Đặng Hoàng Nguyên – SE171946

**RANSOMWARE**

* Ransomware is a category of malware used by hackers to encrypt data and hold it captive until the ransom is paid. Ransomware attacks can devastate businesses by stealing data to sell on the Dark Web, exposing private information, or erasing it completely if they are not stopped or discovered quickly after infection.
* Ransomware prevents access to the files of a victim. The next step is for targets to get a notice requesting payment in order to regain access to their information. Ransomware comes in two different flavors. Files that have been encrypted by ransomware (crypto ransomware) are changed into ciphertext and become illegible. Lock screens that fill the entire screen with a ransom note are used by non-encrypting ransomware.
* Ransomware spreads via email attachments, malicious URLs, Malvertising, pirated software
* Impact of ransomware:
* Loss of proprietary or sensitive information, whether temporary or permanent.
* Interruption of routine operations.
* Losses in money incurred while restoring systems and files.
* Potential reputational damage to a company.

**ADWARE**

* Adware is unwelcome software that displays advertising on your screen, usually while you're using a web browser. Some security experts consider it to be the precursor to the contemporary PUP (potentially unwanted program)
* There are two basic methods for adware to infiltrate your system. In the first, after downloading a program—typically shareware or freeware—adware is silently installed without your awareness or consent. That's because the creator of the application joined the adware distributor.
* As contrast to businesses, individuals are the primary targets of adware. It also follows the particular user across all possible platforms, including Windows PCs and Macs, smartphones, and almost all browsers. It uses the "too good to be true" marketing strategy to lure in potential victims by promising freebies or discounts on new software, movies, or other items.

**TROJAN**

-Trojan: A Trojan, often known as a Trojan horse, is a type of malware that masks its real contents in order to trick a user into believing it to be a safe file. The "payload" carried by a Trojan, like the wooden horse used to capture Troy, is unknown to the user, but it can serve as a delivery system for a number of threats.

- A backdoor or ransomware could be part of the harmful payload carried by a Trojan horse. The backdoor would provide the malware's creator unauthorized access to the computer's data and system resources. More malware could be downloaded through the backdoor as a result. Trojans assist the controller in stealing user data (including IP addresses and passwords). Trojans are used by online criminals to launch ransomware attacks, and they give the controller the ability to spy on the victim. Trojans can change, block, copy, erase, and slow down computers and/or devices.

- The Trojan Spread: To propagate Trojans, cybercriminals use social engineering. Malicious email attachments with innocent-looking subject lines are deceived victims into clicking on them. The Trojan executes itself when it is run. Another common method of propagating Trojans is drive-by downloads. Without the victim's consent, the Trojan program is automatically downloaded onto the device or computer via the drive-by download method.

- Impact via Keylogging, data corruption, and remote access are effects (Backdoor)