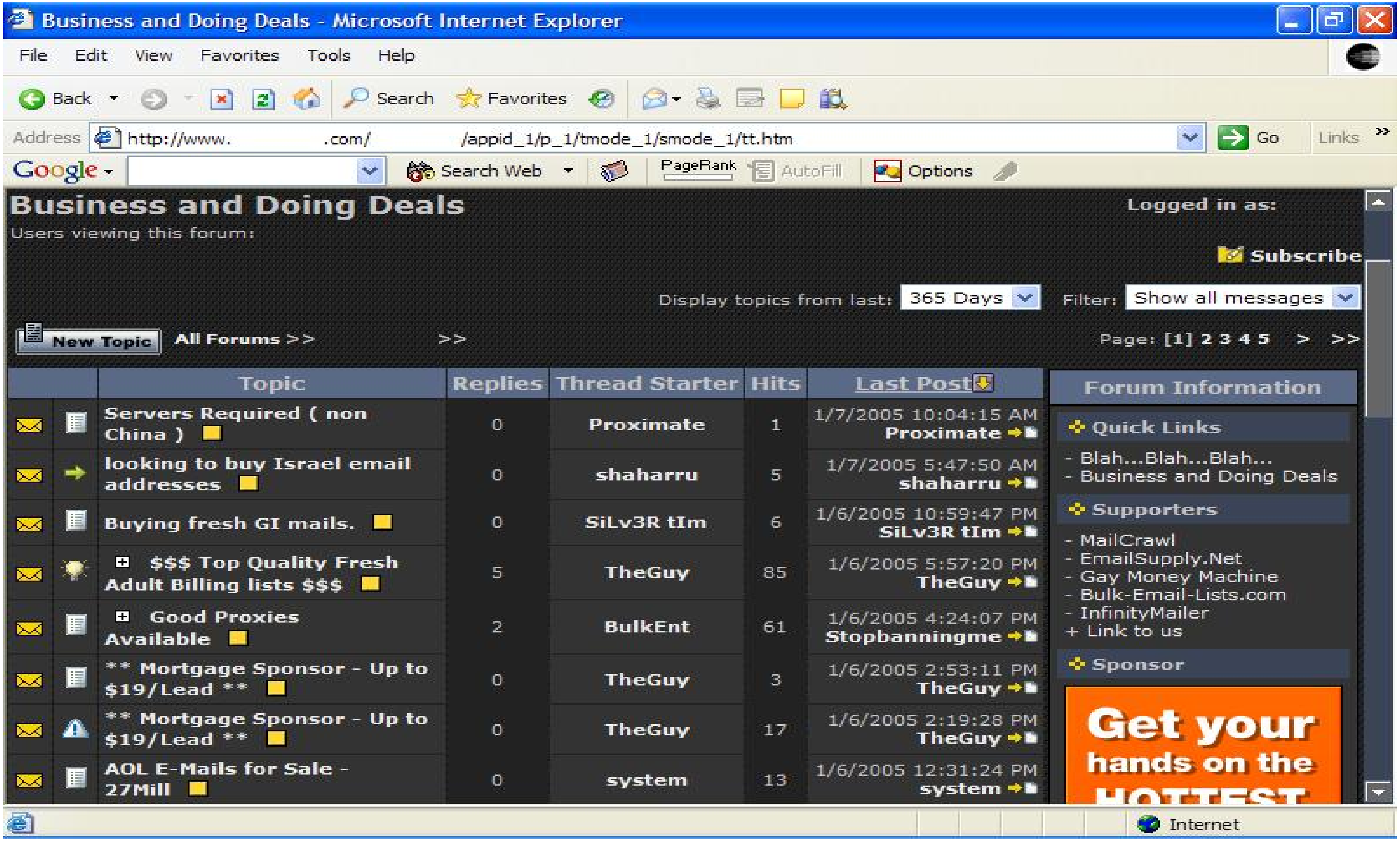
Thanks !

AIM:
ICQ:
E-Mail:

Report Abuse | Date 10/6/2004 3:47:51 AM

Global Crossing®

Appendix: Spammer Bulletin Board


Business and Doing Deals - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Address
http://www.   .com/   /appid_1/p_1/tmode_1/smode_1/tt.htm
Go
Links
Google
Search Web
PageRank
AutoFill
Options
Internet

Business and Doing Deals

Users viewing this forum:

Logged in as:

Subscribe

Display topics from last: 365 Days Filter: Show all messages

New Topic All Forums >> >>

Page: [1] 2 3 4 5 > >>

		Topic	Replies	Thread Starter	Hits	Last Post
		Servers Required (non China)	0	Proximate	1	1/7/2005 10:04:15 AM Proximate
		looking to buy Israel email addresses	0	shaharru	5	1/7/2005 5:47:50 AM shaharru
		Buying fresh GI mails.	0	SiLv3R tIm	6	1/6/2005 10:59:47 PM SiLv3R tIm
		$$$ Top Quality Fresh Adult Billing lists $$$	5	TheGuy	85	1/6/2005 5:57:20 PM TheGuy
		Good Proxies Available	2	BulkEnt	61	1/6/2005 4:24:07 PM Stopbanningme
		** Mortgage Sponsor - Up to $19/Lead **	0	TheGuy	3	1/6/2005 2:53:11 PM TheGuy
		** Mortgage Sponsor - Up to $19/Lead **	0	TheGuy	17	1/6/2005 2:19:28 PM TheGuy
		AOL E-Mails for Sale - 27Mill	0	system	13	1/6/2005 12:31:24 PM system

Forum Information

Quick Links

- Blah...Blah...Blah...
- Business and Doing Deals

Supporters

- MailCrawl
- EmailSupply.Net
- Gay Money Machine
- Bulk-Email-Lists.com
- InfinityMailer

+ Link to us

Sponsor

Get your hands on the HOTTEST