============Start lecture 5 notes==========================

### Q. What is a botnet?

• A botnet or robot network is a group of computers running a computer application controlled and manipulated only by the owner or the software source.

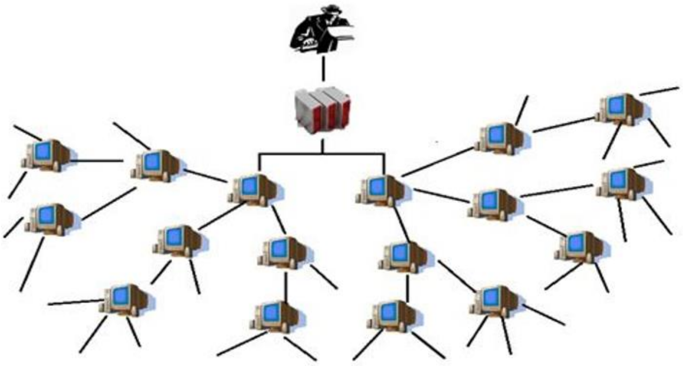
• A botnet may refer to a legitimate network of several computers that share program processing amongst them.

• Usually → group of computers infected with the malicious kind of robot software, the bots

• Once the robot software has been successfully installed in a computer → this computer becomes a zombie or a drone

• Large botnet → >5,000 bots • Small botnet → <5,000 bots

• Usually, the owners of the zombie computers do not know that their computers are bots

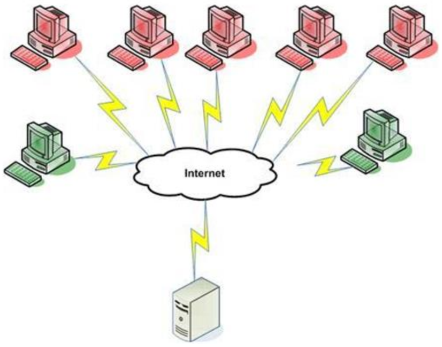


### Q. How are distributed denial of service (DDOS) attacks carried out?

➢ DDoS attack is an attack on a computer system or network that causes a loss of service to users.

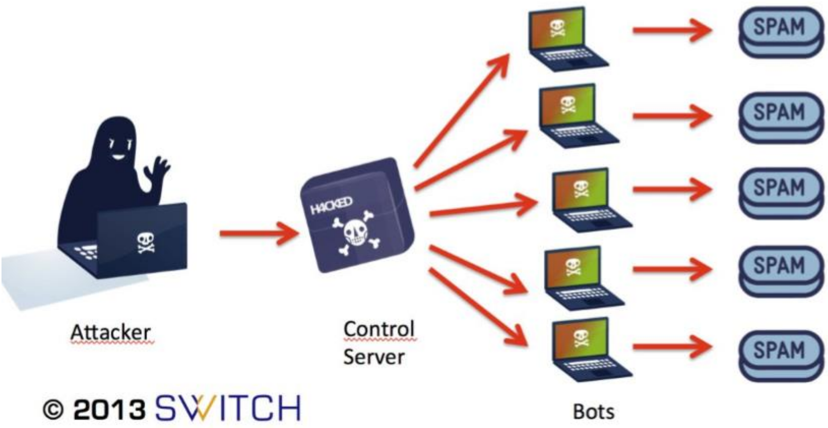
➢ Typically the loss of network connectivity and services by consuming the bandwidth of the victim network or overloading the computational resources of the victim system.

➢ Most commonly implemented and also very often used are TCP SYN and UDP flood attacks.

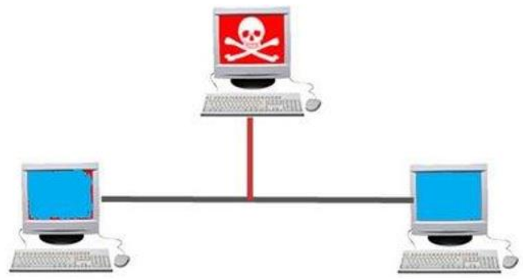


**Q. Describe 8 potential uses of botnets.**

**1. Spamming,**



**2. Sniffing Traffic**



**3. Keylogging,**

➢ Capturing of keys struck on a keyboard ➢ Encrypted communication channels → packet sniffing is useless, decrypt key is missing. ➢ Keylogger → capture info before encryption! ➢ Keylogger filter → capture specific data e.g. around “paypal.com” ➢ Keylogger on thousands of bots → paypal.com accounts quickly!

**4. Spreading new malware**

➢ Most common use. ➢ Easy → all bots implement HTTP, FTP, POP, SMTP etc. ➢ 10,000 host botnet → very fast spreading malware

**5. Advertisement Addons and Browser Helper Objects**

**6. Google AdSense abuse**

**7 Manipulating online polls/games**

**8. Attacking Internet Relay Chat (IRC) Networks**

**9. Mass identity theft**

**Q. What is a Rootkit and mention two malicious applications of rootkits.**

“A rootkit is a set of programs and code that allows a permanent or consistent, undetectable presence on a computer that allows access at the most basic level to a computer's function.”

• Many rootkits can hide files and directories. • Other features in a rootkit are usually for remote access and eavesdropping.

• Rootkits are not inherently “bad”, and they are not always used by the “bad guys”.

• Large corporations also use rootkit technology to monitor and enforce their computer-use regulations.

**Q. Give account of two primary functions of rootkits.**

Rootkits provide two primary functions:

➢ Remote Command and Control: control over files, causing reboots or "Blue Screens of Death," and accessing the command shell (that is, cmd.exe or /bin/sh).

➢ Software Eavesdropping: sniffing packets, intercepting keystrokes, and reading e-mail, capture passwords and decrypted files, or even cryptographic keys.

**Q. How do rootkits operate?**

• Rootkits work using a simple concept called modification. • In general, software is designed to make specific decisions based on very specific data. • A rootkit locates and modifies the software so it makes incorrect decisions. • There are many places where modifications can be made in software. Some examples: ➢ Patching ➢ Easter Eggs ➢ Spyware Modding ➢ Source Code Modding

**Q. List four steps that can be taken to defend against rootkits.**

Same prevention as other malware:

1. Keep systems patched.

2. Cover all the infection vectors (e.g., email attachments, Web downloads, removable media) with antivirus technologies and keep the signatures up to date.

3. Refrain from engaging in dangerous activities → torrent sites, cracked software etc.

4. Disable unneeded features and services; don't install unneeded applications.

**Q. How do you deal with a kernel level rootkit?**

• When a kernel-mode Rootkit is suspected, you cannot trust anything the kernel is telling you about the system. • Solution – Toss out the kernel and investigate with trusted tools