Ethical Hacking

Session 6

Trojans, Viruses and Worms

Learning Objective 1-2

1. Describe the purpose and indications of Trojans
2. Explain the types of Trojan
3. Define the way to detect Trojans
4. Explain virus and its effects on computers
5. List the types of virus

Learning Objective 2-2

6. Describe the working of viruses
7. Identify the difference between the viruses and worms
8. Apply virus analysis tools
9. Explain virus detection methods
10. Identify malware
11. Describe Malware analysis procedure

Introduction 1-3

- Computer systems are harmed without the user's knowledge because of:

- With the help of these, a hacker use the data in the system and perform illegal activities.

Introduction 2-3

Trojan

- Frequently occurs in a form of social engineering and convinces the user to install it in the system.

Computer Virus

- Is a malware program or a piece of code that replicates while preparing copies of the data files in the other computer system or data storage device.
- Detects in the system and driver where it starts the replication process.

Introduction 3-3

Computer worms

- Are harmful programs that affect the system, delete data, slow-down the processor of a computer and a network.

Malware

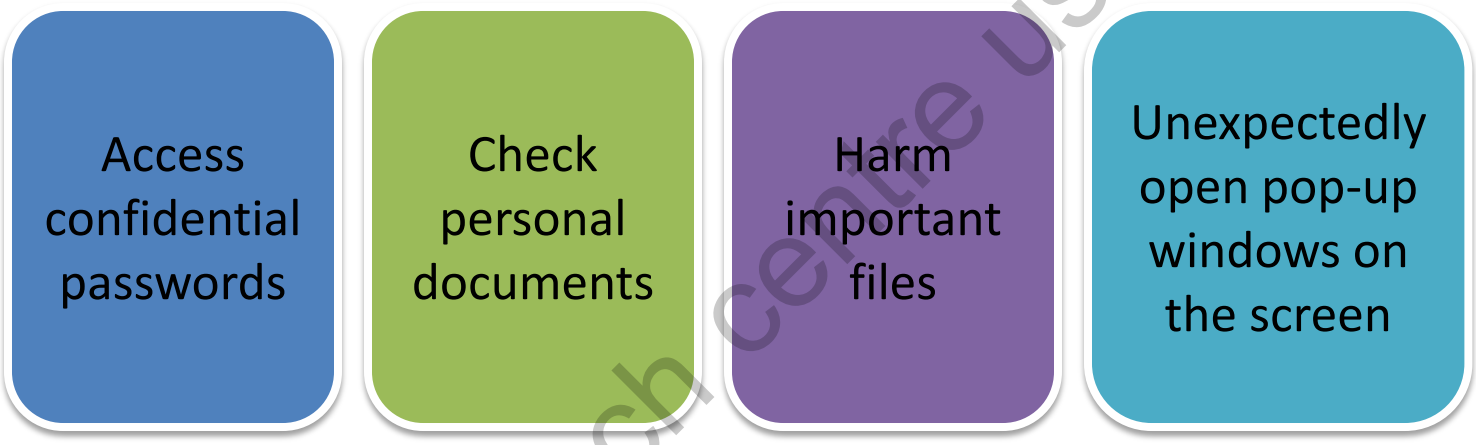
- Is malicious software, meant to interrupt the computer system operations, information or data files.
- Helps hacker to get an unauthorised access.

What is a Trojan? 1-6

- **A Trojan or Trojan Horse:**
  - Is a disguised malware program that contains harmful and malicious code that damages the software files in a computer system.
  - Appears on the system as useful software in a routine in an interesting way and influences the user to install it on the system.
  - Starts damaging the data files in the system once it gets installed or activated.

What is a Trojan? 2-6

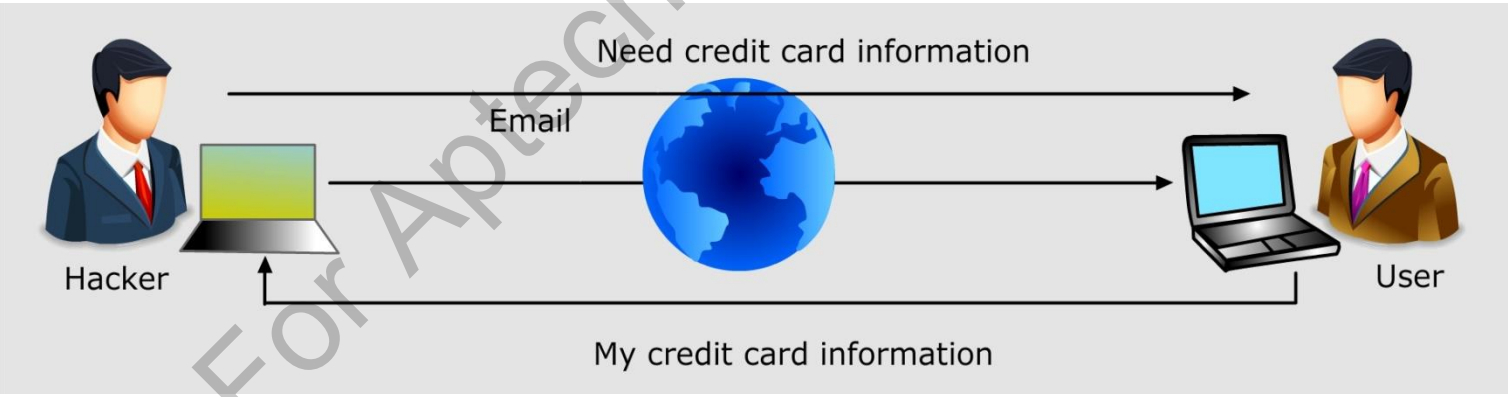
- A hacker uses Trojan programs to:



- Attackers get unauthorised access to the systems and can control it to deploy their attacks.

What is a Trojan? 3-6

- A hacker sends a mail and sets up Trojan to get access of the following, as shown in figure.
  - Credit card details
  - Facebook password
  - E-banking details
  - Personal property information



What is a Trojan? 4-6

- Trojans frequently occur in the form of social engineering such as:
  - False mails
  - Unprotected Internet pop-up messages
  - Interesting pictures
- Trojans:
  - Convinces the user to install it on the system.
  - Are downloaded with an online program or software package.
  - Can be noticed because of the reduction in the processing speed.

What is a Trojan? 5-6

- Attackers/hackers use Trojan programs to:
  - Operate files on the victim's system
  - Administer processes
  - Run commands from remote locations
  - Disturb keystrokes
  - Observe pictures on the screen
  - Access the system and restart or sometimes shut down infected hosts

What is a Trojan? 6-6

- Following are some common Trojans:

NetBus 2	Master's Paradise
GirlFriend	BackOrifice
NetBus	Whack-a-Mole

Purpose of Trojans 1-2

- Trojans:

Affect computer systems without the user's knowledge.

Help a hacker to use the data and perform illegal activities.

Purpose of Trojans 2-2

- Trojans access the systems for the following purposes:
  - Manipulate, delete or replace important data files or operating system files
  - Steal personal information such as bank details, codes, passwords, ATM and credit card details
  - Harm a victim's system and damage the data
  - Operate a victim's PC to deploy malicious files, spyware, adware and so on
  - Create false traffic and make DOS attacks
  - Disable antivirus and Firewall and modify the system settings
  - Copy video and audio files
  - Use a victim's PC as a server to attack multiple PCs and networks and to perform illegal activities
  - Link system to Botnet
  - Stealing money from online accounts

Indications of a Trojan Attack 1-3

- Trojan attacks give many indications to the users in different ways.
- Users have to identify them and take necessary steps to prevent them during the initial stages.

Indications of a Trojan Attack 2-3

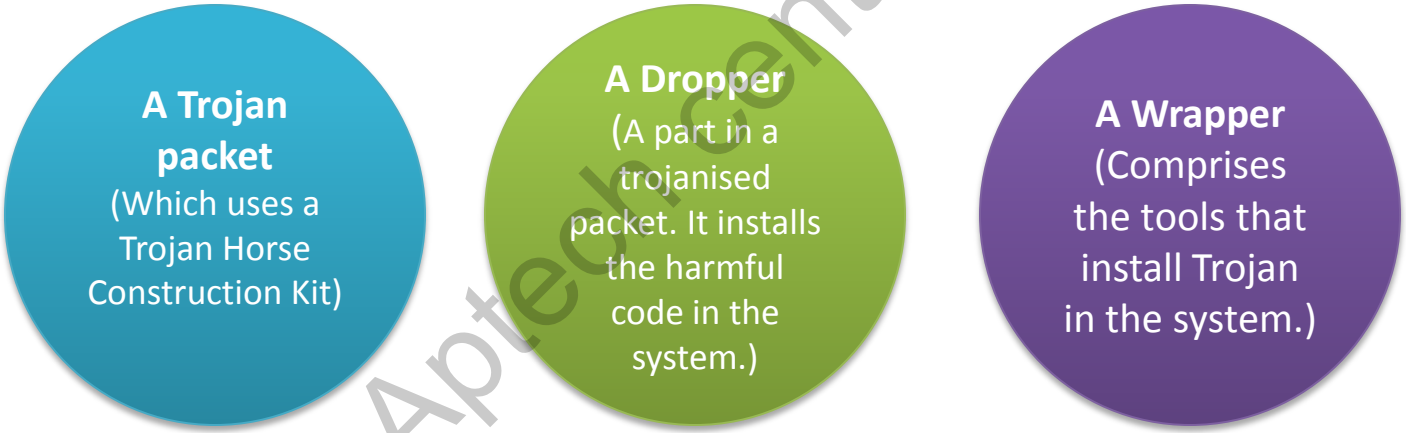
- Following are some indications that can help a user understand that a Trojan has entered the system:
  - Weird chat boxes appear on the screen suddenly
  - The browser will open unknown pages on the screen
  - CD drawer opens and closes automatically
  - Operating system will stop and ask to restart the PC
  - Antivirus and firewall will be disabled
  - Screen colour setting changes unexpectedly
  - The Start icon or taskbar disappears from screen
  - Computer setting changes
  - The account names and passwords changes
  - IP scanning will start automatically

Indications of a Trojan Attack 3-3

- Screensaver changes
- Credit card account/password changes
- Unexpected purchase bills will be added in the E-bill
- Some important files will disappear
- Settings of Wallpaper or background changes
- System functions will be affected
- The computer restarts repeatedly
- Mouse pointer will disappear sometimes and will click some other files than expected ones
- Task Manager window will not appear on the screen by pressing CTRL+ALT+DLT

How to Infect Systems Using a Trojan? 1-2

- Users need to understand how a hacker uses Trojans to infect their systems.
- The hacker aims to infect the system by creating:



How to Infect Systems Using a Trojan? 2-2

- A hacker can execute the Trojan program in the following three steps:

Different Ways a Trojan Can Get into a System 1-2

- There are many ways a Trojan can get into a user's system.
- Trojan appears in a tricky and interesting manner on your screen and grabs the attention of the user.
- A user falls victim to these things and clicks it.
- To identify the Trojan, a user needs to be careful and should understand the ways by which a Trojan enters a system.

Different Ways a Trojan Can Get into a System 2-2

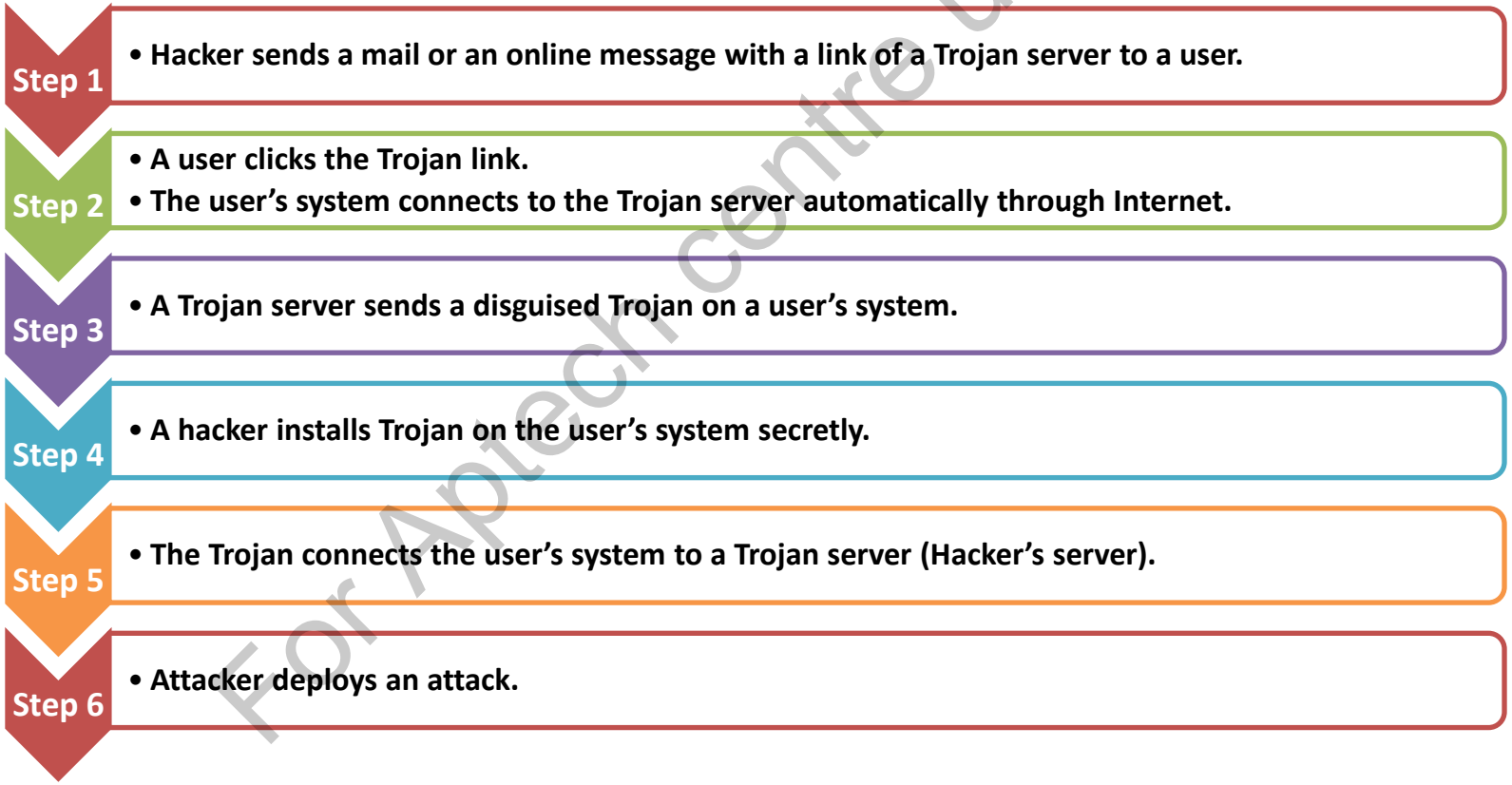
- Following are some of the ways that a Trojan enters a victim's system:
  - Email attachment
  - Instant messenger attachment
  - Internet Relay Chat (IRC)
  - NetBIOS file sharing
  - Internet software/program
  - Advertisement of free programs
  - Freeware Antivirus
  - Spyware tools
  - Screensavers
  - System optimisers
  - Pictures
  - Games
  - Videos
  - Music

How to Deploy a Trojan? 1-3

- A Trojan infects the system when a user clicks a harmful link or an attachment that was received through an email, online messages, IRCs and so on.
- A hacker uses these ways and deploys a Trojan in the user's system to get an access to a user's data.

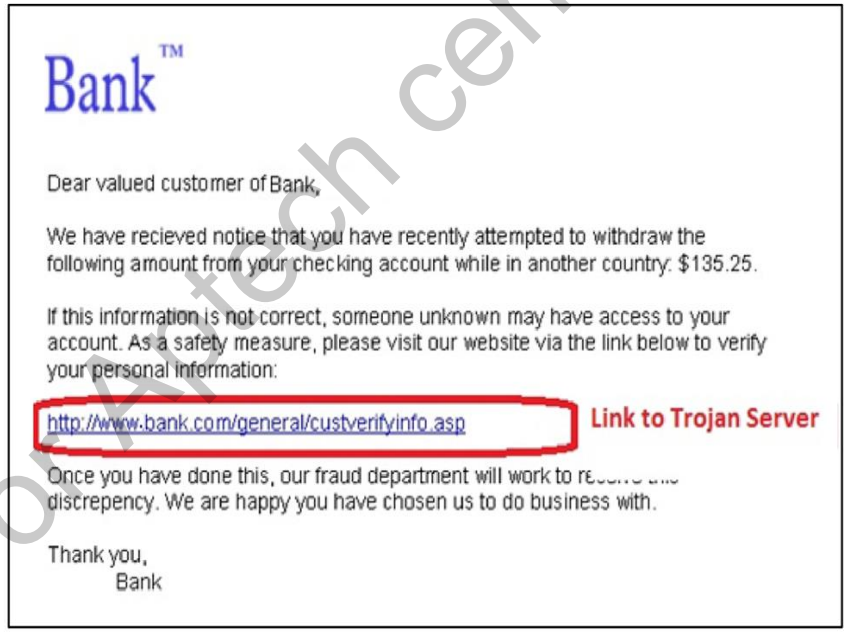
How to Deploy a Trojan? 2-3

- A hacker uses following steps to deploy Trojan in the victim's system:



How to Deploy a Trojan? 3-3

- The following example shows a phishing email that a hacker sends through the mail to the users on a system.
- If user clicks the link, system will download the Trojan and affect the system performance.



Types of Trojans 1-2

- An attacker creates various types of Trojans to prepare different types of attacks on users' systems.
- Each Trojan has its own functionality to harm the user's system.

Types of Trojans 2-2

- Some common types of Trojan are as follows:

  - Remote Access Trojans (RATs)
  - E-banking Trojans
  - Command Shell Trojans
  - Data-Sending Trojans
  - GUI Trojan
  - ICMP Trojan
  - Denial-of-Service Trojans
  - HTTP/HTTPS Trojans
  - Destructive Trojans
  - Covert Channel Trojan
  - Document Trojans
  - Proxy Trojans
  - Email Trojans
  - FTP Trojans
  - Defacement Trojans
  - Security Software Disabler Trojans
  - Botnet Trojans
  - Proxy Server Trojans
  - VNC Trojans

How to Detect Trojans? 1-2

- A user should:
  - Take proactive measures to detect Trojans on the system.
  - Beware of 'executable' files such as .exe, .bat, .jpeg and so on, as sometimes these files may have a Trojan.
  - Understand file extension as Trojans have similar types of extensions.
  - Always scan device drivers and need to check whether the drivers, applications, files and so on are downloaded from authentic original source site.

- Trojans are often installed with device drivers and get downloaded from suspicious sources.

How to Detect Trojans? 2-2

- Few of the ways to detect Trojans are as follows:

Scan for suspicious open ports	Scan for suspicious running processes
Scan for suspicious files and folder	Scan for suspicious OS services
Scan for suspicious registry entries	Scan for suspicious running processes
Scan for suspicious network activities	Run Trojan scanner
Scan for suspicious device drivers	

Trojan Countermeasures

- Following are the Trojan countermeasures that a user has to use if Trojan is detected in the system:
  - A user should check the source files and make sure that any downloaded file is from an authentic source.
  - The user should communicate with a trusted PC, person, company and so on and should not click on any suspicious link.
  - It is important to take a back-up of important files.
  - Users should turn-off the system and disconnect the Internet modem when the work is done.
  - Users can install and run Trojan scanners or new anti-virus programmes as they have anti-Trojan capabilities.
  - It is important to install Firewall security that checks inbound and outbound communication.

Introduction to Viruses 1-2

- A computer viruses are:
  - Malware programs or a pieces of code that replicates while preparing copies of data files in another computer system or data storage device.
  - Harmful to systems and tend to damage the data without the user's knowledge.
  - Man-made and can be dangerous as they use the system memory and harm the computer.

Introduction to Viruses 2-2

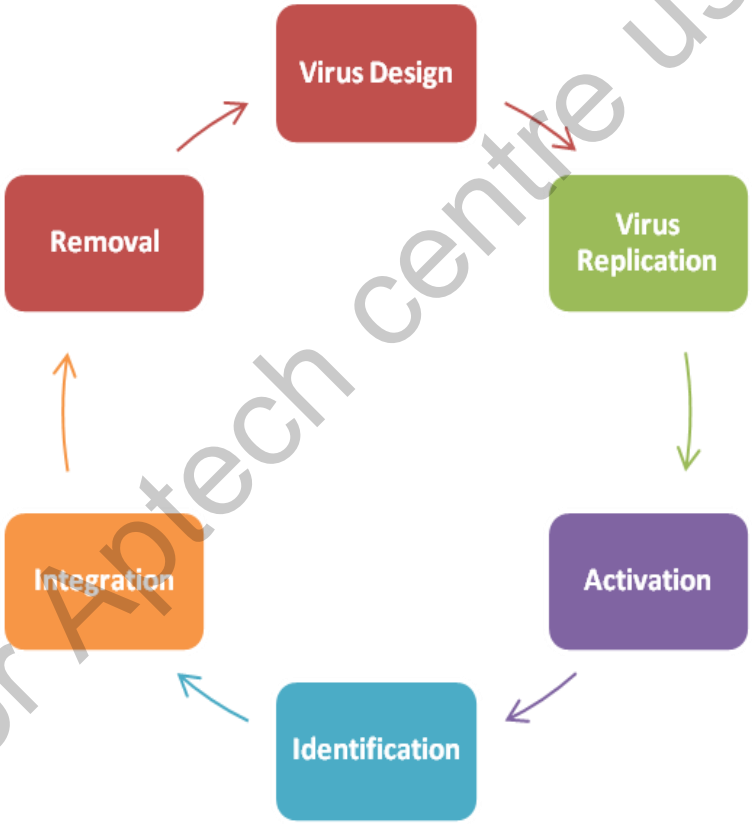
- Once a virus is detected in a system or driver and if it starts the replication process, the system or driver is 'infected'.

- Viruses are generated to:
  - Access personal information
  - Damage data and system
  - Harm the computer memory and hard disk.

- Most viruses run on the Windows-based operating systems.

Stages of Virus Life 1-3

- The different stages of virus life are as follows:



Stages of Virus Life 2-3

- The different stages of virus life are as follows:

Stage 1: Virus Design	• A hacker generates/types the virus code in a programming language or construction kits.
Stage 2: Virus Replication	• The generated viruses start replicating themselves in the system and increase the virus.
Stage 3: Activation	• A virus gets activated when a user performs any activity. • The virus starts infecting the drivers or the files in the system.

Stages of Virus Life 3-3

- The different stages of virus life are as follows:

Stage 4: Identification	• The virus is detected by the user when the computer starts malfunctioning.
Stage 5: Integration	• A capable anti-virus, installed on the system, starts defending against the virus and its replication.
Stage 6: Removal	• Users install anti-virus updates and scan the computer. The scan process removes the virus.

Why Viruses are Created? 1-2

- There are thousands of reasons of creating the viruses by the people.

- The two common purpose of creating viruses are:

Expectations of financial benefits	Causing damage to the system

Why Viruses are Created? 2-2

- Some more common reasons why hackers create viruses are as follows:
  - Control the system for some specific tasks
  - Make money
  - Damage and steal important and private data such as ATM credit card numbers and passwords, security codes and so on
  - Take revenge and prove that the virus can be prepared to damage particular software, application, network, system and so on
  - Perform pranks
  - Destruct the security systems of public, private or government organisations
  - Spread the Cyber terrorism

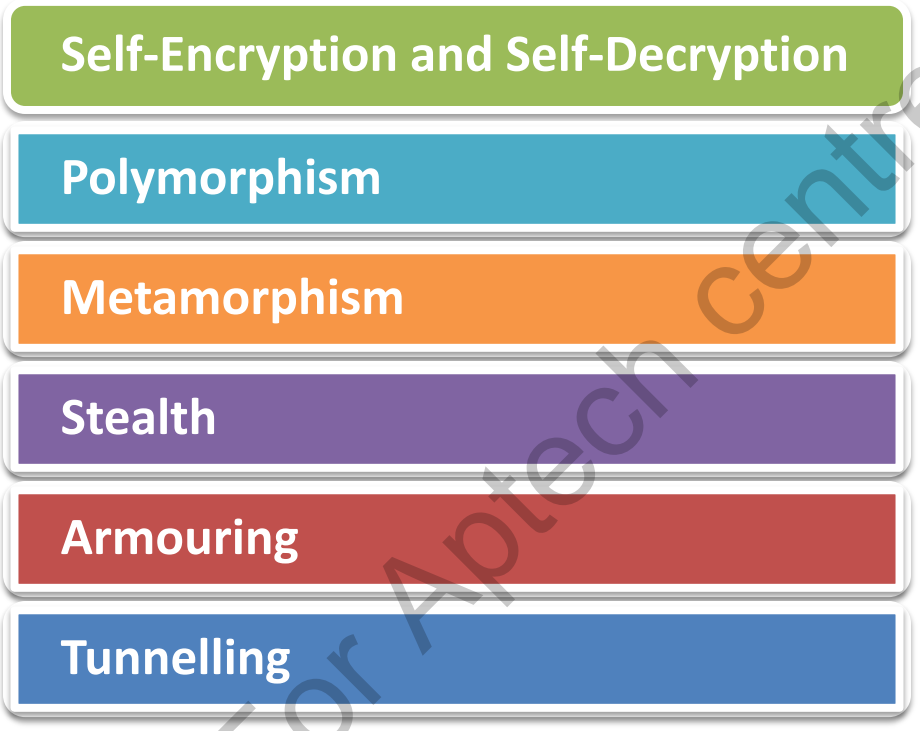
Virus Obfuscation Techniques 1-8

- Most viruses are created using one or more obfuscation techniques or ways of constructing a virus that makes it more difficult to detect.

- If a virus is hard to detect, it is likely to spread more widely.

Virus Obfuscation Techniques 2-8

- The following are commonly used obfuscation techniques:



Virus Obfuscation Techniques 3-8

Self-Encryption and Self-Decryption

- Some viruses can encrypt and decrypt their virus code bodies, concealing them from direct examination.
- Viruses that employ encryption might use multiple layers of encryption or random cryptographic keys, which make each instance of the virus to appear different, even though the underlying code is the same.

Virus Obfuscation Techniques 4-8

Polymorphism

- Polymorphism is a particularly robust form of self-encryption.
- A polymorphic virus generally makes several changes to the default encryption settings, as well as altering the decryption code.
- In a polymorphic virus, the content of the underlying virus code body does not change; encryption only alters its appearance.

Virus Obfuscation Techniques 5-8

Metamorphism

- The idea behind metamorphism is to alter the content of the virus itself, rather than hiding the content with encryption.
- The virus can be altered in several ways.
- For example, by adding unneeded code sequences to the source code or changing the sequence of pieces of the source code, a virus can be altered.
- The altered code is then recompiled to create a virus executable that looks fundamentally different from the original.

Virus Obfuscation Techniques 6-8

Stealth

- A stealth virus uses various techniques to conceal the characteristics of an infection.
- For example, many stealth viruses interfere with OS file listings so that the reported file sizes reflect the original values and do not include the size of the virus added to each infected file.

Virus Obfuscation Techniques 7-8

Armouring

- The intent of armouring is to write a virus so that it attempts to prevent antivirus software or human experts from analysing the viruses' functions through disassembly, traces and other means.

Virus Obfuscation Techniques 8-8

Tunnelling

- A virus that employs tunnelling, inserts itself into a low level of the OS so that it can intercept low level OS calls.
- By placing itself below the antivirus software, the virus attempts to manipulate the OS to prevent detection by antivirus software.

Indications of Virus Attack

- Following are the indications of a virus attack:
  - Computer starts functioning in unexpected manner and performs some abnormal activities
  - Computer processes slowly and may take hours to perform a single task
  - Driver and file names get changed unexpectedly
  - System starts, stops or hangs sometimes
  - Error messages appear repeatedly
  - Hard disk shows accessing multiple times
  - Browser window freezes and stops functioning
  - Anti-virus gets disabled and firewall stops working

How does a Computer Get infected by Viruses?

- A user can determine that a computer system is affected by virus when the following problems are seen in the system:
  - The latest anti-virus will fail to run on a system
  - New plug-ins will not be installed or updated
  - Installing pirated software
  - Opening infected email attachments and files
  - Downloading files or attachments without verifying the source

Types of Viruses 1-2

- Following are some of the common types of viruses in the computer:
  - System or Boot Sector Viruses
  - File Extension Viruses
  - File and Multipartite Viruses
  - Klez
  - Companion/Camouflage Viruses
  - File Overwriting or Cavity Viruses
  - Cluster Viruses
  - Macro Viruses
  - Encryption Viruses (This is the Obfuscation technique, recommend to delete it)
  - Sparse Infector Viruses
  - Shell Viruses

Types of Viruses 2-2

- Following are the components of a computer system that can affect by virus:
  - System drivers
  - System files
  - Source code
  - Macros
  - Supporting files such as DLL and INI
  - Disk clusters
  - BAT files

Working of Virus

- If a virus enters a system, it starts infecting the data files by replicating themselves initially.
- Later, it attacks the files and damages them.
- Viruses work in the following two phases:

Infection Phase	Attack Phase
• Viruses start increasing themselves by the replication process and attach to the .exe files in the system. • Some files start the infection process when a user starts executing them and the other files starts infecting the data files when users activate them.	• Viruses activate themselves in coordination with the system files and try to damage the system. Some viruses replicate and start deleting files. • This process slows down the session timing. These viruses harm the target once they spread.

Computer Worms

- **Computer worms:**
  - Are harmful programs that affect the system, delete the data and slow-down the processor of a computer and a network.
  - Replicate and execute themselves in the system.
  - Start spreading throughout the system independently and harm data files on the computer.
- **Hackers:**
  - Often create worms to spread in a network with the help of existing resources. Some other worms use a payload and harm the host system.
  - Utilise worm payload and install backdoors in a system. These worms prepare the botnets that are useful for the hacker to perform a cyber attack.

Difference between Virus and Worms 1-3

- **Viruses and worms:**
  - Are generally used by the hackers to damage the system files.
  - Are similar as both are malicious and harm the computer.
  - Create the Trojans and backdoors to transfer themselves from one system to other.

- Hackers make changes in a system to get access to a victim's computer to perform the illegal activities.

Difference between Virus and Worms 2-3

- A worm itself is a virus that replicates itself and utilises computer memory.
- A virus attaches itself to the other programs in the system.
- Worms are activated whenever a file and information transfers on a computer system.
- It starts spreading automatically in the system via the infected network. Virus does not have this feature.

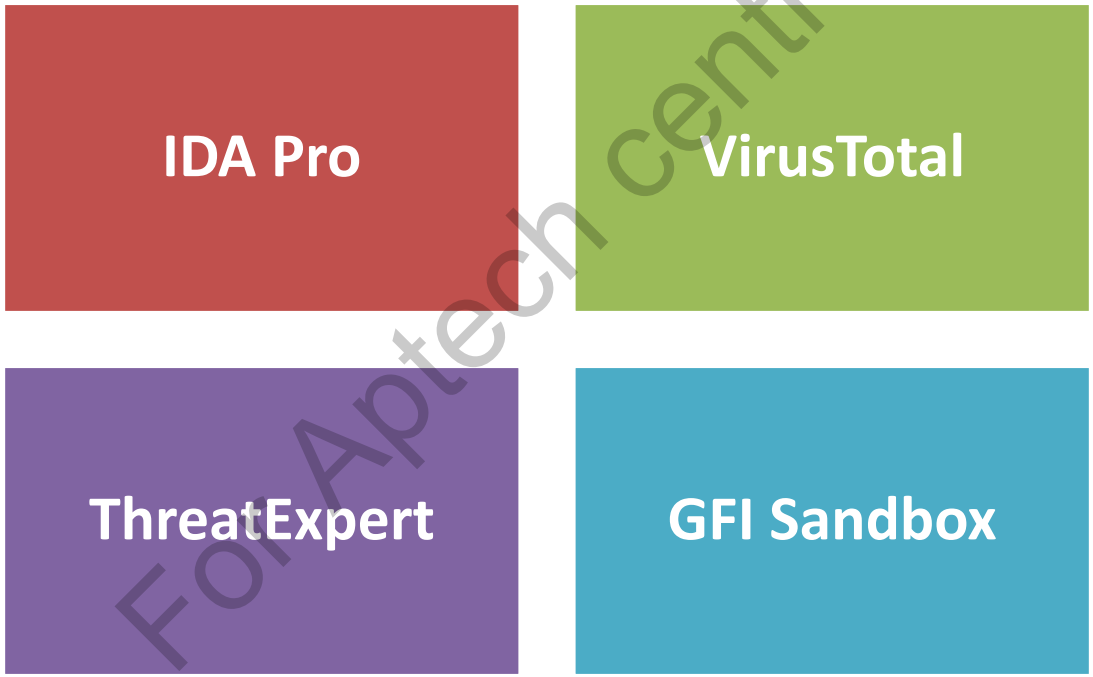
Difference between Virus and Worms 3-3

- Following table shows the difference between the computer virus and worm:

	Computer Virus	Computer Worm
Definition	A virus is a malicious code or a program that connects to the system application and runs with it.	A worm replicates itself and use existing resources in the system.
Spreading Speed	Viruses are slower than worms.	Worms are faster than viruses.
Infecting Files	Virus deletes or does change in the existing files or the location of the files.	Worms do not delete the system files but only dominates or take control of the memory.
Spreading Process	A virus transfers through the user's files, folders or programs through the network or storage devices in other systems.	A worm uses network to replicate and spread in other computers without human intervention.
Infection process in the computer system	A virus enters in a system file or a program.	It identifies weak area in the system and starts infecting through the replication process.

Virus Analysis Tools 1-10

- A user can analyse the virus if the virus, its type and its location in the system is known.
- Following are the virus analysis tools:



Virus Analysis Tools 2-10

IDA Pro

- Is a unique interactive virus analysis tool.
- Disassembles multi-processor united along with a local and remote debugger.

Virus Analysis Tools 3-10

VirusTotal

- Is a free online Web site that checks virus infected files.
- Comprises multiple anti-viruses and scan-engines that check a user's files and verifies those files. A user can upload a 64 MB file in this online tool and get the report on email.
- Also scans suspicious URLs and is available in multiple languages.

Virus Analysis Tools 4-10

GFI Sandbox

- Is a tool that filters the viruses and spam through email.
- Is also monitors and scans networks.
- Is used by professionals for a quick analysis of suspicious files.
- Helps users protect their files from the online hackers by searching for viruses and malwares.
- Helps users to identify the virus and its threat in a controlled environment.
- Helps users provide the report of virus execution process, system modification done by virus-generated network traffic.

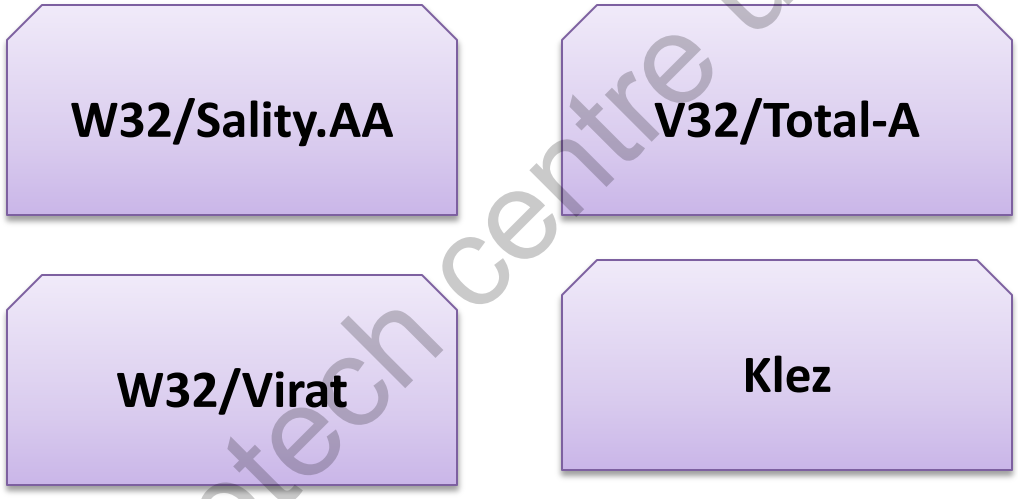
Virus Analysis Tools 5-10

ThreatExpert

- Is an advanced threat analysis tool that analyses a virus and the risks that occur while executing it.
- Is an automated tool that analyses the sample and generates a detailed report with all technical reasons behind the virus threats.

Virus Analysis Tools 6-10

- Following are the examples of virus analysis:



Virus Analysis Tools 7-10

- **W32/Sality.AA:**
  - Is a virus which perform as a keylogger.
  - Spreads through the emails by piggy-banking on **W32/Netsky.T** worm.
  - Infects .exe and .scr files on the drives and eliminates Windows based drivers.
  - Creates the files such as `<system>\vcmgcd32.dll` and `<system>\vcmgcd32.dll_`.
  - Deletes all .vdb and .avc files.
  - Changes `<Windows>\system.ini` by adding `[MCIDRV_VER]` and `DEVICE=<random string>`.

Virus Analysis Tools 8-10

- **V32/Total-A:**
  - Is an email-aware virus appears with an attachment as BinLaden_Brasil.exe.
  - Shows subject as a conflict in Afghanistan.

Virus Analysis Tools 9-10

- **W32/Virat:**
  - Is a member of polymorphic memory-resident attaching file infectors.
  - Tries to infect .exe and .scr files.
  - Sets the command to provide user access to the .asp, .php, .htm and html files at the site where virus is trapped.

Virus Analysis Tools 10-10

- **Klez:**
  - Is a virus where emails appear with selected subject haphazardly.
  - Arrives as an email attachment.
  - Is a mass-mailing virus that lives in memory.

Virus Detection Methods

- Following are the virus detection methods that help users to detect the viruses:

Scanning	Integrity checking	Interception based on a virus signature
• User can write a scan program once the virus is identified. • The scanning program checks the system for signature string characteristics of the virus.	• The integrity checking products read the entire disk of the system and record integrity data that work as a signature for the system fields and files.	• The interceptor observes the written requests of the operation system.

Malware 1-3

- **Malware:**
  - Is malicious software, meant to interrupt computer system operations, information or data files.
  - Helps hacker to get an access using a malware programme.
  - Is also known as computer pollutant as it disturbs the computer system.
  - Contains destructive bugs and appears as software.
  - Displays as legitimate software sometimes and may be received from official Websites.
  - Appears as an attractive program but that may contain harmful malware.

Malware 2-3

- Malwares are generated in the form of codes, scripts, content or software and include the following in it:

  - Trojan horses
  - Spyware
  - Adware
  - Ransomware
  - Rogue security software
  - Worms
  - Keyloggers
  - Dialers
  - Rootkits
  - BHOs
  - Govware
  - Malicious programs

Malware 3-3

- Users or organisations use firewalls, anti-virus, anti-malware to protect the computer systems against malware attacks.
- These scanning tools help the users to identify and prevent malware spread in the computer network.
- Most of the malwares appear in emails, messages, images with a fishing clickable links.
- User gets attracted towards the clickable item/links and fall victim to malware.

Online Malware Testing

- Following are the online malware testing tools:

Sunbelt CWSandbox or ThreatAnalyzer

- Is online security service that enables users to analyse malware application and threat activities.
- Utilises native windows.
- Does not use emulators and virtual environment to test malware.
- Reads the interaction between applications and detects suspicious behaviours of activities.

VirusTotal

- Is a free online malware scanning service that observes and analyses suspicious URLs and files in a system or a network.
- Is an online scanner that provides the facility to detect worms, viruses, trojans and all malwares identified in the computer system.

Malware Analysis Procedure

- Following are the online malware testing tools:

Step 1	• A user should make sure that malware is inactive in a system and then carry out the static analysis.
Step 2	• Users should gather information about string values and packaging and compressing techniques.
Step 3	• It is important to ensure that the network connection is plugged-in and working properly without errors.
Step 4	• The virus should be run and the process should be observed by using the **Process Monitor** and **Process Explorer**.
Step 5	• Information of network traffic should be recorded by using **NetResident** and **TCPView** tool.
Step 6	• The files, processes and the changes in the registry should be identified by using **RegShot**.
Step 7	• **OllyDbg** and **Proc Dump** debugging tools can be used to gather information about the service requests, DNS tables, incoming and outgoing attempts and so on.

Online Malware Analysis Services

- Few online malware analysis services are as follows:
  - Avast! Online scanner (*http://onlinescan.avast.com*)
  - Kaspersky File Scanner (*http://www.kaspersky.com*)
  - Dr. Web Online Scanners (*http://vms.drweb.com*)
  - ThreatExpert (*http://www.threatexpert.com*)
  - Filterbit (*http://www.filterbit.com*)
  - Malware Protection Center (*http://www.microsoft.com*)

Virus and Worms Countermeasures

- Following are the virus and worms countermeasures:

  - One should search and study about latest viruses and worms.
  - One should not add an infected external harddisk, pendrive, CD or DVD to the system.
  - A user should scan the external storage devices using the updated anti-virus and scanner.
  - The pop-up blocker and the Internet firewall should be turned on.
  - Disk clean up, defragmentation and registry scanner should be run once a week.
  - Anti-virus and anti-spyware software should be run once a week.
  - File extension should be checked and double file extension files should be ignored/ removed.
  - Instant messengers should be used carefully as it transfers viruses and worms
  - A user should not click unknown links, attachments and images.

Summary 1-5

- Trojan frequently occur in a form of social engineering such as false mails, unprotected Internet pop-up messages or interesting pictures and convince the user to install it in the system.
- Some common Trojans are NetBus 2, Master's Paradise, GirlFriend, BackOrifice, NetBus, Whack-a-Mole and so on.
- Trojans affect computer systems without the user's knowledge and help a hacker to use the data and perform illegal activities.

Summary 2-5

- To infect the system, create:
  - A Trojan packet (Which uses a Trojan Horse Construction Kit)
  - A dropper (A part in a trojanised packet). It installs the harmful code in the system.)
  - A wrapper (Comprises the tools that install Trojan in the system.)
- A user should take proactive measures to detect Trojans on his/her system.
- A user should beware of 'executable' files such as .exe, .bat, .jpeg and so on, as Trojans have similar types of extensions.

Summary 3-5

- A computer virus is a malware program or a piece of code that replicates while preparing copies of the data files in the other computer system or data storage device.
- Once a virus is detected in the system or driver and if it starts the replication process, the driver is 'infected'.
- The two common purposes of creating viruses are expecting financial benefits and damaging the system.

Summary 4-5

- If virus enters a system, it starts infecting the data files by replicating initially and later, it attacks files and damages them.
- Viruses work in following two phases, Infection phase and Attack phase.
- Computer worms are harmful programs that affect the system, delete the data, slow-down the processor of a computer and a network.
- A virus is a malicious code or a program that connects to the system application and runs with it, whereas a worm replicates itself and use existing resources in the system.

Summary 5-5

- Virus analysis tools are IDA Pro, VirusTotal, GFI sandbox and ThreatExpert.
- Scanning, Integrity checking and Interception based on a virus signature are Virus Detection Methods.
- Malware is malicious software to interrupt the computer system operations, information or data files. A hacker can also get an access using the malware program.
- Sunbelt CWSandbox or ThreatAnalyzer and VirusTotal are online malware resting tool.