Orion Health Services

Ransomware Incident Investigation Report

Prepared by: Cybersecurity Analyst (Graduate)

Incident Type: Ransomware Attack

Severity: Critical

Executive Summary

On Monday morning, Orion Health Services experienced a ransomware attack resulting in system disruption and potential exposure of sensitive data. The attack originated from a phishing email containing a malicious Excel attachment sent to a finance team member. Credential harvesting tools were used, and multiple systems were encrypted.

Incident Timeline

Morning: Unusual outbound traffic detected

Midday: Employees locked out of systems

Afternoon: Ransom note discovered

Attack Vector

Initial access was achieved via phishing, followed by macro execution within an Excel file.

Indicators of Compromise

- Overseas IP login
- Mimikatz credential harvesting
- .orionlock encrypted files

Systems Affected

- File Server
- HR and Finance Systems
- Backup Server (partial encryption)

Compromised Data

- Employee payroll records
- Patient appointment schedules

- Internal credentials

Response Actions

Affected systems were isolated, compromised accounts disabled, and logs preserved for forensic analysis.

Recommendations

Implement MFA, enhance phishing training, improve backup resilience, and strengthen access controls.

Conclusion

This incident underscores the importance of layered security controls and user awareness within healthcare environments.