Few Known Cyberthreats

Denial of service attack: A denial-of-service attack (DoS attack) generally consists of the concerted efforts of a person/persons to prevent an internet site or service from functioning efficiently. A DoS attack is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have.

Distributed denial of service: In a distributed denial-of-service (DDoS) attack, large numbers of compromised systems (sometimes called a Bot net) attack a single target, thereby causing a denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby, denying the service of the system to legitimate users.

Ransom ware: Ransomware is a type of malicious software from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.

Malware: Malware is the term for maliciously crafted software code. Special computer programmes now exist that enable intruders to fool an individual into believing that traditional security is protecting him during online banking transactions. Attacks involving malware are a factor in online financial crime.

Phishing: Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details, often for malicious reasons, by disguising as a trustworthy entity in an electronic communication. Spear phishing and whaling are types of phishing attempts directed to specific individuals or companies and senior executives or high profile targets respectively.

Vishing: Vishing is the illegal access of data via voice over Internet Protocol (VoIP). Vishing is IP telephony's version of phishing and uses voice messages to steal identities and financial resources. The term is a combination of 'voice' and 'phishing'.

Drive-by downloads: Drive-by download means two things, each concerning the unintended download of computer software from the Internet:

a. Downloads which a person has authorized but without understanding the consequences (e.g. downloads which install an unknown or counterfeit executable program, ActiveX component, or Java applet) automatically

b. Any download that happens without a person's knowledge, often a computer virus, spyware, malware, or crimeware.

Advanced persistent threats (APTs): In an APT, an intruder or group of intruders infiltrate a system and remain undetected for an extended period. The intruder leaves networks and systems intact so that the intruder can spy on business activity and steal sensitive data while avoiding the activation of defensive countermeasures. The recent Solar Winds breach of United States government systems is an example of an APT.

Man-in-the-middle attacks: Man-in-the-middle is an eavesdropping attack, where a cybercriminal intercepts and relays messages between two parties in order to steal data. For example, on an unsecured Wi-Fi network, an attacker can intercept data being passed between a guest's device and the network.

Browser Gateway frauds: The information sent and received from a PC/device is routed through an undesired path on the network thereby exposing it to unauthorised entity. The only gateway to the outside world for the PC/device is the browser that has been compromised.

Ghost administrator exploits: A ghost administrator exploit is a code that takes advantage of a software vulnerability or security flaw to gain the Administrator's rights/privileges in the system. This exploit allows the attacker to mask his identity in order to remotely access a network and gain Administrator rights/privileges, or move deeper into the network. In some cases, an exploit can be used as part of a multi-component attack. Instead of using a malicious file, the exploit may instead drop another malware, which can include backdoor viruses and/or spyware to steal user information from the infected systems.