RANSOMWARE INCIDENT REPORT

Prepared by: Zakeria Daniels
Date: (Insert Today’s Date)

SUMMARY

A workstation became encrypted by ransomware. The user reported a ransom note and inaccessible files. Root cause identified as a malicious attachment executed via phishing email.

TIMELINE OF EVENTS

- 2:14 PM – User reported inability to open files
- 2:16 PM – Ransom note discovered on desktop
- 2:20 PM – Workstation isolated from network
- 2:30 PM – Malicious processes terminated
- 3:00 PM – System reimaged
- 4:00 PM – Data restored from offline backup

INDICATORS OF COMPROMISE (IOCs)

- Ransom note: READ_ME.txt
- Encrypted extensions: .locked, .enc
- Malicious PowerShell command executed
- Hash of ransomware binary (placeholder)
- Outbound traffic to C2 IP: 46.17.250.163

ACTIONS TAKEN

- Immediately isolated infected workstation
- Disabled associated user account
- Blocked malicious IPs and C2 domains
- Removed all ransomware executables
- Reimaged workstation
- Restored from clean backup

RECOVERY

- System rejoined to domain
- Verified no lateral movement occurred

- Monitored logs for 72 hours
- Reset and strengthened credentials

RECOMMENDATIONS

- Increase macro restrictions for Office files
- Conduct enterprise-wide patch review
- Deploy enhanced ransomware detection rules
- Add IOCs to SIEM watch lists