DAY 5 - DARK WEB, AND REAL CYBERATTACKS

Dark Web

- **Definition:** hidden part of the internet not indexed by search engines and accessible only through special browsers like Tor
- **used for:** Privacy-focused communication, whistleblowing, anonymous journalism.
- **Illicit Use:** Illegal marketplaces, data trading, malware sales, hacking forums.

Terms to know:

- **Tor Browser:** Allows anonymous browsing by routing traffic through multiple encrypted layers.
- **Deep Web ≠ Dark Web:** Deep web includes content behind logins (e.g., your email inbox), while the dark web is deliberately hidden.

3 Major Real-world Cyberattacks

1. WannaCry Ransomware Attack (2017)

- **Type:** Ransomware
- **What happened:** Exploited a Windows vulnerability (EternalBlue).
- **Impact:** Affected over 200,000 computers in 150+ countries, with total damages ranging from hundreds of millions to billions of dollars.
- **Victims:** NHS (UK hospitals), FedEx, Nissan.
- While Microsoft had released patches previously to close the exploit, much of WannaCry's spread was from organizations that had not applied these or were using older Windows systems that were past their end of life. These patches were imperative to cyber security, but many organizations did not apply them, citing a need for 24/7 operation, the risk of formerly working applications breaking because of the changes, lack of personnel or time to install them, or other reasons.

- **Key takeaway:** Importance of software patching and updates.

2. Equifax Data Breach (2017)

- **Type:** Data breach
- **What happened:** Hackers exploited a vulnerability in Apache Struts.
- **Impact:** Personal data (SSNs, birth dates) of 147 million people exposed, making it one of the largest cybercrimes related to **identity theft**.
- The Equifax data breach began on May 12, 2017, when Equifax had not yet updated its credit dispute website with the latest version of Apache Struts. Exploiting this vulnerability, hackers gained access to internal servers within Equifax's corporate network.
- **Key takeaway:** Critical need for patch management and secure systems.

3. SolarWinds Supply Chain Attack (2020)

- **Type:** Nation-state, supply chain
- **What happened:** Hackers inserted malware into SolarWinds' Orion software updates.
- **Impact:** U.S. government agencies and major corporations were compromised.
- **Key takeaway:** Supply chain security is vital.