

The New Global Village



Botnets: An Update

Jim Lippard, Director, Information Security Operations, Global Crossing

InfraGard Phoenix

December 12, 2005

Agenda



1. Botnet overview

Bot and botnet defined, botnet basics, the botnet economy.

2. Botnet trends and numbers

Botnet controllers, phishing attacks, spam, denial of service attacks.

3. Botnet users

Those who have been caught.

4. Botnet defense

Prevention, detection, and response.

5. The future of botnets

Botnet overview: Definitions



Bot: An Internet software agent designed to perform some task or set of tasks, intended to interact with network-based services as though it were a person. Bots may be web crawlers, chat/IRC bots, attack bots, fraud bots, etc. The bots we're talking about are those put on computer systems without the permission (and often without the knowledge) of the owner—usually end-user Windows machines with connectivity from commercial broadband ISPs.

Botnet: A collection of bots under the control of a single entity, usually through a command-and-control server using IRC as the control channel. Legitimate botnets: SETI@Home, Distributed.net, Google Compute. (Note that none of these take full control of the operating system; criminal botnets usually do.)

Botnet controller: A system controlling a botnet. Usually a compromised Unix host at one of a relatively small number of commercial webhosting providers, running ircd.

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.

Botnet overview: Human roles defined



One person can fill multiple functions, but these are also commonly distinct roles, with commercial relationships between them.

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.

Virus writer: Develops mechanism for delivering infection using exploit code.

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.

Botnet overview: Botnet history and uses



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.

2005: Bot infections via Zotob (August), Toxbot (October), Sober (November-December). (Sober.W, X, Y, Z impersonated FBI, CIA, German and Austrian federal police, UK National High-Tech Crime Unit (NHTCU), etc.)

Botnet overview: Example bots



Korgobot

SpyBot (variants/offshoots include AgoBot, Phatbot, SDBots)

Optix Pro

rBot

Toxbot

Zotob

AgoBot/Phatbot is notable for featuring 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.

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). The computing power and bandwidth alone make compromising a system desirable and useful.

Botnet overview: Phatbot feature list



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

Botnet overview: Botnet uses



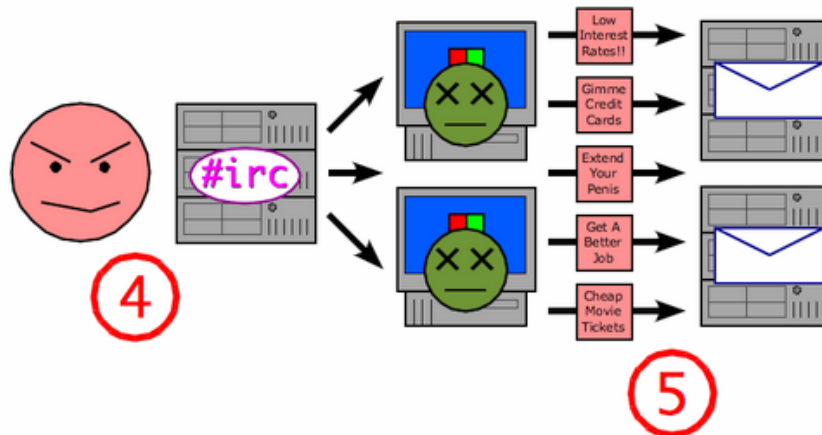
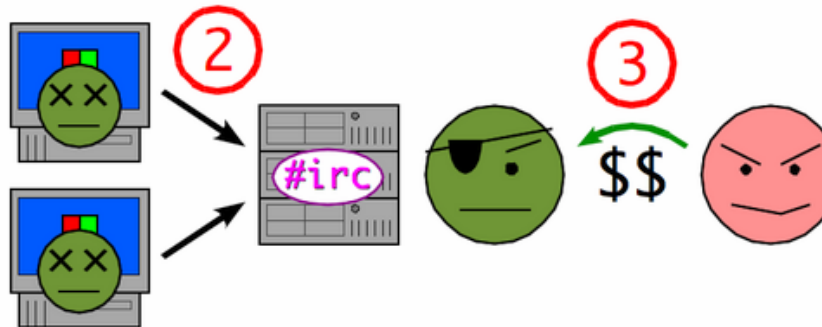
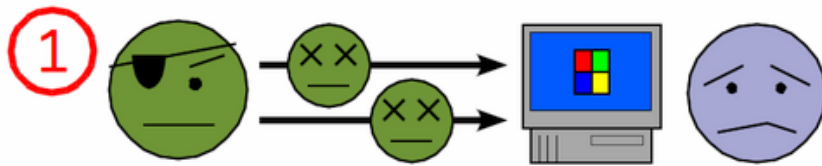
Botnets are used as an economic mechanism for shifting costs of business (often illegal business) to others, including the costs of being caught engaging in illegal activity.

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.**

Botnet overview: Bot life cycle



1. Miscreant (botherd) launches worm, virus, or other mechanism to infect Windows machine.
2. Infected machines contact botnet controller via IRC. 2.5: Infection vector closed.
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 overview: 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 - Blah...Blah...Blah... - Business and Doing Deals Supporters - MailCrawl - EmailSupply.Net - Gay Money Machine - Bulk-Email-Lists.com - InfinityMailer + Link to us Sponsor 
	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

Botnet overview: 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

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

Botnet overview: 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

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

Botnet overview: IRC conversation



<A> Unconfirmed Orders 14
<A> Cash Earned \$4,740.30
<A> Amount Due: \$183.86
<A> hghaaaahaha'
<A> you are weak
<A> im glad i got all my emails out last year
<A> last year i could pull 40/k a month easy
 wow !!
<A> this year same time, its like 4/k
<A> wierd how spam changes in a year
<A> guess its like hiv, everyone is spreading it
<C> and more people are hating it
<C> hehe
 ive pulled in alot this month

(From National Cyber-Forensics & Training Alliance, early 2004.)

Botnet trends and numbers



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%

A majority of viruses contain backdoors or create botnets. (MessageLabs, 2004 Annual Report)

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

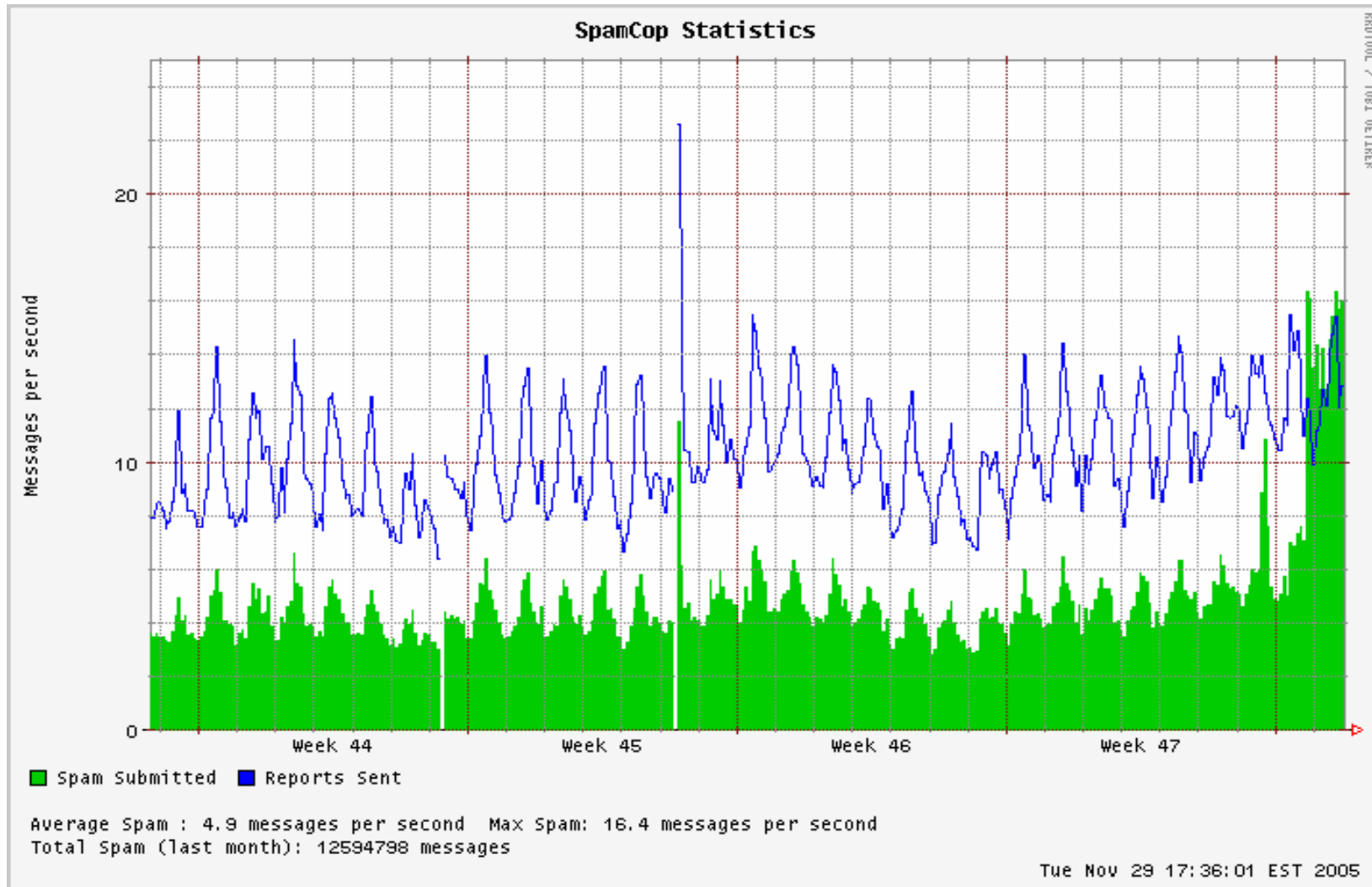
(Source: MessageLabs 2004 Annual Report, September 2005 report.)

Denial of Service Attacks (reported):

2002: 48 (16/mo). 2003: 409 (34/mo). 2004: 482 (40/mo). Jan. 1-Dec. 12, 2005: 297 (26/mo). (1Q: 77—26/mo, 2Q: 64—21/mo, 3Q: 84—28/mo, 4Q to Dec. 12: 74—31/mo)

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

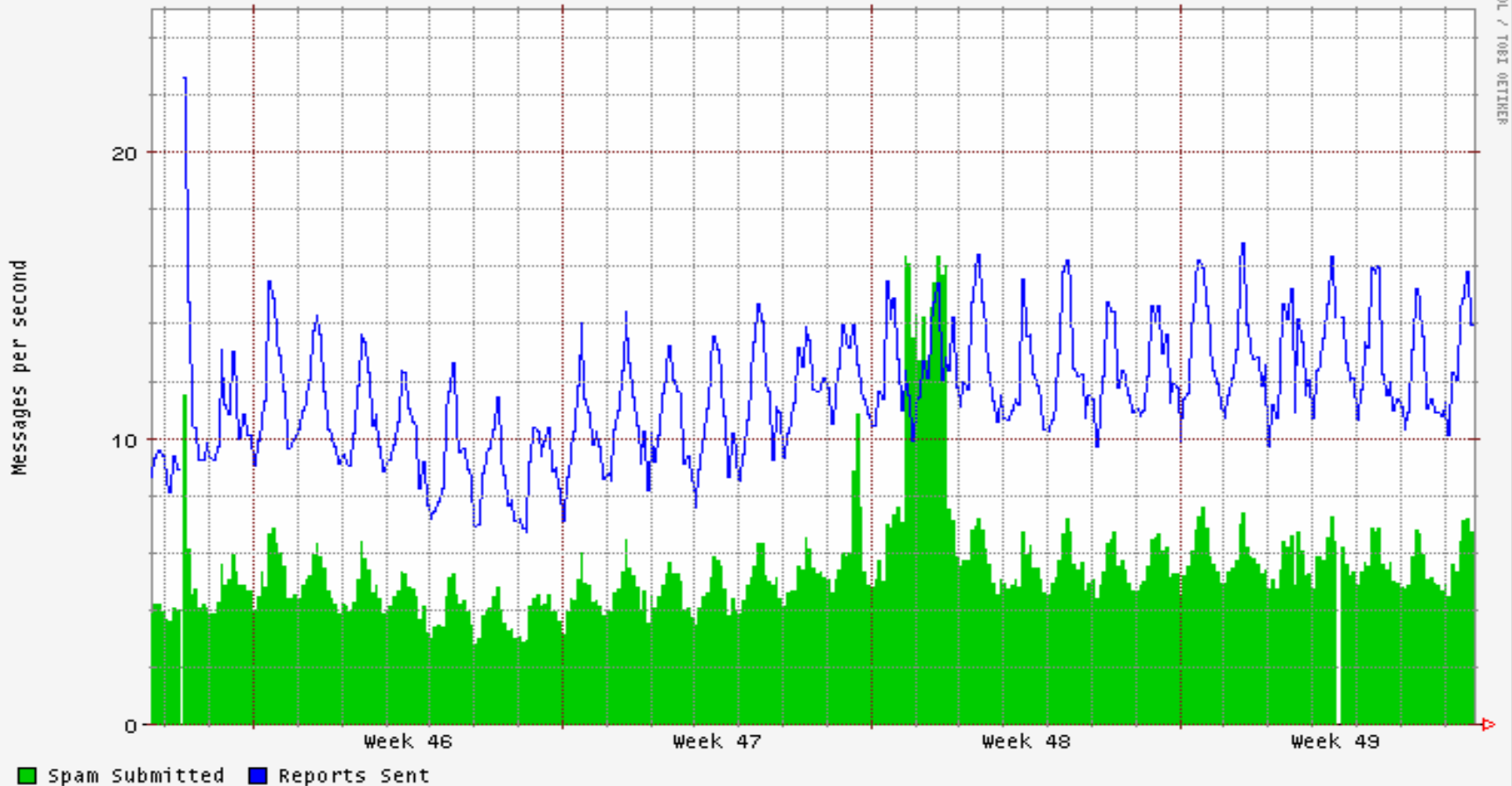
Botnet trends: SpamCop Stats, Nov. 2005



Botnet trends: SpamCop Stats, Dec. 2005



SpamCop Statistics



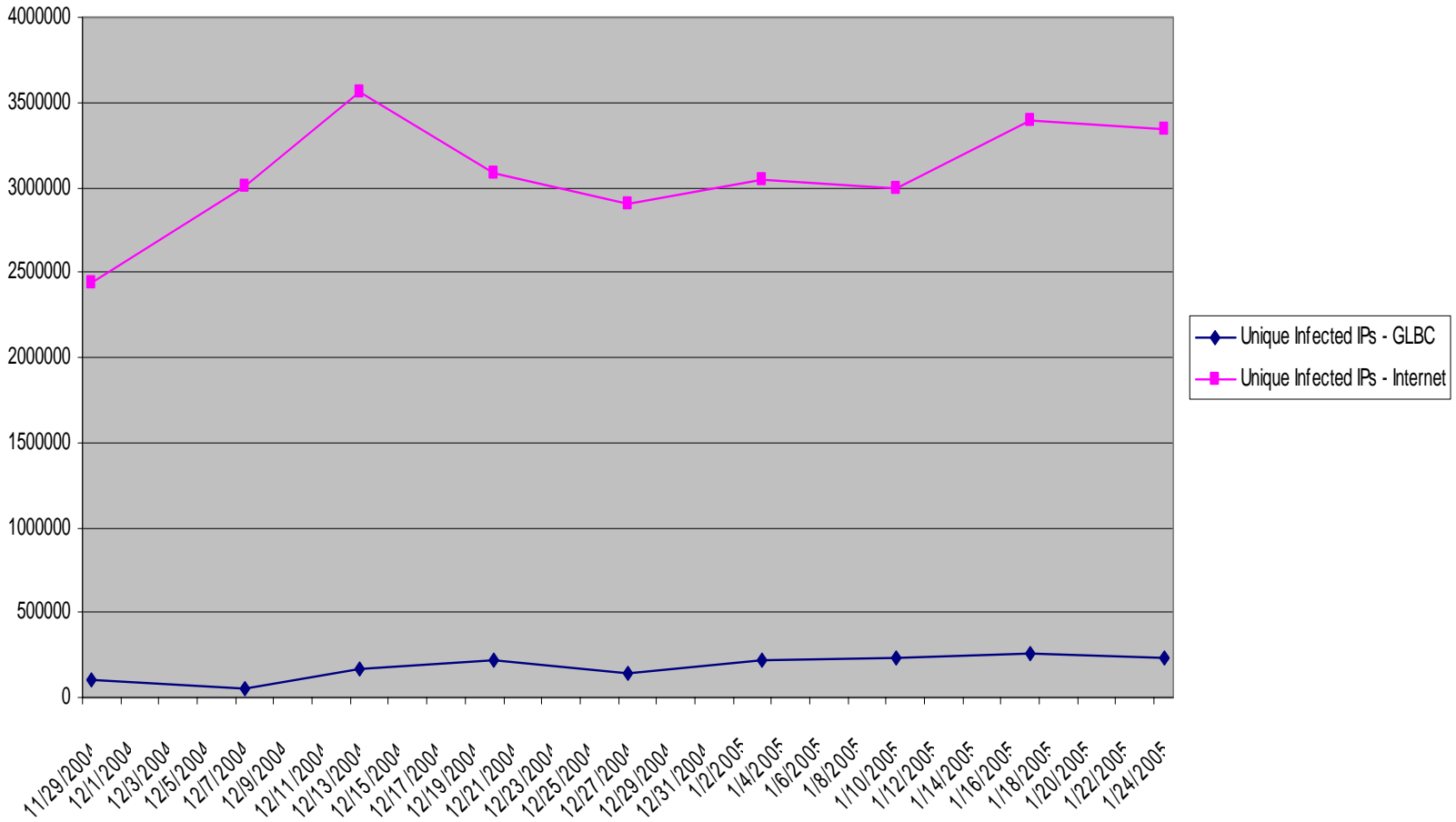
Average Spam : 5.5 messages per second Max Spam: 16.4 messages per second
Total Spam (last month): 14203244 messages

Sun Dec 11 16:01:01 EST 2005

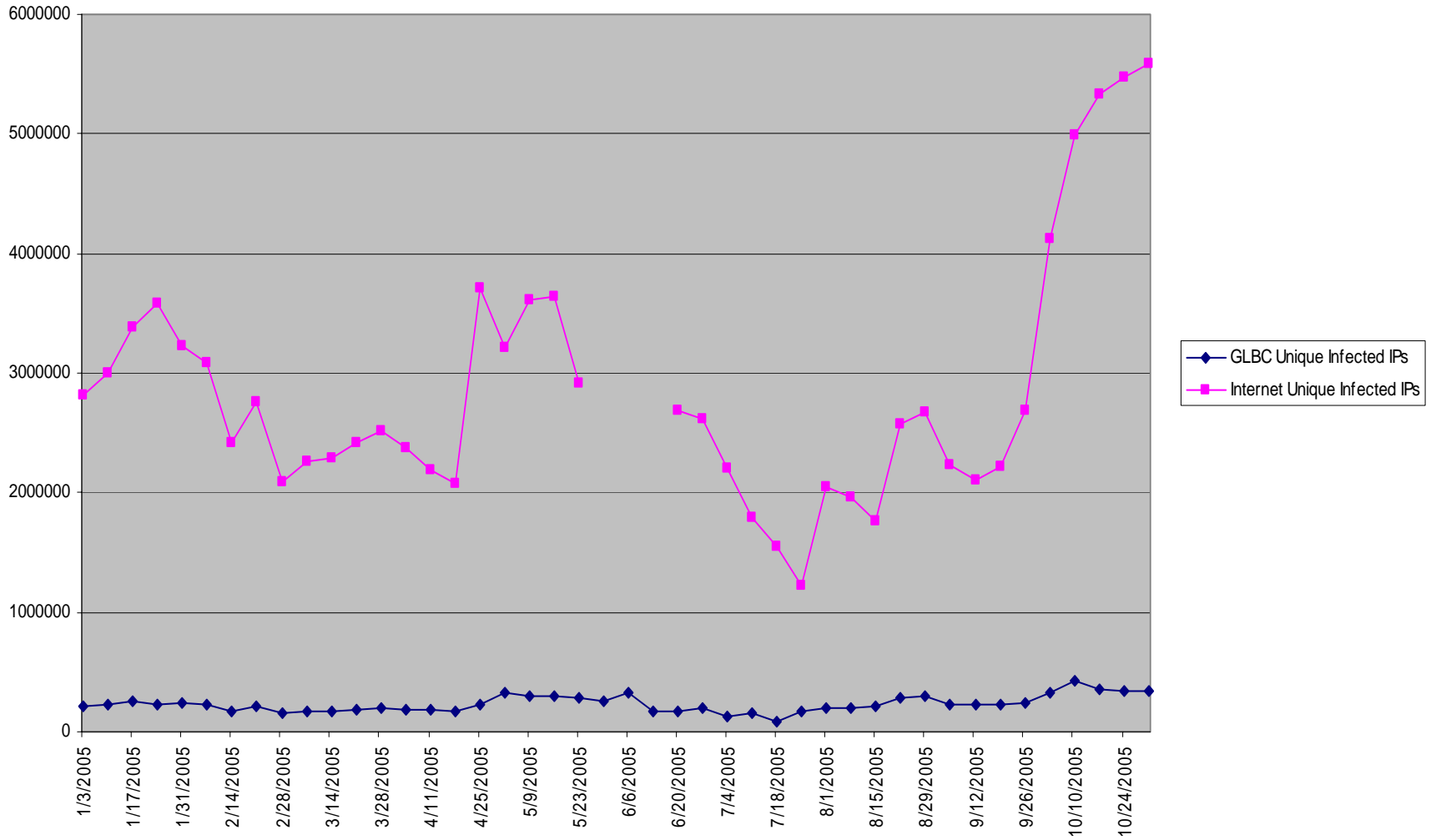
Botnet trends: Infected IPs Jan 2004-Jan 2005



Unique Infected IPs



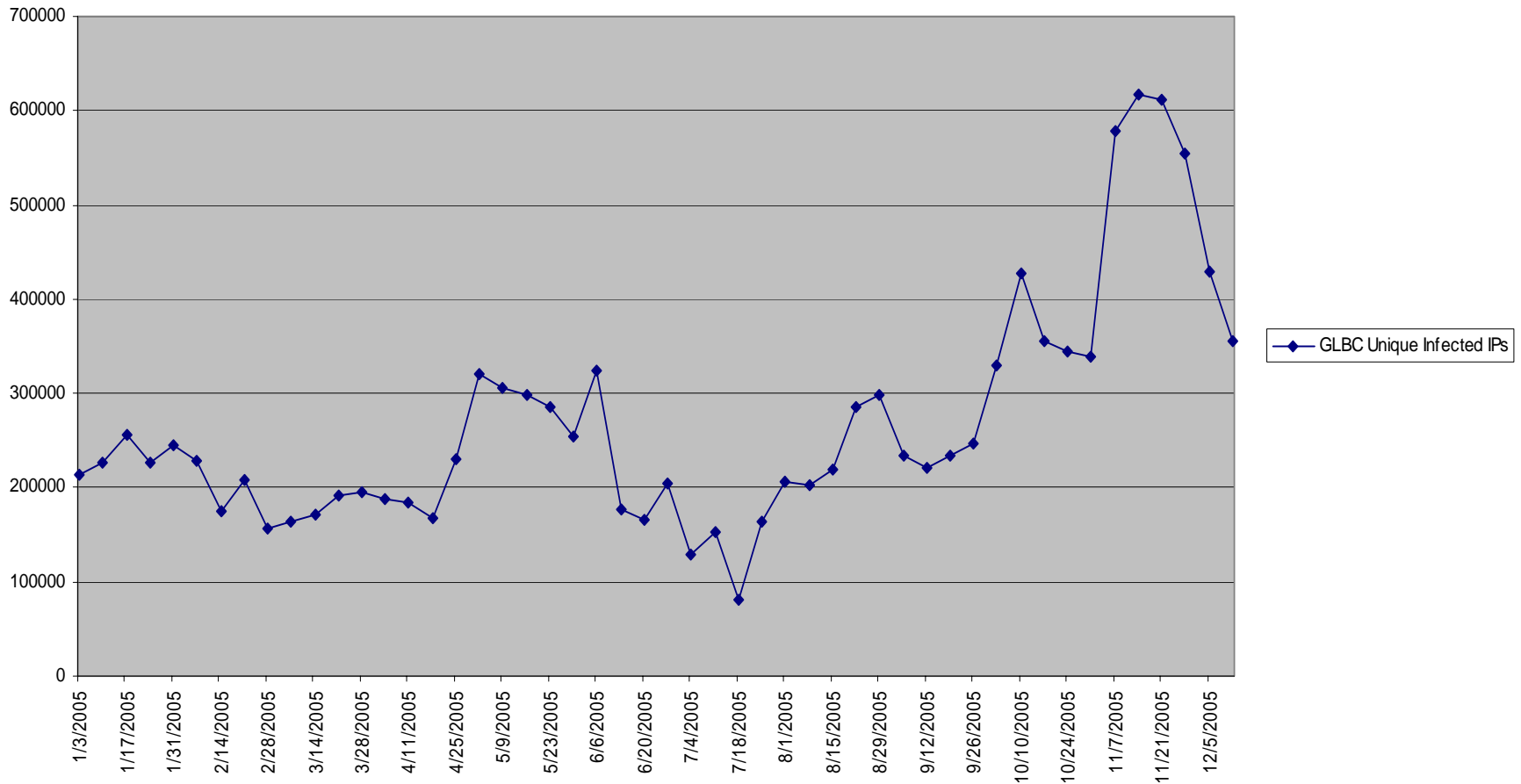
Botnet trends: Internet/GLBC downstream infected hosts



Botnet trends: GLBC downstream malware-infected hosts



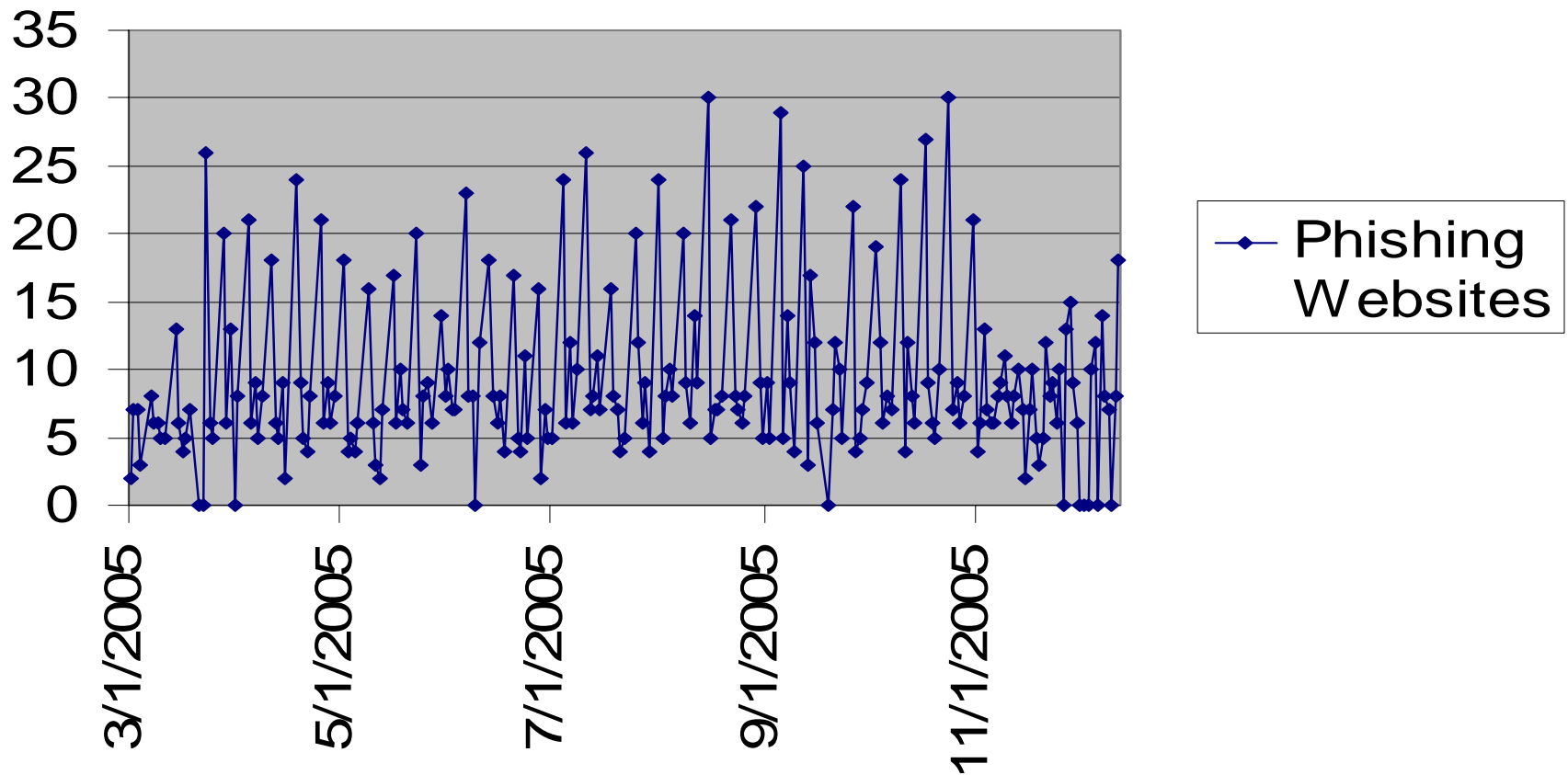
GLBC Unique Infected IPs



Botnet trends: Phishing websites downstream of AS 3549 (per day)



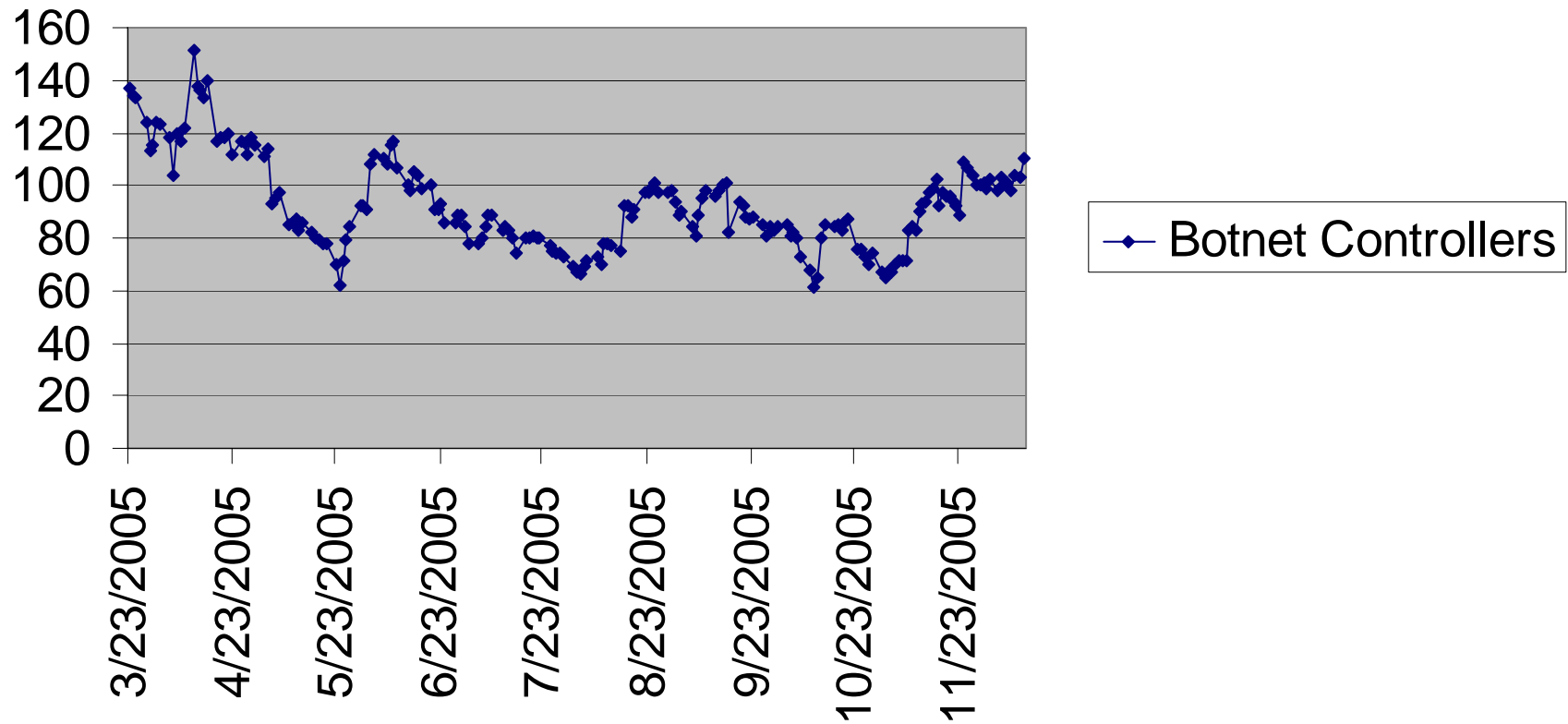
Phishing Websites



Botnet trends: Botnet controllers downstream of AS 3549 (per day)



Botnet Controllers



Botnet trends: 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	LAMB DANET-AS European Backbone	11	11

Botnet trends: Top botnet controller sources, Aug. 15, 2005



ASNs with 10 or more unresolved and open suspect C&Cs:			
ASNumber	Responsible Party	Count	Open/Unresolved
21840	SAGONET-TPA - Sago Networks	53	34
30058	FDCSERVERS - FDCservers.net LL	65	32
30083	SERVER4YOU - Server4You Inc.	41	28
12832	LYCOS-EUROPE Lycos Europe GmbH	31	27
23522	CIT-FOONET - CREATIVE INTERNET	25	23
174	COGENT Cogent/PSI	45	23
13680	AS13680 Hostway Corporation Ta	22	22
6461	MFNX MFN - Metromedia Fiber Ne	23	18
27595	ATRIVO-AS - Atrivo	27	16
15083	INFOLINK-MIA-US - Infolink Inf	19	15
4766	KIXS-AS-KR Korea Telecom	41	15
8560	SCHLUND-AS Schlund + Partner A	28	14
27645	ASN-NA-MSG-01 - Managed Soluti	19	12
13237	LAMBANET-AS European Backbone	15	12
1113	TUGNET Technische Universitaet	12	11
13301	UNITEDCOLO-AS Autonomous Syste	16	11
6939	HURRICANE - Hurricane Electric	12	10
16265	LEASEWEB LEASEWEB AS	13	10
21698	NEBRIX-CA - Nebrix Communicati	25	10

Botnet users



The following slides cover some recent arrests of people involved in various aspects of the botnet economy. Not all were direct users of botnets.

Maksym Vysochanskyy/OEM Spammer: \$400K-\$1M loss. Spamming, sold pirated software and counterfeit goods; arrested in Thailand May 2003.

Jay Echouafni/Paul Ashley/Foonet: Denial of service with botnets.

Foonet is still a major source of botnet controllers.

Netherlands case: 3 Romanians with fake Belgian passports, giant (1.5M+ bot) botnet(s) (Toxbot/Codbot).

Tucson cashers: \$600K+; 17 charged.

“Shadowcrew”: \$4M credit card fraud; busted by U.S. Secret Service.

“Botmaster”: Adware/affiliate program.

Ruslan Ibragimov/send-safe.com: Professional appearance, criminal operation.

Microsoft lawsuits in Washington state court against 13 spam operations.

Botnet users: Maksym Vysochanskyy/OEM Spammer



Guilty Plea in International Software Piracy and Financial Crime Prosecution: Case Involves Extradition for Intellectual Property Crimes (November ...

File Edit View Go Bookmarks Tools Help

http://www.cybercrime.gov/vysochanskyyPlea.htm

Customize Links Free Hotmail Windows Marketplace Windows Media Windows

 [Email this Document!](#)

**Department Of Justice
U.S. Attorney's Office
District of Columbia**
11th Floor, Federal Building
450 Golden Gate Avenue, Box 36055
San Francisco, California 94102
Assistant US Attorney
Christopher P. Sonderby
Office: (408) 535-5037

**For Immediate Release
November 29, 2005**

Guilty Plea in International Software Piracy and Financial Crime Prosecution:
Case Involves Extradition for Intellectual Property Crimes

SAN JOSE - United States Attorney Kevin V. Ryan announced that Maksym Vysochanskyy, a/k/a Maksym Kovalchuk, 27, of Ternopil, Ukraine, pleaded guilty late yesterday afternoon in federal court in San Jose to charges of criminal copyright infringement, trafficking in counterfeit goods, and prohibited monetary transactions stemming from his global distribution of counterfeit computer software over the Internet from December 2000 to May 2003. The case is one of the first to involve an extradition in a prosecution alleging intellectual property offenses.

The guilty plea follows defendant's extradition from Thailand, where he was arrested in May 2003 on a provisional arrest warrant by the Royal Thai Police with the assistance of law enforcement agents from the U.S. Secret Service and U.S. Postal Inspection Service. A criminal complaint filed at the time showed that Mr. Vyschanskyy's overseas arrest was made possible when U.S. agents monitoring his email traffic observed him make travel plans from Ukraine to Thailand, and flew to Bangkok to meet him. After contested proceedings, Mr. Vysochanskyy was extradited to San Jose to face federal charges in March 2004. He has been held in custody as a flight risk since his arrival in the United States.

United States Attorney Kevin V. Ryan stated: "This ground-breaking case demonstrates the resolve of this office and its pioneering CHIP Unit to combat the theft of the nation's intellectual property, whether the threat arises at home or from abroad. It also serves as an example to individuals abroad who seek to profit from the theft of our nation's intellectual property that the Department of Justice will vigorously seek their extradition to the United States to achieve justice."

According to the plea agreement and court records, from December 2000 to May 2003, Mr. Vysochanskyy sold counterfeit software programs on eBay and by operating numerous Web sites, including cdservice.org, biacds.net and gold-cds.com. The counterfeit software programs included titles owned by Adobe, Autodesk, Borland and

Done

start not... Pre... Vol... GL... levi... Inf... Mo... Guil... 7:27 PM

Botnet users: Jay Echouafni / Foonet



FBI Crime Alert - Saad Echouafni - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://www.fbi.gov/mostwant/alert/echouafni.htm


Customize Links Free Hotmail Windows Marketplace Windows Media Windows

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)

Done

Botnet users: Netherlands criminals



InformationWeek > Security > Dutch Police Crush Big 'Botnet,' Arrest Trio > October 10, 2005 - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://informationweek.com/story/showArticle.jhtml?articleID=171204550

Go James Ancheta

Customize Links Free Hotmail Windows Marketplace Windows Media Windows

HOME NEWS BLOGS RSS FEEDS
EVENTS RESEARCH REPORTS WHITE PAPERS SUBSCRIPTIONS

SEARCH

WINDOWS SOFTWARE HARDWARE SECURITY OUTSOURCING MANAGEMENT INDUSTRIES

Industry-Specific News | InformationWeek 500 | Banking | Wall Street & Technology | Insurance | Healthcare | Government | Small Business

SECURITY

Dutch Police Crush Big 'Botnet,' Arrest Trio

Oct. 10, 2005

A huge network of 100,000 PCs was used to conduct a denial-of-service attack against an unidentified U.S. company in an extortion attempt, and for many other nefarious deeds, according to Dutch police.

By Gregg Keizer
[TechWeb News](#)

E-Mail This Article
Print This Article
Discuss This Article
Write To An Editor
Subscribe To InformationWeek

Dutch police arrested three men for creating a botnet of more than 100,000 compromised PCs, authorities in the Netherlands said Friday. They allege the botnet was used in an attempt to extort a U.S. company, to steal PayPal and eBay accounts, and to install adware and spyware.

The pinch is among the biggest [botnet](#) scores ever for law enforcement, Dutch authorities said. "With 100,000 infected computers, the dismantled botnet is one of the largest ever seen," the Public Prosecution Service (Openbaar Ministerie, or OM) said in a statement. The network of hijacked PCs and servers consisted of machines worldwide.

The three men, ages 19, 22, and 27, allegedly used the Toxbot (aka Codbot) Trojan to infect the machines, on which they then installed adware and spyware. The massive botnet was also used to conduct a [denial-of-service](#) (DoS) attack against an unidentified U.S. company in an extortion attempt to squeeze payment for not bringing down the firm's Web site.

TECHWEBCASTS & MICROCASTS

- [Adopt a world-class, web app management strategy that works](#)
Strategies to gain 360 ° visibility and control over J2EE application performance.
- [Improving Decision-Making Via Real-Time Analytics](#)
Benefits of "thin-slicing" insurance data for faster decision-making & improved responsiveness.
- [Optimizing Infrastructure](#)
Explore the business and technological drivers and advantages of server consolidation and virtualization.

RELATED STORIES

- [Cracked: Sober Worm Update Scheme](#) 12/09/05
- [Forecast 2006: Hackers May Hit Mobile Devices, Cisco Routers, Microsoft Vista](#) 12/09/05
- [Antivirus Vendors Struggle To Keep Up With Attacks](#) 12/09/05
- [Microsoft To Fix Two Flaws Next Week](#) 12/09/05

RELATED CONTENT

- [2005 InformationWeek 500 Report](#)
- [Business Intelligence 2005](#)
- [InformationWeek National IT Salary Study 2005](#)

Download the free *Architect's Guide to Data Center Needs*

Done

start not... Pre... Vol... GL... levi... Inf... Mo... Inf... 7:10 PM

Botnet users: Tucson cashers busted



KGUN9.com :: Clear, Accurate, To The Point - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://www.kgun9.com/story.php?id=899

Go James Ancheta

Customize Links Free Hotmail Windows Marketplace Windows Media Windows

11.07.2005

TUCSON ATM THIEVES ARRESTED FOR INTERNATIONAL SCAM

By Craig Smith

Federal authorities say it's a high-dollar scam that stretched from Southern Arizona across 19 foreign countries.

They say Arizona thieves milked local ATMs for at least \$600,000 and sent half that money to other thieves overseas.

In all, 17 Arizonans stand charged with using modern technology to steal cash.

Investigators say the suspects used the internet to reach foreign criminals who already had plenty of bank account data.

A lot of it came from phishing-- that's when you get an e-mail that looks like a legitimate message from your bank. It asks you to send in account information that opens the door to your money. Investigators say they found evidence Arizona thieves used information from the foreign internet scamsters to make credit and a-t-m cards able to turn stolen information into cash.

"Part of the relationship between the suppliers around the world and the people who were involved in cashing here in Tucson was that the people involved in cashing had to pay fifty percent of their take to the suppliers," said Paul Charlton, U.S. Attorney for Arizona. "We know there was approximately 300 thousand dollars paid by the cashers here to the suppliers so that the total loss is approximately 600 thousand dollars."

The indictment says cash machines at Casino del Sol took the biggest hit-- more than \$162,000.

Authorities say a lot of the money sent overseas went to countries like Pakistan, Morocco and Egypt. Groups in those countries have a history of terrorist activity but the government will not say if any of the stolen money was used to bankroll terrorists.



OTHER KGUN9 HEADLINES

- HEATED PUBLIC HOUSING HEARING IN NOGALES
- TEEN CLUB CANCELS CONCERTS IN WAKE OF SHOOTING
- TUCSON POLICE INVESTIGATING FATAL SHOOTING OUTSIDE TEEN NIGHT CLUB
- BISHOPS URGE MORE COMPASSION FOR ILLEGAL IMMIGRANTS
- PIMA SUPERVISOR SAYS HE WON'T RUN FOR CONGRESS
- I-10 LETTUCE CRASH
- COMMISSIONER WARNS OF RISK OF TERRORISM FROM UNGUARDED RAILS
- ADULT BUSINESS DROPS LAWSUIT AGAINST PIMA COUNTY
- BISHOPS URGE MORE COMPASSION FOR ILLEGAL IMMIGRANTS
- TOBACCO TAX COULD INCREASE

Arizona Daily Star
FROM THE FRONT PAGE

Done

start not... Pre... Vol... GL... levi... Inf... Mo... KG... 7:14 PM

Botnet users: Shadowcrew



Shadowcrew six plead guilty to credit card fraud | The Register - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://www.theregister.co.uk/2005/11/18/shadowcrew/

Go James Ancheta

Customize Links Free Hotmail Windows Marketplace Windows Media Windows

— Quick Jump —

Reg Shops
[Cash'n'Carrion](#)
[Mobile Gadgets](#)
[Computer Components](#)
[Hosting](#)
[Offers](#)

News Services
[Reg Newsletters](#)
[Week's Headlines](#)
[Reg Mobile](#)
[Reg Archive](#)
[DeskTop News Alerts](#)
[US Edition](#)
[XML](#)

Top Stories
[Alienware Area-51 m5500 notebook](#)
[eBayer pays £470 for photo of Xbox 360](#)
[eBay pulls Excel vulnerability auction](#)
[BOFH: Beware the lie-detecting mouse](#)
[The sophist and the open source baking farce](#)

The Register » Security » Identity »

Shadowcrew six plead guilty to credit card fraud

Dragged into the light

By [John Leyden](#)
Published Friday 18th November 2005 14:08 GMT
[Get breaking Security news straight to your desktop - click here to find out how](#)

A further six people linked to the trade in stolen personal information and credit card details via the notorious Shadowcrew web site pleaded guilty on Thursday. The six are among 28 people [charged](#) last year following an undercover investigation, codenamed Operation Firewall, mounted by the US Secret Service against Shadowcrew.com, a members-only underground web site that became an online marketplace for credit card fraudsters and counterfeit identification document forgers.

The group of six pleaded guilty to one count of conspiracy to defraud in New Jersey on Thursday in exchange for the state dropping other charges pending against them, [Wired reports](#). They were named as: Andrew Mantovani, 23, and Brandon Monchamp, 22, of Arizona; Kim Taylor, 47, and Omar Dhanani, 22, of California; Jeremy Stephens, 31, of North Carolina; and Jeremy Zielinski, 22, of Florida. In total, 12 people have now pleaded guilty to Shadowcrew-related charges.

Shadowcrew members allegedly trafficked in at least 1.7m stolen credit card numbers and caused total losses in excess of \$4m. Victims of this carding activity included banks and credit card companies, who bore the brunt of losses, as well as consumers whose identities and credit histories were damaged by identity theft.

Mantovani, suspected of co-founding Shadowcrew.com, also pleaded guilty to a second charge of trafficking in stolen identity information involving the sale of address and birth

Reg Jobs

- Oracle 8i / 9i / 11i Apps Technical Consultant - London - £50K (£50K + bens, London)
- Java / Swing Developers x 5 (£50 p / hd, Hook)
- Database Administrator / Developer (SQL / ORACLE DBA, DTS) (24-28k + Bens Neg, London, City)
- Business Analysts (35-45k + 20% bonus + car, Wiltshire, South West)
- Java / Documentum Team Leader - Investment Banking, London (up to £75, 000, Marylebone)
- Credit Risk Analyst - SAS / SPSS - Financial Services (To £40, 000 + bens, Cardiff, South Wales)

In association with **jobsite**

Done

start not... Pre... Vol... GL... levi... Inf... Mo... Sh... 7:16 PM

Botnet users: Jeanson James Ancheta (“Botmaster”)



The FBI has confirmed that U.S. adware developer 180solutions is the American business whose cooperation with law enforcement played a part in the October breakup of a European botnet scheme. Dutch authorities say three men were arrested in connection with a scheme in which hundreds of thousands of computers were allegedly infected with malicious computer code and then used as zombie PCs to commit additional crimes.

In a similar case, a federal grand jury yesterday indicted Jeanson James Ancheta of Downey, California. The indictment, filed in U.S. District Court in Los Angeles, alleges Ancheta wrote and disseminated malware that assembled armies of infected PCs (known as bots, because they essentially become programmed to function as automatons or robots), then sold access to those PCs to hackers and spammers.

Ancheta also allegedly used the botnets (or networks of bots) to generate income from the surreptitious installation of adware on the infected computers, according to the indictment. U.S. prosecutors say the botnets in the American case involved roughly 400,000 PCs.

In the Netherlands case, published reports say that authorities believe the botnet may have consisted of more than a million zombie PCs. According to information provided by the Dutch prosecutor's office, the three men were charged with illegal access to computers, damage to digital networks, installation of adware and spyware, illegal access to PayPal accounts, and receiving stolen goods.

In the American case, U.S. prosecutors charge that Jeanson James Ancheta of Los Angeles, as well as an unnamed co-conspirator, used a botnet to disseminate and install adware from two firms: Loudcash and Gammacash. The unauthorized installations resulted in regular payments of thousands of dollars per month from both firms to Ancheta and his cohort, who authorities believe is based in Florida, prosecutors said.

(PC World, <http://abcnews.go.com/Technology/PCWorld/story?id=1314632>)

Botnet users: 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

Botnet users: 13 spam operations sued by Microsoft, Aug. 17, 2005



Stopping Zombies Before They Attack: Microsoft Teams with Federal Trade Commission and Consumer Action to Promote PC Protection: "Don't Get ...

File Edit View Go Bookmarks Tools Help

http://www.microsoft.com/presspass/features/2005/oct05/10-27Zombie.msp

Microsoft

PressPass - Information for Journalists

PressPass Home | PR Contacts | Fast Facts About Microsoft | Site Map | Advanced Search | RSS Feeds

Microsoft News
Product News
Consumer News
International Contacts
Legal News
Security & Privacy News
Events
News Archive

Corporate Information
Microsoft Executives
Fast Facts About Microsoft
Image Gallery

Related Sites
Analyst Relations
Community Affairs
Essays on Technology
Executive E-Mail
Investor Relations
Microsoft Research

Stopping Zombies Before They Attack: Microsoft Teams with Federal Trade Commission and Consumer Action to Promote PC Protection
"Don't Get Tricked on Halloween" campaign and new lawsuit extend efforts by Microsoft to crack down on illegal methods used by spammers to distribute unsolicited e-mail.

WASHINGTON, D.C., Oct. 27, 2005 – Like medical researchers studying a strain of a contagious virus, Microsoft Internet Safety Enforcement investigators carefully experimented this summer with a tiny piece of malicious code used by computer criminals to hijack personal computers. The investigators began by placing a single copy of the code onto a healthy computer and then connected the computer to the Internet.

Almost immediately, the researchers noticed the first rumblings of life. The infected computer sent an alert with its Internet location and hijack status to a distant server. Then, connection requests from hundreds of Internet Protocol (IP) addresses poured into the machine, commanding the infected computer to distribute millions of illegal spam e-mails.

These requests meant one thing: the investigators had successfully created a "zombie" computer.

Today, Microsoft, the U.S. Federal Trade Commission (FTC) and Consumer Action, a public watchdog and education group, launched a campaign aimed at helping consumers prevent their computers from getting turned into zombies.

Timed to coincide with National Cyber Security Awareness Month and Halloween on Oct. 31, the "Don't Get Tricked on Halloween" campaign alerts computer users to the threat of zombie computers and how to protect their personal computers (PCs) from being infected with malicious code. In addition, Microsoft is announcing a legal enforcement action that for the first time specifically targets illegal e-mail operations that connect to zombie computers to send spam.

"The only way to slow the spread of zombies and other online threats is by going after them as resolutely and in as many ways as possible," says Tim Cranton, director of Microsoft's Internet Safety Enforcement programs.

Related Links

Press Releases:

- [Don't Get Tricked on Halloween: Federal Trade Commission, Consumer Action and Microsoft Warn Internet Users of Zombie Computers](#) – Oct. 27, 2005

Presentation:

- [How Zombie PCs Operate: A Graphical Presentation](#) – Oct. 27, 2005 (Microsoft PowerPoint file, 1.1 MB)

Feature Stories:

- [Q&A: Microsoft Teams with National Cyber Security Alliance for Awareness Month](#) – Oct. 3, 2005

Virtual Newsrooms:

- [Security & Privacy](#)

Done

start n. v. A S. T. B. T. S. C

10:37 AM

Botnet defense: Multiple problems to address



- 1. Endpoint/client security.** The end user's computers are vulnerable to attack, compromising authentication credentials and control of the host. A fake site can be made completely indistinguishable from a real one—control of your OS means potential control of the display and keyboard.
- 2. Network security.** Malicious traffic flows freely; compromised hosts stay on the network.
- 3. Web site/server security.** The mechanisms by which users gain access tend to be weak and easily obtained from end users (unencrypted username/password); the same problems which afflict clients are also prevalent (failure to patch, lack of adequate security mechanisms).
- 4. The human element.** People are fooled even by bad fakes, don't adequately take steps to secure systems, they buy things advertised in spam, they sell service to criminals.
- 5. The economic element.** The current environment (given the above) provides large financial benefits to criminal use of these resources with tiny risk of being caught. The costs incurred are in most cases small and distributed over a large number of people (the end users).

Botnet defense: 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 unauthorized use of services: two-factor authentication (not a panacea, but raises the bar), better encryption on bank cards.

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

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



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.



Response

Nullrouting of botnet controllers

Quarantining of bots, automated notifications

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

Undercover investigation (ICCC, FBI, security researchers)

Civil and criminal prosecution

Botnet defense: 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	MALWAREURL	MYDOOM
NACHI	PHATBOT	PHISHING	SCAN445	SCANNERS	SINIT
SLAMMER	SPAM	SPYBOT	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, phishing Websites, or malware distribution sites (marked with BOTNETS, PHISHING, or MALWAREURL respectively) may be null routed by Global Crossing following a separately emailed notice.

This report is sent every day. 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—and continue to offer partial solutions that don't address key aspects of the problem.**

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 but do not currently have incentive to take adequate action (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”)

An AOL/National Cyber Security Alliance study released December 11, 2005 found that 25% of Internet users receive phishing emails each month, and 70% of recipients thought the emails might be from the companies they claimed to be from (i.e., 17.5% of Internet users are fooled). 6% admitted submitting information in response to a phishing attack; 15% said their credit card or bank information had been misused or their identity information stolen and misused.

(http://www.staysafeonline.info/pdf/safety_study_2005.pdf)

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