WHAT IS MALWARE?

Malware — or "malicious software" — is any program designed to harm your device and data. Several types of malware — including trojans, viruses, ransomware, spyware and worms — can be installed on your company's computers.

What Can Malware Do?

- Steal Your Sensitive Information
- Slow Your Computer
- Restrict Access to Your Files
- Spread Throughout Your Network
- Disrupt Daily Operations

Symptoms of Malware

- Slow computer
- Lack of storage
- Crashing or freezing
- Pop-ups and unwanted programs
- Spam

How to Prevent Malware Infections

- Install anti-malware software
- Perform regular employee security training
- Avoid clicking unknown links and pop-ups
- Keep your system up to date
- Implement network security

Types of Malwares

1. Virus
2. Worms
3. Trojan
4. Adware
5. Spyware
6. Ransomware

VIRUS (VITALINFORMATION RESOURCE UNDER SEIZE)

- ✔ Founder- Fred Cohen
- ✔ First Virus-Creeper-1971_Bob Thomas
- ✔ First Boot Sector Virus-Brain-1986
- ✔ Viruses piece of software that infects programs
- modifies them to include a copy of the virus
- replicates and goes on to infect other content
- easily spread through network environments
- when attached to an executable program a virus can do anything that the program is permitted to do

- executes secretly when the host program is run
- specific to operating system and hardware
- takes advantage of their details and weaknesses

How does a computer get a virus?

- Sharing music, files, or photos with other users
- Visiting an infected website
- Opening spam email or an email attachment
- Downloading free games, toolbars, media players and other system utilities
- Installing mainstream software applications without thoroughly reading license agreements

How do computer viruses spread?

Viruses can be spread several ways, including via networks, discs, email attachments or external storage devices like USB sticks

How are computer viruses removed?

Antiviruses have made great

- Worms
- Trojan
- Ransomware

WORM (WRITE ONCE READ MANY)

- Founder-Robert Morris
- Write worm- Ray Tomlinson
- First Worm- Morris Worm
- Run -Independently

A computer worm is a type of malware that spreads copies of itself from computer to computer. A worm can replicate itself without any human interaction, and it does not need to attach itself to a software program in order to cause damage.

How do computer worms work?

Worms can be transmitted via software vulnerabilities. Or computer worms could arrive as attachments in spam emails or instant messages (IMs). Once opened, these files could provide a link to a malicious website or automatically download the computer worm. Once it's installed, the worm silently goes to work and infects the machine without the user's knowledge.

Worms can modify and delete files, and they can even inject additional malicious software onto a computer. worms can also steal data, install a backdoor, and allow a hacker to gain control over a computer and its system settings.

How to tell if your computer has a worm

- Keep an eye on your hard drive space
- Monitor speed and performance

- Be on the lookout for missing or new files

VIRUS VS WORMS

The primary difference between a virus and a worm is that viruses must be triggered by the activation of their host; whereas worms are stand-alone malicious programs that can self-replicate and propagate independently as soon as they have breached the system. Worms do not require activation—or any human intervention—to execute or spread their code.

TROJAN HORSE

A Trojan horse, or Trojan, is a type of malicious code or software that looks legitimate but can take control of your computer. A Trojan is designed to damage, disrupt, steal, or in general inflict some other harmful action on your data or network.

Action performed by trojan horse is given below: -

- Deleting data
- Blocking data
- Modifying data
- Copying data
- Disrupting the performance of computers or computer networks

TYPES OF TROJAN VIRUSES

Some of the most common types of Trojan virus include:

Backdoor Trojans - This type of Trojan allows hackers to remotely access and control a computer, often for the purpose of uploading, downloading, or executing files at will.

Exploit Trojans -These Trojans inject a machine with code deliberately designed to take advantage of a weakness inherent to a specific piece of software.

Rootkit Trojans -These Trojans are intended to prevent the discovery of malware already infecting a system so that it can affect maximum damage.

Banker Trojans -This type of Trojan specifically targets personal information used for banking and other online transactions.

Distributed Denial of Service (DDoS) Trojans - These are programmed to execute DDoS attacks, where a network or machine is disabled by a flood of requests originating from many different sources.

Downloader Trojans -These are files written to download additional malware, often including more Trojans, onto a device.

HOW TO INSTALL THEM ON VICTIM 'S COMPUTER?

For attacking on the victommachine:- Beast 2.06 (anti virus must be activated)

Build Server->Basic->->reverse connection->Notifications-> Get IP->exeicon->choose window file->take the server icon->save server

*Server file has been created-anyhow make victim execute this file in his pc.For this make it useful software and give it to victim for executing it.

Opening the Trojan Binder Yup

Yup+ browsing-CCsetup303-?Execution method

Attaching other file

Server.exe->creation attributes->Hidden+system

Target->Windows folder->Tools->(Choosing the icon for final product)->cc cleaner->saving

Server+CCsetup303=cc cleaner

VM ware->Windowsxp professional->copy cc cleaner and install it now you are eligible to access the system.

ADWARE

- Adware (or advertising software) displays pop-up advertisements when you are online.
- Adware has the potential to become malicious and harm your device by slowing it down, hijacking your browser and installing viruses and/or spyware.

How does adware work?

Adware creators and distributing vendors make money from third parties via either:

- Pay-per-click (PPC) — they get paid each time you open an ad.
- Pay-per-view (PPV) — they get paid each time an ad is shown to you.
- Pay-per-install (PPI) — they get paid each time bundled software is installed on a device.

How to tell if you have an adware infection

Signs that you may be infected with unwanted adware include:

Computer adware infection signs

- An unexpected change in your web browser home page
- Web pages that you visit not displaying correctly
- Being overwhelmed with pop-up ads — sometimes even if not browsing the internet
- Slow device performance
- Device crashing
- Reduced internet speeds
- Redirected internet searches
- Random appearance of a new toolbar or browser add-on

Mobile adware infection signs

- On your phone, signs are similar:
- Your phone is slow
- Apps take longer to load
- Your battery drains quickly
- Your phone has apps you don’t remember downloading
- There is unexplained data usage and higher than expected phone bills
- There are numerous ad pop-ups

SPYWARE

Spyware is a type of malicious software that is installed on your computer or mobile device without your consent. It can gain access to your sensitive personal information and then relay it to other parties, some malicious.

Types of spyware

- Adware
- Trojans
- **Inter tracking**is a common practice used to follow your web activities—like browsing history and downloads—mostly for marketing purposes

What does spyware do?

Infiltrates your device: This could happen when you visit a malicious website, unwittingly install a malicious app, or even open a file attachment.

Captures your data: Once the spyware is on your device, it begins to collect data, which could be anything from your web activity to screen captures or even your keystrokes.

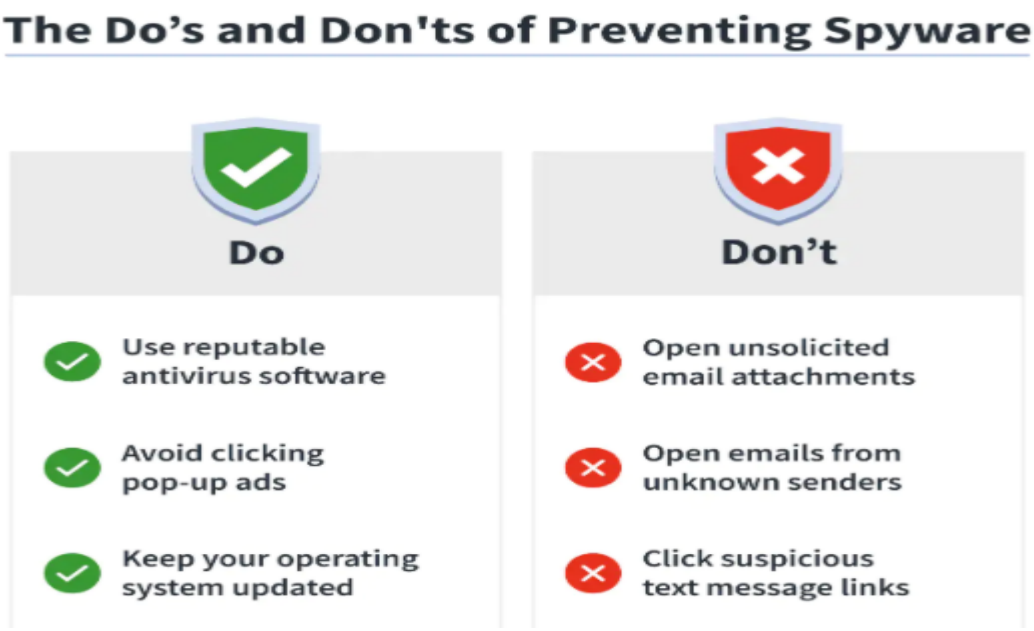
Provides data to a third party: The captured data is then supplied to the spyware creator, where it is either used directly or sold to third parties.

The data collected through spyware may include things like:

- Web browsing history
- Keyboard strokes
- Email address
- Login credentials (usernames and passwords)
- Credit card details and account PINs

Signs of a spyware infection

- Your device is slow, crashes unexpectedly, or starts displaying error messages.
- Your device is running out of hard drive space.
- You're annoyed by frequent and persistent pop-ups.
- Your browser redirects you to pages you haven't navigated to.
- Your browser no longer points to your usual homepage.
- You discover icons for programs you didn't download on your device. ·
- Your browser displays a new toolbar or plugin you didn't add.



Is spyware a virus?

Spyware and computer viruses are in the same family—they're both malicious types of software. But there are some differences. Spyware is a type of malware that collects your personal information and gathers data about you without your consent. Viruses are a type of malicious software designed to spread from your device to other devices.

RANSOMWARE

The idea behind ransomware, a form of malicious software, is simple: Lock and encrypt a victim's computer or device data, then demand a ransom to restore access.

In many cases, the victim must pay the cybercriminal within a set amount of time or risk losing access forever. And since malware attacks are often deployed by cyberthieves, paying the ransom doesn't ensure access will be restored.

Ransomware holds your personal files hostage, keeping you from your documents, photos, and financial information. Those files are still on your computer, but the malware has encrypted your device, making the data stored on your computer or mobile device inaccessible.

- First Ransomware-AIDS/PC Cyborg/example-Locky-2016
- Wannacry-2017 (50 countries)

How do ransomware attacks work?

Ransomware attacks work by gaining access to your computer or device, and then locking and encrypting the data stored on it.

How does this happen?

It often happens when victims mistakenly download malware through email attachments or links from unknown sources — which happen to be hackers.

While a ransom is demanded, there's no guarantee your data will be restored if you pay that ransom. Even if you pay, the attackers may never give you the decryption key. This makes ransomware tricky to navigate.

Computer Virus	**Worm**	**Trojan Horse**	**Adware**	**Spyware**
1. Non self-replicating.	1. Self-replicating.	1. Non self-replicating.	1. Non self-replicating.	1. Non self-replicating.
2. Produces copies of itself using host file as carrier.	2. Does not produce copies of itself using host file as carrier (independent program).	2. Does not produce copies of itself using host file as carrier (independent program).	2. Produces copies of itself using host file as carrier.	2. Does not produce copies of itself using host file as carrier (independent program).
3. Cannot control PC remotely.	3. Cannot control PC remotely.	3. Can control PC remotely.	3. Cannot control PC remotely.	3. Can control PC remotely.
4. Can be detected and deleted using anti-virus software.	4. Can be detected and deleted using anti-virus software.	4. Can be detected and deleted using anti-virus and anti-rootkit software.	4. Can be detected and deleted using anti-virus and anti-adware software.	4. Can be detected and deleted using anti-virus and anti-spyware software.