CYBER GYAN VIRTUAL INTERNSHIP PROGRAM

Centre for Development of Advanced Computing (CDAC), Noida

Submitted By:

Kamlesh Kumar

Project Trainee, (May-June) 2025

TOPIC NAME

Implementation and Detection of Ransomware Attacks

Techniques Used:

Behavioral Monitoring

Anomaly Detection (Machine Learning)

Signature-Based Detection (YARA)

Why Important?: Ransomware causes financial and operational damage.

PROBLEM STATEMENT

Challenge: Detect ransomware before significant damage.

- Issues with Existing Solutions:
- Slow detection of new variants.
- Reliance on outdated signatures.

Goal:

- Real-time monitoring of file system.
- Anomaly detection via CPU/file activity.
- Signature matching with YARA.

TECHNOLOGY/TOOLS TO BE USED

- Python, Tkinter (GUI)
  - watchdog (File Monitoring)
  - scikit-learn (Isolation Forest)
  - psutil (CPU Monitoring)
  - YARA (Signature Detection)
  - Infrastructure:
  - Single machine (Ubuntu, IP: 192.168.1.100)
  - Monitored directories: ~/Documents, /home/kamli/test_files
  - Architecture:

ABOUT THE ATTACK/TOPIC/PROBLEM STATEMENT

- Ransomware: Malicious software that encrypts files, demanding payment for access.
- Problem: Rapid, undetected attacks cause data loss and financial damage.
- Challenge: Existing solutions miss new variants or rely on outdated signatures.
- Goal: Develop a real-time detection system using behavioral, anomaly, and signature-based methods.
- Scope: Monitor file changes, CPU usage, and scan for known ransomware signatures.

WHAT ARE THE REASONS BEHIND THE PROBLEM(TELL ABOUT THE ISSUES WHY THIS PROBLEM/ATTACKS ARE HAPPENING)

- Sophisticated Malware: Ransomware variants evolve rapidly, evading traditional antivirus.
- Exploited Vulnerabilities: Unpatched software and weak passwords enable easy access.
- Phishing Attacks: Users unknowingly download malware via malicious emails or links.
- Lack of Awareness: Insufficient cybersecurity training leads to human errors.
- Profit Motive: High financial gains encourage cybercriminals to target organizations.
- Delayed Detection: Slow response times allow ransomware to encrypt critical data.

SUGGEST SOME POSSIBLE SOLUTIONS/COUNTERMEASURES

- Real-Time Monitoring: Deploy systems to track file changes and CPU usage instantly.
- Machine Learning: Use anomaly detection (e.g., Isolation Forest) to flag unusual behavior.
- Signature Detection: Scan files with YARA to identify known ransomware patterns.
- Regular Backups: Maintain offline backups to restore data without paying ransom.
- User Training: Educate users to avoid phishing emails and malicious links.
- Patch Management: Update software regularly to close vulnerabilities.

THANKYOU