Working of zombies and Trojan horses

introduction

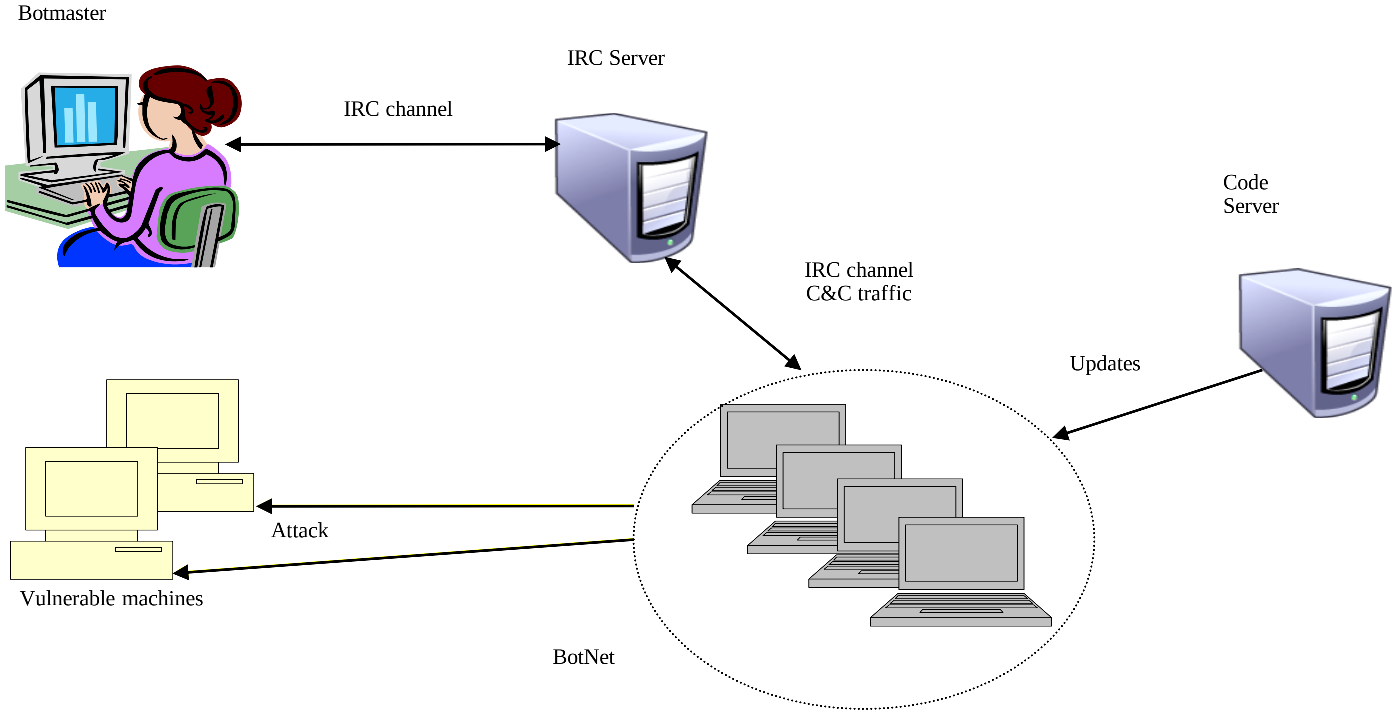
- Trojan horses are so good at disguising themselves
- Zombie – also called Bot
  - Computer taken over by someone else to do the bidding
  - Zombie has to follow the commands of zombie master
  - Do no act on their own
- Most of the time, people do not even know that their PCs are zombies and sending spam messages
- Trojans are infected just like zombies
  - Also, through software downloads

Working of zombies and bot network

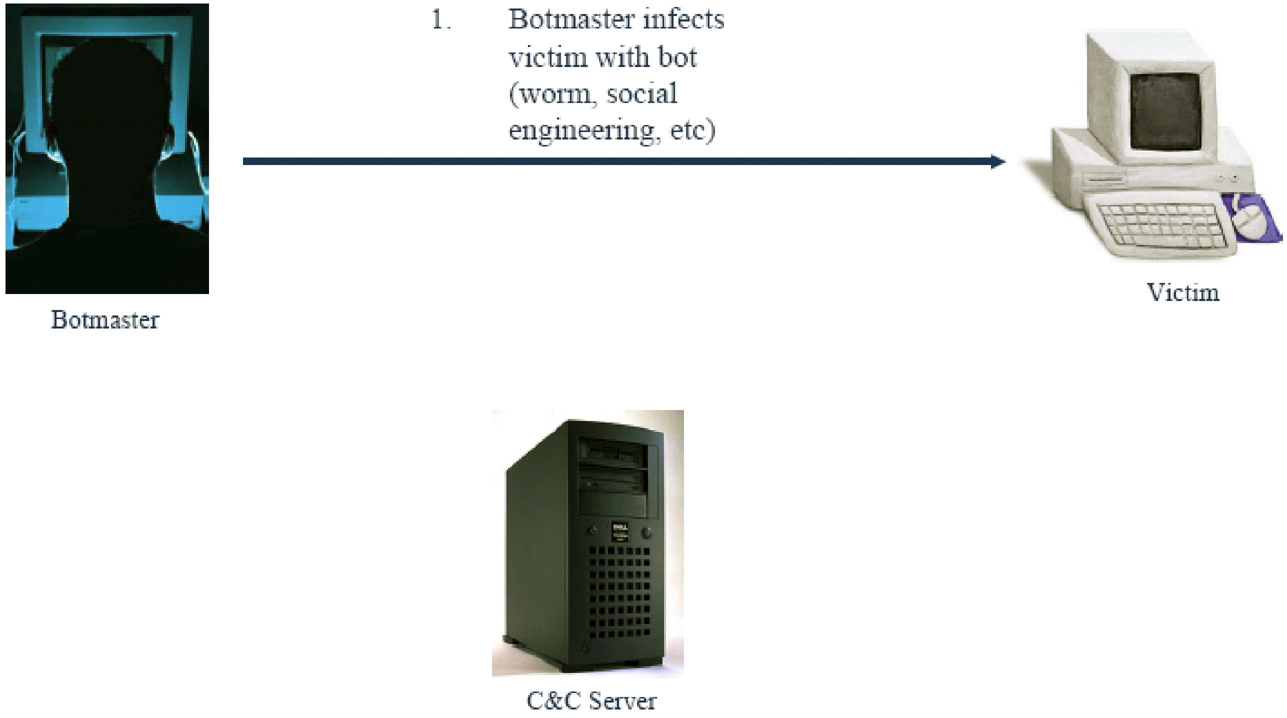
- Zombie is computer that can be controlled remotely, typically by a single person
- A single zombie network was made of more than 1.5 million PCs
- A PC can be infected by email, file transfer or by using in no security precautions
- Zombie software turns off the PC’s antivirus
- Zombie connects itself to IRC (Internet Relay Chat) and informs others that it is ready to accept commands
- Owner then sends commands over IRC to zombies ordering them to send spam or phishing messages – hence owner can’t be traced

Botnet

- Network of compromised/bot-infected machines (*zombies*) under the control of a human attacker (botmaster)



How The Botnet Grows



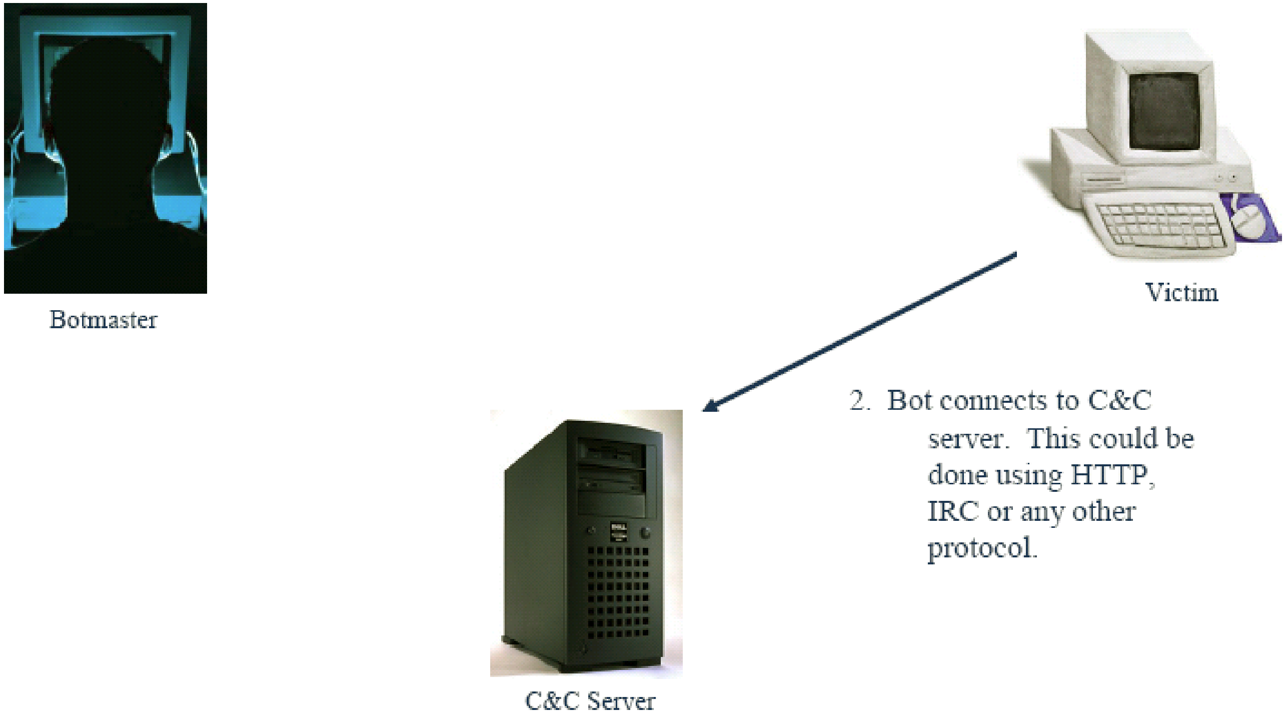
1. Botmaster infects victim with bot (worm, social engineering, etc)

Botmaster

Victim

C&C Server

How The Botnet Grows



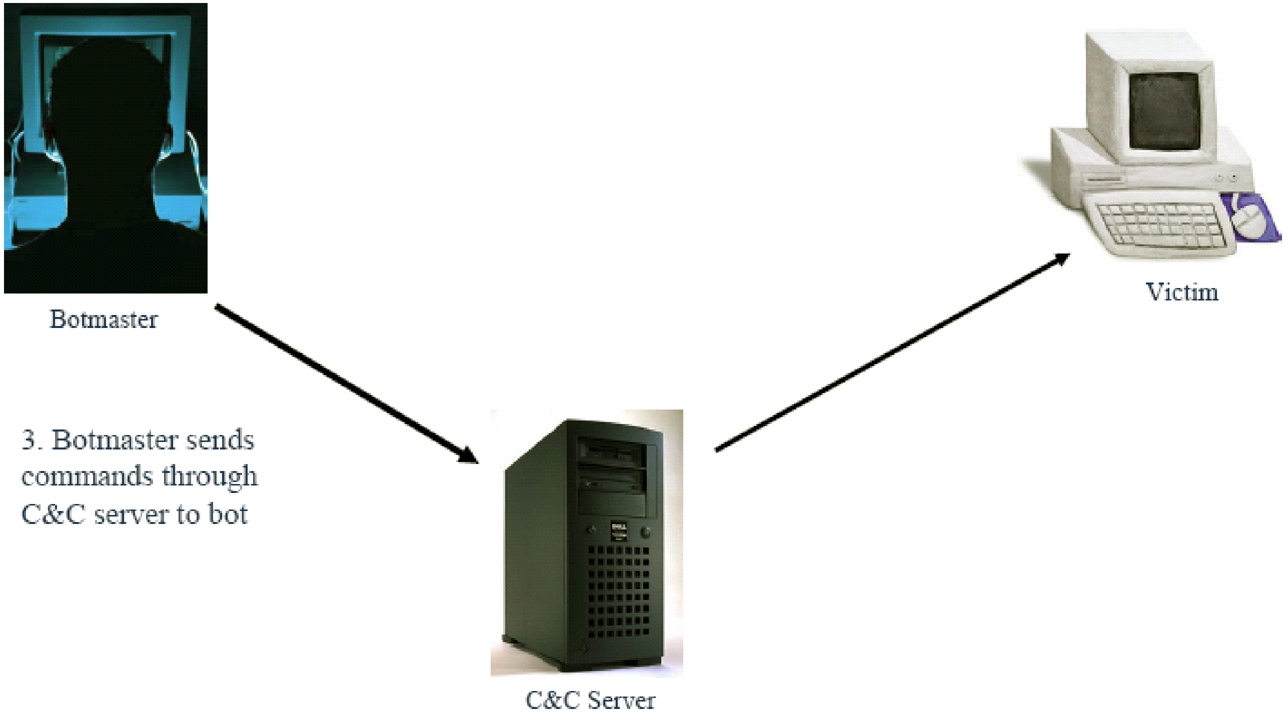
Botmaster

Victim

C&C Server

2. Bot connects to C&C server. This could be done using HTTP, IRC or any other protocol.

How The Botnet Grows



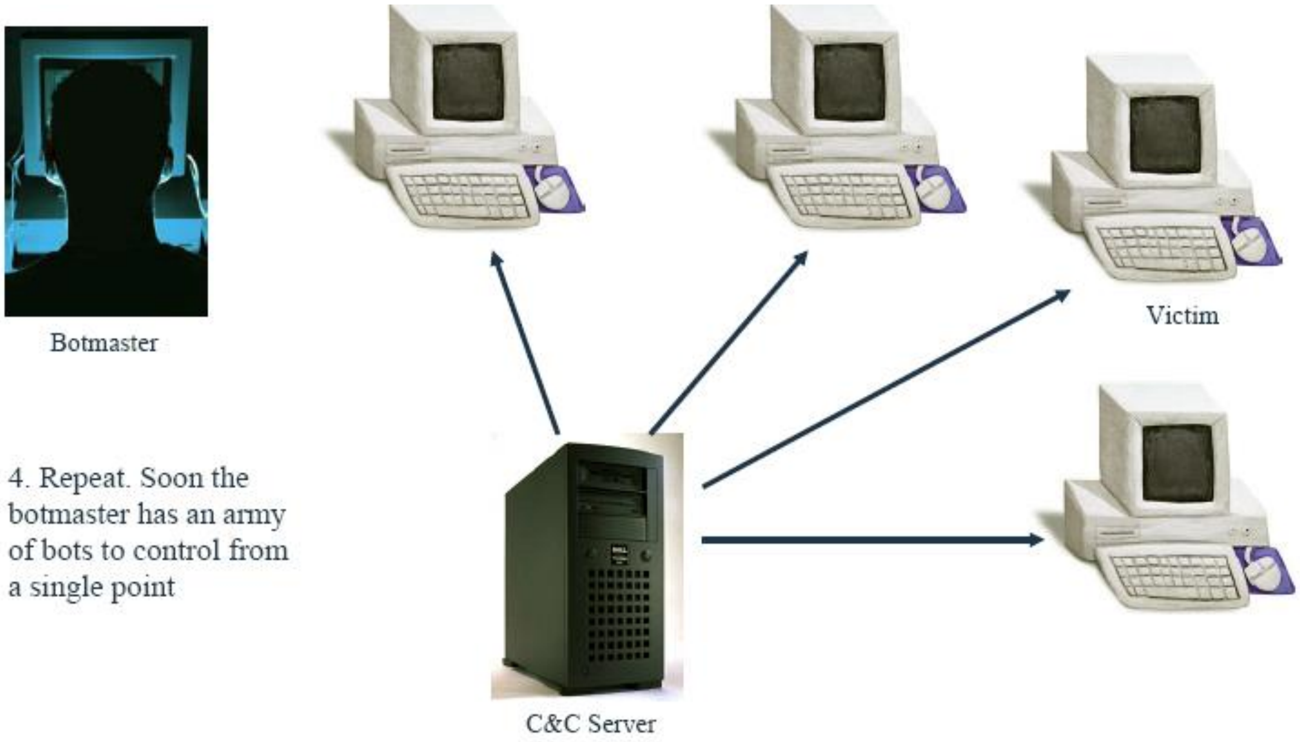
Botmaster

3. Botmaster sends commands through C&C server to bot

C&C Server

Victim

How The Botnet Grows

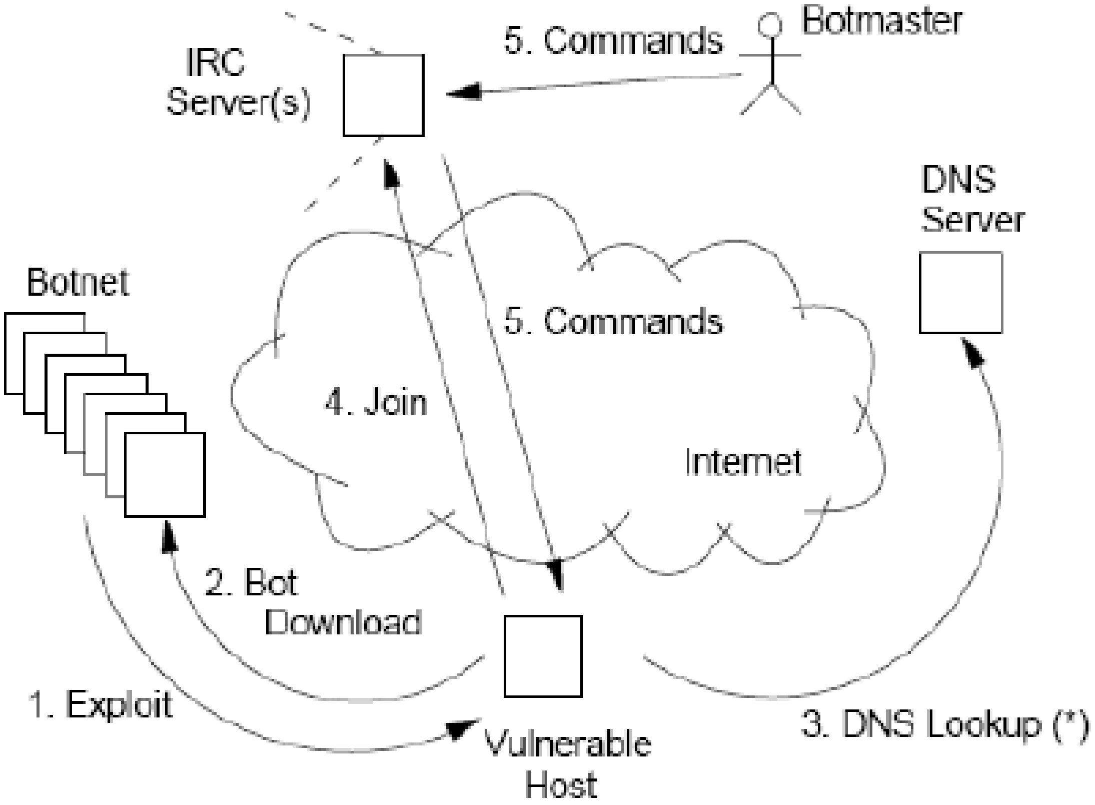


4. Repeat. Soon the botmaster has an army of bots to control from a single point

Recruiting New Machines

- Exploit a vulnerability to execute a short program (exploits) on victim's machine
  - Buffer overflows, email viruses, Trojans etc.
- Exploit downloads and installs actual bot
- Bot disables firewall and A/V software
- Bot locates IRC server, connects, joins
  - Typically need DNS to find out server's IP address
  - Authentication password often stored in bot binary
- Botmaster issues commands

Recruiting New Machines



Working of Trojan horses

- Malware that lets an intruder take control of your PC or steal information
- Emails stolen information to the intruder
- Trojan named *downloader* downloads spyware
- When an open port is observed, intruder issues commands checking for the Trojan
    - If Trojan is found, intruder establishes connection

Working of zombie and Trojan protection

- Run antivirus software and regularly update it
- Use inbound blocking firewall
- Use outbound blocking firewall
- Shutdown common ports used by Trojans and zombies

How Are They Used

- Distributed Denial of Service (DDoS) attacks
- Sending Spams
- Phishing (fake websites)
- Addware (Trojan horse)
- Spyware (keylogging, information harvesting)
- Storing pirated materials

Zombie money trail

- Amount of money paid to run zombie networks varies according to how many zombies a person controls and total aggregated bandwidth of network
- Rental for using network of zombies
- Zombie networks are involved in extortion cases

Thank you