

The New Global Village



Defending Against Botnets

Jim Lippard, Director, Information Security Operations, Global Crossing

ASU Cyber Security Week

November 2, 2005

Agenda



1. **Evolution of botnets**
2. **What's the problem?**
3. **Current botnet ecology and life cycle**
4. **Why botnets?**
5. **Defense mechanisms: prevention, detection, response**
6. **What does the future hold?**

Evolution of botnets



Rise of the botnets

Botnets today

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 collections of compromised machines under the control of a single entity, usually via a single controlling host—a botnet controller.**
- **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.**
- **Other common bots: Korgobot, SpyBot, Optix Pro, rBot, SDBots, Toxbot.**
- **A majority of viruses contain backdoors/create botnets (MessageLabs, 2004 Annual Report). About 9% of spam is sent via botnets (MessageLabs, September 2005 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).**

What's the problem?



Malicious traffic trends

GLBC downstream malware-infected hosts

Internet-wide malware-infected hosts

GLBC downstream phishing websites

GLBC downstream botnet controllers

Malicious traffic trends



Drop in DoS attacks and email-based attacks other than phishing.

Percentage of email that is spam:

2002: 9%. 2003: 40%. 2004: 73%. 3Q 2005: 66.7%

Percentage of email containing viruses:

2002: 0.5%. 2003: 3%. 2004: 6.1%. 3Q 2005: 2.4%

Number of phishing emails:

Total through September 2003: 293

Total through September 2004: >2 million

Monthly since September 2004: 2-9.1 million

September 2005: 4.8 million

(Source: MessageLabs 2004 end-of-year report, September 2005 report.)

Denial of Service Attacks (reported):

2002: 48 (16/mo). 2003: 409 (34/mo). 2004: 482 (40/mo). Jan. 1-Oct. 28, 2005: 246 (25/mo). (1Q: 77—26/mo, 2Q: 64—21/mo, 3Q: 84—28/mo, Oct: 23)

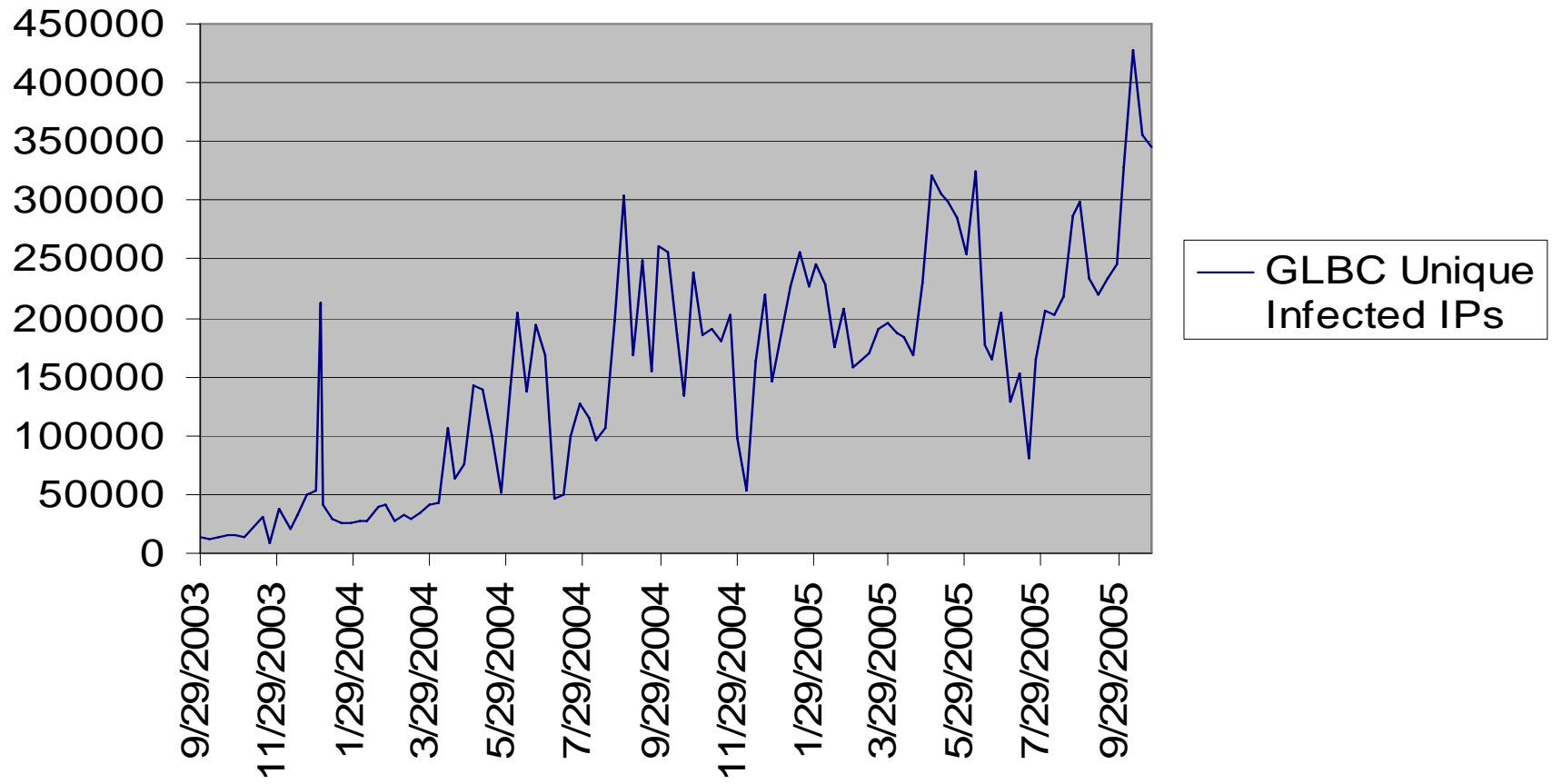
(2005 minus Sep's 40: 206—23/mo)

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

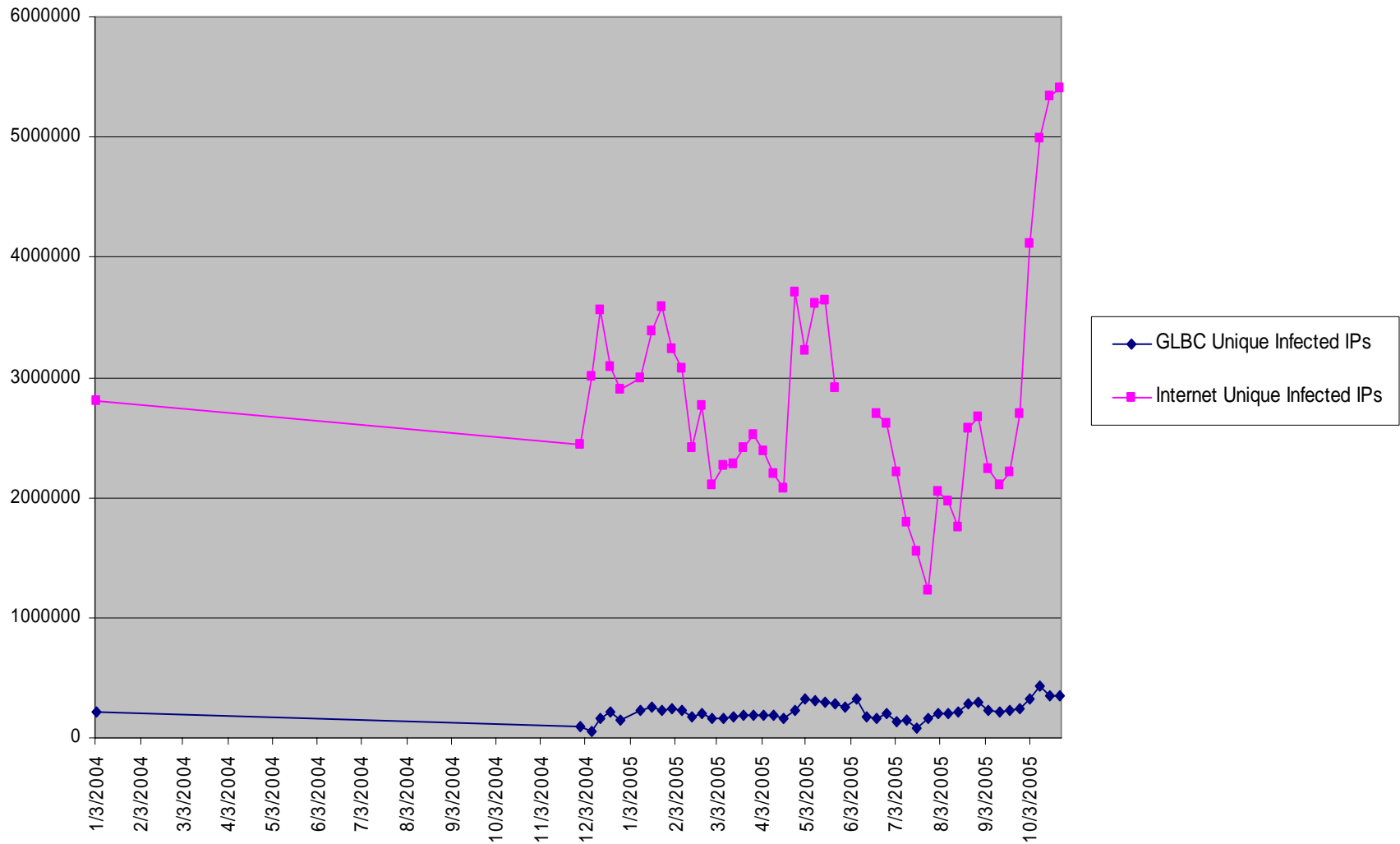
GLBC downstream malware-infected hosts (per week)



Unique Infected IPs



Infected hosts: Internet/GLBC downstreams (per week)



Phishing websites



Mar. 2005: 6

Apr. 2005: 22

May 2005: 25

Jun. 2005: 46

Jul. 2005: 213

Aug. 2005: 256

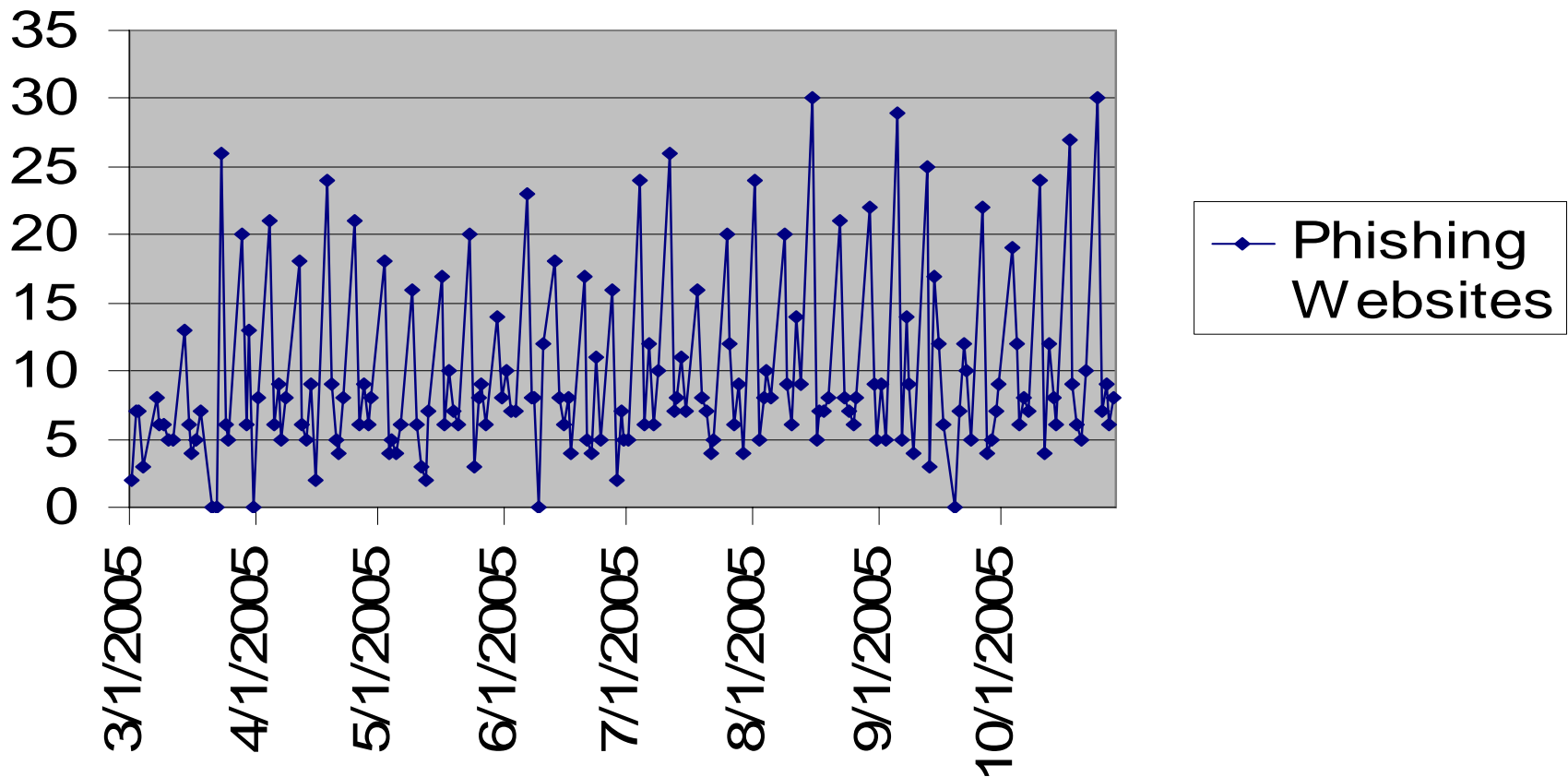
Sep. 2005: 219

Oct. (1-28) 2005: 223

Phishing websites downstream of AS 3549 (per day)



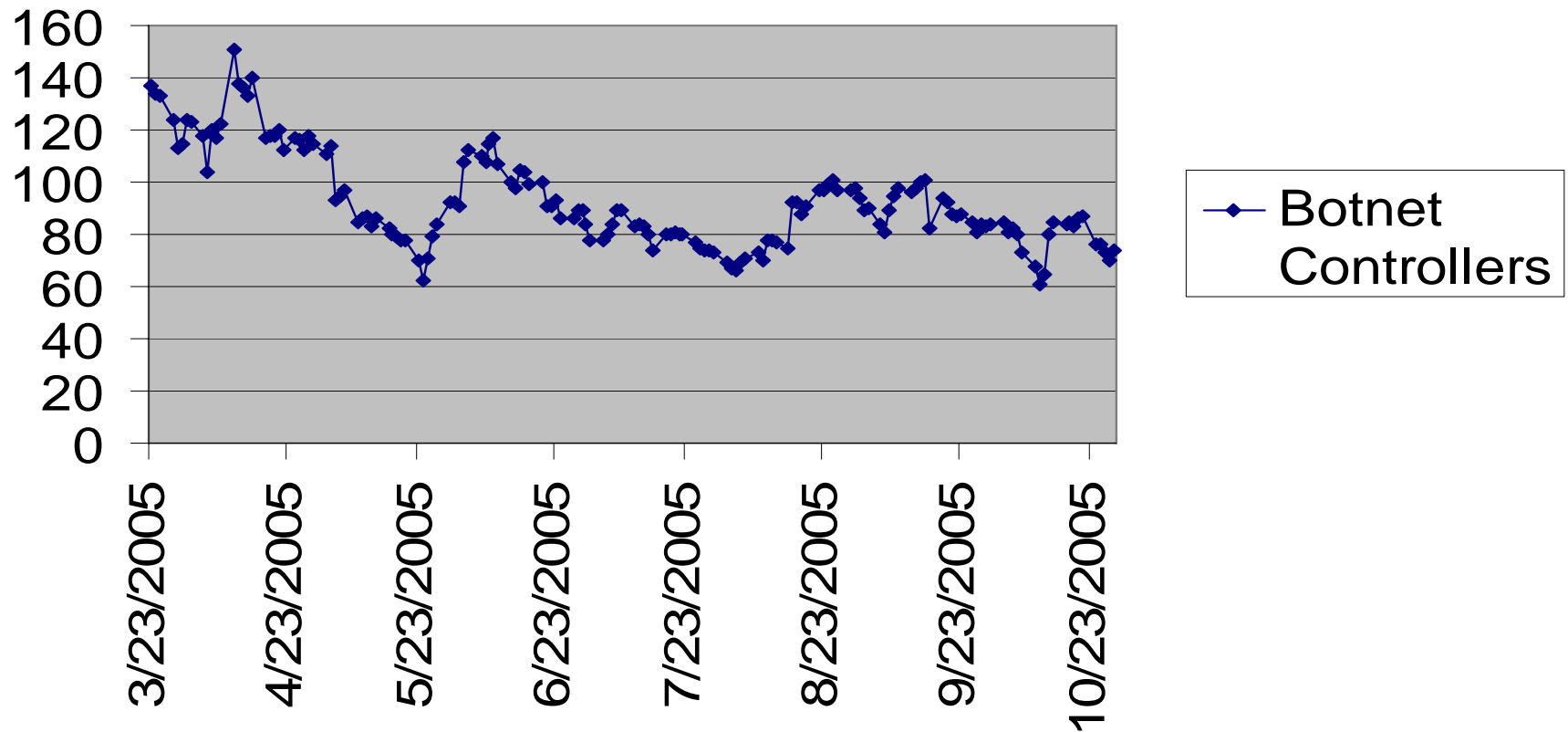
Phishing Websites



Botnet controllers downstream of AS 3549 (per day)



Botnet Controllers



Current botnet ecology and life cycle



System components

Human components

Bot life cycle

Botnet life cycle

System components



Botnet controllers: Usually compromised Unix hosts located in webhosting colo space, running ircd.

Bots: Usually compromised Windows hosts with connectivity from commercial broadband ISPs.

Spam senders: Usually located in webhosting colo space, may be bogus company, fake webhoster or fake ISP.

Proxy web interface or custom application: May be hosted/distributed through legitimate large ISPs.

Marketing/deal-making locations: Public IRC channels, web-based message boards.

Top sources of botnet controllers



As of June 7, 2005, data from Prof. Randall Vaughn, Baylor Univ., posted to NANOG.

ASN	Responsible Party	Unique C&Cs	Open-unresolved
6517	YIPESCOM - Yipes Communication	60	41
21840	SAGONET-TPA - Sago Networks	90	24
25761	STAMINUS-COMM - Staminus Commu	86	20
4766	KIXS-AS-KR Korea Telecom	43	20
13680	AS13680 Hostway Corporation Ta	22	19
21698	NEBRIX-CA - Nebrix Communicati	24	18
13301	UNITEDCOLO-AS Autonomous Syste	27	17
21788	NOC - Network Operations Cente	29	16
29415	EUROWAN-ASN OVANET - EuroWan d	16	15
13749	EVERYONES-INTERNET - Everyones	24	14
30083	SERVER4YOU - Server4You Inc.	21	14
25700	SWIFTDESK - SWIFTDESK VENTURE	13	13
23522	CIT-FOONET - CREATIVE INTERNET	14	12
27595	ATRIVO-AS - Atrivo	31	11
13237	LAMBDANET-AS European Backbone	11	11

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.phatwolk starts phatwolk 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.emailhttp 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

Ruslan Ibragimov/send-safe.com



Bulk Email Software Send-Safe - easy anonymous mailing! - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://www.send-safe.com/

Customize Links Free Hotmail Windows Marketplace Windows Media Windows

 **send-safe**
REAL ANONYMOUS MAILER

buy online
SECURE

Home
[Screenshots](#)
[Testimonials](#)
[Download](#)
ORDER NOW!
[Members area](#)
[Resellers area](#)
[FAQ](#)
[Manual](#)
[Standalone version](#)
[Proxy scanner](#)
[HoneyPot Hunter](#)
[List Manager](#) **NEW!**
[Email Verifier](#)
[Proxy Central](#) **NEW!**
[Links](#)
[Contact](#)

- ◆ 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 upgrades, 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](#)

Done

1506 Items All folders are up to date. Connected

start | Inbox - Micr... | Bulk Email So... | sec.phx.gblx... | not connect... | GX Policies | 8:27 AM

Spammer Bulletin Board



Business and Doing Deals - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Refresh Print Mail News RSS

Address http://www. .com/ /appid_1/p_1/tmode_1/smode_1/tt.htm Go Links

Google Search Web PageRank AutoFill Options

Business and Doing Deals

Users viewing this forum: Logged in as: [Subscribe](#)

Display topics from last: Filter:

[New Topic](#) [All Forums >>](#) [>>](#) Page: [1] 2 3 4 5 > >>

	Topic	Replies	Thread Starter	Hits	Last Post	Forum Information
	Servers Required (non China)	0	Proximate	1	1/7/2005 10:04:15 AM Proximate	Quick Links <ul style="list-style-type: none">- Blah...Blah...Blah...- Business and Doing Deals Supporters <ul style="list-style-type: none">- MailCrawl- EmailSupply.Net- Gay Money Machine- Bulk-Email-Lists.com- InfinityMailer+ Link to us Sponsor <div style="background-color: orange; color: white; padding: 5px; text-align: center;">Get your hands on the HOTTEST</div>
	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	

Internet

Looking for an Exploit



Looking for an exploit, or several. - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Refresh Print Mail News RSS Feeds

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

Google Search Web PageRank AutoFill Options

Looking for an exploit, or several.

Users viewing this topic: Logged in as:

Tree Style Subscribe Printable Version

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

Login	Message
 Poland I'm still new here... Posts: 38 Joined: 4/24/2004	<p>Looking for an exploit, or several.</p> <p>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.</p> <p>Will pay, and the sooner the better.</p> <p>Thanks ! 🍌</p> <hr/> <p>AIM: ICQ: E-Mail:</p>

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

Internet

Trojan software wanted



Wanted - Trojan Software - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Refresh Print Mail News RSS Feeds

Address http://www. .com/ /m_19460/p_6/tmode_1/smode_1/tm.htm Go Links

Google Search Web PageRank AutoFill Options

Wanted - Trojan Software

Users viewing this topic:

Logged in as:

Tree Style Subscribe Printable Version

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

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

Page: [1]

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

Jump to: Business and Doing Deals

Internet

Human components



Botherd: Collects and manages bots.

Botnet seller: Sells the use of bots (or proxies) to spammers.

Spammer: Sends spam.

Sponsor: Pays spammer to promote products or services.

Exploit developer: Develops code to exploit vulnerabilities.

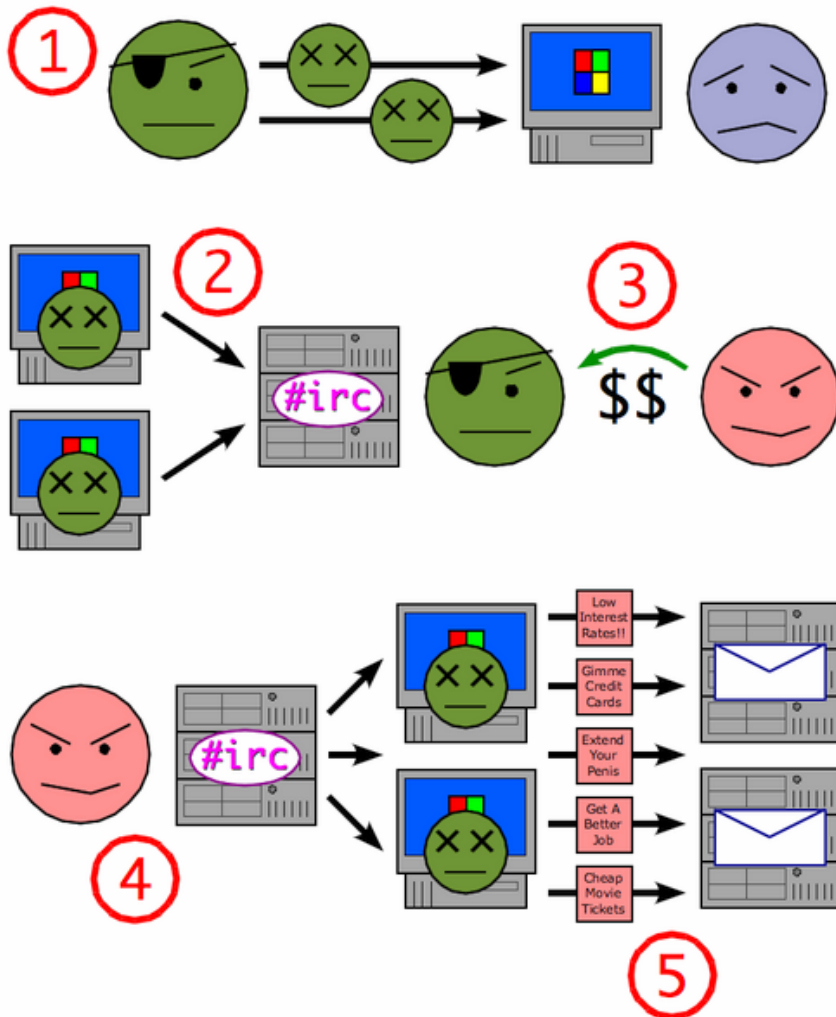
Bot developer: Develops (or more commonly, modifies existing) bot code.

Money launderer (“payment processor”): Work-at-home opportunity to process payments/laundry money for “sponsors.”

Phishers: Collectors of user identity and bank information.

Cashers: Use phished bank data to make fake ATM cards and withdraw funds.

Bot life cycle



1. Miscreant (botherd) launches worm, virus, or other mechanism to infect Windows machine.
2. Infected machines contact botnet controller via IRC.
3. Spammer (sponsor) pays miscreant for use of botnet.
4. Spammer uses botnet to send spam emails. (Usually NOT through IRC channel; typically botherd will open proxy ports on bots and provide proxy list to spammer.)

(Image from Wikipedia.)

Botnet life cycle



- 1. Compromise of controller.**
- 2. Distribution of malware—compromise of individual bots.**
- 3. Bots connect to controller; form botnet.**
- 4. Botnet activity—used by botnet for own purposes or use sold to others.**
- 5. Botnet controller identified by NSP/ISP security; monitored or shutdown.**
- 6. Bots become idle or attempt to contact another controller; some bots have vulnerabilities repaired.**

Why botnets?



Botnets are used as an economic mechanism for shifting costs of business (often illegal business) to others, including the costs of being caught engaging in illegal activity.

Botnets (a) create a buffer between a criminal and criminal activity and (b) provide a massive information processing resource at minimal cost to the criminal.

Some financial transactions which botnets facilitate:

- Sale of the use of bots.**
- Use of bots for marketing the sale of products and services (often fraudulent or illegal) via spam.**
- Use of bots for extortion (denial of service against online gambling companies, credit card processors, etc.).**
- Use of bots to send phishing emails to steal personal identity and account information.**

Defense mechanisms: prevention, detection, response



Prevention

Prevent infections at the host: Endpoint Security, Vulnerability Management.

Prevent malware delivery on the network: Firewalls, Intrusion Prevention Systems, “Clean IP,” Mail Filtering, Composite Blocking List.

Prevent sale of services to miscreants: AUPs, contracts, customer screening.

Prevent phishing: Tools to identify fake websites for end users.

Defense mechanisms: prevention, detection, response



Detection

Detection of host infections: Host Intrusion Detection Systems (IDS's), honeypots, monitoring botnet controller activity.

Detection of malware on the network: Network IDS, Netflow, Darknets/Internet Motions Sensors/Internet Telescopes, “honey monkeys.”

Detection of spam operations/miscreants: Spamhaus, monitoring miscreant communications.

Defense mechanisms: prevention, detection, response



Response

Nullrouting of botnet controllers

Quarantining of bots, automated notifications

Bot simulation/intentional infection/monitoring (Microsoft Honey Monkeys, Decoy Bot)

Undercover investigation (ICCC, FBI)

Civil and criminal prosecution (Microsoft August 2005 lawsuits against 13 spam operations using bots)

Daily customer 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	DEFACEMENT	DIPNET	DNSBOTS	MYDOOM	NACHI
PHATBOT	PHISHING	SCAN445	SCANNERS	SINIT	SLAMMER
SPAM	TOXBOT				

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.

What does the future hold?



**A continued arms race between miscreants and defenders:
Defenders will infiltrate, monitor, and prosecute.**

Miscreants will find new mechanisms to conceal their activity and place further layers of misdirection between themselves and their actions (P2P botnets without controllers, encryption, onion routing). They will continue to find new mechanisms to infect systems and create bots (email delivery, direct network infection, web-delivered code)—duping humans to doing the work for them will continue to be the most difficult issue to address.

The economic aspects of this activity need to be recognized to adequately address it—forcing miscreants to “internalize externalities” (bear the costs they are shifting to others), or to shift the costs to entities that are positioned to address the problem (e.g., ISP liability for malicious network traffic from direct customers).

Consequences of inaction



“For all online users, the report found that concern about identity theft is substantial, and is changing consumer behavior in major ways. Four in five Internet users (80 percent) are at least somewhat concerned someone could steal their identity from personal information on the Internet. Nearly nine out of ten users (86 percent) have made at least one change in their behavior because of this fear:

- 30 percent say they have reduced their overall use of the Internet.**
- A majority of Internet users (53 percent) say they have stopped giving out personal information on the Internet.**
- 25 percent say they have stopped buying things online.**
- 54 percent of those who shop online report they have become more likely to read a site’s privacy policy or user agreement before buying.**
- 29 percent of those who shop online say they have cut back on how often they buy on the Internet.”**

(Consumer Reports WebWatch, “Leap of Faith: Using the Internet Despite the Dangers”)

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>

“Know Your Enemy: Tracking Botnets,” <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/>

The Strider Honey Monkey Project: <http://research.microsoft.com/HoneyMonkey/>

Christopher Abad, “The economy of phishing,”

http://www.firstmonday.org/issues/issue10_9/abad/

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

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

Gary Warner, “Phishing Investigations: It’s Time to Make Some Decisions,” April 26, 2005, Infragard Birmingham, AL.

Consumer Reports WebWatch, “Leap of Faith: Using the Internet Despite the Dangers,”

<http://www.consumerwebwatch.org/dynamic/web-credibility-reports-princeton.cfm>

Jim Lippard

james.lippard@globalcrossing.com