Incident Report

FULL INCIDENT REPORT – RANSOMWARE INCIDENT

Summary:

Endpoint exhibited pre-encryption behaviour: mass file rename, PowerShell beaconing.

Timeline:

- 10:22 AM: Suspicious PowerShell launched
- 10:23 AM: LSASS access attempt blocked
- 10:25 AM: File rename spike detected
- 10:28 AM: Network beacon to 45.x.x.x on port 8443
- 10:30 AM: Host isolated by SOC

Root Cause:

User opened malicious attachment leading to remote access malware.

Actions Taken:

- Host isolated
- Sessions revoked
- Password reset
- Malware removed
- Forensic artefacts preserved

Lessons Learned:

Improve email filtering, enforce conditional access policies.