APT

1. Advanced persistent threat (APT) attacks: APT attacks are sophisticated, long-term attacks on a specific target by a skilled attacker. They often involve multiple stages, including reconnaissance, infiltration, and exfiltration of data.
   1. Password Attacks: Password attacks involve the use of brute-force techniques to crack passwords or trick users into revealing their passwords. Once the attacker gains access to a user's account, they can use it to access the organization's network.
   2. Watering Hole Attacks: In this type of attack, the attacker infects a website that the targeted organization's employees frequently visit with malware. When an employee visits the site, the malware infects their computer and gives the attacker access to the organization's network.
   3. Malware Attacks: This involves the use of malware to infiltrate an organization's network. The attacker sends an email with a malicious attachment or a link to a website that installs the malware onto the victim's computer.
   4. Supply Chain Attacks: In this type of attack, the attacker infiltrates a supplier or partner of the targeted organization and then uses their access to gain entry to the targeted organization's network.
   5. Zero-Day Exploits: These are attacks that take advantage of previously unknown vulnerabilities in software or systems. The attacker exploits the vulnerability before the developer has had a chance to patch it, giving them access to the organization's network.
2. APT attacks affecting casual internet user:
   1. Password Attacks: Most common way of hacking different types of accounts. Most users use passwords with their name or birthday contained in it, which makes it a lot easier to guess. A common practice is also to use the same password for every website, which makes it even more dangerous.