

Incident Response Plan

Organization: VATI Financial Services

Incident Title: Ransomware Attack on VATI Financial Services

Date of Incident: Monday, February 17, 2025

Incident Reported By: Muritala Ajarat

Incident Coordinator: Miss Esther

1. Incident Description

VATI Financial Services has been hit by a ransomware attack that encrypts employee files, leaving a ransom note demanding 50 Bitcoin for decryption. Unauthorized access was detected from an unfamiliar IP address, and SIEM logs indicate mass file encryption. The ransomware exploited an unpatched vulnerability in the company's file-sharing server, spreading internally and affecting backup systems.

2. Incident Response Steps

Phase 1: Preparation

- Ensure IR team is trained in handling ransomware incidents.
- Verify availability of recent, isolated backups.
- Conduct regular security awareness training for employees.

Phase 2: Identification

- Indicator of compromise
- Files renamed with "locked" extension.
- Presence of ransom note demanding Bitcoin.
- Unauthorized remote access logs.
- SIEM alerts for unusual file modifications.
- Unusual outbound network traffic to an external server.
- Confirm attack timeline and scope through forensic analysis.

Phase 3: Containment

- **Short-Term Containment:**
 - Disconnect infected systems from the network.
 - Disable compromised accounts.
 - Block malicious IP addresses and domains.

- **Long-Term Containment:**

Patch the exploited vulnerability.

Restrict access to critical systems.

Implement enhanced monitoring.

Phase 4: Eradication

- Remove malware from infected systems.
- Scan all endpoints for dormant threats.
- Update security configurations and firewalls.

Phase 5: Recovery

- Restore affected systems from secure backups.
- Validate system integrity before reconnecting to the network.
- Monitor systems for signs of reinfection.

Phase 6: Lessons Learned

- Conduct a post-incident review to improve future response.
- Implement additional security measures.
- Update and test the Incident Response Plan regularly.

Post-Incident Report

1. Summary of Incident

On Monday, February 17, 2025, VATI Financial Services suffered a ransomware attack that encrypted critical files and backups. Attackers demanded 50 Bitcoin for decryption, and analysis confirmed the infection was due to a phishing email containing a malicious attachment.

2. Timeline of Events

Date & Time	Event Description
Monday, February 10, 2025	Phishing email received by multiple employees.
Wednesday, February 12, 2025	Some employees unknowingly open the malicious attachment.
Saturday, February 15, 2025	Malware remains dormant until activation over the weekend.
Sunday, February 16, 2025	Mass encryption of files and ransom note delivery.
Monday, February 17, 2025	Incident identified, and containment initiated.
Tuesday, February 18, 2025	Eradication and system recovery efforts executed.
Wednesday, February 19, 2025	Security measures reinforced, post-incident analysis conducted.

3. Root Cause Analysis

- **Cause:** Employees opened a phishing email containing a ransomware payload.
- **Security Gaps Identified:**
 - Lack of email filtering and phishing awareness.
 - Unpatched file-sharing server exploited.
 - Insufficient network segmentation.

4. Impact on Organization

- **Operational Disruptions:** Employees unable to access critical files.
- **Financial Loss:** Potential costs for recovery and security enhancements.
- **Reputation Damage:** Loss of customer trust due to security breach.

5. Recommendations for Future Prevention

1. **Strengthen Email Security Measures:** Implement advanced phishing filters and conduct regular employee training.
2. **Patch and Update Systems Promptly:** Ensure all vulnerabilities are addressed in a timely manner.
3. **Implement Stronger Access Controls:** Enforce multi-factor authentication (MFA) and limit administrative privileges.
4. **Enhance Backup Security:** Maintain offline backups and test recovery procedures.
5. **Deploy Network Segmentation:** Restrict access between critical systems to contain potential threats.

6. Conclusion

The ransomware attack on VATI Financial Services highlighted critical security gaps that have since been addressed through improved training, system updates, and network security measures. Moving forward, the company will continuously enhance its cybersecurity posture to prevent similar incidents.