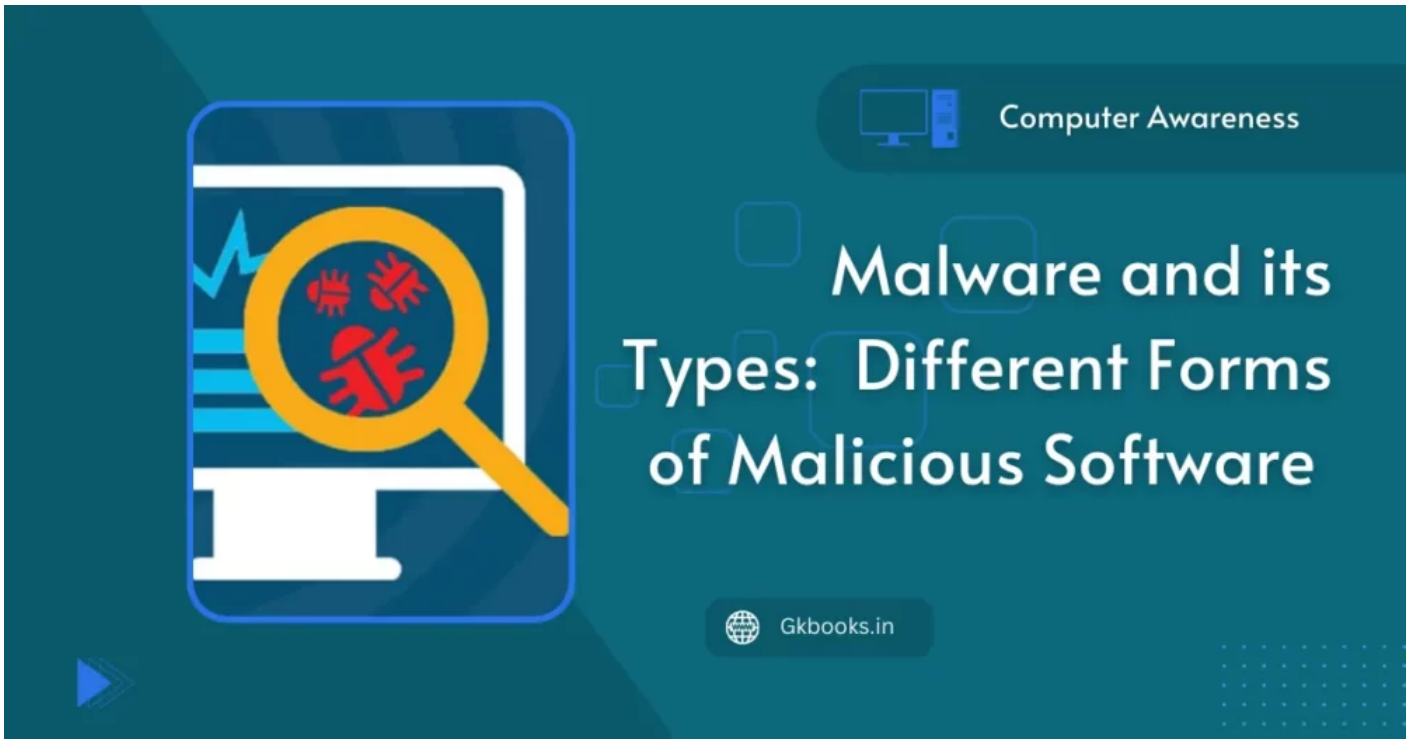
Malware and its Types: Understanding the Different Forms of Malicious Software – Complete Details



Malware, or malicious software, comes in many forms. Learn about the different types of malware, including viruses, worms, trojans, and ransomware, and how to protect your devices from these cyber threats.

Computer Security and Privacy Issues, including knowledge of malware and its types, is a crucial aspect of Computer Awareness. Understanding this information is vital for preparing for competitive exams that test general computer knowledge. Staying informed on these topics helps ensure the safe and secure use of technology in both personal and professional settings.

Malware

- Malware, short for malicious software, refers to any program created with the intent of gaining unauthorized access to a computer system for the benefit of a third party. This includes a wide range of harmful programs such as viruses, worms, Trojan horses, ransomware, spyware, and other malicious software that are designed to cause harm to a computer system. These malware programs can be spread through various means such as email attachments, malicious websites, or infected software downloads.

Types of Malware

- There are different types of malware, each with its own specific characteristics and attack methods.

- Among the different types of malware, viruses, worms, ransomware, spyware, and Trojan horses are the most well-known.

- Let’s briefly discuss all these types of malware and how they attack a computer.

Viruses

- Among the different types of malware, the most common type of malware is a computer virus.

Computer VIRUS full form

- The term **“Virus” stands for “Vital Information Resources under Siege”** and refers to malicious software that can harm your data, files, and programs by replicating itself.

What is Computer Virus?

- These are a type of malware that attach themselves to legitimate files and programs, spreading to other computers through shared network connections or removable storage devices.

How does a Computer Virus work?

- A computer virus is a form of malware that infects a legitimate file and spreads when that file is shared or executed by another user. The malicious code within the file can cause harm to the system and potentially spread to other systems through shared files or infected applications or software.

- The malicious code within the virus can range from harmless to harmful, potentially modifying or deleting data on a computer.

- Activation of a virus typically occurs when an infected file is opened, at which point the virus may infect other programs on the computer.

- It’s important to be aware of the potential risks and take precautions to protect your computer from becoming infected with a virus.

Worms

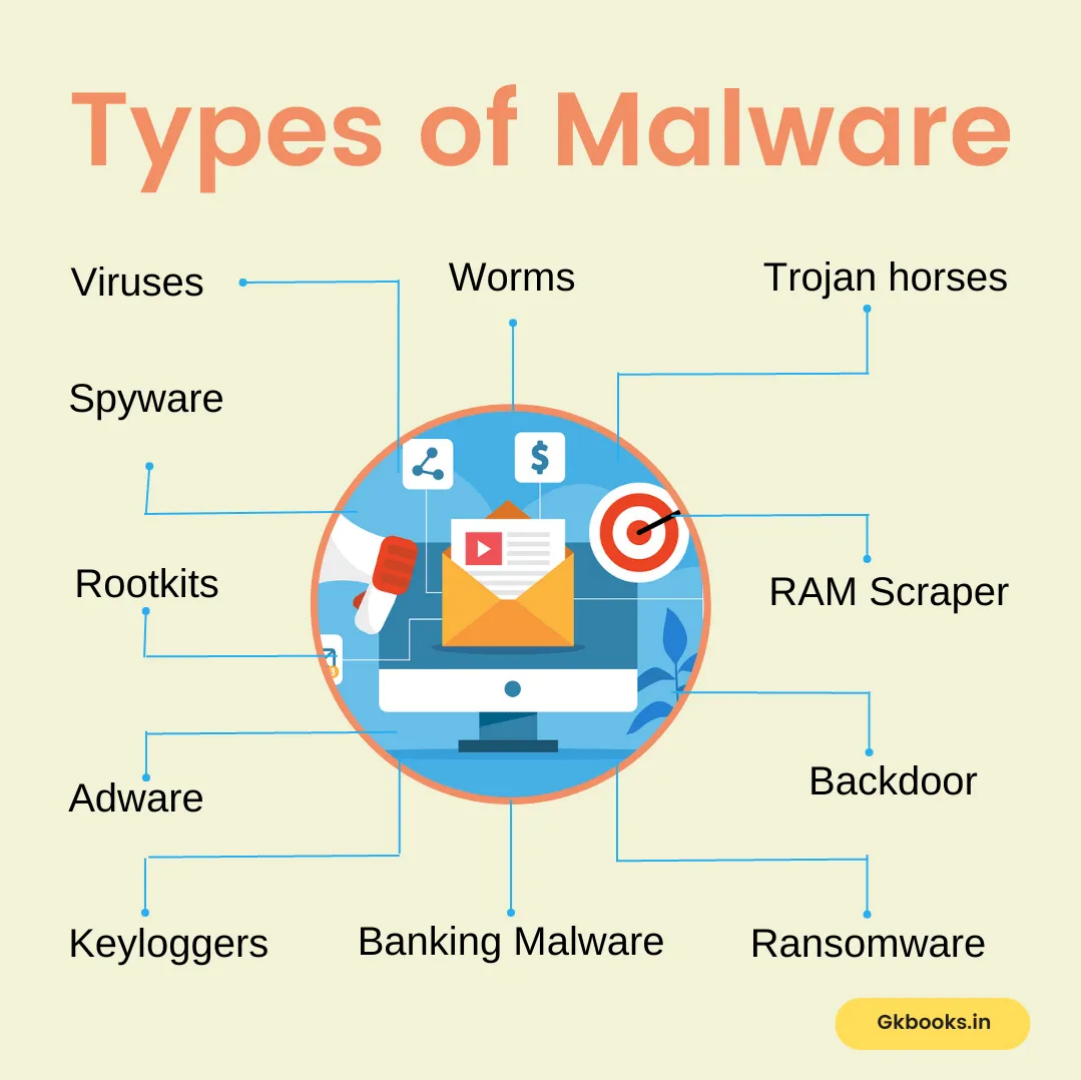
What is a Worm?

- These are self-replicating malware that attaches to different files and searches for ways to spread to other computers, such as through shared network storage.

How Worm infected systems?

- They are usually infected on a system via the Internet or shared network storage. Unlike viruses, worms do not require a host program to run and can propagate on their own.

- It often damages systems and reduces network performance, and can spread quickly once it infects a host.



Malware and its Types

Trojan horses

What are trojan horses?

- They are malware masquerading as legitimate programs, tricking users into installing and running them on their systems.

- It carries out malicious operations under the appearance of a desired operation such as playing an online game.

How do trojan horses affect the computer system/network?

- A Trojan enables attackers to gain unauthorized access to the device, perform keylogging, steal sensitive information, and even control the device remotely.

Example of trojan horses

- One example of a Trojan is the Emotet malware, which was first identified in 2014 and continues to target victims' financial information, even after a global effort to dismantle it in 2021.

Key Difference between Trojan Horses and VIRUS

- A Trojan horse differs from a virus in that it attaches itself to non-executable files, such as images and audio files, rather than executable files.

Difference between Trojan Horse and Virus

Feature	Trojan Horse	Virus
Definition	Malicious software that disguises itself as a legitimate program but performs harmful actions	Malicious software that infects a computer when an infected file is run or opened
Spreads through infected software, files, emails, and networks	Spreads through disguised attachments, links, and downloads	Method of Spread
Purpose	Can give unauthorized access to user data or control over the infected device	Can cause harm to files, steal information, or damage system
Detection	Can be difficult to detect as it often hides behind legitimate programs	Can be detected by antivirus software

Ransomware

- Ransomware, which was not commonly known in the past, is now frequently seen in news headlines. Ransom, as the name implies, means money or other payment demanded the release of a prisoner.

- Ransomware blocks access to files or entire systems to force the owner or user to perform a task according to the attacker.

- In a computer system this type of malware encrypts a user's files, making them inaccessible, and demands payment in exchange for the decryption key.

Ransomware Examples (Recently In news)

- A rapidly evolving **ransomware operation called Nevada** has caught the attention of security experts, who have noted its expanding capabilities. This locker, which targets both Windows and VMware ESXi systems, has shown marked improvement in its functionality.

Real-World Example of Ransomware Attack

WannaCry ransomware attack (2017)

- It affected hundreds of thousands of computers in more than 150 countries, causing widespread disruption and financial losses estimated at tens of millions of dollars.

NotPetya ransomware attack (2017)

- The attack was initially targeted at Ukraine but had far-reaching effects, causing significant disruption to business and critical infrastructure in several countries. The estimated financial loss in this attack is in billions of dollars.

Stuxnet worm (2010)

- This highly sophisticated attack targeted Iran's nuclear facilities and is considered the first known example of a state-sponsored cyber attack. It was able to cause significant physical damage to equipment and set back Iran's nuclear program by several years.

Spyware

What is a Spyware?

- Spyware is a type of malware that is intended to enter a computer device, collect information about the user, and transmit it to a third party without the user's consent.

- While some spyware may be legitimate software used for monitoring data for commercial purposes such as advertising, malicious spyware is often used to profit from stealing data.

How Spyware affects a system

- Both legitimate and fraudulent, spyware surveillance activities can lead to data breaches and misuse of personal information.

- Additionally, spyware can negatively impact network and device performance, slowing down daily activities.

What kind of data does spyware steal?

- Data compromised by spyware often includes collecting sensitive, confidential information from a victim's computer and transmitting it to the attacker such as:

  - Login credentials — passwords and usernames
  - Account PINs
  - Credit card numbers
  - Monitored keyboard strokes
  - Tracked browsing habits
  - Harvested email addresses

Adware

- This type of malware displays unwanted advertisements on a user's computer, often in the form of pop-ups or banners.

- It monitors a user's browsing and download history in order to display pop-up or banner advertisements that entice the user to make a purchase.

- For instance, an advertiser might use cookies to keep track of the web pages a user visits to more effectively target advertising.

Rootkits

- This type of malware is designed to hide the presence of other malware on a system, making it difficult to detect and remove. They are intended to give hackers access and control over a targeted device.

- While most rootkits target the software and operating system (OS), some can also infect the hardware and firmware of a computer.

- Rootkits are skilled in hiding their presence, but they remain active even while concealed. Most rootkits take advantage of software vulnerabilities to modify system files.

Banking Malware

- This type of malware is used to steal sensitive information such as credit card details and login credentials of online banking services.

Backdoor

- A backdoor is a secret way to bypass normal security measures, such as authentication or encryption, on a computer, device, or software.
- It is often used to remotely access a computer or access encrypted files.
- Backdoors can be used to access, damage, delete or steal sensitive information.
- They can be hidden within a program, as a separate program, or built into the firmware or operating system.
- Backdoors can be created by the manufacturer for legitimate purposes, such as resetting user passwords.

RAM Scraper

- A RAM scraper is a type of malware that extracts sensitive data that is temporarily stored in RAM. This malware typically targets point-of-sale (POS) systems, such as cash registers, as they may temporarily store unencrypted credit card numbers before they are encrypted and sent to the back end.

Keyloggers

- A keylogger is a **type of malware that records** and **tracks keystrokes** on a **device.**
- It can install or infect a system through hardware or software methods.
- Hardware keyloggers are physically inserted into keyboards, while software keyloggers are typically downloaded through malicious links or downloads.
- These keyloggers are used by cybercriminals to collect sensitive information, such as **login credentials, from victims.**
- One such example is the **Agent Tesla keylogger,** which first appeared in 2014 and continues to be a prevalent threat.
- Its latest versions can also capture screenshots of the infected device.
- To protect against keylogger attacks, it’s recommended to use a password manager, which eliminates the need to enter login information manually and thus prevents it from being recorded by the keylogger.

Malware and its Types: in a nutshell

Malware	Mode of Attack	Harmful Effects	Real-World Example
Viruses	Activation of a virus typically occurs when an infected file is	Computer virus can range from harmless to harmful,	Mydoom virus

	opened	potentially modifying or deleting data on a computer	
Worms	It infected on a system via the Internet or shared network storage	It often damages systems and reduces network performance, and can spread quickly once it infects a host.	Stuxnet
Trojan Horses	It acts as a legitimate program, tricking users into installing them and running them on their systems	Trojans give attackers backdoor access to a device, perform keylogging, install viruses or worms, and steal data	Emotet
Ransomware	Ransomware blocks access to files or entire systems to force the owner or user to perform a task according to the attacker.	Malware that encrypts data or locks computers until a ransom is paid	RYUK
Spyware	Downloads onto a device without the user's permission. I	It steals users' data to sell to advertisers and external users.	DarkHotel
Adware	Monitors a user's browsing and download history in order to display advertisements	Displays unwanted advertisements on a user's computer, often in the form of pop-ups or banners.	Fireball
Rootkits	It infected the software and operating systems (OS)	A rootkit is software used by cybercriminals to gain control over a target computer or network.	Zacinto
Banking Malware	Attacks online banking systems such as financial institution's login webpage	Used to steal sensitive information such as credit card details and login credentials of online banking services	Shylock
Backdoor	It bypasses common security measures to open a file or program, such as authentication or encryption on a computer, device or software.	Backdoors can be used to access remote fie, damage, delete or steal sensitive information.	PoisonTap
RAM Scraper	Attacks random access memory (RAM) to collect temporarily stored data	It can collect credit card numbers from a point-of-sale (POS) system	Rdasrv / Alina
Keyloggers	Records and tracks keystrokes on a device to obtain login credentials	Used by cybercriminals to collect sensitive information, such as login credentials, from victims.	Olympic Vision

Frequently Asked Questions (FAQs)

Q1. What malware is most difficult to remove?

Answer: Rootkits

Q2. What type of malware can propagate itself?

Answer: Computer worms

Q3. Is A Trojan malware?

Answer: A Trojan Horse is a type of malware that disguises itself as legitimate code or software.

Q4. Who is the father of malware?

Answer: Frederick B. Cohen.
• He is an American computer scientist and inventor of computer virus protection techniques.