Security Operations Center (SOC) Incident Report

Incident Summary

Date & Time of Detection: January 1, 2025, 9:47 PM EST

Incident ID: INC-2025-0042

Incident Type: Ransomware Attack

Severity Level: Critical

Affected Systems: Corporate file servers, employee workstations, database servers

Incident Description: At approximately 9:47 PM, the SOC detected unusual file encryption activity on multiple corporate file servers. Employees reported receiving ransom notes demanding payment in Bitcoin to recover encrypted files. Further investigation revealed that an employee's workstation was the initial infection vector, leading to lateral movement across the network.

Root Cause Analysis (RCA)

Root Cause: The ransomware was introduced via a phishing email containing a malicious attachment disguised as an invoice. The email bypassed initial security checks, and an employee unknowingly executed the malware.

Attack Vector: Phishing email with an embedded malicious macro in a Word document.

Indicators of Compromise (IoCs):

- Malicious email sender: **billing@fakevendor.com**
- Malicious file hash: **7d3f5e4b8a9c1f6eabc456def1237890**
- Ransom note filename: **README_RECOVER_FILES.txt**
- C2 server IP: **192.168.56.22**

Detection & Analysis: The security monitoring system detected an anomaly when multiple workstations began encrypting files at an abnormal rate. The SOC team identified a connection to a known ransomware command-and-control (C2) server, confirming an active attack.

Mitigation & Remediation Steps

Immediate Response Actions:

- Isolated affected systems from the network to prevent further encryption.
- Blocked the malicious C2 server IP at the firewall level.
- Reset passwords for all compromised user accounts.
- Disabled affected user accounts pending investigation.

Remediation Steps:

- Restored affected systems from secure backups.
- Conducted a forensic analysis to identify the full extent of the compromise.
- Implemented stricter email filtering and attachment scanning policies.
- Deployed Endpoint Detection & Response (EDR) to detect similar future threats.
- Enhanced security awareness training for employees on phishing attacks.

Post-Incident Validation:

- Verified backup integrity and restoration procedures.
- Conducted a penetration test to ensure all vulnerabilities were mitigated.

Lessons Learned

Gaps Identified:

- Email filtering failed to catch the phishing attempt.
- Employees lacked awareness of the dangers of opening unsolicited attachments.
- Endpoint security controls did not detect the ransomware payload before execution.

Process Improvements:

- Strengthened email security policies by enabling sandboxing for attachments.
- Implemented user access controls to limit file modifications.
- Developed an internal ransomware response playbook.

Training Recommendations:

- Conduct simulated phishing exercises monthly.
- Require employees to complete cybersecurity awareness training annually.