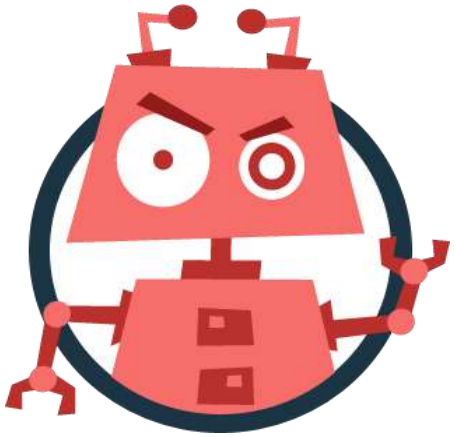
SEMINAR REPORT ON

BOTNET

BY : DHRUV GARG
2020099
BCA 2ND

INDEX

WHAT IS A BOTNET?



- The term bot is short for robot.
- Criminals distribute malware turning our computer into a bot.
- Computers perform automated tasks over the internet without us knowing it.
- Criminals use bots to infect large number of computers.
- These computers form a network which is popularly called as **botnet**.

RISKS OF BOTNET

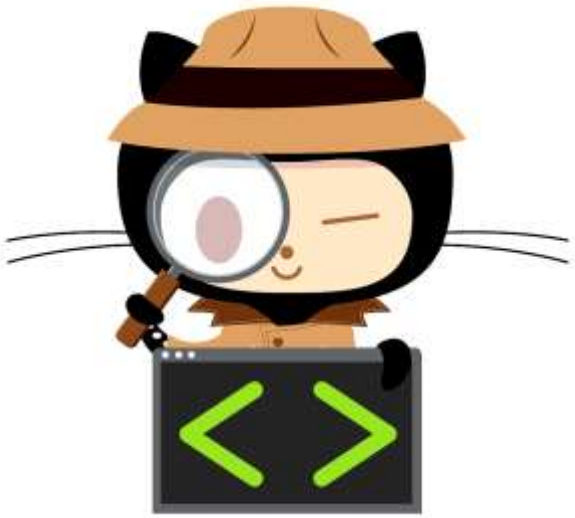
Criminals use botnets to

- Send out spam email messages.
- Spread viruses.
- Attack computers + servers.
- Commit other kinds of crime + fraud.

If our computer becomes part of a botnet, then our computer might slow down and we might be helping cyber criminals indirectly.

HISTORY OF BOTNET

- Bots originally used to automate tasks
  - IRC, IM, MUDS, online-games
- Evolved into a way to automate malicious attacks
  - Spam, control a pc, propagate etc…
- Botnets started with DOS against servers
  - Stacheldraht, Trinoo, Kelihos



BOTNETS CLASSIFICATION

Botnets can be classified into two prime categories:

- Legal botnets
- Illegal botnets

LEGAL BOTNETS

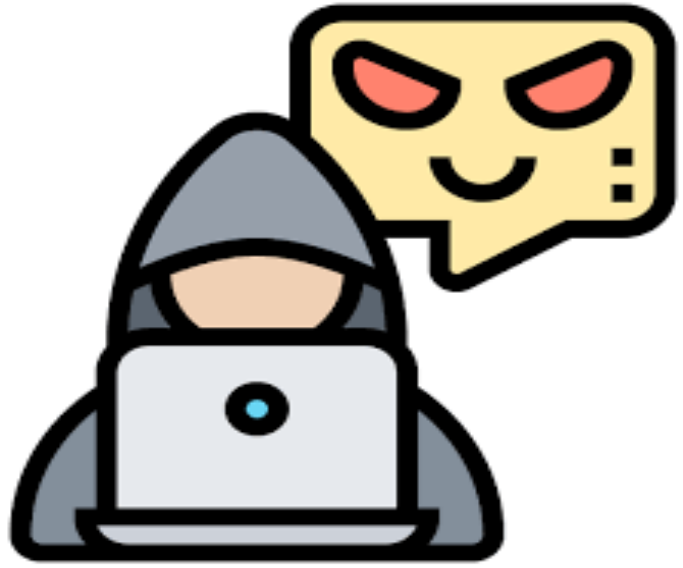
- The term botnet is widely used when several IRC bots have been linked and set channel modes on other bots and users while keeping IRC channels free from unwanted users.
- This is where the term is originally from, since the first illegal botnets were similar to legal botnets.
- A common bot used to set up botnets on IRC is **eggdrop**.

ILLEGAL BOTNETS

- Botnets sometimes infect computers whose security defences have been violated and control granted to a third party.
- Each such infected device, known as a "bot", is created when a computer is penetrated by software from a malware distribution.
- The botmaster directs the activities of these infected computers through communication channels formed by IRC and HTTP.

MOST WANTED BOTNETS

- **Zeus-** Compromised U.S. 3.6 million computers.
- **Koobface-** Compromised U.S. 2.9 million computers.
- **TidServ-** Compromised U.S. 1.5 million computers.
- **Trojan.Fakeavalert-** Compromised U.S. 1.4 million computers.
- **TR/Dldr.Agent.JKH-** Compromised U.S. 1.2 million computers.



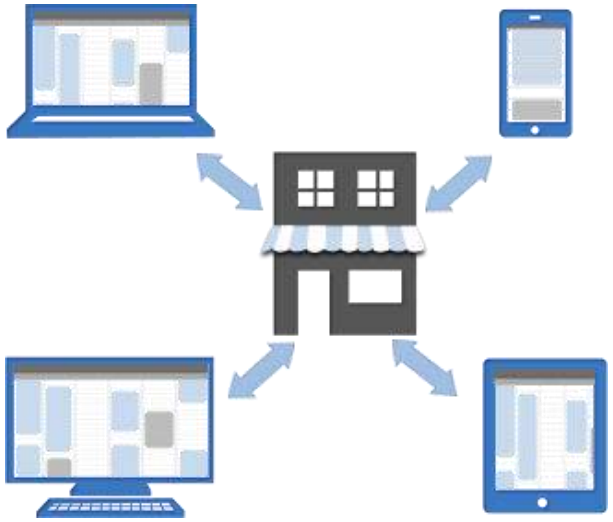
WHAT IS A BOT?

- A "bot" is a type of **malware that allows an attacker to take control over an affected computer**.
- Bots are usually part of a network of infected machines.
- Since a bot infected computer does the bidding of its master, many people refer to these victim machines as **zombies**.
- The cybercriminals that control these bots are called **botmasters**.

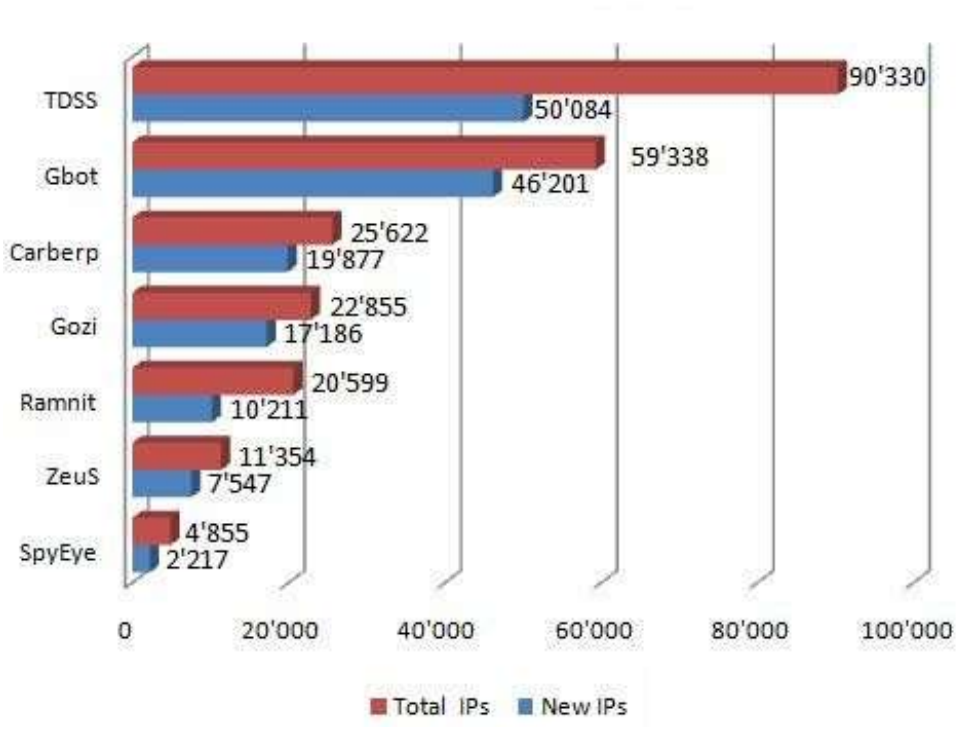
C+C MECHANISM

COMMAND AND CONTROL MECHANISM

- A collection of computers is useless without some control mechanism.
- The command and control constitutes the interface between the botnet and the botmaster.
- The botmaster commands the c&c.
- The c&c commands the bots.



BOTNET STATISTICS



DOSNET

- A type of botnet & mostly used as a term for malicious botnets.
- DoSnets are used for DDoS attacks which can be very devastating.
- Well-known DoSnet software includes
  - → TFN2k
  - → Stacheldraht
  - → Trinoo.

DOSBOT

- The denial of service bot is the client which is used to connect to the network.
- It's also the software which performs any attacks.
- The vast majority of the bots are written in the
  - → C
  - → C++
  - → Java

CONTROLLING BOTNET

Some of the Botnet Commands from Win32 bot family:

Command	Function
.capture.	Generates and saves an image or video file.
.download.	Downloads a file from a specified URL to the victim's computer.
.find file.	Finds files on the victim's computer by name and returns the paths of any files found.
.getcdkeys.	Returns product keys for software installed on the victim's computer.
.key log.	Logs the victim's keystrokes and saves them to a file.
.open.	Opens a program, an image, or a URL in a web browser.
.procs.	Lists the processes running on the victim's computer.

HOW BOTS WORK?

- Bots creep into a person's computer in many ways.
- Bots often spread themselves across the internet by looking for vulnerable, unprotected computers to infect.
- When they find an exposed computer, they quickly infect the machine and then report back to their master.
- Their goal is then to stay hidden until they are instructed to carry out a task.

PROTECT AGAINST BOTS

- Limityour user rights when online.
- Install top-rated securitysoftware.
- Increase the security settings on your browser.
- Update automatically to latestsystem patches.
- Configure your software's settings toupdate automatically.
- Never click on attachments unless you can verify the source.

MOBILE BOTNETS

- Targets smartphones, attempting to gain complete access to the device and its contents as well as providing control to the botmaster.
- Mobile botnets give admin rights of the compromised mobile devices, enabling hackers to
  - → Send e-mail or text messages
  - → Make phone calls
  - → Access contacts and photos, and more.

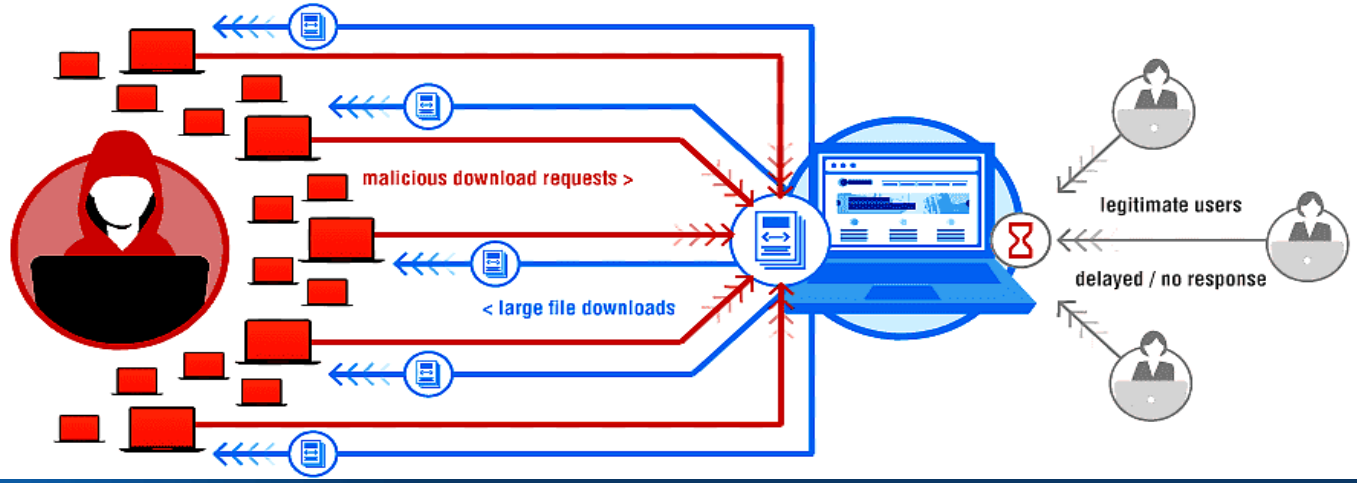
EXAMPLES OF MOBILE BOTNETS

- The Dreamdroid malware that compromised the Android devices.
- The iPhone SMS attack that affected iPhone + iPad devices.
- The Commwarrior affected Symbian series mobile devices.
- The Zitmo that targeted Blackberry users.

ADVANTAGES

❖ With the help of honeynets we are able to learn some key information (e.g. **IP address of the server or nickname of The bot**) that Enable us to Observe botnets We can extract the sensitive information about bots in a semi-automated fashion with the help of a classical **Honeywall**.

- We are able to monitor the typical commands issued by attackers and sometimes we can even capture their communication. This helps us in learning more about the motives of attackers and their tactics.



REFRENCES


Microsoft


MICROSOFT
DIGITAL
CRIMES
UNIT


Symantec.


sandvine


bing


KASPERSKY lab


TREND
MICRO


WIKIPEDIA

ANY QUESTIONS? ☺

THANK  U