Assignment 5

Ransomware Attack Analysis: Ryuk (2018–2020)

Overview

- **Targets**: Enterprises, governments, healthcare organizations .
- **Impact**: Paralyzed organizations by encrypting critical files (e.g., hospitals lost patient records) .

Technical Breakdown

1. Exploitation

- **Phishing Emails** : Attackers sent fake emails with malicious attachments (opening it triggers malware) .
- **Exploiting Weaknesses**: Used tools like TrickBot (another malware) to steal passwords .

2. Encryption Mechanism

- **Symmetric Encryption** : AES-256 to encrypt files (fast and efficient for bulk data).
- **Asymmetric Encryption** :
  - AES keys encrypted with RSA-4096 .
  - Private RSA key held by attackers, making decryption without payment infeasible.
- **Targeted File Types** :
  - Databases (e.g., SQL), backups, Office documents, and system files .

3. Lateral Movement

- **Techniques**:
  - Pass-the-Hash : Used stolen credentials to authenticate to other systems .
  - Windows Management Instrumentation (WMI) : Executed commands on remote machines.
- **Goals**:
  - Disable backups and security tools (e.g., antivirus).
  - Maximize impact by encrypting critical infrastructure.

4. Mitigation Strategies

1. **Phishing Defense**:

- Block macro-enabled Office files via email gateways.
- Train users to identify suspicious emails.

2. **Credential Hardening**:
   - Enforce multi-factor authentication (MFA) .
   - Regularly change admin passwords.
3. **Network Segmentation**:
   - Isolate critical systems (e.g., finance, backups) from general networks .
4. **Backup Best Practices**:
   - Maintain offline, immutable backups.
   - Test restoration processes quarterly.

Cyber Kill Chain Mapping

Stage	Ryuk Activities
Reconnaissance	Researched high-value targets (e.g., hospitals with weak security postures).
Weaponization	Embedded malicious code in Office docs; paired with TrickBot .
Delivery	Sent phishing emails to employees .
Exploitation	Triggered macros to execute payload; exploited unpatched Windows vulnerabilities.
Installation	Deployed Ryuk ransomware and established persistence connection .
Command & Control	Used encrypted C2 channels to exfiltrate data and relay ransom demands.
Actions on Objectives	Encrypted files, deleted backups, and demanded Bitcoin payments.