Malware & types of malware

The word ‘malware’ is a contraction of ‘malicious software’. Malware is intrusive software that is intentionally designed to cause damage to computers and computer systems. By contrast, software that causes unintentional damage is usually referred to as a software bug.

Malware may be introduced to a network through phishing, malicious attachments, malicious downloads, social engineering, or flash drives. In this overview, we look at common malware types.

Adware

Adware, a contraction of ‘advertising-supported software’, displays unwanted and sometimes malicious advertising on a computer screen or mobile device, redirects search results to advertising websites, and captures user data that can be sold to advertisers without the user's consent. Not all adware is malware, some is legitimate and safe to use.

Users can often affect the frequency of adware or what kinds of downloads they allow by managing the pop-up controls and preferences within their internet browsers or using an ad blocker.

Spyware

Spyware is a form of malware that hides on your device, monitors activity, and steals sensitive information like financial data, account information, logins, and more. Spyware can spread by exploiting software vulnerabilities or else be bundled with legitimate software or in Trojans.

Ransomware and crypto-malware

Ransomware is malware designed to lock users out of their system or deny access to data until a ransom is paid. Crypto-malware is a type of ransomware that encrypts user files and requires payment by a specific deadline and often through a digital currency such as Bitcoin. Ransomware has been a persistent threat for organizations across industries for many years now. As more businesses embrace digital transformation, the likelihood of being targeted in a ransomware attack has grown considerably.

Trojans

A Trojan (or Trojan Horse) disguises itself as legitimate software to trick you into executing malicious software on your computer. Because it looks trustworthy, users download it, inadvertently allowing malware onto their device. Trojans themselves are a doorway. Unlike a worm, they need a host to work. Once a Trojan is installed on a device, hackers can use it to delete, modify or capture data, harvest your device as part of a botnet, spy on your device, or gain access to your network.

Viruses

A virus is a piece of code that inserts itself into an application and executes when the app is run. Once inside a network, a virus may be used to steal sensitive data, launch DDoS attacks, or conduct ransomware attacks. Usually spread via infected websites, file sharing, or email attachment downloads, a virus will lie dormant until the infected host file or program is activated. Once that happens, the virus can replicate itself and spread through your systems.

Worms

One of the most common types of malware, worms, spread over computer networks by exploiting operating system vulnerabilities. A worm is a standalone program that replicates itself to infect other computers without requiring action from anyone. Since they can spread fast, worms are often used to execute a payload—a piece of code created to damage a system. Payloads can delete files on a host system, encrypt data for a ransomware attack, steal information, delete files, and create botnets.

Keyloggers

A keylogger is a type of spyware that monitors user activity. Keyloggers can be used for legitimate purposes – for example, families who use them to keep track of their children's online activity or organizations which use them to monitor employee activity. However, when installed for malicious purposes, keyloggers can be used to steal password data, banking information, and other sensitive information. Keyloggers can be inserted into a system through phishing, social engineering, or malicious downloads.

Bots and botnets

A bot is a computer that has been infected with malware so it can be controlled remotely by a hacker. The bot – sometimes called a zombie computer – can then be used to launch more attacks or become part of a collection of bots called a botnet. Botnets can include millions of devices as they spread undetected. Botnets help hackers with numerous malicious activities, including DDoS attacks, sending spam and phishing messages, and spreading other types of malware.

How Computer infected by virus

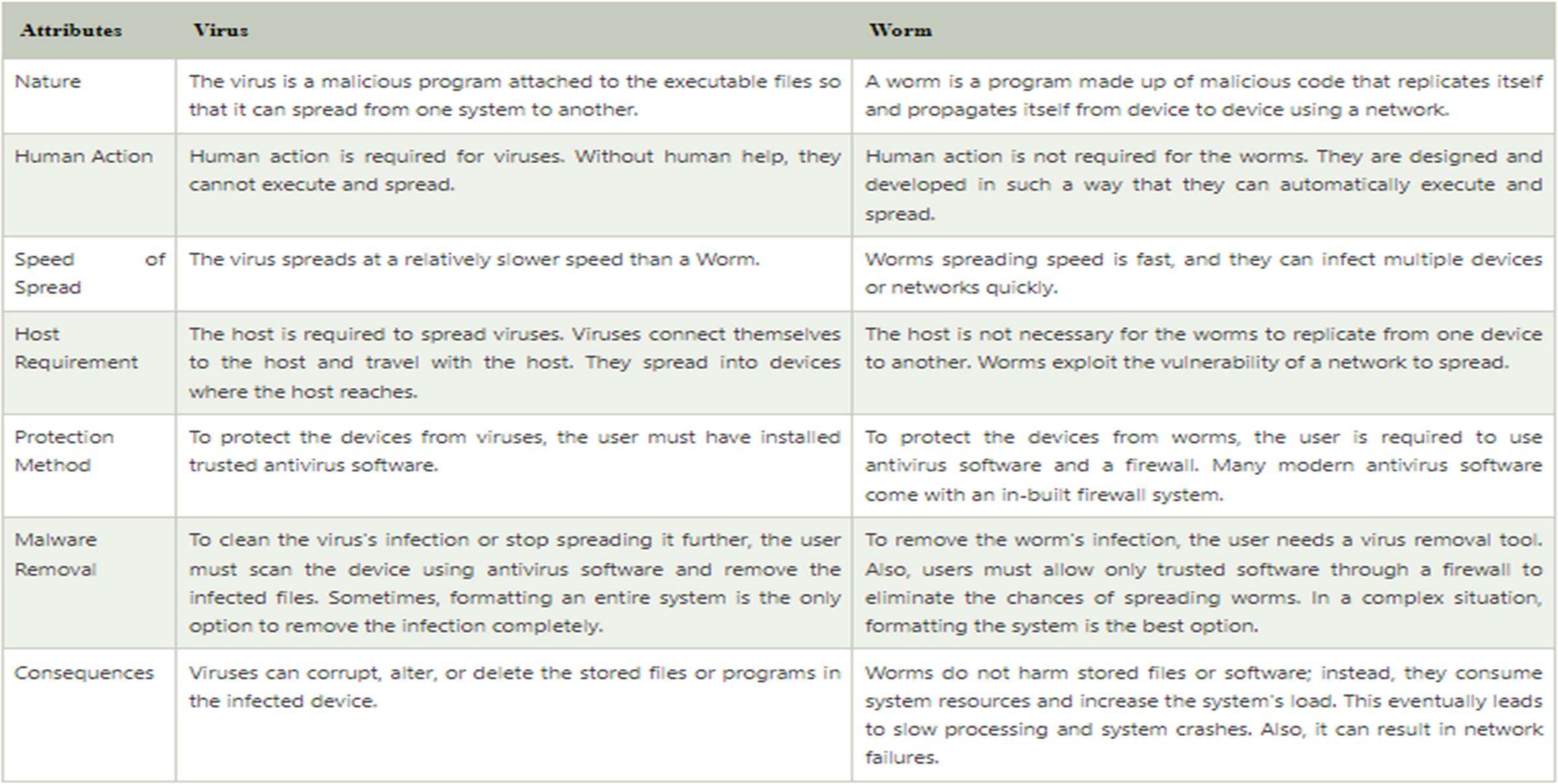
Typically, computer viruses spread through malicious online downloads, infected email attachments, or by plugging in infected hardware like an external flash drive (USB stick). Computer viruses can spread through almost any method of file sharing, as long as the virus can avoid detection by antivirus programs.

- ❑ **Accepting without reading**
- ❑ **Downloading any infected software**
- ❑ **Opening e-mail attachments**
- ❑ **Inserting or connecting an infected disk, disc, or drive**
- ❑ **Visiting unknown links**
- ❑ **Not running the latest updates**
- ❑ **Pirating software, music, or movies**
- ❑ **No antivirus spyware scanner**

Defend against virus attack worm and worm program

- **Get a good anti-virus**
- **Know what malicious programs look like**
- **Be wary of e-mail attachment**
- **Avoid the Third Party Downloads**
- **Have a Hardware-based firewall and deploy DNS**
- **Don’t Forget to Avoid Autorun**
- **Check SSL before dealing with E-commerce:**
- **Regular Backup Your Data:**

Worms different from virus



Attributes	Virus	Worm
Nature	The virus is a malicious program attached to the executable files so that it can spread from one system to another.	A worm is a program made up of malicious code that replicates itself and propagates itself from device to device using a network.
Human Action	Human action is required for viruses. Without human help, they cannot execute and spread.	Human action is not required for the worms. They are designed and developed in such a way that they can automatically execute and spread.
Speed of Spread	The virus spreads at a relatively slower speed than a Worm.	Worms spreading speed is fast, and they can infect multiple devices or networks quickly.
Host Requirement	The host is required to spread viruses. Viruses connect themselves to the host and travel with the host. They spread into devices where the host reaches.	The host is not necessary for the worms to replicate from one device to another. Worms exploit the vulnerability of a network to spread.
Protection Method	To protect the devices from viruses, the user must have installed trusted antivirus software.	To protect the devices from worms, the user is required to use antivirus software and a firewall. Many modern antivirus software come with an in-built firewall system.
Malware Removal	To clean the virus's infection or stop spreading it further, the user must scan the device using antivirus software and remove the infected files. Sometimes, formatting an entire system is the only option to remove the infection completely.	To remove the worm's infection, the user needs a virus removal tool. Also, users must allow only trusted software through a firewall to eliminate the chances of spreading worms. In a complex situation, formatting the system is the best option.
Consequences	Viruses can corrupt, alter, or delete the stored files or programs in the infected device.	Worms do not harm stored files or software; instead, they consume system resources and increase the system's load. This eventually leads to slow processing and system crashes. Also, it can result in network failures.