Introduction to Ransomware:

Ransomware is a type of Malware which encrypts the files and in return demands the Ransome payment to restore the access.Ransomeware attacks are one of the dangerous cyber threats increasing day by day and harder to detect.These attacks primarily targets the Individuals,Government Institutions,Bussinesses.

How Ransomware Works:

Infection: The attackers deliver the malware through the Phishing emails, malicious downloads or exploited software's.

Execution: Once the attackers gain the access to the system, they can execute the malicious scripts.

Encryption: Attackers Encrypt the system files with their own keys using the cryptographic libraries

Ransom:Attackers demand the ransomware(money) to decrypt the system files in some times thay demand twice or thrice based upon the data.

Persistence & Spread:The attackers maintain the persistence once they established the connection and slowly spreading the malware into the network to afftect the multiple devices.

Types of Ransomware:

Locker Ransomware – Locks the user out of their system but does not encrypt files (e.g., WinLocker).

Crypto Ransomware – Encrypts files and demands ransom payment for decryption (e.g., WannaCry, Ryuk, REvil).

RaaS (Ransomware-as-a-Service) – Cybercriminals sell the ransomware kits for others to use in attacks (e.g., LockBit)(malwares)

Encryption Algorithms:

AES(Advanced encryption standard):It is a symmetric algorithm widely used in many ransomeware attacks due to its speed and security based on the key sizes were AES-256 is one of the strongest.

RSA(Rivest-Shamir-Adleman):This is an asymmetric algorithm which uses the public key and private key .It is used in the ransomeware to encrypt the AES encryption key since rsa is slower AES is used to encrypt the files and RSA to lock the AES key.

Fernet:

Fernet is one of the highest security encryption method which uses the AES-128 in CBC mode with HMAC-SHA256 for the authentication and it has a feature were ensures the data integrity for the encrypted files don't be altered.This makes the fernet strong candidate for the ransomeware and it prevents the unauthorized decryption without having the original key.

Ransomeware attacks:
Ryuk (2018-2021):

> This is one of the highly targeted ransmware used in sophisticated cyberattacks against businesses, hospitals, and government agencies. Used a **double-extortion** method making victims had to pay to unlock files and prevent their stolen data from being leaked. The ransom demands were often in the hundreds of thousands to millions of dollars.

NOTPETYA:

This attack is Originally believed to be ransomware, but it was actually a wiper attack (designed to destroy data rather than restore it).It spread through a trojanized software update of accounting software used in Ukraine.Unlike normal ransomware, even if victims paid the ransom, data recovery was impossible.

Defense Mechanisms Against Ransomware

Regular Backups:

- Make sure to keep the data updated regularly and storing it offline, cloud-based backups to prevent the data loss in case of attack
- Backups should follow this which is **3-2-1 rule**:
  - 3 copies of data
  - 2 stored on different media
  - 1 kept offline to keep the data secure

Endpoint Security:

Detecting and stopping ransomware is made easier by safeguarding the systems with firewalls, antivirus software, and Endpoint Detection & Response (EDR) solutions. EDR programs track the behaviour of files and can spot odd encryption activities before files are erased. The awareness of users is crucial to teach people to spot harmful attachments, phony links, and social engineering techniques because phishing emails are often the first step in ransomware investigations. Companies should regularly teach their staff in cybersecurity awareness to lower the likelihood that they may fall for frauds.