Regenerating a Controlled Environment for Analyzing Ransomware Behavior, Encryption, and Security Impact.

- A Practical Demonstration of RCE and Word Macro Exploits

Presented by :

Sai Sanjana Kambalapally – G01506405
Chaithra Reddy Pasunuru – G01475757
Sri Teja Kale – G01501801

WHAT IS A RANSOMWARE ?

Ransomware is a type of malware that encrypts files or locks systems and demands a ransom for decryption, typically in cryptocurrency.

Delivery methods often involve

- **phishing emails**
- **malicious macros** in Office files
- **remote code execution (RCE)** via known exploits (e.g., CVE-2017-0144, CVE-2017-0199)
- **exposed services** like SMB and RDP.
- **Ransomware-as-a-Service** (RaaS) has made attacks more accessible

ABSTRACT

This presentation demonstrates a simulated ransomware attack in a safe, isolated environment to study malware behavior, encryption mechanisms, and overall system impact. By leveraging a real-world remote code execution vulnerability and malicious Word macros, we analyze how ransomware can penetrate systems, encrypt user data, and demand ransom. The simulation emphasizes understanding attacker techniques and implementing effective defensive strategies.

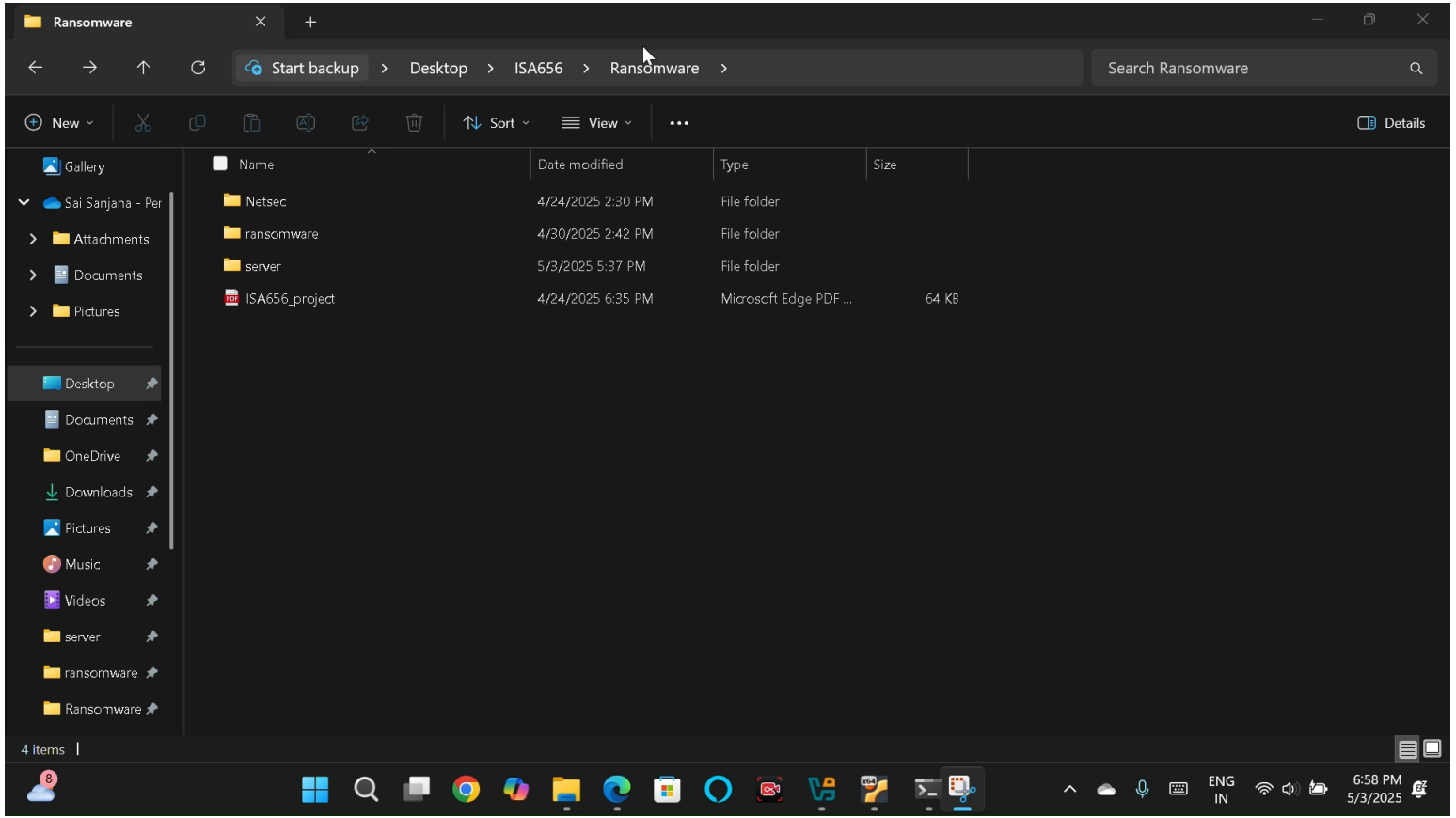
WHY WE CHOOSE THIS TOPIC ?

- Ransomware is the top cybersecurity threat across industries
- Healthcare, education, and government sectors are prime targets
- Real-world relevance with high-profile incidents (e.g., Locky, WannaCry, Ryuk)
- Combines multiple security domains: cryptography, networking, threat response.

REAL-WORLD CASE STUDY: LOCKY

- **Victim:** Hollywood Presbyterian Medical Center (2016)
- **Attack Vector:** Macro-enabled Word document via phishing
- **Result:** 10-day downtime, $17,000 ransom paid, >$100K indirect loss
- **Relevance:** Our simulation mirrors this structure

DEMONSTRATION



ENCRYPTION TECHNIQUES USED

- AES-CTR (stream cipher): efficient, used for file encryption
- RSA-2048: used for secure key exchange with attacker
- Why AES+RSA combo is common in modern ransomware ?
- File types targeted (.docx, .pdf, .png, .sql, etc.)

SECURITY IMPACT OF RANSOMWARE

- **Confidentiality:** Exfiltrated files may be leaked (double extortion)
- **Availability:** Systems locked, operations halted, backups destroyed
- **Integrity:** Data corrupted or overwritten, essential software disrupted
- **Trust & Compliance:** Legal penalties (HIPAA, GDPR); reputational loss

GENERAL RANSOMWARE DEFENSE TECHNIQUES

- Prevent Initial Access
- Detect Early-Stage Activity
- Limit Spread
- Prepare for Recovery
- Respond and Contain

CONCLUSION

- We successfully simulated a realistic ransomware scenario
- Demonstrated infection, encryption, ransom demand, and recovery
- Analyzed real-world relevance and countermeasures

THANK YOU !!
ANY QUESTIONS ???