1. Introduction:

Ransomware is a type of malware used by attackers to attack or locks user’s system or data and ask the user to pay ransom to gain access to data or system. Ransomware is a real threat to systems that attackers can inject to user’s system and encrypt the user data or system using encryption algorithms like AES, RSA or some modern-day ransomware also uses a combination of symmetric and asymmetric algorithms for encryption of user data or system and then ask the user to pay ransom for accessing system or data by displaying the message about how the user can get back their data, files, or system.

1.1 Types of Ransomware attack:

There are two types of Ransomware attack, one is Locky Ransomware, and another is Crypto Ransomware. These two classes of Ransomware define the way of attack, one is Lock Screen Ransomware that simply locks or encrypts the user system or desktop or input system and keeps the user inaccessible by simply showing extortion message, also known as Locker Ransomware. And another is Crypto or Encryption Ransomware that encrypts the user data or files and asks to pay ransom is also known as cryptographic ransomware.

Ransomware attackers change their targets from individuals to organizations such as banking, government offices, hospitals, and more. The attacker uses different ways to penetrate the user system with ransomware attack that is known as deployment location of attack like spam mails, compromised websites, downloading/opening any malicious file, logging into any already infected PC, installing pirated software, and more.

1.2 Phases of Attack:

The working of Ransomware attack can be described by using different phases. These phases are Distribution Phase, Reconnaissance Phase, Preparation Phase, Hijacking phase, Extortion phase. In the Distribution phase, the attacker tries to find system vulnerability and sends ransomware
malware to victim’s system. In Reconnaissance phase, ransomware collects detail information about victim’s system. In preparation phase, it receives encryption key from C&C server if it is not in payload and starts looking for file for encryption. In Hijacking phase, this is the phase where ransomware starts encrypting files found in previous phase by using encryption key. In Extortion phase, the last phase of ransomware attack which starts after encryption is done and shows the message about attack and how to get your files back by paying ransom. We can also say that this is working life cycle of Ransomware attack.

![Diagram of Ransomware Phases](image)

In Ransomware attack, payments are done by using cryptocurrency that is bitcoin is used for collecting the ransom amount. Attacker creates new wallet each time that for every new attack and its identifier is send to victim for collecting the amount. After paying certain ransom amount victim receives decryption key to unlock its system. Command and control server(C&C) is nothing but a sever that is used by some type of ransomware to decide which files to be encrypted and sends encryption and decryption key to victim’s system. [1]