Challenges posed by Botnets

S.S.Sarma, CISSP, CEH

CERT-In
Department of Information Technology
Government of India
Objective

• Understanding Bots, Botnets
• Activities of Botnets and Impact
• Presence of Bots and Botnets in India
• Mitigation of Botnet Attacks
Understanding Botnets

- **Bot**
  - Derived from the word “Robot”. ‘Bot’ is a generic term used to describe an automated process
  - Gets installed on user computer without their knowledge
  - Bot infected machines, pass the control of the machine to a remote attacker and act as per the attackers command
  - Popularly known as zombie machines
Understanding Botnets

• Botnet
  – A network of compromised computers (Infected with Bots) – work as zombies
  – Bot infected machines opens a backdoor and listen for commands issued by attackers
  – Media for controlling botnets
    • IRC channel
    • P2P
    • Instant Messaging
    • Web sites
Understanding Botnets

• Bot Herder
  – finds vulnerable systems
  – Exploit the vulnerable systems
  – install their bot program
  – The infected machine then has become one of many zombies in a botnet and responds to commands given by the bot herder

• Command & Control
  – The exercise of authority and direction by Bot herder over Bots within the Botnet to perform desired tasks
IRC Botnet

Bad Guy
Controlling the Botnet
Sending commands using IRC Server.

IRC Server
XXX.XXX.XXX

Bot Client n

Bot Client 1

Bot Client 2

Bot Client 3

Bot Client 4
• IRC
  – Internet Relay Chat (IRC) is a form of real-time Internet chat
  – Designed for group (many-to-many) communication in discussion forums called channels
  – Allows one-to-one communication and data transfers via private message
  – IRC Networks
    • EFnet, IRCnet, QuakeNet, Undernet
  – IRC Clients
    • mIRC, Bersirc, KVIrc, Trillian, Visual IRC, X-Chat
Understanding Botnets - IRC

• **Channel**
  – The basic means of communication in an established IRC session
  – Users can join to a channel using the command /join #channelname and send messages to it
  – Controlled by channel operator. The channel operator can restrict the usage of the IRC channel.

• **Mode**
  – Users and channels have modes, such as Private, Secret etc

• **Nick**
  – Nickname is the identification name of the logged in user
Understanding Botnets - P2P

- Computer network that uses diverse connectivity between participants in a network
- Uses the cumulative bandwidth of network participants
- The P2P overlay network consists of all the participating peers as network nodes.
- Overlay networks permits routing messages to destinations not specified by an IP address through “distributed hash tables”
- Examples
  - Napster, KaZaA, Gnutella, eDonkey
P2P Botnets

• Decentralised C&C
  – Bot herder only has to become one of the peers to broadcast his commands over the network.

• Different (modular) functions
  – SPAM Node
  – DNS Node
  – Proxy Node
Botnets – Activities and Impact

- SPAM
- Phishing
- DDoS
- Spyware, Keyloggers
- Malware Propagation
Botnets – Activities and Impact

Spam and Phishing

• **Spambot**
  – Program designed to collect e-mail addresses from the Internet in order to build mailing lists for sending Spam. Crawls the web and gathers e-mail addresses from Web sites, newsgroups, special-interest group (SIG) postings, and chat-room conversations
  – Example Agobot

• **SOCKS enabled Bots**
  – Email program sends email using the bot as a relay
  – If an anti-spam program blacklists the bot’s IP address, the herder activates the SOCKS proxy on another bot, and his spam seems to originate from a new, clean IP address.

• **Phishing**
  – Phishing website Hosting supported by Botnets
  – Provide dynamic/Fast-Flux DNS for reliable hosting of Phishing websites
  – Aid in spamming the phishing emails
Botnets – Activities and Impact

Distributed Denial of Service attacks

• Flooding
  – TCP Syn
  – UDP
  – ICMP
  – HTTP GET
Botnets – Activities and Impact

Recent DDoS attacks

• Attacks on websites of Estonia
  – ICMP and TCP Syn Floods
  – Upto 100 Mbps traffic for 10 Hours

• DDoS on websites of Canada (August 2007)
  – Due to Spam by Storm Botnet

• Attacks on root DNS servers (February 2007)

• DDoS attack on website of National Australia Bank (October 2006)
Botnets – Activities and Impact

• Spyware, Adware
  – Installation of BHOs
• Keyloggers
  – Info stealers, CD Keys
• Piracy, IP theft
• Malware Propagation
  – Downloaders
  – Emails with malicious attachments
• Ransomware
  – Encrypts user’s data and demands money
Types of Bots - Evolution

- GT bot (Global Threat) – 1998
- Agobot, Gaobot, Phatbot – 2002
- SDbot, Spybot – 2002
  - Spreads by NetBIOS, DCom, UPNP, RPC
  - Use backdoors created by Mydoom, Bagel,
- Rbot – 2003
  - Complex in structure, Packs executables
- Mytob
  - Convergence of mass mailing Worm and SD Bot
- Q8 Bots
  - UNIX/LINUX
- Perl based Bots
- P2P botnets
- Transpired in October 2006
- The network generally consists of one control server (running multiple peer-nets on different ports), several template servers, and around 500 peers per port
- Uses its own spam engine
- downloads templates for sending spam messages from the remote control server
- The spam templates uses GIF file, size of which is modified each time spam is sent, templates encrypted with AES
- AES-based challenge-response authentication method is used to prevent third-parties from being able to download the templates from the template server
- Suspected to be involved in DDoS attacks on Estonian websites
How Spamthru works

1. Malware writer spams out a “stub” infection.
2. The “Stub” finds vulnerable machines and "recruits" them into a botnet.
3. The “Stub” downloads the complete spamthru from a compromised website and the compromised computer joins the botnet.
4. Botnet “zombies” execute attack.

Thousands of “zombie” machines awaiting instructions to launch an attack.

Source: Secureworks
Botnet - Storm

- Transpired in January 2007
- Also known as Zhelatin, Peacomm, Tibs
- Propagates through SPAM
- Sends various types of SPAM
- Hides on machine with rootkit technology
- Adds malicious drivers such as wincom32.sys, spoolsv.sys
- VM aware
- Uses fast-flux DNS for hosting on named sites
- Binary has gone through many revisions
- P2P based network of Bots – eDonkey protocol
- Features of P2P network have evolved with time
- uses **Kademlia** a distributed hash table for decentralized peer to peer computer communication
- Growing in numbers - estimated at 50 million?
Bot infected systems tracked in India

![Chart showing bot infections tracked in India from June 2007 to March 2008.](chart.png)

- Jun-07: 760
- Jul-07: 14835
- Aug-07: 4934
- Sep-07: 1976
- Oct-07: 1370
- Nov-07: 1020
- Dec-07: 1020
- Jan-08: 2102
- Feb-08: 1279
- Mar-08: 15160
C&C Servers controlling Bots in India

<table>
<thead>
<tr>
<th>Month</th>
<th>C&amp;C(All)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jun-07</td>
<td>93</td>
</tr>
<tr>
<td>Jul-07</td>
<td>138</td>
</tr>
<tr>
<td>Aug-07</td>
<td>55</td>
</tr>
<tr>
<td>Sep-07</td>
<td>57</td>
</tr>
<tr>
<td>Oct-07</td>
<td>57</td>
</tr>
<tr>
<td>Nov-07</td>
<td>48</td>
</tr>
<tr>
<td>Dec-07</td>
<td>46</td>
</tr>
<tr>
<td>Jan-08</td>
<td>45</td>
</tr>
<tr>
<td>Feb-08</td>
<td>48</td>
</tr>
<tr>
<td>Mar-08</td>
<td>70</td>
</tr>
</tbody>
</table>
Botnet - Mitigation

• Enterprises
  – Information Security Policies and Procedures
  – User awareness

• CERTs/ CSIRTs
  – Early warning
  – Advise malicious URLs, IP addresses
  – Advise attack trends and countermeasures

• ISPs
  – Response to Botnet information received from CERT
  – Sensitize customers about Bot infection

• Registrars
  – Check malicious websites
  – Verify registrant details
Botnet - Mitigation

• Vendors
  – Anti virus
  – Perimeter Security – IDS/IPS
  – Secure OS and applications

• Law Enforcement
  – Investigate Botnet attacks and Incidents

• Users
  – Follow security best practices
References

- http://www.secureworks.com/research/threats/spamthru/?threat=spamthru
- www.wikipedia.org
- Black Energy DDoS Bot Analysis- Jose Nazario, Arbor Networks
Thank You

www.cert-in.org.in