Bots and Botnets

CS-431
Dick Steflik

DDoS

- One of the most common ways to mount a Distributed Denial of Service attacks is done via networks of zombie computers taking instructions from a central point
- Early net were controlled via proprietary software written by the network owner
- Today they are mostly controlled by an IRC channel
  - This makes it easier to control the network and easier for the owner to hide

IRC

- Internet Relay Chat
  - Jarkko Oikarinen; 1988
  - Real time Internet Chat (synchronous conferencing)
    - Designed for group conferencing
      - Can do private one-to-one messaging
    - TCP Port 195 but usually run on 6667 to avoid having to run the server as root.
    - RFC 1459 also RFCs 2810-2813
    - Network is usually arranged in an acyclic graph (tree)
      - Messages only need go down the required branches
    - Communications are facilitated via channels
      - Channels can be global to all servers or local to a single server in the network

IRC (more)

- Users and Channels have modes
  - User Modes
    - i – invisible, cannot be seen without a common channel or knowing the exact name
    - s - Receives server notices
    - w - Receives wallops
    - o - ser is an IRC operator (ircop)

IRC (more)

- Users and Channels have modes
  - Channel Modes
    - o– channel operator
    - p – private channel
    - s – secret channel
    - i – invite only
    - t – topic set by channel operator
    - n - Users cannot send external messages from outside the channel
    - m – channel is moderated
    - l – limited number of users
    - b – hostmasks (IRC addresses) not allowed on channel
    - v – gives user voice status
    - k – sets a channel key

IRC (more)

- A user who creates a channel becomes the channel operator
  - operators have more privileges than users
- IRC Bots
  - Bots are a special type of IRC client and are often used for performing automated administrative tasks for the net
  - treated as a regular user by the servers
    - but could be a trojan horse installed on a user machine; this constitutes a zombie

Zombies

- Network connected computers compromised by a hacker, a virus or a trojan horse program
- Owners of zombie computers are usually unaware their machine is compromised
- Most spam is sent from zombie computers
- Used as the bots in many BotNets
- Used to mount large scale DDoS attacks

Bot Uses

- DDos
- Spamming
- Sniffing and Keylogging
- Identity Theft
- Hosting of Illegal Software (or content)

Types of Bots

- GT-Bot – based on windows IRC client mIRC
  - uses core to hide itself on user machine
- Agobot – most popular bot used by crackers
  - written in C++, released under GPL
  - can be controlled by IRC or other protocols
  - uses many mechanism to run stealthy
- DSNX – Dataspy Network X
  - C++ released under GPL
  - plug-in architecture makes it easy to add functionality
- SDBot
  - written in C , released under GPL
  - harder to use but popular

An Attack

- Attacker spreads a trojan horse to infect various hosts
  - hosts become zombies and connect to IRC server on a specific channel as regular user users
    - channel may be encrypted or open
- IRC Server can be on a public network or installed on one of the compromised hosts
- Bots listen to the channel for instructions from the operator
- operator instructs the net to do “it's stuff”

For Reading

- http://www.windowsecurity.com
- http://www.wikipedia.org
  - zombie computer
  - IRC
  - RFC-1459 and RFCs 2810 – 2813