INCIDENT RESPONSE PLAN

Incident: Ransomware Attack on VATI Financial Services

Date: 05/03/2025- 08/03/2025

Recorded By: Oluwatobiloba Alaadejare

Recorded Information and Events

Event	Detail
Incident Description	VATI Financial Services experienced a ransomware attack affecting employee systems. The ransomware encrypted files and renamed them a ".locked" extension, rendering them inaccessible. A ransom note demanding 50 Bitcoin appeared on infected systems, and the attacker threatens to permanently delete files within 72 hours unless payment is made.
Indicators of Compromise (IoCs):	Renamed files with a ".locked" extension. Presence of a ransom note on infected systems demanding Bitcoin. Unauthorized remote access from unfamiliar IP addresses. Unusual file modifications and mass encryption activity in logs. High outbound network traffic to an external server.
Identification of Malware	Verify that the attack is a ransomware attack. Review the SIEM logs to identify the scope of the ransomware attack, including systems affected and unusual activities. Conduct network traffic analysis to understand the data exfiltration and communication with the attacker Collect IoCs:List all IoCs, including file extensions (.locked), IP addresses associated with the attack. Tools:

	● SIEM (Security Information and Event Management) tools ● Endpoint detection and response (EDR) solutions ● Network traffic monitoring tools
Containment	Immediately isolate infected systems from the network to prevent further spread and encryption of files. Separate critical systems and backups from the rest of the network to reduce the potential impact of the ransomware. Use firewall rules to block unauthorized remote access from the unfamiliar IP addresses identified in the logs. Tools: ● Network segmentation tools ● Firewalls ● Endpoint isolation tools
Eradication	Conduct a thorough search for the ransomware payload on all affected systems. Remove any identified ransomware files or scripts to ensure they cannot activate again. Patch the unpatched vulnerability in the file-sharing server that allowed the ransomware to spread. Use antivirus or endpoint detection tools to scan all infected systems and confirm complete removal of the ransomware. Tools: ● Antivirus/antimalware solutions ● Vulnerability scanning tools

Recovery	Try decrypting backups with available tools. Rebuild infected systems from a known good state. Closely monitor the systems after recovery to detect any signs of the ransomware reappearing or further unauthorized activities. Gradually reintegrate systems back into the network once confirmed to be free from malware. Tools: ● Backup restoration tools ● System monitoring tools
Lessons	Conduct a meeting with the incident response team, IT, and other stakeholders to evaluate the response process. Identify gaps in the incident response process and areas for improvement. Conduct training for employees on how to recognize phishing emails and suspicious attachments to reduce the likelihood of future attacks. Implement multi-factor authentication (MFA). Regularly patch all systems and software to prevent exploitation of known vulnerabilities. Conduct regular vulnerability assessments. Resources: ● Internal documentation ● Incident review meetings ● Employee training programs

Communication	Immediately stakeholders,IT, legal, and compliance teams, of the attack's scope and impact. Keep affected employees informed about the ongoing response efforts and instructions for system recovery. Notify relevant regulatory authorities Send notifications to clients or customers if personal data was potentially compromised, outlining actions taken and any assistance they may require.
Documentation	Maintain detailed logs of every step taken during the incident, including actions to contain, eradicate, and recover from the attack. Estimate the financial impact of the attack, downtime costs, and recovery expenses. Tools: ● Incident tracking tools ● Financial reporting tools