Computer Network Security

TE - IT

Lecture -9
02/08/2022

Session: 11:00 - 12:00 PM

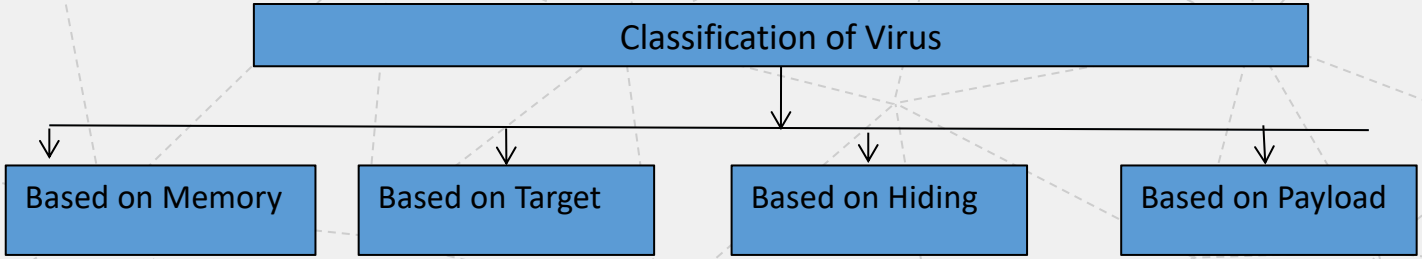
Prof. Stella J
Department of Information Technology
Xavier Institute of Engineering

Module-1

✓ Contents

1. Worms
2. Trojans
3. Logic Bombs
4. Botnets
5. Rootkits
6. Keyloggers
7. Attack Agents
8. Dos and DDOS Attack

Viruses



1. Resident Virus
2. Temporary Resident Virus
3. Non - Resident Virus
4. Swapping mode
5. User Process
6. Kernel Process

1. Compiled Virus
a. File Infectors Virus
b. Boot Sectors Virus
2. Interpreted Virus
a. Macro Virus
b. Script Virus
3. Multiparite Virus

1. No hiding
2. Encryption
3. Oligomorphic
4. Metamorphic
5. Polymorphic
6. Stealth
7. Armoring
8. Tunneling
9. Retro

1. No Payload
2. Non Destructive Payload
3. Destructive
4. Droppers

Viruses - Based on Memory

Virus: It is a category of Malicious Code that cannot self replicate itself to deliver the payload.

1. Resident Virus - Stays in Memory and affect the file which is opened
2. Temporary Resident Virus - stays for sometime and vacate the memory
3. Non - Resident Virus - do not stay in memory. It copies its payload to the files directly
4. Swapping mode - It uses swap space for residing. When It affects it goes from swap sapce to memory, performs attack and return back to swap space from memory.
5. User Process - It runs on user level access and priviliges. Infects only user files
6. Kernel Process- It is installed on the system level applications. It runs with administrative access and infect any file in the system

Viruses - Based on Target

1. Compiled Virus - It run as machine Executable, directly run by OS. Its source code run as EXE files
a. File Infectors Virus - Corrupts specific type of file, Corrupts the header to run directly the malicious code
b. Boot Sectors Virus - Infects boot sectors on the hard disk
2. Interpreted Virus - It runs at the execution timeline by line
a. Macro Virus - It presents within the document. The code blocks are usually automates the calculation steps within the document
b. Script Virus - It affects windows batch scripts, linux shell scripts and affects the power shell
3. Multiparite Virus - It spreads infection throughout the system.

Viruses - Based on hiding

1. No hiding - no special measure to hide
2. Encryption - virus uses encryption to hide
3. Oligomorphic - it is a semi polymorphic which uses several decryption routines
4. Metamorphic - it has mutation engines that changes the apperance of the viruses
5. Polymorphic - it changes the virus body insted of appearance
6. Stealth - Inorder to hide, it restores the older properties of the file
7. Armoring - It uses various technique for removal and detection
8. Tunneling - It attach themselves in the system interrupts
9. Retro - It bypass the security tools such as firewalls, IDS and security programs

Viruses - Based on Payload

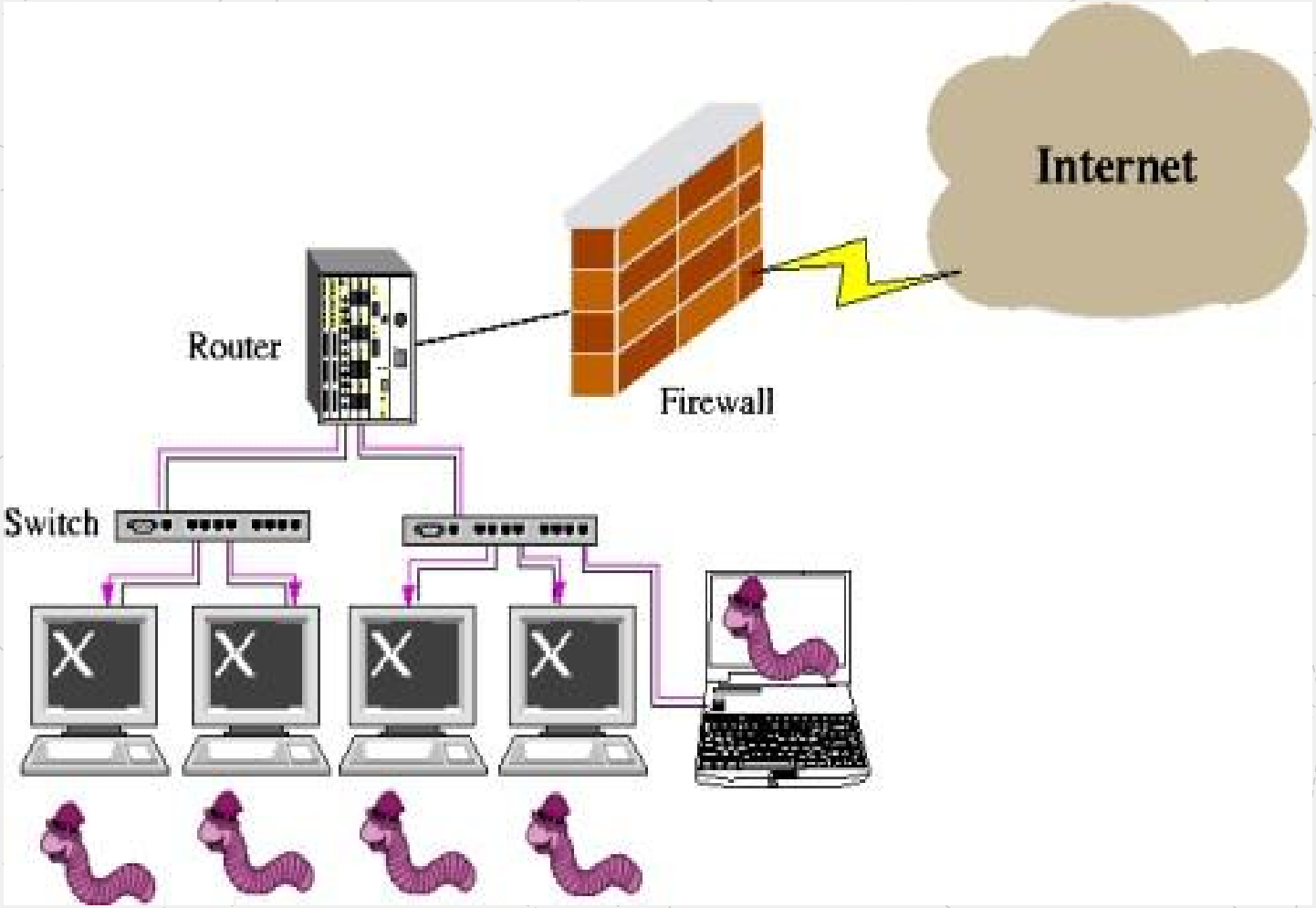
1. No Payload - It just slow down the system
2. Non Destructive Payload -It affects the device drivers such as keyboard, mouse, CD Rom and generate multiple pop ups
3. Destructive - causes severe damage, affects boot sector, file programs, applications
4. Droppers - It sits on the system and let the attacker use the systems resources to launch other attacks

Worms

“Worms are smaller malicious programs that can self replicate and trigger without needing a user action”

2 Types

1. **Network service worms:** These worms spread by exploiting vulnerabilities in the network service associated with an OS.
2. **Mass mailing worms:** It spreads through emails.
It reaches a system via an email, infects it and then looks for other email addresses in the system to send a copy of itself to other users.


Internet
Router
Firewall
Switch

Trojans

Trojans is a computer program that appears to have a useful function, but also has a hidden and malicious function that evades security mechanisms, sometimes by exploiting legitimate authorisations of a system entitiy that invokes the program

Example: Tiny Banker Trojan
It Targets the Financial Institution websites, discovered in 2012. It infects thousands of computers in Turkey

1. It steals the keystrokes
2. It gets the page information and collects the sensitive information

Logic Bombs

“Logical Bombs are malicious program that trigger when specific conditions met”

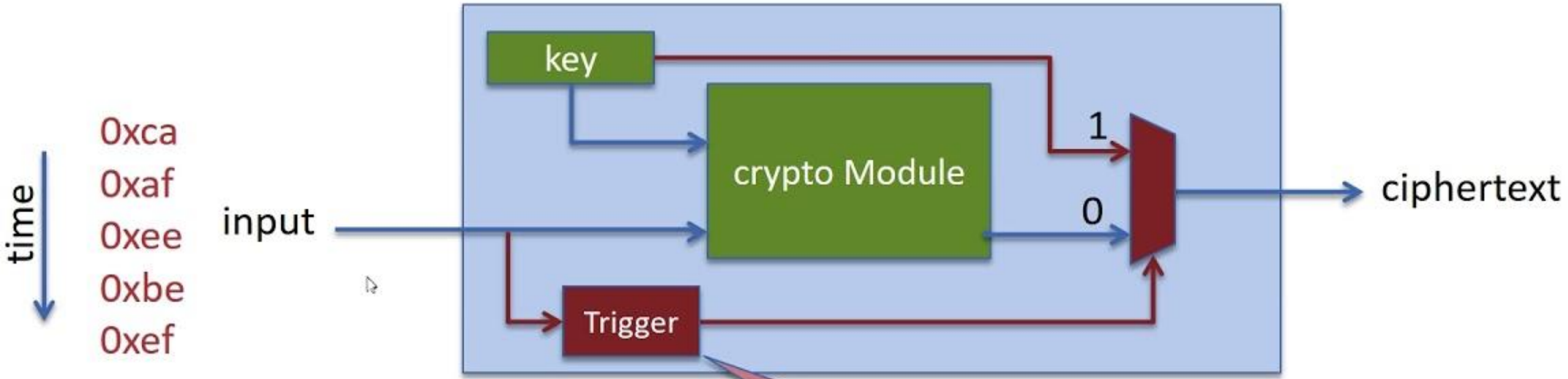
Logic Bombs can trigger based on several conditions:

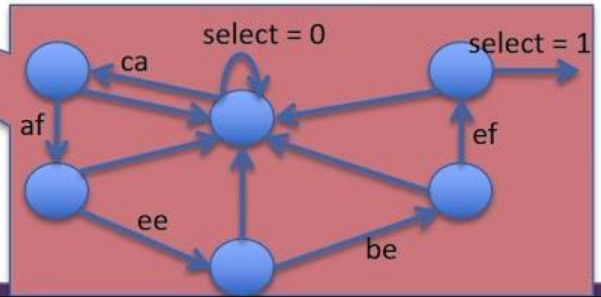
1. Date and Time on the system
2. Presence or absence of certain files or user on the system
3. Presence or absence of certain software or programs on the system

Usually the target of logic bombs is data corruption. It is important to have regular backup of the system to avoid loss of data due to logic bombs.

Example of a Hardware Trojan

Sequential Trojan (Timebombs)





Properties of Hardware Trojan:

- very small
- mostly passive

Keyloggers

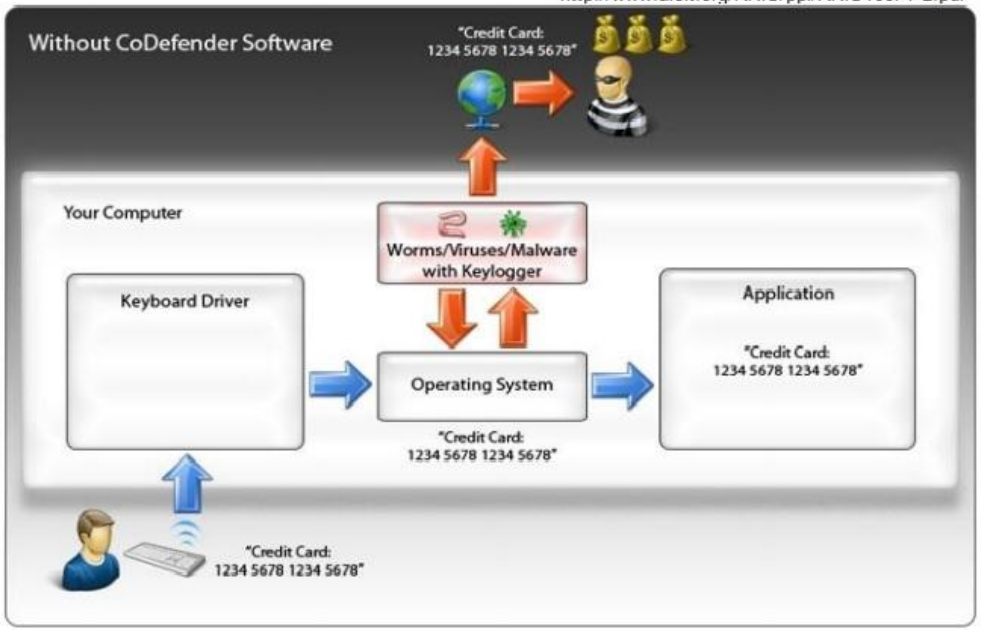
Keyloggers or simply keystroke loggers are malware programs that capture your keystrokes on the keyboard

Software Based - Keyloggers installed on the system as part of malware programs.

Hardware Based - Attacker plugs in some sort of hardware device to get the keystroke information.

Blutooth keyboards keystroke can be easily hacked with the radio frequency

http://www.aicit.org/RNIS/ppl/RNIS168PPL.pdf



Keylogging process

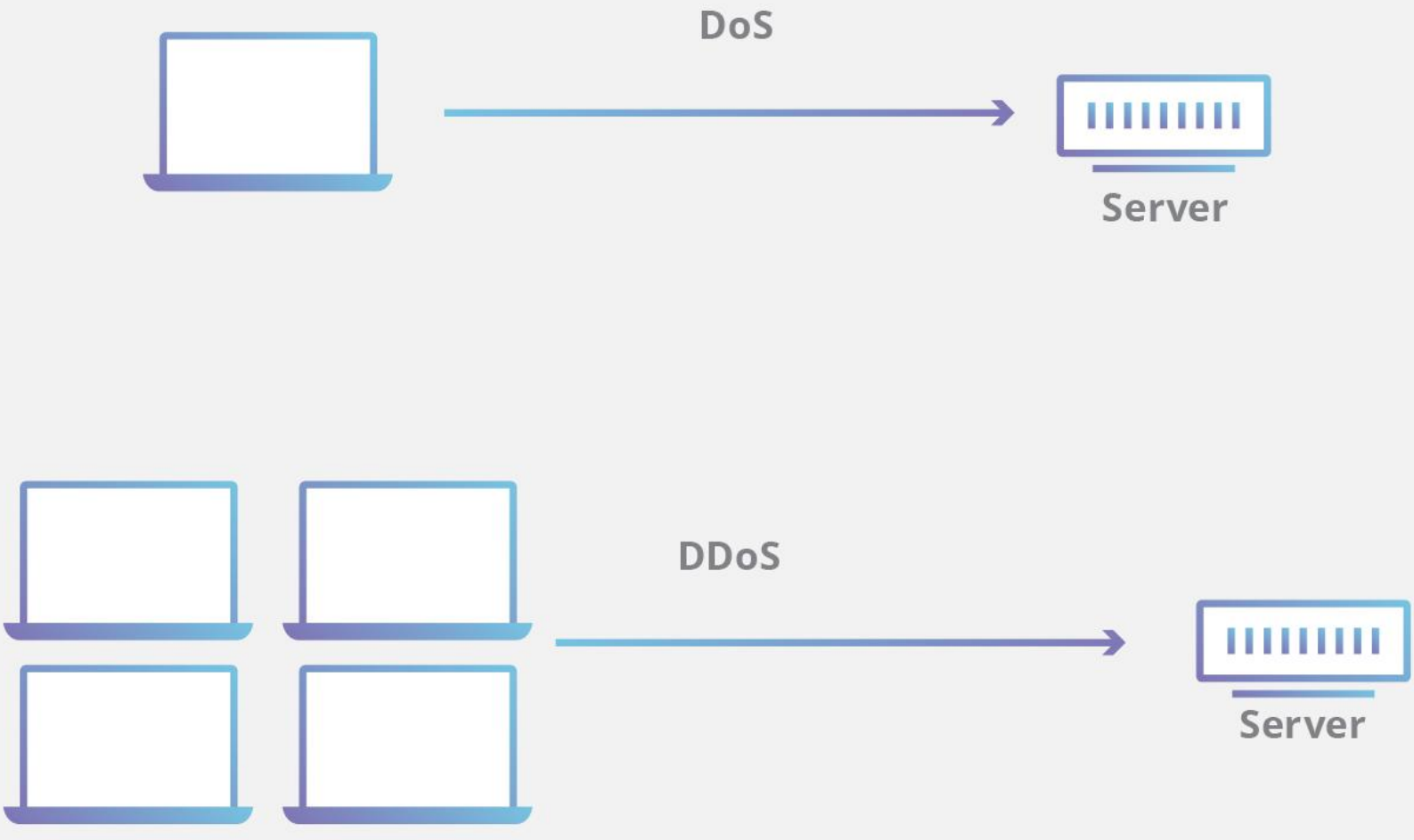
DOS and DDOS Attack

DOS Attack: Denial of Service is an attack from a single source such that the resources are exhausted on the target beyond its serving capacity.

DDOS Attack: Distributed Denial of Service is an attack from multiple sources such that the resources are exhausted on the target beyond its serving capacity.

Types of DDOS:

1. HTTP Flood - It restricts the access of webserver
2. Ping Flood - Target machine sent with many ping request, fails to respond
3. Ping of Death - Target machine is sent with so many ping request to confuse it to process, results in crash
4. Smurf Attack: The victims IP address as the receipient for receiving responses from broadcast communication.


DoS
Server
DDoS
Server

Backdoors:

Backdoor refers to a mechanism using which you can bypass the access control system to gain unautorized acess.

It is an undocumented way of gaining access to a computer system.

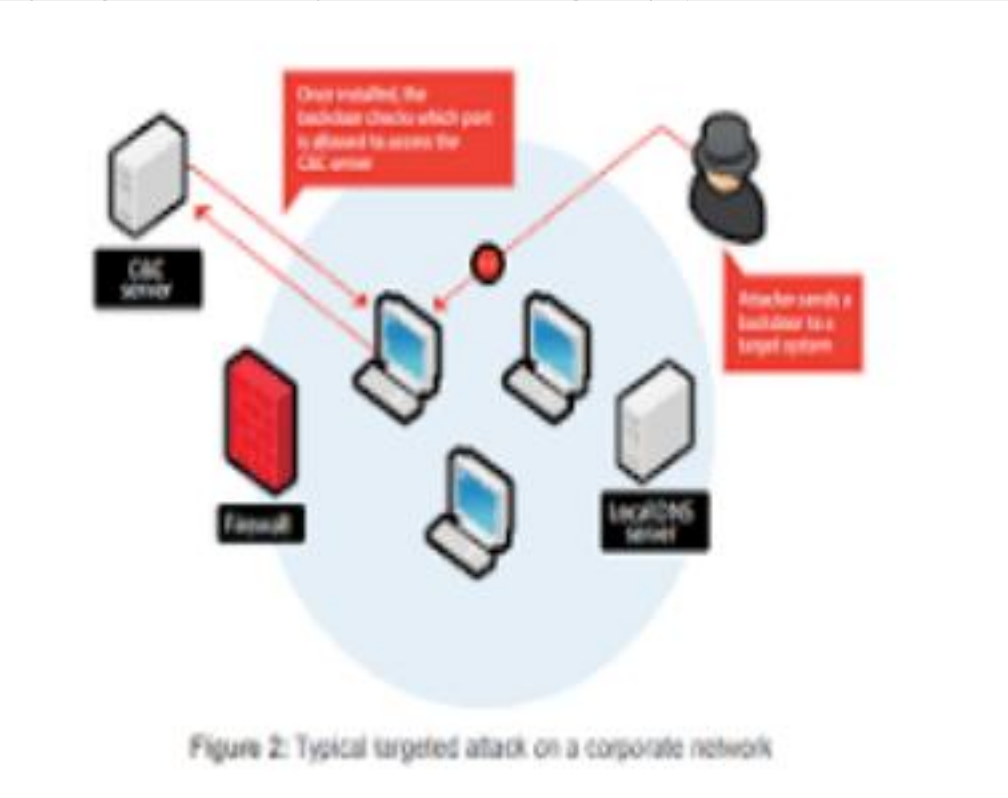


Figure 2: Typical targeted attack on a corporate network

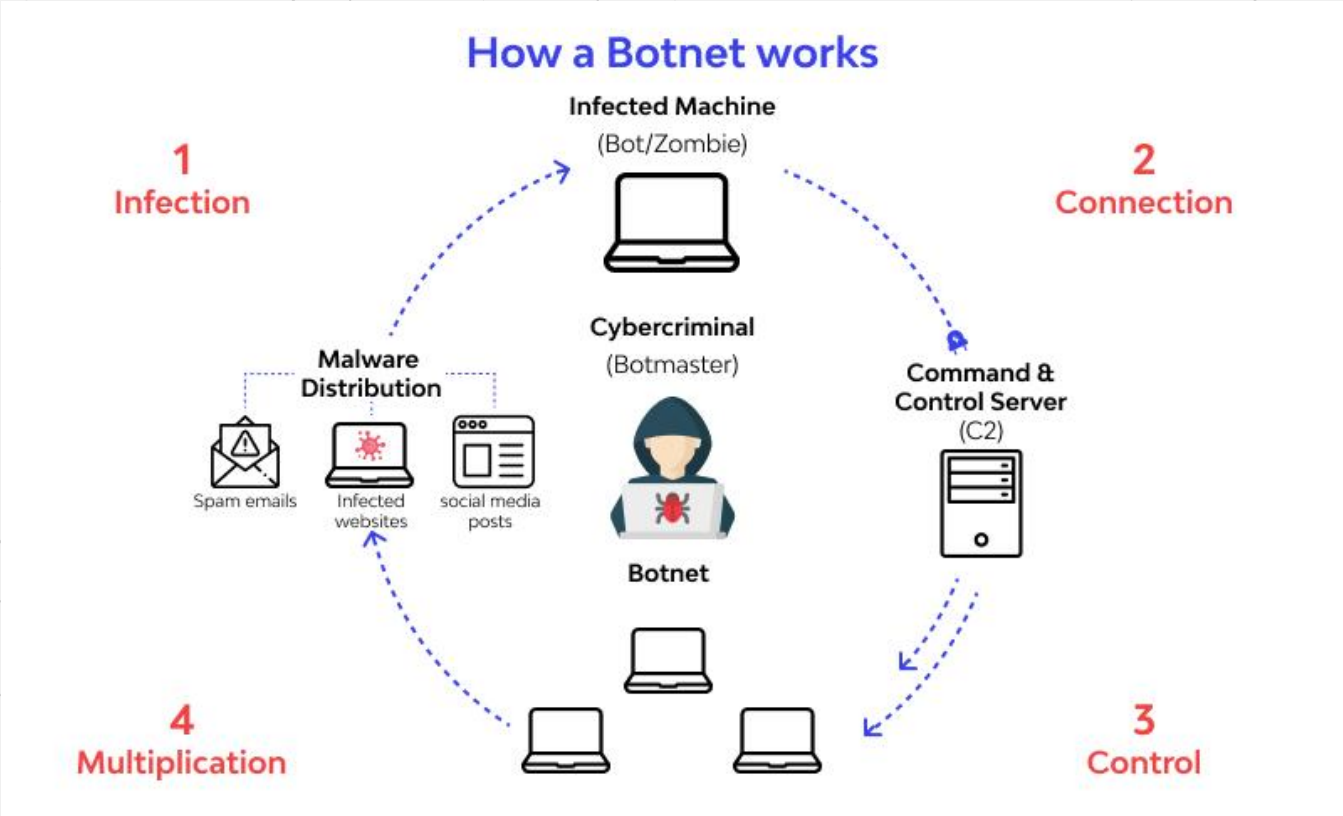
Botnets:

A botnet refers to a group of computers which have been infected by an attacker and is under his/her complete control

Components:

1. Attacker
2. Bot
3. Command and Control Center
4. Control Protocol
5. Target

Botnets:


How a Botnet works
Infected Machine
(Bot/Zombie)
1
Infection
2
Connection
Cybercriminal
(Botmaster)
Malware
Distribution
Command &
Control Server
(C2)
Spam emails
Infected
websites
social media
posts
Botnet
4
Multiplication
3
Control

THANK YOU