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.


**2003-2005:** 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.


- 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:

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):
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

GLBC Unique Infected IPs
Phishing websites

Mar. 2005: 6
Apr. 2005: 22
May 2005: 25
Jun. 2005: 46
Jul. 2005: 213
Aug. 2005: 256
Sep. 2005: 219
Phishing websites downstream of AS 3549 (per day)
Botnet controllers downstream of AS 3549 (per day)
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.

<table>
<thead>
<tr>
<th>ASN</th>
<th>Responsible Party</th>
<th>Unique C&amp;Cs</th>
<th>Open-unresolved</th>
</tr>
</thead>
<tbody>
<tr>
<td>6517</td>
<td>YIPESCOM - Yipes Communication</td>
<td>60</td>
<td>41</td>
</tr>
<tr>
<td>21840</td>
<td>SAGONET-TPA - Sago Networks</td>
<td>90</td>
<td>24</td>
</tr>
<tr>
<td>25761</td>
<td>STAMINUS-COMM - Staminus Commu</td>
<td>86</td>
<td>20</td>
</tr>
<tr>
<td>4766</td>
<td>KIXS-AS-KR Korea Telecom</td>
<td>43</td>
<td>20</td>
</tr>
<tr>
<td>13680</td>
<td>AS13680 Hostway Corporation Ta</td>
<td>22</td>
<td>19</td>
</tr>
<tr>
<td>21698</td>
<td>NEBRIX-CA - Nebrix Communicati</td>
<td>24</td>
<td>18</td>
</tr>
<tr>
<td>13301</td>
<td>UNITEDCOLO-AS Autonomous Syste</td>
<td>27</td>
<td>17</td>
</tr>
<tr>
<td>21788</td>
<td>NOC - Network Operations Cente</td>
<td>29</td>
<td>16</td>
</tr>
<tr>
<td>29415</td>
<td>EUROWAN-ASN OVANET - EuroWan d</td>
<td>16</td>
<td>15</td>
</tr>
<tr>
<td>13749</td>
<td>EVERYONES-INTERNET - Everyones</td>
<td>24</td>
<td>14</td>
</tr>
<tr>
<td>30083</td>
<td>SERVER4YOU - Server4You Inc.</td>
<td>21</td>
<td>14</td>
</tr>
<tr>
<td>25700</td>
<td>SWIFTDESK - SWIFTDESK VENTURE</td>
<td>13</td>
<td>13</td>
</tr>
<tr>
<td>23522</td>
<td>CIT-FOONET - CREATIVE INTERNET</td>
<td>14</td>
<td>12</td>
</tr>
<tr>
<td>27595</td>
<td>ATRIVO-AS - Atrivo</td>
<td>31</td>
<td>11</td>
</tr>
<tr>
<td>13237</td>
<td>LAMBDANET-AS European Backbone</td>
<td>11</td>
<td>11</td>
</tr>
</tbody>
</table>
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.cleanup removes paths 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 an HTTP flood
- ddos.synflood starts an SYN flood
- ddos.udpflood starts a UDP flood
- redirect.stop stops all redirects running
- redirect.uptime sets the uptime of the redirect
- 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.cdrkey makes the bot get a list of cdrkeys
- harvest.emails makes the bot get a list of emails via http
- harvest.emails makes the bot get a list of emails
- waste.system changes the server the bot connects to
- waste.connect reconnects to the server
- waste.handlers writes the exception to the server
- waste.quit disconnects the bot from the server
- 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.connect makes the bot join a channel
- waste.gethost prints netinfo when host matches
- waste.quit disconnects the bot from the server
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!
Trojan software wanted

Wanted - Trojan Software - Microsoft Internet Explorer

Login

Message

TonyPony
I'm still new here...

Wanted - Trojan Software

Any body got a system for sale?

Please don't bother to reply if the AV's already got it.

Page: [1]

Wanted - Trojan Software

Users viewing this topic:

Post Reply

All Forums >>

>>Business and Doing Deals >>

Page: [1]
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/launder 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. 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 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 botherd 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.
Prevention

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


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.
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
- T0KBOT

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 | 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 | 206.165.93.5 | 2005-03-23 22:13:40 NACHI | 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
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.)
   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