# Incident Report: Ransomware Attack on Acme Financial Services

## Date of Incident:

March 10, 2025

## Reported By:

John Doe, SOC Analyst

## Incident Type:

Ransomware Attack

## Incident Severity:

Critical

## 1. Summary of the Incident

At 08:30 AM UTC on March 10, 2025, a phishing email containing a malicious attachment was opened by an employee at Acme Financial Services. By 08:45 AM, ransomware had executed and encrypted key business files, impacting financial records, HR data, and customer transactions. The attackers demanded 5 Bitcoin for decryption keys.

Immediate response efforts were initiated at 09:15 AM, isolating infected systems, and backup restoration began at 11:30 AM using offline snapshots from March 9, 2025. Full recovery was achieved by 04:00 PM, and a post-incident review was conducted to prevent future occurrences.

## 2. Incident Detection and Response Timeline

|  |  |
| --- | --- |
| Time (UTC) | Event |
| 08:30 AM | Employee opens phishing email and executes malicious attachment. |
| 08:45 AM | Ransomware encrypts key files. |
| 09:00 AM | SIEM detects unusual file modifications and network traffic anomalies. |
| 09:15 AM | SOC confirms encryption activity and activates Incident Response Team. |
| 09:45 AM | Security team isolates infected endpoints and disconnects affected servers. |
| 10:30 AM | Crisis communication team drafts internal advisory. |
| 11:30 AM | Backup restoration initiated using last clean snapshot. |
| 02:30 PM | Threat intelligence confirms attack linked to BlackCat ransomware group. |
| 04:00 PM | Systems fully restored, forensic analysis begins. |
| 06:00 PM | Security patches deployed, phishing awareness training initiated. |
| 07:00 PM | Final incident report submitted, regulatory authorities notified. |

## 3. Impact Assessment

Affected Systems: Financial transaction database, HR file server, Customer support systems

Downtime: 7.5 hours

Data Compromised: No confirmed exfiltration detected

Financial Impact: Estimated recovery cost: $250,000

## 4. Root Cause Analysis

Entry Point: Phishing email impersonating IT support

Attack Vector: Malicious email attachment executing ransomware payload

Security Gaps: Lack of MFA, delayed SIEM alerts, insufficient phishing awareness training

## 5. Containment and Mitigation Actions

Isolated infected endpoints and disabled compromised accounts.

Blocked C2 (command and control) communications from infected hosts.

Updated email filtering rules and enabled URL sandboxing.

## 6. Lessons Learned & Preventative Measures

Enforced MFA for all privileged accounts.

Implemented real-time alerting and automated response playbooks.

Increased backup frequency and integrity testing.

## 7. Conclusion

This ransomware attack was effectively mitigated due to prompt response efforts and structured incident handling. However, security improvements such as MFA enforcement, SIEM tuning, and user training are critical to preventing future incidents.