



RANSOMWARE: EVOLUTION, IMPACT, AND DEFENSE

DANIYAL HAIDER(13298)

ANAS KHALID(13465)



AGENDA

- What is Ransomware.
- The Evolution of Ransomware.
- Impact on Individuals.
- Impact on Organizations.
- Defense Strategies.
- Best Practices.
- Conclusion

WHAT IS RANSOMWARE?

- Ransomware is a type of malicious software that either locks your computer or encrypts your files so you can't access them. The attackers then demand a ransom, usually money, to unlock your files or system. Ransomware often spreads through phishing emails, unsafe downloads, or by taking advantage of security weaknesses in software.

THE EVOLUTION OF RANSOMWARE

- In the early 2000s, ransomware started with basic scams, like fake police warnings asking for small fines. In the 2010s, more dangerous types appeared, like CryptoLocker, which locked files using strong encryption. In 2017, huge attacks like WannaCry and NotPetya caused major global damage. Today, ransomware has become even more professional, with services for hire (Ransomware-as-a-Service) and new methods like stealing data before encrypting it.

IMPACT ON INDIVIDUALS

For individuals, ransomware can mean losing important photos, files, and memories. It can also lead to identity theft if personal information is stolen. Paying the ransom can be expensive, and even if you pay, there's no guarantee you will get your data back. Victims often feel stressed, frustrated, and helpless after an attack.

IMPACT ON ORGANIZATIONS

For companies and organizations, ransomware can shut down their operations for days or even weeks. They can lose millions of dollars in ransom, recovery, and legal costs. Their reputation can suffer badly, and they might face fines if they lose customer data under laws like GDPR or HIPAA. A well-known example is the Colonial Pipeline attack in 2021, which disrupted gas supplies across parts of the U.S.

DEFENSE STRATEGIES

To defend against ransomware, we need a three-part plan: prevention, detection, and response.

Prevention means training employees to spot phishing emails, keeping software updated, and splitting networks to stop ransomware from spreading.

Detection means keeping an eye on the system for anything strange and using threat intelligence tools.

Response means having backups ready and a team trained to act fast during an attack.

BEST PRACTICES

- Some of the best ways to stay safe are: keeping offline backups of important data, using strong passwords and two-factor authentication (MFA), encrypting sensitive files, and practicing how to respond to an attack with drills and training.

CONCLUSION

- Ransomware keeps changing and getting stronger, which means we have to stay ready and careful. A strong defense needs people, good processes, and the right technology working together. By staying informed and prepared, we can better protect ourselves and our data.



THANK YOU