TASK 5

22/1/2026

Malware - short for Malicious software is the umbrella term for any code designed to harm, exploit, or access a device without permission. Just like any real sickness, these malware also have their own different symptoms and transmission methods; different malware types behave in unique ways to infect a computer.

Different types of Malware are:

1. Virus
   A virus needs a host file to spread across the network. It attaches to a legitimate program (like a Word document or a game installer). Crucially, we must launch the file so that it can activate and spread.
   Indication - Since viruses attach to legitimate files, their behaviour is often tied to app performance.
2. Worm
   A worm, which lives in its own computer memory, unlike a virus, can spread on its own using the network connections to copy itself to other computers automatically. A worm is like a standalone creature. It doesn't attach to another or any file.
   Indication - Worms live to spread, so their behaviour is almost entirely network-focused. High network traffic, Resource Drain, and email storms.
3. Trojans
   The name comes from Greek mythology, where the soldiers hid inside the giant wooden horse to sneak into the city of Troy. Here,e the concept is the same: a malware that disguises itself as useful/legitimate software that tricks you into installing it. Unlike viruses and worms, trojans aren't trying to replicate themselves on their own; they use social engineering, effectively manipulating us into opening the backdoor. This is like unlocking a window in your house so a thief can climb in whenever they want. A common specific type is a **RAT (Remote Access Trojan)**, which gives a hacker full control over your machine—allowing them to see your screen, log your keystrokes, or turn on your webcam without you knowing.
   Indication - Trojans hide, so their indicators are subtle and often relate to "phoning home." Look out for Unusual Outbound Connections, New Admin Accounts, etc.
4. Ransomware
   Ransomware is a malware that locks one out of their system or encrypts their files, then demands ransom to regain access. It enters via a Trojan, an email link, or a network vulnerability. Then encrypts the user data, this key step. Then a pop shows either pay or lose your data, and we publish your private data online.
   Indication - Ransomware is loud and destructive, so its behaviours are high-speed and high-impact. Eg: Mass File Renaming ,Shadow Copy Deletion, Decoy Documents.

Feature	**Virus**	**Worm**	**Trojan**	**Ransomware**
What is it?	Infected file attachment	Self-copying program	Fake software	Digital extortion
Replication	Yes	Yes	No	No
Needs Host?	Yes	No	No	No
Trigger	Human runs file	Automatic	Human installs	Automatic / Dropped
Method	Corrupts files	Clogs networks	Deceives user	Encrypts data
Goal	Spread / Damage	Spread fast	Steal access	Money

To prevent malware attack i’d recommend these tips

1. **Zero Trust Mindset:** Treat every email attachment and link with suspicion, especially if it creates urgency
2. **least Privilege:** Never use your computer as the "Root" or "Administrator" user for daily tasks. Use a standard account and only use ‘sudo’ when necessary. If malware strikes a standard user, it can't easily destroy the whole system.
3. **Disable Unused Services:** If you don't need Bluetooth or SSH running, turn them off. Less running code means fewer doors for hackers to try.
4. **Extension Hygiene:** Use an ad-blocker (like **uBlock Origin**) in your browser. It blocks the "Malvertising" scripts that try to infect you via ads.

Tools used

Gemini - Guided learning for Deep understanding of the concepts using real-world examples.
Google Docs - For creating the document
IBM Cloud - To find a Malware hash
VirusToTAL - For finding the hash details.
Grammarly - For grammar correction