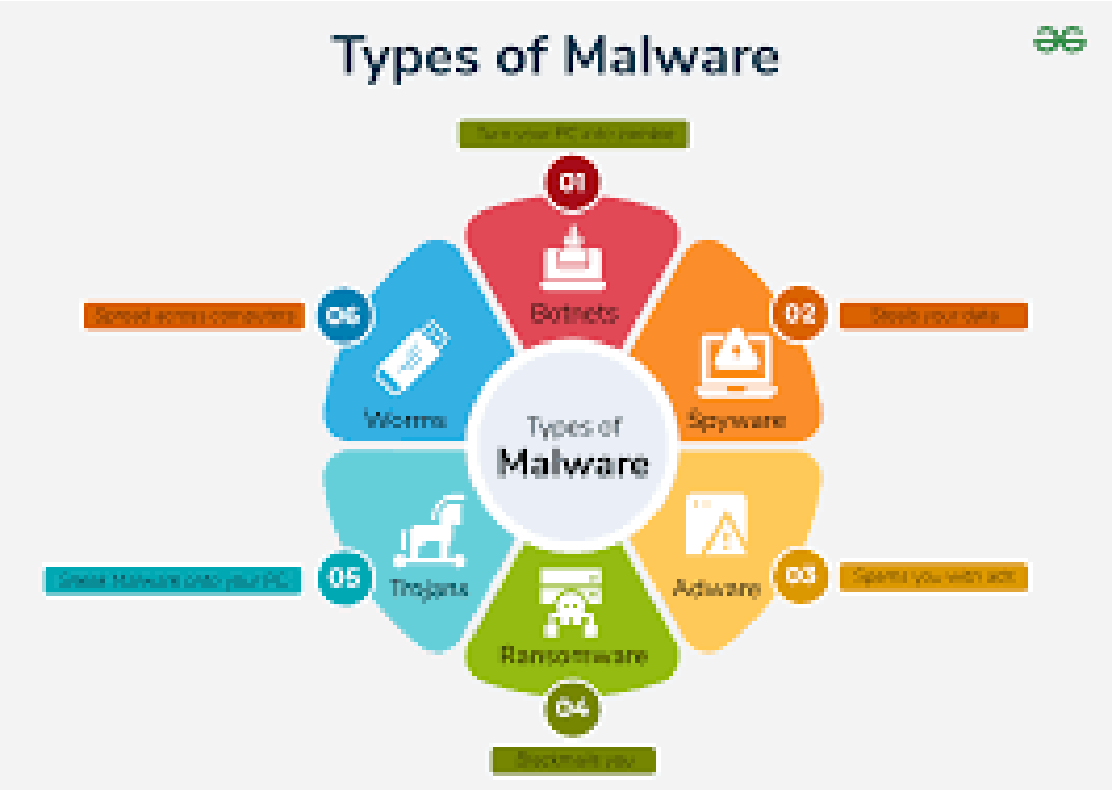
Week 3, Day 1 – Malware Research & Report

Understanding Malware and Its Impact

Malware, or **malicious software**, is any program created with the intent to harm or exploit systems. It's like a **digital disease**—some types spread fast like a virus, while others secretly spy on you. The impact of malware can range from slowing down a personal laptop to shutting down entire government organizations.



Here's a breakdown of **six common types of malware** and how they cause damage:

1.Virus – The Infectious Attacker

What it does: Attaches itself to files and spreads when the file is opened.
Impact: Slows down computers, corrupts data, and spreads through emails or USB drives.

Example: Imagine you download a free eBook, but when you open it, a hidden virus starts corrupting your important work files.

2.Worm – The Silent Spreader

What it does: Unlike a virus, worms don't need human interaction; they **self-replicate** and spread through networks.
Impact: Overloads networks, crashes systems, and disrupts businesses.

Example: The **Morris Worm (1988)** slowed down 10% of the internet, causing major panic.

3.Ransomware – The Digital Kidnapper

What it does: Locks your files and demands a ransom to unlock them.

Impact: Businesses and hospitals have lost **millions of dollars** to ransomware attacks.

Example: You open an invoice email, but instead of a bill, all your files suddenly get locked with a ransom note demanding **Bitcoin payment** to get them back.

4. Trojan Horse – The Fake Friend

What it does: Disguises itself as a useful program but carries hidden malware inside.

Impact: Steals passwords, installs spyware, or

creates system backdoors for hackers.

Example: You download a **“free photo editor”**, but behind the scenes, it’s **stealing your banking details**.

5. Spyware – The Invisible Stalker

What it does: Secretly records everything you do, including keystrokes, passwords, and browsing habits.

Impact: Used for identity theft, online banking fraud, and corporate spying.

Example: Some spyware logs everything you type, so if you enter your **email and password**, a hacker gets a copy instantly.

6. Adware – The Pop-up Bombardment

What it does: Shows excessive advertisements, some of which lead to **more malware**

infections.

Impact: Slows down systems and can redirect you to fake login pages.

Example: Have you ever tried watching a movie on a shady website, only to get **bombarded with pop-ups**? That's likely **adware at work**.

Famous Malware Attacks and How They Worked

Now that we understand the types of malware, let's look at **two real-life attacks** that caused chaos worldwide.

1. WannaCry Ransomware (2017) – The Global Blackout

🛠️ **How it worked:**

- WannaCry spread using a **Windows vulnerability** called **EternalBlue**, which was leaked from the NSA (National Security Agency).
- It was **a self-replicating worm**, meaning **once one computer was infected, it spread to others automatically**.
- When infected, users saw a **ransom note** demanding **$300–$600 in Bitcoin** to unlock their files.

⚠️ **Impact:**

- **Hospitals in the UK (NHS)** were hit hard, forcing surgeries to be canceled.
- Over **200,000 computers in 150+ countries** were affected.
- Estimated **$4 billion in losses**.

🛡️ **How was it stopped?**

- A security researcher found a **“kill switch”**—a domain name hardcoded into the malware. By registering the domain, they **accidentally stopped WannaCry from spreading further**.

📌 **Lesson Learned:** Keeping **software updated** is crucial. Microsoft had **already released a patch**, but many organizations didn’t install it in time.

2. Stuxnet (2010) – The First Cyber Weapon

💣 **What made it special?**

Unlike normal malware that steals passwords or money, **Stuxnet was designed to destroy physical machines**—specifically **Iran’s nuclear program**.

🛠️ **How it worked:**

- Stuxnet was **a highly sophisticated worm** that targeted **industrial control systems (ICS)**.
- It specifically attacked **Siemens PLCs (Programmable Logic Controllers)**—the brains behind nuclear centrifuges.
- Once inside, it **silently made the centrifuges spin out of control**, **damaging Iran's nuclear facilities without them knowing**.

⚠️ **Impact:**

- Destroyed **1,000+ nuclear centrifuges** in Iran, **delaying their nuclear program** by years.
- Considered the **world's first cyber weapon**—believed to be created by the **U.S. and Israel**.

📌 **Lesson Learned: Cyberwarfare is real**—governments are now investing billions in offensive hacking.

Recent Cyber Attacks in India

1.AIIMS Ransomware Attack (2023):

In 2023, the All India Institute of Medical Sciences (AIIMS) in Delhi suffered a ransomware attack that led to server shutdowns and disrupted healthcare services. Patient data was potentially compromised, underscoring the vulnerabilities in critical infrastructure and the dire need for robust cybersecurity measures in the healthcare sector.

2.**Cyber Attacks Amid India-Canada Diplomatic Row (2023):**

Following diplomatic tensions between India and Canada in 2023, the Indian Cyber Force (ICF) launched cyber attacks against Canadian entities. Notably, the ICF took down the Canadian military's website using Distributed Denial of Service (DDoS) attacks, rendering it unavailable for two hours. Other targets included the House of Commons and Elections Canada websites, as well as defacements of various Canadian business websites. These attacks highlighted the role of hacktivist groups in geopolitical conflicts.

📌 Conclusion – My Key Takeaways

As I researched malware, I realized it’s not just about viruses and slow computers. The **biggest threats today** involve **ransomware, cyber-espionage, and attacks on critical infrastructure**. The fact that **a piece of code can**

shut down hospitals or even nuclear facilities is both **terrifying and fascinating**.

If I had to summarize my biggest takeaways, they would be:

~~ Regular software updates could have prevented attacks like WannaCry.

~~ Human error (clicking malicious links) is still the biggest security risk.

~~ Governments and hackers are now using malware as weapons—it's not just criminals anymore.

This research made me realize how **important cybersecurity really is**. Protecting systems is no longer an option—it's a necessity.