RANSOMWARE: A PRIME CYBERSECURITY THREAT IN 2024

OVERVIEW, ACTORS, MODUS OPERANDI, AND MITIGATION

LUCÍA ROLDÁN LEÓN

WHAT IS RANSOMWARE?

- - Malicious software that encrypts data or locks systems, demanding payment for access.
- - Increasingly uses double extortion: encrypting data and threatening to leak it.

AFFECTED INFORMATION RESOURCES

- - Critical sectors: healthcare, financial services, and public infrastructure.
- - Broad target scope: from individuals to multinational organizations.

MODUS OPERANDI

- - Infiltration via phishing emails, malicious downloads, or software vulnerabilities.
- - Encryption of files and demand for cryptocurrency payments.
- - Use of Ransomware-as-a-Service (RaaS) for accessibility.

THREAT ACTORS

- - Financially motivated cybercriminals.
- - State-sponsored entities.
- - RaaS enabling less sophisticated attackers.

PROTECTION MEASURES

- - Multi-layered defenses: endpoint protection, backups, employee training.
- - Network segmentation and strict access controls.
- - Regular vulnerability assessments and patch management.
- - Collaboration with law enforcement and information sharing.